PD CEN/TS 419241:2014

BSI Standards Publication

Security Requirements for Trustworthy Systems Supporting Server Signing

National foreword

This Published Document is the UK implementation of CEN/TS 419241:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 82798 3
ICS 35.240.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2014.

Amendments/corrigenda issued since publication

Date	Text affected

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

Ref. No. CEN/TS 419241:2014 E

Contents

Page

Foreword

This document (CEN/TS 419241:2014) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

Successful implementation of European Directive 1999/93/EC on a community framework for electronic signatures requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products.

In 1999 the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players, to create the European Electronic Signature Standardization Initiative (EESSI).

Within this framework the Comité Européen de Normalisation / Information Society Standardization System (CEN/ISSS) and the European Telecommunications Standards Institute / Electronic Signatures and Infrastructures (ETSI/ESI) were entrusted with the execution of a work programme to develop generally recognized standards to support the implementation of Directive 1999/93/EC and the development of a European electronic signature infrastructure.

This document will describe security requirements for a server-side system using certificates in order to create advanced electronic signatures (AdES) in accordance with the requirements of the European Directive on Electronic Signature 1999/93. The signature is to be supported by a qualified certificate, or other public key certificate issued for the purposes of signing, issued by a Trust Services Provider (TSP) operating to recognized good practices (e.g. ETSI EN 319 411-3 (aka ETSI/TS 102 042) or ETSI EN 319 411-2 (aka ETSI/TS 101 456)). The document will include requirements for the use of the appropriate protection profiles for the Signature Creation Device (SCDev).

The purpose of the trustworthy system is to produce an advanced electronic signature created under sole control of a natural person, or a legal person (such advanced electronic signatures produced by legal persons are called electronic seals).

The Signature Generation Service Provider (SGSP) operates the trustworthy system in an environment with a security policy which incorporates general physical, personnel, procedural and documentation security requirements as defined in ETSI EN 319 411-2 / ETSI EN 319 411-3.

This document is identified as CEN/TS 419241 within the Rationalised Framework for Electronic Signature Standardization ETSI SR 001 604.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: 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 the United Kingdom.

Introduction

The European Directive 1999/93/EC establishes a framework of requirements for the use of electronic signatures. This Directive also introduces the notion of advanced electronic signature which is defined as legally equivalent to a hand-written one if generated by a physical person using a qualified certificate stored in a Secure Signature Creation Device (SSCD).

Since the publication of the Directive, other forms of electronic signatures have appeared in order to meet market needs (e.g. e-Invoicing, e-Procurement). These other forms do not necessarily require the use by a natural or legal person of a secure signature creation device and/or qualified certificate.

One of these forms is an electronic signature created using a networked server. The Signature Creation Data (SCD) is under control of an individual user but held centrally within a shared server, instead on a secure signature creation device held by the signatory.

It is not the intent of this standard to limit the type of public key certificate, qualified or otherwise, used by the networked signing server.

The main objective of this standard is to define requirements and recommendations for a networked signing server which may process electronic certificates used by natural or legal persons for electronically signing documents.

This document specifies basic requirements for server signing. Additional specifications may be issued which provide more detailed requirements. For further details see ETSI SR 001 604.

1 Scope

1.1 General

This document specifies security requirements and recommendations for Trustworthy System Supporting Server Signing (TW4S) that generate advanced electronic signatures as defined in Directive 1999/93/EC. This document may also be applied to electronic signatures complying to Article 5(1) of Directive 1999/93/EC employing a Secure Signature Creation Device (SSCD) compliant with Annex III and supported by a qualified electronic signature.

The Server Signing Application (SSA) runs on a networked server supporting one or more signatories to remotely sign electronic documents using centralized signature keys held on the signing server under sole control of the signatory.

An SSA is intended to deliver to the user or to some other application process in a form specified by the user, an Advanced- or where applicable a Qualified - Electronic Signature associated with a Signer's Document as a Signed Data Object.

This document:

- provides commonly recognized functional models of TW4S;
- specifies overall requirements that apply across all of the services identified in the functional model;
- specifies security requirements for each of the services identified in the SSA.
- specifies security requirements for sensitive system components which may be used by the SSA (e.g. Signature Creation Device (SCDev)).

This document does not specify technologies and protocols, but rather identifies requirements on the security on technologies to be employed.

1.2 Out of scope

The following aspects are considered to be out of scope:

- other trusted services that may be used alongside this service such as signature validation service, time-stamping service and information preservation service,
- any application or system outside of the SSA,
- the legal interpretation of any form of signature (e.g. the implications of countersignatures, of multiple signatures and of signatures covering complex information structures containing other signatures).

1.3 Audience

This document specifies security requirements that are intended to be followed by:

- providers of SSA systems.
- Trust Service Providers (TSP) offering signature generation service.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 419211 (all parts), *Protection profiles for secure signature creation device*

CWA 14167-2, *Cryptographic module for CSP signing operations with backup — Protection profile — CMCSOB PP*

CWA 14167-3, *Cryptographic module for CSP key generation services protection profile — CMCKG-PP*

CWA 14167-4, *Cryptographic module for CSP signing operations — Protection profile — CMCSO PP*

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 19790:2006, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Advanced Electronic Signature
electronic signature which meets the following requirements:

— it is uniquely linked to the signer;

— it is capable of identifying the signer;

— it is created using means that the signer can maintain under his sole control; and

— it is linked to the data to which it relates in such a manner that any subsequent alteration of the data is detectable

[SOURCE: Directive 1999/93/EC]

3.2
Certificate
electronic attestation that links a signature verification data to a person, and confirms the identity of that person

[SOURCE: Directive 1999/93/EC]

3.3
Certificate Identifier
unambiguous identifier of a Certificate

3.4
Certification Service Provider
entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

[SOURCE: Directive 1999/93/EC]

3.5
Data Content Type
signature attribute that expresses the encoding format of the Signers’ Document (SD)

3.6
Data To Be Signed
data (e.g. a document or parts of a document) to be signed as well as any signature attributes that are bound together with the data by the signature

NOTE Data To Be Signed is the input to the cryptographic signing algorithm. The specific way that Data To Be Signed and any signature attributes are fed as input is defined in the specifications of the signature type in use.

3.7
Electronic Signature
data in electronic form attached to - or logically associated with - other electronic data and which serves as a method of authentication of that data

[SOURCE: Directive 1999/93/EC]

3.8
Qualified Certificate
certificate which meets the requirements laid down in Annex I of the Directive [i.e. Dir. 1999/93/EC] and is provided by a certification service provider who fulfils the requirements laid down in Annex II of that Directive

[SOURCE: Directive 1999/93/EC]

3.9
Qualified Electronic Signature
advanced electronic signature which is based on a qualified certificate and which is created by a secure signature creation device

Note 1 to entry: This definition based on Article 5.1 of Directive 1999/93/EC.

