Public Notary Transparency
Internet-Draft
Intended status: Standards Track
Expires: June 24, 2016
December 22, 2015

S. Kent
BBN Technologies
R. Andrews
Symantec

Syntactic and Semantic Checks for Domain Validation Certificates
draft-kent-trans-domain-validation-cert-checks-02

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-DV] 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 will expire on June 24, 2016.

Copyright Notice

Table of Contents

1. Introduction

The following checks are extracted from the CA Browser Forum (CABF) document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" version 1_2_3 [CABF-DV]. (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 DV 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 1 (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 certificates of CAs (that MUST begin the certificate validation path) 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 are applied to the EE certificate but not the subordinate CA certificate.

[CABF-DV] 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 1. 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]) to the SCT.

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 1.

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. DV Certificate Field Syntax Requirements

1. Version number: The certificate MUST be an X.509 v3 certificate. This requirement is derived from Appendix B of [CABF-DV], where it is explicitly stated for Root and Subordinate CA certificates. Since other portions of [CABF-DV] mandate support for extensions and only v3 certificates can contain extensions [RC5280], this requirement is inferred to apply to EE certificates as well.

2. serialNumber: No requirements beyond those imposed by [RFC5280] are mandated by [CABF-DV]. Section 9.6 of [CABF-DV] suggests that a serial number contain at least 20 bits of entropy so the minimum serialNumber length should be 20 bits.

3. signature: For any certificate issued after December 31, 2010, the allowed digest algorithms are: SHA-1, SHA-256, SHA-384 or SHA-512. If RSA is used to sign the certificate, the minimum modulus size is 2048 bits. (No requirement is imposed on the public exponent.) If DSA is used to sign the certificate, the following pairs of values are permitted: L= 2048, N= 224 or L= 2048, N=256). If the certificate signature is based on ECC (presumably ECDSA), the allowed curves are NIST P-256, P-384 and P-521. To verify that a certificate employs an accepted digest and signature algorithm, one examines the OID contained in this field. OIDs defined in the following RFCs are applicable here: [RFC4055], [RFC5480], and [RFC5758]. (This set of checks does not apply to certificates issued before the date cited above.)

4. issuer: The Issuer name MUST contain the countryName attribute and it MUST contain an ISO-3166-1 country code. This requirement is derived from section 9.1.4 of [CABF-DV]. The Issuer name MUST contain the organizationName attribute. This requirement is derived from section 9.1.3 of [CABF-DV].

5. validity: An EE certificate issued after July 1, 2012 MUST not contain a validity interval longer than 60 months. ([CABF-DV] establishes criteria in Section 9.4.1 that describe the circumstances under which EE certificates may be issued with validity intervals between 39 and 60 months. Since these criteria cannot be evaluated without external knowledge, this RFC adopts the 60-month limit for syntactic checking.)

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

A. it MAY contain a commonName attribute. If this attribute is present, it MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension. This requirement is derived from section 9.2.2 of [CABF-DV]. Thus verification of this attribute requires comparing values in this attribute against the content of the subjectAltName extension, which MUST be present (see below).

B. it MAY contain an organizationalUnitName attribute. This requirement is derived from section 9.2.6 of [CABF-DV].

C. if the name does not contain an organizationName attribute, then the streetAddress attribute MUST NOT be present. If the organizationName attribute is present, the streetAddress attribute MAY be present. This requirement is derived from section 9.2.4b of [CABF-DV].

D. if the name does not contain an organizationName attribute, then the localityName attribute MUST NOT be present. If the organizationName attribute is present, the localityName attribute MAY be present. This requirement is derived from section 9.2.4c of [CABF-DV].

E. if the name does not contain an organizationName attribute, then the stateOrProvinceName attribute MUST NOT be present. If the organizationName attribute is present, and the localityName is absent, then the stateOrProvinceName attribute MUST be present. If the organizationName attribute is present, and the localityName is present, then the stateOrProvinceName attribute MAY be present. This requirement is derived from section 9.2.4d of [CABF-DV].

F. if the name does not contain an organizationName attribute, then the postalCode attribute MUST NOT be present. If the name contains an organizationName attribute, then the postalCode attribute MAY be present. This requirement is derived from section 9.2.4e of [CABF-DV].

G. if the name contains an organizationName attribute, then the countryName attribute MUST be present. If the name does not contain an organizationName attribute, then the countryName attribute MAY be present. This requirement is derived from section 9.2.5 of [CABF-DV].

