



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

WORKSHOP AGREEMENT

CWA 14172-3

November 2001

ICS 35.040; 35.240.60

EESSI Conformity Assessment Guidance - Part 3: Trustworthy
Systems Managing Certificates for Electronic Signatures

This CEN Workshop Agreement can in no way be held as being an official standard as developed by CEN National Members.

© 2001 CEN

All rights of exploitation in any form and by any means reserved world-wide for CEN National Members

Ref. No CWA 14172-3:2001 E

Contents

| | page |
|--|------|
| Contents..... | 2 |
| Foreword..... | 3 |
| 1 Scope..... | 4 |
| 2 Definitions and abbreviations | 5 |
| 2.1 Definitions..... | 5 |
| 2.2 Abbreviations..... | 6 |
| 3 Guidance on conformity assessment of Trustworthy Systems | 7 |
| 3.1 Introduction..... | 7 |
| 3.2 Trustworthy Systems | 7 |
| 3.3 Introduction to IT Audit | 8 |
| 3.4 Introduction to conformity assessment of Trustworthy Systems | 10 |
| 3.5 Guidance on requirements for IT Auditors | 11 |
| 3.6 Guidance on the use of CWA 14167-1..... | 12 |
| Annex 1 References and bibliography..... | 14 |

Foreword

Successful implementation of the European Directive 1999/93/EC on a Community framework for electronic signatures requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products. Therefore, the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players: the European Electronic Signature Standardisation Initiative (EESSI).

In July 1999, EESSI delivered its initial recommendations in the EESSI Expert Report. The report contained an overview of the requirements for standards-related activities, as well as a work programme to meet these requirements. A work repartition was drawn up, allocating between CEN/ISSS and ETSI the standardisation activities. The work was carried out by CEN/ISSS in the E-Sign project and by ETSI SEC in the ESI WG. The results are documented in a series of CEN Workshop Agreements (CWA) and ETSI standards.

The production of this CEN Workshop Agreement (CWA) was formally agreed at the Kick-Off meeting of the CEN/ISSS Electronic Signatures Workshop (WS/E-SIGN) on 16-17 December 1999, in response to the initial work plan of the European Electronic Signature Standardization Initiative (EESSI).

This CWA has been developed through the collaboration of a number of contributing partners in the E-SIGN Workshop, gathering a wide mix of interests, representing different sectors of industry (manufacturers, end-users, service providers, legal experts, academia, accreditation bodies, standardization organisations and national standards bodies) as well as representatives of the national public and European authorities.

The present CWA has received the support of representatives of these sectors. A list of company experts who have supported the document's contents may be obtained from the CEN/ISSS Secretariat.

The final review/endorsement round for this CWA was started on 2001-09-04 and was successfully closed at the Workshop's plenary meeting on 2001-10-03. The final text of this CWA was submitted to CEN for publication on 2001-10-05.

This CWA has been issued in five parts:

- Part 1 - General
- Part 2 - Certification Authority services and processes
- Part 3 - Trustworthy systems managing certificates for electronic signatures
- Part 4 - Signature creation applications and procedures for electronic signature verification
- Part 5 - Secure signature creation devices.

This series of documents provides guidance on conformity assessment against the requirements specified in the other Workshop Agreements and the ETSI standard concerning services, processes, systems and products related to electronic signatures. The present document is intended to be applicable to later versions of the related documents should they be revised after its publication, unless a later version of it is produced which conflicts with this statement, in which case the latest version shall apply.

1 Scope

This document provides guidance on conformity assessment of Trustworthy Systems against the specification CWA 14167-1 “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures”. The guidance is intended for use by IT Auditors as well as manufactures and suppliers of Trustworthy Systems (TWSs) and certification-service-providers (CSPs) using TWSs.

