BS EN 419211-5:2013

BSI Standards Publication

Protection profiles for secure signature creation device

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

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS EN 419211-5:2013

National foreword

This British Standard is the UK implementation of EN 419211-5:2013.

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.

© The British Standards Institution 2013. Published by BSI Standards Limited 2013

ISBN 978 0 580 71699 7

ICS 03.160; 35.040; 35.240.15

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2013.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN 419211-5:2013

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-5

December 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application

Profils de protection pour dispositif sécurisé de création de signature - Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature

Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung

This European Standard was approved by CEN on 12 October 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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2013 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 419211-5:2013 E

Documents
Document Sharing Hub

Full document details: BS EN 419211-5:2013

Contents

Page

Foreword ... 3
Introduction ... 4
1 Scope ... 5
2 Normative references ... 5
3 Conventions and terminology ... 5
3.1 Conventions ... 5
3.2 Terms and definitions ... 5
4 PP introduction ... 5
4.1 PP reference ... 5
4.2 PP overview ... 6
4.3 TOE overview ... 6
5 Conformance claims ... 8
5.1 CC conformance claim ... 8
5.2 PP claim, Package claim ... 8
5.3 Conformance rationale ... 8
5.4 Conformance statement ... 9
6 Security problem definition ... 9
6.1 Assets, users and threat agents ... 9
6.2 Threats ... 10
6.3 Organizational security policies ... 10
6.4 Assumptions ... 10
7 Security objectives ... 10
7.1 Security objectives for the TOE ... 10
7.2 Security objectives for the operational environment ... 11
7.3 Security objectives rationale ... 12
8 Extended components definition ... 14
9 Security requirements ... 14
9.1 Security functional requirements ... 14
9.2 Security assurance requirements ... 18
9.3 Security requirements rationale ... 19
Bibliography ... 24

Documents
Document Sharing Hub

Full document details: BS EN 419211-5:2013

Foreword

This document (EN 419211-5:2013) 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 June 2014, and conflicting national standards shall be withdrawn at the latest by June 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 series of European Standards, *Protection profiles for secure signature creation device* 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*

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.

Documents
Document Sharing Hub

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, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2004, Annex B and Annex C on the protection profile secure signature creation devices, “EAL 4+”.

Preparation of this document as a protection profile (PP) follows the rules of the Common Criteria version 3.1 [2], [3] and [4].

Documents
Document Sharing Hub

Full document details: BS EN 419211-5:2013

1 Scope

This European Standard specifies a protection profile for a secure signature creation device that may generate signing keys internally and communicate with the signature creation application in protected manner: secure signature creation device with key generation and trusted communication with signature creation application (SSCD KG 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.

prEN 419211-1:2011, *Protection profiles for secure signature creation device — Part 1: Overview*[1)]

3 Conventions and terminology

3.1 Conventions

This document is drafted in accordance with the CEN-CENELEC Internal Regulations Part 3 and content and structure of this document follow the rules and conventions laid out in Common Criteria 3.1.

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 prEN 419211-1:2011 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application
Version:	1.0.1
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	2012–11–14
Registration:	BSI-CC-PP-0072
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 generation, trusted communication with signature creation application

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

Documents
Document Sharing Hub
Full document details: BS EN 419211-5:2013

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[2)] 1999/93/EC 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 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 generation and trusted communication with signature creation application (PP SSCD KG TCSCA) includes the security requirements for SSCD with key generation generating signature creation data (SCD) and creating digital signature to be used for (qualified or advanced) electronic signatures as described in the core PP [5]. 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 KG [5]. The implication of this conformance claim is explained in 5.3 hereinafter.

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 subclause 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 signature creation data (SCD) the TOE 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.

---

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

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.

AVA Documents
Document Sharing Hub

Full document details: BS EN 419211-5:2013

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE. Figure 5 in prEN 419211-1:2011 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.

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:

— initializing 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 authorization. A signature can be obtained on a document prepared by a signature creation application component running on personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN initiates the electronic 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);

Documents
Document Sharing Hub

Full document details: BS EN 419211-5:2013