CA/Browser Forum

RECOMMENDATIONS for the PROCESSING of EXTENDED VALIDATION SSL CERTIFICATES

January 2, 2014

Version 2.0

Table of Contents

1. Foreword

This document contains recommendations by the CA/Browser Forum, for processing and rendering the results of Extended Validation certificates in relying party software applications (e.g., browser software). This document may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Questions concerning this document or suggestions for its 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 EV 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 recommendations for Application Software Suppliers who create software that processes or displays Extended Validation certificates.

3. Normative references

[BRs] "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates," CA/Browser Forum. Available at: https://cabforum.org/baseline-requirements-documents/

[EVSSL] "Guidelines for the Issuance and Management of Extended Validation Certificates", CA/Browser Forum. Available at: https://cabforum.org/extended-validation/

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

[RFC 6960] S. Santesson, et al., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", RFC 6960, June 2013.

4. Terms and definitions

Application Software Supplier - A supplier of Internet browser software or other relying-party application software, including certificate verification software and user agents, that processes, uses, or displays Extended Validation Certificates.

Certificate Policy (CP) – A named set of rules that indicates the applicability of a named certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Practices Statement (CPS) - One of several documents forming the governance framework in which Certificates are created, issued, managed, and used

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. In the EU directive (1999/93/CE) "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Certificate Verification Software – Software that performs PKIX verification of certificates substantially conformant to RFC 5280 and RFC 6960.

Certificate Viewer – Software that converts the ASN.1-formatted certificate, including numeric object identifiers, into human readable form.

Extended Validation (EV) - The process of certificate issuance and management defined in [EVSSL].

Extended Validation Certificate: A certificate issued and managed in accordance with [EVSSL] and with contents conforming to [EVSSL].

Relying Party: Any natural person or Legal Entity that relies on a valid certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a certificate.

Root Store – a collection of Root CA public keys that applications may use as trust anchors for RFC 5280 certification path validation.

Root Store Manager - An entity that manages a Root Store. In some cases, an Application Software Supplier might perform some of the root store management, in which case it is to be considered as a Root Store Manager for those purposes.

User Agent – Software that retrieves, renders and facilitates end-user interaction with Web content, including but not limited to browsers, media players, web applications, and mobile applications that render web content.

5. Introduction

The CA/Browser Forum has defined minimum requirements for the issuance and management of Extended Validation 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 should also satisfy the recommendations that are laid out in this document. Note that [EVSSL] incorporates by reference the CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [BRs].

6. Identifying EV entities

6.1. Identifying an EV CSP

A Root Store Manager shall determine whether a CSP is qualified to issue EV SSL certificates by means of the CSP's audit report. The Root Store Manager should check that the report was issued by an auditor certified to conduct audits in accordance with an audit program specified in [EVSSL]. The report should be current and it should identify no outstanding deficiencies.

These checks should 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, Root Store Managers 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 Root Store Manager 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 one or more root certificates designated to issue EV certificates, and has its own EV policy identifier to identify EV certificates issued in accordance with [EVSSL]. Alternatively, the CSP may choose to use the CA/Browser Forum's EV OID: 2.23.140.1.1. The policy identifier for a particular CSP should be confirmed by reference to the CSP's Certificate Policy (CP) or Certification Practices Statement (CPS). The Root Store Manager should store the distinct certificate policy identifier associated with each root certificate, for example, as meta-data.

7. Root-embedding program

A Root Store Manager should notify the CA/Browser Forum of their intent to manage a root store. The CA/Browser Forum recommends that the Root Store Manager implement the following procedures.

7.1. Notification

Notify the CA/Browser Forum in a message sent to any of the following email addresses:

questions@cabforum.org; management@cabforum.org; or public@cabforum.org

This is intended to ensure that the CA/Browser Forum is aware of the Root Store and to simplify the effort of identifying all possible CSPs for possible inclusion in the Root Store. The notice should include the terms upon which such CSPs will be included, such as those described in Sections 7.2 through 7.6 below, as appropriate. This requested notice to the CA/Browser Forum is not necessary for subsequent CSPs or root certificates that the Root Store Manager intends to add.

