



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

WORKSHOP AGREEMENT

CWA 14172-2

July 2001

ICS 35.040; 35.240.60

EESSI Conformity Assessment Guidance - Part 1: Certification
Authority services and processes

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 14172-2:2001 E

Contents

Contents.....	2
Foreword.....	3
1 Scope.....	4
2 Definitions and abbreviations	5
2.1 Definitions.....	5
2.2 Abbreviations.....	5
3 Guidance on conformity assessment of Certification Authority services and processes.....	6
3.1 Introduction.....	6
3.2 Certification Authority.....	6
3.3 Introduction to conformity assessment of Certification Authorities.....	7
3.4 Guidance on requirements for independent bodies, assessors, and assessment teams	7
3.5 Guidance on the conformity assessment process	10
3.6 Guidance on the use of ETSI TS 101 456.....	13
Annex 1 References and bibliography.....	15

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 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 Electronic Signatures Workshop (WS/E-SIGN) 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 2001-03-15 and was successfully closed at the Workshop's plenary meeting on 2001-04-04. The final text of this CWA was submitted to CEN for publication on 2001-05-09.

The purpose of this document is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures developed under the European Electronic Signature Standardisation Initiative (EESSI) by the CEN/ISSS Workshop on Electronic Signatures and the ETSI SEC ESI Working Group. The guidance is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to these standards.

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 Certification Authorities (CAs) against the standard ETSI TS 101 456 V1.1.1 (2000-12) – “Policy requirements for certification authorities issuing qualified certificates”. The guidance is intended for use by independent bodies and their assessors.

2 Definitions and abbreviations

2.1 Definitions

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

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>

2.2 Abbreviations

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

CA	Certification Authority
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CPS	Certification Practice Statement
CWA	CEN Workshop Agreement
E-SIGN	CEN/ISSS Electronic Signatures project
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standardization Institute
ETSI SEC	ETSI Security Technical Committee
ETSI SEC ESI	ETSI SEC Electronic Signatures and Infrastructures
ISO	International Organization for Standardization
QCP	Qualified Certificate Policy
SSCD	Secure Signature Creation Device
TS	Technical specification

3 Guidance on conformity assessment of Certification Authority services and processes

3.1 Introduction

This chapter provides guidance on conformity assessment of Certification Authorities (CAs) based on the standard ETSI TS 101 456 V1.1.1 (2000-12) – “Policy requirements for certification authorities issuing qualified certificates” (often referred to as “Qualified Certificate Policy” or “QCP”). The guidance is intended for use by independent bodies and their assessors.

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, Certification Authority; highlights the concept of CA as used in the QCP.
- Section 3.3, Introduction to conformity assessment of Certification Authorities; describes in general terms the contents of the QCP as standard for assessment of CAs, the use of the QCP by independent bodies, and the intention of the guidance in achieving harmonised assessment practices.
- Section 3.4, Guidance on requirements for independent bodies, assessors, and assessment team. It provides guidance based upon current practices in accreditation / certification of management systems.
- Section 3.5, Guidance on the conformity assessment process; describes the assessment process in terms of current practices applied in the certification of rather complex management systems such as Information Security Management Systems; this kind of assessment process is considered applicable for the assessment of CAs.
- Section 3.6, Guidance on the use of ETSI TS 101 456; providing guidance on a number of elements in the QCP that were felt requiring special attention in order to achieve harmonisation of assessments.

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 document is 2.

The term “shall” is used throughout the guidance in this chapter to indicate those provisions which, reflecting the requirements of ETSI TS 101 456, 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 independent bodies, assessors and CAs. 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 Certification Authority

In the scope of ETSI TS 101 456, the Certification Authority (CA) is the certification-service-provider issuing qualified certificates as defined in the Directive. The CA has overall responsibility for the provision of the certification services identified in the standard. The CA's key is used to sign the qualified certificates it issues. The CA is identified in the certificate as the issuer.

