Public Notary Transparency
Internet-Draft
Intended status: Standards Track
Expires: June 19, 2015

S. Kent
BBN Technologies
R. Andrews
Symantec

December 16, 2014

Syntactic and Semantic Checks for Extended Validation Certificates
draft-kent-trans-extended-validation-cert-checks-00

Abstract

Certificate Transparency (CT) [RFC6962-bis] is a system for publicly logging the existence of X.509 certificates as they are issued or observed. The logging mechanism allows anyone to audit certification authority (CA) activity and detect the issuance of "suspect" certificates. Detecting mis-issuance of certificates is a primary goal of CT.

A certificate is considered to be mis-issued if it fails to meet syntactic and/or semantic criteria associated with the type of certificate being issued. Mis-issuance can be detected by CT log servers, whose feedback to a CA could prompt the CA to not issue a suspect certificate. (Preventing the mis-issuance of such a certificate is preferable to issuing it and detecting it later.)

Compliant CT log servers could offer these checks to a CA submitting a pre-certificate to be logged. These checks are intended to be used in an environment in which CAs optionally assert the version of the EV guidelines to which the submitted pre-certificate purportedly conforms. Log servers would then perform the checks of supported [CABF-EV] versions and include the CA's assertion and the log server's result in its Signed Certificate Timestamp (SCT).

Monitors can also perform checks to detect suspect certificates on behalf of certificate Subjects. Checks performed by a Monitor also serve to double check log servers that claim to have checked a certificate, to identify those that are not doing the checks properly, e.g., because of errors, compromise, or conspiracy. This provides Monitors and CT clients with additional information when choosing which logs to use.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Table of Contents

1. Introduction

The following checks are extracted from the CA Browser Forum (CABF) document "Guidelines for the Issuance and Management of Extended Validation Certificates" version 1.5.2 [CABF-EV]. (If a new version

of the CABF guidelines is created that alters any of the checks described below, a new CCID value MUST be assigned.) These requirements are used to define what constitutes mis-issuance of a certificate in the context of certificate transparency (CT) for Web PKI certificates. The CABF guidelines from which these checks are derived include many aspects of CA operation that are outside of the scope of CT-based detection of certificate mis-issuance, i.e., they impose requirements that could not be verified by a Monitor examining certificate logs. Hence this document was created to provide an enumeration of EV certificate checks for the Web PKI CT context.

The checks enumerated below are to be applied to any certificate submitted to a log with the Certificate Class ID (CCID) value of 2 (see Section X of [CT RFC]). Note that "root" CA certificates are not subject to verification against these criteria. Each log maintains a list of the root CAs for which it is willing to accept SCT generation requests. This implies that the log operator has already determined that these CAs, and their corresponding self-signed certificates, are acceptable. A subordinate CA certificate will be checked only if it is submitted as the target of an SCT. If a subordinate CA certificate appears as part of a chain submitted for SCT generation, but is not the last certificate (the End-Entity or EE certificate) in that chain, the checks enumerated below should be applied to the EE certificate but not the subordinate CA certificate.

[CABF-EV] describes both syntactic and semantic requirements for certificate issuance. This document deals primarily with syntactic checks, but also describes how semantic checks are to be performed. A log MAY perform the syntactic checks enumerated below if a certificate is submitted with a CCID value of 2. If a log performs these syntactic checks, it adds the SSV value appropriate for the outcome of the check (see Section Z of [CT-RFC]).

Monitors SHOULD perform both the syntactic and semantic checks described below for all certificates that they protect, and which are marked with a CCID value of 2.

2. Syntactic Checks

An X.509 certificate consists of a set of fields (all but two of which are mandatory), a set of optional extensions, a public key and a signature. This section defines the syntactic requirements imposed on the certificate fields. The following sections deal with extensions, public keys, and signatures.

2.1. EV Certificate Field Syntax Requirements

[CABF-EV] establishes syntactic requirements for EV certificates. Many of these requirements are the same as for DV certificates. The syntactic checks for DV certificates appear in [RFC-DV]. To avoid possible inconsistency between that RFC and this one, when the syntactic check for an EV certificate is the same as for a DV certificate, the phrase "same as for DV certificates" is inserted.

1. Version number: same as for DV certificates

2. certificate serial number: same as for DV certificates (Note that this is not the Subject Registration Number attribute discussed below.)

