QUẢN LÝ VERSION

THÔNG TIN CÁC CÁN BỘ THAM GIA

BẢNG CÁC THUẬT NGỮ SỬ D

STT	Thuật ngữ trong Chuẩn	Diễn giải
1	API	Giao diện chương trình ứng dụng
2	ASN	Tóm tắt cú pháp ký hiệu
3	CA	Cơ quan chứng thực
4	CC	Tiêu chí chung, ISO / IEC 15408, Tiêu chí đánh giá về bảo mật CNTT
5	CEN	Ủy ban tiêu chuẩn hóa châu Âu
6	CRL	Danh sách chứng thư số thu hồi
7	CSC	Hiệp hội chữ ký đám mây
8	DSS-X	Dịch vụ chữ ký số mở rộng
9	DSV	Digital Signature Value:Giá trị ch ữ ký số
10	DTBS/R	Đại diện của dữ liệu sẽ được ký
11	DTBS	Data To Be Signed:Dữ liệu sẽ đư ợc ký
12	DTBSF	Định dạng của dữ liệu sẽ được ký
13	DTBSR (Data To Be Signed Representation)	Đại diện của Dữ liệu được ký
14	EAL	Mức đảm bảo đánh giá
15	ECDSA	Thuật toán chữ ký số đường cong Elliptic
16	eID (electronic Identification)	xác thực điện tử
17	EN	Tiêu chuẩn Châu Âu
18	ETSI	Viện tiêu chuẩn viễn thông châu Âu
19	EUSCP (EU SSASC Policy)	Chính sách SSASC của EU
20	HTTP	Giao thức truyền văn bản
21	ISO/IEC	Tổ chức tiêu chuẩn quốc tế / Ủy ban kỹ thuật điện quốc tế
22	ISO	Tổ chức tiêu chuẩn quốc tế
23	ISSS	Hệ thống tiêu chuẩn hóa xã hội thông tin
24	JPEG	Nhóm chuyên gia chụp ảnh chung
25	JSON	Ký hiệu đối tượng tập lệnh Java
26	JWT	Mã thông báo web JSON

27	LSCP (Lightweight SSASC Policy)	Chính sách SSASC nhẹ
28	LT	dài hạn
29	LTA	Lưu trữ dài hạn
30	NCP (Normalized Certificate Policy)	Chính sách chứng thư chuẩn hóa
31	NSCP (Normalized SSASC Policy)	Chính sách SSASC được chuẩn hóa
32	OASIS (Organization for the Advancement of Structured Information Standards)	Tổ chức vì sự tiến bộ của các tiêu chuẩn thông tin có cấu trúc
33	OCSP	Giao thức trạng thái chứng chỉ trực tuyến
34	OID	Mã định danh đối tượng
35	PNG	Đồ họa mạng di động
36	QES (Qualified Electronic Signature)	Chữ ký điện tử đủ tiêu chuẩn hoặc con dấu điện tử đủ tiêu chuẩn
37	QSCD (Qualified electronic Signature/Seal Creation Device)	Thiết bị tạo chữ ký / đóng dấu điện tử đủ tiêu chuẩn
38	RA	Cơ quan đăng ký
39	RSA	Rivest, Shamir, và Adman
40	SAD	Signature Activation Data:Dữ liệu kích hoạt chữ ký
41	SAM	Mô-đun kích hoạt chữ ký
42	SAML	Ngôn ngữ đánh dấu truy cập bảo mật
43	SAP	Giao thức kích hoạt chữ ký
44	SCA	Signature Creation Application:Ứng dụng tạo chữ ký
45	SCAL	Mức độ đảm bảo kiểm soát duy nhất
46	SCAL1	Đảm bảo kiểm soát duy nhất cấp 1
47	SCAL2	Đảm bảo kiểm soát duy nhất cấp 2
48	SCASC	SCASC Signature Creation Application Service Component:Thành phần dịch vụ ứng dụng tạo chữ ký

49	SCASP	SCASP Signature Creation Application Service Provider:Nhà cung cấp dịch vụ ứng dụng tạo ch ữ ký
50	SCDev (Signature Creation Device)	Thiết bị tạo chữ ký
51	SCP (SSASC Policy)	Chính sách SSASC
52	SCS (Signature Creation Service)	Dịch vụ tạo chữ ký
53	SCSP (Signature Creation Service Provider)	Nhà cung cấp dịch vụ tạo chữ ký
54	SD (Signer's Document)	Tài liệu của người ký
55	SDO (Signed Data Object)	Đối tượng dữ liệu đã ký
56	SDOC	Trình soạn thảo đối tượng dữ liệu đã ký
57	SDR	Đại diện tài liệu của người ký
58	SIC	Thành phần tương tác người ký
59	SLA (Service-Level Agreement)	Thỏa thuận cấp dịch vụ
60	SSA (Server Signing Application)	Ứng dụng ký máy chủ
61	SSA	Ứng dụng ký máy chủ
62	SSASC (Server Signing Application Service Component)	Thành phần dịch vụ ứng dụng ký máy chủ
63	SSASP (Server Signing Application Service Provider)	Nhà cung cấp dịch vụ ứng dụng ký máy chủ
64	SSA	Ứng dụng ký máy chủ
65	TSA (Time-Stamping Authority)	Cơ quan dấu thời gian
66	TSP (Trust Service Provider)	Nhà cung cấp dịch vụ ủy thác
67	TSP	Nhà cung cấp dịch vụ ủy thác
68	URI	Mã định danh tài nguyên thống nh ất
69	URI (Uniform Resource Identifier)	Mã định danh tài nguyên thống nh ất
70	URL	Trình định vị tài nguyên thống nhấ t
71	URN	Tên tài nguyên thống nhất
72	XML	Ngôn ngữ đánh dấu mở rộng

73	XSD	Định nghĩa lược đồ XML
74	CA	Cơ quan chứng nhận
75	Chính sách chữ ký	Chính sách tạo chữ ký, chính sách gia tăng chữ ký, chính sách xác thực chữ ký hoặc bất kỳ sự kết hợp nào của chữ ký, áp dụng cho cùng chữ ký hoặc bộ chữ ký
76	Chính sách tạo chữ ký	Tập hợp các ràng buộc tạo chữ ký được xử lý hoặc được SCA x ử lý
77	Chính sách tạo chữ ký	Tập hợp các ràng buộc tạo chữ ký được xử lý hoặc được xử lý b ởi SCASC hoặc SSASC
78	Chữ ký AdES (kỹ thuật s ố)	Chữ ký số là chữ ký CAdES hoặ c chữ ký PAdES hoặc chữ ký XAdES
79	Chữ ký số	Đơn vị dữ liệu được thêm vào ho ặc chuyển đổi mật mã dữ liệu cho phép người nhận đơn vị dữ liệu chứng minh nguồn và tính toàn vẹ n của đơn vị dữ liệu và bảo vệ ch ống giả mạo, ví dụ: bởi người nhậ n
80	Chữ ký xác thực	Bộ khóa ký và chứng chỉ ký tươ ng ứng
81	CM	Mô-đun mật mã được chứng nhậ n theo [EN 419 221-5]
82	CSR	Yêu cầu ký chứng nhận
83	Đại diện của Dữ liệu sẽ đ ược ký (data to be signed represenation)	Dữ liệu được định dạng được sử dụng để tính giá trị chữ ký số (ví dụ: giá trị băm) để xác định liệu chữ ký có phù hợp với một doanh nghiệp cụ thể hoặc mục đ ích pháp lý
84	Dịch vụ tạo chữ ký (signature creation sevice)	Cấu hình phần mềm và / hoặc mô-đun mật mã phần cứng được sử dụng để tạo chữ ký số. Dịch vụ TSP triển khai ứng dụng tạo chữ ký và / hoặc ứng dụng ký máy ch ủ
85	Dịch vụ ủy thác (trust service)	Dịch vụ điện tử giúp tăng cường niềm tin và sự tự tin trong các giao dịch điện tử

86	Đơn vị ủy thác (delegated party)	Nhà thầu phụ của TSP hoặc nhà cung cấp eID được thông báo theo quy định eIDAS được sử dụ ng để xác thực
87	DTBS/R (s)	Một hoặc một bộ DTBS/R.
88	Dữ liệu kích hoạt chữ ký (Signature activation data)	Bộ dữ liệu được thu thập bởi SAP, được sử dụng để kiểm soát với mức độ tin cậy cao của một hoạt động chữ ký nhất định, đượ c thực hiện bởi một mô-đun mật mã thay mặt cho người ký thuộc quyền kiểm soát duy nhất của ng ười ký. SAD có thể là kết quả củ a các hoạt động mật mã.
89	Dữ liệu nhận dạng người (person identification data)	Bộ dữ liệu cho phép nhận dạng cá nhân hoặc pháp nhân hoặc thể nhân đại diện cho một pháp nhân được thành lập
90	Giá trị chữ ký số (digital signature value)	Kết quả của một hoạt động mật mã liên quan đến khóa ký. Trong tài liệu này: Con dấu, Chữ ký, Ch ữ ký số hoặc Dấu kỹ thuật số biể u thị chữ ký số.
91	Giá trị chữ ký số (digital signature value)	Kết quả của việc chuyển đổi mật mã của một đơn vị dữ liệu cho phép người nhận đơn vị dữ liệu đ ể chứng minh nguồn và tính toàn vẹn của đơn vị dữ liệu và bảo vệ chống giả mạo, (bởi người nhận).
92	Giao thức kích hoạt chữ ký (signature activation protocal)	Giao thức thu thập SAD được sử dụng để kiểm soát hoạt động chữ ký trên (bộ) DTBS / R, sử dụng khóa ký của người ký
93	Giấy chứng nhận (certificat)	Giấy chứng nhận cho chữ ký điện tử
94	Hệ số xác thực (authentication factor)	Mẩu thông tin và / hoặc quy trình được sử dụng để xác thực hoặc xác minh danh tính của một thực thể
95	Hệ thống đáng tin cậy hỗ trợ ký máy chủ (trustworthy system supporting server signing)	Hệ thống máy khách-máy chủ sử dụng khóa ký dưới sự kiểm soát của người ký, để tạo chữ ký số."

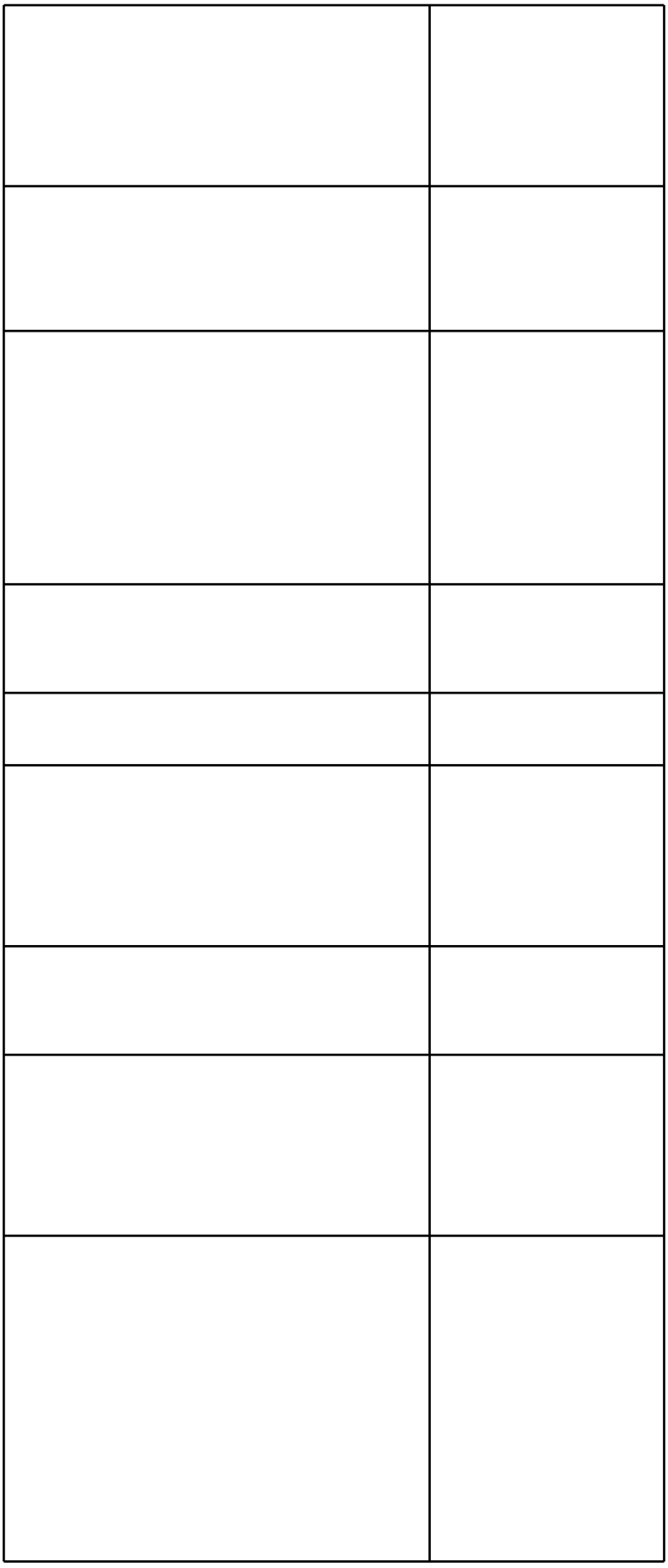
96	Khóa ký (siging key)	Khóa riêng của cặp khóa mật mã bất đối xứng được sử dụng để tạo chữ ký số
97	Khóa ký một lần (one-time signing key)	Khóa ký được tạo, sử dụng và xử lý dựa trên một ủy quyền duy nhất, thường được liên kết với một phiên ký DTBS/R (s). Trái ngược với các khóa ký có thể được sử dụng trong một số phiên ký.
98	Mô-đun kích hoạt chữ ký (signature activation module)	Phần mềm được định cấu hình sử dụng SAD để đảm bảo mức độ tin cậy cao rằng các khóa ký được sử dụng dưới sự kiểm soát duy nhất của người ký
99	Người ký (signer)	Thực thể (thể nhân hoặc pháp nhân) là người tạo chữ ký số
100	Nhà cung cấp dịch vụ tạo chữ ký (signature creationg service provider SCSP)	Nhà cung cấp dịch vụ cung cấp dịch vụ tạo chữ ký"
101	Nhà cung cấp dịch vụ ứng dụng ký máy chủ (server signing application service provider SSASP)	TSP vận hành một thành phần dịch vụ ứng dụng ký máy chủ (SSASC).
102	Nhà cung cấp dịch vụ ứng dụng tạo chữ ký (signature creation application service provider-SCASP)	TSP vận hành một thành phần dịch vụ ứng dụng tạo chữ ký
103	Nhà cung cấp dịch vụ ủy thác (trust service provider TSP)	Đơn vị cung cấp một hoặc nhiều dịch vụ ủy thác (trust service).
104	Nhà cung cấp dịch vụ ủy thác (trust service provider)	Thể nhân hoặc pháp nhân cung cấp một hoặc nhiều dịch vụ ủy thác
105	Nhận dạng điện tử (electronic identification eID)	Quá trình sử dụng dữ liệu nhận dạng người ở dạng điện tử đại diện duy nhất hoặc một thể nhân hoặc pháp nhân, hoặc một thể nhân đại diện cho một pháp nhân

106	Nhận dạng điện tử (electronic identification) có nghĩa là	Vật liệu và / hoặc đơn vị phi vật chất chứa dữ liệu nhận dạng ngư ời và đó là được sử dụng để xác thực cho một dịch vụ trực tuyến
107	Nhận dạng điện tử có ngh ĩa tham chiếu	Dữ liệu được sử dụng trong SSASC làm tham chiếu đến phư ơng tiện nhận dạng điện tử để xác thực người ký
108	Quy định của eIDAS	Quy định (EU) số 910/2014 của Nghị viện châu Âu và của Hội đồ ng về dịch vụ nhận dạng và ủy thác điện tử đối với các giao dịch điện tử trên thị trường nội bộ và bãi bỏ Chỉ thị 1999/93 / EC
109	Quy tắc áp dụng chữ ký	Bộ quy tắc, áp dụng cho một hoặ c nhiều chữ ký số, xác định các yêu cầu
110	Ràng buộc tạo chữ ký	Tiêu chí được sử dụng khi tạo ch ữ ký số
111	Thành phần dịch vụ ứng d ụng ký máy chủ (remote signature creation device component SSASC)	Thành phần dịch vụ TSP sử dụng 1 ứng dụng ký máy chủ tạo giá trị chữ ký số thay mặt cho người ký.
112	Thành phần tương tác ng ười ký (Signer's interaction component)	Thành phần phần mềm và / hoặc phần cứng được người ký sử dụ ng để hỗ trợ SAP
113	Thiết bị tạo chữ ký (signature creation device SCDev)	Phần mềm hoặc phần cứng được định cấu hình được sử dụng để tri ển khai dữ liệu tạo chữ ký và để t ạo ra một giá trị chữ ký số.
114	Thiết bị tạo chữ ký từ xa (remote signature creation device)	Thiết bị tạo chữ ký được sử dụng từ xa từ góc độ người ký và áp d ụng giao thức kích hoạt chữ ký đ ể cung cấp quyền kiểm soát hoạt động ký thay mặt và đảm bảo mứ c độ tin cậy cao rằng các khóa ký được sử dụng dưới sự kiểm soát duy nhất của người ký

115	Thiết bị tạo chữ ký từ xa (remote signature creation device)	Thiết bị tạo chữ ký được sử dụng từ xa từ góc độ người ký và cung cấp kiểm soát hoạt động ký thay mặt người ký.
116	thiết bị tạo chữ ký từ xa (remote signature creation device)	Thiết bị tạo chữ ký sử dụng từ xa từ góc độ người ký và cung cấp điều khiển hoạt động ký kết nhân danh của người ký
117	Thiết bị tạo chữ ký từ xa	Thiết bị tạo chữ ký được sử dụng từ xa từ góc độ người ký và cung cấp quyền kiểm soát hoạt động ký thay mặt cho người ký
118	Thiết bị tạo chữ ký	Phần mềm hoặc phần cứng được định cấu hình được sử dụng để tri ển khai dữ liệu tạo chữ ký và để t ạo giá trị chữ ký số
119	Ứng dụng khách	Ứng dụng chạy trong môi trường người ký truy cập các dịch vụ do SCASC và / hoặc SSASC cung cấp
120	Ứng dụng ký máy chủ (server signing application SSA)	Ứng dụng sử dụng thiết bị tạo ch ữ ký từ xa để tạo giá trị chữ ký s ố thay mặt cho người ký
121	Ứng dụng tạo chữ ký (SCA)	Ứng dụng trong hệ thống tạo chữ ký tạo chữ ký số AdES và dựa vào SCDev để tạo giá trị chữ ký số. SCDev có thể được quản lý b ởi SSASC.
122	Ứng dụng tạo chữ ký (signature creationg application-SCA)	Ứng dụng trong hệ thống tạo chữ ký tạo chữ ký số AdES và dựa vào SCDev để tạo giá trị chữ ký số. SCDev có thể được quản lý b ởi SSASC.
123	Xác thực (authentication)	Cung cấp sự đảm bảo danh tính c ủa một thực thể

ỤNG TRONG CHUẨN

Quy định tại VN	Ghi chú thêm
có/chưa/tương đương/…	



STT	Số tham chiếu	Tiêu chí/nhóm tiêu
	<Số tham chiếu	<Tên nhóm tiêu chí/
1		Introduction
2	1	Scope
3	2	References

4	2.1	Normative references

5	2.2	Informative references
6	3	Definition of terms, abbreviations and notations

7	3.1	Terms

8	3.2	Abbreviations

9	3.3	Notation

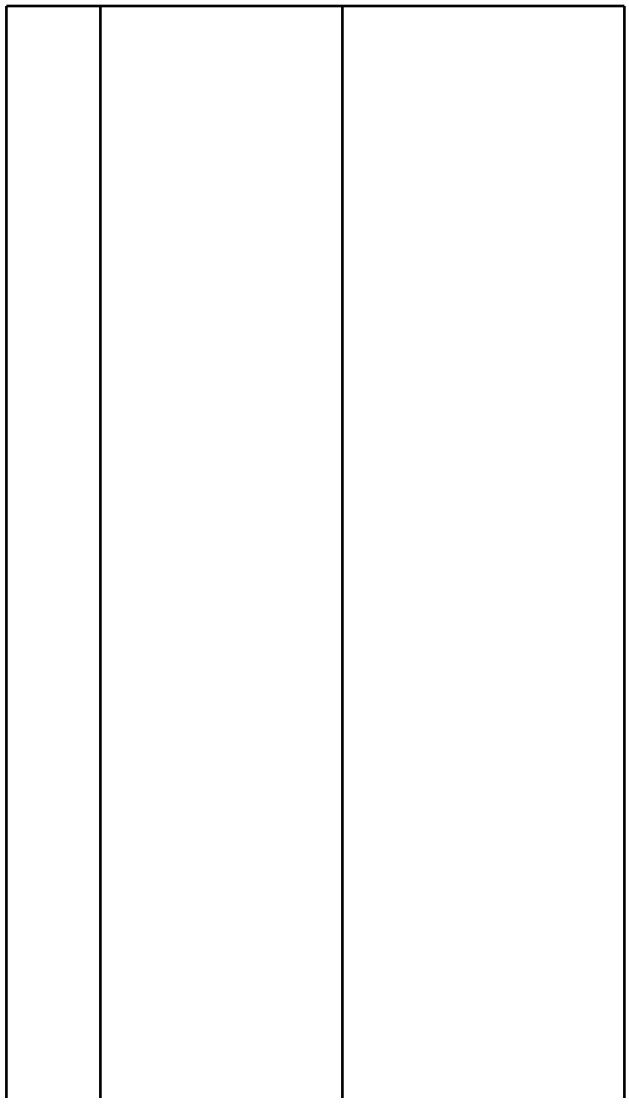
1	4.1	General policy requirements concepts
2	4.2	Signature creation application service component applicable documentation

2.1	4.2.1	Signature creation application service component practice statement

2.2	4.2.2	Signature creation application service component policy
2.3	4.2.3	Terms and conditions

2.4	4.2.4	Other documents associated with signature creation

3	4.3	Architecture
4	5	Risk assessment
5	6	Policies and practices



5.1	6.1	Trust service practice statement

5.2	6.2	Terms and Conditions

5.3	6.3	Information security policy

6	7	Signature creation application service management and operation
6.1	7.1	Internal organization

6.2	7.2	Human resources
6.3	7.3	Asset management

6.4	7.4	Access control
6.5	7.5	Cryptographic controls
6.6	7.6	Physical and environmental security

6.7	7.7	Operation security

6.8	7.8	Network security

6.9	7.9	Incident management

6.10	7.10	Collection of evidence
6.11	7.11	Business continuity management

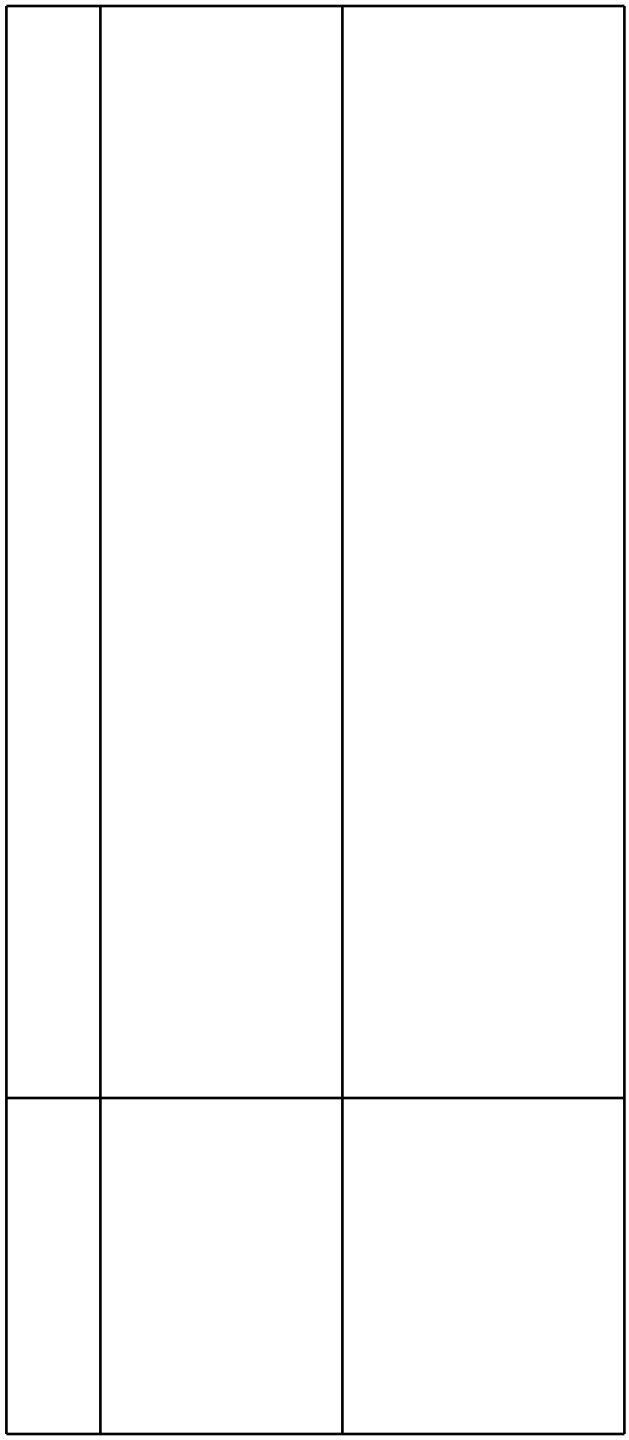
6.12	7.12	Termination and termination plans

6.13	7.13	Compliance and legal requirements
7	8	Signature creation application service component technical requirements

7.1	8.1	Interface
7.2	8.2	AdES digital signature creation

		creation
8	9	Framework for definition of signature creation application service component policy built on the present document

		Annex A (informative)



		Annex B (normative):
		Annex C (informative):

Yêu cầu
<Nội dung yêu cầu trong tiêu chuẩn>
The creation of digital signatures can involve different tasks provided by trust service providers. This can cover not only the creation and management of certificates as described in ETSI EN 319 411-1 [i.7] but also the management of signing keys as described in ETSI TS 119 431-1 [i.8] or the creation of the AdES digital signature as described in the present document. The present document gives no restrictions on where signing key management is done. It can be handled either by a server signing application service component SSASC as described in ETSI TS 119 431-1 [i.8] or directly by the client in a signature creation device (SCDev).
The present document provides policy and security requirements for trust service providers (TSP) implementing a service component supporting AdES digital signature creation. This component contains a signature creation application and is thus called signature creation application service component (SCASC). However, it is more than just the SCA. It contains service elements around which parts of the driving application as defined in ETSI TS 119 102-1 [1] and ETSI TS 119 101 [2] can be implemented. The present document does not give restrictions on whether something is covered within a signature creation application or outside, as long as it is done by the SCASC. The present document gives no restrictions on the type of TSP implementing such a service component. The present document aims at supporting the creation of digital signatures in European and other regulatory frameworks. NOTE 1: Specifically, but not exclusively, the present document is aimed at trust services, supporting the creation of digital signatures in accordance with the requirements of the Regulation (EU) No 910/2014 [i.1] for electronic signatures and electronic seals (both advanced and qualified). Annex B contains specific requirements for SCASC in the context of Regulation (EU) No 910/2014 which aim at providing best practice requirements for the creation of advanced electronic signatures and seals based on X.509 certificates. NOTE 2: Specifically, but not exclusively, digital signatures in the present document can be used to create electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1]. The present document may be used by competent bodies as the basis for

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.
Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.
NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.
The following referenced documents are necessary for the application of the present document.
[1] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".
[2] ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
[3] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".
[4] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".
[5] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".
[6] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".
[7] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI);

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. .

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.3] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents". .

[i.4] CEN EN 419 241-1: "Trustworthy Systems Supporting Server

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.2] and the following apply:

AdES (digital) signature: digital signature that is either a CAdES signature, or a PAdES signature or a XAdES signature

digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

digital signature value: result of the cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

remote signature creation device: signature creation device used remotely from signer perspective and provides control of signing operation on the signer's behalf

server signing application: application using a remote signature creation device to create a digital signature value on behalf of a signer

server signing application service component: TSP service component employing a server signing application

server signing application service provider: TSP operating a server signing application service component

signature applicability rules: set of rules, applicable to one or more digital signatures, that defines the requirements

for determination of whether a signature is fit for a particular business or legal purpose

NOTE: Signature applicability rules can be implicit, or can be stated in a human readable document and/or in a machine processable from. ETSI TS 119 172-1 [i.3] can be used for this purpose.

signature creation application: application within the signature creation system that creates the AdES digital signature and relies on the SCDev to

For the purposes of the present document, the abbreviations given in ETSI TS 119 001 [i.2] and the following apply:

CA Certification Authority
DTBS Data To Be Signed
DTBSR Data To Be Signed Representation
OID Object IDentifier

QES Qualified Electronic Signature or Qualified Electronic Seal
SAD Signature Activation Data
SCA Signature Creation Application
SCASC Signature Creation Application Service Component
SCASP Signature Creation Application Service Provider
SCDev Signature Creation Device
SCS Signature Creation Service
SCSP Signature Creation Service Provider
SD Signer's Document
SDO Signed Data Object
SLA Service-Level Agreement
SSA Server Signing Application
SSASC Server Signing Application Service Component
SSASP Server signing application service provider
TSA Time-Stamping Authority
URI Uniform Resource Identifier

The requirements identified in the present document include:
a) requirements applicable to any TSP conforming to the present document. Such requirements are indicated by clauses without any additional marking;
b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]".
The requirements in the present document are identified as follows:
<the 3 letters identifying the elements of services > - < the clause number> - <2 digit number - incremental>
The elements of services are:
• OVR: General requirement (requirement applicable to more than 1 component)
• ASI: AdES signing interface
The management of the requirement identifiers for subsequent editions of the present document is as follows:
• When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
• When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
• The requirement identifier for deleted requirements are left and completed with "VOID".
• The requirement identifier for modified requirement are left v

The present document is structured in line with ETSI EN 319 401 [9]. It incorporates ETSI EN 319 401 [9] requirements by reference and adds requirements relevant for a SCASP
See ETSI EN 319 401 [9], clause 4 for guidance for guidance on general policy requirements

Trust services can encompass but is not limited to the issuance of public key certificates, provision of registration services, time-stamping services, long term preservation services, e-delivery services and/or signature validation services.
These policy requirements are not meant to imply any restrictions on charging for TSP's services.
The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objectives will be met.
When implementing controls of clause 7, ISO/IEC 27002:2013 [i.3] should be applied.
NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSP can employ in providing services.

The signature creation application service provider (SCASP) develops, implements, enforces, and updates a SCASC practice statement which is a trust service practice statement such as defined in ETSI EN 319 401 [9], instantiated for a signature creation application service component. See clause 6.1.
The SCASC practice statement describes how the SCASP operates its service and is owned by the SCASP. The SCASC practice is tailored to the organizational structure, operating procedures, facilities, and computing environment of a TSP. The recipients of the practice statement can be auditors, subscribers and relying parties.
NOTE: The presence of some elements is mandatory in the SCASC practice statement as requested in the present document, however the present document places no restriction on the form of the SCASC practice statement; it can be included in a general TSP practice statement document that covers other services delivered by that TSP or it can be a standalone document. Annex A provides a recommended table of content.

The present document provides requirements identified as necessary to support a high-level SCASC policy, to be endorsed by a SCASP and reflected in its practice statement.

6.1 Trust Service Practice statement
REQ-6.1-03: The TSP shall have a statement of the practices and procedures for the trust service provided.
NOTE: The present document makes no requirement as to the structure of the trust service practice statement.