The CA may make use of other parties to provide parts of the certification service. However, the CA always maintains overall responsibility and must ensure that the policy requirements identified in the standard are met. The CA may subcontract all the component services, including the certificate generation service. However, the key used to generate the certificates is identified as belonging to the CA, and the CA maintains overall responsibility for meeting the requirements defined in the standard and liability for the issuing of certificates to the public as required in the Directive.

3.3 Introduction to conformity assessment of Certification Authorities

ETSI TS 101 456 specifies minimum policy requirements relating to CAs issuing Qualified Certificates. The standard defines a comprehensive set of policy requirements for the provision of the range of services which underpin certificate issuance and the overall certificate management process, e.g.: services for registration, certificate generation, certificate dissemination, revocation management, revocation status, and if applicable signature creation device provision. In addition to the certification service processes, the requirements cover CA management and operation relating to information security and to organisational reliability and competence of personnel. The CA's provisions to comply with the policy requirements are referred to in this chapter as "CA's management system".

Whilst recognising that the CA carries the ultimate responsibility for ensuring that the components of its service are conformant with the requirements of ETSI TS 101 456, the standard and this guidance may be used as the basis for assessing the conformance of individual service components. The assessment of the overall service may then re-use the results of these assessments of service components.

An independent body may use the standard as the basis for confirming that a CA meets the requirements for issuing Qualified Certificates. Such confirmation is based upon assessment of the CA by an assessment team deployed by the independent body. The assessment team performs assessment of the documentation and operation of the CA against the requirements of the standard and reports its observations to the independent body.

This publication specifies guidance, the observance of which is intended to ensure that assessors of independent bodies operate in a consistent and reliable manner, thereby facilitating their acceptance on a national and international basis. The guidance is based upon the applicable documents in the EN 45000 series of standards and the relating guidelines published by the European co-operation for Accreditation (EA). In particular, EA document EA-7/03, providing guidelines for the accreditation of bodies operating certification of Information Security Management Systems, has been taken into account.

This publication should serve as a foundation for the recognition of national systems in the interests of international trade.

Conformity assessment of CAs is voluntary. Public confidence in the trustworthiness of electronic signatures would be provided to users when the signatures have been issued by CAs that have successfully completed a conformity assessment process. The independent bodies responsible for performing conformity assessment should make public statements of capability of CAs whilst permitting the CAs to keep details of their internal processes and information security measures confidential. Voluntary conformity assessment could be used to demonstrate to the system of supervision of certification-service-provision in a Member State established in accordance with Article 3 sub 3 of the Directive that a CA complies with the requirements of Annex II of the Directive. It is of course depending on the legal requirements in a Member State whether other methods of demonstrating compliance could exist.

It is strongly recommended that the different supervision systems, voluntary schemes, and independent bodies operating within voluntary schemes in the Member States establish liaison in order to adopt common practices, thereby facilitating mutual recognition.

3.4 Guidance on requirements for independent bodies, assessors, and assessment teams

Guidance on requirements for independent bodies

G.2.1 Independent bodies confirming that CAs meet the requirements of ETSI TS 101 456 should comply with the requirements for reliability and competence in the applicable standards of the EN 45000 series.

Guidance on qualification criteria for individual assessors

G.2.2 Each individual assessor deployed by an independent body for performing conformity assessment of CAs should be qualified based on the following criteria:

- 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 standard ETSI TS 101 456.
- 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 organisational reliability.
- f) Having appropriate understanding of the principles and processes related to risk assessment and risk management.
- g) Having successfully followed a training course of at least five days on the subject of management system assessment and the management of assessment processes.
- h) 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 organisations.
- i) Having knowledge and attributes to manage the assessment process.
- j) Keeping up own knowledge and skills of Public Key Infrastructure, Information Security Management, and management system assessment.
- k) Prior to assuming responsibility for performing as an assessor, the candidate should have gained experience in the entire process of CA assessment. This experience should have been gained by participation under supervision of qualified (lead) assessors in a minimum of four assessments for a total of at least 20 days, including documentation review, implementation assessment and assessment reporting.
- l) All relevant experience should be current.

