RENIEC

Identidad digital

Modelos y estándares de firma remota en la UE

REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC

Lima, Marzo 2017.
PERÚ

SEGURIDAD DE EXTREMO A EXTREMO

- La **eficacia** de la firma digital descansa sobre la **confianza** que se pueda tener en ésta, la que a su vez depende de la **seguridad** con la que se genera
- El **eslabón más débil** en la cadena es el que determina el nivel de seguridad de un sistema
- **Las políticas establecidas y los esquemas de acreditación, auditoría o certificación** permiten demostrar que las entidades, el software o dispositivo de firma y los servicios necesarios para la generación de la firma digital **son confiables**
- Existen **firmas electrónicas de especial calidad** generadas bajo esquemas regulados y auditados a las que se atribuye la **presunción de validez y eficacia jurídica** de la firma manuscrita, por ejemplo, la firma digital de la IOFE
- **Principio de seguridad en la implantación y utilización de medios electrónicos para la prestación de servicios de gobierno electrónico** (Reg. Art. 41.4)

REGULACIÓN TÉCNICA EN LA IOFE

Guía de acreditación de ECs y la firma remota

El Reglamento en sus artículos 7 y 8 establece que la firma digital se genera bajo el control exclusivo del suscriptor, siendo éste quien mantiene el control exclusivo de su clave privada

Guía de Acreditación de Entidades de Certificación:

- Anexo 1 (6.2.1): *Los módulos criptográficos usados por los titulares o suscriptores… deben cumplir los requerimientos de FIPS 140-2 nivel 1 como mínimo.*
- Anexo 1 (3.2.1): *La EC debe establecer en su CPS el procedimiento para probar la posesión de la clave privada, el cual puede ser hecho por el suscriptor o por la ER…*
- Anexo 1 (4.2.2): *…se debe requerir al suscriptor y titular: ser razonablemente diligente en la custodia de su clave privada con el fin de evitar usos no autorizados… notificar sin retrasos injustificables la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, token criptográfico o tarjeta inteligente).*

Guía de acreditación de ECs y la firma remota

- Anexo 1 (4.12.1): *No está permitido para la EC/ER emisora el almacenamiento del original, copia o backup alguna de las claves privadas… a excepción de los certificados de cifrado…*

  En caso que la EC brinde el servicio de almacenamiento de claves de cifrado, dicha entidad debe establecer en su CPS u otra documentación relevante sus políticas y prácticas al respecto…deberá incluirse acuerdos para la seguridad de las claves…

  El contrato de suscriptor deberá contemplar el consentimiento del depósito/ almacenamiento de las claves privadas de cifrado.

  En los casos en que la EC establezca determinadas obligaciones para los suscriptores o titulares en relación al acceso a las claves privadas de cifrado, el acuerdo del suscriptor debe recoger claramente tales obligaciones.

REGULACIÓN TÉCNICA SOBRE FIRMA ELECTRÓNICA EN LA UNIÓN EUROPEA

Conceptos

- ***Trust Service Provider (TSP)* o pretador de servicios de confianza:** es aquella entidad que provee uno o más servicios electrónicos de confianza
- ***Qualified Trust Service Provider (QTSP)* o prestador cualificado de servicios de confianza:** un prestador de servicios de confianza que presta uno o varios servicios y al que el organismo de supervisión ha concedido acreditación y efectúa auditorías regularmente
- ***Signature Generation Service Provider (SGSP)* o prestador de servicios de generación de firmas remotas:** *TSP* que brinda servicios para posibilitar la gestión remota segura del dispositivo de creación de firma del suscriptor y la generación de firmas electrónicas por medio de tal dispositivo
- La **firma electrónica avanzada** es aquella creada usando datos de creación de firma electrónica (claves privadas o SCD) **que el suscriptor pueda, con un alto nivel de confianza, usar bajo su exclusivo control**
- La **firma electrónica reconocida o cualificada** es una firma electrónica avanzada creada por un dispositivo de creación de firmas electrónicas cualificado y que está basada en un certificado cualificado

