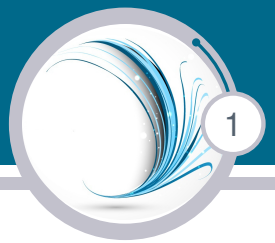
Transport Layer Security (TLS) Authentication using ITS ETSI and IEEE Certificates

IETF-104/IPWAVE Group

Télécom ParisTech & CISCO & OnBoard Security

29th March 2019

Plan



1. Motivations & Objective
2. Use Cases
3. Extension Overview
4. TLS Extension

Motivations

- Motivation: New Certificate Format
  - C-ITS[1] networks are highly mobile with a limited bandwidth.
  - In C-ITS systems, actors' permissions are important and actors' identity is often private.

- ETSI and IEEE created standards for size-optimized attribute certificates to secure data exchange in highly dynamic vehicular environments
- ETSI TS 103 097 is a profile of IEEE 1609.2

[1] Cooperative Intelligent Transportation System

Objective

- Enable Client/Server authentication using C-ITS certificates
- Vehicles and roadside will be provisioned with C-ITS certificates
- Permission-based certificates are more suited for ad-hoc networks than identity-based certificates

Use cases and “customers”

- Vehicle reporting environmental data to a server (SAE J2945/3)
- Vehicle diagnostics (ISO 21177)
- Fleet management (ISO 21177)
- Electric vehicle charging (USDoE / VTTI)
- Connecting an RSU to a traffic signal controller (Connected Vehicle Pilot Deployments)

Extension Overview


```
/* Managed by IANA */
 enum {
     X509(0),
     RawPublicKey(2),
     1609Dot2(3),
     (255)
 } CertificateType;

 struct {
     select (certificate_type) {

         /* certificate type defined in this document.*/
          case 1609Dot2:
          opaque cert_data<1..2^24-1>;

          /* RawPublicKey defined in RFC 7250*/
         case RawPublicKey:
         opaque ASN.1_subjectPublicKeyInfo<1..2^24-1>;

         /* X.509 certificate defined in RFC 5246*/
         case X.509:
         opaque cert_data<1..2^24-1>;

          };

        Extension extensions<0..2^16-1>;
    } CertificateEntry;
```

TLS Extension

One new value referring the IEEE certificate is added to the client-certificate-type and the server-certificate-type as defined in RFC 8446.

CertificateVerify

- In standard TLS, the CertificateVerify field is a "raw" signature
- C-ITS (IEEE 1609.2) certificates are closely associated with 1609.2 SignedData
  - Existing C-ITS security libraries output and input SignedData, not signature
- Therefore in this I-D, the CertificateVerify field is a 1609.2 SignedData
  - Maintain tight binding between C-ITS certificate and thing it’s signing
  - TLS implementation must use client_certificate_type, server_certficate_type to determine which process to use to sign and verify
  - Approach has been verified on and off TLS mailing list

IETF history

- Presented draft to TLS WG and IPWAVE WG at IETF 103 (Bangkok, 2018)
- Applied for and received code point from IANA for TLS certificate type
  - 2018-11-08: “In accordance with instructions from the reviewers, we’ve added the following entry to the TLS Certificate Types registry: Value: 3 Extension Name: 1609Dot2 Recommended: N Reference: [draft-tls-certieee1609] https://www.iana.org/assignments/tls-extensiontype-values We’ll update the reference when the IESG notifies us that they’ve approved the document and when the RFC Editor notifies us that they’ve assigned an RFC number.”

Summary

- C-ITS certificates:
  - Will be widely used in the near future
  - Have size advantages
  - As attribute certificates, are more suited to ad-hoc M2M environments than other authentication methods
- Significant industry demand for support for C-ITS certificates in TLS
- IETF/IANA has assigned code point for certificate type, but customers need a stable draft
- Request that IPWAVE considers adopting the draft

Thank You!
https://tools.ietf.org/html/draft-tls-certieee1609-02