An assessor performing as assessment team leader (Lead Assessor) should additionally fulfil the following requirements:

- m) Having acted as qualified assessor in at least three complete CA assessments.
- n) Having demonstrated to possess adequate knowledge and attributes to manage the assessment process.
- o) Having demonstrated the capability to communicate effectively, both orally and in writing.

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

Note: Initially, independent bodies may not be able to find individuals that would satisfy the criteria under b), k) and m) above. If an independent body wishes to qualify assessors and lead assessors that do not fulfil these criteria, the independent body should be able to provide recorded evidence that justifies qualifying assessors and lead assessors on the basis of other, relevant, experience.

Guidance on a Code of Conduct for assessors

G.2.3 Assessors deployed for performing CA assessments should observe a Code of Conduct fulfilling at least the following:

- a) To act in a trustworthy and unbiased manner in relation to both the body by which the assessor is employed, contracted or otherwise engaged and any other organisation 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 organisation 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 organisations 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 assessment 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 authorised in writing by both the assessed organisation and the body by which the assessor is or was deployed.
- e) Not to act in any way prejudicial to the reputation or interest of the body by which the assessor is or was deployed.
- f) In the event of any alleged breach of the code of conduct, to co-operate fully in any formal enquiry procedure.

Guidance on assessment team competence

G.2.4 The following requirements apply to the assessment team as a whole:

- a) 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 assessment team:
 - i) managing the team,
 - ii) knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of certification service and information security,
 - iii) knowledge of the current technical state-of-art regarding Public Key Infrastructure,
 - iv) knowledge of performing information security related risk assessments so as to identify assets, threats and the vulnerabilities of the CA and understanding their impact and their mitigation and control,
 - v) knowledge of organisational reliability issues.
- b) The assessment team should be competent to trace indications of security incidents in the CA's operations back to the appropriate elements of the CA's management system.

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

Guidance on the use of technical experts

G.2.5 In order to ensure that the assessment team has at its disposal all necessary expertise, Technical Experts with specific knowledge regarding the subjects listed in G.2.4 a) ii) through v), but who do not satisfy all qualification criteria in G.2.2 for individual assessors, may be used to assist the assessment team. Such Technical Experts should at all times be responsible to the team leader and not function independently of the assessors in the team.

3.5 Guidance on the conformity assessment process

G.2.6 The independent body should review before the assessment what records are considered as confidential or sensitive by the CA such that the assessment team could not examine these records during the assessment of the CA. The independent body should judge whether the records that can be examined warrant an effective assessment. If the independent body concludes that an effective assessment is not warranted, the body should inform the CA that the assessment could take place only when the CA has accepted appropriate access arrangements to confidential or sensitive information.

G.2.7 The organisational structure of the CA could be such that the same activity is performed at a number of sites. The independent body undertaking the conformity assessment may opt for assessing a sample of these sites. In this case the independent body should maintain procedures that include the full range of issues below in the building of their sampling programme.

Prior to undertaking its first assessment based on sampling, the independent body should publish the sampling methodology that it employs. The procedures of the independent body should ensure that the initial review of the conformity assessment contract with the CA identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined in accordance with the provisions below.

Where a CA has a number of similar sites that support the provision of its certification services, the following requirements should be fulfilled.