3.10
Secure Signature Creation Device
signature creation device that meets the requirements laid down in Annex III of the EU Directive

[SOURCE: Directive 1999/93/EC]

3.11
Signatory
Signer
person who holds a signature creation device and acts either on his own behalf or on behalf of the natural or legal person he represents

[SOURCE: Directive 1999/93/EC]

Note 1 to entry: The term ‘signer’ is used throughout this document as a synonym.

3.12
Server Signing Application
application that provides a remote access to the Signature Creation Application (SCA)

3.13
Signature Creation Application
application that creates an electronic signature, using the digital signature produced by an SCDev connected to the SCA

3.14
Signature Creation Data
unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

[SOURCE: Directive 1999/93/EC]

3.15
Signature Creation Data Identifier
unambiguous identifier of a SCD

3.16
Signature Creation Device
configured software or hardware used to implement the SCD

[SOURCE: Directive 1999/93/EC]

Note 1 to entry: Secure Signature Creation Device (SSCD) or Hardware Security Module (HSM) are examples of Signature Creation Devices (SCDev).

3.17
Signature Creation Environment
physical, geographical and computational environment of the signature creation system

3.18
Signature Generation Service Provider
Trust Service provider which provides trust services that allow secure remote management of signatory's signature creation device and generation of electronic signatures by means of such a remotely managed device

3.19
Signature Invocation
non-trivial interaction between the signer and the SSA or SCDev that is necessary to invoke the start of the signing process in the SSA/SCDev to generate the Signed Data Object (SDO), and that is the 'Wilful Act' of the signer

3.20
Signature Policy
set of rules for the creation and validation of an electronic signature, that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need, and under which the signature can be determined to be valid

[SOURCE: ETSI/TS 101 733]

3.21
Signature Suite
combination of a signature algorithm with its parameters, a key generation algorithm, a padding method, and a cryptographic hash function

[SOURCE: ETSI/TS 102 176]

3.22
Signed Data Object (s)
document(s) or parts of the document(s) for which an electronic signature has been generated, along with the electronic signature

3.23
Signer’s Activation Data
data (e.g. PIN, password or biometric data, one time password or cryptographically generated authentication token) which is used to authenticate the signer to the SCDev and which is required to allow the use of the SCD held on the SCDev and which may be referred to as 'Activation Data' in other documents

3.24
Signer's/Signers’ Document
document for which one or more signers intend to create an Electronic Signature or for which an Electronic Signature was created

3.25
Trusted Path
path between two entities or components within an SSA that provides integrity and authenticity

3.26
Trust Service Provider
entity which provides electronic services which enhances trust and confidence in electronic transactions

3.27
Trustworthy System Supporting Server Signing
Server-side system using SCD in order to create Advanced Electronic Signatures (AdES) in accordance with the requirements of the European Directive on Electronic Signatures [i.e. Directive 1999/93/EC]

Note 1 to entry: The system includes at least an SSA and an SCDev.

4 Symbols and abbreviations

AdES	Advanced Electronic Signature
CC	Common Criteria, ISO/IEC 15408, *Evaluation criteria for IT security*
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CSP	Certification Service Provider
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
EC	European Commission
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISSS	Information Society Standardization System
PIN	Personal Identification Number
PKC	Public Key Certificate
QC	Qualified Certificate
QES	Qualified Electronic Signature
SAD	Signer's Activation Data
SCA	Signature Creation Application
SCD	Signature Creation Data

SCDev	Signature Creation Device
SCDid	Signature Creation Data Identifier
SD	Signers' Document
SDO	Signed Data Object
SGSP	Signature Generation Service Provider
SSA	Server Signing Application
SSCD	Secure Signature Creation Device
TS	Technical Specifications
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
WS/E-SIGN	CEN/ISSS Electronic Signatures workshop

5 Description of Trustworthy Systems Supporting Server Signing

5.1 General

This clause describes the different concepts of server signing in order to clarify how the requirements found in the next section should be implemented.

5.2 Signature Creation and Server Signing Objectives

The purpose of the SSA and the SCDev is to take an SD and the related signature attributes, form them into Data To Be Signed (DTBS) and produce over them an Advanced, or where applicable a Qualified, Electronic Signature and to produce a Signed Data Object (SDO) as a result.

The form of signature to be created including whether it is a Qualified or Advanced Electronic Signature comes within the scope of the applicable signature policy legal requirements.

5.3 AdES bound to a natural or legal person

The electronic signature for an electronic document applied in compliance with this standard can be the signature of a natural or legal person. Within the scope of the current document the term "signatory" is used to denote both a legal or natural person, and the term electronic signature is also used to denote an electronic seal created by a legal person.

In case the electronic signature is a natural person's, the identity of this natural person can be supplemented by that of a legal person to indicate that the natural person is acting in connection with a legal person when signing a document. This may be indicated using e.g. the "organizationName" within the subject of the natural person's certificate.

5.4 Levels of sole control

The Directive requires advanced electronic signature to be created under the sole control of the signatory.

Two levels of sole control are identified in the present document:

— Level 1: the signer authentication is not enforced by the SCDev but by the SSA environment and the SCA uses the signer's SCD linked by the SSA to the authenticated identity of the signer; it is not expected that such implementations would meet the requirements of sole control as it would be expected for an SSCD;

- Level 2: the signer authentication is enforced by the SCDev by a means that the signer uses for signing (the SAD or derivate thereof) in order to enable the use of the corresponding SCD; the signer authentication is aimed to achieve the same level of assurance of sole control as what would be achieved by a stand-alone SSCD.

The decision to use level 1 or 2 sole controls rests on the applicable legal requirements depending on the signature policy and legal requirements applicable to the type of documents being signed.

5.5 Batch Server Signing

In some EU Member States it is possible to sign a batch of documents, without requiring the signer to inspect and explicitly approve each document. This means that the signer has only to apply sole controls to the signing process for a batch rather than each individual document.

Other countries allow signing a batch where the signer does not need to explicitly approve each document, but gets an opportunity to inspect before signing, such as giving links to the documents in the batch.

Other countries may not allow the batch signing. In this case, it is to be ascertained if this prohibition blindly applies to any kind of advanced electronic signatures or solely to qualified ones.

As the legal applicability of batch signing depends on legal and application environment, the SSA should have configuration profiles to allow or disallow batch signing for AdES and QES.

5.6 SCD

5.6.1 General

Directive 1999/93/EC defines two main electronic signature types: an Advanced Electronic Signature and an Advanced Electronic Signature based on a Qualified Certificate (so called Qualified Electronic Signature). They have different implications as to where the SCD (usually called “private key”) is generated, kept and used.

AdES do not strictly require private keys to be generated and kept in hardware devices, while implementations of QES used in practice have this feature as a basic distinction.