2 Definitions and abbreviations

2.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

| | |
|---------------------------|--|
| Audit | <i>Systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.</i> |
| Process | <i>A series of procedures and actions that have to be conducted in order to manage and enable the provision of an electronic trust Service.</i> |
| Product | <i>A good (hardware, software, or both) which performs against a particular specification and which can contribute towards the construction of a System built to fulfil a particular, service-focused function.</i> |
| Service | <i>The carrying-out of a function (or a series of functions) that provides a definable benefit to an end user. In the context of this document we are concerned primarily with electronic trust services, such as those associated with (Digital) Certificate Management.</i> |
| System | <i>The composition of Information Technology products and components (both hardware and software, and including processors, storage, networks, telecommunications, etc.) organised to support the provision of a particular electronic trust Service. This requires that the system be specifically, configured, integrated, installed in a physical environment and operated according to defined Processes.</i> |
| Trustworthy System | <i>An information system or product implemented as either hardware and/or software that produces reliable and authentic records which are protected against modification and additionally ensures the technical and cryptographic security of the processes supported by it.</i> |

2.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---------------------|---|
| <i>CC</i> | Common Criteria for Information Technology Security Evaluation |
| <i>CEN</i> | Comité Européen de Normalisation (European Committee for Standardization) |
| <i>CEN/ISSS</i> | CEN Information Society Standardization System |
| <i>CSP</i> | Certification-Service-Provider |
| <i>CWA</i> | CEN Workshop Agreement |
| <i>E-SIGN</i> | CEN/ISSS Electronic Signatures project |
| <i>EDP</i> | Electronic Data Processing |
| <i>EESSI</i> | European Electronic Signature Standardization Initiative |
| <i>ETSI</i> | European Telecommunications Standardization Institute |
| <i>ETSI SEC</i> | ETSI Security Technical Committee |
| <i>ETSI SEC ESI</i> | ETSI SEC Electronic Signatures and Infrastructures |
| <i>ISO</i> | International Organization for Standardization |
| <i>IT</i> | Information Technology |
| <i>ITSEC</i> | Information Technology Security Evaluation Criteria |
| <i>NQC</i> | Non-Qualified Certificate |
| <i>PKI</i> | Public Key Infrastructure |
| <i>QC</i> | Qualified Certificate |
| <i>SCD</i> | Signature Creation Device |
| <i>SSCD</i> | Secure Signature Creation Device |
| <i>TS</i> | Technical specification |
| <i>TWS</i> | Trustworthy System |

3 Guidance on conformity assessment of Trustworthy Systems

3.1 Introduction

This chapter provides guidance on conformity assessment of Trustworthy Systems (TWSs) against the specification CWA 14167-1 “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures”. The guidance is intended for use by IT Auditors as well as manufactures and suppliers of TWSs and CSPs using TWSs.

This chapter is composed of six sections:

- Section 3.1, Introduction; is an overview of the guidance and explains the numbering of guidance and the use of the terminology concerning requirements.
- Section 3.2, Trustworthy Systems; highlights the concept of TWSs.
- Section 3.3, Introduction to IT Audit; describes the principles of the IT Audit.
- Section 3.4, Introduction to conformity assessment of Trustworthy Systems; describes in general terms the contents of CWA 14167-1 as specification for assessment of TWSs.
- Section 3.5, Guidance on requirements for IT Auditors; provides guidance on requirements for competence and conduct of IT Auditors.
- Section 3.6, Guidance on the use of CWA 14167-1; provides guidance on performing IT Audits against the security requirements specified in CWA 14167-1.

To uniquely identify the guidance elements within the series of guidance documents, each element is numbered **G.<guidance document Part number>.<sequence number>**. The part number of this guidance document is 3.

The term “shall” is used throughout the guidance in this chapter to indicate those provisions which, reflecting the requirements of CWA 14167-1, are mandatory. The term “should” is used to indicate those provisions that, although they constitute guidance for the application of the requirements, are expected to be adopted by IT Auditors. Any variation from the guidance should be an exception. Such variations should only be permitted on a case-by-case basis after it has been demonstrated that the exception meets the relevant requirements and the intent of this guidance in an equivalent way.