A SCASC policy describes what is offered and can contain diverse information beyond the scope of the present document to indicate the applicability of the service. A SCASC policy is defined independently of the specific details of the specific operating environment of a SSASP. The recipients of the service policy can be auditors, subscribers and relying parties.
The present document can be referred by such a SCASC policy to provide information about the level of the service.
SCASPs conforming to the present document's normative requirements except those defined in annex B may use in its documentation the following specific OID:
itu-t(0) identified-organization(4) etsi(0) CREATION SERVICE-policies(19431) ades (2) policy-identifiers(1) main (1) SCASPs conforming to the present document's normative requirements including those defined in annex B may use in its documentation the following specific OID:
itu-t(0) identified-organization(4) etsi(0) CREATION SERVICE-policies(19431) ades (2) policy-identifiers(1) eu-advancedx509 (2)
A SCASC policy is not necessarily part of the SCASP's documentation (as per ETSI EN 319 401 [9] a practice statement and general terms and conditions are sufficient); e.g. a SCASC policy can be shared by a community and not owned by the SCASP. Also, the present document does not put constraints on the form of the SCASC policies; a SCASC policy can be a stand-alone document or be provided as part of the practice statements and/or the general terms and conditions.
The present document does not put any limitation on the content of the SCASC policies but it is requested that the SCASP provides minimal information about the service it offers (see clauses 6.1 and 6.2).

In addition to the SCASC practice statement and, when issued by the SCASP, the SCASC policy, the SCASP also issues terms and conditions, see clause 6.2. Terms and conditions can cover a broad range of commercial terms or technical terms that are not necessarily communicated to the customer, etc. The terms and conditions are specific to a SCASP. The recipients of the terms and conditions can be the subscribers and the relying parties.
NOTE: The presence of some elements is mandatory in the terms and conditions as requested in the present document, however the present document places no restriction on the form of terms and conditions; it can be a standalone document for a public audience, or it can be split over subscriber's agreement(s) and information to relying parties. The form and content of the terms and conditions can also depend on national regulations.

Besides the description of the practices employed by the SCASP to offer the AdES digital signature creation service, it is important to document the criteria under which the signatures are created and, beyond this, can then be determined as fitting a certain business need.

Two documents can be used for these purposes:

• A signature creation policy which is the set of signature creation constraints processed by the SCA. A signature creation policy can be identified by means of an OID;

• Signature applicability rules that can be structured as per ETSI TS 119 172-1 [i.3] and can include a signature creation policy containing the signature creation constraints to be applied by the SCA, as well as other criteria showing the applicability of the created signature so certain business needs.

NOTE: The use of signature applicability rules is outside the scope of the present document but can be applied as an extension to the signature creation service as covered by the present document.

The SCASC practice statement, the signature creation policy and the signature applicability rules are different types of documentation; the SCASC practices statement describe how the SCASP operates its service, while the signature creation policy states the constraints to be processed by a SCA when creating a signature. Going beyond the scope of a signature creation policy, the signature applicability rules state the rules and assumptions used by a user to decide whether a signature created according to these rules is fit for purpose.

The owner of the SCASC practice statement is a SCASP, while the owner of the signature applicability rules is usually the signatory.

A TSP service component supporting AdES digital signature creation (SCASC) receives the document(s) and/or hash(es) of document(s) to be signed and optionally some signing parameters, collects all necessary information to create the signature, prepares the data-to-be-signed representation (DTBSR) and sends this to the SCDev. The SCDev can be either in the user's environment or managed by a remote server signing application service component (SSASC) as described in ETSI TS 119 431-1 [i.8]. For the purpose of the present document, it is assumed that the SCDev handles the authentication and the agreement to sign with the user and returns the digital signature value, without going into details if this is done by the SCDev itself or the component managing the SCDev. The authorization to use the signing key within the SCDev can go through the SCASC but can also be done directly by communication between the signer and the SCDev. The digital signature value is included by the SCASC into the digital signature.
NOTE: The SCASC represents the signature creation application in CEN EN 419 241-1 [i.4].

The requirements specified in ETSI EN 319 401 [9], clause 5 shall apply

The requirements specified in ETSI EN 319 401 [9], clause 6.1 shall apply.
In addition, the following particular requirements apply

When the SCASC supports the inclusion of time-stamp tokens in the AdES digital signature, the SCASC practice statement shall list which TSA are used
The SCASC practice statement shall specify all the supported signature creation polices
The SCASC practice statement shall specify all the supported signature formats
The SCASC practice statement shall specify all the supported signature classes. NOTE: ETSI TS 119 102-1 [2] describes different signature classes
The SCASP shall identify in the SCASC practice statements the obligations of all external organizations supporting its services including the applicable policies and practices

The requirements specified in ETSI EN 319 401 [9], clause 6.2 shall apply In addition, the following particular requirements apply
To specify the trust service policy being applied, the SCASC terms and conditions shall list or make reference to (e.g. through OIDs), and briefly describe, the supported SCASC policies it conforms to
To specify the trust service policy being applied, the SCASC terms and conditions may use the OIDs defined in clause 4.2.2
The main OID, as defined in clause 4.2.2, shall only be used in relation with an SCASC if the SCASC conforms to the normative requirements in the main part of the present standard (excluding annex B).
The eu-advanced-x509 OID, as defined in clause 4.2.2, shall only be used in relation with an SCASC if the SCASC conforms to the normative requirements in the main part of the present standard and the ones in annex B.
The terms and conditions shall indicate the rights and obligations of the SCASP and the signer

The terms and conditions shall describe the options supported by the service. At least: a) the supported signature formats, EXAMPLE: CAdES [3], [4], XAdES [5], [6] or PAdES [7],[8]. b) the supported signature parameters, c) if the to be signed document can be provided only as a hash, and d) the supported signature creation devices (SCDev) in the user's environment or the supported SSASCs creating the digital signature value for the signer.
The terms and conditions shall include Service-Level Agreement (SLA) elements for the availability of the service and when applicable, other SLA information such as response times
The terms and conditions shall provide a notice that the SLA can be affected by the practices, policies and SLAs of other TSPs, not under the control of the SCASP like the CA issuing the certificate used for the signature or a TSA used for a time-stamp
The terms and conditions shall explain how the SCASP processes personal data
The requirements specified in ETSI EN 319 401 [9], clause 6.3 shall apply. In addition, the following particular requirement apply

The security policy should document the security and privacy controls implemented to protect personal data. NOTE: If the SCASP has access to the to be signed data, then this can contain confidential information as well as personal data
The requirements specified in ETSI EN 319 401 [9], clause 7.1 shall apply

The requirements specified in ETSI EN 319 401 [9], clause 7.2 shall apply
The requirements specified in ETSI EN 319 401 [9], clause 7.3 shall apply

The requirements specified in ETSI EN 319 401 [9], clause 7.4 shall apply
The requirements specified in ETSI EN 319 401 [9], clause 7.5 shall apply
The requirements specified in ETSI EN 319 401 [9], clause 7.6 shall apply. In addition the following particular requirement apply
The following requirement specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SCA: GSM 1.4

The requirements specified in ETSI EN 319 401 [9], clause 7.7 shall apply. In addition, the following particular requirements apply
The following requirements specified in ETSI TS 119 101 [1], clause 5.2 should apply to the SCA: GSM 1.2 and GSM 1.3.
The following requirements specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SCA: GSM 2.4
The SCASC shall implement all mandatory requirements from ETSI TS 119 101 [1] referenced above regardless of whether the requirement is imposed on the DA or the SCA

The requirements specified in ETSI EN 319 401 [9], clause 7.8 shall apply

The requirements specified in ETSI EN 319 401 [9], clause 7.9 shall apply

The requirements specified in ETSI EN 319 401 [9], clause 7.10 shall apply. In addition the following particular requirements apply
Any AdES digital signature creation operation shall be logged, together with identification of the subscriber when this information is known
Event logs shall be marked with the time of the event
The frequency of processing, the retention period, the protection, the back-up procedures of the collection system, the archiving procedures and the vulnerability assessment of the event logs shall be documented in the SCASC practice statement
The implementation of requirements OVR-7.10.1 and OVR-7.10.2 shall take the applicable privacy requirements into account
Event logs should include the type of the event, the event success or failure, and an identifier of the person and/or component at the origin for such an event
The requirements specified in ETSI EN 319 401 [9], clause 7.11 shall apply In addition, in order to provide business continuity as specified in the terms and conditions the following particular requirements apply

Measures should be implemented to avoid interruptions of the service due to intentional or unintentional behaviour of users or third parties
When adding time-stamps to the signature, the SLA of the SCASP should take the SLA of the corresponding TSA into account
The requirements specified in ETSI EN 319 401 [9], clause 7.12 shall apply

The requirements specified in ETSI EN 319 401 [9], clause 7.13 shall apply In addition, the following particular requirements apply
When personal data is processed by a third party, if needed by the law, an appropriate agreement shall be made with third party processors of personal data in order to ensure that they do comply with the legal requirements, including the implementation of technical, organizational and legal measures to protect the personal data. NOTE 1: The data to be signed is to be considered as personal data
The SCASC shall not store the SD after processing when not necessary. NOTE 2: If the SCASP works in combination of a preservation service there can be a need to keep such data
The SCASP shall have the overall responsibility for meeting the requirements defined in clauses 5 to 8 even when some or all of its functionalities are undertaken by sub-contractors
When the SCASC has a machine accessible interface to contact its service, it should use the protocol defined in ETSI TS 119 432 [i.9].
The connection between the SCASC and the SCDev used for creation of the digital signature value shall be secured
When the SCASC presents the document to the signer, it shall describe in its SCASC practice statement how it guarantees that What You See Is What You Sign (WYSIWYS)

When the SCASC presents the document to the signer in an interpreted way, the SCASC practice statement shall clearly state how it interprets specific data EXAMPLE: The document to be signed is XML format, and the practice statement states which software is used for the presentation or which rules are followed to present the different XML tags
When the SCASC presents the document to the signer, the SCASC practice statement or the terms and conditions shall state which content types can be correctly presented
When the SCASC presents the document to the signer, the interface shall warn the signer if it cannot accurately present all parts of the SD according to the data content type
When the SCASC provides a graphical user interface to the client the requirements UI 1 and UI 2 from ETSI TS 119 101 [1] should apply
When the SCASC presents the document to the signer, it shall have a workflow where it is clear to the signer that the signer consents to the signing of the document
When the SCASC presents the document to the signer, SCP 13 and SCP 47 of ETSI TS 119 101 [1] shall apply
When the SCASC presents the document to the signer, the SCASC should allow to download the document to be signed
When the SCASC presents the document to the signer, the SCASC should log for how long the document was presented to the signer
When the SCASC presents the document to the signer and the document was downloaded, the SCASC should log such an event
The SCASC shall guarantee the integrity and confidentiality of the received information
The cryptographic algorithms used should be selected from algorithms recommended by ETSI TS 119 312 [i.5] NOTE 1: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations
The cryptographic algorithms applied shall be as defined in signature creation policy
SCP 14, SCP 31, SCP 37 and SCP 61 of ETSI TS 119 101 [1] shall apply
The SCASC shall inform the signer of the commitment type NOTE 2: This information can be given within the signature policy
The SCASC should include the signing certificate chain into the signature
The signer shall be able to know which signature creation policy will be applied

The signer shall be able to know which signature creation policy was applied when creating a specific the signature EXAMPLE 1: The information on which signature creation policy will or was applied for a specific signature can be known from the user account of the signer EXAMPLE 2: The signature creation policy can be added as a signed attribute to the signature EXAMPLE 3: The SCASP has only one signature creation policy in force at each time, and from the time of signature it is clear which version applies
The SCASC should provide the signature to the signer
If the SCASC has access to the signed data, it should provide the signed data together with the signature to the signer NOTE 3: In case the signature is enveloped in or enveloping the signed data, OVR-8.2-09 follows directly from OVR-8.2-08
When building a SCASC policy built on requirements defined in the present document; the policy shall incorporate, or further constrain, all the requirements identified in clauses 5 to 8
When building a SCASC policy built on requirements defined in the present document; the policy shall identify any variances it chooses to apply
When building a SCASC policy built on requirements defined in the present document; subscribers shall be informed, as part of implementing the terms and conditions, of the ways in which the specific policy adds to or further constrains the requirements of the policy as defined in the present document
When building a SCASC policy built on requirements defined in the present document; there shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the policy
When building a SCASC policy built on requirements defined in the present document; a risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the policy for the stated community and applicability
When building a SCASC policy built on requirements defined in the present document; the policy shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy
When building a SCASC policy built on requirements defined in the present document; a defined review process shall exist to ensure that the policy is supported by the practices statements

When building a SCASC policy built on requirements defined in the present document; the TSP should make available the policies supported by the TSP to its user community
When building a SCASC policy built on requirements defined in the present document; revisions to policies supported by the TSP should be made available to subscribers
When building a SCASC policy built on requirements defined in the present document; a unique object identifier shall be obtained for the policy (e.g. OID or URI)
1. Introduction 1.1 Overview 1.1.1 TSP identification 1.1.2 Supported signature creation application service component policy/ policies (formal OID/URI identification) 1.2 Signature creation application service component environment 1.2.1 SCASC actors 1.2.3 Service architecture 1.3 Definitions and abbreviations 1.3.1 Definitions 1.3.2 Abbreviations 1.4 Policies and practices 1.4.1 Organization administrating the TSP documentation 1.4.2 Contact person 1.4.3 TSP (public) documentation applicability This clause describes the set of documents related to the SCASC, their applicability, and position of the present practice statement within the documentation, their distribution points. At a minimum the following documents exist and need a short description: • the present practice statement (formal OID/URI identification should be used); • the terms and conditions; • the service policy (can be referred) one or more of the above documents identify the supported signature creation policy/policies (with formal OID/URI identification). The supported signature creation policy/policies are generally detailed in the SCASC service policy/policies. • risk assessment and Information security policy

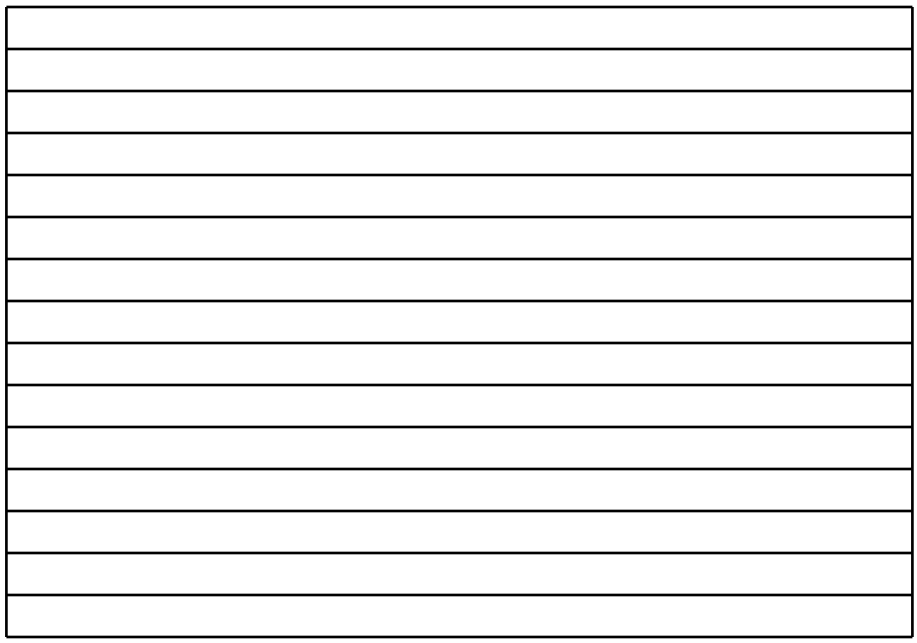
2. Trust Service management and operation
This clause may be common to all services offered by the TSP – except for CA services where the table of content described by IETF RFC 3647 should be applied.
(Either the same clause is reproduced for each service practice statement, in which case, because every service policy and security requirements add elements specific to the services, such requirements need to be addressed in addition, OR there is a common clause that is referred to from each service practice statement).
2.1 Internal organization
2.1.1 Organization reliability
(This clause identifies the obligations of all external organizations supporting the TSP services including the applicable policies and practices (per ETSI EN 319 401 [9])
2.1.2 Segregation of duties
2.2 Human resources
2.3 Asset management
2.3.1 General requirements
2.3.2 Media handling
2.4 Access control
2.5 Cryptographic controls
2.6 Physical and environmental security
2.7 Operation security
2.8 Network security
2.9 Incident management
2.10 Collection of evidence
2.11 Business continuity management
2.12 TSP termination and termination plans
2.13 Compliance

