CA/Browser Forum

RECOMMENDATIONS for the PROCESSING of EXTENDED VALIDATION SSL CERTIFICATES

August 14 2013

Version 2.0

Table of Contents

1. Foreword

This document contains recommendations, established 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 rely on Extended Validation certificates.

3. Normative references

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

[EVSSL] "Guidelines for the Issuance and Management of Extended Validation Certificates", CA/Browser Forum. Available at: https://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 Software Supplier - A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root 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.

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].

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

An Application Software Supplier shall recognize a CSP that is qualified to issue EV SSL certificates by means of the CSP's audit report. The Application Software Supplier should check that the report was issued by an auditor certified to conduct audits in accordance with an acceptable audit program. 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, Application Software Suppliers 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 Software Supplier 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]. 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 Application Software Supplier should store the distinct certificate policy identifier associated with each root certificate, for example, as meta-data.

7. Root-embedding program

Application Software Suppliers that intend to rely upon EV certificates issued by CSPs may implement the following procedures.

7.1. Notification

The Application Software Supplier that intends to rely on EV certificates in a new application may announce its intention in a message sent to the following email address:

questions@cabforum.org

This is intended to ensure that the CA/Browser Forum is aware of the application and simplify the effort of identifying all possible CSPs for possible inclusion in the application. The notice should include the terms upon which such CSPs will be included, as described in Sections 7.2 through 7.6 below. It need not be performed for each new CSP or root certificate that the Application Software Supplier intends to add.

7.2. Agreement

The Application Software Supplier may wish to enter into an agreement separately with each CSP. These agreements should be non-discriminatory, and offer equivalent protections to all relying parties. The agreements should formalize the rights and obligations of the Application Software Supplier 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 Software Supplier's public-key inclusion process

b) The application's root certificate 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 Software Supplier 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 certificate-embedding process. Note: this should not commit the Application Software Supplier 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 Application Software Supplier 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 Application Software Suppliers to test their certificates. Application Software Suppliers should make full use of this mechanism to verify the correct operation of their application.

8. CSP Public-Key Integrity Protection

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

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 Section 14, *EV Treatment*, below) only to certificates that validate successfully.

10. Cryptographic Algorithms and Minimum Key Sizes

The relying application should be capable of processing the cryptographic algorithms and key sizes listed in [EVSSL]. The relying application 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 and these recommendations.

11. Certificate Contents

The relying application 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.

12. Policy Identifier

The relying application should 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 application should grant the EV treatment (see Section 14, *EV Treatment*, below) only to certificates that contain the appropriate policy identifier.

13. Revocation Checking

Applications should confirm that the EV certificate has not been revoked before accepting it.

Certificates for which confirmation has never been obtained must not be granted the EV treatment (see Section 14, *EV Treatment*, below), and should not be treated as trusted certificates.

The application 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 all available alternative services.

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 Software Suppliers should consider the EV treatment offered by 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 Application Software Supplier confirm (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 [EVSSL].

15.1. EV OIDs in Subject Distinguished Name Fields

The Application Software Supplier should ensure that all EV specific OIDs used in Subject Distinguished Name fields are rendered into their human readable format (translated accordingly) as follows:

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, 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.