# SVENSK STANDARD
# SS-EN 419211-6:2014

Fastställd/Approved: 2014-10-12
Publicerad/Published: 2014-10-13
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 03.160; 35.040; 35.240.15

SWEDISH STANDARDS INSTITUTE

## Skyddsprofil för säker signaturanordning – Del 6: Anslutning av signaturanordning med nyckelimport och säker kommunikation till applikation för signaturgenerering

## Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application

# Standarder får världen att fungera

*SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.*

**Delta och påverka**
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

**Ta del av det färdiga arbetet**
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

**Utveckla din kompetens och lyckas bättre i ditt arbete**
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

**Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.**

# Standards make the world go round

*SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.*

**Take part and have influence**
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

**Get to know the finished work**
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

**Increase understanding and improve perception**
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

**If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00**

Europastandarden EN 419211-6:2014 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av EN 419211-6:2014.

The European Standard EN 419211-6:2014 has the status of a Swedish Standard. This document contains the official version of EN 419211-6:2014.



*Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.*

*Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.*

Denna standard är framtagen av kommittén för Teknik och stödsystem för personlig identifiering, SIS/TK 448.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN 419211-6

October 2014

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

# Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung

This European Standard was approved by CEN on 25 July 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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**

# Contents

Page

# Foreword

This document (EN 419211-6:2014) 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.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2015 and conflicting national standards shall be withdrawn at the latest by April 2015.

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 supersedes CWA 14169:2004.

In comparison with CWA 14169, the entire document has been revised. Refer to EN 419211-1:2014, Annex A for more details.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: 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

This series of European Standards specifies Common Criteria protection profiles for secure signature creation devices and is issued by the European Committee for Standardization (CEN) as an update of the Electronic Signatures (E-SIGN) CEN workshop agreement, CWA 14169:2004, Annex B and Annex C on the protection profile secure signature creation devices, "EAL 4+".

This series of European Standards consists of the following parts:

— *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 channel to certificate generation application*

— *Part 5: Extension for device with key generation and trusted channel to signature creation application*

— *Part 6: Extension for device with key import and trusted channel to signature creation application*

Preparation of this document as a protection profile (PP) follows the rules of ISO/IEC 15408.

# 1 Scope

This European Standard specifies a protection profile for a secure signature creation device that may import signing keys and communicate with the signature creation application in protected manner: secure signature creation device with key import and trusted communication with signature creation application (SSCD KI TCSCA).

# 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 419211-1:2014, *Protection profiles for secure signature creation device — Part 1: Overview*

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*[1)]

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

# 3 Conventions and terminology

## 3.1 Conventions

This document is drafted in accordance with the CEN/CENELEC directive and content and structure of this document follow the rules and conventions laid out in ISO/IEC 15408.

Normative aspects of content in this European Standard are specified according to the Common Criteria rules and not specifically identified by the verbs “*shall*” or “*must*”.

## 3.2 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in EN 419211-1 apply.

---

1) ISO/IEC 15408-1, ISO/IEC 15408-2 and ISO/IEC 15408-3 respectively correspond to *Common Criteria for Information Technology Security Evaluation*, Parts 1, 2 and 3.

# 4 PP introduction

## 4.1 PP reference

| | |
|---|---|
| Title: | Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application |
| Version: | 1.0.4 |
| Author: | CEN / CENELEC (TC224/WG17) |
| Publication date: | 2013-04-03 |
| Registration: | BSI-CC-PP-0076 |
| CC version: | 3.1 Revision 4 |
| Editor: | Arnold Abromeit, TÜV Informationstechnik GmbH |
| General status: | final |
| Keywords: | secure signature creation device, electronic signature, digital signature, key import, trusted communication with signature creation application |

## 4.2 PP overview

This Protection Profile is established by CEN as a European Standard for products to create electronic signatures. It fulfils requirements of Directive 1999/93/EC[2)] of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

In accordance with Article 9 of this European Directive this standard can be indicated by the European Commission in the Official Journal of the European Communities as a generally recognized standard for electronic signature products.

This protection profile defines security functional requirements and security assurance requirements that comply with those defined in Annex III of the Directive for a secure signature creation device (SSCD). This secure signature creation device is the target of evaluation (TOE) for this protection profile.

European Union Member States may presume that there is compliance with the requirements laid down in Annex III of the Directive when an electronic signature product is evaluated to a Security Target (ST) that is compliant with this Protection Profile (PP).

This Protection Profile about secure signature creation device with key import and trusted communication with signature creation application (PP SSCD KI TCSCA) includes the security requirements for SSCD with key import importing signature creation data (SCD) and creating digital signature to be used for (qualified or advanced) electronic signatures as described in the core PP [3]. Additionally, the TOE of this PP supports a trusted communication with a signature creation application for protection of authentication data and data to be signed. These security features allow using the TOE in a more complex operational environment. It conforms to the core PP SSCD KI [3]. The implication of this conformance claim is explained in 5.3 hereinafter.

---

[2)] This European Directive is referred to in this PP as “the Directive”.

The assurance level for this PP is EAL4 augmented with AVA_VAN.5.

## 4.3 TOE overview

### 4.3.1 Operation of the TOE

This section presents a functional overview of the TOE in its distinct operational environments:

— The preparation environment, where it interacts with a certification service provider through a SCD/SVD generation application to import the signature creation data (SCD) and a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the signature creation data (SCD) the certification service provider has generated. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference-authentication data (RAD).

— The signing environment where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting electronic signature[3)]. The TOE and the SCA communicate through a trusted channel to ensure the integrity of the DTBS respective DTBS/R.

— The management environments where it interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE. Figure 5 in EN 419211-1:2014 illustrates the operational environment.

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case, the TOE provides a function to identify each SCD and the signature creation application (SCA) can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The electronic signature created with the TOE is a *qualified electronic signature* as defined in **the Directive** if the certificate for the SVD is a qualified certificate (Annex I). Determining the state of the certificate as qualified is beyond the scope of this standard.

The SCA is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash values required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash value over the input as needed by the kind of input and the used cryptographic algorithm. The TOE and the SCA communicate through a trusted channel in order to protect the integrity of the DTBS/R.

The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a password, e.g. PIN, a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD. The TOE may provide a user interface to directly receive verification authentication data (VAD) from the user, alternatively, the TOE receive the VAD from the signature creation application. If the signature creation application handles requesting obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

---

[3)] At a pure functional level the SSCD creates an electronic signature; for an implementation of the SSCD, in that meeting the requirements of this PP and with the key certificate generated as specified in the Directive, Annex I, the result of the signing process can be used as to create a qualified electronic signature.