Phụ lục

Bộ tiêu chí đánh giá các tiêu chuẩn về chính sách quản lý, vận hành, khai thác cung cấp dịch vụ đối với hình thức ký số từ xa theo quy định tại Thông tư số 16/2019/TT-BTTTT

(Kèm theo Hướng dẫn các bước xin cấp phép cung cấp dịch vụ chứng thực chữ ký số để triển khai dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa của Trung tâm Chứng thực điện tử quốc gia)

STT	Tham Chiếu	Chi tiết	Mô tả đáp ứng	Kết quả
1	**Quy trình quản lý rủi ro**			
1.1	REQ-5-01 EN 119 431-1	CA sẽ thực hiện đánh giá rủi ro để xác định, phân tích và đánh giá rủi ro dịch vụ tin cậy có tính đến các vấn đề kinh doanh và kỹ thuật.	1. Quyết định ban hành quy trình quản lý rủi ro đã được phê duyệt. 2. Quy trình quản lý rủi ro được phê duyệt: có đầy đủ tên, mã hiệu, ngày ban hành, ngày sửa đổi, người soạn thảo, người phê duyệt. 3. Hồ sơ đánh giá rủi ro gần nhất. 4. Báo cáo rủi ro phải có. - Nhận diện rủi ro. - Đánh giá rủi ro. - Kế hoạch xử lý rủi ro. - Xem xét rủi ro. - Hạ cấp rủi ro. 5. Báo cáo đánh giá rủi ro phải được phê duyệt của lãnh đạo đơn vị đảm bảo. - Chấp nhận rủi ro. - Kế hoạch xử lý rủi ro cụ thể. 6. Rủi ro phải được xem xét tối thiểu 1 năm một lần bởi lãnh đạo đơn vị.	Đối với các CA đã có quy trình quản lý rủi ro và đi vào hoạt động được hơn 01 năm thì phải đáp ứng tất cả các tiêu chí hiện có cho Quy trình quản lý rủi ro. Nếu không thì tối thiểu phải đạt được các tiêu chí sau: 1. Quyết định ban hành quy trình quản lý rủi ro đã được phê duyệt. 2. Quy trình quản lý rủi ro được phê duyệt: có đầy đủ tên, mã hiệu, ngày ban hành, ngày sửa đổi, người soạn thảo, người phê duyệt. 3. Quy chế/ chính sách ATTT cần phủ được các vùng rủi ro.

1.2	REQ-5-02 EN 119 431-1	CA phải lựa chọn các biện pháp xử lý rủi ro thích hợp, có tính đến kết quả đánh giá rủi ro. Các biện pháp xử lý rủi ro phải đảm bảo rằng mức độ an toàn tương xứng với mức độ rủi ro ..	1. Kiểm tra báo cáo rủi ro. - Nhận diện rủi ro. - Đánh giá rủi ro. - Kế hoạch xử lý rủi ro. - Xem xét rủi ro. - Hạ cấp rủi ro. 2. Báo cáo đánh giá rủi ro phải được phê duyệt của lãnh đạo đơn vị đảm bảo. - Chấp nhận rủi ro. - Kế hoạch xử lý rủi ro cụ thể.	- Con người (tuyển dụng, đào tạo, thuyên chuyển, tạm nghỉ, nghỉ việc). - Quy trình (phát triển, thiết kế, vận hành, bảo trì bảo dưỡng). - Công nghệ (phát triển, thiết kế, vận hành, bảo trì bảo dưỡng). ☐ Đạt ☐ Không đạt
1.3	REQ-5-03 EN 119 431-1	CA phải xác định tất cả các yêu cầu bảo mật và quy trình hoạt động cần thiết để thực hiện các biện pháp xử lý rủi ro đã chọn, như được ghi trong chính sách bảo mật thông tin và quy chế cung cấp dịch vụ	Quy chế/ chính sách ATTT cần phủ được các vùng rủi ro. - Con người (tuyển dụng, đào tạo, thuyên chuyển, tạm nghỉ, nghỉ việc). - Quy trình (phát triển, thiết kế, vận hành, bảo trì bảo dưỡng). - Công nghệ (phát triển, thiết kế, vận hành, bảo trì bảo dưỡng).	
1.4	REQ-5-04 EN 119 431-1	Việc đánh giá rủi ro phải được thường xuyên xem xét và sửa đổi.	Kết quả đánh giá rủi ro phải được thống kê và có biện pháp khắc phục tối thiểu 1 năm một lần và được phê duyệt lãnh đạo đơn vị.	
1.5	REQ-5-05 EN 119 431-1	Ban lãnh đạo của CA sẽ phê duyệt việc đánh giá rủi ro và chấp nhận rủi ro còn lại đã được xác định.	Báo cáo đánh giá rủi ro phải được phê duyệt của lãnh đạo đơn vị đảm bảo. - Chấp nhận rủi ro. - Kế hoạch xử lý rủi ro cụ thể.	

2	**Quy trình quản lý an toàn thông tin**			
2.1	REQ-6.3-01 EN 119 431-1 Theo ISO 27001	CA cần phải xác định các chính sách bảo mật thông tin được ban lãnh đạo phê duyệt và đưa ra phương pháp tiếp cận của tổ chức để quản lý an toàn thông tin.	- Quyết định ban hành quy trình quản lý an toàn thông tin đã được phê duyệt. - Tài liệu SOA tuyên bố đáp ứng đảm bảo an toàn thông tin theo các quy định + QT ATTT nội bộ, từ xa + QT ATTT nguồn nhân lực (tuyển dụng, đào tạo, thuyên chuyển, tạm nghỉ, nghỉ việc) + QT QUẢN LÝ tài sản thông tin (trách nhiệm, phân loại) + QT quản lý truy cập (truy cập mạng, ứng dụng, vật lý) + QT quản lý mã hóa (quản lý mật mã CMS, quản lý mật mã vận hành) + QT quản lý AT vật lý và môi trường + QT quản lý vận hành + Quản lý các điểm yếu kỹ thuật + AT quản lý trao đổi thông tin + Tiếp nhận phát triển và duy trì hệ thống thông tin + An toàn trong quản lý đối tác và bên thứ ba + Xử lý sự cố an toàn thông tin + Đảm bảo tính liên tục của hệ thống - Kiểm tra kênh thông tin của CA, chứng thư số SSL nếu công bố thông tin qua trang web.	Đối với quy trình quản lý an toàn thông tin của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt ê. ☐ Đạt ☐ Không đạt
2.2	REQ-6.3-02 EN 119 431-1	Các thay đổi đối với chính sách bảo mật thông tin sẽ được thông báo cho cơ quan quản lý nhà nước (nếu có theo Thông tư 17/2014/TT-BTTTT). Điều này bao gồm những người đăng ký,	Changelog về chính sách bảo mật thông tin được công bố cho cơ quan quản lý nhà nước liên quan bao gồm ở mục bên	

		bên phụ thuộc, cơ quan đánh giá, cơ quan giám sát hoặc cơ quan quản lý khác.		
2.3	REQ-6.3-03 EN 119 431-1	CA cần phải có các biện pháp kiểm soát và quy trình vận hành cho các cơ sở sở dữ liệu, nơi đặt hệ thống và tài sản thông tin cung cấp dịch vụ.	Các chính sách an toàn thông tin, chính sách sửa đổi bổ sung, duy trì, biện pháp kiểm soát, quy trình vận hành của cơ sở, hệ thống, tài sản cung cấp dịch vụ cần có quyết định ban hành kèm theo.	
2.4	EQ-6.3-04 EN 119 431-1	CA phải công bố và trao đổi về các chính sách bảo mật thông tin cho tất cả nhân viên nằm trong diện ảnh hưởng bởi chính sách đó.	- Tài liệu chứng minh ban hành chính sách an toàn thông tin nội bộ của tổ chức. - Tài liệu đào tạo an toàn thông tin là bằng chứng một phần của chương trình đào tạo đối với các cá nhân nằm trong diện ảnh hưởng bởi chính sách.	
2.5	EQ-6.3-05 EN 119 431-1	CA phải chịu trách nhiệm chung về việc tuân thủ các thủ tục/quy trình được quy định trong chính sách an toàn thông tin, kể cả các chức năng của CA do RA hoặc đối tác đảm nhận.	- Tài liệu ban hành chính sách an toàn thông tin nội bộ của tổ chức bao gồm nội dung quản lý ATTT với đối tác nhà cung cấp. - Nội dung của chính sách an toàn thông tin phải thể hiện CA chịu trách nhiệm chung về việc tuân thủ các thủ tục/quy trình được quy định.	
2.6	EQ-6.3-06 EN 119 431-1	CA phải xác định trách nhiệm của RA, đối tác và đảm bảo rằng RA, đối tác có nghĩa vụ thực hiện bất kỳ biện pháp kiểm soát nào theo yêu cầu của CA.	Kiểm tra hợp đồng cam kết để xác định vai trò, trách nhiệm của 02 bên. (Thông tư 31/2020/TT-BTTTT)	

2.7	REQ-6.3-07 EN 119 431-1	Chính sách an toàn thông tin của CA và việc kiểm kê tài sản để bảo mật thông tin sẽ cần xem xét theo các khoảng thời gian đã được lên kế hoạch hoặc nếu có những thay đổi quan trọng để đảm bảo tính phù hợp, đầy đủ và hiệu quả liên tục	Chính sách quản lý tài sản, định kỳ kiểm tra theo thời gian đã được quy định trong chính sách để đảm bảo những sự thay đổi đều được cập nhật liên tục và đầy đủ	
2.8	REQ-6.3-08 EN 119 431-1	Mọi thay đổi ảnh hưởng tới mức độ an toàn thông tin (thiết bị bảo mật, con người, đối tác trực tiếp liên quan đến hệ thống an toàn thông tin) phải được chấp thuận bởi ban lãnh đạo	Văn bản thay đổi ảnh hưởng tới mức độ an ninh cần được ban lãnh đạo phê duyệt chấp thuận. Kiểm tra bằng chứng chứng minh kết quả phê duyệt thay đổi (nếu có).	
2.9	REQ-6.3-09 EN 119 431-1	Cấu hình của hệ thống CA phải được kiểm tra thường xuyên để đảm bảo không có những vi phạm chính sách bảo mật của CA.	- Định kỳ kiểm tra cấu hình an ninh hệ thống của CA đáp ứng các yêu cầu về chính sách bảo mật được CA đưa ra. - Tài liệu chứng minh việc kiểm tra định kỳ đối với cấu hình của hệ thống CA như: Biên bản kiểm tra, kết quả kiểm tra, quyết định khắc phục liên quan đến những chính sách bảo mật bị vi phạm. (Nếu có)	
2.10	REQ-6.3-10 EN 119 431-1	Khoảng thời gian tối đa giữa hai lần kiểm tra phải được ghi lại trong tuyên bố dịch vụ	Quy định về thời gian tối đa giữa 2 lần kiểm tra phải được ghi trong quy trình quản lý ATTT của CA.	

