



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD
Sekcia informačnej bezpečnosti a elektronického podpisu
Budatínska č. 30, 850 07 Bratislava 57

METODIKA AUDITU

SCA a SVS pre ZEP

Bratislava 17. mája 2005.

Kontakty pre získanie informácií

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Sekcia informačnej bezpečnosti a elektronického podpisu

Budatínska č. 30, 850 07 Bratislava 57

<http://www.nbusr.sk/sep/default.html>

e-mail: sep@nbusr.sk

Metodika auditu SCA a SVS pre ZEP

Dokument vypracoval:

Július Šiška, PhD. – KPMG

Tento dokument upravuje procesy auditu SW aplikácií pri vytváraní a overovaní zaručeného elektronického podpisu podľa zákona 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov.

Zaručený elektronický podpis môže byť vyhotovovaný a overovaný len v bezpečnom prostredí, v tzv. „Systéme vyhotovovania a overovania podpisu“ (SCVS – Signature Creation & Verification System), ktorý v sebe zahŕňa certifikovaný, bezpečný HW produkt na vyhotovovanie zaručeného elektronického podpisu (SSCD) a certifikovanú SW aplikáciu (SCVA) na plnenie podporných funkcií pre vyhotovovanie a overovanie zaručeného elektronického podpisu.

Cieľom dokumentu je zaručiť jednotný a opakovateľný postup posudzovania SW aplikácií pri vytváraní a overovaní zaručeného elektronického podpisu.

Dokument je napísaný v anglickom jazyku, aby nedošlo k nepresnostiam pri preklade odborných termínov z existujúcich štandardov CWA 14170, CWA 14171, CWA 14172-4. Anglický názov metodiky auditu SCVA a SVS pre ZEP je Signature Creation Application (SCA) and Signature Verification Systems Audit Methodology, Version 3. Takýto názov je uvádzaný aj na web stránkach NBÚ.

**Signature Creation Application (SCA) and Signature
Verification Systems Audit Methodology
Version 3**

1	Foreword	4
2	Audit methodology	4
2.1	Scope.....	4
2.2	Certification process	5
2.2.1	Accreditation Body	5
2.2.2	Certification Body.....	5
2.2.3	Certificate issuer	5
2.2.4	Assessor	5
2.2.5	The Manufacturer.....	5
2.2.6	Certification steps	6
2.3	Level of assurance.....	7
2.4	Request for audit	7
2.5	Request for certification.....	7
2.6	Request for re-certification	7
2.7	Accreditation of Assessors.....	7
2.8	The Manufacturer's declaration of conformity.....	7
2.9	Audit	8
2.9.1	Audit recurrence.....	8
2.9.2	Audit compliance statement.....	8
2.10	Decision to certify.....	9
2.11	Suspension, withdrawal or cancellation of certification or compliance statement 9	
2.12	Contents of certificate of conformity	10
2.13	Confidentiality	10
2.14	Appeal	10
3	Requirements for Assessors.....	11
3.1	Audit team competence.....	11
3.2	Individual auditors competence	11
3.3	Cryptographic team.....	13
3.4	Use of technical experts	13
4	Requirements for the Manufacturer, SCA and SVS	13
4.1	SCA and SCS documentation	14
4.2	SVS documentation	14
4.3	SCDev documentation	15
4.4	Software development documentation.....	15
5	Methodology management.....	16
6	Registers of accredited Assessors, issued certificates.....	16
7	Audit content.....	17
7.1	Signature Creation Systems components.....	17
7.2	Signature Verification Systems components	17
7.3	Legislative requirements	18
7.4	Software development maturity models	18
8	Vocabulary	19
9	References.....	19

1 Foreword

This document defines methodology for certification of applications for creation and/or verification of electronic signatures. The described methodology is based on following existing standards:

- CWA 14170 [1]
- CWA 14171 [2]
- CWA 14172-4 [3].

The main purpose of the certification performed using this methodology is to provide assurance argument that evaluated applications for creation and/or verification of electronic signatures meet the EU 1999/93/EC Directive and local legislation requirements for electronic signatures. As it is not possible to cover all possible requirements laid by local legislatives in various countries, some requirements stated in this document may be insufficient or obsolete in some countries.

Terminology used throughout this document is consistent with terminology introduced in CWA 14170. Moreover, acronym SVS will denote signature verification system¹. Hereinafter the term “the Methodology” will be used to refer to this document: Signature Creation Application (SCA) and Signature Verification System Audit Methodology.