3. Signature creation application service component technical requirements

3.1 Interfaces
This clause contains requirements, control objectives and controls in connection with clause 8.1. in ETSI TS 119 431-2.
3.2 AdES digital signature creation
This clause contains requirements, control objectives and controls in connection with clause 8.2. in ETSI TS 119 431-2

NOTE: This clause aims at providing best practices for the creation of advanced electronic signatures/seals based on X.509 certificates. OVR-B.1-01: [CONDITONAL] Where the SCASC is used to create an advanced electronic signature, the signing certificate shall identify the signatory. OVR-B.1-02: [CONDITONAL] Where the SCASC is used to create an advanced electronic seal, the signing certificate shall identify the creator of the seal. OVR-B.1-03: The signing certificate shall be contained in the created AdES signature.
Table C.1 maps the requirements from the present document with the requirements on advanced electronic signatures or seals as specified directly by Regulation (EU) No 910/2014 [i.1] (Tables 1 and 2) or indirectly via requirements on valid QES as specified by Regulation (EU) No 910/2014 [i.1] (Table 3).
Article 26 Requirements for advanced electronic signatures "An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory; OVR-B.1-01 OVR-8.2-04 referencing from ETSI TS 119 101 [1] SCP 37: "The SCA shall protect the reference to or copy of the signing certificate within the signature from undetected replacement after the signature has been created."
(b) it is capable of identifying the signatory; OVR-B.1-03

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and The sole control is out of scope of the present document. If a SSASC is used, this is covered in ETSI TS 119 431-1 [i.8]. See note.
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable." OVR-8.2-02 The cryptographic algorithms used should be selected from algorithms recommended by ETSI TS 119 312 [i.5].
NOTE: The SSASC can limit the list of supported SCDev in its terms and conditions (OVR-6.2-05).
Article 36 Requirements for advanced electronic seals "An advanced electronic seal shall meet the following requirements:
(a) it is uniquely linked to the creator of the seal; OVR-B.1-02 OVR-8.2-04 referencing from ETSI TS 119 101 [1] SCP 37
(b) it is capable of identifying the creator of the seal; OVR-B.1-03
(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and The sole control is out of scope of the present document. If a SSASC is used, this is covered in ETSI TS 119431-1 [i.8]. See note.
(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable." OVR-8.2-04 referencing from ETSI TS 119 101 [1] SCP 14
NOTE: The SSASC can limit the list of supported SCDev in its terms and conditions (OVR-6.2-05).



Diễn giải yêu cầu
<Phần này sẽ diễn giải theo ý hiểu yêu cầu cần phải đáp ứng là gì
TPS cung cấp: - Tạo và quản lý chứng thư - Quản lý khóa ký - Tạo chữ ký số AdES Quản lý khóa ký có thể được xử lý bởi: - Thành phần dịch vụ ứng dụng ký máy chủ (SSASC). - Hoặc trực tiếp bởi khách hàng trong một thiết bị tạo chữ ký (SCDev).
Tài liệu hiện tại cung cấp các yêu cầu chính sách và bảo mật cho các nhà cung cấp dịch vụ ủy thác (TSP) triển khai thành phần dịch vụ hỗ trợ tạo chữ ký số AdES. Thành phần này chứa một ứng dụng tạo chữ ký và do đó được gọi là thành phần dịch vụ ứ ng dụng tạo chữ ký (SCASC). Tuy nhiên, nó không chỉ là ứng đụng tạo chữ ký (SCA).

Các tài liệu tham khảo sau đây là cần thiết cho việc áp dụng tài liệu này.
[1] ETSI TS 119 101: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Yêu cầu chính sách và bảo mật cho các ứng dụng để tạo chữ ký và xác nhận chữ ký".
[2] ETSI TS 119 102-1 (V1.2.1): "Chữ ký điện tử và cơ sở hạ tầng (ESI); Thủ tục tạo và xác nhận chữ ký số AdES; Phần 1: Tạo và xác thực".
[3] ETSI EN 319 122-1: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số CAdES; Phần 1: Khối xây dựng và chữ ký cơ sở CAdES".
[4] ETSI EN 319 122-2: "Chữ ký điện tử và cơ sở hạ tầng (ESI); chữ ký số CAdES; Phần 2: Chữ ký CAdES mở rộng".
[5] ETSI EN 319 132-1: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số XAdES; Phần 1: Khối xây dựng và chữ ký cơ sở XAdES".
[6] ETSI EN 319 132-2: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số XAdES; Phần 2: Chữ ký XAdES mở rộng".
[7] ETSI EN 319 142-1: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số PAdES; Phần 1: Xây dựng chữ ký cơ sở khối và chữ ký PAdES".
[8] ETSI EN 319 142-2: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số PAdES; Phần 2: Hồ sơ chữ ký PAdES bổ sung".
[9] ETSI EN 319 401: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Yêu cầu chính sách chung đối với nhà cung cấp dịch vụ ủy thác".

- Chữ ký AdES (kỹ thuật số): chữ ký số là chữ ký CAdES hoặc chữ ký PAdES hoặc ch
ữ ký XAdES
- C**hữ ký số:** dữ liệu được thêm vào hoặc chuyển đổi mật mã của đơn vị dữ liệu cho phép người nhận đơn vị dữ liệu chứng minh nguồn và tính toàn vẹn của đơn vị dữ liệu và bảo vệ chống giả mạo, ví dụ: bởi người nhận
- G**iá trị chữ ký số:**kết quả của việc chuyển đổi mã hóa của một đơn vị dữ liệu cho phép người nhận của đơn vị dữ liệu để chứng minh nguồn gốc và tính toàn vẹn của các đơn vị dữ liệu và bảo vệ chống lại giả mạo ví dụ bởi người nhận
- T**hiết bị tạo chữ ký từ xa (remote signature creation device):** thiết bị tạo chữ ký sử dụng từ xa từ góc độ người ký và cung cấp điều khiển hoạt động ký kết nhân danh của ngư ời ký
- Ứ**ng dụng ký máy chủ (server signing application - SSA):**ứng dụng sử dụng thiết bị t ạo chữ ký từ xa để tạo giá trị chữ ký số thay mặt cho người ký
-**Thành phần dịch vụ ký ứng dụng máy chủ (server signing application service component-SSASC):** Thành phần dịch vụ TSP sử dụng ứng dụng ký máy chủ SSA
- N**hà cung cấp dịch vụ ứng dụng ký máy chủ (server signing application service provider - SSASP):** TSP vận hành một thành phần dịch vụ ứng dụng ký máy chủ
- Q**uy tắc áp dụng chữ ký:** bộ quy tắc, áp dụng cho một hoặc nhiều chữ ký số, xác định các yêu cầu
để xác định liệu chữ ký có phù hợp với một doanh nghiệp cụ thể hoặc mục đích pháp lý
- Ứ**ng dụng tạo chữ ký (signature creationg application-SCA):**ứng dụng trong hệ thố ng tạo chữ ký tạo chữ ký số AdES và dựa vào SCDev để tạo giá trị chữ ký số. SCDev có thể được quản lý bởi SSASC.
-**Thành phần dịch vụ ứng dụng tạo chữ ký (signature creation application service component-SCASC):** Thành phần dịch vụ TSP sử dụng ứng dụng tạo chữ ký
-**Nhà cung cấp dịch vụ ứng dụng tạo chữ ký (signature creation application service provider-SCASP):** TSP vận hành một thành phần dịch vụ ứng dụng tạo chữ ký
ràng buộc tạo chữ ký: tiêu chí được sử dụng khi tạo chữ ký số

"Đối với mục đích của tài liệu hiện tại, các chữ viết tắt được đưa ra trong ETSI TS 119 001 [i.2] và áp dụng như sau:
- CA: Cơ quan chứng nhận
- DTBS: Data To Be Signed - Dữ liệu sẽ được ký
- DTBSR: Data To Be Signed Representation - Đại diện của Dữ liệu được ký
- OID - Định danh đối tượng
- QES - Qualified Electronic Signature - Chữ ký điện tử đủ tiêu chuẩn hoặc con dấu điện tử đủ tiêu chuẩn
- SAD - Signature Activation Data - Dữ liệu kích hoạt chữ ký
- SCA - Signature Creation Application - Ứng dụng tạo chữ ký
- SCASC -SCASC Signature Creation Application Service Component - Thành phần dịch vụ ứng dụng tạo chữ ký
- SCASP -SCASP Signature Creation Application Service Provider - Nhà cung cấp dịch vụ ứng dụng tạo chữ ký
- SCDev -Signature Creation Device- Thiết bị tạo chữ ký
- SCS -Signature Creation Service- Dịch vụ tạo chữ ký
- SCSP -Signature Creation Service Provider- Nhà cung cấp dịch vụ tạo chữ ký
- SD -Signer's Document- Tài liệu của người ký
- SDO -Signed Data Object- Đối tượng dữ liệu đã ký
- SLA -Service-Level Agreement- Thỏa thuận cấp dịch vụ
- SSA -Server Signing Application- Ứng dụng ký máy chủ
- SSASC -Server Signing Application Service Component- Thành phần dịch vụ ứng dụng ký máy chủ
- SSASP -Server signing application service provider- Nhà cung cấp dịch vụ ứng dụng ký máy chủ
- TSA -Time-Stamping Authority- Cơ quan dấu thời gian
- URI -Uniform Resource Identifier- Mã định danh tài nguyên thống nhất

Các yếu tố của dịch vụ bao gồm:
• OVR: Yêu cầu chung (yêu cầu áp dụng đối với hơn 1 thành phần)
• ASI: Giao diện ký AdES

SCASP:
Các dịch vụ ủy thác có thể bao gồm nhưng không giới hạn ở việc cấp khóa công khai của chứng thư, cung cấp dịch vụ đăng ký, dịch vụ mốc thời gian, dịch vụ bảo trì giải hạn, dịch v ụ gửi điện tử và/hoặc dịch vụ xác thực chữ ký.
Các yêu cầu của chính sách này không có nghĩa là giới hạn bất kỳ việc tính phí cho dịch vụ của TSP.
Các yêu cầu được mô tả theo các mục tiêu bảo mật, kèm theo là các yêu cầu cụ thể của bi ện pháp quản lý để thỏa mãn các mục tiêu cần thiết.

Nhà cung cấp dịch vụ ứng dụng tạo chữ ký (SCASP) phát triển, triển khai, thi hành và cập nhật một tuyên bố thực hành SCASC là một tuyên bố thực hành dịch vụ ủy thác TSP, đượ c khởi tạo cho một thành phần dịch vụ ứng dụng tạo chữ ký.
Tuyên bố thực hành SCASC mô tả cách SCASP vận hành dịch vụ của mình và được sở h ữu bởi SCASP. Thực tiễn SCASC được điều chỉnh theo cơ cấu tổ chức, quy trình vận hành, cơ sở vật chất và môi trường điện toán của TSP. Người nhận tuyên bố thực hành có thể là kiểm toán viên, người đăng ký và các bên liên quan.

REQ-6.1-01: TSP sẽ chỉ định tập hợp các chính sách và thực tiễn phù hợp cho các dịch vụ ủy thác mà TSP đang cung cấp.
REQ-6.1-02: Tập hợp các chính sách và thực tiễn sẽ được phê duyệt bởi ban quản lý, đượ c công bố và truyền đạt tới nhân viên và các đối tác bên ngoài có liên quan.
REQ-6.1-03: TSP sẽ có một tuyên bố về các thông lệ và quy trình cho dịch vụ ủy thác đượ c cung cấp.

Chính sách SCASC mô tả những gì được cung cấp và có thể chứa thông tin đa dạng ngoài phạm vi của tài liệu hiện tại để chỉ ra khả năng áp dụng dịch vụ. Chính sách SCASC được xác định độc lập với các chi tiết cụ thể của môi trường hoạt động cụ thể của SSASP. Bên nhận chính sách dịch vụ có thể là kiểm toán viên, thuê bao và các bên liên quan.

Ngoài tuyên bố thực hành SCASC và khi được SCASP ban hành, chính sách SCASC, SCASP cũng ban hành các điều khoản và điều kiện, xem điều 6.2. Các điều khoản và điều kiện có thể bao gồm một loạt các điều khoản thương mại hoặc thuật ngữ kỹ thuật không nh ất thiết phải được truyền đạt tới khách hàng, v.v ... Các điều khoản và điều kiện dành riêng cho SCASP.
Người nhận các điều khoản và điều kiện có thể là người đăng ký và các bên liên quan.

- Chính sách tạo chữ ký là tập hợp các ràng buộc tạo chữ ký được SCA xử lý. Chính sách tạo chữ ký có thể được xác định bằng phương tiện của OID;
- Các quy tắc áp dụng chữ ký có thể được cấu trúc theo ETSI TS 119 172-1 [i.3] và có th ể bao gồm chính sách tạo chữ ký có các ràng buộc tạo chữ ký được SCA áp dụng, cũng như các tiêu chí khác thể hiện khả năng áp dụng của tạo chữ ký để nhu cầu kinh doanh nhất định.

Tuyên bố thực hành SCASC, chính sách tạo chữ ký và quy tắc áp dụng chữ ký là các loại tài liệu khác nhau; tuyên bố thực hành SCASC mô tả cách SCASP vận hành dịch vụ của mình, trong khi chính sách tạo chữ ký nêu rõ các ràng buộc được SCA xử lý khi tạo chữ ký.

Chủ sở hữu của tuyên bố thực hành SCASC là một SCASP, trong khi chủ sở hữu của các quy tắc áp dụng chữ ký thường là người ký.

- SCASC - thành phần dịch vụ TSP, hỗ trợ tạo chữ ký số AdES bằng nhận tài liệu hoặc giá trị băm của tài liệu cần ký và tùy chọn các tham số ký, thu thập tất cả thông tin cần thiết để tạo chữ ký, chuẩn bị đại diện của dữ liệu được ký (DTBSR) và gửi dữ liệu này đến SCDev.
- SCDev có thể ở trong môi trường người dùng hoặc được quản lý bởi một thành phần dịch vụ ứng dụng ký máy chủ từ xa (SSASC)
- SCDev xử lý xác thực và thỏa thuận ký với người dùng và trả về giá trị chữ ký số, mà không đi sâu vào chi tiết nếu điều này được thực hiện bởi chính SCDev hoặc thành phần qu ản lý SCDev . Việc ủy quyền sử dụng khóa ký trong SCDev có thể đi qua SCASC nhưng cũng có thể được thực hiện trực tiếp bằng cách liên lạc giữa người ký và SCDev. Giá trị ch ữ ký số được SCASC đưa vào chữ ký số.
- SCASC đại diện cho ứng dụng tạo chữ ký (SCA).