3	**Quy trình quản lý tài sản**			
3.1	REQ-7.3.1-01 EN 119 431-1	CA phải đảm bảo mức độ bảo vệ thích hợp đối với tài sản của mình bao gồm cả tài sản thông tin.	Quy trình quản lý tài sản có quy định mức độ bảo vệ thích hợp (Phân theo cấp độ hệ thống thông tin) của CA bao gồm cả tài sản thông tin, tài sản phần cứng và tài sản phần mềm.	Đối với quy trình quản lý tài sản của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt
3.2	REQ-7.3.1-02 EN 119 431-1	CA phải duy trì một bản kiểm kê của tất cả các tài sản thông tin và phải phân loại phù hợp với đánh giá rủi ro	- Danh sách tài sản thông tin đã được phân loại phù hợp với tiêu chí đánh giá rủi ro (Phân theo cấp độ hệ thống thông tin). - Tài sản phải được kiểm kê hàng năm và có bảng thống kê cụ thể.	
3.3	REQ-7.3.2-01 EN 119 431-1	Tất cả các phương tiện phải được xử lý an toàn theo các yêu cầu của sơ đồ phân loại thông tin. - Phương tiện chứa dữ liệu nhạy cảm phải được xử lý an toàn khi không còn cần thiết . - Đặc biệt: CA phải duy trì một bản kiểm kê của tất cả các tài sản thông tin và phải phân loại phù hợp với việc đánh giá rủi ro.	Giải pháp xử lý dữ liệu an toàn khi không còn cần thiết (không sử dụng, chuyển đổi mục đích sử dụng, huỷ dữ liệu) Tài liệu chứng minh các thiết bị không còn cần thiết đã không còn sử dụng hoặc dữ liệu bên trong đã bị huỷ (Nếu có).	
3.4	REQ-7.3.1-02 EN 119 431-1	Đặc biệt: CA phải duy trì một bản kiểm kê của tất cả các tài sản thông tin và phải phân loại phù hợp với việc đánh giá rủi ro.	Danh sách tài sản thông tin được phân loại phù hợp với quy trình quản lý rủi ro đã được mô tả (Phân theo cấp độ hệ thống thông tin).	

4	**Chính sách an toàn vật lý**			
4.1	REQ-7.6-01, ETSI EN 319 401 [2018]	CA cần kiểm soát quyền truy cập vật lý vào các thành phần của hệ thống CA có tính bảo mật quan trọng đối với việc cung cấp các dịch vụ và giảm thiểu rủi ro liên quan đến bảo mật vật lý	- Lối vào tòa nhà chính, nơi đặt thiết bị của CA như Trung tâm dữ liệu, Máy chủ PKI và các thiết bị Mạng và lối vào mỗi khu vực an ninh sẽ được quay video suốt ngày đêm. Việc lưu log phải được xem xét kỹ lưỡng và duy trì ít nhất một năm. - Hệ thống an ninh truy cập vật lý sinh trắc học phải được cài đặt để kiểm soát và kiểm tra việc truy cập vào địa điểm hoạt động. - Luôn có màn hình giám sát sự xâm nhập trái phép thông qua hệ thống camera. - Khu vực lễ tân luôn có nhân viên tiếp nhận để kiểm soát truy cập vật lý vào hệ thống của CA. - Hệ thống kiểm soát truy cập phải được cài đặt để kiểm soát và kiểm tra thông tin chi tiết của nhân viên sử dụng Hệ thống. - Việc kiểm kê thẻ truy cập sẽ được CA duy trì và được xem xét định kỳ. - Danh sách cập nhật nhân sự có thẻ / chìa khóa sẽ được duy trì và lưu trữ thường xuyên trong thời gian ba năm. Việc mất thẻ / chìa khóa truy cập sẽ được báo cáo ngay lập tức cho Quản trị viên bảo đảm an toàn thông tin hệ thống. - Hệ thống báo động và phát hiện xâm nhập phải được lắp đặt ở mọi lớp bảo mật với nguồn điện dự phòng đầy đủ có khả năng tiếp tục hoạt động ngay cả trong trường hợp mất nguồn điện chính.	Đối với chính sách an toàn vật lý của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt

			- Nhật ký truy cập sẽ được duy trì tại địa điểm hoạt động của CA và được kiểm tra định kỳ. Tất cả nhân viên ra vào các cơ sở hoạt động của CA phải được ghi nhật ký. - Hệ thống phát hiện xâm nhập sẽ được sử dụng để giám sát và ghi lại các truy cập vật lý vào hệ thống Chứng thực Chữ ký Số trong và sau giờ hành chính.	
4.2	REQ-7.6-02, ETSI EN 319 401 [2018]	Quyền truy cập vật lý vào các thành phần của hệ thống CA có tính bảo mật quan trọng đối với việc cung cấp các dịch vụ sẽ được giới hạn cho các cá nhân được ủy quyền.	Giới hạn quyền truy cập vật lý đối với các cá nhân được ủy quyền (Bảng nhân sự quản trị hệ thống CA, ai có quyền truy cập bằng cách kiểm tra trên hệ thống cửa từ, thẻ từ): - Các nhân viên có tên cụ thể sẽ chịu trách nhiệm vận hành, cũng như bố trí vật lý thực tế tại trung tâm dữ liệu 24/7. - Tất cả nhân viên của CA phải được xác minh danh tính và được uỷ quyền trước khi họ được đưa vào danh sách truy cập để truy cập thực tế vào hệ thống. Tất cả nhân viên phải đeo thẻ để ra vào hệ thống. - Quyền truy cập vật lý vào hệ thống của CA nên được giới hạn cho những cá nhân được ủy quyền, được bảo vệ thông qua các chu trình an ninh hạn chế và sẽ được vận hành dưới sự kiểm soát của nhiều người (ít nhất là giám sát kép). - Quyền truy cập sẽ bị giới hạn đối với từng cá nhân theo danh sách truy cập. - Bất kỳ nhân viên nào không có trong danh sách tiếp cận hệ thống sẽ phải ra khỏi khuôn viên hệ thống. Tất cả các cá	

			nhân, không phải là nhân viên vận hành, phải đăng nhập và đăng xuất khỏi địa điểm vận hành và sẽ có nhân viên vận hành đi cùng. - Quyền truy cập vào các thành phần cơ sở hạ tầng thiết yếu cho hoạt động của CA như bảng điều khiển nguồn, cơ sở hạ tầng truyền thông, hệ thống chứng nhận chữ ký số, hệ thống cáp, v.v. sẽ bị hạn chế đối với nhân viên có thẩm quyền. - CA phải đảm bảo rằng không một cá nhân nào có thể có quyền truy cập vào hệ thống duy trì tất cả thông tin liên quan đến việc tạo, phát hành và quản lý chứng thư số cũng như khóa bí mật của CA. Tối thiểu từ 2 cá nhân trả lên mới có thể truy cập bằng thẻ từ và sinh trắc học.	
4.3	REQ-7.6-03, ETSI EN 319 401 [2018]	Các biện pháp kiểm soát phải được thực hiện để tránh mất mát, hư hỏng hoặc xâm nhập tài sản và gián đoạn hoạt động kinh doanh.	- Lối vào tòa nhà chính, nơi đặt thiết bị của CA như Trung tâm dữ liệu, Máy chủ PKI và các thiết bị Mạng và lối vào mỗi khu vực an ninh sẽ được quay video suốt ngày đêm. Việc lưu log phải được xem xét kỹ lưỡng và duy trì ít nhất một năm. - Hệ thống an ninh truy cập vật lý sinh trắc học phải được cài đặt để kiểm soát và kiểm tra việc truy cập vào địa điểm hoạt động. - Luôn có màn hình giám sát sự xâm nhập trái phép thông qua hệ thống camera. - Khu vực lễ tân luôn có nhân viên tiếp nhận để kiểm soát truy cập vật lý vào hệ thống của CA.	

			- Hệ thống kiểm soát truy cập phải được cài đặt để kiểm soát và kiểm tra thông tin chi tiết của nhân viên sử dụng Hệ thống. - Việc kiểm kê thẻ truy cập sẽ được CA duy trì và được xem xét định kỳ. - Nhật ký truy cập sẽ được duy trì tại địa điểm hoạt động của CA và được kiểm tra định kỳ. Tất cả nhân viên ra vào các cơ sở hoạt động của CA phải được ghi nhật ký.	
4.4	REQ-7.6-04, ETSI EN 319 401 [2018]	Các thành phần quan trọng đối với hoạt động an toàn của dịch vụ tin cậy phải được đặt trong một vành đai an ninh được bảo vệ với bảo vệ vật lý chống lại sự xâm nhập, kiểm soát truy cập thông qua vành đai an ninh và báo động để phát hiện xâm nhập.	Phân tách hệ thống thành các vùng "secure zone" kết hợp các biện pháp bảo vệ để giảm thiểu thiệt hại, tránh mất mát, xâm phạm vào các tài sản và gián đoạn hoạt động kinh doanh (Hệ thống CA nằm tách biệt ví dụ quây lồng, cửa bảo vệ)	
4.5	REQ-7.6-05, ETSI EN 319 401 [2018]	Các biện pháp kiểm soát phải được thực hiện để tránh xâm phạm hoặc đánh cắp thông tin và các phương tiện xử lý thông tin.	- Danh sách cập nhật nhân sự có thẻ / chìa khóa sẽ được duy trì và lưu trữ thường xuyên trong thời gian ba năm. Việc mất thẻ / chìa khóa truy cập sẽ được báo cáo ngay lập tức cho Quản trị viên bảo đảm an toàn thông tin hệ thống. - Nhật ký truy cập sẽ được duy trì tại địa điểm hoạt động của CA và được kiểm tra định kỳ. Tất cả nhân viên ra vào các cơ sở hoạt động của CA phải được ghi nhật ký. - Hệ thống phát hiện xâm nhập sẽ được sử dụng để giám sát và ghi lại các truy cập vật lý vào hệ thống Chứng thực Chữ ký Số trong và sau giờ hành chính.	

5	**Chính sách quản lý thủ tục**			
5.1	REQ-7.4-04 ETSI EN 319 401	CA sẽ quản lý quyền truy cập của người dùng của các nhà khai thác, quản trị viên và kiểm toán viên hệ thống.	Quy trình quản lý quyền truy cập, quyền truy cập phải có một số nội dung cơ bản sau: - Nhân sự truy cập phải được khai báo và xét duyệt trước 01 ngày để truy cập hệ thống. - Nhân sự khi vào hệ thống cần xuất trình giấy tờ định danh để đối chiếu với bản photo đã nộp từ khi khai báo và hoàn thiện các thủ tục cần thiết trước khi truy cập. - Mỗi nhân sự truy cập hệ thống phải có thẻ truy cập. - Sau khi ra khỏi hệ thống phải trả thẻ truy cập và nhận lại giấy tờ định danh. Ngoài ra, đối với phần mềm hệ thống, mỗi nhân viên sẽ được cấp tài khoản riêng và được phân quyền để truy cập.	Đối với chính sách quản lý thủ tục của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt
5.2	REQ-7.4-05 ETSI EN 319 401	Việc quản lý sẽ bao gồm quản lý tài khoản người dùng và sửa đổi hoặc loại bỏ quyền truy cập kịp thời.	- CA sẽ có quyền quản lý người dùng, phân quyền, loại bỏ quyền truy cập khi nhân sự chịu trách nhiệm nghỉ phép hoặc không còn nắm giữ vai trò trong hệ thống.	
5.3	REQ-7.4-06 ETSI EN 319 401	Quyền truy cập vào thông tin và các chức năng của hệ thống ứng dụng sẽ bị hạn chế theo chính sách kiểm soát truy cập.	Chính sách kiểm soát truy cập (Chính sách ATTT của Công ty): - CA phải kiểm soát và hạn chế được quyền truy cập hệ thống đối với từng vai đã được phân quyền.	

