draft-wouters-tls-oob-pubkey-01

IETF
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2012

P. Wouters
Xelerance
J. Gilmore

S. Weiler
SPARTA, Inc.
T. Kivinen
AuthenTec
H. Tschofenig
Nokia Siemens Networks
October 31, 2011

TLS out-of-band public key validation
draft-wouters-tls-oob-pubkey-01

Abstract

This document specifies a new TLS certificate type for exchanging raw public keys or their fingerprints in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) for use with out-of-band authentication. Currently, TLS authentication can only occur via PKIX or OpenPGP certificates. By specifying a minimum resource for raw public key exchange, implementations can use alternative authentication methods.

One such method is using DANE Resource Records secured by DNSSEC, Another use case is to provide authentication functionality when used with devices in a constrained environment that use whitelists and blacklists, as is the case with sensors and other embedded devices that are constrained by memory, computational, and communication limitations where the usage of PKIX is not feasible.

draft-wouters-tls-oob-pubkey-01

```
 client_hello,
 cert_type="RawPublicKey" ->

                            <-  server_hello,
                                cert_type="RawPublicKey",
                                certificate,
                                server_key_exchange,
                                certificate_request,
                                server_hello_done

 certificate,
 client_key_exchange,
 certificate_verify,
 change_cipher_spec,
 finished                   ->

                            <- change_cipher_spec,
                               finished

Application Data        <------->     Application Data


enum { X.509(0), OpenPGP(1),
   RawPublicKey([TBD]), RawPublicKeySHA256([TBD]),
   (255) } CertificateType;

struct {
   select(ClientOrServerExtension)
       case client:
         CertificateType certificate_types<1..2^8-1>;
       case server:
         CertificateType certificate_type;
   }
```

Moving forward

- Is there enough interest in the TLS WG to make this a WG item?
- Working Group thoughts on sending/receiving hash(pubkey) instead of pubkey?
- Is subjectAltname good enough as raw pubkey container?
- If DANE becomes a standard before this document Paul Wouters and Paul Hoffman commited to write required draft