2 Audit methodology

This chapter describes the general procedures that must be followed by Assessors, Manufacturer and Certification Bodies evaluating and certifying SCA and/or SVS. Definitions of specific terms used in this chapter:

- *Nonconformity*: non-fulfilment of a specified requirement. Application does not provide any control to thwart a threat underlying the requirement. Application with existing nonconformity can not pass process of accreditation. Extremely significant nonconformities may result in an immediate stop of audit process with negative result of audit;
- *Deficiency*: imperfection or weakness in fulfilling a specified requirement. Deficiency means only minor deviation from requirement, which is in nature fulfilled. Large amount of deficiencies can also lead to negative result of audit.

The term “*must*” is used to denote absolute requirements laid by this Methodology.

2.1 Scope

This document specifies necessary steps needed to be performed and evaluated to gain sufficient assurance about the security of SCA and signature verification system. The scope of this certification methodology is as follows:

¹ This methodology deals with signature verification application, though CWA 14171 uses terminology signature verification system. To be consistent with CWA 14171, SVS acronym will be used throughout the methodology.

- Assessment of SCA;
- Assessment of communication between SCA and SCDev;
- Assessment of SVS.

This methodology is intended to be independent of used technologies, communication protocols and algorithms.

Certification described in this document does not cover:

- Assessment of the SCDev;
- Assessment of the SCS and instances in operation;
- Certification of Manufacturer for its software development quality.

Technical specifications CWA 14170 and CWA 14171 also state requirements on operation of SCA and/or SVS in public systems besides requirements laid directly on applications SCA and SVS. This methodology does not expect the SCA and/or SVS instances operation assessment, so the Methodology does not address this issue. The Methodology assesses only whether the Manufacturer sets security requirements for operations in provided documentation. If the SCA (SVS) is not operated under full signer control then only operator's conformity statement with the Manufacturer's operational requirements is required.

2.2 Certification process

Parties participating in process of certification are presented in Figure 1 Certification parties for the SCA.

2.2.1 Accreditation Body

Accreditation Body accredits Assessors fulfilling requirements for Assessors laid by this Methodology.

2.2.2 Certification Body

Certification Body issues guidance on fulfilling requirements laid by local legislative. Certification Body issues localized versions of forms required for certification of SCA and/or SVS and approves form of certification process.

2.2.3 Certificate issuer

Upon positive compliance statement of the Assessor, Certification issuer issues certificate for the SCA and/or SVS.

2.2.4 Assessor

Assessor – performs certification audit and works out final compliance statement on base of which is issued or not issued certificate by the Certification Body.

2.2.5 The Manufacturer

The Manufacturer develops SCA and/or SVS and all necessary documentation.

2.2.6 Certification steps

Step 1:

- Manufacturer develops SCA and/or SVS.
- Manufacturer submits request for certification to the Certification Body.
- Manufacturer provides the Certification Body with signature policy and format of electronic signature for approval.

Step 2:

- Manufacturer contracts an accredited Assessor to perform certification audit against this certification scheme.
- Assessor performs audit.
- After the signature policy and signature format are approved by the Certification Body the Assessor prepares final compliance statement.

Step 3:

- Manufacturer provides the Certification Body with the Assessor's compliance statement.

Step 4:

- Certification Body verifies whether Assessor meets requirements for Assessors laid in this document.
- Certification Body grants Approval based on Assessor's compliance statement and issues Certificate.