5.4	REQ-7.4-07 ETSI EN 319 401	Hệ thống của CA phải cung cấp đủ các biện pháp kiểm soát bảo mật máy tính để tách các vai trò đáng tin cậy được xác định trong các hoạt động của CA, bao gồm cả việc tách biệt các chức năng quản trị và vận hành bảo mật. Đặc biệt, việc sử dụng các chương trình tiện ích hệ thống sẽ bị hạn chế và bị kiểm soát.	Có danh sách máy tính/ứng dụng/tiện ích nằm trong chính sách/quy định. Có biện pháp kiểm soát đối với các ứng dụng/tiện ích bị hạn chế: - Danh sách các thiết bị, chương trình được cài đặt trong hệ thống phải được cập nhật thường xuyên và có báo cáo đến cơ quan quản lý để cập nhật tình trạng hệ thống. - Báo cáo thay đổi Danh sách thiết bị hoặc nhân sự theo báo cáo đột xuất theo TT17/2014/TT-BTTTT (nếu có)	
5.5	REQ-7.4-08 ETSI EN 319 401	Nhân sự của CA phải được xác minh và xác thực trước khi sử dụng các ứng dụng quan trọng liên quan đến dịch vụ.	- Nhân sự phải khai báo, được chấp nhận, và cung cấp giấy tờ định danh để xác thực. Ngoài ra để truy cập hệ thống cần các yếu tố xác thực đa yếu tố.	
5.6	REQ-7.4-09 ETSI EN 319 401	Nhân sự của CA phải chịu trách nhiệm về các hoạt động của họ.	- Điều khoản trách nhiệm nhân viên của CA đối với các hoạt động (hợp đồng hoặc cam kết của nhân viên ký với công ty): được quy định trong hợp đồng hoặc cam kết trong quy định trách nhiệm nhân sự.	
6	**Quy trình quản lý nhân sự**			
6.1	REQ-7.2-01 ETSI EN 319 401	CA phải đảm bảo rằng các nhân viên và nhà thầu hỗ trợ mức độ đáng tin cậy trong hoạt động của CA.	Danh sách nhân sự, RA được kiểm tra kỹ càng và cam kết mức độ tin cậy trong các hoạt động liên quan tới CA (Danh sách các bên thứ 3 cung cấp cho CA, nhân sự đầu mối). - Danh sách nhân sự gồm 4 vai và phân rõ trách nhiệm của từng vị trí: vận hành hệ thống, cấp chứng thư số, đảm bảo ATTT hệ thống, kiểm toán viên hệ thống (nv kiểm soát, thống kê hệ thống),	Đối với quy trình quản lý nhân sự của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê ☐ Đạt ☐ Không đạt

			đối với các nhân sự này cần có các yếu tố sau: + Các nhân sự có bằng TN đại học trở lên chuyên ngành: ĐTVT, ATTT, CNTT + Hợp đồng lao động còn thời hạn. + Sơ yếu lí lịch của các nhân sự: Có chứng thực chữ ký của người kí - Đối với RA: + HĐ đại lý theo TT31/2020/TT-BTTTT còn thời hạn. +ĐKKD thay đổi lần gần nhất của đại lý	
6.2	REQ-7.2-02 ETSI EN 319 401	CA phải tuyển dụng nhân viên và các nhà thầu phụ (nếu có) những người có chuyên môn, độ tin cậy, kinh nghiệm và trình độ chuyên môn cần thiết và đã được đào tạo về các quy tắc bảo mật và bảo vệ dữ liệu cá nhân phù hợp với các dịch vụ được cung cấp và chức năng công việc.	Tài liệu chứng minh việc đào tạo nhân sự đối với từng vai trò trong hệ thống. - Phỏng vấn trực tiếp đối với các nhân sự được phân vai theo tài liệu đào tạo của CA.	
6.3	REQ-7.2-03 ETSI EN 319 401	Nhân sự của CA phải có khả năng đáp ứng yêu cầu về "kiến thức chuyên môn, kinh nghiệm và trình độ chuyên môn" thông qua đào tạo chính thức và chứng chỉ hoặc kinh nghiệm thực tế, hoặc kết hợp cả hai.	Danh sách thông tin các chứng chỉ, chứng nhận cho trình độ chuyên môn, kinh nghiệm cần thiết của các nhân viên chứng minh (tương đương) đã được đào tạo về các quy tắc, tiêu chuẩn bảo mật bảo vệ dữ liệu cá nhân phù hợp với các dịch vụ được cung cấp và chức năng công việc	

6.4	REQ-7.2-04 ETSI EN 319 401	Các tài liệu liên quan đến nhân sự phải bao gồm các bản cập nhật thường xuyên (ít nhất 12 tháng một lần) về các mối đe dọa mới và các phương pháp bảo mật hiện tại.	- Các chứng chỉ, chứng nhận của nhân sự liên quan phải được cập nhật 12 tháng 1 lần. - So sánh các mối đe doạ mới và các mối đe doạ đã thống kê theo tài liệu đào tạo. - Kiểm tra sự hiểu biết của nhân viên về các mối đe doạ mới, khác biệt của mối đe doạ mới với mối đe doạ đã được thống kê.	
6.5	REQ-7.2-05 ETSI EN 319 401	Các biện pháp kỷ luật thích hợp sẽ được áp dụng đối với nhân viên vi phạm các chính sách hoặc quy trình của CA	Chế tài kỷ luật áp dụng đối với nhân viên vi phạm các chính sách hoặc quy trình của CA (Quy chế của công ty)	
6.6	REQ-7.2-06 ETSI EN 319 401	Các vị trí và trách nhiệm bảo mật, như được quy định trong chính sách bảo mật thông tin của CA, sẽ được ghi lại trong bản mô tả công việc hoặc trong các tài liệu có sẵn cho tất cả nhân viên liên quan.	Tài liệu hóa các vai trò, trách nhiệm an ninh như đã được quy định trong chính sách bảo mật thông tin của CA. Tất cả sẽ được ghi lại trong bản mô tả công việc hoặc trong các tài liệu có sẵn đối với các nhân viên liên quan. (Vai trò trách nhiệm của nhận sư và văn bản giao việc)	
6.7	REQ-7.2-07 ETSI EN 319 401	Các vị trí chủ chốt, liên quan đến tính bảo mật của hoạt động của CA phải được xác định rõ ràng.	- Vai trò của từng vị trí: + Quản trị hệ thống: Chịu trách nhiệm cài đặt, cấu hình và bảo trì hệ thống ký số, với các quyền truy cập thông tin an ninh, hệ thống nhất định. + Đảm bảo ATTT hệ thống: Chịu trách nhiệm quản lý, việc triển khai các chính sách quy chế an ninh bảo mật và có quyền truy cập các thông tin liên quan đến an ninh. + Vận hành hệ thống và cấp CTS: Chịu trách nhiệm vận hành hệ thống ký số hàng ngày và có quyền truy cập hệ	

			thống sao lưu-phục hồi. Và chịu trách nhiệm về việc cấp CTS +Kiểm toán hệ thống: Chịu trách nhiệm kiểm định hệ thống, đánh giá tuân thủ so với các chính sách an ninh, bảo mật. Được phép truy cập các thông tin lưu trữ và kiểm toán - Phỏng vấn chi tiết từng nhân sự tương ứng với từng vị trí trong hệ thống.	
6.8	REQ-7.2-08 ETSI EN 319 401	Các vị trí chủ chốt phải do ban lãnh đạo quy định chức danh.	Quyết định ban hành có mô tả vị trí, vai trò của các nhân sự chủ chốt trong hệ thống.	
6.9	REQ-7.2-09 ETSI EN 319 401	Các vị trí chủ chốt sẽ được ban lãnh đạo bổ nhiệm và người đó phải hoàn thành chức năng nhiệm vụ đó	Quyết định của ban lãnh đạo về việc quy định chức danh cho các vị trí chủ chốt và kiểm tra việc nắm bắt công việc của từng vị trí theo hình thức phỏng vấn.	
6.10	REQ-7.2-10 ETST 319 401	Nhân sự của CA (cả tạm thời và cố định) phải có bản mô tả công việc được xác định theo chức năng nhiệm vụ được giao hoàn thành với sự phân biệt quyền lợi và trách nhiệm, xác định mức độ của vị trí dựa trên nhiệm vụ và cấp độ truy cập, sàng lọc,đánh giá nhân viên về đào tạo và nhận thức.	Danh sách nhân sự, RA được kiểm tra kỹ càng và cam kết mức độ tin cập trong các hoạt động liên quan tới CA (Danh sách các bên thứ 3 cung cấp cho CA, nhân sự đầu mối). - Danh sách nhân sự gồm 4 vai và phân rõ trách nhiệm của từng vị trí: vận hành hệ thống, cấp chứng thư số, đảm bảo ATTT hệ thống, kiểm toán viên hệ thống (nv kiểm soát, thống kê hệ thống).	
6.11	REQ-7.2-11 ETST 319 401	Mô tả chức năng, trách nhiệm của các nhân sự tham gia hệ thống Remote Signing.	+ Các nhân sự có bằng TN đại học trở lên chuyên ngành: ĐTVT, ATTT, CNTT + Hợp đồng lao động còn thời hạn. + Sơ yếu lí lịch của các nhân sự: Có chứng thực chữ ký của người kí - Đối với RA:	

			+ HĐ đại lý theo TT31/2020/TT-BTTTT còn thời hạn, ĐKKD thay đổi lần gần nhất của đại lý	
6.12	REQ-7.2-12 ETST 319 401	Nhân sự phải thực hiện các thủ tục và quy trình hành chính và quản lý phù hợp với các quy trình quản lý an toàn thông tin của CA	HĐLĐ, văn bản cam kết có điều khoản, cam kết thực hiện các thủ tục và quy trình hành chính, quản lý phù hợp đối với các quy trình quản lý an toàn thông tin đối với nhân sự tham gia hệ thống. Các tài liệu kết quả đào tạo liên quan. Đánh giá bằng phương pháp phỏng vấn trực tiếp.	
6.13	REQ-7.2-13 ETST 319 401	Nhân viên quản lý phải có kinh nghiệm hoặc được đào tạo liên quan đến dịch vụ được cung cấp, quen thuộc với các thủ tục bảo mật dành cho Nhân viên chịu trách nhiệm bảo mật và kinh nghiệm về bảo mật thông tin và khả năng đánh giá rủi ro đủ để thực hiện các chức năng quản lý.		
6.14	REQ-7.2-14 ETST 319 401	Tất cả Nhân sự của CA trong các vị trí chủ chốt phải không có xung đột lợi ích có thể ảnh hưởng đến tính công bằng trong hoạt động của CA.	Danh sách nhân sự thể hiện một nhân sự chỉ được tham gia 01 vị trí bất kì trong hệ thống.	
6.15	REQ-7.2-15 ETST 319 401	Nhân viên an ninh: Chịu trách nhiệm chung trong việc quản lý việc thực hiện các quy trình bảo mật. (bao gồm khôi phục hệ thống)	Văn bản quy định chức năng, nhiệm vụ của nhân viên trong hệ thống	
6.16	REQ-7.2-15 ETST 319 401	Quản trị viên Hệ thống: Được phép cài đặt, cấu hình và duy trì các hệ thống đáng tin cậy của CA để quản lý dịch vụ. (bao gồm khôi phục hệ thống)		