Conceptos

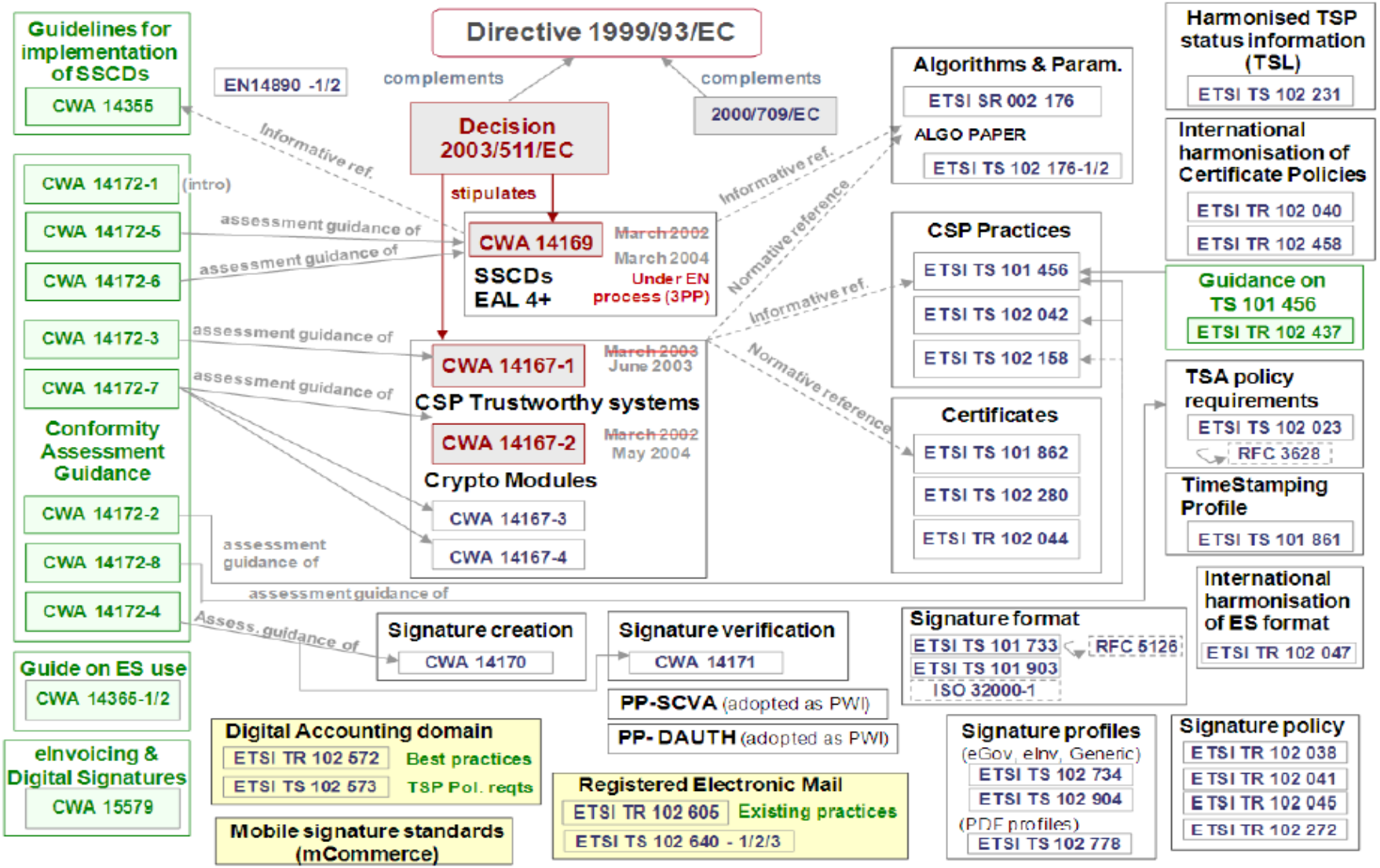
Especificación técnica CEN/TS 419 241:

"Este documento describirá los requisitos de seguridad para un sistema implementado en un servidor de red para la creación de firmas electrónicas avanzadas (AdES) basadas en certificados digitales. En concordancia con los requisitos de la Directiva Europea de Firma Electrónica 1999/93, la firma será soportada por un certificado digital cualificado, u otro certificado emitido para uso de firma, emitido por un Prestador de Servicios de Confianza (TSP) operando de acuerdo a buenas prácticas (por ejemplo EN 319411-3, también conocido como TS 102 042 o EN 319411-2, también conocido como TS 101 456). Se incluirá requisitos para el uso de perfiles de protección adecuados para el dispositivo de creación de firma (SCDev).

El propósito del sistema confiable es producir una firma electrónica avanzada creada bajo el exclusivo control de una persona natural, o de una persona jurídica…

El Proveedor de Servicios de Generación de Firmas (SGSP) opera el sistema confiable en un entorno con una política de seguridad que incorpora requisitos de seguridad generales, físicos, de personal, de procedimientos y para la documentación conforme se definen en EN 319411-2 y EN 319411-3."

Problemática de la estandarización europea



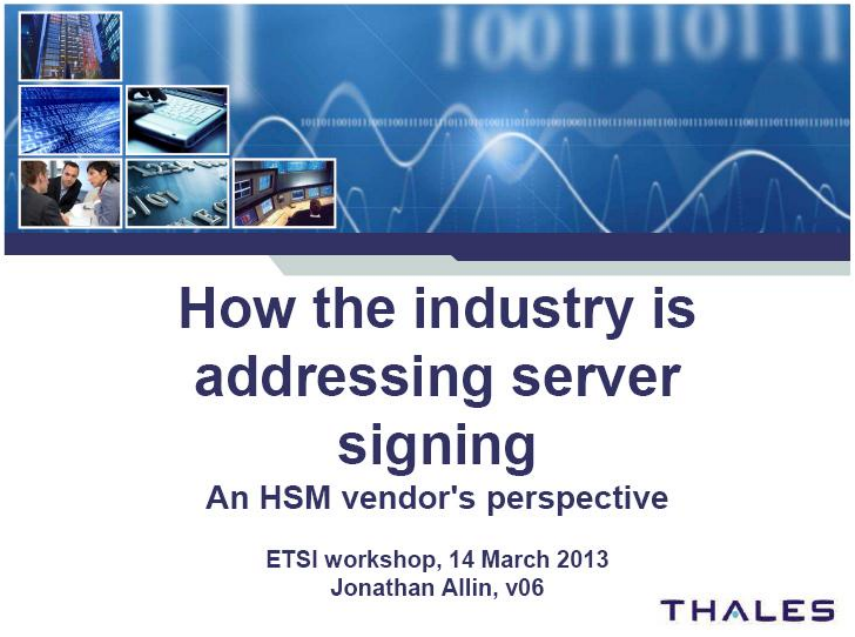
Problemática de la estandarización europea

- **Estudio sobre aspectos de estandarización de las firmas electrónicas** (SEALED, DLA Piper et al, CE, 2007) concluye en que la multiplicidad de estándares junto con la falta de lineamientos para su uso, las dificultades para acceder a estos y la carencia de una orientación específica a los negocios es perjudicial para el reconocimiento mutuo y la interoperabilidad de la firma electrónica

- **Mandato M/460** a los organismos de estandarización europeos en el campo de las tecnologías de la información y telecomunicaciones aplicado a las firmas electrónicas (CE, diciembre 2009), dado con el alcance de lograr la interoperabilidad de la firma electrónica a nivel europeo, definiendo un marco racionalizado para la estandarización de la firma electrónica y los lineamientos para su implementación

Problemática de la firma remota

Taller de ETSI sobre firma remota (2013):

