CA/Browser Forum

REQUIREMENTS for the PROCESSING of EXTENDED VALIDATION SSL CERTIFICATES

24 July 2012

Version 2.0

Deleted: GUIDELINES

Deleted: 19 January 2009

Deleted: 1

A request to make a translated version of these requirements should be submitted to questions@cabforum.org.

Deleted: guideline

Table of Contents

Deleted: 1. Foreword . 4¶
2. Scope . 4¶
3. Normative references . 4¶
4. Terms and definitions . 4¶
5. Introduction . 4¶
6. Identifying EV entities . 5¶
6.1. Identifying an EV CSP . 5¶
6.2. Identifying an EV certificate . 5¶
7. Root-embedding program . 5¶
7.1. Notification . 5¶
7.2. Agreement . 5¶
7.3. Process description . 5¶
7.4. Communication . 6¶
7.5. Schedule . 6¶
7.6. Membership . 6¶
7.7. Software Verification . 6¶
8. CSP Public-Key Integrity Protection . 6¶
9. Certificate Validation . 7¶
10. Cryptographic Algorithms and Minimum Key Sizes . 7¶
11. Certificate Contents . 7¶
12. Revocation Checking . 7¶
13. EV Treatment . 7¶
14. Security considerations . 7¶
15. Conclusion . 8¶

1. Foreword

This document contains requirements, established by the CA/Browser Forum, for processing and rendering the results of extended validation in Internet applications. These requirements may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Questions concerning these requirements or suggestions for their improvement may be directed to the CA/Browser Forum at

questions@cabforum.org.

2. Scope

The EV SSL Certificate Guideline [EVSSL] document establishes minimum requirements for the issuance and management of SSL certificates for organizations of various types. It describes processes for validating certificate contents prior to issuance, and requirements for the operation and audit of certification authorities.

This document contains requirements for application developers who rely on extended validation certificates.

3. Normative references

[EVSSL] "EV SSL Certificate Guidelines Version 1.3", CABForum, November 2010. Available at: http://www.cabforum.org/documents.html.

[RFC 5280] D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

4. Terms and definitions

Application developer - A software maker whose product relies upon public-key certificates by embedding the root public key of one or more certificate service providers.

Certificate service provider (CSP) - A certification authority whose relying parties take no special software installation or configuration steps to establish reliance, e.g. a commercial CA or government CA.

Extended validation - The process of certificate issuance and management defined in [EVSSL].

5. Introduction

The CA/Browser Forum has defined minimum requirements for the issuance and management of SSL certificates [EVSSL]. These requirements establish a minimum level of assurance in the information contained in a properly validated certificate. Certificates issued in accordance with these requirements are called Extended Validation certificates. In order to achieve the expected level of assurance in the certificate contents, the relying application also has to satisfy certain requirements. Those requirements are laid out in this document.

Deleted: The Guidelines for the Processing of Extended Validation Certificates

Deleted: recommendations

Deleted: Guidelines

Deleted: guideline

Deleted: Extended validation

Deleted: recommendation

Deleted: ISSU

Deleted: Guidelines for the Issuance and Management of Extended Validation Certificates

Deleted: , v1.1

Deleted: April

Deleted: 2008

Deleted: ISSU

Deleted: ISSU

6. Identifying EV entities

6.1. Identifying an EV CSP

An application developer shall recognize a CSP that is qualified to issue EV SSL certificates by means of the CSP's audit report. The application developer must check that the report was issued by an auditor certified to conduct audits in accordance with an acceptable audit program. The report must be current and it must identify no outstanding deficiencies.

These checks must be repeated upon expiry of the audit report. It is common for an auditor to take several months to issue his or her report following completion of the audit engagement. Therefore, application developers should communicate with a CSP around the time of expiry, in order to confirm that the CSP is taking the steps necessary to maintain its EV status.

Where the CSP has not operated an EV service for the minimum amount of time required by the audit program, the application developer should accept a pre-issuance readiness audit in place of an audit report.

6.2. Identifying an EV certificate

An EV certificate is distinguishable from a non-EV certificate by the presence of a distinct certificate policy identifier. Each CSP has its own EV policy identifier. The policy identifier for a particular CSP must be confirmed by reference to the CSP's certificate policy (CP) or certification practices statement (CPS).

Deleted: .

7. Root-embedding program

Application developers that intend to rely upon EV certificates issued by CSPs should implement the following procedures.

7.1. Notification

The application developer should announce its intention in a message sent to the following email address:

questions@cabforum.org

7.2. Agreement

It is recommended that the application developer enter into an agreement separately with each CSP. These agreements should offer equivalent protections to all relying parties. The agreements should formalize the rights and obligations of the application developer and the CSP, and define the governing law and jurisdiction for dispute resolution.

7.3. Process description

The agreement should describe the following:

a) The application developer's public-key inclusion process

b) The application's root distribution process

c) General requirements on the CSP

d) Documentation requirements on the CSP

e) Technical requirements on the CSP

f) The process for replacing a CSP public key (if applicable)

7.4. Communication

The agreement should describe the expected sequence and method of communication between the application developer and the CSP (for example: receipt confirmation, status updates, requests for additional information, etc. will be communicated: by e-mail, by online forum, by bulletin board, etc.).