6.17	REQ-7.2-15 ETST 319 401	Người vận hành hệ thống: Chịu trách nhiệm vận hành các hệ thống chủ chốt của CA hàng ngày. Được phép thực hiện sao lưu hệ thống.		
6.18	REQ-7.2-15 ETST 319 401	Kiểm soát hệ thống: Được ủy quyền để xem các bản lưu trữ và nhật ký kiểm tra các hệ thống đáng tin cậy của CA.		
6.19	REQ-7.2-16 ETST 319 401	Nhân sự của CA phải được chính thức bổ nhiệm vào các vị trí chủ chốt bởi quản lý cấp cao chịu trách nhiệm về bảo mật yêu cầu nguyên tắc "đặc quyền ít nhất" khi truy cập hoặc khi định cấu hình quyền truy cập.	Chính sách/quy định của CA về chức năng nhiệm vụ (Hợp đồng lao động, hoặc danh sách phân công nhiệm vụ đối với các nhân sự tham gia hệ thống)	
6.20	REQ-7.2-17 ETST 319 401	- Nhân viên sẽ không có quyền truy cập vào các chức năng quan trọng cho đến khi hoàn thành các kiểm tra cần thiết.	Quy trình kiểm soát truy cập	
7	**Quy trình lưu trữ nhật ký**			
7.1	REQ-7.10-01 ETSI EN 319 401	CA phải ghi lại và giữ cho người dùng có thể truy cập được trong một khoảng thời gian thích hợp, kể cả sau khi các hoạt động của CA chấm dứt, tất cả thông tin liên quan đến dữ liệu do CA cung cấp và tiếp nhận, đặc biệt, nhằm mục đích cung cấp bằng chứng trong	Cơ chế ghi lại và giữ phiên truy cập của người dùng trong 1 khoảng thời gian rõ ràng (trong vòng 24 tháng). Các thông tin log liên quan đến phiên làm việc của người dùng đó phải được lưu lại nhằm mục đích tra cứu sau này	Đối với quy trình lưu trữ nhật ký của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt

		tố tụng pháp lý và mục đích đảm bảo tính liên tục của dịch vụ		
7.2	REQ-7.10-02 ETSI EN 319 401	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 phải được duy trì	Cơ chế bảo vệ dữ liệu log ghi lại. Đảm bảo bảo mật và toàn vẹn (CA cung cấp giải pháp đảm bảo tính bảo mật và toàn vẹn của dữ liệu log sau đó là chứng minh giải pháp).	
7.3	REQ-7.10-03 ETSI EN 319 401	Hồ sơ liên quan đến hoạt động của các dịch vụ sẽ được lưu trữ hoàn toàn và bí mật theo các thông lệ kinh doanh được công bố.	Tài liệu quy định lưu trữ dữ liệu log được lưu trữ (chỉ người quản trị nắm giữ được vị trí lưu log. Không cho những nhân sự khác biết vị trí lưu log)	
7.4	REQ-7.10-04 ETSI EN 319 401	Hồ sơ liên quan đến hoạt động của các dịch vụ phải được cung cấp nếu có yêu cầu nhằm mục đích cung cấp bằng chứng về hoạt động chính xác của các dịch vụ cho mục đích tố tụng pháp lý.	Quy định về việc sử dụng dữ liệu log phục vụ cho mục đích tố tụng pháp lý	
7.5	REQ-7.10-05 ETSI EN 319 401	Thời gian chính xác của các sự kiện quan trọng về môi trường, quản lý khóa và Thời gian đồng bộ hóa của CA phải được ghi lại.	Log phải lưu lại mốc thời gian chính xác các sự kiện quan trong. Môi trường, quản lý khóa, thời gian đồng bộ hóa (Theo nguồn thời gian đạt chuẩn của viện đo lường).	
7.6	REQ-7.10-06 ETSI EN 319 401	Thời gian được sử dụng để ghi lại các sự kiện theo yêu cầu trong nhật ký đánh giá sẽ được đồng bộ hóa với UTC ít nhất một lần một ngày	Hệ thống lưu log phải được đồng bộ hóa với nguồn thời gian đạt chuẩn của viện đo lường ít nhất 1 lần 1 ngày	

7.7	REQ-7.10-07 ETSI EN 319 401	hồ sơ liên quan đến dịch vụ sẽ được lưu giữ trong một khoảng Thời gian thích hợp để cung cấp bằng chứng pháp lý cần thiết và như được thông báo trong các điều khoản và điều kiện của CA	Mốc thời gian cụ thể, thích hợp trong quá trình lưu trữ log	
7.8	REQ-7.10-08 ETSI EN 319 401	Các sự kiện phải được ghi lại theo phương pháp không thể dễ dàng bị xóa hoặc phá hủy (trừ trường hợp được chuyển một cách có mục đích sang phương tiện lưu trữ dài hạn) trong khoảng Thời gian được yêu cầu lưu giữ.	Cơ chế ghi log phải không có cơ chế xóa, hủy dữ liệu trong thời gian yêu cầu lưu trữ. Phải có cơ chế ghi lại và giữ phiên truy cập của người dùng trong 1 khoảng thời gian rõ ràng (trong vòng 24 tháng). Các thông tin log liên quan đến phiên làm việc của người dùng đó phải được lưu lại nhằm mục đích tra cứu sau này	
7.9	OVR-6.4.5-02 ETSI 119 431-1	Tất cả các sự kiện bảo mật sẽ được ghi lại, bao gồm các thay đổi liên quan đến chính sách bảo mật, khởi động và tắt hệ thống, sự cố hệ thống và lỗi phần cứng, hoạt động của tường lửa và bộ định tuyến và các nỗ lực truy cập hệ thống SSASC (Ứng dụng ký số).	Quy định danh sách log được lưu trữ và kiểm tra thực tế kèm tài liệu Quá trình kiểm tra ghi log, phải đảm bảo các sự kiện được nêu ra phải đc lưu và có cơ chế lưu. Log/camera phải bao gồm các sự kiện như: • Khởi động và tắt hệ thống; • Khởi động và tắt ứng dụng của CA; • Tạo, xóa, đặt mật khẩu hoặc thay đổi hệ thống; • Đặc quyền của một số nhân sự chính tham gia hệ thống; • Thay đổi đối với khóa của CA hoặc bất kỳ chi tiết nào khác liên quan. • Các thay đổi đối với chính sách tạo chứng thư số, ví dụ như thời hạn hiệu lực;	
7.10	OVR-6.4.5-03 ETSI 119 431-1	Ở mức tối thiểu, các sự kiện sau phải được ghi lại: - các sự kiện quan trọng về môi trường, quản lý khóa CA (tạo, sử dụng và hủy); - các sự kiện ký của người dùng (ví dụ: ký thành công với khóa ký của người ký và quản lý yêu cầu		

		DTBS/R); - Xác thực người dùng trong SAP (Giao thức kích hoạt chữ ký); - Quản lý SAD (Dữ liệu kích hoạt chữ ký) của người ký bởi CA; - Khởi động và tắt chức năng tạo dữ liệu kiểm tra (đánh giá data); - Các thay đổi của các tham số đánh giá - Sự kiện ký người dùng phải bao gồm chứng chỉ liên kết với khóa ký. Tất cả các truy cập vào CA cần được ghi lại - CA phải chỉ định những gì được thực hiện (tức là các hành động được thực hiện) trong trường hợp không thể chuyển thông tin đánh giá đến bất kỳ bộ nhớ ngoài nào.	• Nỗ lực đăng nhập và đăng xuất hệ thống; • Cố gắng truy cập trái phép vào hệ thống của CA; • Cố gắng truy cập trái phép các folder hệ thống; • Tạo cặp khoá; • Tạo và thu hồi Chứng thư số ; • Cố gắng khởi tạo loại bỏ, bật và tắt người đăng ký cũng như cập nhật và khôi phục khóa của họ; • Các thao tác đọc và ghi không thành công trên CRL.	
7.11	OVR-6.4.5-04 ETSI 119 431-1 SRG_AA.2 CEN EN 419 241-1	CA PHẢI duy trì đánh giá dữ liệu và đảm bảo rằng các biện pháp được thực hiện để lưu trữ tất cả đánh giá data - Đánh giá function chỉ được phép thêm thông tin - CA phải bảo vệ các hồ sơ đánh giá được lưu trữ trong quá trình đánh giá khỏi bị xóa trái phép - Hồ sơ kiểm tra CÓ THỂ bị xóa khi được lưu trữ vào bộ nhớ ngoài.	Các cơ chế kiểm toán. Bao gồm các chính sách để duy trì thực hiện đánh giá cũng như đảm bảo lưu trữ dữ liệu đánh giá. Ngoài ra hệ thống hỗ trợ có cơ chế đảm bảo chỉ được thêm vào, ko được sửa - xóa (chỉ xóa với trường hợp backup lưu trữ ngoài). Đảm bảo các tiêu chí bảo mật đối với các dữ liệu đánh giá --> Liên quan đến license support của CA	

7.12	OVR-6.4.5-05 ETSI 119 431-1	Tất cả hồ sơ đánh giá (bao gồm cả ghi nhật ký đánh giá dịch vụ cụ thể) phải chứa những điều sau: - Ngày giờ của sự kiện. - Loại sự kiện - Danh tính của thực thể (ví dụ: người dùng, quản trị viên, quy trình) chịu trách nhiệm về hành động; - Sự thành công hay thất bại của sự kiện được đánh giá.	Các dữ liệu đánh giá phải đảm bảo đầy đủ các thông tin, thông số được nêu ra ở mục tiêu chí.	
7.13	OVR-6.4.5-06 ETSI 119 431-1 SRG_AA.7 của CEN EN 419.241-1	Có cơ chế đảm bảo dữ liệu đánh giá không được sửa, xóa. Dữ liệu đánh giá được lưu trữ phải đảm bảo an toàn, không có khả năng thay đổi thông tin khi dữ liệu được lưu.	Cơ chế đảm bảo dữ liệu đánh giá không được sửa, xóa. Dữ liệu đánh giá được lưu trữ phải đảm bảo an toàn, không có khả năng thay đổi thông tin khi dữ liệu được lưu. Cơ chế ghi log phải không có cơ chế xóa, hủy dữ liệu trong thời gian yêu cầu lưu trữ. Phải có cơ chế ghi lại và giữ phiên truy cập của người dùng trong 1 khoảng thời gian rõ ràng (trong vòng 24 tháng). Các thông tin log liên quan đến phiên làm việc của người dùng đó phải được lưu lại nhằm mục đích tra cứu sau này	
7.14	'OVR-6.4.5-07 ETSI 119 431-1 SRG_AA.8 of CEN EN 419 241-1	Để đảm bảo độ chính xác về thời gian của các sự kiện được đánh giá, yêu cầu SRG_SO.2.2 được áp dụng.	Hồ sơ đánh giá đúng với thời gian triển khai	

