SVENSK STANDARD
SS-EN 419211-2:2013

Fastställd/Approved: 2013-08-16
Publicerad/Published: 2013-08-20
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 03.160; 35.040; 35.100.05; 35.240.15

Skyddsprofil för säker signaturanordning – Del 2: Signaturanordning med nyckelgenerering

Protection profiles for secure signature creation device – Part 2: Device with key generation

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 419211-2:2013 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av EN 419211-2:2013.

The European Standard EN 419211-2:2013 has the status of a Swedish Standard. This document contains the official version of EN 419211-2:2013.

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 419211-2

July 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 2: Device with key generation

Profils de protection des dispositifs sécurisés de création de signature - Partie 2: Dispositif avec génération de clé

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 2: Geräte mit Schlüsselerzeugung

This European Standard was approved by CEN on 8 May 2013.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 419211-2:2013: E

Contents

Page

Foreword

This document (EN 419211-2:2013) 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 January 2014, and conflicting national standards shall be withdrawn at the latest by January 2014.

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.

This document was submitted to the Enquiry procedure under reference prEN 14169-2.

The EN 419211 series 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.

Correspondence and comments regarding this protection profile about secure signature creation device with key generation (PP SSCD KG) can be referred to the CEN/TC 224 Secretary.

According to the CEN-CENELEC Internal Regulations, the national standards organisations 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.

1 Scope

This European Standard specifies a protection profile for a secure signature creation device that may generate signing keys internally: secure signature creation device with key generation (SSCD KG).

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.

prEN 419211-1, *Protection profiles for secure signature creation device — Part 1: Overview*[1)]

ISO/IEC 15408-1:2009[2)] *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

ISO/IEC 15408-3[2)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

3 Conventions and terminology

3.1 Conventions

The content and structure of this document follow the rules and conventions laid out in ISO/IEC 15408-1.

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

3.2 Terms and definitions

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

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 2: Device with key generation
Version:	2.0.1.
Author:	CEN (TC224/WG17)
Publication date:	2013
Registration:	BSI-CC-PP-0059-2009-MA-01
CC version:	3.1 Revision 3

1) To be published. This document was submitted to the Enquiry procedure under reference prEN 14169-1.

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

Editor:	Arnold Abromeit, TÜV Informationstechnik GmbH
General status:	final draft
Keywords:	secure signature creation device, electronic signature, digital signature

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[3)] 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 Union as a generally recognised 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 describes core security requirements for a secure device that can generate a signing key[4)] (signature creation data, SCD) and operates to create electronic signatures with the generated key. A device evaluated according to this protection profile and used in the specified environments can be trusted to create any type of digital signature. As such, this PP can be used for any device that has been configured to create a digital signature. Specifically this PP allows the qualification of a product as a device for creating an advanced electronic signature as defined in the directive.

After an SSCD has generated a signing key, the corresponding public key (signature verification data, SVD) has to be provided as input to a certificate generation application (CGA). Security requirements for export of the SVD are described in a protection profile that extends this PP (prEN 419211-4, *Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application)*[5)] and not in this document.

When operated in a secure environment for signature creation a signer may use an SSCD that fulfils only these core security requirements to create an advanced electronic signature.[6)] Security requirements for an SSCD used in environments where the communication between SSCD and the signature creation application (SCA) is assumed to be protected by the SSCD and the SCA are described in a separate protection profile that extend this PP (prEN 419211-5, *Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application*)[7)] and not in this document.

These extended Protection Profiles claim conformance to this PP.

---

3) This European Directive is referred to in this PP as “the directive”.

4) An SSCD that can generate its own SCD/SVD was defined in the previous version of this PP (CWA 14169) as a Type 3 SSCD. The notion of types does not exist anymore in this series of ENs. In order to refer to the same functionality, a reference to EN 419211-2 (i.e. Part 2) should be used.

5) This document was submitted to the Enquiry procedure under reference prEN 14169-4.

6) An advanced electronic signature is defined as an electronic signature created by an SSCD using a public key with a public key certificate created as specified in the directive.

7) This document was submitted to the Enquiry procedure under reference prEN 14169-5.

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 certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the SCD the TOE has generated. The initialisation environment interacts further with the TOE to personalise 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 digital signature[8)].

— 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 2 in Part 1 of this standard 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 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 digital signature created by the TOE may be used to create an advanced electronic signature as defined in Article 5.1 of the directive. Determining the state of the certificate as qualified is beyond the scope of this standard.

The signature creation application is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorised 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 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, is requesting or obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

A certification service provider and a SSCD-provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions may include:

---

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

— initialising the RAD;

— generating a key pair;

— storing personal information of the legitimate user.

A typical example of an SSCD is a smart card. In this case, a smart card terminal may be deployed that provides the required secure environment to handle a request for signatory authorisation. A signature can be obtained on a document prepared by a signature creation application component running on a personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorisation PIN, initiates the digital signature creation function of the smart card through the terminal.

4.3.2 Target of evaluation

The TOE is a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole lifecycle as to be used in a signature creation process solely by its signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature.

The TOE provides the following functions:

a) to generate signature creation data (SCD) and the correspondent signature-verification data (SVD);

b) to export the SVD for certification;

c) to, optionally, receive and store certificate info;

d) to switch the TOE from a non-operational state to an operational state; and

e) if in an operational state, to create digital signatures for data with the following steps:

   1) select an SCD if multiple are present in the SSCD;

   2) authenticate the signatory and determine its intent to sign;

   3) receive data to be signed or a unique representation thereof (DTBS/R);

   4) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

The TOE may implement its function for digital signature creation to conform to the specifications in ETSI TS 101 733 (CAdES) [3], ETSI TS 101 903 (XAdES) [4] and ETSI TS 101 903 (PAdES) [5].

The TOE is prepared for the signatory's use by:

a) generating at least one SCD/SVD pair; and

b) personalising for the signatory by storing in the TOE:

   1) the signatory’s reference authentication data (RAD);

   2) optionally, certificate info for at least one SCD in the TOE.

After preparation, the SCD shall be in a non-operational state. Upon receiving a TOE, the signatory shall verify its non-operational state and change the SCD state to operational.