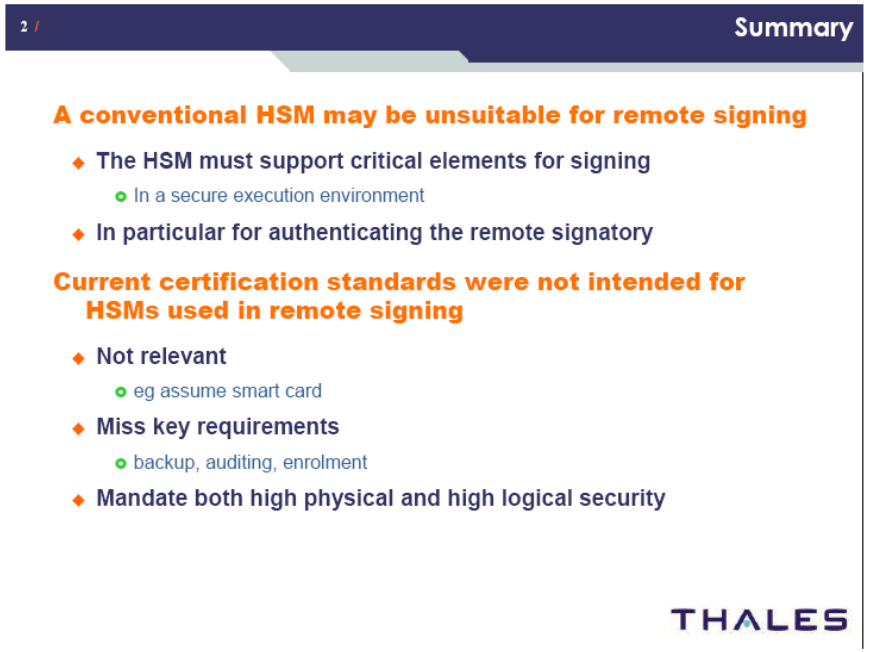


How the industry is addressing server signing

An HSM vendor's perspective

ETSI workshop, 14 March 2013
Jonathan Allin, v06

THALES

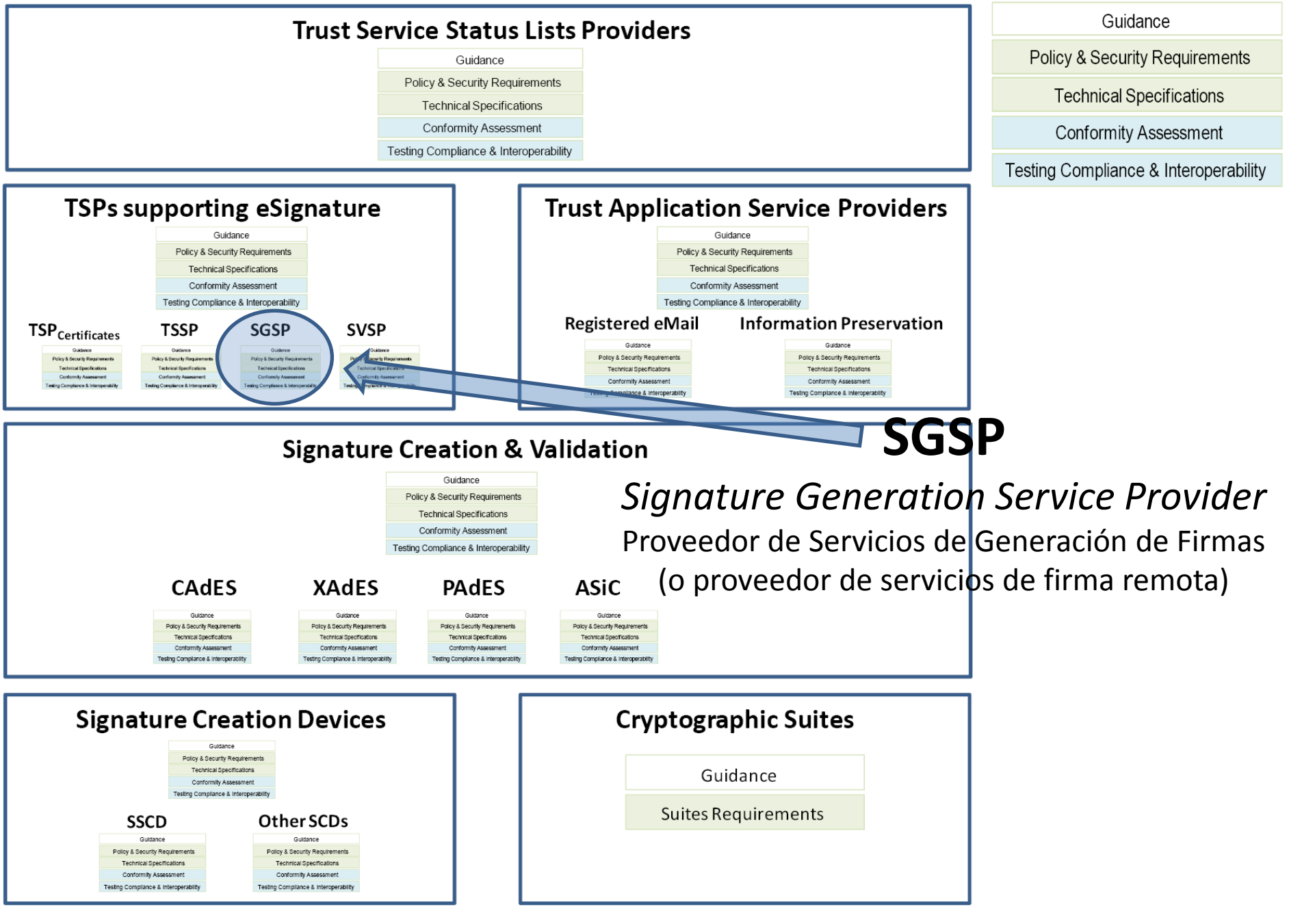


«Un HSM convencional puede no ser adecuado para la firma a distancia…»