5.6.2 SCD for AdES

To generate advanced electronic signatures and to guarantee high flexibility, the SCD (e.g. private keys) does not necessarily have to be created, stored and used inside cryptographic hardware (e.g. HSM or SSCD). The SCD could also be stored in a file.

When using files, specific external security measures should be implemented in addition to protecting the files themselves from tampering (deletion, modification); e.g. access should be controlled by means of password based encryption or by means of a secret sharing scheme.

Nevertheless this specification recommends that the SSA uses SCD inside a cryptographic hardware in order to produce AdES documents.

The sole control level of SCD for AdES can be either level 1 or 2.

5.6.3 SCD for QES

Wherever QES are used, one basic requirement is that the signer's SCD be used inside an SSCD. This makes suitable security measures easier to implement because the device itself vouches for key confidentiality and provides a reasonable confidence that it is used solely by authorized people.

Nevertheless, some organisational measures should be necessary, to bolster such basics as enforcing the access secret confidentiality and the signing device integrity.

The sole control level of SCD for QES shall be level 2.

5.6.4 Signer's authentication and SAD

As SCD is remote from the signer, the signer shall be authenticated by the SSA in order to use the signer's SCD to ensure sole control. In that case, the SSA is trusted to activate the SCD belonging to the authenticated signer.

In order to reach level 2 sole control and to ensure a comparable level of assurance as expected with an SSCD, multi-factor (at least 2) authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge) with the SCDev is required (details in 6.4).

To produce a QES, a level 2 sole control is needed between the signer and the SCDev.

5.6.5 Privileged system users

Remote access to the SSA is managed by privileged system users (security officer and/or system administrator, see SRG_M.1.2).

Privileged system users means a person (or persons) responsible for the practical and technical administration of an SSA. Individuals that are part of a group of privileged system users:

- are named persons,

- have physical access to the hardware implementing the server signing functions,

- have extensive privileges to administer the SSA through all relevant applications and interfaces.

It is assumed that only privileged system users have physical access to the hardware and can administer the SSA.

5.7 Functional model

5.7.1 General

This section presents a conceptual architecture of a TW4S in order to present its scopes, its components and its activation mechanisms.

It does not represent any physical architecture, which in practice will use for example, multiple servers and devices for load sharing or redundancy.

5.7.2 Scopes of requirements depending of sole control levels

A TW4S provides secure remote management of signatory's signature creation device and generation of electronic signatures by means of such a remotely managed device.

There are two scopes for the requirements:

- Level 1 includes the server system and the core components of the SSA:

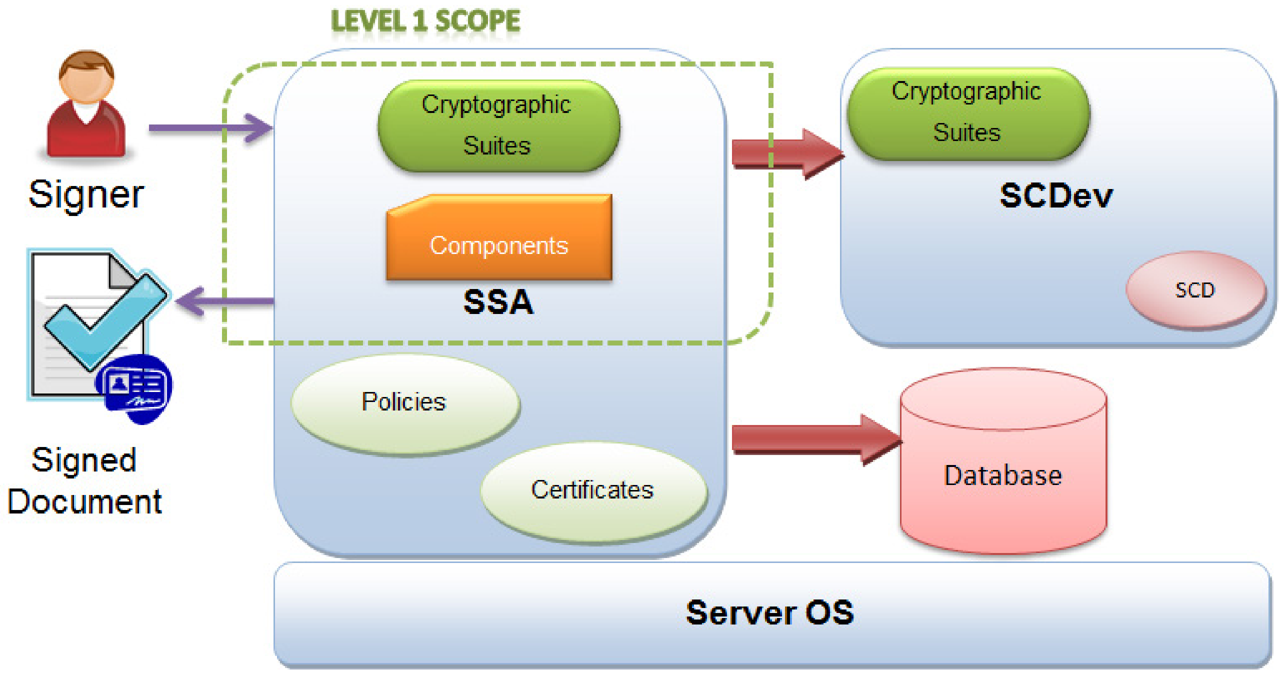

Figure 1 — Scope for level 1 sole control

— Level 2 also includes the SCDev in order to enhance the level of assurance of the sole control:

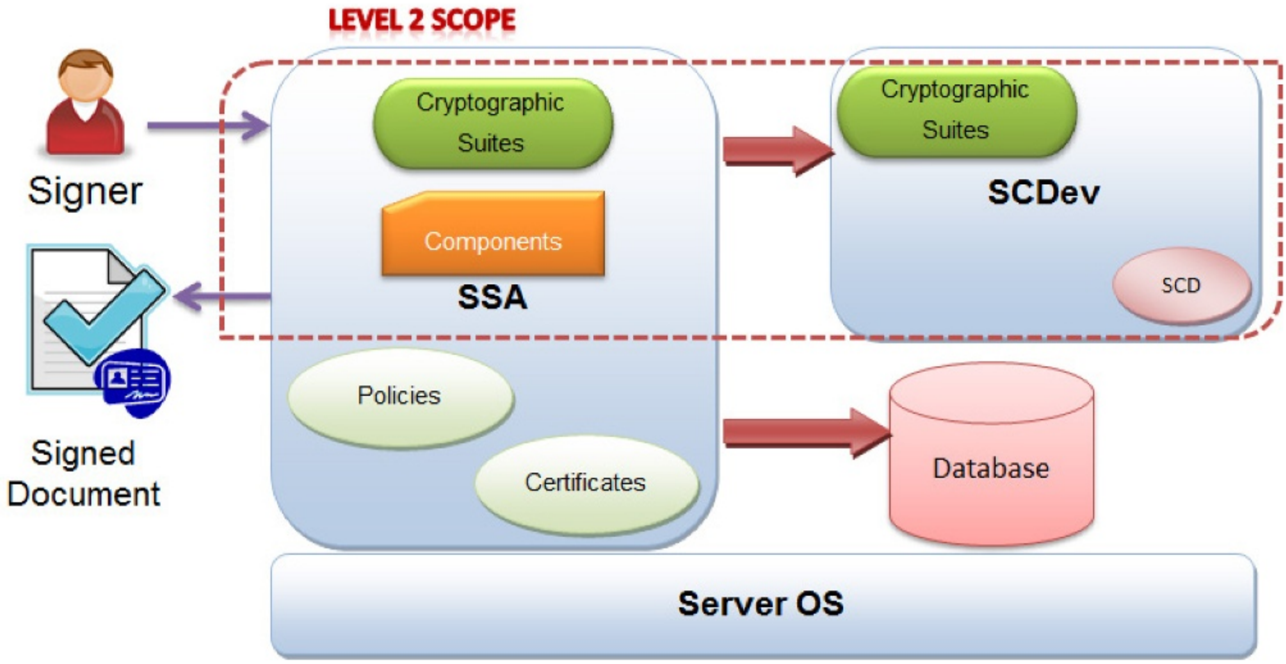

Figure 2 — Scope for level 2 sole control

5.7.3 SSA Core Components

The core parts of an SSA for which this document specifies requirements are the set of trusted components:

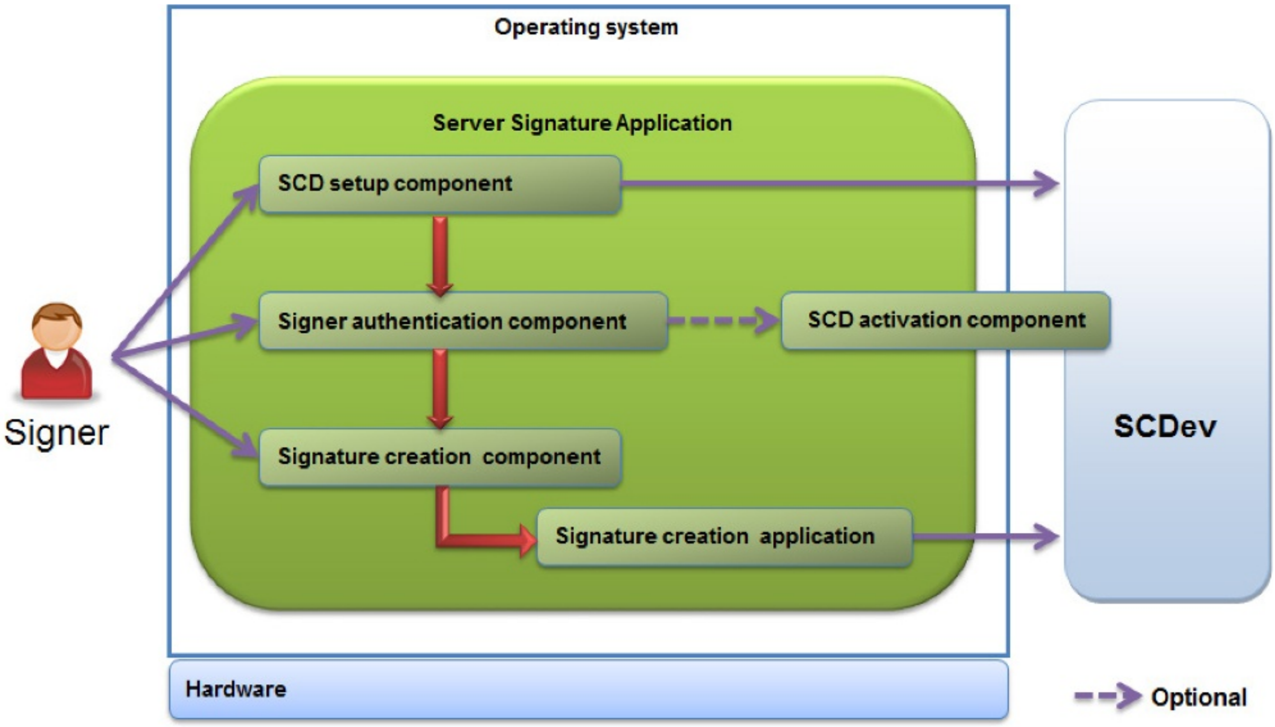
Operating system
Server Signature Application
SCD setup component
Signer authentication component
SCD activation component
Signature creation component
Signature creation application
Signer
SCDev
Hardware
Optional

Figure 3 —SSA Core Components

- SCD setup component – to set up signing keys within the signing system with corresponding SAD;
- Signer authentication component – to authenticate the signer and to identify the SCD to use. This service is responsible for the SCD of multiple signatories;
- Signature creation component – to interface the authenticated signer with the SSA in order to create the SDO. The signature creation application should be implemented according to CWA 14170.
- SCD activation component – to generate and validate SAD or derivative thereof, this component is also part of the SCDev. Optional for level 1 but mandatory to reach level 2 sole control.

5.7.4 SCD activation mechanisms

5.7.4.1 General

This section presents some examples of SCD activation mechanisms in order to create an electronic signature.

This is not exclusive. Any other architecture compliant with Clause 5 can be implemented.

The applicable requirements from Clause 5 depend on the chosen level of Sole Control:

Sole Control	6.2	6.3	6.4
Level 1	Yes	Yes	No
Level 2	Yes	Yes	Yes

TW4S typically use a set of signer's SCD within one or several SCDev.

The SCD can be securely stored outside the SCDev and loaded dynamically, but key management mechanisms are outside the scope of this document.