3.2 Trustworthy Systems

Directive 1999/93/EC stipulates in Annex II item (f) that certification-service-providers (CSPs) must use trustworthy systems and products, which are protected against modification and ensure the technical and cryptographic security of the processes supported by them. In relation to the use of TWSs, CWA 14167-1 considers the following requirements in Annex II of importance as well:

- Annex II (a) – demonstrate the reliability necessary for providing certification services;
- Annex II (b) – ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- Annex II (c) – ensure that the date and time when a certificate is issued or revoked can be determined precisely;
- Annex II (g) – take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data.

CWA 14172-3:2001 (E)

Based on the requirements in the Directive, CWA 14167-1 provides in its chapter 4 an overview of a CSP system broken down into a number of services. Some of these services provide mandatory functionality, termed 'Core Functionality' whereas others are optional services providing 'Supplementary Functionality'. Through these functionalities, a CSP provides and manages certificates used for the support of electronic signatures. The CWA is based on the primary assumption that Public Key Infrastructure (PKI) will be used for the management of certificates.

Core Functionality covers the following CSP services:

- Registration Service – to verify the identity and, if applicable, any specific attributes of a Subscriber;
- Certificate Generation Service – to create certificates;
- Dissemination Service – to provide certificates and policy information to Subscribers and Relying Parties;
- Revocation Management Service – to allow the processing of revocation requests;
- Revocation Status Service – to provide certificate revocation status information to relying parties.

Supplementary Functionality covers two optional CSP services:

- Subscriber Device Provision Service – to prepare and provide a Signature Creation Device (SCD) to Subscribers. This includes Secure-Signature-Creation Device (SSCD) provision;
- Time Stamp Service – provides a CSP Time Stamp Service, which may be needed for signature verification purposes.

TWSs for which the manufacturer, supplier or CSP claims conformance to CWA 14167-1 may consist of a number of subsystems each providing specific CSP functionality. CSPs must at least implement Core Functionality to meet the requirements of Directive 1999/93/EC. A CSP can choose to implement any Supplementary Functionality as deemed necessary by national, business or market requirements.

TWSs that provide the functionality required by a CSP shall meet the security requirements specified in CWA 14167-1. The CWA specifies security requirements for each of the Core and Supplementary Functionalities. In addition, TWSs are required to have generic security functionality. The general security requirements are applicable to all CSP services and deal with managing and operating TWSs, ensuring CSP business continuity, and providing time synchronisation.

Directive 1999/93/EC specifies the requirements for Certification-Service-Providers issuing Qualified Certificates (QCs). CWA 14167-1 caters for security requirements of systems for both QCs and Non-Qualified Certificates (NQCs) and indicates the areas where differentiation is required.

3.3 Introduction to IT Audit

Since the emergence of electronic data processing auditing in the late 1960s, EDP Audit has become an important part of financial auditing, business development, systems development, and security auditing. The discipline is now referred to as Information System (IS) Audit or Information Technology (IT) Audit. The objective of IT Audit is to assess the use of IT and to advise on such use. IT Audit is focused in particular on quality characteristics such as reliability, security, conformity, continuity, manageability, traceability, confidentiality, effectiveness and efficiency. It is used for any or all of the following:

- to manage information and develop information systems;
- to evaluate the effectiveness and efficiency related to the use of resources;
- to support financial auditors in auditing financial statements;
- to improve system and process controls;
- to prevent and detect errors and fraud;
- to reduce risk and enhance system security;

- to plan for contingencies and disaster recovery.

Especially the last four bullets of the list above are within the domain of the IT Auditor specialising in the security of information systems.

