CENTRO CRIPTOLÓGICO NACIONAL

Spanish Information Technology Security Evaluation and Certification Scheme

IT-009

Remote Qualified Electronic Signature Creation Device Evaluation Methodology

Version 1.0

January 2017

Documento del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Copia no controlada en soporte papel.

Index

1 References

1 Presidential Order PRE/2740/2007, dated 19th of September 2007, which approves the Information Security Evaluation and Certification Scheme Regulation.http://oc.ccn.cni.es

2 REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) and repealing Directive 1999/93/EC

3 Commission Implementing Decision (EU) 2016/650 of 25 April 2016

4 CEN/prEN 419241 Trustworthy Systems Supporting Server Signing, (to be published).

5 ISO/IEC IS 15408 Information technology — Security techniques — Evaluation criteria for IT security

6 ISO/IEC IS 18045 Information technology — Security techniques — Methodology for IT security evaluation

2 Acronyms

CAP	Composition Assurance Package
ESR	Essential Security Requirements
rSCDev	Remote Electronic Signature Creation Device
rQSCDev	Remote Qualified Electronic Signature Creation Device
SAM	Signature Activation Module
SCDev	Signature Creation Device
SISECS	Spanish Information Security Evaluation and Certification Scheme
SSA	Server Signing Application
TW4S	Trustworthy System Supporting Server Signing

3 Introduction

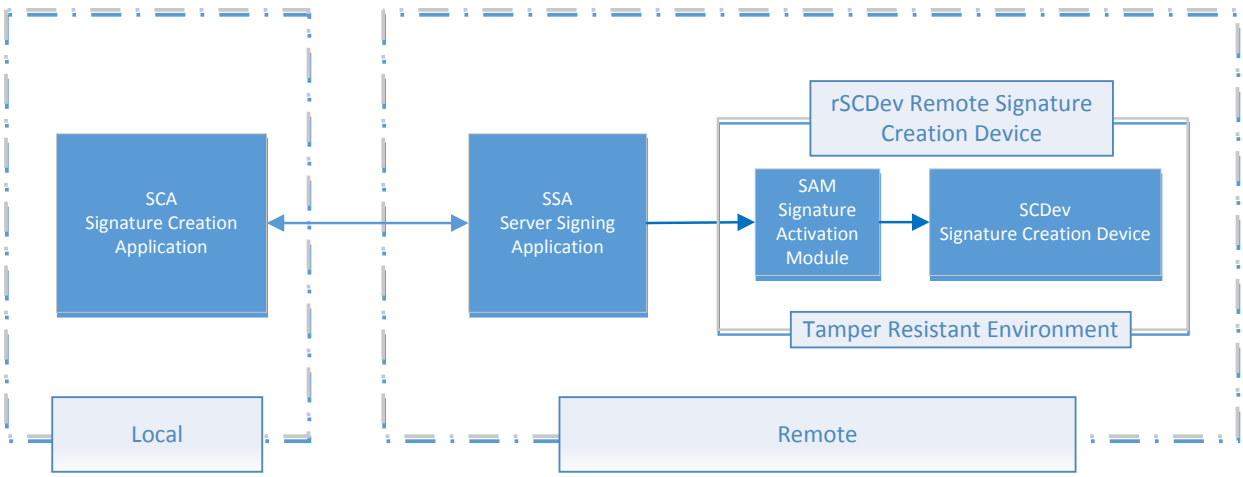
7 The purpose of a Remote Qualified Electronic Signature Creation Device (rQSCDev) is to produce a digital signature, created on behalf of, and under sole control of, a natural person or a legal person, which may be recognised as a qualified electronic signature as defined in the eIDAS 2 Regulation.

4 Scope

8 Trustworthy System Supporting Server Signing (TW4S) may consist of a local and remote environment. The signer is in the local environment and interacts through a local application with the Server Signing Application (SSA) in the remote environment.

9 To ensure the signer has sole control of his signature keys, the signature operation needs to be authorized. This is carried out by a Signature Activation Module (SAM) which can retrieve and activate the signing key within a Signature Creation Device (SCDev), normally implemented as a Cryptographic Module. The Signature Creation Device and the SAM are to be located within a common tamper resistant environment that may be considered as the Remote Signature Creation Device (rSCDev).

