

Internet X.509 Public Key Infrastructure
Warranty Certificate Extension

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document describes a certificate extension to explicitly state the warranty offered by a Certificate Authority (CA) for the certificate containing the extension.

1. Introduction

The warranty certificate extension identifies the warranty policy associated with a X.509 public key certificate [X.509-97, PROFILE]. Often the Certificate Authority (CA) will obtain an insurance policy to ensure coverage of the warranty.

The certificate warranty provides an extended monetary coverage for the end entities. The certificate warranty primarily concerns the use, storage, and reliance on a certificate by a subscriber, a relying party, and the CA. It is common for a CA to establish reliance limits on the use of a certificate. It is not uncommon for a CA to attempt through contractual means to exclude its liability entirely. However, this undermines the confidence that commerce requires to gainfully use certificates.

Alternatively a CA may provide extended coverage for the use of the certificate. Usually, the subscriber pays for the extended warranty coverage. In turn, subscribers are covered by an appropriately drafted insurance policy. The certificate warranty is backed by an insurance policy issued by a licensed insurance company, which results in a financial backing that is far greater than that of the

CA. This extra financial backing provides a further element of confidence necessary to encourage the use of certificates in commerce.

A relying party that has a warranty from a CA may obtain compensation from a CA depending on the conditions for such compensation expressed in either the CA's Certificate Policy, the CA's insurance policy, or both. Evidence of an extended warranty, provided through the certificate extension, will give the relying party additional confidence that compensation is possible, and therefore will enhance trust in the process. Risk for a non-subscriber relying party may be reduced by the presence of a warranty extension with an explicit warranty stated. The warranty extension allows this aspect of risk management to be automated.

When a certificate contains a warranty certificate extension, the extension MUST be non-critical, and MUST contain either a NULL to indicate that no warranty is provided or base warranty data to indicate that a warranty is provided. The extension MAY contain optional qualifiers.

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Warranty Extension Format

Like all X.509 certificate extensions, the warranty certificate extension is defined using ASN.1 [X.208-88, X.209-88].

The non-critical warranty extension is identified by id-pe-warranty.

PKIX Object Identifier Registry

```
id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
                                dod(6) internet(1) security(5) mechanisms(5) pkix(7) }
```

PKIX Arcs

```
id-mod OBJECT IDENTIFIER ::= { id-pkix 0 }      -- modules
id-pe  OBJECT IDENTIFIER ::= { id-pkix 1 }      -- private
certificate extensions
```

PKIX modules

```
id-mod-warranty-extn          OBJECT IDENTIFIER ::= { id-mod 27 }
```

```
id-pe-warranty OBJECT IDENTIFIER ::= { id-pe 16 }
```

A non-null warranty always includes a base warranty. The warranty information includes the period during which the warranty applies, a warranty value, and a warranty type. The warranty type tells the warranty limit against claims. The extension definition supports two alternatives: aggregated and per-transaction. With aggregation, claims are fulfilled until a ceiling value is reached. After that, no further claims are fulfilled. With per-transaction, a ceiling value is imposed on each claim, but each transaction is considered independently.

The warranty extension permits inclusion of two optional warranty qualifiers. The first qualifier provides extended warranty information, the second provides a pointer to the warranty terms and conditions.

When present, the extended warranty information provides information about coverage beyond the scope of the base warranty. Like the base warranty information, the extended warranty information includes the period during which the warranty applies, a warranty value, and a warranty type.

When present, the terms and conditions pointer provides a reference to a document containing the terms and conditions associated with the warranty. The document may be a Certificate Policy that contains this information, a document specifically about the warranty, or a Relying Party Agreement. The pointer is always a uniform resource locator (URL). The URL MUST be a non-relative URL using the http scheme. The URL MUST follow the URL syntax and encoding rules specified in RFC 3986 [URI].

2.1. Warranty Extension Syntax

The syntax for the warranty extension is:

```
Warranty ::= CHOICE {
    none          NULL,          -- No warranty provided
    wData         WarrantyData   } -- Explicit warranty

WarrantyData ::= SEQUENCE {
    base          WarrantyInfo,
    extended      WarrantyInfo OPTIONAL,
    tcURL         TermsAndConditionsURL OPTIONAL }

WarrantyInfo ::= SEQUENCE {
    validity      WarrantyValidityPeriod,
    amount        CurrencyAmount,
    wType         WarrantyType }
```

```

WarrantyValidityPeriod ::= CHOICE {
    sameAsCertificate      NULL,
    explicitPeriod         ValidityPeriod }

ValidityPeriod ::= SEQUENCE {
    notBefore              GeneralizedTime,
    notAfter               GeneralizedTime }

-- CurrencyAmount specifies the currency and a monetary value.
-- Currency codes are defined in [ISO4217]. The monetary value
-- is: amount / (10 ** amtExp10), and the exponent MUST be the
-- minor unit of currency specified in [ISO4217].

CurrencyAmount ::= SEQUENCE {
    currency              INTEGER (1..999),
    amount                INTEGER (0..MAX),
    amtExp10              INTEGER (0..MAX) }

WarrantyType ::= INTEGER {
    aggregated            (0),
    perTransaction       (1) }

TermsAndConditionsURL ::= IA5String -- MUST use http scheme

```

2.2. Warranty Extension Semantics

Warranty is a CHOICE; it is represented either by NULL or WarrantyData. If the CA selects NULL, then the CA is explicitly stating that no warranty is provided. If the CA selects WarrantyData, then the CA is explicitly stating that a warranty is provided, and the fields within the WarrantyData type MUST provide details about that warranty.

