spasm
Internet-Draft June 20, 2017
Intended status: Experimental
Expires: December 22, 2017

Certificate Limitation Policy
draft-belyavskiy-certificate-limitation-policy-00

Abstract

The document provides a specification of the application-level trust model. Being provided at the application level, the limitations of trust can be distributed separately using cryptographically protected format instead of hardcoding the checks into the application itself.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 22, 2017.

1. Introduction

Binary trust model standardized as a set of trusted anchors and CRLs/ OCSP services does not cover all corner cases in the modern crypto world. There is a need in more differentiated limitations. Some of them are suggested by Google when it limits the usage of Symantec's certificates. The CRL profile does not fit the purpose of such limitations. The CRLs are issued by the same CAs that are subject to be limited.

Currently the set of CAs trusted by OS can be used for the validation purposes. In case when a large enough CA becomes untrusted, it cannot be deleted from the storage of trusted CAs because it may cause error of validation of many certificates. The measures usually taken in such cases usually include application-level limitation of certificates lifetimes, refuse to accept EV-certificates in other way than DV, requirements of usage Certificate Transparency, etc.

This document suggests a cryptographically protected format of description of such limitations. This format can be used by applications that use system-wide set of trust anchors for validating purposes or by applications with own wide enough set of trusted anchors in case when the trust anchor for the entity found misbehaving cannot be revoked.

Currently the only way to provide such limitations is hard coding in application itself. Using of CLPs does not allow to completely avoid hard coding but allows to hard code only the minimal set of rarely changing data, such as the certificate to verify the signature and minimal date of issuance (see below).

2. Certificate Limitations Profile

A proposed syntax and overall structure of CLP is very similar to the one defined for CRLs. TBD.

2.1. CLP fields

TBD

2.2. CLP extensions

TBD

2.3. CLP signature

The key used for signing the CLP files should have a special Key Usage bit and/or an Extended Key Usage value.

2.4. CLP entry fields

Each entry in list contains the following fields:

The issuer of the certificate with limited trust.

The serial of the certificate with limited trust.

The fingerprint of the certificate with limited trust (optional).

The flag indicating whether limitations are applied to the certificate itself or to all of its descendants in the chain of trust.

and a subset of the following limitations:

maxPeriodStart (do not trust the certs issued after)

maxPeriodEnd (do not trust the certs after)

validityPeriod (take minimal value from "native" validity period and specified in the limitation file)

ignoreX509Extensions (e.g. EV)

requiredX509extensions (do not trust the certificates)

The limitations are identified by OIDs

2.4.1. Limitations

2.4.1.1. maxPeriodStart

When this limitation is present, no certificate matching the entry and issued after the specified date should not be trusted

2.4.1.2. maxPeriodEnd

When this limitation is present, no certificate matching the entry should be trusted after the specified date.

2.4.1.3. validityPeriod

When this limitation is present, no certificate matching the entry should be treated as valid after specified period from its validFrom.

2.4.1.4. ignoreX509Extensions

When this limitation is present, the extensions listed in this element should be ignored for the matching certificate.

2.4.1.5. requiredX509extensions

When this limitation is present, the extensions listed in this element should be present for the matching certificate.

3. ASN.1 notation

TBD

4. Security considerations

In case when an application uses CLP, it is recommended to specify the minimal date of issuing of the CLP document somewhere in code. It allows to avoid an attack of CLP rollback when the stale version of CLP is used.

5. IANA considerations

6. Acknoledgements

7. References

The current version of the document is available on GitHub https://github.com/beldmit/clp

Author's Address

Dmitry Belyavskiy

Email: beldmit@gmail.com