To perform an IT Audit, the following audit scope elements must be clearly defined:

- **Object**
 - part of the system, the system or combination of systems (product or system audit)
 - realisation (development, manufacturing) of the part of the system, the system or combination of systems (process audit)
 - application (use) of the part of the system, the system or combination of systems (process audit)

Note that the audit object can consist of any combination of the above.
- **Aspect** reliability, security, conformity, continuity, manageability, traceability, confidentiality, etc. as well as sub-aspects such as correctness, timeliness, completeness, effectiveness, efficiency, etc. An IT Audit can comprise multiple aspects and their sub-aspects.
- **Standard(s)** the specification(s) used for review and examination of records and activities concerning the object and its aspect(s).

In addition to scope elements, the audit risk should be considered. Audit risk is the level of risk of issuing an incorrect audit opinion notwithstanding all effort that has been put into the audit. This risk is determined by the desired level of assurance, which in turn depends on the importance of the audit opinion as seen by the parties that would depend on that opinion.

Audit risk could range from zero, where there is complete certainty of a correct opinion, to one, where there is complete certainty of an incorrect opinion. In practice, audit risk will always be greater than zero since it is not possible, due to the limitations in systems, processes and auditing, to be absolutely certain that an incorrect opinion will not occur.

In the case of TWSs, the required level of assurance is determined by the audit client, i.e. the manufacturer or supplier of TWSs or the CSP using their TWSs. The importance of TWSs for managing certificates for electronic signatures is such that a high level of assurance is required. The IT Auditor should therefore plan and perform the audit in such a way that the evidence obtained provides a solid basis for the audit opinion.

Given the high level of assurance required of the audit, the IT Auditor should consider the risk that is inherent in the TWS or TWS component to be audited and the environment in which it is placed. If the audit object can be separated into parts, auditing the parts and their integration separately could decrease the inherent risk. This will often require less overall effort and provide more detailed evidence.

Next, the IT Auditor should strive to minimise the risk that internal controls applied during development and manufacturing of the TWS or TWS components would not have detected deficiencies. Such internal controls should be audit objects by themselves. The IT Auditor should obtain and examine all evidence of the controls that have been applied. Control evidence would include procedures, design documents, development specifications, test specifications, development and test records, production records, etc. In case control evidence cannot be provided or appears to be insufficient, the control risk must be considered as high, causing an increased audit risk. A high control risk in the case of auditing a simple TWS component might be set off by an in-depth audit of the component itself. However, a high control risk in the case of auditing a full TWS would render it impossible to issue an audit opinion that would provide a high level of assurance.

Finally, the IT Auditor should minimise the risk that the audit would not reveal deficiencies in the TWS or TWS component, or in the controls applied during its development and manufacturing. This audit aim can be achieved by putting sufficient effort into the planning and performing of the audit.

Performing an IT Audit consists of planning the audit, review and examination of records and activities, holding a closing meeting to communicate the audit results to the client, issuing a draft audit report to the client for comments, and issuing the final report. The final audit report is issued to the client with a letter that will outline suggested actions to resolve or close recommendations.

An audit recommendation is resolved when the IT Auditor and the client agree on the action that will correct the problem or deficiency that produced the recommendation. An audit recommendation is closed when the agreed-upon corrective action has been completed. At the completion of all corrective actions, the IT Auditor will issue a statement -the Audit Opinion- declaring compliance of the object and its aspects with the applied standard(s).

With respect to the competence of IT Auditors, the following should be noted:

In many countries there is a professional association of IT Auditors. These associations set requirements for IT Audit education and perform registration of IT Auditors. The requirements for registration usually include: completed formal IT Audit education, a number of years practical experience and irreproachable conduct. The associations publish a register of recognised IT Auditors and maintain a code of conduct. The associations have procedures to handle complaints against IT auditors.

3.4 Introduction to conformity assessment of Trustworthy Systems

CWA 14167-1 specifies security requirements on technology components and systems, used by certification-service-providers to create Qualified and Non-Qualified Certificates. The CWA is relevant for manufacturers and suppliers of Trustworthy Systems used for managing certificates, but may be adopted by anyone deploying systems and wanting to meet the requirements of Directive 1999/93/EC.