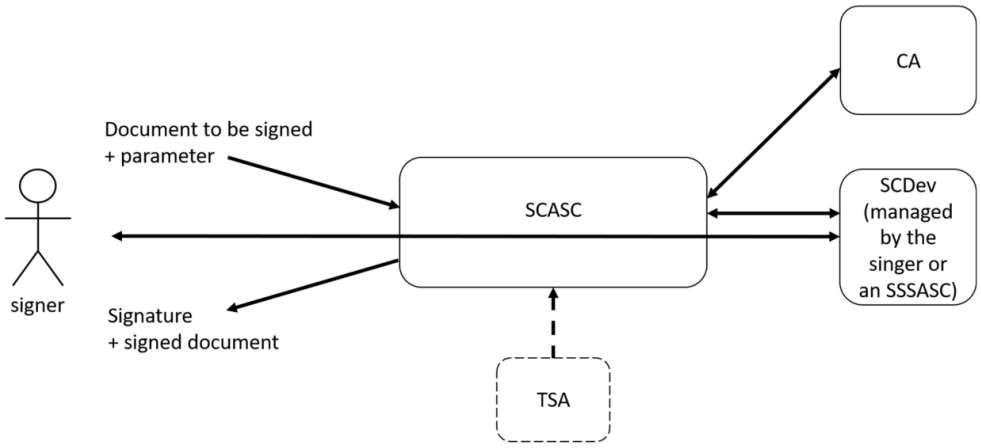


Figure 1: Relations of the TSP service component for AdES digital signature creation

REQ-5-01: TSP sẽ thực hiện đánh giá rủi ro để xác định, phân tính và đánh giá rủi ro của dị ch vụ ủy thác có tính đến các vấn đề kinh doanh và kỹ thuật.
REQ-5-02: TSP sẽ 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 sẽ đảm bảo mức độ bảo mật sẽ tương xứng với mức độ rủi ro.
REQ-5-03: TSP sẽ xác định các yêu cầu bảo mật và quy trình vận hành cần thiết để thực hi ện các biện pháp xử lý rủi ro đã chọn, như đã được ghi trong chính sách bảo mật thông tin và tuyên bố thông lệ của dịch vụ ủy thác (xem điều 6).
REQ-5-04: Quá trình đánh giá rủi ro sẽ được xem xét và sửa đổi thường xuyên.
REQ-5-05: Quản lý của TSP sẽ phê duyệt đánh giá rủi ro và chấp nhận rủi ro tồn đọng đã được xác nhận.

REQ-6.1-01: TSP sẽ chỉ định tập hợp các chính sách và thực tiễn phù hợp cho các dịch vụ ủy thác mà TSP đang cung cấp.
REQ-6.1-02: Tập hợp các chính sách và thực tiễn sẽ được phê duyệt bởi ban quản lý, đượ c công bố và truyền đạt tới nhân viên và các đối tác bên ngoài có liên quan.
REQ-6.1-03: TSP sẽ có một tuyên bố về các thông lệ và quy trình cho dịch vụ ủy thác đượ c cung cấp.
LƯU Ý: Tài liệu này không đưa ra yêu cầu về cấu trúc của tuyên bố dịch vụ ủy thác.
Đặc biệt là:
• REQ-6.1-04: TSP sẽ có một tuyên bố về các thông lệ và quy trình được sử dụng để giải quyết các yêu cầu được xác định cho chính sách hiện hành của TSP.
• REQ-6.1-05: Tuyên bố dịch vụ ủy thác của TSP sẽ xác định nghĩa vụ của tất cả các tổ ch ức bên ngoài có hỗ trợ dịch vụ của TSP bao gồm các chính sách và thực tiễn áp dụng.
• REQ-6.1-06: TSP sẽ được cung cấp cho các thuê bao và tuyên bố thực thi của relying party và các tài liệu liên quan khác khi cần thiết để đánh giá sự phù hợp với chính sách dịch vụ.
• REQ-6.1-07: TSP sẽ có một bộ phận quản lý chịu trách nhiệm chung về TSP với thẩm quyền cuối cùng để phê duyệt tuyên bố của TSP.
• REQ-6.1-08: Quản lý của TSP sẽ triển khai các thông lệ.
• REQ-6.1-09: TSP sẽ xác định một quy trình xem xác các thông lệ bao gồm trách nhiệm duy trì tuyên bố thông lệ của TSP.
• REQ-6.1-10: TSP sẽ thông báo về các thay đổi mà TSP dự định sẽ thay đổi trong tuyên bố thông lệ.
• REQ-6.1-11: Theo phê duyệt như trong điều khoản REQ-6.1-07 ở trên, TSP sẽ sửa đổi tuyên bố thông lệ của TSP ngay lập tức theo yêu cầu của điều khoản REQ-6.1-06.
• REQ-6.1-12: TSP sẽ đề cập trong thông lệ của TSP các quy định được đưa ra để chấm dứt dịch vụ (xem điều 7.12).

REQ-6.1-01: TSP sẽ chỉ định tập hợp các chính sách và thực tiễn phù hợp cho các dịch vụ ủy thác mà TSP đang cung cấp.
REQ-6.1-02: Tập hợp các chính sách và thực tiễn sẽ được phê duyệt bởi ban quản lý, đượ c công bố và truyền đạt tới nhân viên và các đối tác bên ngoài có liên quan.
REQ-6.1-03: TSP sẽ có một tuyên bố về các thông lệ và quy trình cho dịch vụ ủy thác đượ c cung cấp.
LƯU Ý: Tài liệu này không đưa ra yêu cầu về cấu trúc của tuyên bố dịch vụ ủy thác.
Đặc biệt là:
• REQ-6.1-04: TSP sẽ có một tuyên bố về các thông lệ và quy trình được sử dụng để giải quyết các yêu cầu được xác định cho chính sách hiện hành của TSP.
• REQ-6.1-05: Tuyên bố dịch vụ ủy thác của TSP sẽ xác định nghĩa vụ của tất cả các tổ ch ức bên ngoài có hỗ trợ dịch vụ của TSP bao gồm các chính sách và thực tiễn áp dụng.
• REQ-6.1-06: TSP sẽ được cung cấp cho các thuê bao và tuyên bố thực thi của relying party và các tài liệu liên quan khác khi cần thiết để đánh giá sự phù hợp với chính sách dịch vụ.
• REQ-6.1-07: TSP sẽ có một bộ phận quản lý chịu trách nhiệm chung về TSP với thẩm quyền cuối cùng để phê duyệt tuyên bố của TSP.
• REQ-6.1-08: Quản lý của TSP sẽ triển khai các thông lệ.
• REQ-6.1-09: TSP sẽ xác định một quy trình xem xác các thông lệ bao gồm trách nhiệm duy trì tuyên bố thông lệ của TSP.
• REQ-6.1-10: TSP sẽ thông báo về các thay đổi mà TSP dự định sẽ thay đổi trong tuyên bố thông lệ.
• REQ-6.1-11: Theo phê duyệt như trong điều khoản REQ-6.1-07 ở trên, TSP sẽ sửa đổi tuyên bố thông lệ của TSP ngay lập tức theo yêu cầu của điều khoản REQ-6.1-06.
• REQ-6.1-12: TSP sẽ đề cập trong thông lệ của TSP các quy định được đưa ra để chấm dứt dịch vụ (xem điều 7.12).

Công bố các chích sách tạo chữ ký số được hỗ trợ.

Công bố các định dạng chữ ký được hỗ trợ.

Công bố các lớp chữ ký được hỗ trợ.

SCASP cần xác định trong tuyên bố thực hành SCASC: nghĩa vụ của tất cả các tổ chức bên ngoài hỗ trợ các dịch vụ của mình bao gồm các chính sách và thực tiễn áp dụng

REQ-6.2-01: TSP sẽ cung cấp các điều khoản và điều kiện liên quan đến các dịch vụ của TSP cho tất cả thuê bao và relying party. REQ-6.2-02: Các điều khoản và điều kiện ít nhất phải chỉ định cho từng chính sách dịch vụ ủy thác được TSP hỗ trợ như sau: a) Chính sách dịch vụ ủy thác được áp dụng; b) Bất kỳ hạn chế của việc sử dụng dịch vụ; c) Nghĩa vụ của thuê báo (nếu có); d) Thông tin cho các đối tác phụ thuộc vào dịch vụ ủy thác; e) Khoảng thời gian mà nhật ký sự kiện của TSP sẽ được giữ lại; f) Hạn chế trách nhiệm pháp lý; g) Những 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 các dịch vụ vượt qua giới hạn đó; h) Hệ thống pháp luật được áp dụng; i) Thủ tục khiếu nại và giải quyết tranh chấp; j) Dịch vụ ủy thác của TSP đã được đánh giá phù hợp với chính sách dịch vụ ủy thác hay không. Nếu có thì đã được đánh giá qua kế hoạch đánh giá nào. k) Thông tin liên hệ TSP; l) Bất kỳ cam kết liên quan tới tính sẵn sàng sử dụng; REQ-6.2-03: thuê bao và các đối tác phụ thuộc vào dịch vụ ủy quyền sẽ được thông báo chính xác các điều khoản và điều kiện, bao gồm các mục được liệt kê ở trên, trước khi bướ c vào mối quan hệ hợp tác. REQ-6.2-04: Điều khoản và điều kiện sẽ được cung cấp thông qua các phương thức liên lạ c lâu bền. REQ-6.2-05: Điều khoản và điều kiện sẽ được viết bằng một ngôn ngữ dễ hiểu. REQ-6.2-06: Điều khoản và điều kiển có thể được gửi qua đường điện tử.
Để chỉ định chính sách dịch vụ ủy thác đang được áp dụng, các điều khoản và điều kiện của SCASC sẽ liệt kê hoặc tham chiếu đến (ví dụ: thông qua OID) và mô tả ngắn gọn, các chính sách SCASC được hỗ trợ mà nó tuân thủ
Để chỉ định chính sách dịch vụ ủy thác đang được áp dụng, các điều khoản và điều kiện của SCASC có thể sử dụng các OID
Các điều khoản và điều kiện sẽ chỉ ra các quyền và nghĩa vụ của SCASP và người ký

Các điều khoản và điều kiện sẽ mô tả các tùy chọn được dịch vụ hỗ trợ. Ít nhất:
a) Các định dạng chữ ký được hỗ trợ
b) Các tham số chữ ký được hỗ trợ,
c) Nếu tài liệu được ký chỉ có thể được cung cấp dưới dạng băm và
d) Các thiết bị tạo chữ ký được hỗ trợ (SCDev) cho người ký.

Các điều khoản và điều kiện sẽ giải thích cách xử lý dữ liệu cá nhân

REQ-6.3-01: TSP sẽ xác định một chính sách bảo mật thông tin được bộ phận quản lý phê duyệt và đưa ra cách tiếp cận quản lý bảo mật thông tin của tổ chức.
REQ-6.3-02: Các thay đổi trong chính sách bảo mật thông tin sẽ được thông báo cho bên thứ ba, nếu có. Bao gồm các thuê bao, relying party, cơ quan đánh giá, giám sát hoặc các c ơ quan pháp lý khác.
Đặc biệt là:
• REQ-6.3-03: Chính sách bảo mật thông tin của TSP sẽ được ghi lại, triển khai và duy trì bao gồm các biện pháp kiểm soát bảo mật và quy trình vận hành cho các cơ sở, hệ thống và tài sản thông tin cung cấp dịch vụ của TSP.
• REQ-6.3-04: TSP sẽ xuất bản và truyền đạt chính sách bảo mật thông tin tới các nhân viên bị ảnh hưởng.
• REQ-6.3-05: TSP sẽ chịu trách nhiệm vệ việc tuân thủ các quy trình được quy định trong chính sách bảo mật thông tin, ngay cả khi chức năng của TSP được thuê ngoài để thực hiệ n.
• REQ-6.3-06: TSP sẽ xác định trách nhiệm pháp lý của công ty được thuê ngoài và đảm b ảo rằng công ty được thuê ngoài bị ràng buộc phải thực hiện bất kỳ biện pháp kiểm soát nào theo yêu cầu của TSP.
• REQ-6.3-07: Chính sách bảo mật thông tin của TSP và kiểm kê tài sản để bảo mật thông tin (xem điều 7.3) sẽ được xem xét theo các khoảng thời gian theo kế hoạch hoặc nếu có những thay đổi đáng kể xảy ra để đảm bảo tính phù hợp, thỏa đáng và hiệu quả liên tục.
• REQ-6.3-08: Mọi thay đổi có ảnh hưởng tới mức độ bảo mật được cung cấp sẽ phê duy ệt bởi bộ phận quản lý như đã đề cập ợ REQ-6.1-07.
• REQ-6.3-09: Cấu hình của hệ thống TSP sẽ được kiểm tra thường xuyên để phát hiện các thay đổi vi phạm chính sách bảo mật của TSP.

Chính sách bảo mật phải ghi lại các kiểm soát bảo mật và quyền riêng tư được triển khai để bảo vệ dữ liệu cá nhân.

Độ tin cậy của tổ chức

REQ-7.1.1-01: Tổ chức TSP nên đáng tin cậy.

• REQ-7.1.1-02: Dịch vụ ủy thác được thực thi theo cách TSP vận hành không phân biệt.

• REQ-7.1.1-03: TSP nên cho các dịch vụ của họ có thể được truy cập bởi người sử dụng có phạm vi hoạt động nằm trong lĩnh vực hoạt động đã được khai báo và đồng ý tuân thủ các nghĩa vụ của họ như đã quy định trong điều khoản và điều kiện của TSP.

• REQ-7.1.1-04: TSP sẽ duy trì đầy đủ nguồn tài chính và/hoặc có được bảo hiểm trách nhiệm phù hợp, theo luật pháp hiện hành, để chi trả các khoản nợ phát sinh từ các hoạt độ ng của TSP.

• REQ-7.1.1-05: TSP sẽ có ổn định tài chính và nguồn lực cần thiết để vần hành phù hợp v ới chính sách này.

• REQ-7.1.1-06: TSP sẽ có chính sách và thủ tục để giải quyết các khiếu nại và tranh chấp nhận từ phía khách hàng hoặc relying party về việc cung cấp dịch vụ hoặc các vấn đề liên quan khác.

• REQ-7.1.1-07: TSP sẽ có một văn bản thỏa thuận và mối quan hệ hợp đồng tại nơi cung cấp dịch vụ liên quan tới hợp đồng thầu phụ, thuê ngoài hoặc các thỏa thuận bên thứ ba khác.

Phân chia nhiệm vụ:

REQ-7.1.2-01: Các nhiệm vụ và lĩnh vực trách nhiệm xung đột sẽ được tách biệt để giảm c ơ hội sửa đổi trái phép hoặc vô ý hoặc lạm dụng tài sải của TSP.

Nguồn nhân lực
REQ-7.2-01: TSP sẽ đảm bảo rằng nhân viên và nhà thầu hỗ trợ sự tin cậy của các hoạt đ ộng của TSP.
• REQ-7.2-02: TSP sẽ thuê nhân viên và, nếu có thể, các nhà thầu phụ có chuyên môn cần thiết, độ tin cậy, kinh nghiệm, trình độ chuyên môn và cá nhân đã được đào tạo về các quy tắc bảo vệ dữ liệu cá nhân và bảo mật phù hợp với các dịch vụ được cung cấp và chức nă ng công việc.
• REQ-7.2-03: Nhân viêc của TSP phải đáp ứng được yêu cầu "kiến thức, kinh nghiệm và trình độ chuyên môn" thông qua đào tạo và chứng chỉ chính thức hoặc kinh nghiệm thực tế hoặc kết hợp cả hai.
• REQ-7.2-04: Điều này nên bao gồm cập nhật thường xuyên (ít nhất 12 tháng một lần) về các mối đe dọa và thực tiễn bảo mật hiện tại.
LƯU Ý 2: Nhân sự được TSP sử dụng bao gồm các cá nhân tham gia trong việc thực hiện hiện chức năng hỗ trợ của các dịch vụ của TSP. Các cá nhân tham gia giám sát các dịch vụ của TSP không cần phải là nhân viên của TSP.
• REQ-7.2-05: Các biện pháp kỷ luật phù hợp sẽ được áp dụng đối với các nhân viên vi ph ạm các chính sách hoặc thủ tục của TSP.
LƯU Ý 3: Tham khảo điều 7.2.3 của ISO/IEC 27002:2013 [i.3] để biết thêm thông tin.
• REQ-7.2-06: Vai trò và trách nhiệm bảo mật, như đã quy định trong chính sách bảo mật thông tin của TSP, sẽ được lưu lại trong các mô tả công việc hoặc trong các tài liệu có sẵn cliên qua tới các nhân viên lên quan.
• REQ-7.2-07: Các vai trò đáng tin cậy, trong đó tính bảo mật của hoạt động của TSP phụ thuộc, sẽ được xác định rõ ràng sau.
• REQ-7.2-08: Các vai trò đáng tin cậy sẽ được đặt tên bởi bộ phận quản lý.
• REQ-7.2-09: Vai trò đáng tin cậy sẽ được chấp nhận bởi bộ phần quản lý và cá nhân để hoàn thành vai trò.
• REQ-7.2-10: Nhân viên của TSP (tạm thời và chính thức) sẽ có mô tả công việc được xác định theo quan điểm của vai trò được thực hiện với sự phân biệt nhiệm vụ và quyền tối

Yêu cầu chung:
REQ-7.3.1-01: TSP sẽ đảm bảo múc độ bảo vệ thích hợp đối với tài sản của TSP, bao gồ m cả tài sản thông tin.
Đặc biệt là:
• REQ-7.3.1-02: TSP sẽ duy trì danh sách tất cả các tài sản thông tin và phân loại phù hợp với đánh giá rủi ro.
Xử lý phương tiện truyền thông:
REQ-7.3.2-01: Tất cả truyền thông sẽ được xử lý an toàn theo yêu cầu của sơ đồ phân loại thông tin. Truyền thông chứa dữ liệu nhạy cảm sẽ được loại bỏ một cách an toàn khi không còn cần thiết nữa.