7.5. Schedule

The agreement should describe the general schedule, time-frame and deadlines for each milestone of the CSP root-embedding process. Note: this should not commit the application developer to specific dates or time periods; it should merely provide general guidance on:

a) The interval on which new CSP roots enter the process (for instance: monthly, on an on-going basis, etc.)

b) The typical duration of the complete process

c) Deadlines (for instance: code freezes prior to release, etc.)

d) The distribution schedule for accepted roots (for instance: monthly, with new releases, etc.)

Formatted: Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.77" + Tab after: 1.02" + Indent at: 1.02"

7.6. Membership

The application developer should publicly post a list of the CSPs that are currently participating in its program (i.e. CSPs whose public keys have been accepted and that are, or will be, relied upon).

7.7. Software Verification

CSPs that offer EV certificates are required to provide a mechanism for application developers to test their certificates. Application developers should make full use of this mechanism to verify the correct operation of their application.

8. CSP Public-Key Integrity Protection

Relying applications must provide adequate protection against malign threats to the integrity of the application code and the CSP root.

9. Certificate Path Validation

The relying application shall validate the certificate in accordance with [RFC 5280] Section 6. The application shall grant the EV treatment (see *EV Treatment*, below) only to certificates that validate successfully.

Deleted:

Deleted: Section 13

Deleted:

Formatted: Font: Italic

Deleted: below

10. Cryptographic Algorithms and Minimum Key Sizes

The relying application must be capable of processing the cryptographic algorithms and key sizes listed in [EVSSL], with the additional specification that the effective key strength of symmetric algorithms must be at least 128 bits. The relying application MUST NOT grant the EV treatment (see Section 14, below) to certificates whose algorithms and keys do not conform to these requirements.

11. Certificate Contents

The relying application MUST be capable of processing the certificate fields and extensions containing subject attributes that are described in [EVSSL].

With the exception of the Subject OU attribute, the application should treat all certificate contents as trustworthy. CSPs may populate the Subject OU attribute with unverified, but not misleading, information. Therefore, the Subject OU attribute should not be treated as trustworthy.

12. Policy Identifier

The relying application MUST verify that the EV certificate contains a value in its certificate policies extension that matches the distinct certificate policy identifier associated with the issuing CSP, as described in *Identifying an EV certificate*. The application shall grant the EV treatment (see *EV Treatment*, below) only to certificates that contain the appropriate policy identifier.

13. Revocation Checking

Applications MUST confirm that the EV certificate has not been revoked before accepting it. This includes verifying the revocation status of any intermediate CA certificates, in conformance with [RFC 5280] Section 6.3: "This algorithm defines a set of inputs, a set of state variables, and processing steps that are performed for each certificate in the path."

Certificates for which confirmation cannot be obtained MUST NOT be granted the EV treatment (see Section 14, below).

The application should support both CRL and OCSP services. For HTTP schemes, the application may use either the GET or POST method, but SHOULD try the GET method first. If the application cannot obtain a response using one service, then it should try all available alternative services.

The application should follow HTTP redirects and cache-refresh directives.

Response time-out should not be less than three seconds.

14. EV Treatment

In cases where the relying application accepts both EV and non-EV certificates, it is recommended that the application's behavior differ in a distinct way for each type of certificate. Application developers should consider the EV treatment offered by other

Deleted: ¶
Deleted: ISSU
Deleted: should not
Deleted: 13
Deleted: Relying
Deleted: should
Deleted: ISSU
Formatted: Normal, Tab stops: Not at 0.25"
Formatted: Font: Italic
Formatted: Font: Italic
Deleted: must
Deleted:
Deleted: Revocation checking must be performed in accordance with [RFC5280].
Deleted: must not
Deleted: 13

application developers that also recognize EV certificates and, where practical, provide consistent treatment.

15. Security considerations

There are numerous security considerations related to the processing of certificates and reliance on their contents. Here, we confine ourselves to those matters that are specific to EV certificates.

Perhaps the most serious threat to the security of extended validation is the possibility that any one of the CSPs upon which the application relies fails to conform, or maintain conformance with, the EV requirements for issuance and management [EVSSL]. The main safeguard against this possibility is the CSP audit. Therefore, the application developer MUST confirm that the CSP's audit is current, identifies no deficiencies and was conducted by a properly qualified auditor. The audit should provide a level of assurance equivalent to that of a WebTrust for CAs EV audit. See:

http://www.webtrust.org/homepage-documents/item54280.docx

Deleted: ISSU

Deleted: it is important that

Deleted: http://www.webtrust.org/index.cfm/ci_id/43988/la_id/1.htm

16. Conclusion

Not all certificates are equally trustworthy. Their trustworthiness depends upon the strength of their cryptographic protection. But, it also depends on the policies and practices used in their issuance and management. Historically, relying parties have been required to assess the suitability of a CSP's policies and practices for the intended usage. In 2007 (and with later revisions) public CSPs agreed to a common set of policies and practices that establish a minimum level of assurance deemed suitable for common Internet purposes, such as eCommerce and eGovernment. Achieving the intended level of assurance also requires proper behavior by the relying application. This document lays out appropriate requirements on the relying application.