ETSI TR 103 123 V1.1.1 (2012-11)

Technical Report

Electronic Signatures and Infrastructures (ESI); Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates

Reference

DTR/ESI-000118

Keywords

e-commerce, public key, security, TLS/SSL
certificates

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

ETSI ESI issued TS 102 042 [i.1] that specified generic policy requirements for the operation and management practices of certification authorities issuing public key certificates. TS 102 042 [i.1] generalises the principles specified in TS 101 456 [i.3] to make it generally applicable to certification authorities independent of the form of public key certificate.

Examples of such certificates are those used for securing web sites.

The Certification Authority/Browser (CAB) Forum has specified guidelines for the "Issuance and Management of Publicly-trusted Certificates"(referred to in the present document as Baseline Requirements Guidelines - BRG [i.2]) to verify that the public key certificates used for securing access to web sites are issued in a secure manner. The BRG [i.2] requires that the general operation of the Certification Authority is secure and indicates that conformance to TS 102 042 [i.1] as a means of demonstrating that this requirement is met.

The primary purposes of public key certificates issued in accordance with the BRG [i.2] are to:

1) identify the legal entity that controls a Web or service site; and

2) enable encrypted communications with that site.

The Transport Layer Security (TLS) protocols [i.8] and the earlier equivalent Secure Socket Layer (SSL) protocol makes use of public key certificates to secure access to web sites and services.

The present document provides guidance for assessment of CAs issuing Publicly trusted TLS/SSL Certificates against TS 102 042 [i.1] and CAB Forum BRG [i.2].

1 Scope

The present document provides guidance on the assessment of Certification Authorities issuing Certificates primarily for use with Transport Layer Security (TLS) protocol [i.8] or the earlier equivalent Secure Socket Layer (SSL) protocol based on TS 102 042 [i.1] and the CA/Browser Forum Baseline Requirements for the issuance and the management of publicly-trusted certificates, (BRG) [i.2]. The present document is aimed at providing guidance to Certification Authorities issuing Publicly trusted TLS/SSL certificates to be aware of how they may be assessed and for auditors in carrying out assessment of the conformance of such certification authorities according to TS 102 042 [i.1].

Annex A provides a checklist that may be used by auditors in carrying out an audit based on these guidelines.

Annex B provides a suggested framework for the final audit report.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.2] Baseline requirements for the Issuance and Management of Publicly-trusted Certificates, CA Browser Forum.

NOTE: TS 102 042 [i.1] and BRG [i.2] are main references, all other references are as called up by these two documents.

[i.3] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.4] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[i.5] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.6] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

[i.7] ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management".

[i.8] IETF RFC 5246: "The Transport Layer Security Protocol", Version 1.2.

[i.9] ETSI TS 103 090: "Electronic Signatures and Infrastructures (ESI); Conformity Assessment for Trust Service Providers issuing Extended Validation Certificates".

[i.10] ETSI TS 119 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General Requirements and Guidance".

[i.11] Network and Certificate System Security Requirements, CA/Browser Forum.

[i.12] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

3 Definitions, notation and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 042 [i.1] and BRG [i.2] apply.

3.2 Notation

Text copied from TS 102 042 [i.1] is italicised.

3.3 Abbreviations

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

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CAB	Certificate Authority/Browser
CM	Cryptographic Module
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EVCG	Extended Validation Certificate Guidelines
ICT	Information and Communications Technology
IS	Information Security
ISO	International Organization for Standardization
NCP	Normalized Certificate Policy
NetSec-CAB	Network Security Requirements- CA/Browser Forum
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy
PTC	Publicly-Trusted Certificate

NOTE: Within the context of the present document PTC is used synonymously with DVC and OVC.

PTC-BR	Publicly-Trusted Certificate Policy-Baseline Requirements

NOTE: Within the context of the present document PTC-BR is used synonymously with DVCP and OVCP.

SSL	Secure Socket Layer
TLS	Transport Layer Security

TLS/SSL Transport Layer Security/Secure Socket Layer

NOTE: RFC 5246 [i.8] or earlier equivalent Secure Socket Layer protocol.

TSP Trust Service Provider

NOTE: Within the context of the present document CSP and TSP are used synonymously with Certification Authority (CA).

4 Overview

The present document is intended to be used by Auditors as a guidance to assess the compliance of a CA with T 102 042 [i.1] and for CAs to clarify the requirements to be met.

Auditors should ascertain, for each of the present document clauses, that provisions in the corresponding TS 102 042 [i.1] or BRG [i.2] clauses are complied with by the CA. In each of the following clauses, additional provisions may be specified that Auditors should implement.

5 Policies for issuing publicly-trusted certificates

5.1 Overview

The TS 102 042 [i.1] policies relevant to use of PTC (DVC and/or OVC) are:

1) *A Domain Validation Certificate Policy (DVCP): NCP enhanced incorporating requirements of the BRG [i.2] as applicable to domain validation certificates.*

2) *An Organizational Validation Certificate Policy (OVCP): NCP enhanced to incorporate requirements in BRG [i.2] as applicable to organizational validation certificates.*

Auditors should check for available policy documentation (e.g. CP or CPS) and verify that this is in line with the PTC-BR requirements. Auditors should verify the OIDs of the issued certificates as appropriate for the relevant certificate policy as stated in the CP or CPS.

5.2 Identification

A CA is required to include the identifier(s) for the certificate policy (or policies) being supported in the terms and conditions made available to subscribers and relying parties to indicate its claim of conformance. The OIDs used may include the OIDs specified in TS 102 042 [i.1] clause 5.2 items f) and g).