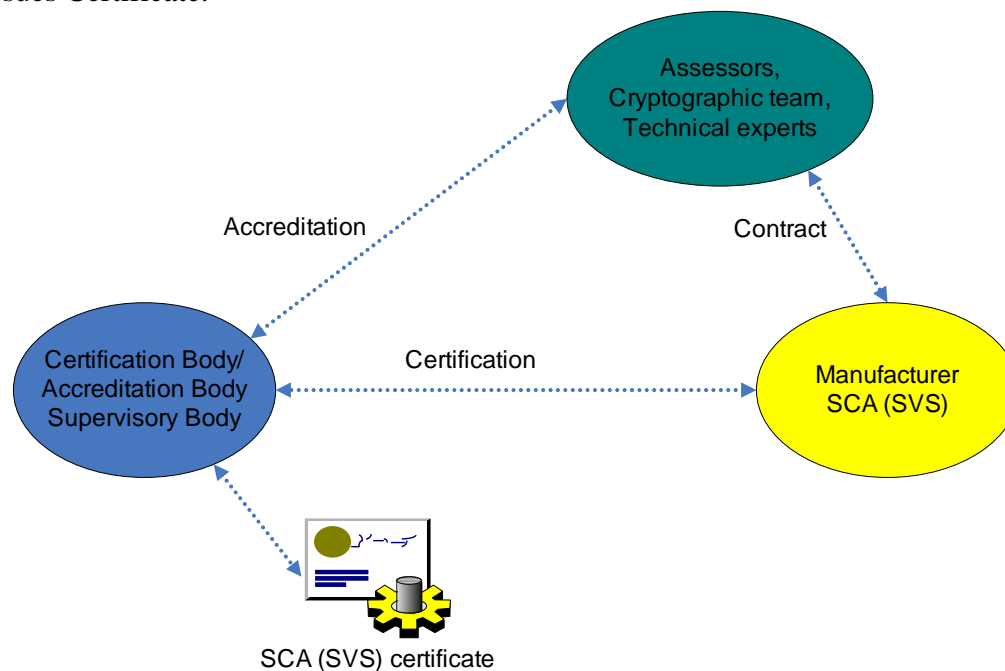


Figure 1 Certification parties for the SCA

2.3 Level of assurance

The certificate of conformity should give third parties – e.g. users of the SCA and/or signature verification application which obtained the certificate of conformity – a justified confidence that the SCA complies with the requirements stated in CWA 14170 and SVS meets requirements stated in CWA 14171.

2.4 Request for audit

The SCA Manufacturer may prepare Request for Proposal for audit. The Manufacturer's declaration of conformity for a Signature Creation Application and/or the Manufacturer's declaration of conformity for a Signature Verification System are parts of request for audit.

Proposals from Assessors state clearly the conditions of the audit and additional obligations of the Manufacturer not covered by this document. For the execution of the audit, the Assessor appoints a team of qualified auditors.

2.5 Request for certification

The SCA Manufacturer which withstands successful certification audit can prepare Request for Certification for Certification Body. Parts of the request for certification are:

- The Manufacturer's declarations of conformity for a SCA
- Final compliance statement worked-out by the Assessor. Necessary content of the final compliance statement is provided in section 2.10 Decision to certify.
- Forms required by local legislation prepared by the Assessor.

2.6 Request for re-certification

In case of changes to SCA (SVS) only in SCA application specific components the Manufacturer may request Certification Body for re-certification. Complete documentation required as for initial certification and documentation of changes will accompany the request.

If changes were made to any of SCA Trusted components (see 7.1 Signature Creation Systems components), then complete certification audit is necessary.

2.7 Accreditation of Assessors

The Accreditation Body accredits Assessors, cryptographic teams and technical experts based on fulfilment of requirement laid on these subjects in section 3 Requirements for Assessors. The Accreditation Body must issue accreditation statement within 1 month from accreditation request. If accreditation request is rejected, the Accreditation Body must state reason of rejection.

2.8 The Manufacturer's declaration of conformity

The Manufacturer's declaration of conformity is a declaration issued by the Manufacturer of SCA (SVS), that SCA (SVS) meets requirements stated in CWA 14170 (CWA 14171) and requirements stated in local legislation.

An example of declaration of conformity can be found in CWA 14172-4 Annex 2 “Part a: Manufacturer’s declaration” for SCA and CWA 14172-4 Annex 3 “Part a: Manufacturer’s declaration” for Signature verification devices.

2.9 Audit

Audit is performed as a part of certification process. Initial audit may be performed before request for certification.

As an audit output, the Assessor prepares a compliance statement. The Assessor makes positive/negative compliance statement on the base of audit findings. If non-conformity preventing successful completion of certification audit occurs during the audit, then the audit may be suspended or completely aborted.

If any non-conformity or deficiencies exist the Manufacturer must express its opinion on the non-conformities or deficiencies. In that case, the Manufacturer must take corrective actions within three months. The audit team assesses the corrective actions taken and reports the final findings. Positive compliance statement can be granted if no non-conformities and deficiencies exist.

Negative compliance statement must be declared if non-conformities or deficiencies still exist after corrective action.

2.9.1 Audit recurrence

The Manufacturer and the Assessor must propose an unambiguous method providing the Certification Body the possibility to find out whether in possible newer versions of the SCA or SVS the trusted components were modified. Recommended mechanism is to compute digital fingerprints of all source code files containing code for the trusted components.