WarrantyData MUST contain information about the base warranty. WarrantyData MAY contain information about an extended warranty. Both base warranty and extended warranty information is provided using the WarrantyInfo type. WarrantyData MAY contain a URL that points to the terms and conditions of the warranty. The URL is provided using the TermsAndConditionsURL type, which is an IA5 string. The IA5String MUST contain a URI [URI] using the http scheme, such as "http://www.example.com/warranty/t_and_c.html".

WarrantyInfo MUST contain the warranty validity period, the currency amount of the warranty, and the type of warranty. The warranty validity period is provided using the WarrantyValidityPeriod type. The currency amount of the warranty is provided using the CurrencyAmount type. The type of warranty is provided using the WarrantyType type.

WarrantyValidityPeriod is a CHOICE; it is represented either by NULL or ValidityPeriod. If the CA selects NULL, then the validity periods of the warranty and the certificate MUST be exactly the same. If the CA selects ValidityPeriod, then the CA is explicitly stating a warranty validity period that is different than the validity period of the certificate. If the validity periods of the warranty and the certificate are the same, then the CA MUST select the NULL choice. The validity periods are expected to be the same in the vast majority of the cases. ValidityPeriod is a SEQUENCE of two GeneralizedTime values. The first (notBefore) GeneralizedTime value MUST indicate the date and time that the warranty becomes valid, and the second (notAfter) GeneralizedTime value MUST indicate the date and time that the warranty expires.

CurrencyAmount is a SEQUENCE of three integers which together specify the currency and a monetary value. The first integer (currency) MUST indicate the currency using one of the currency codes defined in [ISO4217]. The second integer (amount) MUST indicate the value of the warranty. The third integer (amtExp10) MUST indicate the correct placement of the decimal point in the monetary value, and MUST be the minor unit of currency specified in [ISO4217]. For example \$48,525.50 (in US dollars) is represented as:

```
currency =      840
amount   = 4852550
amtExp10 =       2
```

WarrantyType is an integer. A value of zero indicates that claims against the warranty will be aggregated, and once the value of fulfilled claims reaches the warranty currency amount, then no further claim will be fulfilled. A value of one indicates that each claim is handled independently, but no individual claim can exceed the warranty currency amount. The CA MUST select either zero or one for this integer value.

3. Security Considerations

The procedures and practices employed by the CA MUST ensure that the correct values for the warranty are inserted in each issued certificate. Relying parties and users may accept or reject a particular certificate for an intended use based on the information provided in warranty extension. Incorrect representation of the actual warranty may result in otherwise avoidable warranty claims for the CA.

4. IANA Considerations

Certificate extensions and extended key usage values are identified by object identifiers (OIDs). The OIDs used in this document are derived from X.509 [X.509-97]. No further action by the IANA is necessary for this document or any anticipated updates.

5. ASN.1 Module

```

WarrantyExtn
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-warranty-extn(27) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- OID Arcs

id-pe OBJECT IDENTIFIER ::=
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) 1 }

-- Warranty Extension

id-pe-warranty-extn OBJECT IDENTIFIER ::= { id-pe 16 }

Warranty ::= CHOICE {
    none                NULL,                -- No warranty provided
    wData               WarrantyData } -- Explicit warranty

WarrantyData ::= SEQUENCE {
    base                WarrantyInfo,
    extended            WarrantyInfo OPTIONAL,
    tcURL               TermsAndConditionsURL OPTIONAL }

WarrantyInfo ::= SEQUENCE {
    validity            WarrantyValidityPeriod,
    amount             CurrencyAmount,
    wType              WarrantyType }

WarrantyValidityPeriod ::= CHOICE {
    sameAsCertificate   NULL,
    explicitPeriod      ValidityPeriod }

```

```
ValidityPeriod ::= SEQUENCE {
    notBefore      GeneralizedTime,
    notAfter       GeneralizedTime }

-- CurrencyAmount specifies the currency and a monetary value.
-- Currency codes are defined in [ISO4217]. The monetary value
-- is: amount / (10 ** amtExp10), and the exponent MUST be the
-- minor unit of currency specified in [ISO4217].

CurrencyAmount ::= SEQUENCE {
    currency      INTEGER (1..999),
    amount        INTEGER (0..MAX),
    amtExp10      INTEGER (0..MAX) }

WarrantyType ::= INTEGER {
    aggregated     (0),
    perTransaction (1) }

TermsAndConditionsURL ::= IA5String

END
```

6. Normative References

- [ISO4217] ISO. "Codes for the Representation of Currencies and Funds", ISO 4217. 1995.
- [PROFILE] Housley, R., Ford, W., Polk, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.
- [URI] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.
- [X.208-88] CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.
- [X.209-88] CCITT. Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.

7. Informative References

- [X.509-97] ITU-T. Recommendation X.509: The Directory-Authentication Framework. 1997.

Acknowledgements

This document was developed with the expertise and support of Russ Housley, Vigil Security LLC, and Dr. Adrian McCullagh, Freehills Australia.

Authors' Addresses

Duane Linsenbardt
SPYRUS
2355 Oakland Road
Suite 1
San Jose CA 95131
USA

Email: dlinsenbardt@spyrus.com

Sue Pontius
SPYRUS
2355 Oakland Road
Suite 1
San Jose CA 95131
USA

Email: spontius@spyrus.com

Alice Sturgeon
SPYRUS
Suite 1502, 222 Queen St.,
Ottawa ON K0A 2T0
Canada

Email: asturgeon@spyrus.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