5.7.4.2 Activation with level 1 sole control

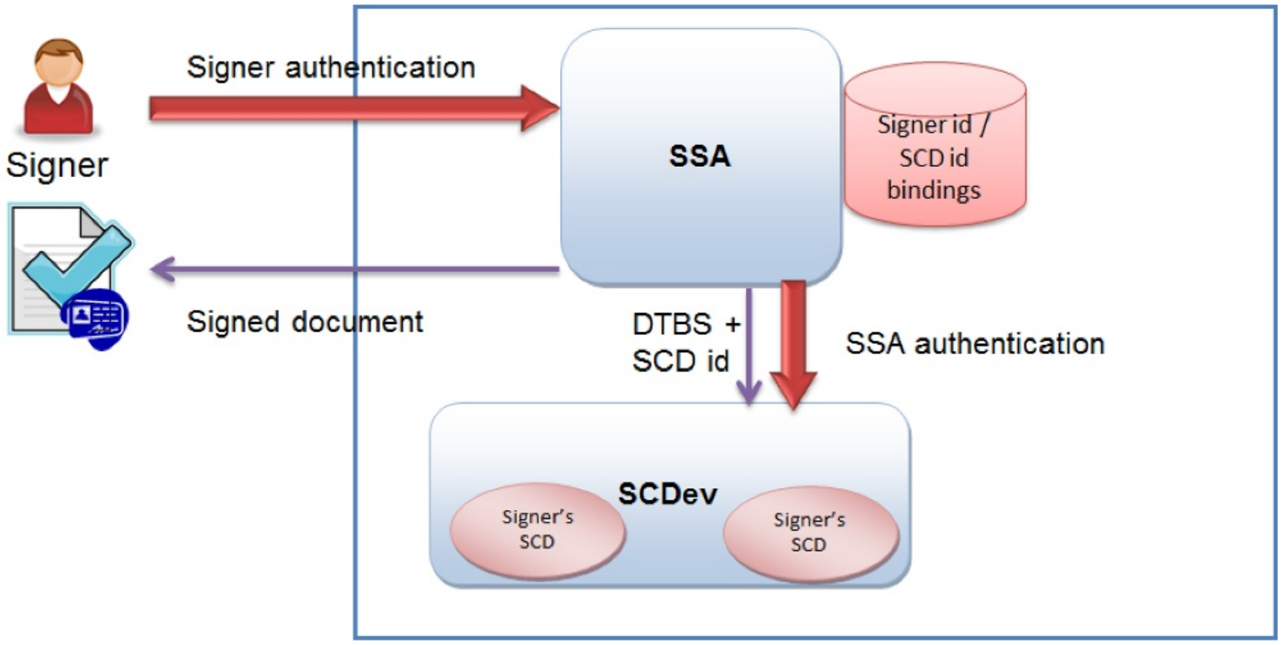

Figure 4 —SCD activation system with level 1 sole control

SCD confidentiality and integrity are ensured by the SCDev. The SCDev can be activated by the SSA. The activation can remain for a given period and/or set of documents to be signed.

The signer is authenticated by the SSA in a secure way. When the authentication succeeds, the corresponding SCD can be used within a certain timeframe. This allows the SSA to be used for bulk/batch signature purposes.

This architecture can be used to produce AdES bound to:

— a natural or legal person with a Public Key Certificate;

— a natural or legal person with a Qualified Certificate;

This architecture cannot be used to produce QES.

5.7.4.3 Activation with level 2 sole control

SCD confidentiality and integrity are ensured by the SCDev. The SCDev can be activated by the SSA with an SAD or derivate thereof provided by the signer. The activation can remain for a given period and/or set of documents to be signed.

The SAD can be generated or derived by a device held by the signer (e.g. OTP generator, smartphone app).

The SAD or derivate thereof is transmitted to the SCDev (possibly via the SSA) in a secure way. When the activation succeeds, the corresponding SCD can be used within a certain timeframe. This allows the SSA to be used for bulk/batch signature purposes.

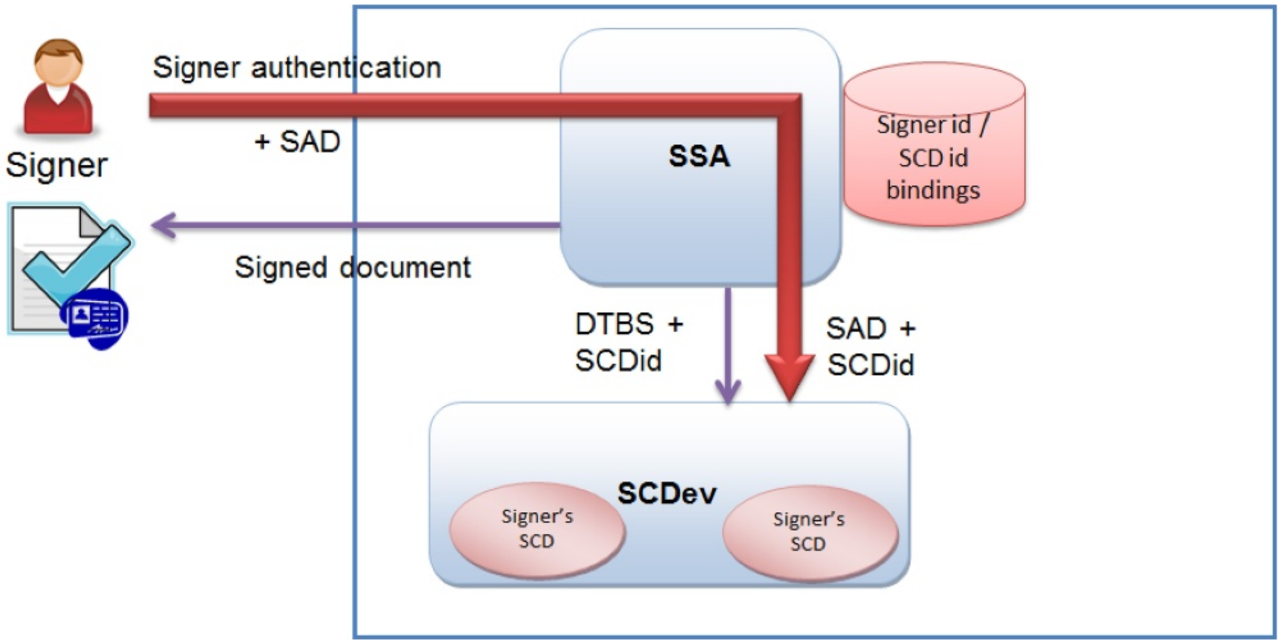

Figure 5 — SCD activation system with level 2 sole control

This architecture can be used to produce QES bound to a natural person with a Qualified Certificate or other form of electronic signature requiring higher assurance of control.

6 Security Requirements

6.1 General

This section describes all requirements applicable to a server signing system in order to be regarded as a TW4S.

All the security requirements of this TS are clearly stated and can be:

- mandatory (indicated by SHALL (NOT));
- optional (indicated by SHOULD (NOT) or (NOT) RECOMMENDED);
- permitted (MAY or MAY (NOT)).

In order to reach level 2 sole control, Subclause 6.4 includes some additional requirements.

6.2 General Security Requirements (SRG)

6.2.1 Management (SRG_M)

6.2.1.1 General

TW4S SHOULD be operated to recognized good practices and SHOULD have policy and procedures for a secure operation in place, based on ETSI EN 319 401.

6.2.1.2 Systems and Security Management (SRG_M.1)

A TSP needs to manage its security in order to operate an SGSP that is a TW4S.

SRG_M.1.1 TW4S SHALL support roles with different privileges.

SRG_M.1.2 As a minimum, TW4S SHALL maintain the following privileged roles:

Security Officers: having overall responsibility for administering the implementation of the security policies and practices.

System Administrators: are authorized to install, configure and maintain TW4S but with controlled access to security-related information.

System Operators: are responsible for operating TW4S on a day-to-day basis and are authorized to perform system backup and recovery.