H. The Subject MAY contain other attributes as specified in Appendix A of [RFC5280]. These attributes MUST NOT contain

metadata such as '.', '-', or ' ' (i.e. space) characters. This requirement is derived from section 9.2.8 of [CABF-DV].

7. subjectPublicKeyInfo: If this field contains an RSA public key the minimum modulus size is 2048 bits. (No requirement is imposed on the public exponent.) If it carries a DSA key, the following pairs of values are permitted: L= 2048, N= 224 or L= 2048, N=256. If the field conveys an ECC (presumably ECDSA) public key, the allowed curves are NIST P-256, P-384 and P-521. To verify that a certificate employs an accepted digest and signature algorithm, one examines the OID contained in this field. OIDs defined in the following RFCs are applicable here: [RFC4055], [RFC5480], and [RFC5758].

8. issuerUniqueId: This is an optional field (a BIT STRING) in a v3 certificate. [CABF-DV] imposes no requirements on this field, so no constraints beyond those in [RFC5280] are applicable.

9. subjectUniqueId: This is an optional field (a BIT STRING) in a v3 certificate. [CABF-DV] imposes no requirements on this field, so no constraints beyond those in [RFC5280] are applicable.

10. signatureAlgorithm: This field MUST match the signature field contained within the certificate (see # 3 above).

11. signatureValue: This field is verified using the public key extracted from the certificate of the Issuer of this certificate, and the algorithms specified in the preceding field.

2.2. DV Certificate Extension Syntax Requirements

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

1. The certificate MUST contain the subjectAltName extension, and that extension MUST contain at least one entry. Each entry MUST be either a dNSName containing a Fully-Qualified Domain Name (FQDN) or an iPAddress. Wildcard FQDNs are permitted. No other entry types are permitted. This requirement is derived from section 9.2.1 of [CABF-DV].

2. A certificate issued to a CA MUST include the certificatePolicies extension. It MAY or MAY NOT be marked CRITICAL. The policyQualifiers field MAY be present, and the policyQualifierId and/or the cPSuri fields may be populated, using the syntax

specified in [RFC5280]. This requirement is derived from Appendix B, Section 3.A of [CABF-DV].

A. If this extension contains the OID 2.23.140.1.2.1, then the Subject field MUST NOT contain an organizationName, streetAddress, localityName, stateOrProvinceName, or postalCode attribute. This requirement is derived from section 9.3.1 of [CABF-DV].

B. If this extension contains the OID 2.23.140.1.2.2, then the Subject field MUST contain organizationName, localityName, and countryName attributes. This requirement is derived from section 9.3.1 of [CABF-DV]. ([CABF-DV] also states that the stateOrProvinceName attribute MUST be present, "if applicable". Since the applicability of this attribute cannot be readily determined, this Appendix views the presence of this attribute as optional.)

3. The basicConstraints extension MUST be present, marked CRITICAL and the cA flag MUST be set TRUE in a CA certificate. This requirement is derived from Appendix B Section 2.D of [CABF-DV]. The presence of this extension is optional for an EE certificate. If the extension is present in an EE certificate it MUST have the cA flag set to FALSE. (If a certificate does not contain this extension it is presumed to be an EE certificate and MUST be processed as such with regard to all other verification checks.)

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 is optional for EE certificates, but if present the same syntactic constraints apply. This requirement is derived from Appendix B, Sections 2.B and 3.B of [CABF-DV].

5. The keyUsage extension MUST be present in a CA certificate and it MUST be marked critical. The keyCertSign and cRLSign bits MUST be set. The digitalSignature bit MAY be set as well. The keyUsage extension MAY be present in an EE certificate. If it is present in an EE certificate, the keyCertSign and cRLSign bits MUST NOT be set. These requirements are derived from Appendix B, Section 2.E of [CABF-DV].

6. The authorityInformationAccess extension MAY be present and, if present, MUST NOT be marked CRITICAL and MUST contain accessMethod 1.3.6.1.5.5.7.48.1 and MAY specify accessMethod 1.3.6.1.5.5.7.48.2. This requirement is derived from Appendix B, Sections 2.C and 3.C of [CABF-DV].