3. signature: same as for DV certificates

4. issuer: same as for DV certificates

5. validity: The maximum validity interval is 27 months.

6. subject: A certificate MAY contain a NULL Subject name. If it contains a non-null Subject name:

   A. It MUST contain the organizationName attribute. This requirement is derived from Section 9.2.1 of [CABF-EV].

   B. It MAY contain a commonName attribute. If this attribute is present, it MUST contain a Fully-Qualified Domain Name (not a wildcard name). This requirement is derived from Section 9.2.3 of [CABF-EV].

   C. It MUST contain the businessCategory attribute, and the value of that attribute must match one of the four allowed values. This requirement is derived from Section 9.2.4 of [CABF-EV].

   D. It MUST contain the jurisdictionCountryName attribute as specified in [CABF-EV]. This requirement is derived from Section 9.2.5 of [CABF-EV]. (Note that this attribute is NOT defined in [RFC5280].)

   E. It MAY contain the jurisdictionLocalityName as specified in [CABF-EV]. This requirement is derived from Section 9.2.5 of [CABF-EV]. (Note that this attribute is NOT defined in [RFC5280].)

F. It MAY contain the jurisdictionStateOrProvinceName as specified in [CABF-EV]. This requirement is derived from Section 9.2.5 of [CABF-EV]. (Note that this attribute is NOT defined in [RFC5280].)

G. It MUST contain the Subject Registration Number (also known as Subject:serialNumber) attribute. This requirement is derived from Section 9.2.6 of [CABF-EV].

H. The countryName, stateOrProvinceName and localityName MUST be present and populated with values consistent with the syntax defined in [RFC5280]. This requirement is derived from Section 9.2.7 of [CABF-EV].

I. The localityName, streetAddress, and postalCode attributes MAY be present and if present, MUST be populated with values consistent with the syntax defined in [RFC5280]. This requirement is derived from Section 9.2.7 of [CABF-EV].

J. Other Subject attributes, as specified in Appendix A of [RFC5280], MAY appear. These attributes MUST NOT contain metadata such as '.', '-', or ' ' (i.e. space) characters. This requirement is derived from section 9.2.8 of [CABF-EV].

7. subjectPublicKeyInfo: same as for DV certificates.

8. issuerUniqueId: same as for DV certificates.

9. subjectUniqueId: same as for DV certificates.

10. signatureAlgorithm: same as for DV certificates.

11. signatureValue: same as for DV certificates.

2.2. Certificate Extension Syntax Requirements

An X.509 v3 certificate may contain extensions. [CABF-EV] mandates the presence of several extensions, and imposes requirements on their content.

1. The subjectAltName extension: same requirements as for DV certificates, except Wildcard FQDNs are not permitted. This requirement is derived from Section 9.2.2 of [CABF-EV].

2. A certificate issued to a Subscriber MUST include the certificatePolicies extension. It MAY or MAY NOT be marked CRITICAL. It MUST contain one or more policy identifiers associated with an extended validation policy of the Issuer.

This requirement is derived from Section 9.3.2 and 9.3.5 of [CABF-EV]. There are two commonly cited references for EV OIDs: http://en.wikipedia.org/wiki/Extended_Validation_Certificate and https://code.google.com/p/chromium/codesearch#chromium/src/net/cert/ev_root_ca_metadata.cc&sq=package:chromium

A log or Monitor checking a certificate that purports to be an EV certificate SHOULD use these references to verify that it contains an appropriate policy OID.

This extension MUST contain certificatePolicies:policyIdentifier, certificatePolicies:policyQualifiers:policyQualifierId (id-qt 1) and certificatePolicies:policyQualifiers:qualifier:cPSuri (the URL for the CA's CPS). This requirement is derived from Section 9.7 paragraph (3) of [CABF-EV].

3. basicConstraints: same as for DV certificates.

4. The cRLDistributionPoints extension MUST be present in a CA certificate. It MUST NOT be marked critical and it MUST contain an HTTP URL. This extension MUST be present in a Subscriber certificate if the certificate does not specify an OCSP responder location in the authorityInformationAccess extension.

5. keyUsage extension: same as for DV certificates.

6. authorityInformationAccess extension: same as for DV certificates

7. extendedKeyUsage extension: same as for DV certificates.