REQ-7.4-01: quyền truy cập vào hệ thống của TSP sẽ được giới hạn cho các cá nhân đượ c ủy quyền. • REQ-7.4-02: Các biện pháp kiểm soát (ví dụ: tường lửa) sẽ bảo vệ các miền mạng nội b ộ của TSP khởi sự truy cập trái phép bao gồm cả truy cập của thuê bao và bên thứ ba. • REQ-7.4-03: Tường lửa nên được cấu hình để ngăn chặn tất cả các giao thức và truy cập không cần thiếtcho hoạt động của TSP. • REQ-7.4-04: TSP sẽ quản trị quyền truy cập người dùng của các nhân viên vận hành, quả n trị viên, kiểm toán viên hệ thống. • REQ-7.4-05: Việc quản trị sẽ bao gồm việc quản lý tài khoản người dùng và sửa đổi hoặ c xóa quyền truy cập kịp thời. • REQ-7.4-06: Quyền truy cập vào thông tin và chức năng hệ thống ứng dụng sẽ bị hạn ch ế theo chính sách kiểm soát truy cập. • REQ-7.4-07: Hệ thống của TSP sẽ cung cấp đầy đủ các phương thức kiểm soát bảo mật máy tính để phân biệt các vai trò đáng tin cậy đã được xác định trong thực tiễn của TSP, bao gồm tách chức năng quản trị an ninh và hoạt động hệ thống. Đặc biệt là việc sử dụng các chương trình tiện ích hệ thống sẽ bị hạn chế và kiểm soát. • REQ-7.4-08: Nhân viên của TSP sẽ được xác xác định và xác thức trước khi sử dụng các ứng dụng quan trọng liên quan tới dịch vụ. • REQ-7.4-09: Nhân viên của TSP sẽ phải chịu trách nhiệm cho các hành động của họ. Ví dụ: Bằng cách lưu trữ lịch sử sự kiện. • REQ-7.4-10: Dữ liệu nhạy cảm sẽ được bảo về khỏi bị tiết lộ thông qua các đối tượng lư u trữ được sử dụng lại (ví dụ: các file đã bị xóa) có thể truy cập được bởi người dùng không được ủy quyền.
REQ-7/5-01: Các biện pháp kiểm soát bảo mật phù hợp sẽ được áp dụng để quản lý mọi khóa mã hóa và mọi thiết bị mã hóa trong suốt vòng đời của chúng.
REQ-7.6-01: TSP sẽ kiểm soát quyền truy cập vật lý vào các thành phần của hệ thống TSP có tính bảo mật rất quan trọng trong việc cung cấp các dịch vụ ủy thác và giảm thiểu rủ i ro liên quan tới bảo mật vật lý. Đặc biệt là: • REQ-7.6-02: Quyền truy cập vật lý tới các thành phần của hệ thống TSP sẽ được giới hạ n cho các cá nhân được ủy quyền. • REQ-7.6-03: Các biện pháp kiểm soát sẽ được áp dụng để tránh mất mát, thiệt hại hoặc l ộ các tài nguyên và làm gián đoạn các hoạt động kinh doanh. • REQ-7.6-04: Các biện pháp kiểm soát sẽ được áp dụng để giảm lộ hoặc mất cắp thông tin và chức năng xử lý thông tin. • REQ-7.6-05: Các thành phần quan trọng cho hoạt động bảo mật của dịch vụ ủy thác phải được đặt trong vùng bảo mật được bảo vệ bằng bảo vệ vật lý chống xâm nhập, kiểm soát truy cập thông tin thông qua vùng bảo mật và báo động khi phát hiện sự xâm nhập.
GSM 1.4: các thư viện mã hóa được kiểm tra theo các tiêu chuẩn tương ứng sẽ được sử d ụng. Nên sử dụng các thư viện đã biết đến nhiều.

Bảo mật kỹ thuật và độ tin cậy của các quy trình được hỗ trợ.
• REQ-7.7-02: Việc phân tích các yêu cầu bảo mật sẽ được thực hiện tại bước thiết kế và đặc tả yêu cầu của bất kỳ dự án phát triển hệ thống nào được thực hiện bởi TSP hoặc đại diện của TSP để đảm bảo rằng bảo mật được tích hợp vào hệ thống.
• REQ-7.7-03: Việc thay đổi các quy trình kiểm soát sẽ được áp dụng chó các bản phát hành, sửa đổi, bản sửa chữa phần mềm gấp và các thay đổi cấu hình áp dụng cho chính sách bảo mật của TSP.
• REQ-7.7-04: Các thủ tục sẽ bao gồm các tài liệu liên quan tới thay đổi.
• REQ-7.7-05: Tính toàn vẹn của hệ thống và thông tin của TSP sẽ được bảo vệ khỏi virus, phần mềm độc hại.
• REQ-7.7-06: Truyền thông được dùng trong hệ thống của TSP sẽ được xử lý an toàn để bảo vệ truyền thông không bị thiệt hại, mất cắp, truy cập trái phép.
• REQ-7.7-07: Quy trình quản lý truyền thông sẽ được bảo vệ chống lại sự lỗi thời và suy giảm của truyền thông trong một khoảng thời gian yêu cầu lưu trữ dữ liệu.
• REQ-7.7-08: Các thủ tục sẽ được thiết lập và triển khai cho các chức vụ tin tưởng và quản trị có ảnh hưởng tới việc cung cấp các dịch vụ.
• REQ-7.7-09: TSP sẽ chỉ định và áp dụng các quy trình để đảm bảo rằng:
a) Các bản vá bảo mật sẽ được ập nhật lên hệ thống trong khoảng thời gian hợp lý sau khi có bản vá.
b) Các bản vá bảo mật sẽ không được cập nhật lên hệ thống nếu như các bản vá đó có thêm các lỗ hổng hoặc tính không ổn định lớn.
c) Lý do không cập nhật bất kỳ bản vá bảo mật sẽ được lưu lại.

GSM 1.2: môi trường ứng dụng mới nhất (quản lý môi trường phần mềm) nên được dùng có bao gồm các sửa lỗi bảo mật mới nhất.
GSM 1.3: Sử dụng các giao thức chuẩn hóa và thư viện đã được kiểm tra và xem xét kỹ lưỡng.

GSM 2.4: SCA/SVA/SAA sẽ duy trì tính toàn vẹn và bảo mật của tất cả thông tin được cung cấp bởi người dùng và bất kỳ luồng dữ liệu giữa ứng dụng và người dùng, ngay cả trong trường hợp môi trường ứng dụng công cộng.

REQ-7.8-01: TSP sẽ bảo vệ mạng lưới và hệ thống khỏi các cuộc tấn công.
• REQ-7.8-02: TSP sẽ phân chia các hệ thống của họ ra thành các mạng lưới hoặc vùng d ựa trên đánh giá rủi ro xem xét mối quan hệ chức năng, logic và vật lý (bao gồm vị trí) giữa các hệ thống và dịch vụ đáng tin cậy.
• REQ-7.8-03: TSP sẽ áp dụng các phương pháp kiểm soát bảo mật giống nhau cho tất cả hệ thống đang ở trong cùng một vùng.
• REQ-7.8-04: TSP sẽ hạn chế quyền truy cập và liên lạc giữa các vùng đến các vùng cần thiết cho hoạt động của TSP.
• REQ-7.8-04: TSP sẽ cấm và tắt các kết nối và dịch vụ không cần thiết.
• REQ-7.8-05: TSP sẽ thường xuyên xem xét các quy luật đã được thiết lập.
• REQ-7.8-06: TSP sẽ giữ tất cả hệ thống quan trọng đối với hoạt động của TSP trong một hoặc nhiều vùng bảo mật (ví dụ: Các hệ thống Root CA. Tham khảo ETSI EN 319 411-1 [i.9]).
• REQ-7.8-07: TSP sẽ tách mạng chuyên dụng để quản trị hệ thống công nghệ thông tin và mạng hoạt động của TSP.
• REQ-7.8-08: TSP sẽ không sử dụng hệ thống dùng cho việc quản trị thực thi chính sách bảo mật để sử dụng cho các mục đính khác.
• REQ-7.8-09: TSP sẽ tách các hệ thống đang hoạt động cho các dịch vụ của TSP ra khỏi các hệ thống được dùng để phát triển và thử nghiệm (ví dụ: hệ thống phát triển, thử nghiệm và dàn dựng)
• REQ-7.8-10: TSP sẽ thiết lập liên lạc giữa các hệ thống đáng tin cậy khác nhau thông qua các kênh đáng tin cậy khác biệt về mặt logic với các kênh liên lạc khác và đảm bảo nhận dạ ng chính xác điểm cuối và bảo vệ dữ liệu của kênh không bị chỉnh sửa hoặc bị tiết lộ.
• REQ-7.8-11: Nếu cần có mức độ sẵn sàng cao của quyền truy cập bên ngoài vào dịch v ụ ủy thác, kết nối mạng bên ngoài sẽ được dự phòng để đảm bảo các dịch vụ luôn sẵn sàng trong trường hợp có lỗi xảy ra.
• REQ-7.8-12: TSP sẽ thực hiên quét lỗ hổng thường xuyên trên các địa chỉ IP public và private được xác định bởi TSP và lưu lại bằng chứng rằng mỗi lần quét lỗ hổng là được thự

REQ-7.9-01: Các hoạt động trên hệ thống liên quan tới truy cập hệ thống IT, sử dụng hệ th ống IT và yêu cầu dịch vụ sẽ được giám sát.
• REQ-7.9-02: Các hoạt động giám sát cần tính đến độ nhạy cảm của bất kỳ thông tin đượ c thu thập hoặc phân tích.
• REQ-7.9-03: Các hoạt động bát thường trên hệ thống cho thấy vi phạm bảo mật tiềm ẩn, bao gồm xâm nhập mạng của TSP sẽ được phát hiện và báo động vi phạm đó.
• REQ-7.9-04: TSP sẽ theo dõi các sự kiên sau:
a) Bật và tắt của chức năng lưu lịch sử sự kiện;
b) Tính sẵn sàng và sử dụng các dịch vụ cần thiết với mạng của TSP.
• REQ-7.9-05: TSP sẽ hành động kịp thời và phối hợp để nhanh chóng ứng phó các sự cố và hạn chế tác động của các vi phạm an ninh.
• REQ-7.9-06: TSP sẽ chỉ định nhân viên có vai trò đáng tin cậy để theo dõi các cảnh báo sự kiện bảo mật quan trọng tiềm ẩn và đảm bảo các sự cố liên quan sẽ được báo cáo theo quy trình của TSP.
• REQ-7.9-07: TSP sẽ thiết lập các thủ tục để thông báo cho các bên phù hợp theo các quy tắc pháp lý hiện hành về bất kỳ vi phạm an ninh hoặc mất tính toàn vẹn nào có ảnh hưở ng đáng kể đến dịch vụ ủy thác được cung cấp và trên dữ liệu cá nhân được duy trì trong 24 giờ kể từ khi vi phạm được xác định.
• REQ-7.9-08: Trường hợp vi phạm bảo mật hoặc mất tính toàn vẹn có thể ảnh hưởng xấu đến một thể nhân hoặc pháp nhân mà dịch vụ ủy thác đã được cung cấp, TSP cũng sẽ thông báo cho pháp nhân hoặc thể nhân về vi phạm an ninh hoặc mất tính toàn vẹn mà không có sự chậm trễ quá đáng.
• REQ-7.9-09: Các hệ thống của TSP sẽ được giám sát bao gồm giám sát hoặc thường xuyên xem xét nhật ký kiểm toán để xác định bằng chứng các hoạt động độc hại thực hiện các cơ chế tự động để xử lý nhật ký kiểm toán và cảnh báo nhân sự biết đến sự kiện bảo m ật quan trọng tiềm ẩn.
• REQ-7.9-10: TSP sẽ giải quyết mọi lỗ hổng nghiêm trọng chưa được xử lý trước đó trong vòng 48 giờ sau khi phát hiện.

REQ-7.10-01: TSP sẽ ghi lại và lưu trữ bằng chứng trong một khoảng thời gian phù hợp, k ể cả sau khi các hoạt động của TSP chấm dứt, tất cả các thông tin liên quan đến dữ liệu do TSP ban hành và nhận được, đặc biệt là cho mục đích cung cấp bằng chứng trong việc tố t ụng pháp lý và mục đích đảm bảo tính liên tục của dịch vụ. Đặc biệt là: • REQ-7.10-02: Duy trì tính bảo mật và tính toàn vẹn của dữ liệu hiện tại và dữ liệu được l ưu trữ liên quan đến hoạt động của các dịch vụ. • REQ-7.10-03: Dữ liệu liên quan đến hoạt động của dịch vụ sẽ được lưu trữ hoàn toàn và bảo mật theo thông lệ kinh doanh được tiết lộ. • REQ-7.10-04: Các hồ sơ liên quan đến hoạt động của các dịch vụ sẽ được cung cấp khi được yêu cầu cho mục đích cung cấp bằng chứng chính xác về hoạt động của dịch vụ cho mục đích tố tụng. • REQ-7.10-05: thời gian chính xác của các sự kiện trong môi trường hoạt động, quản lý khóa và đồng bộ hóa quan trọng của TSP sẽ được ghi lại. • REQ-7.10-06: Thời gian được sử dụng để ghi lại các sự kiện theo yêu cầu nhật ký kiểm toán sẽ được đồng bộ hóa với múi giờ UTC ít nhất một lần một ngày. • REQ-7.10-07: Hồ sơ liên quan tới các dịch vụ sẽ được lưu trữ trong một khoảng thời gian phù hợp để cung cấp bằng chứng pháp lý cần thiết và như đã được đề cập tới trong đi ều khoản và điều kiện của TSP (xem điều 6.3). • REQ-7.10-08: Các sự kiện sẽ được lưu lại theo cách mà các dữ liệu được lưu không thể dễ dàng bị xóa hoặc bị phá hủy (trừ khi được chuyển sang thiết bị lưu trữ lâu dài) trong một khoảng thời gian lưu trữ được yêu cầu.
Bất kỳ hoạt động tạo chữ ký số AdES nào cũng phải được ghi lại, cùng với nhận dạng của người đăng ký khi biết thông tin này
Nhật ký sự kiện sẽ được đánh dấu theo thời gian của sự kiện
Tần suất xử lý, thời gian lưu giữ, bảo vệ, quy trình sao lưu của hệ thống thu thập, quy trình l ưu trữ và đánh giá lỗ hổng của nhật ký sự kiện
Nhật ký sự kiện phải bao gồm loại sự kiện, thành công hay thất bại của sự kiện và số nhận dạng của người và / hoặc thành phần tại nguồn gốc của sự kiện đó
REQ-7.11-01: TSP sẽ xác định và duy trì một kế hoạch liên tục để thực hiện trong trường hợp có thảm họa xảy ra. REQ-7.11-02: Trong trường hợp có thảm họa xảy ra, bao gồm lộ khóa ký bí mật hoặc lộ thông tin của TSP, hoạt động của các dịch vụ sẽ được phục hồi trong khoảng thời gian đã đ ược đề ra trong kế hoạch liên tục, giải quyết mọi nguyên nhân gây ra thảm họa để tránh tái diễn (ví dụ: lỗ hổng bảo mật) bằng các biện pháp khác phục thích hợp.