7.15	OVR-6.4.6-01 ETSI TS 119431-1	CA phải duy trì dữ liệu đánh giá tối thiểu 5 năm sau khi chứng thư số liên quan đến dữ liệu đó ngừng có hiệu lực và theo ràng buộc của pháp luật hiện hành.	Quy định lưu trữ dữ liệu kiểm tra, kiểm toán và kết quả lưu trữ	
8	**Quy trình phục hồi sau sự cố**			
8.1	REQ-7.9-01 ETSI EN 319 401	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 sẽ được giám sát.	- Kiểm soát Bảo mật phải được cài đặt và duy trì trên mỗi Hệ thống Máy tính để ngăn người dùng trái phép xâm nhập vào hệ thống thông tin và ngăn chặn truy cập trái phép vào dữ liệu. - Bất kỳ phần mềm hệ thống hoặc tài nguyên nào của hệ thống máy tính chỉ được truy cập sau khi được hệ thống kiểm soát xác thực truy cập. - Phần mềm kiểm soát truy cập và các tính năng bảo mật của phần mềm hệ thống sẽ được triển khai để bảo vệ tài nguyên. Cần có sự phê duyệt của ban quản lý để cho phép cấp nhận dạng người dùng (ID) và các đặc quyền về tài nguyên. - CA tuân theo các biện pháp kiểm soát truy cập và tính toàn vẹn đã được phê duyệt như phát hiện xâm nhập, quét vi rút, ngăn chặn các cuộc tấn công từ chối dịch vụ và các biện pháp bảo mật vật lý. - Sổ tay Hệ thống Kiểm soát Truy cập ghi lại quyền truy cập được cấp cho các cấp độ người dùng khác nhau sẽ được chuẩn bị để cung cấp hướng dẫn cho Quản trị viên Hệ thống về việc cấp quyền truy cập.	Đối với quy trình phục hồi sự cố của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt

			- Mỗi người dùng sẽ được chỉ định một ID người dùng duy nhất. Người dùng sẽ được đào tạo để giúp người dùng lựa chọn mật khẩu và bảo vệ mật khẩu. - Chia sẻ ID người dùng sẽ không được phép. - Mật khẩu đã lưu trữ sẽ được mã hóa bằng các kỹ thuật mã hóa đã được quốc tế chứng minh để ngăn chặn việc tiết lộ và sửa đổi trái phép. - Mật khẩu đã lưu trữ sẽ được bảo vệ bởi các biện pháp kiểm soát truy cập khỏi tiết lộ và sửa đổi trái phép - Thời gian chờ tự động cho việc không hoạt động của thiết bị đầu cuối nên được triển khai. - Hoạt động của tất cả người dùng sẽ được ghi lại và giám sát chặt chẽ. - Quy trình khởi động và tắt phần mềm bảo mật phải được Tự động hóa. - Không ai có thể thay đổi hoặc sửa tác vụ của hệ điều hành hoặc phần mềm cài trên hệ thống trừ khi có sự cho phép của quản trị hệ thống.	
8.2	REQ-7.9-02 ETSI EN 319 401	Các hoạt động giám sát cần tính đến tính nhạy cảm của bất kỳ thông tin nào được thu thập hoặc phân tích.	Phương án quản lý, phân loại nhằm bảo mật những thông tin nhạy cảm trong quá hoạt động cấp chứng thư số, lịch sử ký số.	
8.3	REQ-7.9-03 ETSI EN 319 401	Các 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 CA, sẽ được phát hiện và báo cáo dưới dạng báo động.	Khả năng phát hiện bất thường của hệ thống như: vi phạm bảo mật, xâm nhập vào mạng CA (Cảnh báo)	

8.4	REQ-7.9-04 ETSI EN 319 401	CA sẽ giám sát các sự kiện sau: a) khởi động và tắt các chức năng ghi nhật ký; b) tính sẵn sàng và việc sử dụng các dịch vụ cần thiết với mạng của CA	Có chức năng giám sát 2 sự kiên bên Kiểm tra log liên quan đến 2 sự kiện bên.	
8.5	REQ-7.9-05 ETSI EN 319 401	CA phải hành động kịp Thời và phối hợp để phản ứng nhanh với các sự cố và hạn chế ảnh hưởng của các vi phạm an ninh.	Chính sách, cơ chế để hành động, phối hợp khi có sự cố và giảm thiểu ảnh hưởng của vi phạm an ninh (Quy trình xử lý sự cố ATTT)	
8.6	REQ-7.9-06 ETSI EN 319 401	CA sẽ chỉ định Nhân viên có chức trách để theo dõi các cảnh báo về các sự kiện an ninh quan trọng tiềm ẩn và đảm bảo rằng các sự cố liên quan được báo cáo phù hợp với các thủ tục của CA.	Phỏng vấn kiểm tra Nhân viên/đơn vị được chịu trách nhiệm theo dõi các cảnh báo về an ninh, các sự cố báo cáo và các thủ tục của CA. (Kiểm tra ngẫu nhiên 1 sự cố và cảnh báo an ninh gần nhất trước đó)	
8.7	REQ-7.9-07 ETSI EN 319 401	CA sẽ thiết lập các thủ tục để thông báo cho các bên thích hợp theo các quy tắc quy định hiện hành về bất kỳ vi phạm bảo mật hoặc mất tính toàn vẹn nào có ảnh hưởng đáng kể đến dịch được cung cấp và dữ liệu cá nhân được duy trì trong đó trong vòng 24 giờ kể từ khi vi phạm xảy ra.	Chính sách, cơ chế ghi rõ CA thiết lập các thông báo cho các bên thích hợp theo các quy tắc quy định hiện hành về bất kỳ vi phạm bảo mật trong vòng 24h kể từ khi vi phạm xảy ra. (Quy trình xử lý sự kiện bất thường và có nội dung thông báo các bên liên quan)	

8.8	REQ-7.9-08 ETSI EN 319 401	Trong trường hợp vi phạm bảo mật hoặc mất tính toàn vẹn có khả năng ảnh hưởng xấu đến một thể nhân hoặc pháp nhân mà dịch vụ đáng tin cậy đã được cung cấp, CA cũng sẽ thông báo cho thể nhân hoặc pháp nhân về vi phạm bảo mật hoặc mất tính toàn vẹn mà không cần chậm trễ quá mức. .	Chính sách, cơ chế ghĩ rõ ngay lập tức thông báo đến 1 thể nhân hoặc pháp nhân mà đã cung cấp dịch vụ khi có vi phạm bảo mật hoặc mất tính toàn vẹn (Quy trình xử lý sự kiện bất thường và có nội dung thông báo các bên liên quan)	
8.9	REQ-7.9-09 ETSI EN 319 401	Hệ thống của CA sẽ được giám sát bao gồm việc giám sát hoặc xem xét thường xuyên nhật ký đánh giá để xác định bằng chứng về hoạt động độc hại thực hiện các cơ chế tự động để xử lý nhật ký đánh giá và cảnh báo cho nhân viên về các sự kiện bảo mật quan trọng có thể xảy ra.	Cơ chế thường xuyên đánh giá, kiểm tra cơ chế ghi log tự động (Quy trình giám sát). Kiểm tra file lưu log	
8.10	REQ-7.9-10 ETSI EN 319 401	CA phải giải quyết bất kỳ lỗ hổng nghiêm trọng nào chưa được CA giải quyết trước đây, trong khoảng thời gian 48 giờ sau khi phát hiện ra.	Cơ chế, chính sách ghi rõ ngay lập tức xử lý, khắc phục trong khoảng 48 giờ sau khi phát hiện ra lỗ hổng mới trong CA (Quy trình xử lý sự kiện bất thường và có nội dung thông báo các bên liên quan)	
8.11	REQ-7.9-11 ETSI EN 319 401	Đối với bất kỳ lỗ hổng nào, với tác động tiềm ẩn, CA sẽ chọn 1 trong 2 biện pháp: Tạo và thực hiện một kế hoạch để giảm thiểu tính dễ bị tấn công; hoặc là Ghi lại cơ sở thực tế để CA xác định rằng lỗ hổng bảo mật không cần khắc phục.	Chính sách ngay lập tức đưa ra biện pháp khi phát hiện có lỗ hổng: Trong đó lựa chọn 1 trong 2 phương án được nêu ra ở bên nhằm khắc phục sự cố: - Kế hoạch gồm các phương án giảm thiểu, khắc phục các nguy cơ bị tấn công - Phân loại sự cố, lỗ hổng bảo mật và phương án xử lý.	

8.12	REQ-7.9-12 ETSI EN 319 401	Các thủ tục báo cáo và ứng phó sự cố sẽ được sử dụng theo cách giảm thiểu thiệt hại do các sự cố và trục trặc an ninh gây ra.	Các quy định đối với thủ tục báo cáo và ứng phó sẽ sử dụng theo kế hoạch giảm thiểu thiệt hại (Quy trình xử lý sự kiện bất thường và có nội dung thông báo các bên liên quan)	
9	**Quy trình đảm bảo tính liên tục của hệ thống**			
9.1	REQ-7.12-01, ETSI 319 401	Các gián đoạn tiềm tàng đối với người đăng ký và các bên tin tưởng phải 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 tin cậy phải được cung cấp.	Quy trình, quy định về việc ngừng cung cấp dịch vụ của CA và những phương án xử lý đối với CTS, dịch vụ khách hàng. Các kế hoạch quản lý sự cố bao gồm: • Các trường hợp gây mất an toàn cho khoá của CA; • Hack hệ thống vật lý và hệ thống phần mềm; • Các Vi phạm an ninh vật lý; • Tính khả dụng của cơ sở hạ tầng nơi đặt hệ thống; • Các trường hợp đăng ký và tạo chứng thư số bất hợp pháp; • Tạm dừng, thu hồi chứng thư số trong thời gian hiệu lực. Kế hoạch khắc phục hậu quả thiên tai phải được phát triển, lập thành văn bản, kiểm tra và duy trì thích hợp để đảm bảo rằng trong trường hợp hệ thống thông tin bị lỗi hoặc bị phá hủy. Khung khắc phục thảm họa bao gồm: • Quy trình khẩn cấp, mô tả hành động tức thì cần thực hiện trong trường hợp có sự cố lớn. • Quy trình dự phòng, mô tả các hành động cần thực hiện để di dời các hoạt động thiết yếu hoặc các dịch vụ hỗ trợ đến địa điểm dự phòng (<24h).	Đối với quy trình đảm bảo tính liên tục của hệ thống của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt

			• Quy trình khôi phục, mô tả hành động cần thực hiện để trở lại hoạt động bình thường tại vị trí ban đầu. Tài liệu bao gồm: • Định nghĩa về một thảm họa; • Điều kiện để kích hoạt kế hoạch; • Các giai đoạn của kế hoạch; • Ai sẽ ra quyết định khi có sự cố xảy ra; • Vai trò của các nhân sự đối với từng phần của kế hoạch; • Thành phần của nhóm phục hồi lại DC; • Quá trình ra quyết định hoạt động trở lại bình thường khi DC đã đủ điều kiện hoạt động. Kế hoạch quản lý thảm họa phải được phát triển, lập thành văn bản, kiểm tra và duy trì thường xuyên. Một số yêu cầu cần xem xét liên quan đến cơ sở hạ tầng CNTT bao gồm: (1) Phần cứng hệ thống; (2) Các yêu cầu lưu trữ dữ liệu hệ thống; (3) DR phải tự động đồng bộ dữ liệu và hoạt động khi DC xảy ra sự cố không thể khắc phục được. (4) Có kế hoạch dự phòng xác định tất cả các biện pháp tạm thờ như việc di dời hệ thống đến một địa điểm dự phòng. Trách nhiệm và cấu trúc báo cáo phải được xác định rõ ràng sẽ có hiệu lực ngay lập tức khi công bố thiên tai. Mỗi thành phần của kế hoạch nên có một người chính và một người dự phòng được chỉ định để thực hiện. Cần tiến hành đào tạo định kỳ cho nhân	

			viên và người dùng liên quan đến hệ thống máy tính và mạng để xác định vai trò và trách nhiệm của họ trong trường hợp xảy ra thiên tai. Kế hoạch khắc phục hậu quả thiên tai cần được cập nhật thường xuyên để đảm bảo tính hiệu quả liên tục. * Có phương án sao lưu dữ liệu định kỳ phục vụ việc phục hồi dữ liệu khi có sự cố xảy ra.	
9.2	REQ-7.12-02, ETSI 319 401	CA phải có phương án khi dừng dịch vụ được cập nhật thường xuyên. Trước khi CA chấm dứt các dịch vụ của mình, các thủ tục sau phải được áp dụng:	Điều khoản trong hợp đồng hoặc kế hoạch chấm dứt cung cấp dịch vụ của CA (trước khi CA ngừng cung cấp dịch vụ), bao gồm: Kế hoạch tương ứng để ứng phó, đảm bảo tính liên tục của hệ thống: • Thỏa thuận tạm ngừng cung cấp dịch vụ; • Thông báo cho cộng đồng người dùng; (nếu có) • Thu hồi chứng thư số; • Trách nhiệm của nhân viên xử lý sự cố; • Điều tra sự gián đoạn dịch vụ; • Quy trình phục hồi dịch vụ; • Giám sát và đánh giá phân tích sự cố. - Có một quy trình báo cáo sự cố an ninh chính thức, đưa ra các hành động cần thực hiện khi nhận được báo cáo sự cố. Điều này bao gồm định nghĩa và tài liệu về các trách nhiệm được giao và các thủ tục cần thiết. Bất kỳ sự cố nào đều được báo cáo cho CA như một vấn đề khẩn cấp.	

			- Có các quy trình và được tuân theo để báo cáo sự cố phần cứng và phần mềm. Có các thủ tục và được tuân theo để đánh giá rằng hành động khắc phục được thực hiện đối với các sự cố được báo cáo. - Các thủ tục để xác định, báo cáo và giải quyết các vấn đề, chẳng hạn như không hoạt động của hệ thống CA; vi phạm về bảo mật Công nghệ thông tin; và hack, sẽ được thiết lập và thông báo cho tất cả nhân viên liên quan. Nó sẽ bao gồm các thủ tục khẩn cấp. Các báo cáo định kỳ sẽ được đệ trình để quản lý xem xét. - Một bàn trợ giúp sẽ được thiết lập để hỗ trợ người dùng giải quyết các vấn đề. Một hệ thống để ghi lại, theo dõi và báo cáo trạng thái để đảm bảo rằng chúng được quản lý và giải quyết kịp thời.	
9.3	REQ-7.12-03, ETSI 319 401	Trước khi CA chấm dứt các dịch vụ, CA phải thông báo cho tất cả thuê bao và các tổ chức khác mà CA có thỏa thuận hoặc hình thức quan hệ đã thiết lập khác, trong đó các bên tin tưởng, CA và có liên quan các cơ quan chức năng như cơ quan giám sát.	Văn bản thông báo về việc chấm dứt dịch vụ mà CA có thỏa thuận hoặc đã thiết lập quan hệ	
9.4	REQ-7.12-04, ETSI 319 401	trước khi CA chấm dứt các dịch vụ của mình, CA sẽ cung cấp thông tin về việc chấm dứt cho các bên phụ thuộc khác.	Văn bản thông báo/cung cấp thông tin về việc chấm dứt dịch vụ đối với các bên phụ thuộc	

9.5	REQ-7.12-05, ETSI 319 401	Trước khi CA chấm dứt các dịch vụ của mình, CA sẽ chấm dứt ủy quyền của tất cả các RA và đối tác thực hiện cung cấp dịch vụ chứng thực chữ ký số công cộng	Điều khoản hoặc quy định của CA sẽ chấm dứt ủy quyền tất cả các RA và đối tác thực hiện cung cấp dịch vụ chứng thực chữ ký số công cộng (Văn bản thể hiện việc chấm dứt nếu có)	
9.6	REQ-7.12-06, ETSI 319 401	Trước khi CA chấm dứt các dịch vụ của mình, CA sẽ chuyển giao nghĩa vụ cho một bên đáng tin cậy để duy trì tất cả thông tin cần thiết để cung cấp bằng chứng về hoạt động của CA trong một khoảng Thời gian hợp lý, trừ khi có thể chứng minh rằng CA không giữ bất kỳ thông tin nào như vậy.	Văn bản thông báo chuyển giao của CA cho bên đáng tin cậy, có thể hiện thời gian chuyển giao và tài liệu chứng minh CA không còn lưu trữ thông tin hồ sơ thuê bao.	
9.7	REQ-7.12-07, ETSI 319 401	trước khi CA chấm dứt các dịch vụ của mình, các khóa bí mật của CA, bao gồm cả các bản sao lưu, sẽ bị hủy hoặc bị rút khỏi sử dụng, theo cách mà khóa bí mật không thể được truy xuất.	Show log của thiết bị HSM về việc tạo hủy khóa (nếu có) để đảm bảo khóa bí mật không bị truy xuất khi CA ngừng cung cấp dịch vụ	
9.8	REQ-7.12-08, ETSI 319 401	trước khi CA chấm dứt các dịch vụ của mình, nếu có thể CA nên thu xếp để chuyển việc cung cấp các dịch vụ tin cậy cho các khách hàng hiện tại của mình cho một CA khác.	Tài liệu chứng minh chuyển giao việc cung cấp dịch vụ tin cậy cho một CA khác đối với các khách hàng hiện tại (nếu có)	

9.9	REQ-7.12-09, ETSI 319 401	CA phải có một thỏa thuận để trang trải các chi phí để đáp ứng các yêu cầu tối thiểu này trong trường hợp CA bị phá sản hoặc vì các lý do khác không thể tự trang trải các chi phí, trong phạm vi ràng buộc của luật hiện hành liên quan đến phá sản.	Quy định tại điểm a khoản 2 điều 13, Nghị định 130/NĐ-CP	
9.10	REQ-7.12-10, ETSI 319 401	CA phải nêu trong thực tiễn của mình các điều khoản được đưa ra để chấm dứt dịch vụ. Điều này sẽ bao gồm: a) thông báo về các thực thể bị ảnh hưởng b) nếu có thể, chuyển các nghĩa vụ của CA cho các bên khác.	Phương án và tài liệu thông báo đến các chủ thể liên quan và CA được nhận nhiệm vụ chuyển giao (nếu có)	
9.11	REQ-7.12-11, ETSI 319 401	CA sẽ duy trì hoặc chuyển cho một bên đáng tin cậy nghĩa vụ của mình là cung cấp khóa công khai hoặc mã thông báo dịch vụ của mình cho các bên tin cậy trong một khoảng thời gian hợp lý.	Kế hoạch chuyển giao, bàn giao thuê bao và thông tin thuê bao cho 1 trong các CA công cộng đủ điều kiện để cung cấp dịch vụ remote signing có thể duy trì tính liên tục của dịch vụ trong trường hợp CA bị thu hồi, tạm dừng hoặc có bất kì rủi ro bất khả kháng nào có thể xảy ra.	

10	**Quy trình kiểm soát an toàn kỹ thuật của hệ thống**			
10.1	6.5.1 Systems and security management 1. OVR-6.5.1-01:The requirements identified in CEN EN 419 241-1 [3], clause SRG_M.1 shall apply.	1. SRG_M1.1 phải hỗ trợ việc phân tách các vai trò với đặc quyền khác nhau.	1.Nhật ký lưu log, tài liệu chứng minh việc phân quyền cho các tài khoản, người chịu trách nhiệm tham gia vào hệ thống. - Đảm bảo phân rõ (tối thiểu phải có) 4 dạng tài khoản đặc quyền với vai trò xác định trong SRG_M.1.2 - Đảm bảo phân rõ tối thiểu 3 vai trò không có đặc quyền trong mục SRG_M.1.3 - Các tài khoản đặc quyền phải được phân tách vai trò rõ ràng. - Thống kê đầy đủ nhân sự có các tài khoản có vai trò đối với hệ thống CA.	Đối với quy trình kiểm soát an toàn kỹ thuật hệ thống của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt
10.2		2. SRG_M.1.2 CA phải hỗ trợ tối thiểu 4 vai trò sau: Security Officers: có trách nhiệm chung trong việc quản lý việc thực hiện các chính sách, yêu cầu bảo mật và có quyền truy cập vào thông tin liên quan đến bảo mật. System Administrators: được phép cài đặt, cấu hình và duy trì CA nhưng được kiểm soát quyền truy cập vào các thông tin liên quan đến bảo mật. System Operators: chịu trách nhiệm vận hành CA hàng ngày và được phép thực hiện sao lưu và phục hồi hệ thống. System Auditors: được ủy quyền để xem các phần lưu trữ và nhật ký kiểm toán của CA nhằm mục đích kiểm tra hoạt động của hệ thống phù hợp với chính sách bảo mật. Security Officers và System Administrator là các người dùng có có đặc quyền với hệ thống. System Operators và System Đánh giáors: là các người dùng có vài trò trên hệ thống thương không thể tác động đến việc cấu hình quản trị trên CA.		

10.3		3. SRG_M.1.3. CA phải hỗ trợ tối thiểu các vài trò không đặc quyền sau: Signer: được phép sử dụng CA bằng cách chuyển SAD như một phần của SAP để ký vào tài liệu hoặc DTBS / R (Data To be Signed Representation), cũng có khả năng được chuyển qua SAP. SCA: được ủy quyền gửi yêu cầu DTBS / R tới CA để được người ký xác nhận. RA: được ủy quyền để gửi chứng chỉ khóa công khai tới CA theo yêu cầu ký chứng chỉ.		
10.4		4. SRG_M.1.4 Một người dùng đặc quyền không được đảm nhận tất cả các vai trò đặc quyền.		
10.5		5. SRG_M.1.5 Người dùng có vai trò đặc quyền KHÔNG được có vai trò không đặc quyền. Người dùng có vai trò không đặc quyền KHÔNG được có vai trò đặc quyền.		
10.6		6. SRG_M.1.6 CA phải có khả năng đảm bảo rằng người dùng được ủy quyền đảm nhận vai trò Security Officer không được ủy quyền đảm nhận vai trò System Đánh giá.		