8. nameConstraints extension: same as for DV certificates

9. Other extensions defined in [RFC5280]: same as for DV certificates.

2.3. Certificate Public Key: same as for DV certificates

2.4. Certificate Signature: same as for DV certificates

3. Semantic Verification of an EV Certificate

The fundamental semantic check that a Monitor MUST perform is to detect bogus certificates on behalf of its clients. A client of a Monitor provides the Monitor with a set of certificates that have been issued to the client. (Note that a client may have multiple certificates issued to its name, and thus there is not a one-to-one mapping between names and public keys.) These certificates MUST be acquired in a secure fashion, not using certificate discovery

protocols or relying on databases operated by a CA or RA. Armed with this information, a Monitor can examine every log entry to determine if it contains the same Subject or subjectAltName as that of a client. If a log entry matches either of these names, and if it contains a public key distinct from the set of keys provided by the Subject, this is evidence of mis-issuance. (Note that a Monitor cannot rely on a log operated by a CA, to detect mis-issuance by that CA.) If a Monitor identifies what appears to be a bogus certificate, it notifies the client. The means by which notification is effected is not specified.

[CABF-EV] imposes a number of requirements on certificate issuance that cannot be verified without access to reference information for the certificate Subject, information about the CA hierarchy, or information about internal procedures of the CA. Monitors are not presumed to be able to perform such checks. Examples of such checks appear in Sections 7, 8, 9.1, and 9.2.4 of [CABF-EV].

Additional semantic checks SHOULD be performed by a Monitor, if it has access to the requisite information. These are enumerated below.

1. A certificate issued to a subordinate CA that is not controlled by a Root CA MUST NOT contain the anyPolicy policy identifier. This requirement is derived from section 9.3.4 (1) of [CABF-EV]. Verification of this requirement requires knowledge of CA organizational relationships and thus may not be available to all Monitors.

2. A certificate issued to a subordinate CA that is not controlled by the issuing CA MUST include one or more policy identifiers defined by the issuing CA that explicitly identify the EV Policies that are implemented by the Subordinate CA. This requirement is derived from section 9.3.4 (1) of [CABF-EV]. If the extension contains any of the OIDs noted explicitly above, it is acceptable. Verification of this requirement requires knowledge of CA organizational relationships and thus may not be available to all Monitors.

3. The Subject's Jurisdiction of Incorporation, Registration, or Place of Business MUST not be in any country with which the laws of the CA's jurisdiction prohibit doing business. This suggestion is derived from Section 11.12.2 (1) (B) of [CABF-EV].

4. The Subject's organizationName attribute MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, although

abbreviations are permitted. This requirement is derived from Section 9.2.1 of [CABF-EV].

5. The Domain Names in the subjectAltName extension MUST be owned or controlled by the Subject, or MUST have been owned or controlled by the Subject at the time of certificate issuance. This requirement is derived from Section 9.2.2 of [CABF-EV].

6. The Domain Name in the Subject Common Name field, if present, MUST be owned or controlled by the Subject, MUST have been owned or controlled by the Subject at the time of certificate issuance. This requirement is derived from Section 9.2.2 of [CABF-EV].

7. The Subject Jurisdiction of Incorporation or Registration Fields MUST not contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. This requirement is derived from Section 9.2.5 of [CABF-EV].

8. The Subject Physical Address of Place of Business Fields MUST contain the address of a physical location of the Subject's Place of Business. This requirement is derived from Section 9.2.7 of [CABF-EV].

4. IANA Considerations

TBD

5. Security Considerations

TBD

6. References

6.1. Informative References

[CABF-EV] CA/Browser Forum, "Guidelines For The Issuance And Management Of Extended Validation Certificates, Version 1.5.2", October 2014, <https://cabforum.org/wp-content/uploads/EV-V1_5_2Libre.pdf>.

6.2. Normative References

[I-D.ietf-trans-rfc6962-bis] Laurie, B., Langley, A., Kasper, E., and R. Stradling, "Certificate Transparency", draft-ietf-trans-rfc6962-bis-04 (work in progress), July 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Stephen Kent
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
US

Email: kent@bbn.com

Rick Andrews
Symantec
350 Ellis Street
Mountain View, CA 94043
US

Email: Rick_Andrews@symantec.com