In case of changes to SCA (SVS) the following steps are necessary:

- If changes are made in any of SCA trusted components, then complete re-audit is necessary. These changes can be detected by the Certification Body based on method and data present in the Assessor’s final compliance statement for previous version of SCA or SVS (see section 2.10 Decision to certify).
- If changes are made only in SCA application specific components, then Certification Body may re-certificate SCA.

2.9.2 Audit compliance statement

The final compliance statement of the Assessor must contain:

- a) Information uniquely identifying the Manufacturer.
- b) Information uniquely identifying name and version of the SCA (SVS).
- c) Intended usage of the product.
- d) The following statement of the Assessor: “SCA (SVS) is in the sense of valid legislation and certification methodology **eligible/ineligible** (in Slovak language “**spôsobilá/nespôsobilá**“) for creation and/or verification of advanced electronic

signature under condition that requirements laid by legislation and requirements of the Manufacturer are fulfilled”.

- e) Compliance statement verifying, that the signature policy and format of electronic signature for the SCA (SVS) in certification process are approved by the Certification Body.
- f) List of all NONCONFORITIES and the most critical DEFICIENCIES found.
- g) Limitations of SCA (SVS) usage.
- h) Conditions of re-audit:
 - Method and data necessary for the Certification Body to verify that trusted components are the original ones audited by the Assessor and provide the Certification Body possibility to find out whether trusted components were modified in newer versions of SCA or SVS.
 - Method and data necessary for Certification Body to verify that compiled and distributed version of the SCA and SVS is the same as the audited one.

2.10 Decision to certify

Certification Body makes decision to certify based on Assessor’s positive compliance statement, review of presented documentation listed in 4 Requirements for the Manufacturer, SCA and SVS and comments from the SCA Manufacturer.

The issued certificate is valid for a given version of SCA for unlimited period of time, excluding suspension, withdrawal or cancellation as described in 2.11 Suspension, withdrawal or cancellation of certification or compliance statement 2.8 The Manufacturer’s declaration of conformity. The contents of the certificate comply with the requirements described in 2.12 Contents of certificate of conformity.

2.11 Suspension, withdrawal or cancellation of certification or compliance statement

The Certification Body has the right to:

- a) Suspend the certificate if non-conformity is found after the SCA and/or SVS is certified;
- b) Withdraw the certificate if after suspension the Manufacturer has not taken any or insufficient corrective actions within a period of two months;
- c) Cancel certificate if Manufacturer ceases to support certified version of SCA or SVS;
- d) Cancel the certificate if the Manufacturer goes into bankruptcy, applies for moratorium or terminates the conduct of business;
- e) Suspend certificates of all applications, if this audit methodology or underlying standards are significantly changed. The Certification Body decides whether the change requires complete audit of applications, audit of part of application or audit is not necessary. After that new certificate may be issued or old certificate may be proclaimed to be valid.

In case of suspension, withdrawal or cancellation, the Certification Body removes the Manufacturer's and SCA's and/or SVS's name from the list of certified applications.

2.12 Contents of certificate of conformity

The certificate of conformity must contain as a minimum the following:

- a) Information regarding the Manufacturer:
 - Full name of the Manufacturer and part of organization concerned
 - Place of business.
- b) Information regarding the Assessor:
 - Name;
 - Place of business;
 - Trademark of the certification organization;
- c) Information regarding the certified SCA (SVS):
 - Version of the certified SCA (SVS) software;
 - The Assessor declaration that the SCA (SVS) fulfils specified requirements;
 - Description of the scope of certification including:
 - Clear identification of the SCA components that are certified;
 - Clear identification of the SCS parts;
 - Clear identification of SCDev with which certification of the SCA was executed;
 - Version of the Methodology used for certification;
- d) (Original) commencing date of the certificate and possible date of extension;
- e) Identification of the certificate;
- f) Signatures of the authorised personnel of the Certification Body.

2.13 Confidentiality

The Assessor keeps strictly confidential any information, oral or written, received from the Manufacturer in the context of the assessment process, unless law requires release of such data. Release of information by the Assessor for investigation by the Certification Body or for fulfilment of obligations to Experts Board in section 5 Methodology management will be stipulated in the standard conditions regarding the certification audit. The information included in the certificate 2.12 Contents of certificate of conformity shall be publicly available.

2.14 Appeal

Appeals, complaints and disputes brought before the Assessor by any party feeling affected by any decision of the Assessor shall be subject to the procedures of the

Assessor. The Assessor shall keep a record of all appeals, complaints and disputes and remedial actions relative to certification.