«Los **estándares** de certificación actuales no fueron diseñados para HSMs a usarse en firmas remotas…»

Marco racionalizado para la estandarización de la firma electrónica

- El marco racionalizado se publica en el reporte especial ETSI SR 001 604 de julio de 2012, documento actualizado en el reporte técnico TR 119 000 de setiembre de 2015
- Presenta una estructura basada en 6 áreas funcionales con sus correspondientes sub-áreas
- Respecto de cada área funcional se tienen cinco tipos de documentos que son: guías, políticas y requisitos de seguridad, especificaciones técnicas, auditorías de conformidad y cumplimiento de pruebas e interoperabilidad
- Al diseñarse el marco racionalizado se encontraba en curso la revisión de la Directiva de firma electrónica, lo que concluyó con la publicación del Reglamento eIDAS. En concordancia con éste, se ampliará su alcance comprendiendo tanto las firmas como la identificación y la autenticación electrónicas



SGSP

Signature Generation Service Provider

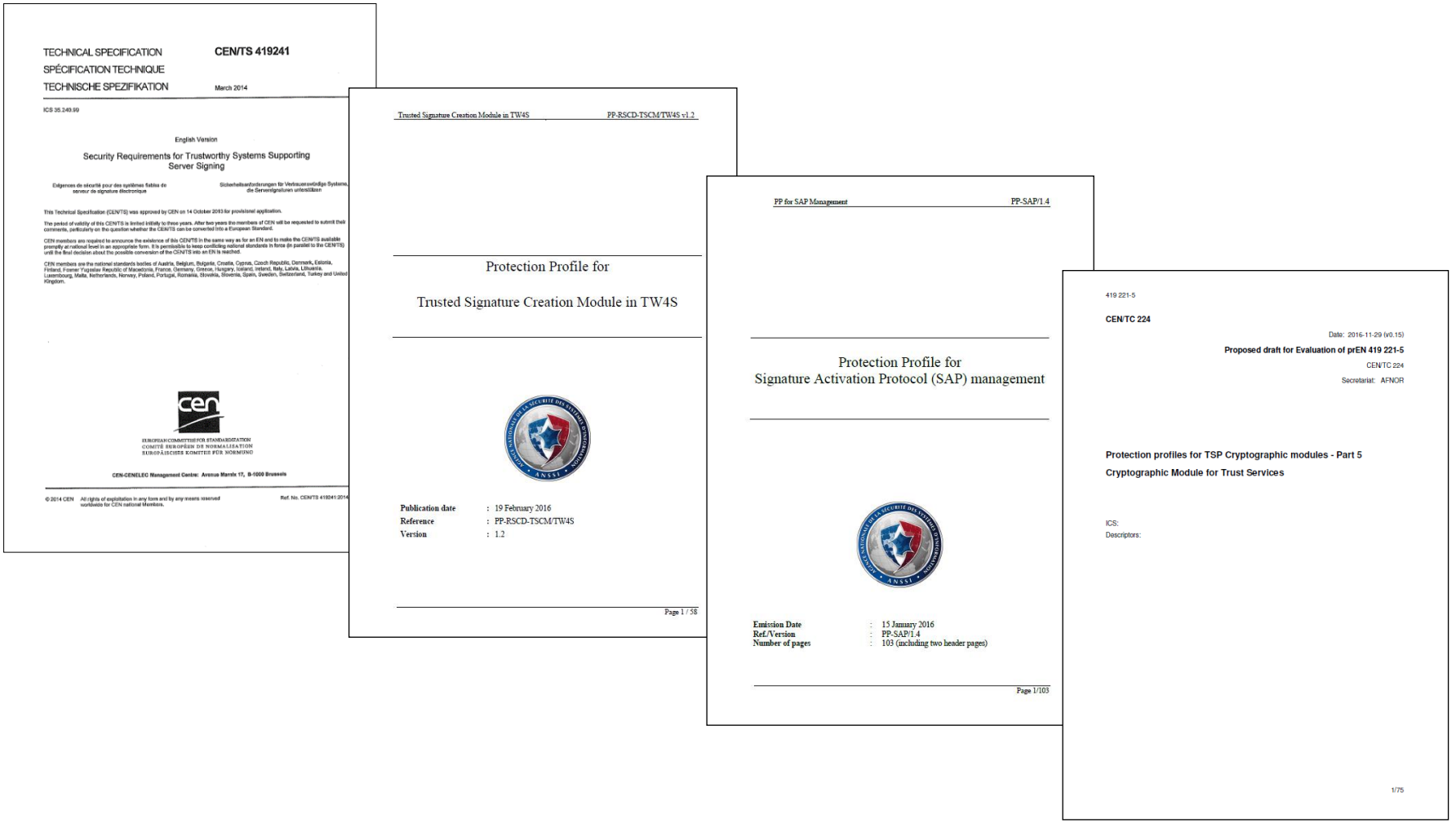
Proveedor de Servicios de Generación de Firmas
(o proveedor de servicios de firma remota)

Área funcional II: Dispositivos de creación de firma y otros relacionados

- Guidance
- Policy & Security Requirements
- Technical Specifications
- Conformity Assessment
- Testing Compliance & Interoperability