- a) All sites of the CA are operating under the same CA's management system that is centrally administered and audited and subject to central management review.
- b) All sites have undergone internal auditing in accordance with the CA's internal auditing procedures.
- c) A representative number of sites have been sampled by the independent body, taking into account the requirements below:
 - i) the results of internal audits of head office and the sites,
 - ii) the results of management review,
 - iii) variations in the size of the sites,
 - iv) variations in the business purpose of the sites,
 - v) complexity of the CA's management system,
 - vi) complexity of the information systems at the different sites,
 - vii) variations in working practices,
 - viii) variations in activities undertaken,
 - ix) potential interaction with critical information systems or information systems processing sensitive information,
 - x) differing legal requirements.
- d) The sample should be partly selective based on the above in point c) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection.
- e) Every site of the CA that is subject to significant threats to assets, vulnerabilities or impacts should be included in the sampling programme.
- f) The surveillance programme should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the CA.
- g) In the case of a nonconformity being observed either at the head office or at a single site, the corrective action procedure should apply to the head office and all sites of the CA organisation.

The conformity assessment process described in G.2.9 below should address the CA's head office activities to ensure that a single management system applies to all sites and delivers central management at the operational level. The conformity assessment should address all the issues outlined above.

G.2.8 The process for conducting assessment should be based on the provisions of ISO 10011-1:1990.

G.2.9 The independent body should perform its conformity assessment of the CA's management system in at least two stages. For the purposes of this guidance, the two stages are described as "assessment stage

1" and "assessment stage 2". The key objectives of each, together with the minimum coverage, are described below.

The independent body should require that the applicant CA is able to demonstrate prior to commencement of the conformity assessment that the CA's management system is documented, implemented, and operational and can be shown to be operational.

Assessment stage 1

In this stage of the assessment, the independent body should obtain and review the documentation on the CA's management system. The objectives of assessment stage 1 are to provide a focus for planning of assessment stage 2 by gaining an understanding of the structure and extent of the CA's management system. Assessment stage 1 includes, but should not be restricted to, the document review. Other elements that could be included in assessment stage 1 are verification of records regarding legal entity, arrangements to cover liability, internal audits, and management review. The independent body and the CA should agree when and where assessment stage 1 is conducted. In every case, the document review should be completed prior to the commencement of assessment stage 2.

The results of assessment stage 1 should be documented in a written report. The independent body should review the report on assessment stage 1 for deciding on proceeding with assessment stage 2 and for selecting assessment team members with the necessary competence.

The independent body should make the CA aware of the further types of information and records that may be required for detailed verification during assessment stage 2.

Assessment stage 2

This stage always takes place at the site(s) of the CA. On the basis of observations documented in the report on assessment stage 1, the independent body drafts an assessment plan for the conduct of assessment stage 2.

The objectives of assessment stage 2 are:

- a) To confirm that the CA adheres to its own policies, objectives and procedures.
- b) To confirm that the implemented CA's management system conforms to the requirements of the standard and is achieving the CA's policy objectives.

G.2.10 ETSI TS 101 456 demands in clause 7.4.10 that the CA shall ensure compliance with legal requirements, specifically data protection. The maintenance and evaluation of legal compliance is the responsibility of the CA. The assessment team should restrict itself to checks and samples in order to establish confidence that the CA's management system has in place appropriate functions to ensure compliance with legislation relevant to its scope of operation.

The assessment team should verify that the CA has evaluated legal and regulatory compliance in all jurisdictions where it intends offering its services and can show that action has been taken in cases of non-compliance with relevant regulations.

G.2.11 It is acceptable that the CA combines the documentation of its CA's management system with the documentation of other management systems (such as quality, health and safety, and environment) as long as the CA's management system can be clearly identified together with the appropriate interfaces to the other systems.

G.2.12 The assessment of the CA's management system can be combined with assessments of other management systems. This combination is possible provided it can be demonstrated that the assessment satisfies all requirements for confirming that the CA meets the requirements for issuing Qualified Certificates. All elements of the CA's management system should appear clearly and be readily identifiable in the assessment reports. The quality of the assessment should not be adversely affected by the combination of the assessments.

G.2.13 In order to provide a basis for the decision to confirm that the CA meets the requirements for issuing Qualified Certificates, the independent body should require clear reports that provide sufficient information to make that decision.