10 The rSCDev, in combination with the SSA, are the basis for the TW4S, that need to be operated in a secure manner, and meeting some requirements for the system to be qualified as such.



5 Evaluation Methodology

11 Until the establishment by the Commission of a list of standards for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices, where a qualified trust service provider manages the electronic signature creation data on behalf of a signatory, the certification of such products shall be based on an process that, pursuant to Article 30(3)(b), uses security levels comparable to those required by Article 30(3)(a) and that is notified to the Commission by the public or private body referred to in paragraph 1 of Article 30 of Regulation (EU) No 910/2014. 3

12 *The certification of a Remote Qualified Electronic Signature Creation Device by the Spanish Information Security Evaluation and Certification Scheme (SISECS) shall be based on the following:*

a. *Products claiming SAM and/or SCDev functionality will be evaluated and certified in accordance to the evaluation criteria defined in 5 ISO/IEC 15408, and with the evaluation methodology laid out in 6 ISO/IEC 18045 "Methodology for IT security evaluation", at a minimum evaluation assurance level of EAL4+AVA_VAN.5.*

b. *Products claiming SAM and/or SCDev functionality will have a Security Target defined for their evaluation that is based on the corresponding Essential Security Requirements (ESR) specified in Annex I. The proper and technically correct compliance of these ESR will be analysed by the SISECS before accepting a product certification request.*

c. *There are no preconceived design rules in regards to SAM and/or SCDev implementations, ranging these from a single product or component meeting all applicable security requirements, to a combination of products whose composition meets the ESR.*

   In the case where two or more products or components are required to meet both the SAM and SCDev functionality, there is an additional need to evaluate the security of their composition, considering their interactions and ensuring that the interface between the components has been evaluated. A vulnerability analysis of the composed SAM and SCDev shall also be performed to consider the possible introduction of vulnerabilities as a result of composing the components.

   The composition of products or components required in combination to meet both the SAM and SCDev functionality will be evaluated and certified in accordance to the evaluation criteria defined in 5 ISO/IEC 15408, and with the evaluation methodology laid out in 6 ISO/IEC 18045 "Methodology for IT security evaluation", applying a Composition Assurance Package of CAP-C.

d. *The security evaluation processes required by this methodology to a single product meeting only the SAM or the SCDev functionality will be regarded*

as certificates of compliance with respect to their individual Security Targets, but not of compliance with respect to their consideration as a rSCDev.

6 Annex I: Essential Security Requirements

6.1 ESRs for SAM

13 Essential Security Requirements to be met by the SAM:

a. The device shall be able to securely create a signer representation, and to protect the signer representation attributes associated both for integrity and if needed in confidentiality (ESR-QSCD-SIGNER-REPRESENTATION).

b. The device shall be able to securely use the Cryptographic Module to generate signer signing key pairs and assign them to the signer representation, protecting the keys for integrity and confidentiality as required (ESR-QSCD-CK GENERATION).

c. The device shall ensure that an administrator with a privileged role is authenticated before any action is performed. It shall also ensure that any modification to the signer representation data, keys, or authentication attributes is performed under control of the signer or a trusted role (ESR-QSCD-ATTR MODIFICATION).

d. The device shall ensure the signer is strongly authenticated before performing any action. The device shall implement a signature activation protocol, which also provides integrity of the transmitted representation of the document to be signed and signature activation data, confidentiality of at least the elements which contains sensitive information, and protection against signature reply (ESR-QSCD-SIGNER AUTH).

e. The device shall ensure that storage and transmission of critical data from the signer to the device, like the representation of the document to be signed or signature authentication data is protected against attacks, modification or disclosure (ESR-QSCD-TRUSTED PATH).

f. The device shall also ensure that no signer data or attributes, neither document to be signed representation or signatures are modified or disclosed while inside the device (ESR-QSCD-INTEGRITY).

g. The device shall generate an audit trail of the relevant security events. The device shall ensure that modifications to this audit trail can be detected (ESR-QSCD-AUDIT)