3 Requirements for Assessors

An Assessor performing certification audit must fulfil requirements laid both on the whole audit team and individuals in the audit team.

3.1 Audit team competence

The audit teams that conduct the audits have to possess relevant and up-to-date knowledge of IS practice. Individual auditors must meet the criteria for auditors as specified in 3.2 Individual auditors competence of this document. The following requirements apply to the audit team as a whole:

In each of the following areas at least one assessor in the team should satisfy the independent body's criteria for taking responsibility within the audit team:

- a) managing the team,
- b) knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of electronic signature, certification service and information security,
- c) knowledge of the current technical state-of-art regarding Public Key Infrastructure,
- d) knowledge of performing information security related risk audits so as to identify assets, threats and the vulnerabilities of the SCA and understanding their impact and their mitigation and control,
- e) knowledge of organizational reliability issues.

An audit team may consist of one person provided that the person meets all the criteria set out above.

3.2 Individual auditors competence

Auditors must comply with the following criteria, based on ISO 19011:2002:

- a) Academic qualifications should have been gained by a programme of studies consisting of a range of inter-related topics in which understanding is achieved by a predefined progression or route. It should be expected that where the assessor has accrued extensive experience and supplementary professional education and training, the requirement for academic qualifications would be significantly outweighed by their practical experience in the field.
- b) Having at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to Public Key Infrastructure and Information Security Management.
- c) Having appropriate understanding of the standards CWA 14170, CWA 14171, CWA 14172-4
- d) Having appropriate understanding of the concepts of management systems in general.
- e) Having appropriate understanding of the issues related to various areas of Public Key Infrastructure, Information Security Management, and organizational reliability.

- f) Having appropriate understanding of the principles and processes related to risk assessment and risk management.
- g) Having the following personal attributes: objective, mature, discerning, analytical, persistent, and realistic. The candidate should be able to put complex operations in a broad perspective and should be able to understand the role of individual units in larger organizations.
- h) Having knowledge and attributes to manage the assessment process.
- i) Keeping up own knowledge and skills of Public Key Infrastructure, Information Security Management, and management system assessment.
- j) Prior to assuming responsibility for performing as an assessor, the candidate should have gained experience in the entire process assessment in at least one of areas:
 - SCA or SVS assessment;
 - PKI assessment;
 - Information system assessment.

This experience should have been gained by participation under supervision of qualified (lead) auditors in a minimum of four assessments for a total of at least 20 days, including documentation review, implementation assessment and assessment reporting.

- k) All relevant experience should be current.

Auditors performing as lead auditor should additionally fulfil the following requirements:

- l) Having acted as qualified assessor in at least three complete assessments of SCA or from the following related areas:
 - PKI assessment;
 - Information system assessment.
- m) Having demonstrated to possess adequate knowledge and attributes to manage the assessment process.
- n) Having demonstrated the capability to communicate effectively, both orally and in writing.

Satisfying more than one of these criteria may be demonstrated by a single instance of professional experience.

Auditors deployed for performing SCA audits must observe the following Code of Conduct:

- a) To act in a trustworthy and unbiased manner in relation to both the body to which the Auditor is employed, contracted or otherwise engaged and any other organization involved in an assessment performed by him/her or by personnel directly under his/her control.
- b) To act independently and impartially, to disclose to the body deploying him/her any relationships he/she may have or may have had with the organization to be assessed

and to decline any assignment that could cause or could be perceived as causing conflict of interest.

- c) Not to accept any inducement, gift, commission, discount or any other profit from organizations assessed, from their representatives, or from any other interested person, nor knowingly allow personnel for whom he/she is responsible to do so.
- d) Not to disclose the observations, or any part of them, of the audit team for which he/she is or was responsible or of which he/she is or was part, or any other information obtained in the course of an assessment, to any third party unless authorized in writing by both the assessed organization and the body by which the Auditor is or was deployed.
- e) Not to act in any way prejudicial to the reputation or interest of the body by which the Auditor is or was deployed.
- f) In the event of any alleged breach of this code, to co-operate fully in any formal enquiry procedure.

3.3 Cryptographic team

Cryptographic team is accredited by Certification Body. Auditors may upon need request cryptographic team for cooperation during audit and cryptographic team members act for purpose of the audit as members of Assessor team.

Members of the cryptographic team need not meet requirements laid on Auditors. Results find out by cryptographic team are part of final compliance statement report.