System Auditors: are authorized to view archives and audit logs of TW4S for the purposes of auditing the operations of the system in line with security policy.

Security officers and system administrators are privileged system users.

System operators and system auditors have privileged roles but are not able to administer or configure the TW4S.

SRG_M.1.3 TW4S SHALL be able to associate users with these roles.

It is important that one user SHALL NOT be able to perform all the functions specified for TW4S. To prevent this, a single user SHOULD NOT be authorized to take on more than one of these roles.

SRG_M.1.4 TW4S SHALL be capable of ensuring that a user authorized to assume a Security Officer role is not authorized to assume a System Auditor role.

SRG_M.1.5 TW4S SHALL be capable of ensuring that a user authorized to assume a System Administrator role and/or a System Operator role is not authorized to assume a System Auditor role and/or a Security Officer role.

6.2.2 Systems and Operations (SRG_SO)

6.2.2.1 Operations Management (SRG_SO.1)

A TSP operating a TW4S needs to ensure that its operations management functions are adequately secure.

SRG_SO.1.1 A TW4S manufacturer SHALL ensure instructions are provided to allow the TW4S to be:

1) correctly and securely operated;

2) deployed in such a way that the risk of systems failure is minimized;

3) protected against viruses and malicious software to ensure the integrity of the systems and the information they process.

To meet the requirements of this TS the TW4S manufacturer SHALL provide system documentation covering the prerogatives of the four roles mentioned in SRG_M.1.2. It SHOULD include:

— Installation Guidance;

— Administration Guidance;

— User Guidance.

6.2.2.2 Time Synchronisation (SRG_SO.2)

The signature generation and the subsequent verification are time related, therefore there is a need to ensure that TW4S are suitably synchronized with a standard time source. This requirement is separate from any time-stamping requirements that may be set up by the TSP.

SRG_SO.2.1 TW4S manufacturers SHALL state the time accuracy of TW4S and how this is ensured.

It is RECOMMENDED that a trusted time source is used to ensure time accuracy.

6.2.3 Identification and Authentication (SRG_IA)

6.2.3.1 General

The Identification and Authentication functions restrict the access to and the use of TW4S to authorized persons only. This is applicable to all management components of the TSP. Identification and Authentication may be provided either by the underlying operating software or directly by the actual component itself.

6.2.3.2 User Authentication (SRG_IA.1)

SRG_IA.1.1 TW4S SHALL require each user to identify him/herself and be successfully authenticated before allowing any action on behalf of that user or role assumed by the user.

SRG_IA.1.2 Re-authentication SHALL be mandatory after log out.

SRG_IA.1.3 Combination of authentication data, where used, SHALL be unpredictable.

SRG_IA.1.4 Mechanisms SHALL be implemented to reduce the risk of an authenticated user session being taken over if the user's input device is left unattended, for example by terminating a user session after a given idle period.

6.2.3.3 Authentication Failure (SRG_IA.2)

SRG_IA.2.1 If the number of unsuccessful authentication attempts from the same user reaches the maximum number of allowed attempts, the TW4S SHALL prevent further user authentication attempts within a certain time frame.

6.2.4 System Access Control (SRG_SA)

6.2.4.1 General

System access control functions restrict use of the objects of TW4S to authorized persons only. This is not applicable to signer access control but to privileged user's access control on all sensitive objects of the TW4S (see SRC_SA for signer access control).

System access control may be provided either by the underlying operating software or directly by the actual component itself. Access rights to specific TW4S objects are determined by the owner of the object based on the identity of the subject attempting to access it and:

a) the access rights to the object granted to the subject or;

b) the privileges held by the subject.

6.2.4.2 Right Management (SRG_SA.1)

SRG_SA.1.1 TW4S SHALL provide the capability of controlling and limiting access for identified individuals to the system or user objects which they own or are responsible for.

SRG_SA.1.2 TW4S SHALL ensure they provide access control to sensitive residual information.

6.2.5 Key Management (SRG_KM)

6.2.5.1 General

A TW4S may use cryptographic keys to provide integrity, confidentiality and authentication functions within its own subsystems and in between subsystems. As such, the unauthorised use, disclosure, modification, or substitution of these keys would result in a loss of security in the TW4S. It is essential that throughout the key lifecycle these keys are securely managed.

Due to the different threats bearing upon the keys of TW4S, depending on where and how they are used, it is important to categorize keys with respect to their risk profile (i.e. sensitivity). For this specification, keys are separated into the following categories:

1) User Signing Keys (User SCD) - signature generation service key pair for producing AdES or QES;

2) Infrastructure Keys – keys used by the TW4S for processes such as key agreement, subsystem authentication, audit log signing, transmitted or stored data encryption, etc. Short term session keys are also categorised as Infrastructure keys;

3) Control Keys – keys used by personnel managing or using the TW4S and that are likely to use authentication, signing or confidentiality with these keys.

In terms of security requirements, User Signing Keys shall be considered as highly sensitive. Consequently, countermeasures for managing the underlying risk should be adapted in both number and effect. Infrastructure keys are also considered as highly sensitive but due to their distributed characteristic they are less sensitive in comparison to user signing keys. The least sensitive keys used by the TSP are considered to be those used by personnel for controlling TW4S as they are used by trusted individuals and have an even shorter lifespan. Session keys, used for single/short transactions are treated as sensitive information but with lower security requirements than the aforementioned categories.

Infrastructure and Control Keys may be either private or secret keys.

6.2.5.2 Keys Generation (SRG_KM.1)

SRG_KM.1.1 Private or secret keys (including User SCD, Infrastructure and Control Keys) SHOULD be generated and maintained in an SCDev.

It is recommended to use an SCDev that:

— meets requirements of the EN 419211 series;

— or meets the requirements identified in CWA 14167-2, CWA 14167-3 or CWA 14167-4;

— or is a trustworthy system which is evaluated at EAL 4 or higher in compliance with the ISO/IEC 15408 series, or at an equivalent security criterion;

— or meets the requirements identified in ISO/IEC 19790:2006, level 3 or higher.

NOTE Demonstrated conformance to FIPS PUB 140-2, level 3 is considered as a fulfilment of this requirement.

SRG_KM.1.2 The SCDev SHOULD support cryptographic algorithms and key lengths in compliance with the rules defined by the ETSI/TS 102 176 series.

Wherever confidentiality or integrity protection services are required (e.g. for backup of CSP-SCD), only cryptographic algorithms and algorithm parameters of equivalent or higher strength SHALL be used.

SRG_KM.1.3 Whenever the SCDev is not used, private or secret keys (including User SCD, Infrastructure and Control Keys) SHOULD be maintained protected to ensure the confidentiality and integrity of the keys.

6.2.5.3 Keys Storage, Backup and Recovery (SRG_KM.2)

SRG_KM.2.1 All private or secret keys (including User SCD, Infrastructure and Control Keys) SHALL be securely stored, i.e. never be stored in an unprotected state.

