PKIX Working Group
Internet-Draft
Expires: December 9, 2002

J. Schlyter
Carlstedt Research & Technology
L. Johansson
Stockholm University

June 10, 2002

DNS as X.509 PKIX Certificate Storage
draft-schlyter-pkix-dns-02

Status of this Memo

This Internet-Draft will expire on December 9, 2002.

Copyright Notice

Abstract

A major problem facing PKIX deployment and implementation is the problem of constructing certificate paths for input to the path validation algorithm. This draft describes the use of the DNS as a certificate store and it's implication for path validation in PKIX.

Table of Contents

1. Introduction

A major problem facing PKIX deployment and implementation is the problem of constructing certificate paths for input to the path validation algorithm described in RFC 2459 [2]. This problem can be solved by successively looking at the issuerAltName extension of each certificate and using the information found there together with a storage and transport protocol for certificates to find a set of candidate certificates associated with the issuerAltName.

Using the CERT RR [5] a certificate can be published using DNS. This draft describes the use of DNS as a certificate store and it's implication for path validation in PKIX.

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 RFC 2119 [1].

2. Storing PKIX certificates in DNS

A PKIX certificate is published in DNS using the CERT RR [5] for a given domain name which SHOULD be equal to the dnsName component of the subjectAltName extension in the certificate. Multiple certificates may be present for each domain name and all SHOULD have the same subject DN. If the domain name does not match the dnsName component of the subjectAltName extension the client SHOULD notify the user of this and allow the user to decide weather to allow the use of the certificate or not.

When constructing a certificate path for validation the client MAY use the AuthorityKeyIdentifier and SubjectKeyIdentifier extensions to select the (set of) certificates to use.

There are a few important cases when multiple CA certificates are published in CERT RRs for given domain name:

Multiple certificates each signed by another member of the same set. This situation occurs when a self-signed certificate issues a certificate under the same DN (for the purpose of adding policy for instance).

Multiple certificates, either self-signed or issued by another CA, with different validity periods.

Root key roll-over as described in section 2.4 of RFC 2510 [3] where exactly 4 certificates would be published using DNS.

3. Certificate lookup algorithm

Given a certificate with a non-empty issuerAltName extension of type dnsName, perform a DNS lookup of the corresponding domain name with the class IN and type CERT. For each of the certificates returned that are of type PKIX, implementations SHOULD verify that the subjectAltName in the certificate contains a component of type dnsName with the same domain name as the one where the certificate was published using the DNS.

If a certificate obtained by this algorithm is a self-signed certificate and was successfully verified by DNSSEC [4], the user SHOULD be given the opportunity to use this certificate as a trust anchor.

The result of this algorithm is a set of of certificates suitable for input to the PKIX path validation algorithm.

4. Example

Client A talks TLS to server B and receives a certificate chain ending in a cert (X) with issuerAltName:dnsName set to ca.example.com.

Client A does path validation on the chain and is unable to find X in its list of trusted roots.

Client A queries the DNS for the CERT record for ca.example.com and receives a set of certificates.

Client A looks for X in the set of certificates. If found, and depending on local configuration, A trusts the certificate for use as a TLS client trust anchor and adds it to the list of trusted roots.

Path validation now succeeds.

5. Security Considerations

This document describes a mechanism for automated download of certificates from DNS with special provision for bridging trust between a PKIX PKI and DNSSEC. However, if only self-signed end-entity PKIX certificates are published using DNS the benefits of PKIX policy and key usage management is lost.

The benefit of this mechanism is a potential for added protection of certificate trust anchors in common use on the Internet by leveraging

DNSSEC infrastructure.

References

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

[2] Housley, R., Ford, W., Polk, T. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[3] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[4] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[5] Eastlake, D. and O. Gudmundsson, "Storing Certificates in the Domain Name System (DNS)", RFC 2538, March 1999.

Authors' Addresses

Jakob Schlyter
Carlstedt Research & Technology
Stora Badhusgatan 18-20
Goteborg SE-411 21
Sweden

EMail: jakob@crt.se
URI: http://www.crt.se/~jakob/

Leif Johansson
Stockholm University
IT and Media Unit
Frescati Hagvag 8
Stockholm SE-106 91
Sweden

Phone: +46 8 16 45 41
EMail: leifj@it.su.se
URI: http://www.it.su.se

Appendix A. Acknowledgements

The author gratefully acknowledges, in no particular order, the contributions of the following persons:

Martin Fredriksson

Niklas Hallqvist

Edward Lewis

Full Copyright Statement

Acknowledgement

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