Accepting full resolver certificate
draft-sonoda-dnsop-accept-certificate-00

Abstract

Full service resolver uses x509 certificate to provide DNS over TLS [RFC7858] DNS over DTLS [RFC8094]. This memo describes How to accept this certificate.

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 https://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 September 22, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Method of using TLSA record - TLSA style

1.1. full service resolver certificate

The certificate common name can be decided freely. Must add full service resolver ip addresses to Subject Alternative Name [RFC5280]. Add TLSA record [RFC7218] of the certificate to full resolver service IP address reverse name. The TLSA record MUST validate DNSSEC.

1.2. accepting full service resolver certificate

Stub resolver begins the TLS handshake and receives Full resolver certificate. If Full service resolver ip not include Subject Alternative Name, Stub resolver deny this certificate. Stub resolver requests TLSA record of full resolver service IP address reverse name and validates the TLSA recedes itself using. This process can use not safety Server. If the TLSA recedes are not validate, Stub resolver deny this certificate. If the TLSA recedes are secure and The TLSA recedes include recede of handshake certificate, Stub resolver can accept this certificate.

1.3. Distribution and update root trust anchor

Root trust anchor distribution and update SHOULD update by OS periodic update.

2. Method of using TLS-PKI - HTTPS style

2.1. full service resolver certificate

The certificate common name can be decided freely. Must add full service resolver ip addresses to Subject Alternative Name [RFC5280].

2.2. accepting full service resolver certificate

Stub resolver begins the TLS handshake and receives Full resolver certificate. If Full service resolver ip not include Subject Alternative Name, Stub resolver deny this certificate. The certificate is trusted by root certificate, Stub resolver can accept this certificate.

3. Operational Considerations

Case of DNSSec chains ot trust is break, TLSA style can’t accept new certificate.
4. Security Considerations

Attack create certificate of full resolver service IP address reverse name, HTTPS style can MIM attack.

5. Normative References


Author’s Address

Manabu Sonoda (editor)
Internet Initiative Japan Inc.

Email: manabu-s@iij.ad.jp