Signature creation and other related devices							Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	4	19	2	0	0	Business driven guidance for signature creation and other related devices	(new)	February 2016
						Policy & Security Requirements		
EN	4	19	2	1	1	Protection profiles for secure signature creation device - Part 1: Overview - Part 2: Device with key generation - Part 3: Device with key import - Part 4: Extension for device with key generation and trusted communication with certificate generation application - Part 5: Extension for device with key generation and trusted communication with signature creation application - Part 6: Extension for device with key import and trusted communication with signature creation application	 - (new part) - prTS 14169-2 - prTS 14169-3 - prTS 14169-4 - prEN 14169-5 - (new part)	published
EN	4	19	2	2	1	Protection Profiles for TSP cryptographic modules - Part 1: Overview - Part 2: Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP) - Part 3: Cryptographic module for CSP key generation services – Protection Profile (CMCKG-PP) - Part 4: Cryptographic module for CSP signing operations without backup – Protection Profile (CMCSO PP) - Part 5: Cryptographic module for trust services	 - (new part) - prTS 14167-2 - prTS 14167-3 - prTS 14167-4 - (new part)	 By end 2015 By end 2015 By end 2015 By end 2015 In 2016
EN	4	19	2	3	1	Protection profile for trustworthy systems supporting time stamping	(new)	In 2016
EN	4	19	2	4	1	Security requirements for trustworthy systems supporting server signing - Part 1: Security requirements - Part 2: Protection profile for trustworthy signature creation module (PP-TSCM) - Part 3: Protection profile for signature activation data management and signature activation protocol (PPSAD+SAP)	CWA 14167-5	 - TS published (EN: 2015) - undefined - undefined
EN	4	19	2	5	1	Security requirements for device for authentication - Part 1: Protection profile for core functionality - Part 2: Protection profile for extension for trusted channel to certificate generation application - Part 3: Additional functionality for security targets	EN 16248 (PP-DAUTH)	published
EN	4	19	2	6	1	Security requirements for trustworthy systems managing certificates for electronic signatures	prTS 14167-1	published
						Technical Specifications		
EN	4	19	2	1	2	Application interfaces for secure elements used as qualified electronic signature (seal-) creation devices - Part 1: Introduction - Part 2: Basic services - Part 3: Device authentication - Part 4: Privacy specific protocols - Part 5: Trusted eServices	EN 14890	Parts 1 & 2: published Other parts: by end 2015
						Conformity Assessment		
						no requirement identified		
						Testing Conformance & Interoperability		
-		-	-	-	-	*no requirement identified*		

Estándares publicados



TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN/TS 419241

March 2014

ICS 35.240.99

English Version

Security Requirements for Trustworthy Systems Supporting Server Signing

Exigences de sécurité pour des systèmes fiables de serveur de signature électronique

Sicherheitsanforderungen für Vertrauenswürdige Systeme, die Serversignaturen unterstützen

This Technical Specification (CEN/TS) was approved by CEN on 14 October 2013 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TS 419241:2014

Trusted Signature Creation Module in TW4S PP-RSCD-TSCM/TW4S v1.2

Protection Profile for

Trusted Signature Creation Module in TW4S

Publication date : 19 February 2016
Reference : PP-RSCD-TSCM/TW4S
Version : 1.2

Page 1 / 58

PP for SAP Management PP-SAP/1.4

Protection Profile for
Signature Activation Protocol (SAP) management

Emission Date : 15 January 2016
Ref./Version : PP-SAP/1.4
Number of pages : 103 (including two header pages)

Page 1/103

---

419 221-5

CEN/TC 224

Date: 2016-11-29 (v0.15)

Proposed draft for Evaluation of prEN 419 221-5

CEN/TC 224

Secretariat: AFNOR

Protection profiles for TSP Cryptographic modules - Part 5
Cryptographic Module for Trust Services

ICS:
Descriptors:

1/75

Área funcional IV: Proveedores de servicios de confianza que soportan **firma** electrónica

TSPs supporting digital signatures and related services							Replaces	Expected publication
				Sub-areas				
				Guidance				
TR	1	19	4	0	0	Business driven guidance for TSPs supporting digital signatures	(new)	Published
				Policy & Security Requirements				
EN	3	19	4	0	1	General policy requirements for trust service providers	Replacing generic parts of TS 101 456, TS 102 042, (TR 102 040), TS	- TS: July 2015 - EN: March 2016
EN	3	19	4	1	1	Policy and security requirements for trust service providers issuing certificates - Part 1: General requirements - Part 2: Requirements for TSP issuing EU qualified certificates - Part 3: *To be made historical* - Part 4: Requirements for TSP issuing code signing certificates	- TS 102 042 (EV & BR), EN 319 411-3 - TS 101 456 (& TR 102 458), EN 319 411-3 - historical - (new)	- TS: July 2015 - EN: March 2016 - historical - undefined
EN	3	19	4	2	1	Policy & security requirements for trust service providers issuing time-stamps	TS 102 023	- TS: July 2015 - EN: March 2016
EN	3	19	4	3	1	Policy and security requirements for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	1	Policy and security requirements for trust service providers providing AdES digital signature validation services	(new)	Undefined
				Technical Specifications				
EN	3	19	4	1	2	Certificate profiles - Part 1: Overview and common data structures - Part 2: Certificate profile for certificates issued to natural persons - Part 3: Certificate profile for certificates issued to legal persons - Part 4: Certifcate profile for web site certificates issued to organisations - Part 5: QCStatements	- (new part) - TS 102 280 & TS 101 862 - (new part) - (new part)	All parts: - TS: July 2015 - EN: March 2016
EN	3	19	4	2	2	Time-stamping protocol and time-stamp profiles	TS 101 861	- TS: July 2015 - EN: March 2016
EN	3	19	4	3	2	Protocol profiles for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	2	Protocol profiles for trust service providers providing AdES digital signature validation services	(new)	Undefined
				Conformity Assessment				
EN	3	19	4	0	3	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers	CWA 14172 (2&8), TS 119 403	- TS: Nov. 2014 - EN: end 2015
				Testing Conformance & Interoperability				
-	-	-	-	-	-	*no requirement identified for such a document*		

Especificación de requisitos de seguridad para sistemas de firma remota TS 419 241-1