Reports from the assessment team to the independent body are required at various stages in the assessment process. In combination with information held on file, these reports should at least contain:

CWA 14172-2:2001 (E)

- a) A description of the organisational structure of the CA, including the use made and organisational structure of other parties (subcontractors) that provide parts of the service.
- b) An account of the assessment including a summary of the document review.
- c) An account of the assessment of the CA's information security risk analysis.
- d) An account of the assessment of the CA's organisational reliability.
- e) Assessment time used and detailed specification of time spent on document review and assessment of the implementation of the CA's management system.
- f) Clarification of nonconformities.
- g) Assessment enquiries that have been followed, rationale for their selection, and the methodology employed.
- h) Recommendation by the assessment team to the independent body concerning the confirmation by the independent body whether the CA meets the requirements for issuing Qualified Certificates.

G.2.14 The individual or committee within the independent body that takes the decision on confirming that the CA meets the requirements should incorporate a level of knowledge and experience in all areas that is sufficient to evaluate the assessment processes and associated recommendations made by the assessment team. Confirmation that the CA meets the requirements should not be given in cases where unresolved nonconformities remain.

G.2.15 The documented statement confirming that the CA meets the requirements should be confined to declared scopes, activities and locations and should provide a short description of the CA's organisation including identification of the legal entity and, if applicable, identification of the part of the legal entity that provides the CA services. In addition, identification and locations should be provided and scope and activities should be described of other parties (subcontractors) that provide parts of the services.

G.2.16 The independent body should require the CA to which a statement of conformity is issued that the CA informs the independent body immediately of any significant changes in business policies, management, practices, processes, and controls particularly if such changes might affect the CA's ability to continue meeting the requirements or the manner in which they are met. Such changes may trigger the need for an advanced surveillance assessment or, in some cases, suspension of the statement of conformity until an assessment by the independent body can be made. The independent body should determine the appropriate course of action as soon as becoming aware of such a change in circumstances.

G.2.17 The independent body should define a programme of periodic surveillance and reassessment at sufficiently close intervals to verify that CAs continue to comply with the requirements. In most cases it is unlikely that a period greater than one year for periodic surveillance would be satisfactory. At each surveillance visit, the implementation of a part of the CA's management system should be verified in each of the areas addressed in ETSI TS 101 456 clauses 7.1 (Certification practice statement), 7.2 (Key management life cycle), 7.3 (Certificate management life cycle), 7.4 (CA management and operation) and 7.5 (Organizational).

In addition, a sample of certification records over the historical period since the previous assessment should be examined. The reports arising from surveillance during the period between the initial assessment and the reassessment should build up to cover in totality the subjects in the guidance on reporting in G.2.13 above. Surveillance reports should contain information on clearing of nonconformities revealed previously.

G.2.18 The independent body should have clear procedures laying down the circumstances and conditions in which the confirmation that the CA meets the requirements will be maintained. If on surveillance or reassessment nonconformities are found to exist, the CA should effectively correct such nonconformities within a time agreed. If correction is not made within the time agreed, confirmation of compliance with the requirements should be reduced, suspended or withdrawn. The time allowed to implement corrective action should be consistent with the severity of the nonconformity and the risk to the assurance of products or services meeting specified requirements.

3.6 Guidance on the use of ETSI TS 101 456

General guidance on the use of ETSI TS 101 456

G.2.19 Clause 5.4 of ETSI TS 101 456 identifies the requirements for CAs claiming conformity to either the qualified certificate policies for QCP public + SSCD or QCP public. CAs claiming conformity to the framework for other qualified certificate policies should be assessed against the requirements identified in clause 8.4 of ETSI TS 101 456.