10.7		7. SRG_M.1.7 CA phải có khả năng đảm bảo rằng người dùng được ủy quyền để đảm nhận một Hệ thống (Vai trò System administrators và / hoặc vai trò System Operator không được phép đảm nhận vai trò system đánh giáor và / hoặc vai trò Security Officers.		
10.8		8. SRG_M.1.8 Phải có danh sách các cá nhân thuộc nhóm người dùng hệ thống có đặc quyền và nhưng người được đào tạo về hệ thống.		
10.9		9. SRG_M.1.9 Chỉ những người dùng hệ thống đặc quyền mới có quyền truy cập vật lý vào phần cứng và có thể quản trị CA.		
10.10		10. SRG_M.1.10 Chỉ những người dùng hệ thống có đặc quyền mới có quyền quản trị CA thông qua các ứng dụng và giao diện có liên quan.		
10.11	6.5.2 Systems and operations 2. OVR-6.5.2-01:The requirements identified in CEN EN 419 241-1 [3], clause SRG_SO.1 shall apply. 3. OVR-6.5.2-02:The requirements identified in CEN EN 419 241-1 [3], clause SRG_SO.2 shall apply.	SRG_SO.1 CA cần đảm bảo các chức năng quản lý, vận hành đủ an toàn. 1. SRG_SO.1.1 CA cần đảm bảo cung cấp hướng dẫn để các nhân sự chịu trách nhiệm có thể vận hành: - Vận hành một cách chính xác và an toàn. - Được triển khai theo cách giảm thiểu tối đa rủi ro hệ thống gặp	Tài liệu được bàn giao từ CA bao gồm nhưng không giới hạn các tài liệu và yêu cầu trong SRG_SO.1 - Nhật ký lưu log, tài liệu chứng minh việc phân quyền cho các tài khoản, người chịu trách nhiệm tham gia vào hệ thống. + Đảm bảo phân rõ (tối thiểu phải có) 4 dạng tài khoản đặc quyền với vai trò xác định trong SRG_M.1.2	Đối với quy trình kiểm soát an toàn kỹ thuật hệ thống của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt

		lỗi. - Được bảo vệ trước virus và phần mềm độc hại đảm bảo tính toàn vẹn của hệ thống và thông tin xử lý trên hệ thống.	+ Đảm bảo phân rõ tối thiểu 3 vai trò không có đặc quyền trong mục SRG_M.1.3. + Các tài khoản đặc quyền phải được phân tách vai trò rõ ràng. + Thống kê đầy đủ nhân sự có các tài khoản có vai trò đối với hệ thống CA - Văn bản chứng minh đồng bộ thời gian với thời gian chuẩn quốc gia của viện đo lường.	
10.12		2. SRG_SO.1.2 CA Phải cung cấp tài liệu về hệ thống, trong đó có các trách nhiệm của bốn vai trò đặc quyền trong hệ thống được đề cập trong SRG_M.1.2 các tài liệu bao gồm: - Hướng dẫn cài đặt. - Hướng dẫn quản trị. - Hướng dẫn sử dụng.		
10.13		SRG_SO.2 1. SRG_SO.2.1 CA PHẢI nêu rõ về độ chính xác về thời gian của CA và cách đảm bảo điều này.		
10.14	OVR-6.5.3-02: Clause SRG_AA.6.1 of CEN EN 419 241-1 [3], regarding system monitoring shall apply.	"Giám sát hệ thống sẽ được áp dụng CA cần tạo cảnh báo thông báo kịp thời các sự kiện bất thường có thể ảnh hưởng đến khả năng của hệ thống máy chủ ký để đáp ứng các yêu cầu bảo mật được xác định trong tiêu chuẩn này. Một cơ chế đưa ra cảnh báo mỗi khi phát hiện ra một sự kiện bất thường NÊN kích hoạt thông báo cho nhân viên quản trị có liên quan. Một cảnh báo CÓ THỂ cũng kích hoạt các hành động tiếp theo để phản ứng với các cuộc tấn công	Tài liệu kiểm tra theo tiêu chí mô tả	Đối với quy trình kiểm soát an toàn kỹ thuật hệ thống của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt

		có thể xảy ra như để cắt đứt con đường tấn công tiềm năng. Ví dụ về các sự kiện bất thường liên quan đến hoạt động của người dùng có thể: - Hành động của người dùng ngoài giờ sử dụng tiêu chuẩn. - Hành động của người dùng được thực hiện với tốc độ bất thường (để phát hiện các can thiệp không phải của con người). - Hành động của người dùng bỏ qua các hoạt động tiêu chuẩn trong các quy trình được xác định. - Phiên người dùng trùng lặp."		
10.15	OVR-6.5.4-01 EN 319 401	CA phải sử dụng các hệ thống và sản phẩm đáng tin cậy được bảo vệ chống lại sự sửa đổi và đảm bảo an ninh kỹ thuật và độ tin cậy của các quy trình.	Các thiết bị vật lý phải có Lisence, chứng chỉ. Các sản phẩm phần mềm phải được ký số (Code signing)	
10.16	OVR-6.5.4-01 EN 319 401	Quy trình kiểm soát thay đổi sẽ được áp dụng cho các bản phát hành, sửa đổi và bản sửa lỗi phần mềm khẩn cấp của bất kỳ phần mềm hoạt động nào và các thay đổi đối với cấu hình áp dụng chính sách bảo mật của CA.	Tài liệu chứng minh kiểm soát thay đổi	
10.17	OVR-6.5.4-01 EN 319 401	Tính toàn vẹn của hệ thống và thông tin CA phải được bảo vệ khỏi vi rút, phần mềm độc hại và trái phép.	Tài liệu chứng minh hệ thống và thông tin CA phải được bảo vệ bởi phần mềm diệt virut, cảnh báo độc hại và trái phép.	

10.18	OVR-6.5.4-01 EN 319 401	CA phải quy định và áp dụng các thủ tục để đảm bảo rằng: a) các bản vá bảo mật được áp dụng trong một thời gian hợp lý sau khi ban hành; b) các bản vá bảo mật không được áp dụng nếu chúng tạo ra các lỗ hổng hoặc tính bất ổn bổ sung lớn hơn lợi ích của việc áp dụng chúng; c) lý do không áp dụng bất kỳ bản vá bảo mật nào phải được ghi lại.	Các tiêu chí đánh giá như mục bên. Chi tiết bổ sung như sau: - Tài liệu ghi lại các bản vá bảo mật được áp dụng và nhật ký sử dụng.	
10.19	OVR-6.5.5-01 ETSI TS 119431-1	CA phải bảo vệ mạng và hệ thống của mình khỏi bị tấn công.	Sơ đồ hệ thống kỹ thuật có tường lửa và các thiết bị có liensce.	
10.20	OVR-6.5.5-01 ETSI TS 119431-1	CA phải phân đoạn hệ thống của mình thành các mạng hoặc vùng dựa trên đánh giá rủi ro xem xét mối quan hệ chức năng, logic và vật lý (bao gồm cả vị trí) giữa các hệ thống và dịch vụ đáng tin cậy.	Mô hình hệ thống được thiết kế thành các phân vùng phục vụ các chức năng riêng biệt: - Phân cùng DMZ: phục vụ việc cung cấp trực tuyến dịch vụ (RA, CRL, OCSP,...), cấp phát chứng thư số (tại CA hoặc RA), ngăn cách với môi trường Internet thông qua hệ thống tường lửa. - Phân vùng lõi: phục vụ việc tạo khoá, lưu trữ CSDL (HSM, CoreCA,...), không kết nối trực tiếp với môi trường Internet.	
10.21	OVR-6.5.5-01 ETSI TS 119431-1	CA phải hạn chế quyền truy cập và thông tin liên lạc giữa các khu vực cần thiết cho hoạt động của CA.	Giữa các phân vùng phải có tường lửa và thiết bị kiểm soát truy cập	

10.22	OVR-6.5.5-01 ETSI TS 119431-1	CA phải cấm hoặc hủy kích hoạt rõ ràng các kết nối và dịch vụ không cần thiết.	Cấu hình tường lửa quy định các port truy cập hệ thống CA, ngoài các port đó thì các port khác không thể truy cập vào hệ thống.	
10.23	OVR-6.5.5-01 ETSI TS 119431-1	CA phải giữ tất cả các hệ thống quan trọng đối với hoạt động của CA trong một hoặc nhiều vùng bảo mật.	Mô hình hệ thống được thiết kế thành các phân vùng phục vụ các chức năng riêng biệt: - Phân cùng DMZ: phục vụ việc cung cấp trực tuyến dịch vụ (RA, CRL, OCSP, ...), cấp phát chứng thư số (tại CA hoặc RA), ngăn cách với môi trường Internet thông qua hệ thống tường lửa. - Phân vùng lõi: phục vụ việc tạo khoá, lưu trữ CSDL (HSM, CoreCA,...), không kết nối trực tiếp với môi trường Internet.	
10.24	OVR-6.5.5-01 ETSI TS 119431-1	CA phải tách riêng mạng chuyên dụng để quản trị hệ thống CNTT và mạng hoạt động của CA.	Tài liệu mô tả đường truyền cung cấp dịch vụ tại DC-DR, đường truyền giám sát từ trụ sở (NOC), đường truyền kết nối giữa DC và DR	
10.25	OVR-6.5.5-01 ETSI TS 119431-1	Hệ thống vận hành cho mô hình ký số từ xa không được xử dụng chung với hệ thống khác	Tài liệu quy định chức năng của hệ thống vận hành ký số theo mô hình remote Signing (mô tả chức năng của từng thiết bị, ví dụ: Database của LDAP lưu trữ danh sách CTS và hs thuê bao, HSM được sử dụng để lưu khóa bí mật của CA và thuê bao…)	
10.26	OVR-6.5.5-01 ETSI TS 119431-1	Nếu yêu cầu mức độ khả dụng cao của truy cập bên ngoài vào dịch vụ tin cậy, kết nối mạng bên ngoài phải được dự phòng để đảm bảo tính khả dụng của các dịch vụ trong trường hợp xảy ra sự cố.	Kết nối bên ngoài phải có SSL để đảm bảo an toàn	

10.27	OVR-6.5.5-01 ETSI TS 119431-1	CA phải thực hiện quét lỗ hổng thường xuyên trên các địa chỉ IP công cộng và cá nhân được CA xác định và ghi lại bằng chứng rằng mỗi lần quét lỗ hổng được thực hiện bởi một người hoặc tổ chức có kỹ năng, công cụ, trình độ, và tính độc lập cần thiết để cung cấp một báo cáo đáng tin cậy.	Tài liệu ghi lại lịch sử thực hiện quét lỗ hổng thường xuyên trên các địa chỉ IP công cộng và cá nhân. Và các báo cáo phân tích đánh giá tác động của các lỗ hổng bảo mật nếu được phát hiện, phương án khắc phục	
11	**Quy định về kiểm tra, tuân thủ**			
11.1		Xem tiêu chuẩn ETSI EN 319 403: Yêu cầu đối với "cơ quan đánh giá phù hợp" trong hoạt động đánh giá các Nhà cung cấp dịch vụ tin cậy.	VNCERT thực hiện đánh giá theo nội dung "Bộ tiêu chí đánh giá các tiêu chuẩn về chính sách quản lý, vận hành, khai thác cung cấp dịch vụ đối với hình thức ký số từ xa theo quy định tại Thông tư số 16/2019/TT-BTTTT", cụ thể: - Quy trình quản lý rủi ro. - Quy trình quản lý an toàn thông tin. - Quy trình quản lý tài sản. - Chính sách an toàn vật lý. - Chính sách quản lý thủ tục. - Quy trình quản lý nhân sự. - Quy trình lưu trữ nhật ký. - Quy trình phục hồi sau sự cố. - Quy trình đảm bảo tính liên tục của hệ thống. - Quy trình kiểm soát an toàn kỹ thuật của hệ thống. - Quy định về quy định kiểm tra, tuân thủ. Trung tâm Chứng thực điện tử quốc gia sẽ tiến hành thẩm định lại kết quả đánh giá của VNCERT và sẽ thực hiện đánh	Đối với quy tđịnh về kiểm tra, tuân thủ của CA được mô tả phải đáp ứng tất cả các tiêu chí được liệt kê. ☐ Đạt ☐ Không đạt