Niveles de control exclusivo de las claves privadas

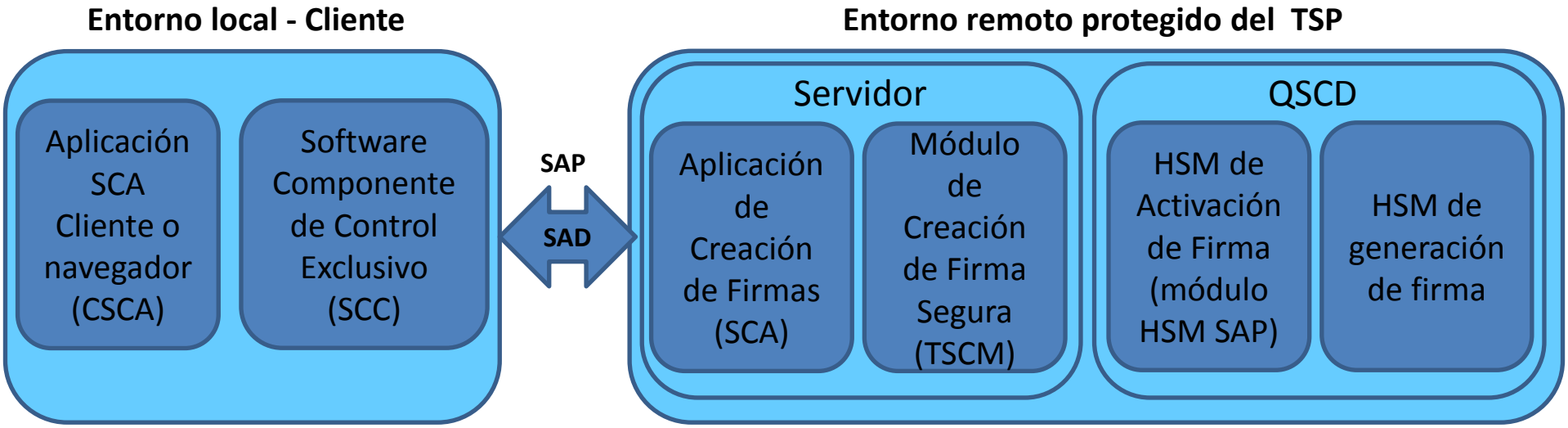
Nivel 1:

- La autenticación frente al sistema puede hacerse mediante un único factor.
- La autenticación del firmante no es exigida por un dispositivo de creación de firma (SCDev) sino por la aplicación de firma remota del servidor (SSA), siendo éste el que establece el vínculo con la identidad autenticada y el que activa las llaves privadas (SCD) del suscriptor para efectuar la firma
- Las llaves privadas (SCD) no necesariamente se gestionan a través de un HSM y, de ser este el caso, no necesariamente se trata de un Dispositivo Cualificado de Creación de Firma (QSCD)
- En este caso las firmas generadas podrán ser firmas electrónicas avanzadas, más no firmas electrónicas cualificadas

Nivel 2

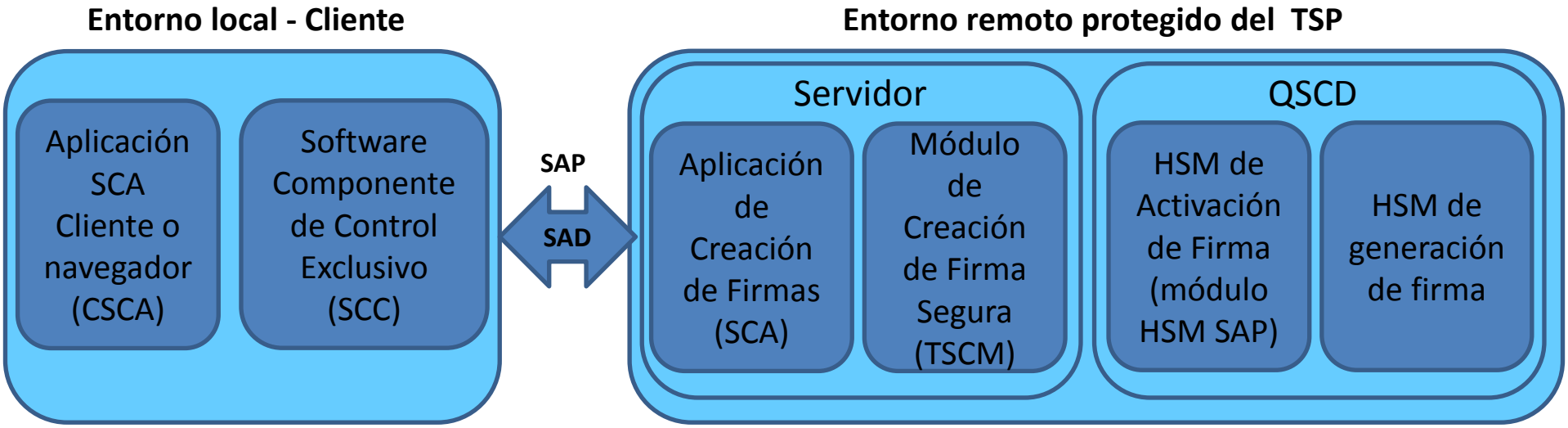
- La autenticación del firmante es exigida por el dispositivo de creación de firma (SCDev) valiéndose del uso protegido de los datos de activación de firma (SAD)
- Se pretende que la autenticación brinde un nivel de confiabilidad equivalente en el control exclusivo de las claves privadas (SCD) al que ofrecen los QSCD *stand-alone*
- Para ello se requiere de una autenticación fuerte o multifactores al suscriptor a través de la posesión de un *token* en combinación con una contraseña
- Para efectuar firmas electrónicas cualificadas es requisito que éstas sean gestionadas en un QSCD (en el caso de firmas remotas, en un HSM)
- Para generar firmas electrónicas remotas cualificadas se requiere del nivel 2 de control exclusivo de las claves privadas
- Las firmas electrónicas cualificadas europeas son comparables a las firmas digitales que se generan en el Perú bajo el marco acreditativo de la IOFE