Members of Cryptographic team must meet following requirements:

- All team member have academic qualifications in areas related in cryptography;
- Each team member must have at least 3 year of provable cryptographic experiences
- Team leader must have at least 10 years of provable cryptographic experiences.

3.4 Use of technical experts

Technical experts with specific knowledge regarding the subjects listed in 3.1 b) through e), but who do not satisfy all qualification criteria in 3.2 for individual auditors, may be part of the audit team. Technical experts should not function independently of the auditors in the team.

4 Requirements for the Manufacturer, SCA and SVS

The Manufacturer must meet following requirements:

- Provide documentation listed in section 4.1. SCA and SCS documentation
- If applicable, provide any of certificates listed in section 7.4.

SCA must meet following requirements:

- Requirements laid on SCA by CWA 14170 in sections
 - 7 Overall Security Requirements of the SCA
 - Sections 8 – 18.

SVS must meet following requirements:

- Requirements laid on SVS by CWA 14171.

4.1 SCA and SCS documentation

- Software development documentation for SCA taken as TOE as stated in 4.4 Software development documentation. Provided documentation for SCA and SCS must contain:
 - Risk analysis;
 - Information flow diagram within SCA;
 - Flow diagram of Signer's Authentication Data within SCA and SCDev;
 - Interface definition between SCA and SCDev with communication protocols and parameters specified;
 - Interface definition for entering Signer's Authentication Data;
 - Requirements laid by Manufacturer on SCS instances and operation (e.g. firewall configuration, configuration of SCDev);
 - Acceptable Signature Policies for the SCA;
- Description of TOE must contain decomposition of SCA into Trusted SCA components and Application specific SCA components as defined in CWA 14170 and described in Figure 2 SCA Components. Decomposition must contain:
 - Description of relevant security properties for each of components and mapping of controls in SCA to security requirements in CWA 14170;
 - Mapping of source code to components;
- Software specifications (initial, changes and validation requirements)
- Documented explanation of configuration parameters related to Signature Creation Parameters (these parameters may implement and set up Signature Policy in SCA);
- The Manufacturer's declaration of conformity with CWA 14170 as described in CWA 14172-4;
- Source codes of the SCA.

4.2 SVS documentation

- Software development documentation for SVS taken as TOE as stated in 4.4 Software development documentation. Provided documentation must contain:
 - Risk analysis;
 - Validation data flow diagram within SVS;
 - Flow diagram of trust point information within SVS;
 - Interface definition between SVS and SCDev with communication protocols and parameters specified;
 - Requirements laid by Manufacturer on SVS instances and operation (e.g. firewall configuration, configuration of SCDev);
 - Acceptable Signature Verification Policies for the SVS;
- Description of TOE will contain decomposition of SVS into components as defined Section 6 of CWA 14171 and listed in 7.1 Signature Creation Systems components. Decomposition must contain:
 - Description of relevant security properties for each of components and mapping of controls in SVS to security requirements stated in CWA 14171
 - Mapping of source code to components;
- Software specifications (initial, changes and validation requirements);

- Documented explanation of configuration parameters related to Signature Verification Process;
- The Manufacturer's declaration of conformity with CWA 14170 as described in CWA 14172-4;
- Source codes of the SVS.

4.3 SCDev documentation

Documentation on all SCDevs supported by SCA and SVS² containing at least following:

- SCDev high-level documentation or reference on source where it is available;
- All SCDev interfaces documentation or reference on source where it is available.

4.4 Software development documentation

- If applicable, software development maturity certificate (ISO 9001, CMM-IS, ISO 15408 EAL 3 of SCA/SVS);
- Manufacturer organisation chart related to software development with responsibilities described;

If none Quality Management System (QMS) certificate for software development is presented, then following documents are required. For the convenience, also ISO 15408-3 EAL3 Assurance Family tags and levels are provided. If software development certificate is provided, then below listed documents are not required.

- Security Target for TOE
- Description of TOE Security Functions
- ACM_CAP.3 Configuration management documentation
- ADO_DEL.1 Documented delivery procedures
- ADO_IGS.1 Documented procedures for the secure installation, generation and start-up of the TOE
- ADV_FSP.1 Functional specification
- AGD_ADM.1 Administrator guidance addressed to system administrative personnel
- AGD_USR.1 User guidance
- ADV_HLD.2 High-level design of TSF
- ADV_RCR.1 Analysis of correspondence between all adjacent pairs of TSF representations that are provided
- ALC_DVS.1 Development security documentation
- ATE_COV.2 Analysis of test coverage
- ATE_DPT.1 Analysis of the depth of testing
- ATE_FUN.1 Testing documentation (results)
- ATE_IND.2 TOE for testing, an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
- AVA_MSU.1 Guidance documentation
- AVA_SOF.1 Analysis of strength of TOE security function for each mechanism identified in the ST as having strength of TOE security function claim.