G.2.20 Chapter 4 of ETSI TS 101 456 describes the general concepts of certification service provision. Clause 4.2 introduces the notion of 'Certification Authority'. The standard stipulates in sections 4.2 and 6.1 that the Certification Authority always maintains overall responsibility for the certification service, even if use is made of other parties (subcontractors) that provide parts of the service. The independent body should clearly identify the legal entity that issues the certificates. This legal entity is the CA and is the subject of the assessment. The CA should co-operate with the assessment team and should ensure the pursuit of assessment trails to review relevant documentation and records and to interview management and personnel of the CA and its possible subcontractors for the activity under consideration. In case the assessment team reports nonconformities, the CA is ultimately responsible for corrective actions.

In order to avoid duplication of assessments, the independent body, whilst recognising that the CA carries the ultimate responsibility for ensuring that the components of its service are conformant with the requirements of ETSI TS 101 456, may accept that the assessment of the overall service re-uses the results of separate assessments of service components. Different independent bodies could carry out the separate assessments of service components. The independent body confirming that the CA meets the requirements for issuing Qualified Certificates should obtain and review the assessment reports concerning the separately assessed service components and should examine the compliance of the involved independent bodies and their assessors with the provisions of this guidance.

Guidance on ETSI TS 101 456, clause 6.1 "Certification authority obligations"

G.2.21 The CA should define and document the practices and procedures used to address the requirements of the standard for the applicable qualified certificate policy. The management of the CA should ensure that this policy is understood, implemented and maintained at all levels of the organisational structure providing the services, including those parties (subcontractors) that provide parts of the services.

G.2.22 The CA should operate a management system in accordance with the elements of the standard and appropriate for the type, range and volume of the work performed. This CA's management system should be documented. Personnel throughout the organisational structure providing the services should use the relevant documentation in the carrying out of their tasks. The management of the CA should ensure effective implementation of the documented procedures and instructions.

G.2.23 The CA's management system documentation should contain an organisation chart showing lines of authority, responsibility and allocation of functions. The qualification requirements and terms of reference for each function should be documented. The names of the individuals to which the functions have been allocated should be documented. The organisation chart and qualification requirements should identify and cover those parties (subcontractors) that provide parts of the services.

Guidance on ETSI TS 101 456, clause 7 "Requirements on CA practice"

G.2.24 Clause 7 of ETSI TS 101 456 consists of a number of sub-clauses starting with the words "The CA shall ensure that..." followed by a specific requirement. This in turn is followed by detailed requirements highlighting aspects of the specific requirement. Where necessary, notes provide explanations of specific or detailed requirements. It is the task of the assessment team to verify the CA's compliance with the detailed requirements such that compliance with the specific requirement can be established.

G.2.25 The introduction of clause 7 states that the policy requirements are not meant to imply any restrictions on charging for CA services. However, clause 7.5.1 a) requires that the policies and procedures under which the CA operates shall be non-discriminatory. Differences in charging for the services by a CA to different subscribers or subscriber groups could cause discrimination.

G.2.26 Clause 7.1 requires the CA to have and make available a certification practice statement (CPS). A CPS is a detailed statement by a CA as to its practices that potentially needs to be understood by subscribers and certificate users (relying parties). ETSI TS 101 456 makes no requirements as to the structure of the CPS. In the interest of international harmonisation, CAs should be encouraged to adopt the CPS structure described in document RFC 2527 "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework."

G.2.27 Clauses 7.2.1 and 7.2.2 define requirements for the CA key generation device and the device holding the CA private signing key. The assessment team deployed by an independent body to assess a CA's management system should not be expected to be equipped for evaluating such devices. The assessment team should verify whether the evidence presented by the CA of compliance of the devices with the requirements is sufficient. Such evidence could consist of evaluation reports and certificates issued by an independent body that is generally recognized as competent in carrying out this type of IT security evaluation.