Modelo de firma remota para firmas cualificadas



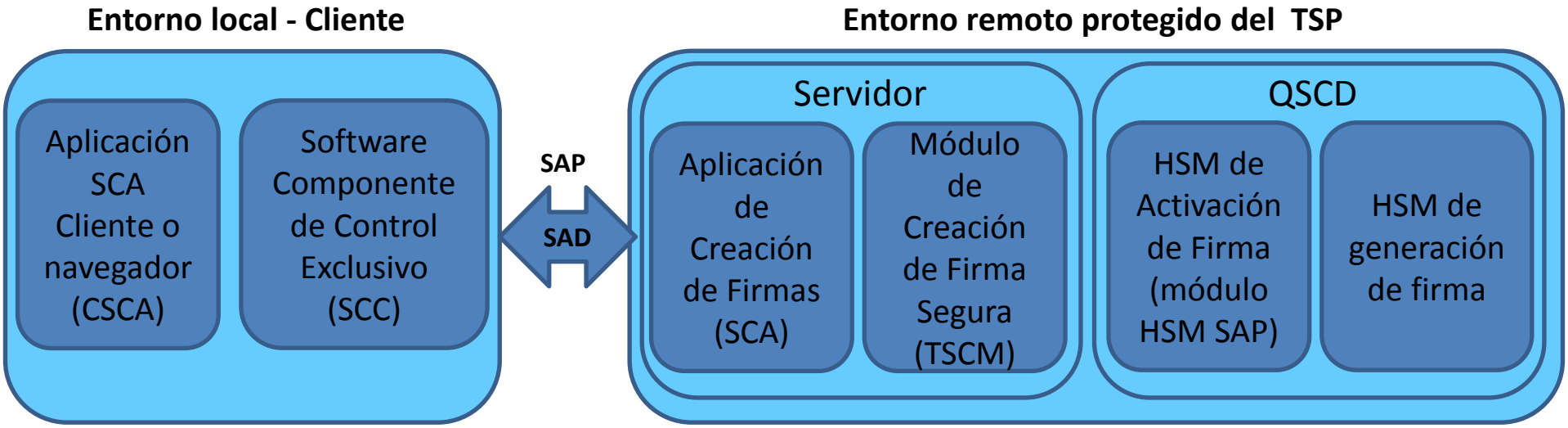
- A través de la Aplicación de Creación de Firmas o SCA (incluyendo la parte local o CSCA) se inicia la solicitud de firma
- El Módulo de Creación de Firmas Confiable o TSCM gestiona las solicitudes de firma
- El módulo HSM SAP brinda control de acceso a la operación de firma que efectúa el HSM de generación de firma en nombre del suscriptor

Modelo de firma remota para firmas cualificadas



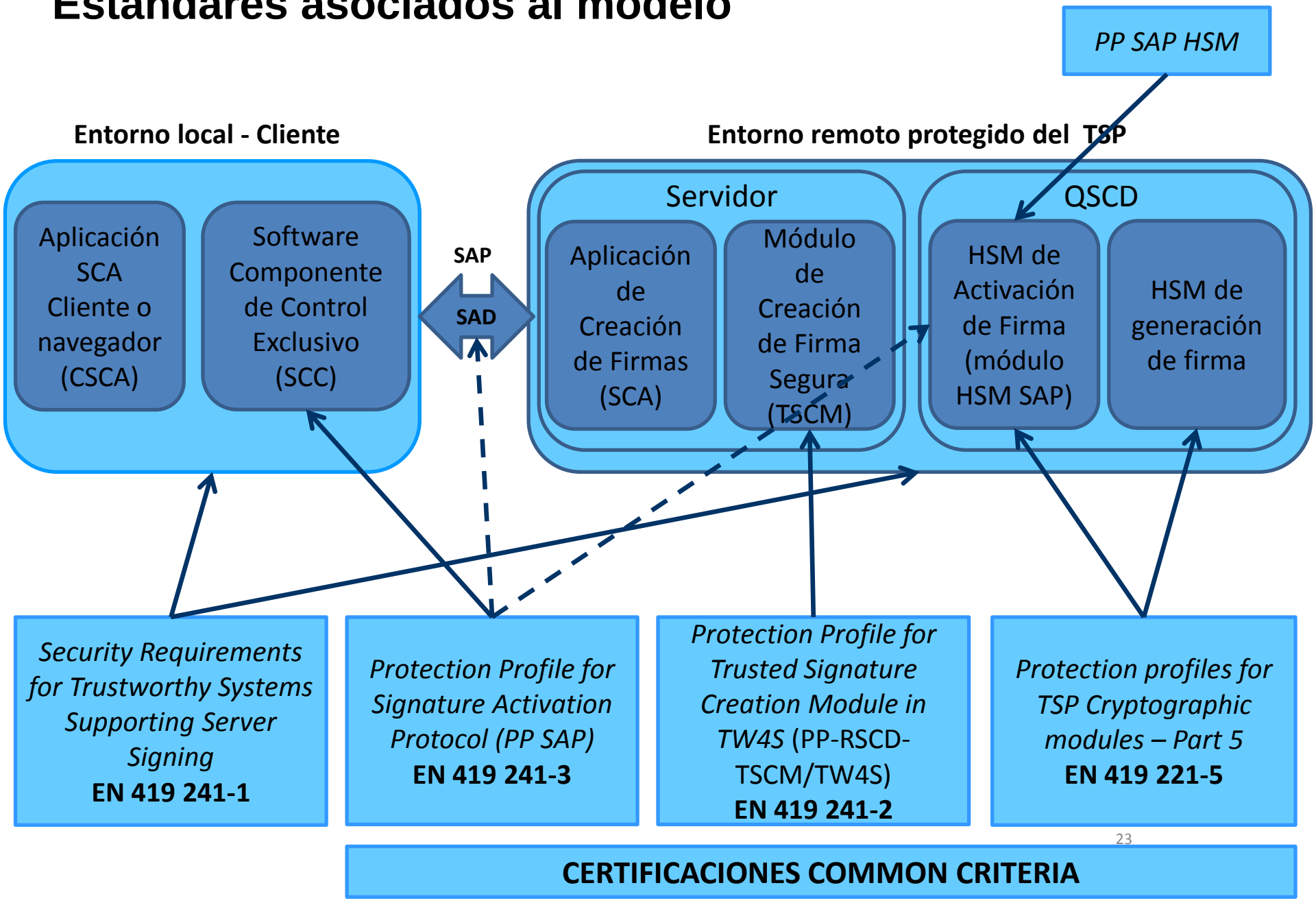
- Los Datos de Activación de Firma (SAD) viajan desde el SCC en el entorno local del cliente hasta el Dispositivo de Creación de Firma Cualificado o QSCD, en particular al módulo HSM SAP de Activación de firma, bajo el Protocolo de Activación de Firma o SAP (canal seguro)
- El Protocolo de Activación de Firma (SAP) genera los Datos de Activación de Firma (SAD) y garantiza el vínculo entre el firmante debidamente autenticado, los datos de firma (claves privadas o SCD) y los datos a firmarse garantizándose el control exclusivo