² Documentation should list all supported models of SCDevs or supported interfaces (e.g. PKCS#11).

- AVA_VLA.1 Analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP (TOE Security Policy)
- AVA_VLA.1 Disposition of obvious vulnerabilities.

5 Methodology management

The Experts Board forms the structure for representation of all parties concerned in issuing qualified certificates, such as users, user organizations, governmental organizations, suppliers, supplier organizations, certification bodies, and professionals.

Initially, members of the Experts Board are from KPMG Slovensko, spol. s r.o. and NBÚ. After that, the composition of the Experts Board will take place by appointment of new members by the Experts Board itself. Members of the Experts Board are expected to possess a broad knowledge of information technology and to have experience in organization and quality management, information security and PKI.

The Experts Board control tasks include:

- a) The processes described in the Methodology;
- b) Use of the criteria in the Methodology;
- c) Qualification of personnel;
- d) Experts Board team composition;
- e) Control and maintenance of auditor performance;
- f) Planning and control at operational level;
- g) Audit programme improvement;
- h) Supervision of application of the Code of Conduct for auditors;
- i) On request, taking part in appeal procedures of Assessors.

The Experts Board maintenance tasks include:

- a) Tracking and evaluating the experiences with the Methodology in the market;
- b) International co-ordination regarding harmonisation;
- c) Updating and implementing changes in the Methodology. Modification of the Methodology can be initiated e.g. by modification of underlying standards;
- d) Publication of the Methodology.

6 Registers of accredited Assessors, issued certificates

Assessors, cryptographic teams and technical experts accredited by Accreditation Body will be listed in a Register published periodically by Accreditation Body.

Certificates of conformity, issued in accordance with the conditions described in this methodology will be listed in a Register published periodically by Certification Body.

7 Audit content

SCA (SVS) may be logically partitioned into components for which are stated security requirements. In the following, the partitioning is given.

The Assessor must during the audit obtain sufficient assurance about fulfilling requirements laid on SCA (SVS). The Manufacturer may use software components from external sources as a part of the SCA (SVS), i.e. components not developed by the Manufacturer. The Assessor must obtain reasonable assurance also on security of such components (sufficient assurance may be e.g. ISO/IEC 15408 EAL 3 certificate for such component).

7.1 Signature Creation Systems components

SCA is in CWA 14170 decomposed into components in two main groups:

- Trusted SCA components
- Application Specific SCA components.

In this document we adopt the same partitioning of SCA in components as in CWA 14170.