5.3 User Community and Applicability

The policy requirements are applicable to Certificates for use with Transport Layer Security protocol [i.8] or the earlier equivalent Secure Socket Layer protocol. Auditors should check that the primary purpose of the certificate is as stated in the certificate policy according to clause 5.3.2 of TS 102 042 [i.1].

5.4 Conformance

a) Conformity Assessment should be carried out in line with TS 103 090 [i.9] (which is based on TS 119 403 [i.10]) and sections 17.1 to 17.6 of BRG [i.2].

b) The auditor should check that regular quality assessment self audits are carried out as in section 17.6 of BRG [i.2].

c) The auditor should verify that delegated third party requirements are met as in section 14.2 of BRG [i.2].

6 Obligations, warranties and liability

6.1 Certification authority obligations and warranties

a) Auditors should verify that the CP or CPS included in the certificate covers the requirements indicated in the PTC-BR.

b) Auditors should verify the CPS, the subscriber agreements and the third party contracts to check its obligations according to clause 6.1 of TS 102 042 [i.1] and sections 7.1.2 and 14.2 of BRG [i.2].

6.2 Subscriber obligations

a) Auditors should verify the subscriber agreements in order to check that the obligations indicated in clause 6.2 a), b), c), d), h), i) and j) of TS 102 042 [i.1] are addressed:

   i) Regarding clause 6.2 i) and j) of TS 102 042 [i.1] (compromise of the subjects private key or the CA) Auditors should verify the procedures to discontinue the usage of the certificate upon information of a CA compromise as indicated in clause 6.2 j).

b) Auditors should also take account of the requirements in:

   i) TS 102 042 [i.1], clauses 7.3.1 item m) and 7.3.4.

   ii) BRG [i.2], section 10.3.

   iii) For revocation procedures, clause 7.3.6 of TS 102 042 [i.1].

   iv) In relation to algorithm and key sizes (item d), Appendix A of BRG [i.2] and Annex A of TS 102 176-1 [i.4] applies. In case of conflict, Appendix A of BRG [i.2] prevails.

6.3 Information for Relying parties

a) Auditors should verify the CA's terms and conditions (see clause 7.3.4):

   i) To check inclusion of specific revocation/suspension policy procedure (see clause 7.3.6 checks on revocation mechanisms).

   ii) To inspect reporting and investigation of issues for example:

      1) To check the terms and conditions and find the contact details in case of an incident, question or complaint.

      2) To check the terms and conditions are published at the company's website and verify the availability of the site.

b) Auditors should check section 13.1.2 of BRG [i.2] related to the problem reporting and response capability.

6.4 Liability

a) Auditors should verify the procedures to provide assurance of minimum levels of liability, insurance coverage, etc.

b) Auditors should also check that disclaimers or limitations of liability are in accordance with applicable laws according to section 18 of BRG [i.2] related to Publicly trusted TLS/SSL certificates.

7 Requirements on CA practice

The CA shall implement the controls that meet the following requirements.

The present document includes the provision of services for registration, certificate generation, dissemination, revocation management and revocation status (see clause 4.2).

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met.

7.1 Certification practice statement

Auditors should verify the following:

a) The CA's certification practice statement addressing all the requirements identified in the applicable certificate policy regarding Publicly trusted TLS/SSL certificates, according to clause 7.1 of TS 102 042 [i.1].

b) The CA's certification practice statement including requirements in section 8.2.1 of BRG [i.2].

c) The identification of policy and practice documents and other documentation placing obligations on external organizations/subcontractors (including registration authorities) as indicated in clause 7.1 c) of TS 102 042 [i.1].

d) The CA's availability of its certification practice statement, and other relevant documentation, as necessary to assess conformance to the certificate policy according to clause 7.1 d) of TS 102 042 [i.1]. The public disclosure of the CPS, policies and procedures through an appropriate and accessible online means that is available 24×7 on a regular basis as indicated in section 8.2.2 of BRG [i.2].

e) CAs and Publicly trusted TLS/SSL certificates issuing CA hierarchy.

f) The CA's commitment with the BRG [i.2] as indicated in section 8.3.

g) The CA's measures to ensure that the described certification practices are properly implemented with senior management taking responsibility for its implementation according to clause 7.1 g) of TS 102 042 [i.1].

NOTE: The disclosures may be structured in accordance with RFC 3647 [i.5] as indicated in section 8.2.2 of BRG [i.2]. See Annex C of TS 102 042 [i.1].

h) [PTC-BR]: the provisions specified in BRG [i.2] sections 8.2.1, 8.2.2 and 8.3.

7.2 Public key infrastructure - Key management life cycle

7.2.1 Certification authority key generation

a) Auditors should verify the CA previous auditor's report on the key generation ceremony as described in section 17.7 of the BRG [i.2]. Also, the certificate signing algorithms used should be checked to comply with TS 102 176-1 [i.4] and Appendix A of BRG [i.2] that will prevail in case of a conflict.

NOTE: The contents of a CA previous auditor's report may include, for example, the date and time of the event, names and roles of the participants of the ceremony, identifier for the keys that were generated, the identifier for the systems used for generation and the location.

b) Auditors should verify the use of a cryptographic device in line with clause 7.2.1 b) sub-item iii, iv or v of TS 102 042 [i.1].

c) The CA key generation should be audited according to clause 7.2.1 a) and c) of TS 102 042 [i.1].

d) Auditors should verify that the documentation providing evidence of the key generation ceremony complies with BRG [i.2] Appendix A (1) and (2) and 17.7.

7.2.2 Certification authority key storage, backup and recovery

a) Auditors should check CA procedures to verify that CA private keys remain confidential and maintain their integrity through use of a cryptographic device indicated in clause 7.2.2 a) sub-items iii, iv or v of TS 102 042 [i.1] and section 16.6 of BRG [i.2].

b) Auditors should verify, if applicable, backups and recovery procedures of the CA private keys as indicated in clause 7.2.2 items c) and d) of TS 102 042 [i.1]. If the CA private keys are backed up outside the secure device, the CA private keys should be protected according to clause 7.2.2 b) of TS 102 042 [i.1].

c) Auditors should also verify that reports exist demonstrating that these procedures have been complied with.

7.2.3 Certification authority public key distribution

NOTE: It is assumed to be the responsibility of suppliers of web browser/operating system software to distribute stores of root certificates securely to end users. It is expected that the web browser suppliers will check the root certificates before its distribution in accordance with the CAs.

The auditor should check that, where possible, the CA verifies that the correct certificate is being used by the web browser software prior confirming to the supplier for the distribution of root certificates.

7.2.4 Key escrow

Not applicable.

NOTE: Publicly trusted TLS/SSL Certificates are not expected to be escrowed.

7.2.5 Certification authority key usage

Auditors should check practices to verify that CA private keys are not used inappropriately as indicated in clause 7.2.5 of TS 102 042 [i.1].

7.2.6 End of CA key life cycle

Auditors should check practices to verify that CA private signing keys are not used beyond the end of their life cycle as indicated in clause 7.2.6 of TS 102 042 [i.1], and recording of life cycle events as in section 15.2 (1) (a) of BRG [i.2].

7.2.7 Life cycle management of cryptographic hardware used to sign certificates

Auditors should verify the CA has properly checked the security of cryptographic hardware throughout its lifecycle as per clause 7.2.7 of TS 102 042 [i.1] and recording of life cycle events as in section 15.2 (1) (b) of BRG [i.2].

7.2.8 CA provided subject key management services

a) If applicable, auditors should check CA procedures to verify that any subject keys, are generated securely and the secrecy of the subject's private key is assured as stated in BRG [i.2], section 10.2.4.

b) In relation to algorithm and key sizes, Appendix A of BRG [i.2] and Annex A of TS 102 176-1 [i.4] applies. In case of conflict, Appendix A of BRG [i.2] prevails.

7.2.9 Secure user devices preparation

Not applicable.

7.3 Public key infrastructure - Certificate Management life cycle

7.3.1 Subject registration

The CA shall ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.

a) Auditors should verify that the CSP registration procedures follow the BRG [i.2] requirements of sections 10 and 11 regarding the request and verification of the information and clause 7.3.1 items a), c), d), h), i), j), k), l), m), n), p) and q) of TS 102 042 [i.1] for every registration.

b) Information used from a previous registration should meet the requirements indicated in section 11 of BRG [i.2].

c) Auditors should check the applicant registration records and verify the requirements of item j of clause 7.3.1 of TS 102 042 [i.1] are met.

d) Auditors should verify that the records regarding these Publicly trusted TLS/SSL certificates are retained at least seven years after any certificate based on that documentation ceases to be valid as stated in BRG [i.2], section 15.3.2.

e) Regarding warranties by the CA, auditors should check section 7.1 of BRG [i.2].

7.3.2 Certificate renewal, rekey and update

Auditors should check the CA procedures to verify that requests for certificates issued to a subject who has already previously been registered are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes according to clause 7.3.2 of TS 102 042 [i.1] and section 15.2 item (2) of BRG [i.2].

7.3.3 Certificate generation

a) Auditors should check the CA procedures to verify that the CA issues certificates securely to maintain their authenticity according to clause 7.3.3 of TS 102 042 [i.1] and section 9 of BRG [i.2].

b) Auditors should check that certificates issued by a root CA address requirements specified in section 12 of BRG [i.2].

c) The certificate content should be checked against Appendix B of BRG [i.2].

7.3.4 Dissemination of Terms and Conditions

Auditors should check that the CA's terms and conditions are made available to subscribers and relying parties as indicated in section 10.3 of BRG [i.2] and clause 7.3.4 of TS 102 042 [i.1].

7.3.5 Certificate dissemination

Auditors should check that that certificates issued by the CA are made available as necessary to subscribers, subjects and relying parties as indicated in clause 7.3.5 of TS 102 042 [i.1].

7.3.6 Certificate revocation and suspension

Auditors should verify that:

a) the CA revocation procedures follow sections 13.1and 13.2 of BRG [i.2] and clause 7.3.6 of TS 102 042 [i.1];

b) the CA revocation entries on a CRL or OCSP are not removed until the expiration date of the revoked certificate as per section 13.2 of BRG [i.2];

c) the CA can accept and respond to revocation or suspension requests on a 24×7 basis as indicated in section 13.1 of BRG [i.2];

d) the CA follow the requirements of BRG [i.2], section 13.2 related to the online 24×7 repository mechanism for automatic checking of the current status of the certificate;

e) the CA follow the revocation events indicated in section 13.1 of BRG [i.2];

f) the CA provides problem reporting and response capability as in section 13.1 of BRG [i.2].

7.4 CA management and operation

Auditors should check that the CA has implemented, documented and tested the requirements specified in NetSec-CAB [i.11].

7.4.1 Security management

Auditors should review if the CA has implemented and documented a system or systems for information security management.

NOTE: See ISO/IEC 27001 [i.6] and ISO/IEC 27002 [i.7] for requirements and a code of practice for information security management.

Auditors should check that administrative and management security procedures of the CA are applied as indicated in sections 14.2 and 16 of BRG [i.2] and clause 7.4.1 of TS 102 042 [i.1].

7.4.2 Asset classification and management

Auditors should check that CA assets and information receive an appropriate level of protection as indicated in clause 7.4.2 of TS 102 042 [i.1].

7.4.3 Personnel security

Auditors should check that personnel and hiring practices enhance and support the trustworthiness of the CA's operations as per section 14.1 of BRG [i.2] and clause 7.4.3 of TS 102 042 [i.1].

7.4.4 Physical and environmental security

Auditors should check that physical access to critical services of the CA is controlled and physical risks to its assets minimized according to clause 7.4.4 of TS 102 042 [i.1] and section 16.5 item (1) of BRG [i.2].

7.4.5 Operations management

Auditors should check that the CA systems are secure and correctly operated, with minimal risk of failure according to clause 7.4.5 of TS 102 042 [i.1] and sections 15.2 and 16.5 items (4 and 5) of the BRG [i.2].

7.4.6 System Access Management

Auditors should check that the CA system access is limited to properly authorized individuals according to clause 7.4.6 of TS 102 042 [i.1].

7.4.7 Trustworthy systems deployment and maintenance

Auditors should check that the CA uses trustworthy systems and products that are protected against modification according to clause 7.4.7 of TS 102 042 [i.1] and section 16.5 item (2) of BRG [i.2].

7.4.8 Business continuity management and incident handling

Auditors should check a business continuity plan exists in the event of a disaster. Auditors should check that this plan covers compromise of the CA's private signing key and verify that the CA operations are restored as soon as possible as indicated in clause 7.4.8 of TS 102 042 [i.1] and section 16.4 of BRG [i.2].

7.4.9 CA termination

Auditors should check CA procedures to verify that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services as covered by the certificate policy, and that they verify continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings as per clause 7.4.9 of TS 102 042 [i.1].

7.4.10 Compliance with Legal Requirements

Auditors should check CA compliance with legal requirements, including the Data Protection Directive as per clause 7.4.10 of TS 102 042 [i.1] and also check section 8.1 of BRG [i.2].

7.4.11 Recording of information concerning certificates

a) Auditors should check that all relevant information concerning a certificate is retained for an appropriate period in particular for the purpose of providing evidence of certification for the purposes of legal proceedings, as per section 15 of the BRG [i.2] and clauses 7.4.11 and 7.3.1 of the TS 102 042 [i.1].

b) Sections 15.1 and 15.2 of BRG [i.2] apply and 15.3 of BRG [i.2] requires that records are retained for at least seven years after any Certificate based on that documentation ceases to be valid. National legal requirements for retention of records for evidence should also be taken into account.

7.5 Organizational

Auditors should check CA procedures to verify that the organization is reliable as per clause 7.5 of TS 102 042 [i.1].

7.6 Additional Requirements

7.6.1 Testing

Auditors should check the availability of testing web pages as in Appendix C of BRG [i.2].

7.6.2 Cross certificates

Auditors should check that the CA discloses all the Cross Certificates as per section 8.4 of the BRG [i.2].

8 Framework for the definition of other certificate policies

8.1 Certificate Policy Management

Auditors should check that the certificate policy is effective as per clause 8.1 of TS 102 042 [i.1].

8.2 Additional requirements

Auditors should check that the subscribers and relying parties are properly informed as per clause 8.2 of TS 102 042 [i.1].

8.3 Conformance

Auditors should check that the CA claims conformance to the TS 102 042 [i.1] and BRG [i.2].

Annex A: Assessment Guidance Checklist

NOTE 1: The following table identifies particularly to a publicly-trusted TLS/SSL certificates assessment. Text quoted from TS 102 042 [i.1]/BRG [i.2] documents are italicised. Additional text is for guidance only and are not normative requirements. Reference should be made to TS 102 042 [i.1] and BRG [i.2] for the precise requirements.

NOTE 2: The audit may use the findings column to record findings which checking the requirement. Requirements which are met or failed to be met may be indicated by OK, or Not OK followed by further information.

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
5.1	Overview	The TS 102 042 [i.1] policies relevant to use of PTC are: *1) A Domain Validation Certificate Policy (DVCP): NCP enhanced incorporating requirements of the BRG [i.2] as applicable to domain validation certificates.* *2) An Organizational Validation Certificate Policy (OVCP): NCP enhanced incorporating requirements in BRG [i.2] as applicable to organizational validation certificates.*	
		BRG [i.2] Requirement	
		8.2	
		Assessment Guidance	
		Auditors should check for available policy documentation (e.g. CP or CPS) and verify that this is in line with the PTC-BR requirements. Auditors should verify the PTC OIDs.	
Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**

5.2	Identification	The identifiers for CP or CPS relevant to the PTC are:
		f) DVCP: Domain Validation Certificate Policy
		itu-t(0) identified-organization(4) etsi(0)
		other-certificate-policies(2042)
		policy-identifiers(1) dvcp (6)
		g) OVCP: Organizational Validation Certificate Policy
		itu-t(0) identified-organization(4) etsi(0)
		other-certificate-policies(2042)
		policy-identifiers(1) ovcp (7)
		By including this object identifiers in a certificate the CA claims conformance to the identified certificate policy
		NOTE: Either CAs own OIDs and/or ETSI OIDs and/or CAB OIDs as indicated in EVCG [i.12] for d and e and BRG [i.2] for f and g can be used.	

		BRG [i.2] Requirement	
		Assessment Guidance	
		The OIDs used may include the OIDs specified in TS 102 042 [i.1] clause 5.2 item f) and g).	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
5.3	User community and applicability	5.3.2	
		BRG [i.2] Requirement	
		8.1	
		Assessment Guidance	
		Auditors should check that the primary purpose of the certificate, as stated in the certificate policy and/or the CPS, meets provisions as in clause 5.3.2 of the TS 102 042 [i.1] and as in section 8.1 of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
5.4	Conformance	*The CA shall only claim conformance to the present document as applied in the certificate policy (or policies) identified in the certificate that it issues.*	
		BRG [i.2] Requirement	
		14.2 and 17.1 to 17.6	
		Assessment Guidance	
		Auditors should verify the CA claims conformance to the CP or CPS and meet all the requirements according to clauses 5.4.1 and 5.4.2 of TS 102 042 [i.1] and sections 17.1 to 17.6 and 14.2 of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
6.1	CA Obligations	*The CA has the responsibility for conformance with the procedures prescribed in this policy, even when the CA functionality is undertaken by sub-contractors.* *The CA shall provide all its certification services consistent with its certification practice statement.*	
		BRG [i.2] Requirement	
		7.1.2 and 14.2	
		Assessment Guidance	
		Auditors should verify the CP or CPS included in the certificate covers the requirements of the PTC-BR, the subscriber agreements and the third party contracts to check its obligations according to clause 6.1 of TS 102 042 [i.1] and sections 7.1.2 and 14.2 of BRG [i.2].	
Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**
6.2	Subscriber obligations	*The CA shall oblige through agreement the subscriber to address all the following obligations. If the subject and subscriber are separate entities, the subscriber shall make the subject aware of those obligations applicable to the subject.*	
		BRG [i.2] Requirement	
		10.3 and Appendix A	
		Assessment Guidance	
		Auditors should verify the subscriber agreements in order to check that the obligations indicated in clause 6.2 a), b), c), d) , h), i) and j) of TS 102 042 [i.1] are addressed: Auditors should verify the procedures to discontinue the usage of the certificate upon information of a CA compromise as indicated in clause 6.2 j) of TS 102 042 [i.1]. Auditors should take account of the requirements in: • TS 102 042 [i.1], clauses 7.3.1 item m) and 7.3.4. • BRG [i.2], section 10.3. • For revocation procedures, clause 7.3.6 of TS 102 042 [i.1]. • In relation to algorithm and key sizes (item d), Appendix A of BRG [i.2] and TS 102 176-1 [i.4] applies. In case of conflict, Appendix A of BRG [i.2] prevails.	

Nº	Subject	TS 102 042 [i.1] Requirements	Findings
6.3	Information for relying party	*The terms and conditions made available to relying parties (see clause 7.3.4) shall include a notice that if it is to reasonably rely upon a certificate* *NOTE: Depending on CA's practices and the mechanism used to provide revocation status information, there may be a delay of up to 1 day in disseminating revocation status information.* See also TS 102 042 [i.1], clauses 7.3.4 and 7.3.6 h) iii)	
		BRG [i.2] Requirement	
		13.1.2, 16.4	
		Assessment Guidance	
		Auditors should verify the CA's terms and conditions (see clause 7.3.4): • To check inclusion of specific revocation /suspension policy procedure (see 7.3.6 checks on revocation mechanisms). • To inspect reporting and investigation of issues for example: - To check the terms and conditions and find the contact details in case of an incident, question or complaint. - To check the terms and conditions are published at the company's website and verify the availability of the site. Auditors should also check section 13.1.2 of BRG [i.2] related to the problem reporting and response capability. Auditors would also check that provisions in BRG [i.2], clause 16.4 that relates to Relying Parties are met.	
Nº	**Subject**	**TS 102 042 [i.1] Requirements**	**Findings**
6.4	Liability	*The CA shall specify any disclaimers or limitations of liability in accordance with applicable laws.*	
		BRG [i.2] Requirement	
		Section 18	
		Assessment Guidance	
		Auditors should verify the procedures to provide assurance of minimum levels of liability, insurance coverage, etc. according to section 18 of BRG [i.2] related to the publicly-trusted certificates.	

Nº	Subject	TS 102 042 [i.1] Requirements	Findings
7.1	CPS	*The CA shall have a statement of the practices and procedures.* See also clause 7.1 and Annex C	
		BRG [i.2] Requirement	
		8.2.1, 8.2.2, 8.3 and Appendix A.	
		Assessment Guidance	
		Auditors should verify the following: a) The CA's certification practice statement addressing all the requirements identified in the applicable certificate policy regarding PTC, according to clause 7.1 of TS 102 042 [i.1]. b) The CA's certification practice statement including requirements in section 8.2.1 of BRG [i.2]. c) The identification of policy and practice documents and other documentation placing obligations on external organisations/subcontractors (including registration authorities as indicated in clause 7.1 c) of TS 102 042 [i.1]. d) The CA's availability of its certification practice statement, and other relevant documentation, as necessary to assess conformance to the certificate policy according to clause 7.1 d) of TS 102 042 [i.1]. The publicly disclosure of the CPS, policies and procedures through an appropriate and accessible online mean that its available 24×7 on a regular basis as indicated in section 8.2.2 of BRG [i.2]. e) CAs and Publicly trusted TLS/SSL certificates issuing CAs hierarchy. f) The CA's commitment with the BRG [i.2] as per section 8.3. g) Processes for managing and reviewing the CPS as specified in TS 102 042 [i.1], clause 7.1 item h) and BRG [i.2], section 8.2.1". NOTE: The disclosures may be structured in accordance with RFC 3647 [i.5]; see Annex C of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.1	CA Key Generation	*The CA shall ensure that CA keys are generated in controlled circumstances.*	
		BRG [i.2] Requirement	
		17.7 and Appendix A	
		Assessment Guidance	
		Auditors should verify the CA Auditor's report on the key generation ceremony as describing in section 17.7 of the BRG [i.2]. Also, the certificate signing algorithms used should be checked to comply with the TS 102 176-1 [i.4] and Appendix A of BRG [i.2] that will prevail in case of a conflict. NOTE 1: Auditors should verify the use of a cryptographic device in line with 7.2.1 b) sub-item iii, iv or v of TS 102 042 [i.1]. NOTE 2: Auditors should check the CA key generation according to clause 7.2.1 a) and c) of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.2	CA key storage, backup and recovery	*The CA shall ensure that CA private keys remain confidential and maintain their integrity.* TS 102 042 [i.1] sections 7.2.2 a), b), c) and d).	
		BRG [i.2] Requirement	
		16.6	
		Assessment Guidance	
		Auditors should check CA procedures to verify that CA private keys remain confidential and maintain their integrity through use of a cryptographic device indicated in clause 7.2.2 a) sub-items iii, iv or v of TS 102 042 [i.1] and section 16.6 of BRG [i.2]. Auditors should also verify, if applicable, backups and recovery procedures of the CA private keys as indicated in clause 7.2.2 items c) and d) of TS 102 042 [i.1]. If the CA private keys are backed up outside the secure device, the CA private keys should be protected according to clause 7.2.2 b) of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.3	CA public key distribution	*The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		NOTE: Auditors should check that, where possible, the CA verifies that the correct certificate is being used by the web browser software prior confirming to the supplier for the distribution of root certificates.	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.5	CA Key usage	*The CA shall ensure that CA private signing keys are not used inappropriately.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check practices to verify that CA private keys are not used inappropriately as indicated in clause 7.2.5 of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.6	End of CA key life cycle	*The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle.*	
		BRG [i.2] Requirement	
		15.2	
		Assessment Guidance	
		Auditors should check practices to verify that CA private signing keys are not used beyond the end of their life cycle as indicated in clause 7.2.6 of TS 102 042 [i.1], and recording of life cycle events as in section 15.2 (1) (a) of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.7	Security of Cryptographic Module (CM) during its lifetime.	*The CA shall ensure the security of cryptographic device throughout its lifecycle.*	
		BRG [i.2] Requirement	
		15.2	
		Assessment Guidance	
		Auditors should verify the CA has properly checked the security of cryptographic hardware throughout its lifecycle as per clause 7.2.7 of TS 102 042 [i.1] and recording of life cycle events as in section 15.2 (1) (b) of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.8	CA provided subject key management services	*The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured.*	
		BRG [i.2] Requirement	
		10.2.4 and Appendix A	
		Assessment Guidance	
		If applicable, auditors should check CA procedures to verify that any subject keys, are generated securely and the secrecy of the subject's private key is assured. In relation to algorithm and key sizes, Appendix A of BRG [i.2] and TS 102 176-1 [i.4] apply.	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.3.1	Subject registration	*The CA shall ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.*	
		BRG [i.2] Requirement	
		7.1, 10, 11 and 15.3.2	
		Assessment Guidance	
		Auditors should verify that the CSP registration procedures follow the BRG [i.2] requirements of sections 10 and 11 regarding the verification of the information and clause 7.3.1 items a), c), d), h), i), j), k), l), m), n), p) and q) of TS 102 042 [i.1] for every registration. Information used from a previous registration should meet the requirements indicated in section 11 of BRG [i.2]. Auditors should check the applicant registration records and verify the requirements of item j of clause 7.3.1 of TS 102 042 [i.1] are met. Auditors should verify that the records regarding the publicly trusted certificates are retained at least seven years after any certificate based on that documentation ceases to be valid as stated in BRG [i.2], section 15.3.2. Regarding warranties by the CA, auditors should check section 7.1 of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.3.2	Certificate renewal	The CA shall ensure that requests for certificates issued to a subject who has previously been registered with the same CA are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes. NOTE: The subscriber may, if the CA offers this service, request a certificate renewal for example where relevant attributes presented in the certificate have changed or when the certificate is nearing expiry.	
		BRG [i.2] Requirement	
		15.2	
		Assessment Guidance	
		Auditors should check the CA procedures to verify that requests for certificates issued to a subject who has already previously been registered are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes according to clause 7.3.2 of TS 102 042 [i.1] and section 15.2 (2) of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.3.3	Certificate generation	*The CA shall ensure that it issues certificates securely to maintain their authenticity.*	
		BRG [i.2] Requirement	
		9, 12 and Appendix B	
		Assessment Guidance	
		Auditors should check the CA procedures to verify that the CA issues certificates securely to maintain their authenticity according to clause 7.3.3 of TS 102 042 [i.1] and section 9 of BRG [i.2]. Auditors should check that certificates issued by a root CA address requirements specified inc section 12 of BRG [i.2] are met. The certificate content should be checked against Appendix B of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.3.4	Dissemination of terms and conditions	*The CA shall ensure that the terms and conditions are made available to subscribers and relying parties.*	
		BRG [i.2] Requirement	
		10.3	
		Assessment Guidance	
		Auditors should check that the CA's terms and conditions are made available to subscribers and relying parties as indicated in section 10.3 of BRG [i.2] and clause 7.3.4 of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.3.5	Certificate dissemination	*The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check that that certificates issued by the CA are made available as necessary to subscribers, subjects and relying parties as indicated in clause 7.3.5 of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.3.6	Certificate revocation and suspension	*The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests.*	
		BRG [i.2] Requirement	
		13.1 and 13.2	
		Assessment Guidance	
		Auditors should verify that: • The CA revocation procedures follow the section 13.1 and 13.2 of BRG [i.2] and clause 7.3.6 of TS 102 042 [i.1]. • The CA revocation entries on a CRL or OCSP are not removed until the expiration date of the revoked certificate as per section 13.2 [i.2]. • The CA can accept and respond to revocation or suspension requests on a 24x7 basis as indicated in section 13.1 of BRG [i.2]. • The CA follow the requirements of BRG [i.2] section 13.2 related to the online 24x7 repository mechanism for automatic checking of the current status of the certificate. • The CA follow the revocation events indicated in section 13.1 of EVCG [i.2]. • The CA provides problem reporting and response capability as in section 13.1 of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.1	Security Management	*The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.*	
		BRG [i.2] Requirement	
		14.2.2 and 16	
		Assessment Guidance	
		Auditors should review if the CA has implemented and documented a system or systems for information security management. NOTE: Auditors should check that administrative and management security procedures of the CA are applied as indicated in sections 14.2.2 and 16 of BRG [i.2] and clause 7.4.1 of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.2	Asset Classification	*The CA shall ensure that its assets and information receive an appropriate level of protection.*	
		BRG [i.2] Requirement	
		16	
		Assessment Guidance	
		Auditors should check that CA assets and information receive an appropriate level of protection as indicated in section 16 of BRG [i.2] and clause 7.4.2 of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.3	Personnel Security	*The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.*	
		BRG [i.2] Requirement	
		14.1	
		Assessment Guidance	
		Auditors should check that personnel and hiring practices enhance and support the trustworthiness of the CA's operations as per section 14.1 of BRG [i.2] and clause 7.4.3 of TS 102 042 [i.1]. Auditors should verify, for example, that: • it is followed a documented procedure to assign individuals to trusted roles; • the responsibilities and tasks and the separation of duties assigned to trusted roles are documented and implemented; • that only trusted roles have access to security and high security zones; • that employees and contractors follow the principle of "least privilege" when accessing to the CA systems; • it is required to have and use a unique credential to authenticate in the CA systems; • it is implemented a process that disables all privilege access within 24 hours upon termination of employment; • a trusted role is following up on alerts of possible critical security events; • a human review process is implemented to review application and system logs every 30 days and validate the integrity of logging processes and verify all operations are working properly.	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.4	Physical and environmental security	*The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized.*	
		BRG [i.2] Requirement	
		16.5	
		Assessment Guidance	
		Auditors should check that physical access to critical services of the CA is controlled and physical risks to its assets minimized according to clause 7.4.4 of TS 102 042 [i.1] and section 16.5 (1) of BRG [i.2]. Auditors should verify, for example, that: • certificate systems are segmented into networks or zones based on their functional, logical and physical relationship; • the root CA is maintained in a high security zone and in an offline state or air-gapped from other networks.	

Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**
7.4.5	Operations Management	*The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure.*	
		BRG [i.2] Requirement	
		15.2 and 16.5	
		Assessment Guidance	
		Auditors should check that the CA systems are secure and correctly operated, with minimal risk of failure according to clause 7.4.5 of TS 102 042 [i.1] and sections 15.2 and 16.5 (4 and 5) of BRG [i.2]. Auditors should verify, for example, that: • multi-factor authentication has been implemented on those systems that support it; • detection and prevention controls are implemented to protect the CA systems against viruses and malware; • it is implemented a procedure to monitor, detect and report any security-related configuration change; • all logs are maintained, archived and retained in accordance with applicable legislation and CA business practices; • timely acquire information on sources of security problems, for example on security problems emerging from staff, manufacturers, the "hacker community", or special mailing lists. The CA can also participate in a Computer Security Incident Response Team (CSIRT); • it is good practice to prevent media obsolescence to test such media timely before the probable media decay time; • it is good practice to timely (within six months of the patch's availability) install security patches in a secure manner; • a proper definition of "security incident" is required to provide CA staff guidance on categorizing and reporting relevant incidents; • it is good practice to periodically (e.g. yearly) report on security incidents /problems to the CA management.	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.6	System access management	*The CA shall ensure that CA system access is limited to properly authorized individuals.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check that the CA system access is limited to properly authorized individuals according to clause 7.4.6 of TS 102 042 [i.1] Auditors should verify, for example, that: • the same security controls are applied to all systems co-located in the same zone; • the CA systems are maintained and protected in a secure zone; • it is implemented and configured security support systems to protect systems and communications inside secure and high security zones; • it is configured each network controllers (e.g. firewalls) with rules to support only the services identified by the CA as necessary to its operations. The use of technical "security baselines" (for routers, firewalls, operating systems, applications etc.) can enhance security very efficiently; • the systems configurations are being reviewing on a weekly basis; • only persons on trusted roles are granted for administration access. An up-to-date list of all persons having access to a security related asset of the CA and their level of access. This should be readily available. Historic access records should also be available; • it is required the trusted roles to log out of or lock workstations when no longer in use; • workstations are configured with inactivity time-outs the log the user off or lock the computer; • all system accounts are reviewed every 90 days and deactivate those that are no longer necessary; • automated mechanism are implemented to process logged system activity and alert personnel; • the account used to access the CA systems is locked out after no more than five failed attempts; • a penetration test is performed on an annual basis and after infrastructure upgrades or modifications and by a person or entity the skills, tools, code of ethics and independence necessary to provide a reliable report. A security audit performed by a third party, including a penetration test, on the CA core ICT infrastructure before going into production is good practice. The audit report can provide extra assurance to the assessor on adequate system access management; • a procedure is implemented to remediate or a plan to mitigate a critical vulnerability within 96 hours of discovery.	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.7	Trustworthy systems deployment maintenance	*The CA shall use trustworthy systems and products that are protected against modification.*	
		BRG [i.2] Requirement	
		16.5	
		Assessment Guidance	
		Auditors should check that the CA uses trustworthy systems and products that are protected against modification according to clause 7.4.7 of TS 102 042 [i.1] and section 16.5 (2) of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.8	Business Continuity Management and incident handling	*The CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible.* *NOTE 1: Other disaster situations include failure of critical components of a CA system, including hardware and software.*	
		EVCG [i.2] Requirement	
		16.4	
		Assessment Guidance	
		Auditors should check business continuity plan exists in the event of a disaster. This auditor should check that this plan covers compromise of the CA's private signing key and verify that the CA operations are restored as soon as possible as indicated in clause 7.4.8 of TS 102 042 [i.1] and section 16.4 of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.9	CA termination	*The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check CA procedures to verify that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services as covered by the certificate policy, and that they verify continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings as per clause 7.4.9 of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.10	Compliance with legal requirements	*The CA shall ensure compliance with legal requirements.*	
		BRG [i.2] Requirement	
		8.1	
		Assessment Guidance	
		Auditors should check CA compliance with legal requirements, including the Data Protection Directive as per clause 7.4.10 of TS 102 042 [i.1] and also check section 8.1 of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.11	Recording of information concerning certificates	*The CA shall ensure that all relevant information concerning a certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.*	
		BRG [i.2] Requirement	
		15, 15.1, 15.2 and 15.3	
		Assessment Guidance	
		Auditors should check that all relevant information concerning a certificate is retained for an appropriate period in particular for the purpose of providing evidence of certification for the purposes of legal proceedings, as per section 15 of BRG [i.2] and clauses 7.4.11 and 7.3.1 of the TS 102 042 [i.1]. Sections 15.1, 15.2 of BRG [i.2] apply and 15.3 of BRG [i.2] requires that records are retained for at least seven years after any certificate based on that documentation ceases to be valid. National legal requirements for retention of records for evidence should also be taken into account.	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.5	Organizational	*The CA shall ensure that its organization is reliable.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check CA procedures to verify that the organization is reliable as per clause 7.5 of TS 102 042 [i.1].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.6.1	Additional BRG requirements. Testing	*Not exist*	
		BRG [i.2] Requirement	
		Appendix C	
		Assessment Guidance	
		Auditors should check the availability of testing web pages as in Appendix C of BRG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.6.2	Cross certificates	*Not exist*	
		BRG [i.2] Requirement	
		8.4	
		Assessment Guidance	
		Auditors should check that the CA discloses all the Cross Certificates as per section 8.4 of the BRG [i.2].	
Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**
8.1	Cross certificates	*The authority issuing the certificate policy shall ensure that the certificate policy is effective.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check that the certificate policy is effective as per clause 8.1 of TS 102 042 [i.1].	
Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**
8.2	Cross certificates	*Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 7.3.4.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check that the subscribers and relying parties are properly informed as per clause 8.2 of TS 102 042 [i.1].	
Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**
8.3	Conformance	*The CA shall only claim conformance to the present document and the applicable certificate policy.*	
		BRG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check that the CA claims conformance to the TS 102 042 [i.1] and BRG [i.2].	