When managing Qualified Certificates, CSPs may adopt specific policies as specified in ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates". To meet the requirements of TS 101 456, the CSP must use trustworthy systems. CSPs using systems that comply with the requirements of CWA 14167-1 are considered to meet the relevant trustworthy system requirements specified in TS 101 456.

CSPs shall only claim conformance to CWA 14167-1 if the CSP uses TWSs that have been audited and determined to be conformant to that CWA. In doing so CSPs may benefit by being able to demonstrate a degree of pre-qualification when applying for recognition under an approval scheme.

Manufacturers and suppliers of TWSs should only claim the TWS's conformance to CWA 14167-1 after having them independently audited and determined to be conformant to that CWA. So as to assist CSPs in providing evidence in support of the assessment of their services, manufacturers and suppliers of TWSs should make available the results of these audits.

Audit of TWSs shall be conducted by an independent auditor qualified to perform the task. Audits may be conducted in the form of an Information Technology (IT) Audit, where auditors would:

- determine whether the TWS is conformant to Non-Qualified Certificate (NQC) requirements or to Qualified Certificate (QC) requirements; this is indicated for each requirement specified in CWA 14167-1 and is explained in CWA 14167-1 §4.4 - Security Levels;
- collect and evaluate evidence;
- determine whether the TWS meets the appropriate requirements specified in sections 4 and 5 of CWA 14167-1.

When submitting their TWSs for conformance audits, manufacturers should provide documentary evidence of:

- their development methodology, including configuration management, used for the development of the TWS;
- Installation Guidance, including procedures for secure installation, generation, and start-up of the TWS. This should include a list of configuration parameters to allow the TWS to be configured to fulfil the requirements of CWA 14167-1;
- Administration Guidance, for configuring, maintaining and administering the TWS such that the required level of security is ensured. Administration guidance is intended to help administrators understand the security functions provided by the TWS;
- User Guidance, intended for use by non-administrative users of the TWS, and by others (e.g. developers) using the TWS's external interfaces. User guidance describes the security functions provided by the TWS and provides instructions and guidelines, including warnings, for secure use of the TWS.

When auditing a TWS, evidence of prior formal Common Criteria (CC) or Information Technology Security Evaluation Criteria (ITSEC) evaluations of TWSs or TWS components may exist and be provided by the client to the IT Auditor. Previously evaluated TWSs or TWS components would not require re-evaluation. However assessment of any non-evaluated aspects of the TWS or TWS component and its overall use within the total system shall be included within the scope of the IT Audit.

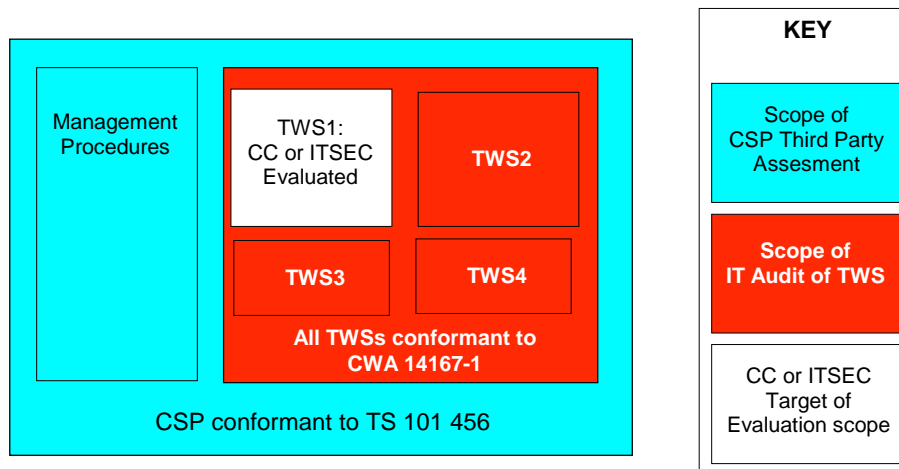


Figure 1 - Complementary scoping of a CSP claiming conformance to TS 101 456

Figure 1, above, depicts a typical scenario of a CSP claiming conformance to TS 101 456, using TWSs conformant to CWA 14167-1, one of which is a CC or ITSEC evaluated TWS. Additionally it outlines the scope of the audit for each case.