6.2 ESRs for Cryptographic Module (SCDev) for Server Signing

14 Essential Security Requirements to be met by the SCDev:

a. The plaintext value of secret keys shall not be made available outside the Cryptographic Module (ESR-CM-NO PLAINTEXT).

b. The Cryptographic Module offers key generation functions and other cryptographic functions provided for users that are endorsed by recognised authorities as appropriate (ESR-CM-CRYPTO QUALITY).

c. The value and critical attributes of keys (secret or public) have their integrity protected by the Cryptographic Module against unauthorised modification. Critical attributes in this context are defined to be those implementation-level attributes of a key that could be used by an attacker to cause the equivalent of a modification to the key value by other means (ESR-CM-KEY INTREGRITY).

d. The Cryptographic Module shall carry out an authentication/authorisation check on all subjects before allowing them to use the Cryptographic Module. In particular, the Cryptographic Module shall always require authorisation before using a secret key (ESR-CM-AUTHORISATION).

e. Any key (secret or public) shall have an unambiguous definition of the purposes for which it can be used, in terms of the cryptographic functions or operations (e.g. encryption or signature) that it is permitted to be used for. The Cryptographic Module shall reject any attempt to use the key for a purpose that is not permitted. (ESR-CM-KEY PURPOSE).

f. The Cryptographic Module shall have an unambiguous definition of the subjects that are permitted to access the key (and the purposes for which this access can be used) and shall allow this to be set to the granularity of an individual subject. (ESR-CM-KEY ACCESS).

g. The Cryptographic Module shall define and apply clearly stated limits on when authorisation and reauthorisation are required in order for a secret key to be used. (ESR-CM-KEY REAUTH).

h. The Cryptographic Module shall provide secure channels to client applications that can be used to protect the confidentiality of sensitive data during transmission between the client application and the Cryptographic Module, or during transmission between separate parts of the Cryptographic Module where that transmission passes through an insecure environment. (ESR-CM-PATH CONDENCIALITY).

i. The Cryptographic Module shall provide secure channels to client applications that can be used to protect the integrity of sensitive data during transmission between the client application and the Cryptographic Module. (ESR-CM-PATH INTEGRITY).

j. The Cryptographic Module shall allow import and export of secret keys only by using a secure method that protects the confidentiality and integrity of the data during transmission. Secret keys shall only be exported in encrypted form. (ESR-CM-KEY SECURE EXPORT/IMPORT).

k. The Cryptographic Module shall allow individual secret keys under its control to be identified as non-exportable, in which case any attempt to export them will be rejected automatically. Public keys may be imported and exported in a manner that protects the integrity of the data during transmission. ((ESR-CM-NO EXPORT).

l. Any method provided by the Cryptographic Module for backing up user data, including secret keys, shall preserve the security of the data and is controlled only by authorised Administrators. The secure backup process shall preserve the confidentiality and integrity of the data during creation, transmission, storage and restoration of the backup data. Backups shall also preserve the integrity of the attributes of keys. (ESR-CM-BACKUP).

m. Random numbers generated and provided to client applications for use as keys, authentication/authorisation data, or seed data for another random number generator that is used for these purposes shall meet a defined quality metric in order to ensure that random numbers are not predictable and have sufficient entropy. (ESR-CM-RNG).

n. The Cryptographic Module shall provide features to protect its security functions against tampering. In particular the Cryptographic Module shall make any physical manipulation within the scope of the intended environment detectable for the administrators of the Cryptographic Module. (ESR-CM-ANTITAMPER).

o. The Cryptographic Module shall detect faults that would cause some other security property to be weakened or to fail, including environmental conditions outside normal operating range, temperature and power, failures of critical Cryptographic Module hardware components, of the random number generator, and corruption of Cryptographic Module software. On detection of a fault, the Cryptographic Module shall take action to maintain its security and the security of the data that it contains and controls. (ESR-CM-FAULT DETECTION).

p. The Cryptographic Module shall create audit records for security-relevant events, recording the event details and the subject associated with the event. The Cryptographic Module shall ensure that the audit records are protected against accidental or malicious deletion or modification of records by providing tamper protection (either prevention or detection) for the audit log. (ESR-CM-AUDIT).