SVENSK STANDARD
SS-EN 419211-1:2014

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

Skyddsprofil för säker signaturanordning – Del 1: Översikt

Protection profiles for secure signature creation device – Part 1: Overview

Provläsningsexemplar / Preview

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

Provläsningsexemplar / Preview

Europastandarden EN 419211-1:2014 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av EN 419211-1:2014.

The European Standard EN 419211-1:2014 has the status of a Swedish Standard. This document contains the official version of EN 419211-1:2014.

© Copyright/Upphovsrätten till denna produkt tillhör SIS, Swedish Standards Institute, Stockholm, Sverige. Användningen av denna produkt regleras av slutanvändarlicensen som återfinns i denna produkt, se standardens sista sidor.

© Copyright SIS, Swedish Standards Institute, Stockholm, Sweden. All rights reserved. The use of this product is governed by the end-user licence for this product. You will find the licence in the end of this document.

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.

Provläsningsexemplar / Preview

Provläsningsexemplar / Preview

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-1

October 2014

ICS 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 1: Overview

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 1: Présentation générale

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 1: Überblick

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

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

Ref. No. EN 419211-1:2014 E

Provläsningsexemplar / Preview

Contents

Page

Provläsningsexemplar / Preview

Foreword

This document (EN 419211-1:2014) 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.

Significant changes between this edition and CWA 14169:2004 can be found in Annex A.

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.

Provläsningsexemplar / Preview

Introduction

This series of European Standards specifies 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 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 communication with certificate generation application*

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

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

Preparation of the documents in this series of European Standards as protection profiles follows the rules of the Common Criteria version 3.1 ([2], [3] and [4]).

Provläsningsexemplar / Preview

1 Scope

This European Standard:

— specifies terms used in specifying protection profiles for secure signature creation devices,

— specifies functional and operational requirements for secure signature creation devices,

— describes the targets of evaluation for these protection profiles.

2 Normative references

Not applicable.

3 Terminology

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

3.1 Legislative references

This European Standard reflects the requirement of a European Directive in the technical terms of a protection profile. The following terms are used in the text to reference this Directive:

3.1.1
the Directive
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on "*a Community framework for electronic signatures"* [1]

Note 1 to entry: References in this document to a specific article and paragraph of Directive 1999/93/EC are of the form "(**the Directive:** n.m)".

3.1.2
annex
one of the annexes, Annex I, Annex II or Annex III of **the Directive**

3.2 Technical terms

3.2.1
administrator
user who performs TOE initialization, TOE personalization, or other TOE administrative functions

3.2.2
advanced electronic signature
digital signature which meets specific requirements in **the Directive: 2.2**

Note 1 to entry: According to **the Directive** a digital signature qualifies as an advanced electronic signature if it:

— is uniquely linked to the signatory;

— is capable of identifying the signatory;

— is created using means that the signatory can maintain under their sole control; and

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

Provläsningsexemplar / Preview

3.2.3
authentication data
information used to verify the claimed identity of a user

3.2.4
certificate
digital signature used as electronic attestation binding signature verification data to a person confirming the identity of that person as legitimate signer (**the directive: 2.9**)

3.2.5
certificate info
information associated with an SCD/SVD pair that may be stored in a secure signature creation device

Note 1 to entry: Certificate info may include:

— a signer's public key certificate, or

— one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values, or

— a public key certificate as defined in X.509.

Note 2 to entry: Certificate info may contain information to allow the user to distinguish between several certificates.

3.2.6
certificate generation application
CGA
collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate

3.2.7
certification service provider
CSP
entity that issues certificates or provides other services related to electronic signatures (**the Directive: 2.11**)

3.2.8
data to be signed
DTBS
all of the electronic data to be signed including a user message and signature attributes

3.2.9
data to be signed or its unique representation
DTBS/R
data received by a secure signature creation device as input in a single signature creation operation

Note 1 to entry: Examples of DTBS/R are:

— a hash value of the data to be signed (DTBS), or

— an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or

— the DTBS.

3.2.10
legitimate user
user of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory

Provläsningsexemplar / Preview

3.2.11
qualified certificate
public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in **Annex II** (**the Directive: 2.10**)

3.2.12
qualified electronic signature
an advanced electronic signature which is based on a qualified certificate and which is created by an SSCD

3.2.13
reference authentication data
RAD
data persistently stored by the TOE for authentication of the signatory

3.2.14
secure signature creation device
SSCD
a signature-creation device which meets the requirements laid down in Annex III

Note 1 to entry: An SSCD may be evaluated according to the security target conforming to a PP as defined in the series of European Standards.

3.2.15
signatory
a person who holds (and is a legitimate user) of an SSCD and acts either on their own behalf or on behalf of the natural or legal person or entity they represent

3.2.16
signature creation application
SCA
application complementing an SSCD with a user interface with the purpose to create an electronic signature

3.2.17
signature creation data
SCD
unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

Note 1 to entry: For the PPs of this standard the SCD is held in the SSCD.

3.2.18
signature creation system
SCS
complete system that creates an electronic signature consisting of an SCA and an SSCD

3.2.19
signature verification data
SVD
data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature

3.2.20
SSCD-provisioning service
service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD