ETSI TR 101 564 V1.1.1 (2011-09)

Electronic Signatures and Infrastructures (ESI);
Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs

Reference
DTR/ESI-000107

Keywords
e-commerce, extended validation certificates,
public key, security

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

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 the technical specification 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 certs are those used for securing web sites.

The Certification Authority/Browser (CAB) Forum has specified guidelines for the "Issuance and Management of Extended Validation Certificates" (EVCG [i.2]) to ensure that the public key certificates used for securing access to web sites are issued in a secure manner. The EVCG [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 Extended Validation Certificates are to:

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

2) enable encrypted communications with that site; and

3) identify the source of executable code.

The Secure Socket layer (SSL)/Transport Layer Security (TLS) protocols makes use of public key certificates to secure access to web sites and services.

EV Code Signing Certificates are intended to be used to verify the identity of a holder of an EV code signing certificate (Subscriber) and the integrity of its code. No particular object is identified in assuring the software protected by an EV Code Signing Certificate, only its distributor is identified.

The present document provides guidance for assessment of CAs issuing EV Certificates against TS 102 042 [i.1] and CAB Forum EVCG [i.2].

1 Scope

The present document provides guidance on the assessment of Certification Authorities issuing Extended Validation Certificates based on TS 102 042 [i.1] and the CA Browser Forum Guidelines for Extended Validation, EVCG [i.2]. The document is aimed at providing guidance to Certification Authorities issuing EV certificates to be aware of how they may be assessed and auditors in carrying out assessment of the conformance of such certification authorities to Extended Validation, such as SSL, code signing and other applications, and TS 102 042 [i.1].

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

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] Guidelines for The Issuance and Management of Extended Validation Certificates, CA Browser Forum.

NOTE: TS 102 042 [i.1] and EVCG [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] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[i.7] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

[i.8] ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

CA	Certification Authority
CAB	Certification Authority/Browser
CM	Cryptographic Module
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
EVCP+	Enhanced Extended Validation Certificate Policy
IS	Information Security
ISO	International Organization for Standardization
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy

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

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSA	Time Stamping Authority

4 Overview

The present document is intended to be used by Auditors as a guidance to assess the compliance of a CSP/CA with TS 102 042 [i.1] and for CSPs 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 EVCG [i.2] clauses are complied with by the CSP. In each of the following clauses, additional provisions may be specified that Auditors should implement.

5 Policies for issuing extended validation certificates

5.1 Overview

The TS 102 042 [i.1] policies relevant to use of EVC are:

4) An Extended Validation Certificate Policy (EVCP) that includes, except where explicitly indicated, all the Normalized Certificate Policy (NCP), as indicated in TS 102 042 [i.1] requirements, plus additional provisions suited to support EVC issue, usage and maintenance as specified in EVCG [i.2].

5) An enhanced Extended Validation Certificate Policy (EVCP+) that includes, except where explicitly indicated, all the extended Normalized Certificate Policy (NCP+), as indicated in TS 102 042 [i.1] requirements, enhanced with additional provisions suited to support EVC issue, usage and maintenance as specified in EVCG [i.2] when the EVCs owner must operate make use of a secure device.

Auditors should check for available policy documentation (e.g. CP or CPS) and ensure that this is in line with the EVCP or ECVP+ requirements. Auditors should verify the EV cert OID.

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 d) and e).

Auditors should check that the certificate either identifies the EVC policies or a certificate policy that incorporates the requirements of the EVC policies according to section 8.2 of EVCG [i.2].

5.3 User Community and Applicability

The policy requirements are applicable to Extended Validation Certificates as specified in section 6.1 EVCG [i.2]. Auditors should check that the primary purpose of the certificate, as stated in the certificate policy, relates to that in section 6.1 of the EVCG [i.2].

5.4 Conformance

NOTE: Requirements and guidance relating to conformity assessment is to be addressed in a separate document.

6 Obligations and liability

6.1 Certification authority obligations

Auditors should verify that the CP included in the certificate covers the requirements EVCP or EVCP+.

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 section 6.2 and 12.2 of EVCG [i.2].

6.2 Subscriber obligations

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

- In case of code signing refer to Appendix G item 7 and Appendix H item 12 of EVCG [i.2].

- Procedures to verify in case of a compromise of the key 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.
- EVCG [i.2], sections 9.3.2 and 9.3.3.
- 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 EVCG [i.2] and TS 102 176-1 [i.4] applies. In case of conflict, Appendix A of EVCG [i.2] prevails.

6.3 Information for Relying parties

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

- To check inclusion of specific revocation/suspension policy procedure (see clause 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 complain.
  - To check the terms and conditions is published at the company's website and verify the availability of the site.

Auditors should also check section 11.1 of EVCG [i.2] related to EVC status checking and section 11.3 of EVCG [i.2] related to the problem reporting and response capability.

6.4 Liability

Auditors should verify the procedures to provide assurance of minimum levels of liability, insurance coverage, etc. according to section 7.1.3 of EVCG [i.2] regarding the minimum assets covered for liability insurance and section 15.2 of EVCG [i.2] related to EV certificates limitations liability. For the purpose of insurance cover the auditor may consider equivalent minimum liability cover in the local currency.

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 EV certificates, according to clause 7.1 of TS 102 042 [i.1].

b) The CA's certification practice statement including the item 3 from section 7.1.2 of EVCG [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 section 7.1.2 (2) and 15.1 of EVCG [i.2] and 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 as indicated in section 6.2.1 item 1 c) of EVCG [i.2]. The publicly disclosure of the CPS, policies and procedures through an appropriate and accessible online mean that its available 24x7 on a regular basis as indicated in section 11.1.1 of EVCG [i.2].

e) CAs and EV issuing CA hierarchy.

f) The CA's commitment with the EVCG [i.2].

g) The CA documentation of the algorithms and parameters employed as indicated in the Appendix A of EVCG [i.2] and TS 102 176-1 [i.4]. In case of conflict, Appendix A of EVCG [i.2] prevails.

h) Processes for managing and reviewing the CPS.

i) The sections 7.1.3 regarding insurances and 15.2 regarding liability of EVCG [i.2].

NOTE: The disclosures may be structured in accordance with RFC 3647 [i.5]; see annex C of TS 102 042 [i.1].

7.2 Public key infrastructure - Key management life cycle

7.2.1 Certification authority key generation

Auditors should verify the CA Auditor's report on the key generation ceremony as describing in section 14.1.5 of the EVCG [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 EVCG [i.2] that will prevail in case of a conflict.

NOTE: The contents of a CA 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

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].

Auditors should check the CA key generation according to clause 7.2.1 a) and c) of TS 102 042 [i.1].

In case of EV code signing certificates, auditors should check requirements in Appendix H of EVCG [i.2] are addressed.

7.2.2 Certification authority key storage, backup and recovery

Auditors should check CA procedures to ensure 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].

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].

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 CAs ensures 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: EV Certificates are not expected to be escrowed.

7.2.5 Certification authority key usage

Auditors should check practices to ensure 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 ensure 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 13.1 (2) (A) (i) of EVCG [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 EVCG [i.2] that will prevail in case of a conflict.

7.2.7 Life cycle management of cryptographic hardware used to sign certificates

Auditors should ensure the CSP 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 13.1 (2) (A) (ii) of EVCG [i.2].

7.2.8 CA provided subject key management services

If applicable, auditors should check CA procedures to ensure 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 EVCG [i.2] and TS 102 176-1 [i.4] applies. In case of conflict, Appendix A of EVCG [i.2] prevails.

7.2.9 Secure user devices preparation

Auditors should check CA procedures to ensure that if it issues to the subject secure user device this is carried out securely as indicated in clause 7.2.9 of TS 102 042 [i.1]. In case of a EV code signing certificate follow indications of Appendix H item 10 of EVCG [i.2].

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.

Auditors should verify that the CSP registration procedures follow the EVCG [i.2] requirements of sections 7.2, 9.1, 9.2 and 10 regarding the verification of the information and clause 7.3.1 items a), c), m) n) p) q) of TS 102 042 [i.1] for every registration. Also, Appendix D, E, F of EVCG [i.2] should be noted.

Information used from a previous registration should meet the requirements indicated in section 10.13 of EVCG [i.2].

Auditors should check the applicant registration records and ensure 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 EV certificates are retained at least seven years after any EV Certificate based on that documentation ceases to be valid as stated in EVCG [i.2], section 13.2.2. Also for dual control in validation information the CSP should follow the indications on section 12.1.3 of EVCG [i.2].

7.3.2 Certificate renewal, rekey and update

Auditors should check the CA procedures to ensure 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 13.1 (B) (i) of EVCG [i.2].

7.3.3 Certificate generation

Auditors should check the CA procedures to ensure that the CA issues certificates securely to maintain their authenticity according to clause 7.3.3 of TS 102 042 [i.1] and section 8 of EVCG [i.2].

- If the certificate is being used for SSL the certificate content should be checked against Appendix B of EVCG [i.2].
- If the certificate is being used for code signing the certificate content should be checked against Appendix H (3) of EVCG [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 10.7.3 (8)(C) of EVCG [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 section 10.7.3 (8) (C) of EVCG [i.2] and clause 7.3.5 of TS 102 042 [i.1].

7.3.6 Certificate revocation and suspension

Auditors should verify that:

- the CA revocation procedures follow the section 11.1, 11.2 of EVCG [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 EVC;
- the CA can accept and respond to revocation or suspension requests on a 24x7 basis as indicated in section 11.2.1 of EVCG [i.2];
- the CA follow the requirements of EVCG [i.2], section 11.1.1 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 11.2.2 of EVCG [i.2];
- the CA provides problem reporting and response capability as in section 11.3 of EVCG [i.2];
- if code signing is supported, the CA follows revocation procedures in appendix H item 13 of EVCG [i.2].

7.4 CA management and operation

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.7] and ISO/IEC 27002 [i.8] 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 section 13.3 of EVCG [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 section 13.3 of EVCG [i.2] and 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 12.1 of EVCG [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 13.3.3 of EVCG [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].

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] and section 13.1 item (C) sub-item (i) of EVCG [i.2].

7.4.7 Trustworthy systems deployment and maintenance

Auditors should check that the *CA shall use trustworthy systems and products that are protected against modification* according to clause 7.4.7 of TS 102 042 [i.1].

7.4.8 Business continuity management and incident handling

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 ensure 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 13.3.3 of EVCG [i.2].

7.4.9 CA termination

Auditors should check CA procedures to ensure 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 ensure 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] and section 13.3.3 of EVCG [i.2].

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 section 15 of EVCG [i.2].

7.4.11 Recording of information concerning certificates

Auditors should check that all relevant information concerning a certificate is retainedfor an appropriate period in particular for the purpose of providing evidence of certification for the purposes of legal proceedings, as per section 13 of the EVCG [i.2] and clauses 7.4.11 and 7.3.1 of the TS 102 042 [i.1].

EVCG [i.2] requires that records are retained for at least seven years after any EV 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 ensure that the organization is reliable as per clause 7.5 of TS 102 042 [i.1] and section 15.2 of EVCG [i.2].

8 Additional EV Requirements

8.1 Time-stamping

Where the CSP provides time-stamping services for EV code signing the auditor should check the TSA applies requirements in Appendix I of EVCG [i.2]. In addition, requirements in TS 102 023 [i.6] should be considered.

8.2 Code signing Authority

Where the CSP provides code signing services with EV code signing the auditor should check the TSA applies requirements in Appendix J of EVCG [i.2].

Annex A (informative): Assessment Guidance Checklist

NOTE 1: The following table identifies particularly to an EVC assessment. Text quoted from TS 102 042 [i.1] / EVCG [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 EVCG [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 EVC are*:* *4) An Extended Validation Certificate Policy (EVCP) that includes, except where explicitly indicated, all the Normalized Certificate Policy (NCP), as indicated in TS 102 042 [i.1] requirements, plus additional provisions suited to support EVC issue, usage and maintenance as specified in EVCG [i.2].* *5) An enhanced Extended Validation Certificate Policy (EVCP+) that includes, except where explicitly indicated, all the extended Normalized Certificate Policy (NCP+), as indicated in TS 102 042 [i.1] requirements, enhanced with additional provisions suited to support EVC issue, usage and maintenance as specified in EVCG [i.2] when the EVCs owner must operate make use of a secure device.*	
		EVCG [i.2] Requirement	
		7.1.2 (1), (2) and (3)	
		Assessment Guidance	
		Auditors should check for available policy documentation (e.g. CP or CPS) and ensure that this is in line with the EVCP or ECVP+ requirements. Auditors should verify the EV cert OID	
Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**
5.2	Identification	The identifiers for CP or CPS relevant to the EVC are: *d) EVCP: Extended Validation Certificate Policy* `itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)` *e) EVCP+: Extended Validation Certificate Policy requiring a secure user device* `itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcpplus (5)` *By including one of these object identifiers in a certificate the CA claims conformance to the identified certificate policy.*	
		EVCG [i.2] Requirement	
		8.2	
		Assessment Guidance	
		Auditors should check that the certificate either identifies the EVC policies or a certificate policy that incorporates the requirements of the EVC policies according to section 8.2 of EVCG [i.2]. The OIDs used may include the OIDs specified in TS 102 042 [i.1] clause 5.2 items d and e).	
Nº	**Subject**	**TS 102 042 [i.1] Requirement**	**Findings**
5.3		No constraints	
		EVCG [i.2] Requirement	
		6.1	
		Assessment Guidance	
		Auditors should check that the primary purpose of the certificate, as stated in the certificate policy, is as in section 6.1 of EVCG [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.*	
		EVCG [i.2] Requirement	
		6.2 and 12.2	
		Assessment Guidance	
		Auditors should verify that the CP included in the certificate covers the requirements EVCP or EVCP+. 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 6.2 and 12.2 of EVCG [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.*	
		EVCG [i.2] Requirement	
		9.3.2, 9.3.3 and Appendix A, G item 7 and H item 12	
		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) and i) of TS 102 042 [i.1] are addressed: - In case of code signing refer to Appendix G item 7 and Appendix H item 12 of EVCG [i.2]. - Procedures to verify in case of a compromise of the key 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] clause 7.3.1 item m) and clause 7.3.4. • EVCG [i.2], sections 9.3.2 and 9.3.3. • 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 EVCG [i.2] and TS 102 176-1 [i.4] applies. In case of conflict, Appendix A of EVCG [i.2] prevails.	
Nª	**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.* *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)	
		EVCG [i.2] Requirement	
		11.1 and 11.3	
		Assessment Guidance	
		Auditors should verify the CA's terms and conditions (see 7.3.4): - To check inclusion of specific revocation /suspension policy procedure (see clause 7.3.6 checks on revocation mechanisms). - To inspect reporting and investigation of issues for example: o To check the terms and conditions and find the contact details in case of an incident, question or complain. o To check the terms and conditions is published at the company's website and verify the availability of the site. Auditors should also check section 11.1 of EVCG [i.2] related to EVC status checking and section 11.3 of EVCG [i.2] related to the problem reporting and response capability.	
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.*	
		EVCG [i.2] Requirement	
		7.1.3 and 15.2	
		Assessment Guidance	
		Auditors should verify the procedures to provide assurance of minimum levels of liability, insurance coverage, etc. according to section 7.1.3 of EVCG [i.2] regarding the minimum assets covered for liability insurance and section 15.2 of EVCG [i.2] related to EV certificates limitations liability. For the purpose of insurance cover the auditor may consider equivalent minimum liability cover in the local currency.	

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 clauses 7.1, 7.3.4 and Annex C.	
		EVCG [i.2] Requirement	
		7.1.2, 6.2.1 item 1 C, 11.1.1, 7.1.3 and 15.2. 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 EV certificates, according to clause 7.1 of TS 102 042 [i.1]. b) The CA's certification practice statement including the item 3 from section 7.1.2 of EVCG [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 section 7.1.2 (2) and 15.1 of EVCG [i.2] and 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 as indicated in section 6.2.1 item 1 c) of EVCG [i.2]. The publicly disclosure of the CPS, policies and procedures through an appropriate and accessible online mean that its available 24x7 on a regular basis as indicated in section 11.1.1 of EVCG [i.2]. e) CAs and EV issuing CA hierarchy. f) The CA's commitment with the EVCG [i.2]. g) The CA documentation of the algorithms and parameters employed as indicated in the Appendix A of EVCG [i.2] and TS 102 176-1 [i.4]. In case of conflict, Appendix A of EVCG [i.2] prevails. h) Processes for managing and reviewing the CPS. i) The sections 7.1.3 regarding insurances and 15.2 regarding liability of EVCG [i.2]. 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.*	
		EVCG [i.2] Requirement	
		14.1.5, Appendix A (1) and (2) Appendix H for code signing	
		Assessment Guidance	
		Auditors should verify: the CA Auditor's report on the key generation ceremony as describing in section 14.1.5 of the EVCG [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 EVCG [i.2] that will prevail in case of a conflict. 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]. Auditors should check the CA key generation according to clause 7.2.1 a) and c) of TS 102 042 [i.1]. In case of EV code signing certificates, auditors should check requirements in Appendix H of EVCG [i.2] are addressed.	

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] clauses 7.2.2 a), b) c) and d).	
		EVCG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check CA procedures to ensure 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] 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.*	
		EVCG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check that, where possible, the CAs ensures 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.*	
		EVCG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check practices to ensure 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.*	
		EVCG [i.2] Requirement	
		13.1 (2) (A) and Appendix A	
		Assessment Guidance	
		Auditors should check practices to ensure 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 13.1 (2) (A) (i) of EVCG [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 EVCG [i.2] that will prevail in case of a conflict.	

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.*	
		EVCG [i.2] Requirement	
		13.1 (2) (A)	
		Assessment Guidance	
		Auditors should ensure the CSP 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 13.1 (2) (A) (ii) of EVCG [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.*	
		EVCG [i.2] Requirement	
		Appendix A	
		Assessment Guidance	
		If applicable, auditors should check CA procedures to ensure 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 EVCG [i.2] and TS 102 176-1 [i.4] applies. In case of conflict, Appendix A of EVCG [i.2] prevails	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.2.9	Secure user device preparation	*The CA shall ensure that if it issues to the subject secure user device this is carried out securely.*	
		EVCG [i.2] Requirement	
		Appendix H item 10	
		Assessment Guidance	
		Auditors should check CA procedures to ensure that if it issues to the subject secure user device this is carried out securely as indicated in clause 7.2.9 of TS 102 042 [i.1]. In case of a EV code signing certificate follow indications of Appendix H item 10 of EVCG [i.2].	

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.*	
		EVCG [i.2] Requirement	
		7.2, 9.1, 9.2, 10, 12.1.3, 13.2.2 and Appendix D, E and F.	
		Assessment Guidance	
		Auditors should verify that the CSP registration procedures follow the EVCG [i.2] requirements of section 7.2, 9.1, 9.2 and 10 regarding the verification of the information and clause 7.3.1 items a), c), m) n) p) q) of TS 102 042 [i.1] for every registration Also, Appendix D, E, F should be noted. Information used from a previous registration should meet the requirements indicated in section 10.13 of EVCG [i.2]. Auditors should check the applicant registration records and ensure the requirements of item j of the clause 7.3.1 of the TS 102 042 [i.1] are met. Auditors should verify that the records regarding the EV certs are retained at least seven years after any EV Certificate based on that documentation ceases to be valid as stated in EVCG [i.2], section 13.2.2. Also for dual control in validation information the CSP should follow the indications on section 12.1.3 of the EVCG [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.*	
		EVCG [i.2] Requirement	
		13.1 (B) (i)	
		Assessment Guidance	
		Auditors should check the CA procedures to ensure 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 13.1 (B) (i) of EVCG [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.*	
		EVCG [i.2] Requirement	
		8, Appendix B, H	
		Assessment Guidance	
		Auditors should check the CA procedures to ensure that the CA issues certificates securely to maintain their authenticity according to clause 7.3.3 of TS 102 042 [i.1] and section 8 of EVCG [i.2]: - If the certificate is being used for SSL the certificate content should be checked against Appendix B of EVCG [i.2]. - If the certificate is being used for code signing the certificate content should be checked against Appendix H (3) of EVCG [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.*	
		EVCG [i.2] Requirement	
		10.7.3	
		Assessment Guidance	
		Auditors should check that the CA's terms and conditions are made available to subscribers and relying parties as indicated in section 10.7.3 (8)(C) of EVCG [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.*	
		EVCG [i.2] Requirement	
		10.7.3 (8)(C)	
		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 section 10.7.3 (8)(C) of EVCG [i.2] and 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.*	
		EVCG [i.2] Requirement	
		11.1, 11.1.1, 11.2, 11.2.1, 11.2.2, 11.3 and Appendix H.	
		Assessment Guidance	
		Auditors should verify that: - the CA revocation procedures follow the sections 11.1, 11.2 of EVCG [i.2] and clause 7.3.6 of ETSI TS 102 042 [i.1]; - the CA revocation entries on a CRL or OCSP are not removed until the expiration date of the revoked EVC; - the CA can accept and respond to revocation or suspension requests on a 24x7 basis as indicated in section 11.2.1 of EVCG [i.2]; - the CA follow the requirements of EVCG [i.2], section 11.1.1 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 11.2.2 of EVCG [i.2]; - the CA provides problem reporting and response capability as in section 11.3 of EVCG [i.2]; - if code signing is supported, the CA follows revocation procedures in Appendix H item 13 of EVCG [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.*	
		EVCG [i.2] Requirement	
		13.3	
		Assessment Guidance	
		Auditors should review if the CA has implemented and documented a system or systems for information security management. Auditors should check that administrative and management security procedures of the CA are applied as indicated in section 13.3 of EVCG [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.*	
		EVCG [i.2] Requirement	
		13.3	
		Assessment Guidance	
		Auditors should check that CA assets and information receive an appropriate level of protection as indicated in section 13.3 of EVCG [i.2] and clause 7.4.2 of TS 102 042 [i.1].	

	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.*	
		EVCG [i.2] Requirement	
		12.1	
		Assessment Guidance	
		Auditors should check that personnel and hiring practices enhance and support the trustworthiness of the CA's operations as per section 12.1 of EVCG [i.2] and clause 7.4.3 of TS 102 042 [i.1].	

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.*	
		EVCG [i.2] Requirement	
		13.3.3	
		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 13.3.3 of EVCG [i.2].	

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.*	
		EVCG [i.2] Requirement	
		13.2.1	
		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 section 13.2.1 of EVCG [i.2].	

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.*	
		EVCG [i.2] Requirement	
		13.1 (C)	
		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] and section 13.1 item (C) sub-item (i) of EVCG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.7	System access management	*The CA shall use trustworthy systems and products that are protected against modification.*	
		EVCG [i.2] Requirement	
		Assessment Guidance	
		Auditors should check that *the CA shall use trustworthy systems and products that are protected against modification* according to clause 7.4.7 of TS 102 042 [i.1].	

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	
		13.3.3	
		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 ensure 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 13.3.3 of EVCG [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.*	
		EVCG [i.2] Requirement	
		13.3.3	
		Assessment Guidance	
		Auditors should check CA procedures to ensure 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 ensure 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] and section 13.3.3 of EVCG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
7.4.10	Compliance with legal requirements	*The CA shall ensure compliance with legal requirements.*	
		EVCG [i.2] Requirement	
		15	
		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 section 15 of EVCG [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.*	
		EVCG [i.2] Requirement	
		13	
		Assessment Guidance	
		Auditors should check that all relevant information concerning a certificate is retainedfor an appropriate period in particular for the purpose of providing evidence of certification for the purposes of legal proceedings, as per section 13 of the EVCG [i.2] and clauses 7.4.11 and 7.3.1 of the TS 102 042 [i.1]. EVCG [i.2] requires that records are retained for at least seven years after any EV 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.*	
		EVCG [i.2] Requirement	
		15.2	
		Assessment Guidance	
		Auditors should check CA procedures to ensure that the organization is reliable as per clause 7.5 of TS 102 042 [i.1] and section 15.2 of EVCG [i.2].	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
8.1	Time-stamping	None	
		EVCG [i.2] Requirement	
		Appendix I	
		Assessment Guidance	
		Where the CSP provides time-stamping services for EV code signing the auditor should check the TSA applies requirements in Appendix I of EVCG [i.2]. In addition, requirements in TS 102 023 [i.6] should be considered.	

Nº	Subject	TS 102 042 [i.1] Requirement	Findings
8.2	Code signing Authority	None	
		EVCG [i.2] Requirement	
		Appendix J	
		Assessment Guidance	
		Where the CSP provides code signing services with EV code signing the auditor should check the TSA applies requirements in Appendix J of EVCG [i.2].	

Annex B (informative): 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 issuggested 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 CSPs.

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

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

2) List of the CSP 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 CSP: 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 CSP has been deemed fully compliant with the requirements established in TS 102 042 [i.1];

        ii. the CSP 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 CSP 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 CSP is substantially compliant with the requirements, although it is wished a more straightforward implementation of the CSP requirements.

        iv. (applicable when the previous item ii. applies) recommendations for the CSP 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 CSP.

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

History

Document history		
V1.1.1	September 2011	Publication