7. The extKeyUsage extension MAY be present in a CA certificate. If present, it need not be marked CRITICAL. If the extension is present in a CA certificate, and if the certificate contains the nameConstraints extension, then the value id-kp-serverAuth MUST be present. This requirement is derived from Section 9.7 and Appendix B, Section 2.G of [CABF-DV]. The extKeyUsage extension MUST be present in an EE certificate. Either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present. id-kp-emailProtection MAY be present. This requirement is derived from Appendix B, Section 3.F of [CABF-DV].

8. The nameConstraints extension MAY appear in CA certificates and need not be marked CRITICAL (contrary to [RFC5280]). If the certificate also contains the extKeyUsage extension and that extension contains the value id-kp-serverAuth, then that extension MUST NOT contain the anyExtendedKeyUsage value in the KeyPurposeId. Moreover, the nameConstraints extension MUST impose constraints on dNSName, iPAddress and DirectoryName name types. Both the permittedSubtrees and excludedSubtrees fields MAY be employed. This requirement is derived from Section 9.7 and Appendix B, Section 2.F of [CABF-DV].

9. Other extensions defined in [RFC5280] MAY be present and MUST be marked with respect to criticality as specified therein.

2.3. Certificate Public Key

2.3.1. RSA Public Keys

1. If a subordinate CA certificate contains an RSA public key, and the certificate has a validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013, that key MUST have a minimum modulus size of 1024 bits. If a subordinate CA certificate contains an RSA public key, and the certificate has a validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013, that key MUST have a minimum modulus size of 2048 bits. This requirement is derived from Appendix A (2) of [CABF-DV].

2. If an EE certificate contains an RSA public key, and the certificate has a validity period ending on or before 31 Dec 2013, that key MUST have a minimum modulus size of 1024 bits. If an EE certificate contains an RSA public key, and the certificate has a validity period ending after 31 Dec 2013, that key MUST have a minimum modulus size of 2048 bits. This requirement is derived from Appendix A (3) of [CABF-DV].

3. The value of the public exponent of an RSA public key MUST be an odd number equal to 3 or more. This requirement is derived from Appendix A (4) of [CABF-DV].

2.3.2. DSA Public Keys

1. If a certificate contains a DSA public key, the minimum modulus and divisor size (in bits) MUST be L= 2048, N= 224 or L= 2048, N= 256. This requirement is derived from Appendix A (2) and (3) of [CABF-DV].

2. If a certificate contains a DSA public key, the public key MUST include all domain parameters. This requirement is derived from Appendix A (4) of [CABF-DV].

2.3.3. ECC Public Keys

1. If a certificate contains an ECC public key, that key MUST employ one of these curves: NIST P-256, P-384, or P-521. This requirement is derived from Appendix A (2) and (3) of [CABF-DV].

2.4. Certificate Signature

The certificate's signatureAlgorithm MUST be SHA-1, SHA-256, SHA-384 or SHA-512. This requirement is derived from Appendix A (2) and (3) of [CABF-DV].

3. Semantic Verification of a DV 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 other than the one(s) provided by the Subject, this is evidence of mis-issuance. A Monitor SHOULD track activity in all logs that are considered trustworthy by its clients. There is no mechanism defined that allows a Monitor to know what logs belong to this set. Thus it is RECOMMENDED that each Monitor make known the set of logs that it tracks, and each client is advised to select a Monitor that satisfies the client's criteria in this regard. 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-DV] 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 7.1, 9.1.3, 9.1.4, 9.2.4a, 9.2.6, 9.4.1 and 9.5 of [CABF-DV].

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 an affiliate of a "root" CA MUST NOT contain the anyPolicy policy identifier. This requirement is derived from section 9.3.3 of [CABF-DV]. 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 an affiliate of a "root" CA MAY include one or more explicit policy identifiers (either 2.23.140.1.2.1 or 2.23.140.1.2.2 or policy identifiers defined by the CA in its CP and/or CPS). It also MAY include the anyPolicy OID. This requirement is derived from section 9.3.3 of [CABF-DV]. 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.

4. IANA Considerations

TBD

5. Security Considerations

TBD

6. References

6.1. Informative References

[CABF-DV] CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.3", October 2014, <https://cabforum.org/wp-content/uploads/BRv1.2.3.pdf>.

6.2. Normative References

[I-D.ietf-trans-rfc6962-bis]
Laurie, B., Langley, A., Kasper, E., Messeri, E., and R. Stradling, "Certificate Transparency", draft-ietf-trans-rfc6962-bis-11 (work in progress), November 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

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