SRG_KM.2.2 If any private or secret keys (including User SCD, Infrastructure and Control Keys), is exported from that SCDev, it SHALL be protected to ensure its confidentiality and integrity to the same or higher security level as within the SCDev.

Wherever the private/secret key is protected by encryption, only cryptographic algorithms and algorithm parameters of equivalent or higher strength SHALL be used.

SRG_KM.2.3 TW4S SHALL ensure that backup, storage and restoration of private or secret key (including User SCD, Infrastructure and Control Keys) are only performed by authorized personnel. Master keys used to protect both user and working keys shall be backed up, stored and reloaded under at least dual control. Such master keys SHALL only be held outside the SCDev in protected form.

6.2.5.4 Key Usage (SRG_KM.3)

SRG_KM.3.1 Private or secret keys (including User SCD, Infrastructure and Control Keys) SHALL only be used for its intended purpose.

SRG_KM.3.2 Private or secret keys (including User SCD, Infrastructure and Control Keys) SHALL NOT be shared except as required to meet their purpose.

SRG_KM.3.3 Access controls SHALL be in place to protect the access and usage of the keys (including User SCD, Infrastructure and Control Keys).

6.2.5.5 Key Distribution (SRG_KM.4)

SRG_KM.4.1 Private or secret keys (including User SCD, Infrastructure and Control Keys) SHALL be transmitted securely.

SRG_KM.4.2 All the keys used to protect other private/secret keys during transmission SHALL be (at least) as strong as the keys transmitted.

6.2.5.6 Key Renewal/Update/Change (SRG_KM.6)

SRG_KM.6.1 Infrastructure and Control Keys SHOULD be changed on a regular basis, with a frequency based on risk assessment.

SRG_KM.6.2 If any of the key algorithms or length is considered to have become unsuitable, keys based on those algorithms SHALL be changed immediately.

SRG_KM.6.3 If any of the keys is compromised or suspected to be compromised, they should be changed immediately.

6.2.5.7 Key Archiving (SRG_KM.7)

SRG_KM.7.1 Private or Secret keys SHOULD NOT be archived.

6.2.6 Accounting and Auditing (SRG_AA)

6.2.6.1 Audit Data Generation (SRG_AA.1)

Each service has additional specific auditing requirements that shall be addressed in addition to these general requirements.

SRG_AA.1.1 As a minimum, the following events SHALL be logged:

- significant TW4S environmental, key management events;
- user signing events (e.g. successful signing with a Signer's SCD);

- start up and shut down of the audit data generation function;
- changes of the audit parameters.

User signing events SHALL include associate certificate subject names.

Additionally it is RECOMMENDED that all access attempts to TW4S be logged.

SRG_AA.1.2 The system SHALL specify what is done (i.e. actions taken) in case of failure of passing audit information to any external storage.

6.2.6.2 Guarantees of Audit Data Availability (SRG_AA.2)

SRG_AA.2.1 The system SHALL maintain audit data and ensure that measures are taken for all audit data to be stored.

SRG_AA.2.2 The audit function SHALL only append information.

SRG_AA.2.3 TW4S SHALL protect the stored audit records in the audit trail from unauthorized deletion.

6.2.6.3 Audit Data Parameters (SRG_AA.3)

SRG_AA.3.1 All audit records (including service specific audit logging) SHALL contain the following parameters:

- date and time of event;
- type of event;
- identity of the entity (e.g. user, administrator, process) responsible for the action;
- success or failure of the audited event.

6.2.6.4 Selectable Audit Review (SRG_AA.4)

SRG_AA.4.1 TW4S SHALL allow searching for events in the audit log based on the date of event, the type of event and/or the identity of the user.

SRG_AA.4.2 The audit records SHALL be in a format that can be processed and be presented in such a way that is suitable for the system auditors to interpret the information.

6.2.6.5 Restricted Audit Review (SRG_AA.5)

SRG_AA.5.1 TW4S SHALL by default deny all user read access to the audit records, except to users that have been granted explicit read access (e.g. those with System Auditor role).

6.2.6.6 Generation of Warning (SRG_AA.6)

SRG_AA.6.1 TW4S SHALL generate a warning notifying in a timely manner unusual events which may have impact on the ability of the signing server system to meet the security requirements identified in this document.

It is recommended that a mechanism that issues a warning whenever an unusual event is detected be implemented. The warning should trigger a notification to relevant administrator personnel.

A warning may also trigger further actions to react to possible attacks such as cutting off the path of potential attack.

Examples of unusual events related to user activities may be (but not limited to):

- User actions outside of standard usage hours.
- User actions executed with an abnormal speed (in order to detect non-human interventions.

— User actions skipping standard activities within defined processes.

— Duplicated user sessions.

6.2.6.7 Guarantees of Audit Data Integrity (SRG_AA.7)

SRG_AA.7.1 TW4S SHALL ensure the integrity of the audit data.

SRG_AA.7.2 TW4S SHALL provide a function to verify the integrity of the audit data.

6.2.6.8 Guarantees of Audit Timing (SRG_AA.8)

SRG_AA.8.1 It is RECOMMENDED that a trusted time source be used to ensure time accuracy of audited events.

6.2.7 Archiving (SRG_AR)

6.2.7.1 Archive Data Generation (SRG_AR.1)

SRG_AR.1.1 TW4S SHALL be capable of generating an archive on a media. The media should be appropriate for storage and subsequent processing, and be able to provide the necessary legal evidence in support of electronic signatures.

SRG_AR.1.2 All audit logs SHALL be archived.

SRG_AR.1.3 Each entry SHALL include the time at which the event occurred.

SRG_AR.1.4 The archive SHALL NOT include any sensitive security parameters, such as TW4S user passwords.

6.2.7.2 Integrity of Archived Data (SRG_AR.3)

SRG_AR.3.1 Unauthorized modifications of each entry in the archive SHALL be prevented. A mechanism to verify the integrity SHALL be in place to detect unauthorized modifications.

6.2.8 Backup and Recovery (SRG_BK)

6.2.8.1 General

This section only covers system information, subject information and all other data that is necessary to restore the system after a failure or disaster. It does NOT cover backup and recovery of keys; such security requirements are in section Key Management (SRG_KM, 6.2.5).

6.2.8.2 Integrity and Confidentiality of Backup Information (SRG_BK.1)

SRG_BK.1.1 Backups SHALL be protected against modification by a mechanism that allows verifying the integrity of the audit data.

SRG_BK.1.2 Sensitive security parameters and other confidential information SHALL be stored in a protected form in order to ensure confidentiality and integrity.

6.2.8.3 Recovery (SRG_BK.2)

SRG_BK.2.1 The system SHALL include a recovery function that is able to restore the state of the system from a backup.

SRG_BK.2.2 A user linked to a role with sufficient privileges SHALL be capable of invoking the recovery function on demand from a backup.