3.5 Guidance on requirements for IT Auditors

G.3.1 The IT Auditor performing audits against CWA 14167-1 should meet the following competence criteria:

- have successfully completed formal IT Audit education;
- have at least four years full time practical workplace experience in IT auditing, of which at least two years have been in a role or function relating to Public Key Infrastructure and Information Security;
- have appropriate understanding of the specifications CWA 14167-1 and ETSI TS 101 456;
- have maintained up-to-date knowledge and skills of Public Key Infrastructure and Information Security.

All relevant experience should be current.

G.3.2 The IT Auditor should be independent, i.e. maintain freedom from those pressures and other factors that compromise, or can reasonably be expected to compromise, the IT Auditor's ability to make unbiased audit decisions. The goal of auditor independence is to support the reliance of parties that depend on Trustworthy Systems.

The IT Auditor should for example:

- have no personal interest in or gain from the objects to be audited and in the organisation(s) submitting these objects for audit;
- have no financial or commercial interest in or gain from the objects to be audited and/or in the organisation(s) submitting these objects for audit;
- have no involvement as owner, shareholder, manager, and/or employee in the organisation(s) that develop(s) and/or manufacture(s) and/or submit(s) the objects for audit;
- have no family or other personal relationship with persons involved in the development and/or manufacturing of the objects to be audited;

CWA 14172-3:2001 (E)

- have no involvement as a consultant or advisor in the development and/or manufacturing of the objects to be audited.

Note that the above examples do not constitute an exhaustive list. It is the responsibility of the IT Auditor to assess each request for audit and justify the reasons for accepting or not accepting the audit assignment.

G.3.3 IT Auditors performing audits against CWA 14167-1 should observe a Code of Conduct fulfilling at least the following:

- to serve in the interest of their employers, stockholders, clients and the general public in a diligent, loyal and honest manner, and not knowingly be a party to any illegal or improper activities;
- to maintain the confidentiality of information obtained in the course of their duties. The information shall not be used for personal benefit nor released to inappropriate parties;
- to perform their duties in an independent and objective manner, and to avoid activities which threaten, or may appear to threaten, their independence and objectivity;
- to maintain competency in the interrelated fields of auditing, Information Technology, Public Key Infrastructure and Information Security through participation in professional development activities;
- to use due care to obtain and document sufficient factual material on which to base audit conclusions and recommendations;
- to inform the appropriate parties of the results of audit work performed;
- to maintain high standards of conduct in both professional and personal activities.

3.6 Guidance on the use of CWA 14167-1

G.3.4 The objective of auditing a TWS is to provide a high level of assurance of compliance with the requirements specified in CWA 14167-1. The IT Auditor should plan and perform the audit in such a way that the evidence obtained provides a solid basis for the audit opinion.

G.3.5 According to CWA 14167-1, a TWS can be broken down into a number of functions for CSP services. For these functions, the CWA specifies General Security Requirements, Core Functionality Security Requirements, and Supplementary Functionality Security Requirements. In order to avoid duplication of audits, the IT Auditor may accept that the audit of a TWS re-uses the results of separate audits of the parts of the system, the systems or combination of systems that provide the functions. Different IT Auditors could carry out the separate audits of functionalities. The IT Auditor confirming that the TWS meets the requirements of CWA 14167-1 should obtain and review the audit reports concerning the separately audited functionalities and take these into account in the audit report on the TWS, ensuring that their individual scopes map acceptably onto the scope of the audit he/she is currently performing.