REQ-7.12-01: Giảm thiểu sự gián đoạn tiềm ẩn cho các thuê bao và relying party. Gián đo ạn tiềm ẩn này xảy ra do việc dừng hoạt động các dịch vụ của TSP. Đặc biệt là tiếp tục duy trì thông tin cần thiết để xác thực tính chính xác của các dịch vụ được cung cấp.
• REQ-7.12-02: TSP sẽ có kế hoạch chấm dứt dịch vụ mới nhất.
Trước khi TSP chấm dứt hoạt động các dịch vụ của TSP, ít nhất phải áp dụng các thủ tục sau:
- REQ-7.12-03: Trước khi TSP chấm dứt cung cấp dịch vụ, TSP sẽ gửi thông báo tới tất c ả các thuê bao và các thực thể khác mà TSP có thỏa thuận hoặc các hình thức quan hệ khác, có bao gồm các relying party, TSP và các cơ quan có thẩm quyền như cơ quan giám sát.
- REQ-7.12-04: Trước khi TSP chấm dứt các dịch vụ của họ, TSP sẽ gửi thông tin chấm d ứt cung cấp dịch vụ tới cho các relying party.
- REQ-7.12-05: Trước khi TSP chấm dứt các dịch vụ của họ, TSP sẽ chấm dứt các quyền cho phép đại diện TSP của các nhà thầu phụ để thực hiện bất kỳ chức năng nào liên quan t ới quy trình cấp token dịch vụ ủy thác.
- REQ-7.12-06: Trước khi TSP chấm dứt các dịch vụ của họ, TSP sẽ chuyển giao nghĩa v ụ duy trì tất cả thông tin cần thiết để cung cấp bằng chứng hoạt động của TSP trong một khoảng thời gian phù hợp cho một bên đáng tin cậy. Trừ khi có thể chứng minh rằng TSP không có các thông tin đó.
- REQ-7.12-07: Trước khi TSP chấm dứt các dịch vụ của họ, các khóa bí mật của TSP bao gồm các bản sao lưu sẽ bị hủy hoặc rút khỏi sử dụng theo cách các khóa bí mật không thể lấy được.
- REQ-7.12-08: Trước khi TSP chấm dứt các dịch vụ của họ, TSP nên thu xếp để chuyển việc cung cấp dịch vụ ủy thác cho các khách hạng hiện tác sang một TSP khác.
• REQ-7.12-09: TSP sẽ sắp xếp để trang trải chi phí đáp ứng các yêu cầu tối thiểu trong tr ường hợp TSP bị phá sản hoặc vì lý do khác mà không tự trang trải chi phí trong giới hạn c ủa luật áp dụng cho trường hợp phá sản.
• REQ-7.12-10: TSP sẽ đề cập các quy định đưa ra để chấm dứt cung cấp dịch vụ. Bao g

Áp dụng REQ-7.13-01: TSP sẽ đảm bảo rằng các hoạt động của họ hợp pháp và đáng tin cậy: Đặc biệt là: • REQ-7.13-02: TSP sẽ cung cấp bằng chứng về cách đáp ứng các yêu cầu pháp lý hiện hành. • REQ-7.13-03: Các dịch vụ ủy thác được cung cấp và các sản phẩm người dùng cuối được dùng trong việc cung cấp các dịch vụ đó sẽ cho phép những người khuyết tật truy cập nếu khả thi. • REQ-7.13-04: Áp dụng các tiêu chuẩn về khả năng tiếp cận như là ETSI EN 301 549 [i.10] • REQ-7.13-05: Các biện pháp kỹ thuật và tổ chức phù hợp sẽ được thực hiện đối với việc xử lý dữ liêu cá nhân bất hợp pháp và vô tính mất mát hoặc phá ủy dữ liệu cá nhân. LƯU Ý: Các TSP hoạt động ở Châu Âu phải đảm bảo các dữ liệu cá nhân được xử lý theo chỉ thị 95/46/EC [i.1] tới ngày 25 tháng 5 năm 2018 và theo quy định (EU) 2016/679 [i.12] đã bãi bỏ chỉ định trước từ ngày 25 tháng 5 năm 2018. Về mặt này, xác thực cho một dịch vụ trực tuyến liên quan đến việc chỉ xử lý các dữ liêu xác thực đầy đủ, phù hợp và không quá mức để cấp quyền quyền truy cập dịch vụ trực tuyến.
Khi dữ liệu cá nhân được xử lý bởi bên thứ ba, nếu cần theo luật, một thỏa thuận phù hợp sẽ được thực hiện với bộ xử lý dữ liệu cá nhân của bên thứ ba để đảm bảo rằng họ tuân thủ các yêu cầu pháp lý, bao gồm cả việc thực hiện kỹ thuật, tổ chức và các biện pháp pháp lý để bảo vệ dữ liệu cá nhân
Hỗ trợ module RESTful hoặc SOAP API với giao diện ETSI TS 119 432.
Kết nối giữa Server Signing Module (SCASC) và SAM+CM (SCDev) sử dụng cơ chế an toàn, bảo mật dựa trên chữ ký số
Hiện thị tài liệu ký tới người ký đảm bảo cơ chế Những gì nhìn thấy là những gì bạn ký.

Hiện thị tài liệu ký tới người ký theo cách thức diễn giải cụ thể.
Khi trình bày tài liệu cho người ký cần nêu rõ loại nội dung nào có thể được trình bày chính xác
Khi trình bày tài liệu cho người ký, giao diện sẽ cảnh báo người ký nếu nó không thể trình bày chính xác tất cả các phần dữ liệu ký theo loại nội dung dữ liệu
Khi trình bày tài liệu cho người ký, nó sẽ có một quy trình làm việc trong đó rõ ràng cho ng ười ký rằng người ký đồng ý với việc ký văn bản
Khi xuất trình tài liệu cho người ký, cho phép tải xuống tài liệu cần ký
Lưu lại các hoạt động ký.
Lưu lại các hoạt động sau khi ký như là tải xuống file.
Đảm bảo tính toàn vẹn và bảo mật của thông tin nhận được
Cho phép có thể chọn thuật toán mật mã (ký/hàm băm an toàn) trước khi ký
Các thuật toán mật mã (ký/hàm băm an toàn) được áp dụng phải được xác định trong chính sách tạo chữ ký
Nên bao gồm chứng thư số trong chữ ký
Công bố chính sách tạo chữ ký nào sẽ được áp dụng cho người ký

Công bố chính sách tạo chữ ký nào sẽ được áp dụng cho người ký khi tạo chữ ký
Cho phép người ký tải xuống tài liệu đã được ký hoặc chữ ký
Cho phép người ký tải xuống tài liệu đã được ký hoặc chữ ký
chính sách được xây dựng; thuê bao cần được thông báo, như là một phần của việc thực hi ện các điều khoản và điều kiện, về cách thức mà chính sách cụ thể bổ sung hoặc hạn chế h ơn các yêu cầu của chính sách như được định nghĩa trong tài liệu này
Chính sách được xây dựng; chính sách cần được phê duyệt và sửa đổi theo quy trình xem xét được xác định, bao gồm cả trách nhiệm duy trì chính sácH

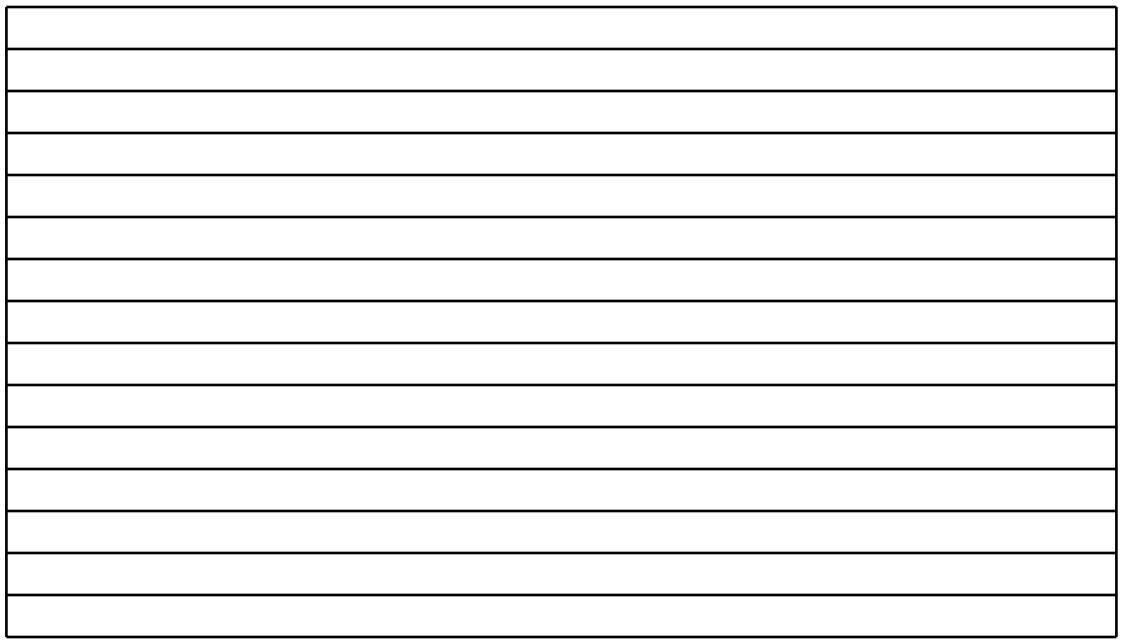
1. Giới thiệu
1.1 Tổng quan
1.1.1 Nhận dạng TSP
1.1.2 Chính sách / chính sách thành phần dịch vụ ứng dụng tạo chữ ký được hỗ trợ (nhận d ạng OID / URI chính thức)
1.2 Môi trường thành phần dịch vụ ứng dụng tạo chữ ký
1.2.1 SCASC
1.2.3 Kiến trúc dịch vụ
1.3 Định nghĩa và viết tắt
1.3.1 Định nghĩa
1.3.2 Viết tắt
1.4 Chính sách và thực tiễn
1.4.1 Tổ chức quản lý tài liệu TSP
1.4.2 Người liên hệ
1.4.3 Khả năng áp dụng tài liệu TSP (công khai)
Điều khoản này mô tả tập hợp các tài liệu liên quan đến SCASC, khả năng áp dụng và vị trí của tuyên bố thực hành hiện tại trong tài liệu, các điểm phân phối của chúng.
Tối thiểu các tài liệu sau tồn tại và cần một mô tả ngắn:
• tuyên bố thực hành hiện tại (nên sử dụng nhận dạng OID / URI chính thức);
• các điều khoản và điều kiện;
• chính sách dịch vụ (có thể được giới thiệu)
một hoặc nhiều tài liệu trên xác định chính sách / chính sách tạo chữ ký được hỗ trợ (với nh ận dạng OID / URI chính thức). Chính sách / chính sách tạo chữ ký được hỗ trợ thường đư ợc nêu chi tiết trong chính sách / chính sách dịch vụ của SCASC.
• đánh giá rủi ro và chính sách bảo mật thông tin

2. Quản lý và vận hành dịch vụ ủy thác
Điều khoản này có thể chung cho tất cả các dịch vụ do TSP cung cấp
2.1 Tổ chức nội bộ
2.1.1 Độ tin cậy của tổ chức
(Điều khoản này xác định nghĩa vụ của tất cả các tổ chức bên ngoài hỗ trợ các dịch vụ TSP bao gồm các chính sách và thực tiễn áp dụng (theo ETSI EN 319 401 [9])
2.1.2 Phân chia nhiệm vụ
2.2 Nhân lực
2.3 Quản lý tài sản
2.3.1 Yêu cầu chung
2.3.2 Xử lý phương tiện truyền thông
2.4 Kiểm soát truy cập
2.5 Kiểm soát mật mã
2.6 An ninh vật lý và môi trường
2.7 Bảo mật hoạt động
2.8 Bảo mật mạng
2.9 Quản lý sự cố
2.10 Thu thập bằng chứng
2.11 Quản lý liên tục kinh doanh
2.12 kế hoạch chấm dứt và chấm dứt TSP
2.13 Tuân thủ

3. Yêu cầu kỹ thuật thành phần dịch vụ tạo chữ ký
3.1 Giao diện
Điều khoản này chứa các yêu cầu, mục tiêu kiểm soát và kiểm soát liên quan đến khoản 8.1. trong ETSI TS 119 431-2.
3.2 Tạo chữ ký số AdES
Điều khoản này chứa các yêu cầu, mục tiêu kiểm soát và kiểm soát liên quan đến khoản 8.2. trong ETSI TS 119 431-2

Cung cấp các thông lệ tốt nhất để tạo chữ ký / con dấu điện tử tiên tiến dựa trên chứng chỉ X.509. OVR-B.1-01: [CONDITONAL] Trường hợp SCASC được sử dụng để tạo chữ ký điện t ử tiên tiến, chứng chỉ ký sẽ xác định người ký. OVR-B.1-02: [CONDITONAL] Trường hợp SCASC được sử dụng để tạo con dấu điện tử tiên tiến, chứng nhận ký sẽ xác định người tạo ra con dấu. OVR-B.1-03: Chứng chỉ ký sẽ được chứa trong chữ ký AdES đã tạo.
Chữ ký điện tử tiên tiến phải đáp ứng các yêu cầu sau: - nó được liên kết duy nhất với người ký SCP 37: CA sẽ bảo vệ tham chiếu hoặc bản sao chứng chỉ ký trong chữ ký khỏi sự thay th ế không bị phát hiện sau khi chữ ký được tạo. - nó có khả năng xác định người ký; - nó được tạo bằng cách sử dụng dữ liệu tạo chữ ký điện tử mà người ký có thể, với mức độ tin cậy cao, sử dụng dưới sự kiểm soát duy nhất của mình - nó được liên kết với dữ liệu đã ký theo cách sao cho mọi thay đổi tiếp theo trong dữ liệu đều có thể phát hiện được." " OVR-8.2-02 Các thuật toán mã hóa được sử dụng nên được chọn từ các thuật toán được đề xuất bởi ETSI TS 119 312 [i.5].

SSASC có thể giới hạn danh sách SCDev được hỗ trợ theo các điều khoản và điều kiện củ a nó (OVR-6.2-05).