G.2.28 Clause 7.5.1 c) requires that the CA is a legal entity. If a CA is part of a larger entity, e.g. a department of a company or institution, the confirmation of conformity should only be granted to the entire legal entity. In such a situation, the structure of the entire legal entity may be subject to assessment by the assessment team of the independent body in order to pursue specific audit trails and/or review records relating to the CA. The part of the legal entity that forms the actual CA may trade under a distinctive name, which should appear on the statement confirming conformity.

CAs who are part of government, or are governmental departments, will be deemed to be legal entities on the basis of their governmental status. The status and structure of such body should be formally documented and the body should comply with all requirements of the standard.

G.2.29 Clause 7.5.1 e) requires that CA's have arrangements to cover liabilities. Such arrangements usually take the form of a professional indemnity insurance. The assessment team deployed by the independent body is not required to judge the coverage provided by such insurance. However, the assessment team should verify whether deductibles stated in the insurance policy as payable by the insured remain within the limits of the financial resources of the CA.

G.2.30 The policies and procedures for the resolution of complaints and disputes, referred to in clause 7.5.1 h), should ensure that all complaints and disputes are dealt with in a constructive and timely manner. Where operation of such procedures has not resulted in the acceptable resolution of the matter or where the proposed procedure is unacceptable to the complainant or other parties involved, the procedures of the CA should provide for an appeals process. The appeals procedure should include provision for the following:

- a) The opportunity for the appellant to formally present its case;
- b) Provision of an independent element or other means to ensure the impartiality of the appeals process;
- c) Provision to the appellant of a written statement of the appeal findings including the reasons for the decisions reached.

G.2.31 Clause 7.5.2 requires independence of the CA for its decisions relating to the services concerning granting and revocation of qualified certificates. If the services of the CA are carried out by an entity that is part of a larger entity, the links of the CA with other parts of the larger entity should be clearly defined and should demonstrate that no conflict of interest exists. Relevant information on activities performed by the other parts of the larger entity should be documented. The management of the larger entity should provide documented insurance that the CA is authorised to operate independently regarding decisions relating to granting and revocation of qualified certificates.

Note: An interpretation of the requirement in clause 7.5.2 that the parts of the CA concerned with certificate generation and revocation management are independent implies that those who make the certification / revocation decision should not have participated in the registration of the certificate concerned.

It is recommended that this interpretation should be clarified in future editions of ETSI TS 101 456.

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.

ETSI TS 101 456 V1.1.1 (2000-12) *Policy requirements for certification authorities issuing qualified certificates*

Bibliography

The following material provides supporting information.

- BSI IT-Grundschutzhandbuch "Bundesamt für Sicherheit in der Informationstechnik - IT-Grundschutzhandbuch Standard-Sicherheitsmaßnahmen", January 2000.
- 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."
- EA-6/01 "EA Guidelines on the Application of EN 45011", June 1999
- EA-7/01 "EA Guidelines on the Application of EN 45012", February 1998.
- EA-7/03 "EA Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems", February 2000.
- EN 45010:1998: "General Requirements for Assessment and Accreditation of Certification/Registration Bodies" (ISO/IEC Guide 61:1996)
- EN 45011:1998: "General Requirements for Bodies Operating Product Certification Systems" (ISO/IEC Guide 65:1996)
- EN 45012:1998: "General Requirements for Bodies Operating Assessment and Certification/Registration of Quality Systems" (ISO/IEC Guide 62:1996)
- EN 45020:1998: "Standardization and Related Activities - General Vocabulary; Corrected 1998-02-26" (ISO/IEC Guide 2:1996)
- ISO 9000:2000: "Quality management systems - Fundamentals and vocabulary."
- ISO 9000-3:1997: "Quality management and quality assurance standards - Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software."
- ISO 10011-1:1990 "Guidelines for auditing quality systems - Part 1: Auditing."
- ISO 10011-2:1991 "Guidelines for auditing quality systems - Part 2: Qualification criteria for quality system auditors."
- ISO 10011-3:1991 "Guidelines for auditing quality systems - Part 3: Management of audit programmes."
- 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."

o - o - o