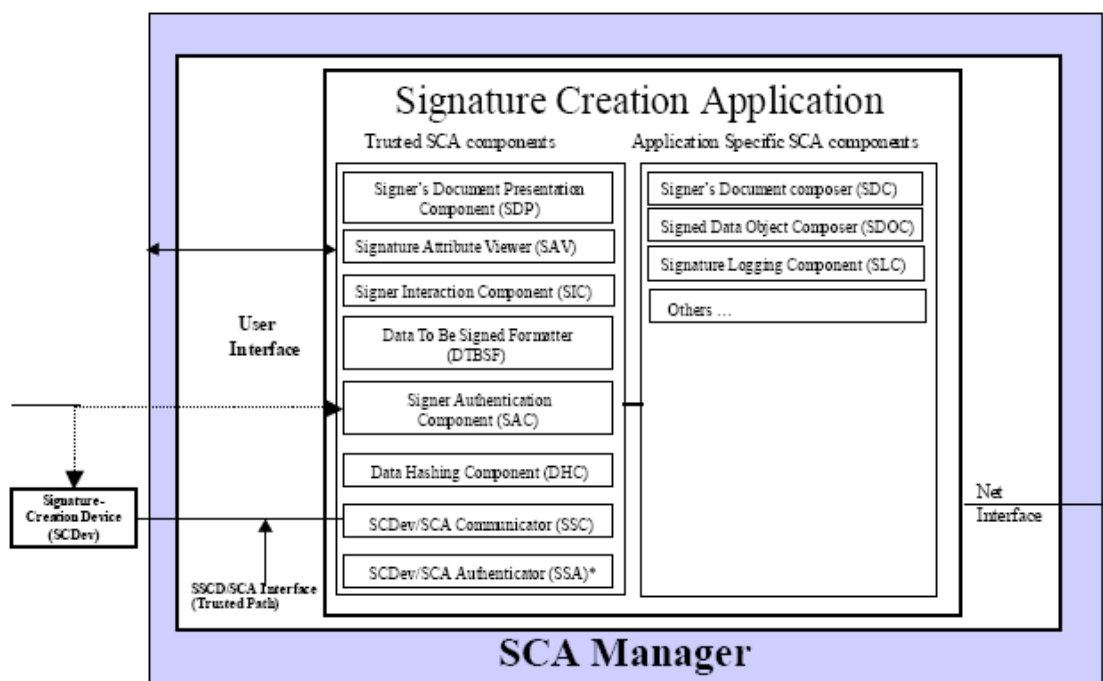


Figure 2 SCA Components

7.2 Signature Verification Systems components

CWA 14171 decomposes SVS for initial verification into following parts:

- the secure signature verification process,

- an interface to enter the Signed Document and to select the electronic signature to be verified (there may be more than one electronic signature attached with the user data),
- an interface for the current time,
- an interface for verification rules to be followed (e.g. a signature policy),
- a display/sound/video interface to present (e.g. display, listen to or visualize) the signed user data with the right format,
- an interface to get the signer's information and the output status after signature verification,
- an optional interface to write in a secure audit trail from an independent Trusted Third Party;
- a network interface to optionally fetch information produced by Trust Service Providers when not provided by the signer (e.g. CA repositories, CRLs repositories, OCSP responders, Time Stamping Authorities);

Additionally the following components can be included in the process:

- where necessary an interface to obtain any status information from available TSLs;
- where applicable an optional interface to get the definition of the Signature Policy.

A SVS for subsequent verifications is composed by CWA 14171 of:

- the secure signature verification process,
- an interface to enter the signer's document and to select the electronic signature to be validated (there may be more than one electronic signature attached with the user data),
- an interface for the current time,
- an interface for verification rules to be followed (e.g. a signature policy),
- a display/sound/video interface to present (e.g. display, listen to or visualize) the signed user data with the right format,
- an interface to get the signer information and the output status after the initial signature verification,
- an optional interface to fetch the recording time of the electronic signature from the secure audit trail of an independent Trusted Third Party.

Additionally the following components can be included in the process:

- where necessary an interface to obtain any status information from available TSLs;
- where necessary an interface to fetch the TST issuing TSU certificate status;
- where applicable an optional interface to get the definition of the Signature Policy.

7.3 Legislative requirements

Directive 1999/93/EC does not specify any formal requirements for signature verification. Recommendations stated in Directive ANNEX IV are covered by requirements stated in CWA 14171.

7.4 Software development maturity models

Holding certificate of any of the following quality management system for software development is considered to be satisfactory assurance of correspondence between provided documentation and source codes:

- ISO 9001:2000 for Software development;
- Capability Maturity Model Integration for Software, v1.1 Level 3 or higher;
- Common Criteria [5] ISO/IEC 15408-3 level EAL 3 or higher.

In case the Manufacturer holds one of above mentioned certificates it is not necessary to audit software development processes related to SCA and/or SVS.

Otherwise, the Assessor must evaluate software development processes necessary for SCA (SVS) development. Evaluation is based on Common Criteria ISO 15408 level EAL 3 or on CMMI-SW against “Level 3: Defined”. Performed software development maturity assessment related to SCA and/or SVS assessment is not equivalent to certification against any one of the above mentioned software development maturity models and serves solely for the purposes of SCA (SVS) assessment.

8 Vocabulary

SCA – Signature Creation Application
SCS – Signature Creation System
SCE – Signature Creation Environment
SCDev – Secure Signature Creation Device
ST – Security Target
SVA – Signature Verification Application
SVS – Signature Verification System
TOE – Target of Evaluation
TSF – TOE Security Functions
TST – Time Stamping Token
TSU – Time Stamping Unit

9 References

- [1] CEN CWA 14170:2004 Security Requirements for Signature Creation Applications
- [2] CEN CWA 14171:2004 Procedures for Electronic Signature Verification
- [3] CEN CWA 14172-4:2004 EESSI Conformity Assessment Guidance – Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification
- [4] Capability Maturity Model for Software, Version 1.1 Technical Report CMU/SEI-93-TR-024 ESC-TR-93-177
- [5] ISO/IEC 15408-3 Part:3 Security assurance requirements