7.2. Agreement

A Root Store Manager may wish to enter into an agreement separately with each CSP prior to Root Store acceptance. Reasons for having such an agreement might include: to formalize the requirements of the root-embedding program and compliance with the EV Guidelines, to set forth any other rights or obligations of the parties, to define the governing law and jurisdiction for dispute resolution, and to address any other matter of importance to the parties. Such agreements should be non-discriminatory.

7.3. Process description

The notice and/or the agreement should describe the following:

a) The Root Store Manager's public-key inclusion process

b) The Root Store's certificate distribution and updating 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 notice and/or the agreement should describe the expected sequence and method of communication between the Root Store Manager 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 notice and/or the agreement should describe the general schedule, time-frame and deadlines for each milestone of the CSP root certificate-embedding process. Note: this should not commit the Root Store Manager to specific dates or time periods; it should merely provide general guidance on:

a) The interval on which new CSP root certificates 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 root certificates (for instance: monthly, with new releases, etc.)

7.6. Membership

The Root Store Manager should publicly post a list of the CSPs that are currently participating in its program (i.e. CSPs whose root certificates 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 Root Store Managers to test their certificates. Root Store Managers should make full use of this mechanism to verify the correct operation of their application.

8. CSP Public-Key Integrity Protection

Root Store Managers should provide adequate protection against malign threats to the integrity of the application code and the CSP root certificates.

9. Certificate Path Validation

Certificate verification software used by Application Software Suppliers shall validate the certificate in accordance with [RFC 5280] Section 6. The EV treatment (see Section 14, *EV Treatment*, below) must not be granted by user agents to certificates for which the agent knows of any failure in path validation.

10. Cryptographic Algorithms and Minimum Key Sizes

Certificate verification software used by Application Software Suppliers should be capable of processing the cryptographic algorithms and key sizes listed in [EVSSL]. User agents should not grant the EV treatment (see Section 14, *EV Treatment*, below) to certificates whose algorithms and keys do not conform to the EV requirements.

11. Certificate Contents

Certificate verification software should 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 by any Application Software.

12. Policy Identifier

The certificate verification software 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 root certificate, as described in Section 6.2, *Identifying an EV certificate*, above. The user agent must grant the EV treatment (see Section 14, *EV Treatment*, below) only to certificates that contain the appropriate policy identifier.

13. Revocation Checking

Certificate verification software should confirm that the EV certificate has not been revoked as part of its verification process.

User agents must not grant the EV treatment (see Section 14, *EV Treatment*, below) to EV Certificates that are known to have been revoked.

Certificate verification software should support both CRL and OCSP services. For HTTP OCSP 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 an alternative service, if available.

14. EV Treatment

In cases where the user agent 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 Software Suppliers should consider the EV treatment offered by the user agents of other Application Software Suppliers 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, it is important that the Root Store Manage confirms (initially, and on an ongoing basis) that the CSP's audit is current, identifies no deficiencies and was conducted by a properly qualified auditor. The audit should be performed in accordance with [BRs] and [EVGs].

15.1. EV OIDs in Subject Distinguished Name Fields

Certificate Viewers should provide text equivalents for any OIDs shown to end users. For example, these EV-specific OIDs used in Subject Distinguished Name fields may be displayed as follows (translated accordingly):

subject:businessCategory (2.5.4.15) - "Business Category"

subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1) - "Incorporation Locality" or "Inc. Locality"

subject:jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) "Incorporation State/Province" or "Inc. State/Province"

subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) - "Incorporation Country" or "Inc. Country"

Subject:serialNumber (2.5.4.5) - "Serial Number"

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, some relying parties have been required to assess the suitability of a CSP's policies and practices for the intended usage (e.g. Section 3.3.5 of ITU X.509 (1997-08) defines Certificate Policy as "A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range"). In 2007 (and with later revisions) public CSPs agreed and browsers participating in the CA/Browser Forum began to collaborate on a common set of policies and practices for CAs 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. Because EV Certificates play an important role in securing the online ecosystem, we provide these recommendations to application developers to help them protect users when visiting EV-protected websites.