6.3 Core Components Security Requirements (SRC)

6.3.1 SCD Setup (SRC_DS) — Cryptographic key (SRC_DS.1)

SRC_DS.1.1 Only algorithms and algorithm parameters defined by the ETSI/TS 102 176 series for being used for signature creation by trustworthy systems SHOULD be used for SCD setup.

SRC_DS.1.2 TW4S SHALL identify signer's SCD with an SCDid.

SRC_DS.1.3 TW4S SHALL protect the integrity of the users' ID and SCDid bindings.

6.3.2 Signer Authentication (SRC_SA)

6.3.2.1 Signer authentication to SSA (SRC_SA.1)

SRC_SA.1.1 TW4S SHALL require each signer to be successfully identified and authenticated before allowing any actions that may impact the sole control of any SCD.

SRC_SA.1.2 Protocols in use SHALL prevent man-in-the-middle attacks, replay attacks, and more generally any form of attacks where a malicious user can use authentication credentials which do not belong to him/her.

SRC_SA.1.3 Access controls SHALL ensure that a user acting as a signer does not have access to sensitive system objects and any functions which gives the user control over another's signing key.

6.3.2.2 Authentication failure handling (SRC_SA.2)

SRC_SA.2.1 For a given user, TW4S SHALL detect when a defined number of consecutive unsuccessful authentication attempts occurs.

SRC_SA.2.2 For a given user, when the defined number of unsuccessful authentication attempts is met, the TW4S SHALL block this user's access for a reasonable amount of time or until the relevant action is performed by an operator with the appropriate role.

6.3.3 Signature Creation (SRC_SC)

6.3.3.1 Cryptographic operation (SRC_SC.1)

SRC_SC.1.1 Only algorithms and algorithm parameters defined by the ETSI/TS 102 176 series for being used for signature creation by trustworthy systems SHOULD be used for signature creation.

SRC_SC.1.2 The signature creation application SHOULD be implemented in compliance with functional requirements of CWA 14170.

NOTE The signature creation application does not need to be independently evaluated.

6.3.3.2 Access control (SRC_SC.2)

SRC_SC.2.1 The TW4S SHALL ensure that the DTBS provided by a user is only signed by the SCD belonging to this user.

6.4 Additional Security Requirements for Level 2 (SRA)

6.4.1 General

The following requirements are only applicable to TW4S implementing level 2 sole control. These requirements concern the SCDev or the SSA or both.

6.4.2 SCD Activation (SRA_DA)

6.4.2.1 General

The signer authentication is enforced by the SCDev by a means that the signer uses for signing (the SAD or derivate thereof) in order to enable the use of the corresponding SCD, multi-factors authentication (at least 2) is needed.

There are many ways to implement a multi-factor authentication. For example:

— multi-factor authentication between the signer and the SCDev using the SAD;

— multi-factor authentication between the signer and an authentication device that will derive and pass on an SAD to the SCDev;

— multi-factor authentication between the signer and the SSA, and then an SAD provided by the signer securely passed on to the signing device.

6.4.2.2 SCD Generation (SRA_DA.1)

SRA_DA.1.1 User's SCD SHALL be generated and maintained in an SCDev that:

— meets requirements of the EN 419211 series;

— or meets the requirements identified in CWA 14167-2, CWA 14167-3 or CWA 14167-4;

— or is a trustworthy system which is evaluated at EAL 4 or higher in compliance with the ISO/IEC 15408 series, or at an equivalent or higher security criterion;

— or meets the requirements identified in ISO/IEC 19790:2006, level 3 or higher.

NOTE Demonstrated conformance to FIPS PUB 140-2, level 3 is considered as fulfilment of this requirement.

SRA_DA.1.2 An SAD or deviate thereof SHALL be provided to the SCDev in order to generate a user’s SCD.

SRA_DA.1.3 The SAD or deviate thereof SHALL be linked to the user’s SCD generated.

6.4.2.3 SAD Generation (SRA_DA.2)

SRA_DA.2.1 The SAD MAY be represented by 1 or more authentication factors.

NOTE for 1-factor SAD, see also specific requirements for activation:SRA_DA.3.5

SRA_DA.2.2 For 1-factor SAD, the SAD SHALL be:

- chosen by the user and transmitted to the TW4S in a secure way based on multi-factor (at least 2) authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge) using a means under the sole control of the user,

- or -

- generated by the TW4S and transmitted to the user in a secure way (i.e. pin mailing, secure e-mail…).

SRA_DA.2.3 For 2+-factor SAD, the SAD factors SHALL be:

- created in a way that 2 (or more) factors will be under the sole control of the user;
- protected so that any keys held within devices are secure.

6.4.2.4 SCD Activation (SRA_DA.3)

SRA_DA.3.1 User's SCD SHALL be activated for a use in an SCDev only (e.g. SSCD or HSM).

SRA_DA.3.2 The TW4S SHALL require each user to present an SAD or deviate thereof to the SCDev in order to be authenticated before allowing any use of the user's SCD.

SRA_DA.3.3 The user's SAD or deviate thereof SHALL be passed on to the SCDev in a secure way.

SRA_DA.3.4 The SAD SHALL be protected against replay attack between users and the SCDev (e.g. with a nonce, timestamp or session token).

SRA_DA.3.5 If the SAD is represented by only 1 factor then the SAD SHALL be transmitted to the TW4S in a secure way based on a multi-factor (at least 2) authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge) using a means under the sole control of the user.

SRA_DA.3.6 System administrators SHALL NOT be able to activate User's SCD.

SRA_DA.3.7 The usage of a SCD MAY be limited (e.g. by time or numbers) before the user shall be required to provide a SAD representing at least one factor to continue signing.

SRA_DA.3.8 After SCD activation and signature creation, user's SAD SHALL NOT be stored anywhere by TW4S.

Bibliography

The following materials, though not specifically referenced in the body of the present document (or not publicly available), give supporting information.

[1] CWA 14167-1, *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures — Part 1: System Security Requirements*

[2] CWA 14170, *Security requirements for signature creation applications*

[3] CWA 14355, *Guidelines for the implementation of Secure Signature-Creation Devices*

[4] EN 14890-1, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic services*

[5] EN 14890-2, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 2: Additional Services*

[6] EN 419251-1, *Security requirements for device for authentication — Part 1: Protection profile for core functionality*

[7] ETSI/TS 102 176 (all parts), *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*

[8] ETSI/TS 102 853, *Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies*

[9] ETSI EN 319 401, *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures*

[10] ETSI EN 319 411-2, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates*

[11] ETSI EN 319 411-3, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates*

[12] ETSI/TS 101 733, *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*

[13] ETSI SR 001 604, *Rationalised Framework for Electronic Signature Standardisation*

[14] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[15] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[16] FIPS PUB 140-2, *Security requirements for cryptographic modules*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™