Annex B: Audit Report Framework

This annex does not place any requirements on the structure on the audit report but provides some guidance on the topics that should be considered for inclusion in the audit report.

It is suggested that auditors clearly address in their reports at least all the topics described hereinafter, in relation to the related clauses, in order to facilitate readers in identifying common issues across different assessment reports so to perform a cross evaluation of CAs.

It is suggested that the final audit report addresses the following topics:

1) Statutory and/or customary environment of the audited CA.

2) List of the CA documents that have been submitted to the auditing team, prior to and during the auditing process, as well as of those that have not been submitted although required.

3) Statement by the auditing team on whether the conditions to conduct an audit were met prior and during to the audit and if it was therefore deemed possible to conduct and conclude the audit and, in case of a negative position, the reasons for this position.

4) If the audit could be conducted, an overall evaluation of the CA: whether it was deemed as fully, partially or not compliant with the provisions of the present document.

5) For each clause of the present document the auditing team should specify their evaluations as follows.

   a) What in the present document was recommended on Auditors to verify:

      i) was verified (this can be assumed by default);

      ii) was not verified; in this case, the reasons for such omission will be clearly explained and if this omission was such to affect the auditing also of other items, that would be clearly indicated, or even of the overall auditing (this would be complementary to the statement as per the previous item 3).

   b) The outcomes of the auditing:

      i) the CA has been deemed fully compliant with the requirements established in TS 102 042 [i.1];

      ii) the CA has been deemed partially compliant or not compliant with the requirements established in TS 102 042 [i.1], in which case the affected requirements will be specified;

      iii) (applicable when the previous item ii) applies) shortcomings found and their severity level;

NOTE 1: The severity levels would be structured at least in three steps. An example of such severity levels definitions would be as follows:

Severity 1: the CA is not compliant with the requirement at issue;

Severity 2: the requirement at issue may not be met in some circumstances, yet workarounds for achieving the desired compliance goal exist and can be easily applied;

Severity 3: the CA is substantially compliant with the requirements, although it is wished a more straightforward implementation of the CA requirements.

      iv) (applicable when the previous item ii) applies) recommendations for the CA to implement in order to comply with the requirements established in TS 102 042 [i.1].

NOTE 2: These recommendations will be specified on a high level, since the way to implement them is be left to the CA.

6) A possible range of dates when the CA the next audit should occur.

History

Document history		
V1.1.1	November 2012	Publication