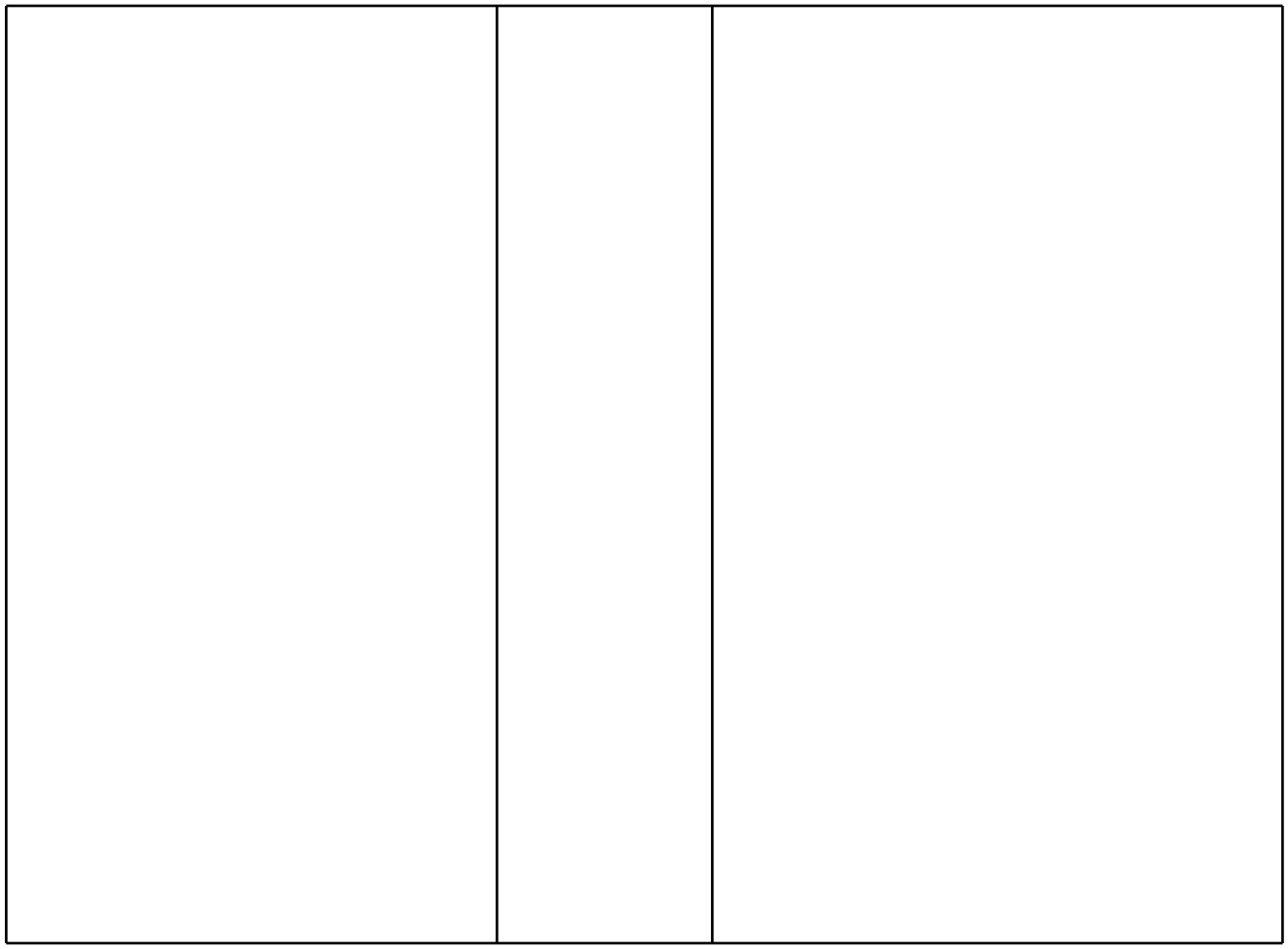


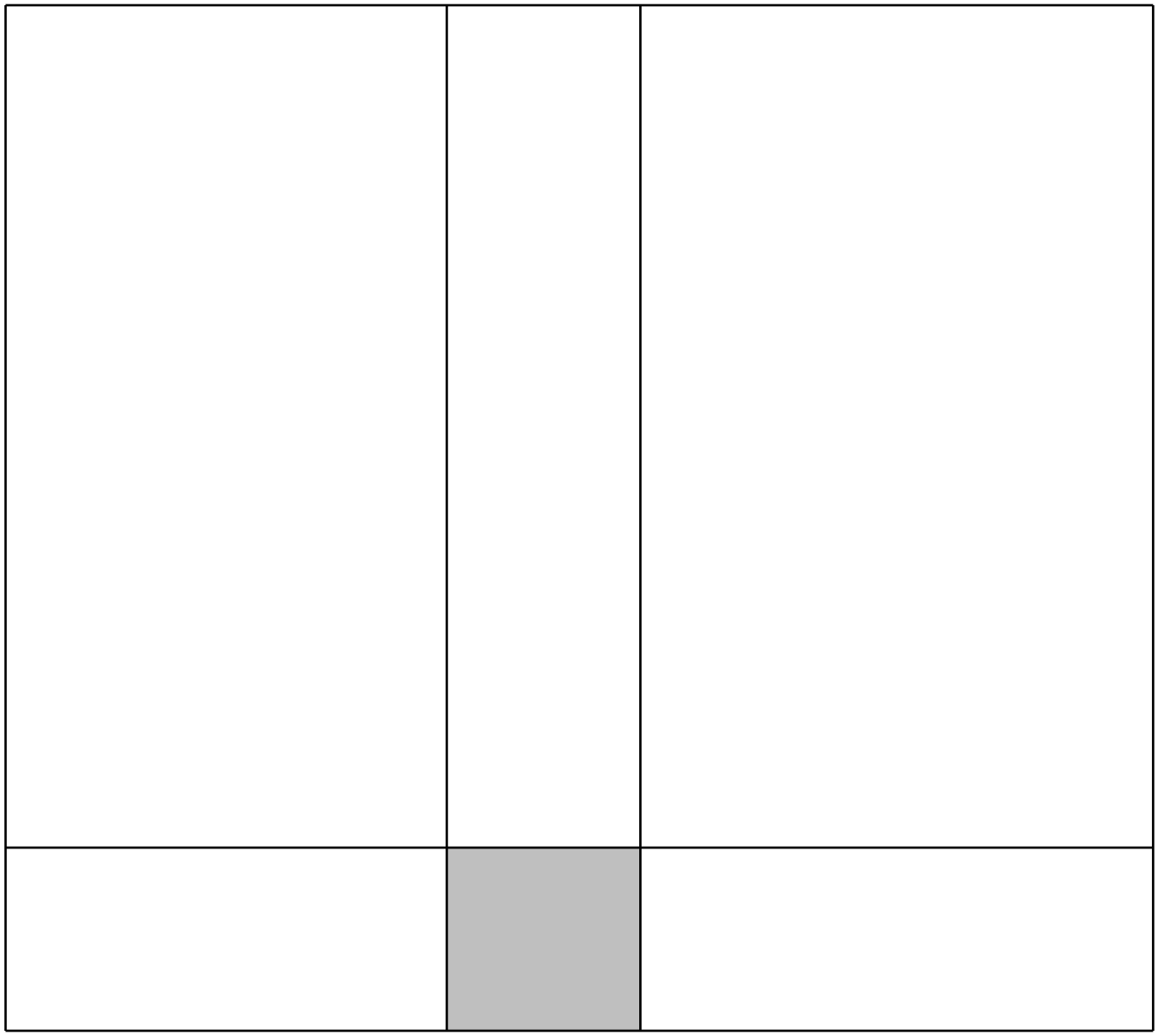
Điều kiện đáp ứng	Yêu cầu	Tài liệu tham chiếu
<Phần này cụ thể yêu cầu cần phải đáp ứ	<Bắt buộc, khuyế	<Tài liệu tham chiếu để hiểu chi tiết hơn>
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	ETSI TS 119 431-1
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	ETSI TS 119 102-1 ETSI TS 119 101

		Các tài liệu tham khảo sau đây là cần thiết cho việc áp dụng tài liệu này. [1] ETSI TS 119 101: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Yêu cầu chính sách và bảo mật cho các ứng dụng để tạo chữ ký và xác nhận chữ ký". [2] ETSI TS 119 102-1 (V1.2.1): "Chữ ký điện tử và cơ sở hạ tầng (ESI); Thủ tục tạo và xác nhận chữ ký số AdES; Phần 1: Tạo và xác thực". [3] ETSI EN 319 122-1: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số CAdES; Phần 1: Khối xây dựng và chữ ký cơ sở CAdES". [4] ETSI EN 319 122-2: "Chữ ký điện tử và cơ sở hạ tầng (ESI); chữ ký số CAdES; Phần 2: Chữ ký CAdES mở rộng". [5] ETSI EN 319 132-1: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số XAdES; Phần 1: Khối xây dựng và chữ ký cơ sở XAdES". [6] ETSI EN 319 132-2: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số XAdES; Phần 2: Chữ ký XAdES mở rộng". [7] ETSI EN 319 142-1: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số PAdES; Phần 1: Xây dựng chữ ký cơ sở khối và chữ ký PAdES". [8] ETSI EN 319 142-2: "Chữ ký điện tử và cơ sở hạ tầng (ESI); Chữ ký số PAdES; Phần 2:

Kiểm tra SCP được công bố	M	

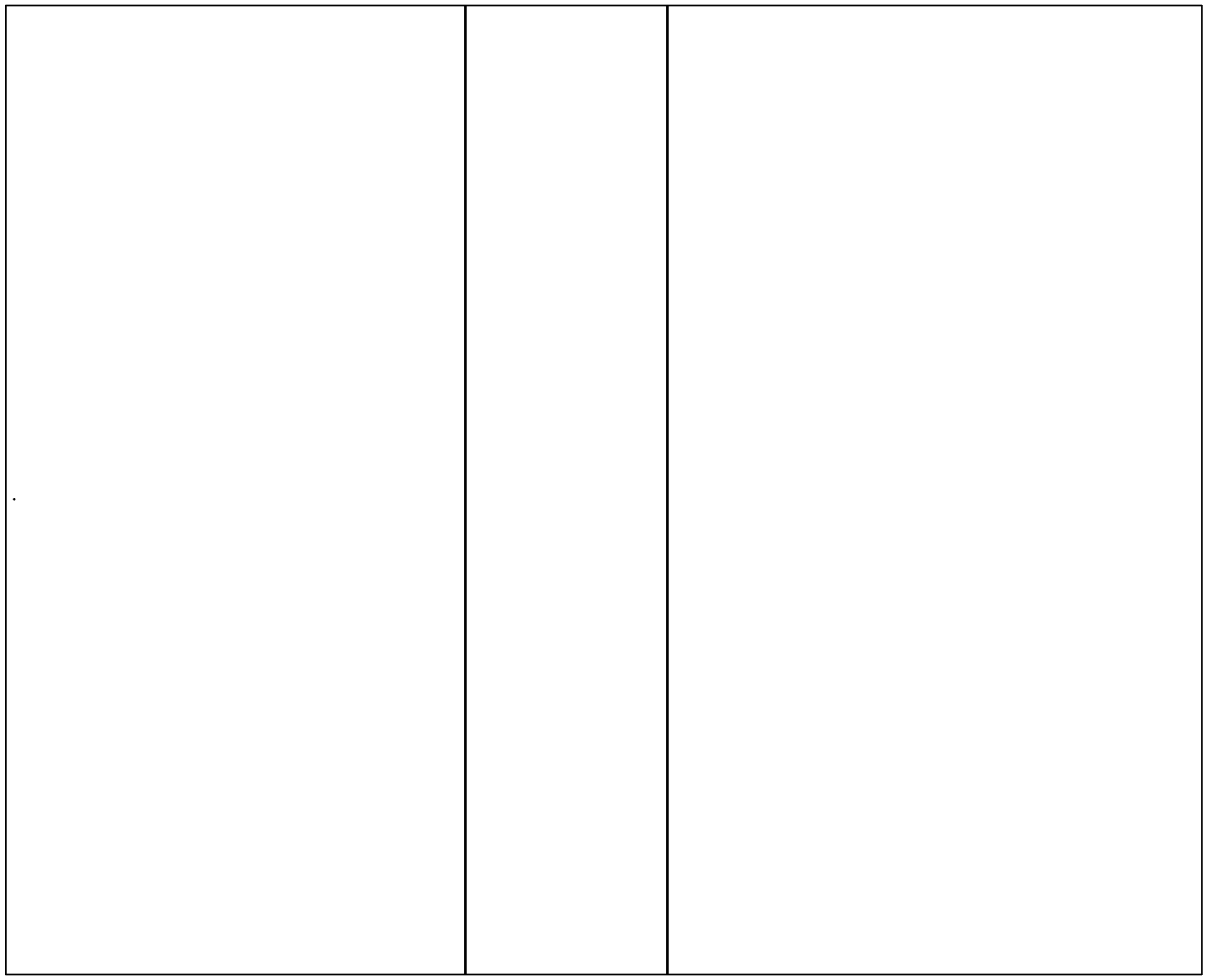
Kiểm tra SCP được công bố	M	



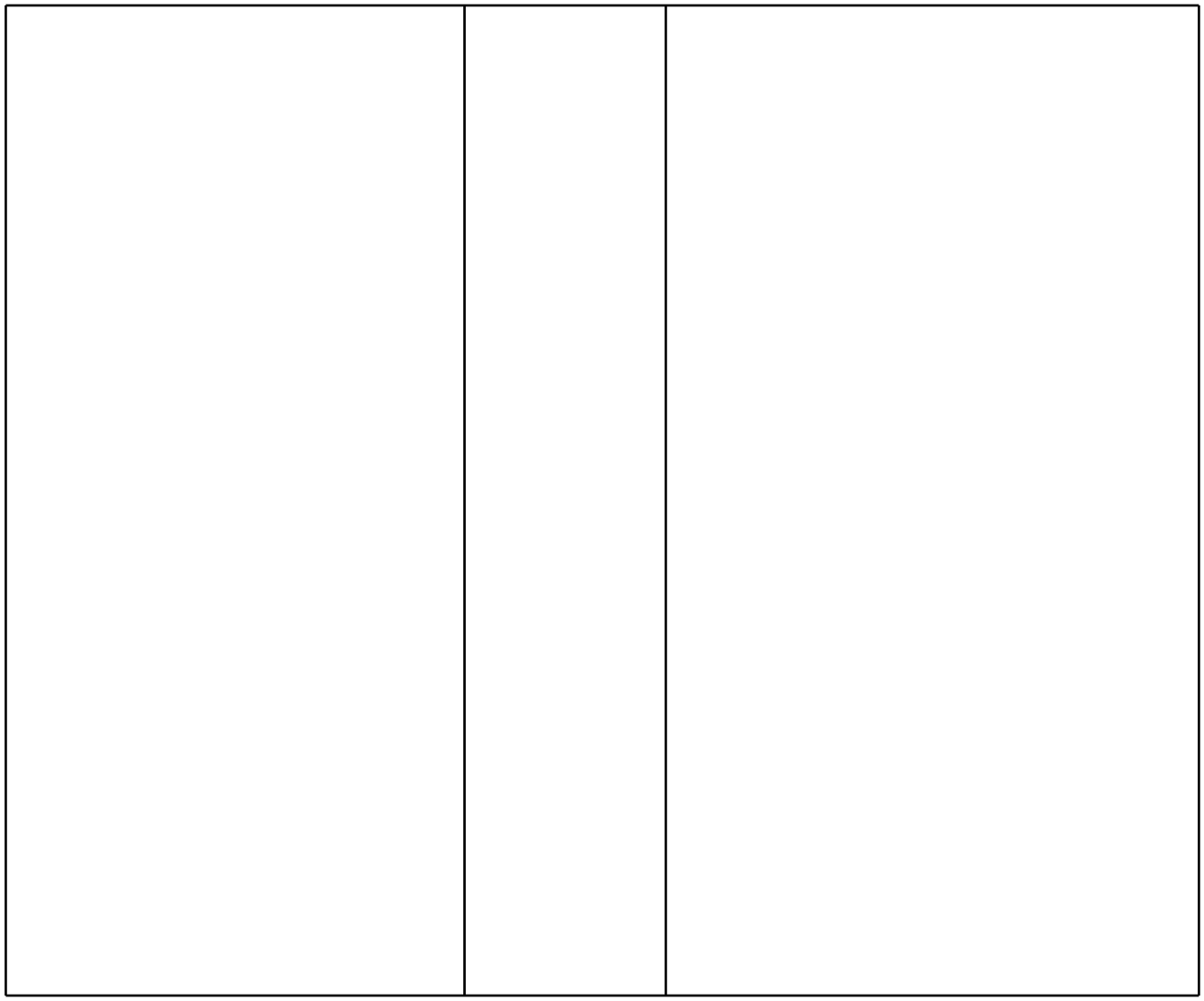


Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố	M	



Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	



Kiểm tra SCP được công bố	M	

Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	

Kiểm tra SCP được công bố	M	
.		
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	

Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	

Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	

Kiểm tra SCP được công bố	M	

.		
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố	M	

Kiểm tra SCP được công bố	M	
Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Kiểm tra SCP được công bố Hồ sơ kỹ thuật được công bố	M	

Tiêu chuẩn tương đương	
<Tương đương với quy định tại chuẩn nào RFC,	Đơn vị thực hiện