			giá với các yêu cầu về kỹ thuật của hệ thống Remote Signing. Trung tâm Chứng thực điện tử quốc gia chấp nhận và kiểm tra lại kết quả đánh giá của Các tổ chức được khuyến nghị theo công văn số 105/NEAC-TDPC ngày 26/3/2021 và các tổ chức có năng lực đánh giá. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn, kiểm tra, đánh giá việc áp dụng các tiêu chuẩn thuộc Danh mục tiêu chuẩn bắt buộc áp dụng 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 quy định tại Điều 1 Thông tư số 16/TT-BTTTT.	
11.2	OVR-6.7.2-01 Mục Financial Responsibility của tiêu chuẩn ETSI TS 119431-1	CA phải duy trì đủ nguồn lực tài chính và / hoặc mua bảo hiểm trách nhiệm thích hợp, theo luật hiện hành, để trang trải các trách nhiệm pháp lý phát sinh từ các hoạt động của mình.	Tuân thủ theo khoản 2 điều 13 Nghị định 130/NĐ-CP quy định về điều kiện tài chính bao gồm các Giấy xác nhận ký quỹ, HĐ ký quỹ …	
11.3	(Điều OVR-6.7.4-01 Mục Privacy of personal information của tiêu chuẩn ETSI TS 119431-1)	CA Các biện pháp kỹ thuật được tổ chức thích hợp phải được triển khai để chống lại các hoạt động trái phép hoặc bất hợp pháp với dữ liệu cá nhân và chống lại việc vô tình làm mất hoặc phá hủy hoặc làm hỏng dữ liệu cá nhân.	Quy trình lưu trữ thông tin Thuê bao: Các thủ tục và biện pháp kiểm soát bảo mật để bảo vệ quyền riêng tư và bảo mật dữ liệu của người đăng ký dưới sự quản lý của CA sẽ được thực hiện. Thông tin thuê bao cung cấp không được tiết lộ cho bên thứ ba nếu không được sự đồng ý của chủ thuê bao, trừ trường hợp thông tin đó được yêu cầu tiết lộ theo quy định của pháp luật. * Dạng giấy (đóng gói, dịch vụ giao hàng, người chịu trách nhiệm,…).	

			* Dạng điện tử. Bước 1: Đại lý chuyển hồ sơ về nhà cung cấp theo 2 hình thức: Hồ sơ điện tử: đại lý up lên hệ thống bán hàng của CA. Hồ sơ bản cứng: gửi chuyển phát (có hợp đồng chuyển phát) hoặc mang trực tiếp đến CA. Bước 2: CA tiếp nhận và kiểm tra tính hợp lệ của hồ sơ – một bộ hồ sơ bao gồm: đơn đăng ký, giấy xác nhận thông tin khách hàng, bản sao hợp lệ các giấy tờ: Đối với cá nhân: CMND của khách hàng. Đối với tổ chức: ĐKKD, CMND của người đại diện pháp luật. Đối với cá nhân thuộc tổ chức: ĐKKD, CMND của người đại diện pháp luật, CMND của cá nhân, giấy bổ nhiệm chức danh của khách hàng trong tổ chức. Bước 3: Đóng quyển bản cứng. Bước 4: Nhập thông tin khách hàng, tình trạng hồ sơ lên phần mềm quản lý hồ sơ. Chú ý: Quy trình này đặt ra các quy tắc liên quan đến quá trình lưu trữ, cụ thể cho loại dữ liệu sẽ được lưu trữ. Nó bao gồm các thông tin như tiêu chí lưu trữ, cơ chế và cách lưu trữ được sử dụng, thời hạn lưu giữ cũng như những người được ủy quyền thực hiện việc lưu trữ. (5 năm). Tất cả thông tin được lưu giữ hoặc sao lưu phải được lưu trữ tại CA và phải	

			được bảo vệ bằng bảo mật vật lý hoặc kết hợp bảo vệ vật lý và mật mã. Các vị trí này phải bảo vệ đầy đủ khỏi các mối đe dọa từ môi trường như nhiệt độ, độ ẩm và từ tính. Thông tin được lưu giữ trên phần mềm phải được xác minh định kỳ về tính toàn vẹn của dữ liệu.	
11.4	(Điều OVR-6.7.6-01 Mục Representation and Warranties của tiêu chuẩn ETSI TS 119431-1)	CA phải chịu trách nhiệm chung về việc tuân thủ các thủ tục được quy định trong chính sách bảo mật thông tin của mình, ngay cả khi chức năng của CA do người thuê ngoài đảm nhận.	Các điều kiện của bên thứ 3 được quy định trong hợp đồng, quy định về trách nhiệm (Mẫu hợp đồng theo Thông tư 31/2020/TT-BTTTT)	
11.5	(Điều OVR-6.7.6-01 Mục Representation and Warranties của tiêu chuẩn ETSI TS 119431-1)	CA phải xác định trách nhiệm của người thuê ngoài và đảm bảo rằng người thuê ngoài có nghĩa vụ thực hiện bất kỳ biện pháp kiểm soát nào theo yêu cầu của CA. Lưu ý: CA có trách nhiệm tuân thủ các thủ tục được quy định trong chính sách này, ngay cả khi chức năng của CA do bên thuê ngoài đảm nhận.		
11.6	(Điều OVR-6.7.6-01 Mục Representation and Warranties của tiêu chuẩn ETSI TS 119431-1)			
11.7	(Điều OVR-6.7.13-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1)	Các điều khoản và điều kiện phải nêu rõ cho mỗi chính sách dịch vụ tin cậy được CA hỗ trợ đối với hệ thống pháp luật hiện hành;		

11.8	(Điều OVR-6.7.13-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1)	CA phải có các chính sách và thủ tục để giải quyết các khiếu nại và tranh chấp nhận được từ khách hàng hoặc các bên phụ thuộc khác về việc cung cấp dịch vụ hoặc bất kỳ vấn đề liên quan nào khác.	Quy trình giải quyết khiếu nại riêng CA và đáp ứng Thông tư 05/2011/TT-BTTTT.	
11.9	(Điều OVR-6.7.15-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1)	CA phải đảm bảo rằng nó hoạt động một cách hợp pháp và đáng tin cậy: CA phải cung cấp bằng chứng về cách nó đáp ứng các yêu cầu pháp lý hiện hành.	CA sẽ có các chứng chỉ, các quy trình, điều kiện kỹ thuật tuân thủ theo Nghị định số 130/2018/NĐ-CP, Thông tư số 16/2019/TT-BTTTT hoặc các chứng chỉ kiểm toán của các tổ chức được nêu trong Công văn 105/NEAC-TĐPC	
11.10	(Điều OVR-6.8.1-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1	Tổ chức CA phải đáng tin cậy.	Tổ chức CA phải có giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng do Bộ TTTT cấp.	
11.11	(Điều OVR-6.8.1-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1	CA phải đảm bảo những người đăng ký hoạt động có thể truy cập các dịch vụ của mình để kiểm tra thông tin chứng thư số bằng đường dẫn "kiểm tra trạng thái CTS", đường dẫn "trạng thái thu hồi CTS, đường dẫn kiểm tra trạng thái CTS trực tuyến	CA có mô tả và hướng dẫn kiểm tra CTS trực tuyến, các đường dẫn CRL, OCSP và kiểm tra hợp đồng cung cấp dịch vụ giữa CA và thuê bao thể hiện theo mẫu tại TT31/2020/TT-BTTTT.	
11.12	(Điều OVR-6.8.1-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1	CA phải có sự ổn định tài chính và các nguồn lực cần thiết để hoạt động phù hợp với chính sách này.	Điều kiện về tại chính theo Khoản 2 Điều 13 Nghị định số 130/2018/NĐ-CP.	

11.13	(Điều OVR-6.8.1-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1	CA phải có các chính sách và thủ tục để giải quyết các khiếu nại và tranh chấp được từ khách hàng hoặc các bên tin tưởng khác về việc cung cấp dịch vụ hoặc bất kỳ vấn đề liên quan nào khác.	CA phải ban hành quy trình giải quyết khiếu nại cho riêng mình và đáp ứng Thông tư 05/2011/TT-BTTTT.	
11.15	(Điều OVR-6.8.1-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1	CA phải có một thỏa thuận được lập thành văn bản và mối quan hệ quy định bằng hợp đồng trong đó việc cung cấp dịch vụ liên quan đến hợp đồng phụ, thuê ngoài hoặc các thỏa thuận của bên thứ ba khác.	Kiểm tra các điều kiện của bên thứ 3 bằng hình thức kiểm tra hợp đồng, quy định về trách nhiệm (Hợp đồng theo Thông tư 31/2020/TT-BTTTT)	
11.16	(Điều OVR-6.8.1-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1	Các nhiệm vụ và lĩnh vực trách nhiệm xung đột phải được tách biệt để giảm cơ hội sửa đổi trái phép hoặc vô ý hoặc sử dụng sai tài sản của CA.		
11.17	(Điều OVR-6.8.1-01 Mục Dispute resolution procedures của tiêu chuẩn ETSI TS 119431-1	CA phải cung cấp các điều khoản và điều kiện liên quan đến dịch vụ của mình cho tất cả thuê bao và các bên tin tưởng.		
11.18		Các điều khoản và điều kiện ít nhất phải chỉ rõ cho từng chính sách dịch vụ tin cậy được CA hỗ trợ như sau: a) chính sách dịch vụ tin cậy đang được áp dụng; Đã bật chế độ hỗ trợ trình đọc màn hình. b) bất kỳ hạn chế nào trong việc sử dụng dịch vụ; c) nghĩa vụ của thuê bao, nếu có;	Kiểm tra các điều kiện của bên thứ 3 bằng hình thức kiểm tra hợp đồng, quy định về trách nhiệm (Hợp đồng theo Thông tư 31/2020/TT-BTTTT)	

		d) thông tin cho các bên tin tưởng dịch vụ tin cậy; e) khoảng thời gian mà nhật ký sự kiện của CA được lưu giữ; f) trách nhiệm pháp lý; g) các hạn chế trong việc sử dụng các dịch vụ được cung cấp bao gồm giới hạn cho các thiệt hại phát sinh từ việc sử dụng dịch vụ vượt quá hạn chế đó; h) hệ thống pháp luật hiện hành; i) thủ tục khiếu nại và giải quyết tranh chấp; j) dịch vụ tin cậy của CA được đánh giá là phù hợp với chính sách dịch vụ tin cậy chưa và nếu có thì thông qua sơ đồ đánh giá sự phù hợp như thế nào; k) thông tin liên hệ của CA; l) bất kỳ cam kết nào liên quan đến tính khả dụng của dịch vụ.		
11.19		Thuê bao và các bên dựa vào dịch vụ tin cậy phải được thông báo về các điều khoản và điều kiện chính xác, bao gồm các mục được liệt kê ở trên, trước khi tham gia vào hợp đồng.	Văn bản quy định hoặc xác nhận trước khi tham gia vào HĐ (đơn đăng ký)	
11.20		TC4. Các điều khoản và điều kiện phải được cung cấp thông qua một phương tiện liên lạc lâu dài.	Hướng dẫn tra cứu thông tin của thuê bao, đường link tra cứu thông tin thuê bao	

11.21		TC5. Các điều khoản và điều kiện phải có sẵn bằng ngôn ngữ dễ hiểu.		
11.22		TC6. Các điều khoản và điều kiện có thể được đăng dưới dạng điện tử.		

❖ *Để đảm bảo cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa, các Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng cần đáp ứng 100% các tiêu chí đánh giá được mô tả ở trên.*