G.3.6 A separate audit of a system providing the functionality of a CSP service should cover that service completely, i.e. a system should not be further subdivided for auditing. The part of the system, the system or combination of systems that provide the functionality for one or more of the following complete services should be the audit object:

- Registration Service – verifying the identity and, if applicable, any specific attributes of a Subscriber;
- Certificate Generation Service – creating certificates;
- Dissemination Service – providing certificates and policy information to Subscribers and Relying Parties;
- Revocation Management Service – processing of revocation requests;
- Revocation Status Service – providing certificate revocation status information to relying parties.
- Subscriber Device Provision Service – preparing and providing a Signature Creation Device (SCD) to Subscribers. This includes Secure-Signature-Creation Device (SSCD) provision;
- Time Stamp Service – providing Time Stamp Services.

The applicable General Security Requirements specified in CWA 14167-1 should be covered in the audit of the system providing the functionality of the service(s) concerned. However, the evidence submitted to support the audit may be based upon prior assessment of components of the system against recognised references and processes.

G.3.7 To provide a high level of assurance, it is essential for the IT Auditor to have full insight into the internal controls applied during development and manufacturing of the system that provides the functionality of the CSP services. The scope of the audit should therefore cover the development and manufacturing processes. The evidence that should be verified would include development procedures, design documents, development specifications, test specifications, development and test records, production procedures and work instructions, production records, etc. The audit should determine the effectiveness of the procedures in relation to the required security level of the system. Should evidence of internal controls applied during development and manufacturing not exist or be considered insufficient, the IT Auditor should not issue a positive audit opinion.

G.3.8 The IT Auditor should specify the scope of the audit in the following terms:

- **Object**
 - the system (or part of the system or combination of systems) including identification of its hardware and software components;
 - whether the system covers all or only certain CSP services, including in either case identification of the CSP service(s) actually covered by the system;
 - whether the system is used for NQC or QC;
 - the applicable clauses of CWA 14167-1 (General Security Requirements and Core and/or Supplementary Functionalities);
 - processes, procedures and records relevant to the development and manufacturing of the system;
 - documentation for use of the system (Installation, Administration, and User Guidance).
- **Aspect** security of the system and the sub-aspect effectiveness -in relation to security- of the development and manufacturing procedures as well as effectiveness of the documentation for use.
- **Standard** CWA 14167-1.

G.3.9 Evidence of prior formal Common Criteria (CC) or Information Technology Security Evaluation Criteria (ITSEC) evaluations of a component may be present and provided by the client to the IT Auditor. Previously evaluated components would not require re-evaluation. However assessment of any non-evaluated aspects of the component and its overall use within the system or TWS shall be included within the scope of the IT Audit.

G.3.10 In case of auditing the security requirements of a system consisting of discrete components, the integration of these components and the testing of the integrated system shall be included within the scope of the IT Audit.

Annex 1 References and bibliography

References

The following normative document contains provisions that, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this CWA are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures*

Bibliography

The following material provides supporting information:

- BSI IT-Grundschutzhandbuch "Bundesamt für Sicherheit in der Informationstechnik - IT-Grundschutzhandbuch Standard-Sicherheitsmaßnahmen", January 2000.
- CCIMB-99-031 "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model", Version 2.1, August 1999
- CCIMB-99-032 "Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements", Version 2.1, August 1999
- CCIMB-99-033 "Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements", Version 2.1, August 1999
- Directive 1999/93/EC "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures".
- ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates"
- ISO 15408-1:1999 "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model"
- ISO 15408-2:1999 "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements"
- ISO 15408-3:1999 "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements"
- ISO/IEC 17799:2000: "Information technology -- Code of practice for information security management."
- RFC 2527 "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", March 1999."