Network Working Group
Internet Draft
Intended Status: Standards Track
Expires: April 18, 2011

R. Housley
Vigil Security
T. Polk
NIST
S. Turner
IECA

October 18, 2010

DNSSEC-centric PKI
draft-turner-dnssec-centric-pki-00.txt

Abstract

This draft is input to the KIDNS discussion. The procedures defined herein provide a general Public Key Infrastructure (PKI) mechanism that leverages DNSSEC. This is compatible with RFC 5280.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

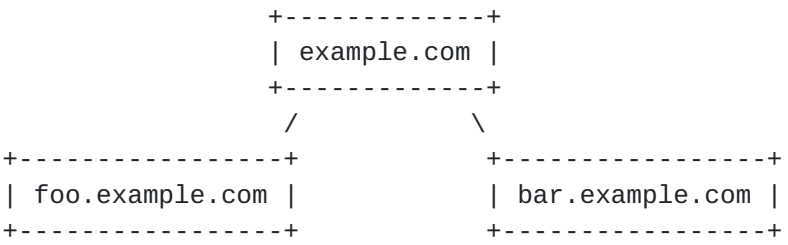
This Internet-Draft will expire on April 18, 2011.

1. Introduction

This draft is not to be construed as direction from I*. It is the output of an actual "interim" Bar BoF held at conference room H located in Fairfax, Virginia after the IAB/IESG OAM workshop on 2010-10-13.

Certification Authorities (CAs) take great care to ensure that the private key holder is associated with the domain name contained in the certificate. DNSSEC [RFC4033][RFC4034][RFC4035] offers an opportunity to eliminate complicated off-line processes. This relationship can be easily demonstrated by having the zone administrator for the domain name in question post the certificate [RFC5280] in the DNS and digitally sign the resulting zone.

With the following hierarchy:



Administrators of foo.example.com and bar.example.com can choose to either trust the root (i.e., the signer of example.com) or another entity that they have included in the DNS entry they control.

1.1. Terminology

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. Procedures

Perform a DNSSEC retrieval on the domain name, verifying the chain of trust to a locally configured DNSSEC trust anchor.

If a Certification Authority (CA) certificate is returned, rather than an end-entity (EE) certificate, construct a certification path. It is a matter of local policy whether the CA certificate is accepted as a trust anchor (TA) directly, or MUST chain to a currently configured TA. To differentiate CA certificates from EE certificates, the CA certificate MUST include basic constraints extension and the cA boolean MUST be set to true [RFC5280].

If the application provides an EE certificate (e.g., Transport Layer Security (TLS)) issued by this CA certificate, this means only obtaining a Certificate Revocation List (CRL). If no EE certificate is available (e.g., Secure Multipurpose Internet Mail Extensions (S/MIME)), then follow the Subject Information Access (SIA) extension to obtain other certificates. SHOULD be no more than one hop to the EE certificate.

If an EE certificate is returned, the certificate is intended for direct use with some application. As above, it is a matter of local policy whether this EE certificate is accepted as trusted directly, or MUST chain to a currently configured TA.

Verify that the dNSName in the certificate's subject alternative name extension [RFC5280] is consistent with the expected host name.

If the certificate contains a critical External Key Usage (EKU) or Key Usage (KU) extension [RFC5280], verify that the key usages are consistent with this application.

3. Examples

For S/MIME [RFC5750][RFC5751], the originator wants to send to a signed and encrypted email. (For signatures, the originator does not need the recipient's certificate.) To encrypt the message, the originator needs the recipient's key agreement or key transport certificate. To obtain the recipients certificate, the originator composes the email, selects sign and encrypt, and hit send. The mail client/DNSSEC client reviews the local store and determines that no certificate is available. The mail client then queries the DNS to determine whether certificates are available for that domain.

If a CERT resource record (RR) [RFC4398] is available, the mail client examines the certificate to determine if it is a CA certificate or end certificate. For domains with multiple users, the

certificate would be a CA certificate and would include a SIA extension [RFC5280]. The mail client follows the URL in an access description that asserts id-ad-caRepository, using the protocol implied by the accessLocation URL. For example, the mail client can query the repository for certificates issued to john.doe@example.com. If an appropriate certificate is available (and validates according to local policy), the client can encrypt the message. The originator includes their own certificates in the message, so this process is not required to validate or decrypt the original message or for a response.

For TLS [RFC5246], when the TLS looks up the IP address in the DNS it can also request the CERT RR. If the certificate that is provided in the TLS handshake matches the one retrieved from DNSSEC, then the client can accept it as a trusted certificate for that site, provided local policy allows this. If the CA certificate is returned in the TLS handshake, the TLS client can verify that the TLS server certificate was issued under that CA.

For IPsec [RFC4301], the model is similar to TLS.

4. Security Considerations

Like [RFC5280], trust and revocation configuration decisions will affect the security of the system.

When CA certificates are returned, the proposed solution assumes that the entire CA certificate is returned. For EE certificates, a hash could be returned instead of the entire certificate.

Need to say something caching versus revocation for optimization.

5. IANA Considerations

None

6. Acknowledgements

We'd like to thank the lovely Carly for bringing the libations during the "interim" Bar BoF. In addition, we'd like to thank Yuengling, Anheuser-Busch, and Samuel Adams for all of their efforts.

7. Normative References

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

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4301] Kent, S., and K. Seo, " Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4398] Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", RFC 4398, March 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S. Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, January 2010.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

Authors' Addresses

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com

Tim Polk
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA

Email: tim.polk@nist.gov

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com