Modelo de firma remota para firmas cualificadas

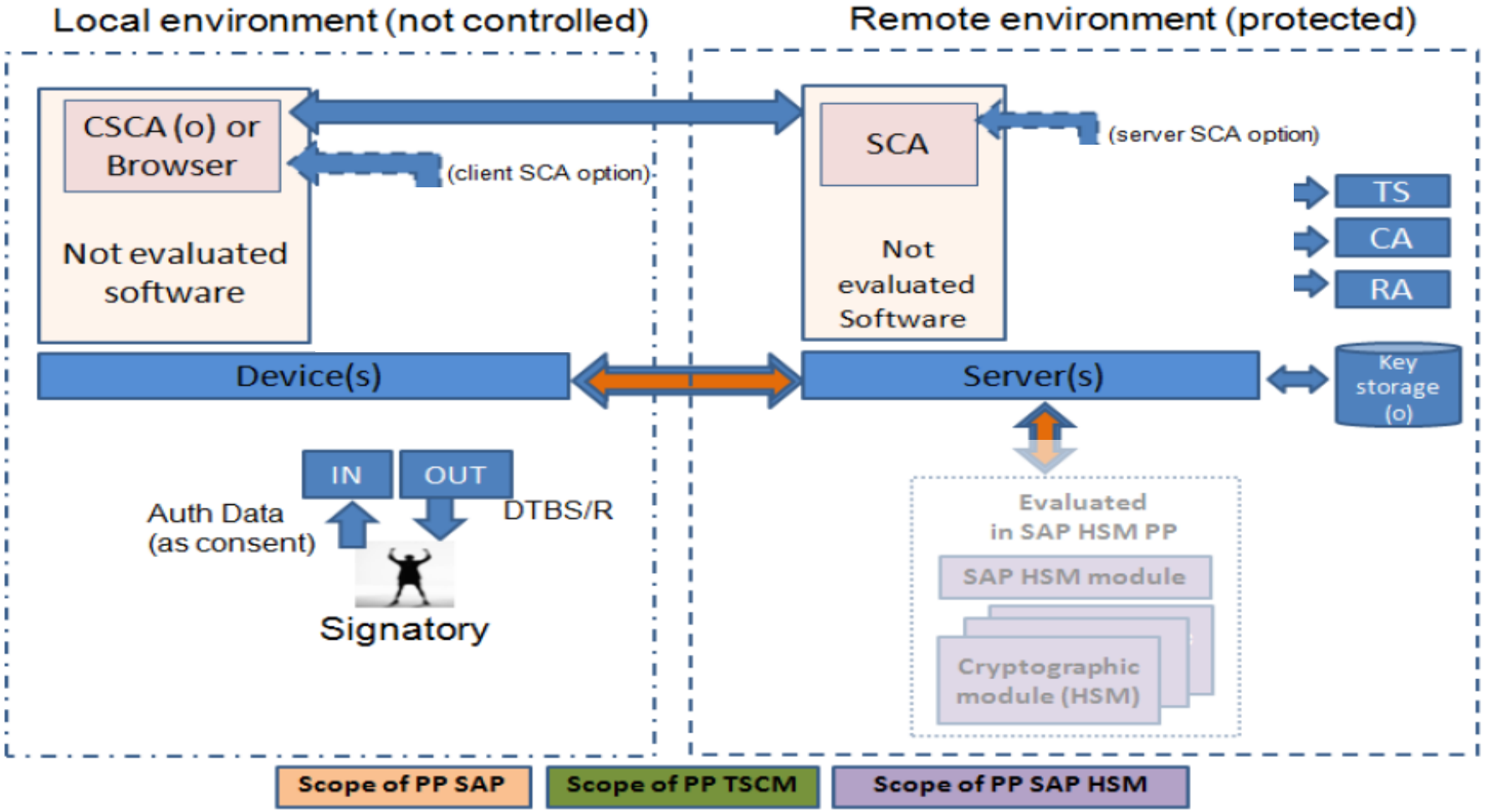


- La combinación del SCC con el TSCM y el QSCD interactuando a través del SAP constituyen un Dispositivo de Creación de Firma Cualificado Remoto (RQSCD)
- Bajo este modelo se implementa un control exclusivo de las claves privadas de nivel 2 y, en la medida que se utilicen certificados digitales cualificados, se posibilita la generación de firmas electrónicas cualificadas de manera remota

Estándares asociados al modelo



Modelo de firma remota para firmas electrónicas (no cualificadas)



(Fuente: Protection Profile for Signature Activation Protocol (SAP) management, ANSSI, 15ENE2016)

GRACIAS

Modelos y estándares de firma remota en la UE

REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC

Lima, Marzo 2017.
PERÚ