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

IETF-103/TLS Group

Télécom ParisTech & CISCO
5th Of November 2018
1. Motivations & Objective
2. Use Cases
3. Extension Overview
4. TLS Extension
Motivations:

- C-ITS\(^1\) networks are highly mobile with a limited bandwidth.
- X.509 certificates are not optimized for bandwidth and delay-sensitive applications

That is why size-optimized certificates were standardized by ETSI and IEEE to secure data exchange in highly dynamic vehicular environments in Intelligent Transportation System (ITS).

\(^1\)Cooperative Intelligent Transportation System
Objective:

- We need an authentication method more optimized for bandwidth and processing time to support delay-sensitive applications.
- Enable Client/Server authentication using C-ITS certificates
Use cases

- Secured communication between a vehicle and a server on the Internet:
  - e.g. vehicle data upload on a remote log server
  - e.g. vehicle software update
  - e.g. traffic light information via 3G/LTE communication (SPAT \(^2\))
  - e.g. connected cloud services
  - e.g. connected infotainment

\(^2\)Signal Phase and Timing adapter
Use cases

 Authentication between an ITS-Station and a server should be possible using C- ITS certificates:
 e.g. rent company
 e.g. car manufacturer
 e.g. wireless electric vehicle charging
/* Managed by IANA */
enum {
    X509(0),
    RawPublicKey(2),
    1609Dot2(?), /* Number 3 will be requested for 1609.2 */
    (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;
One new value referring the IEEE certificate is added to the client-certificate-type and the server-certificate-type as defined in RFC 8446.
For privacy considerations in a vehicular environment, the use of IEEE/ETSI certificates is recommended for many reasons:

- The purpose of these certificates is to provide privacy relying on geographical and/or temporal validity criteria, and minimizing the exchange of private data.
- Extend the Transport Layer Security protocol (TLS) by using ETSI/IEEE certificates to securely exchange data between multiple vehicular network components.

IANA is asked to register a new value in the "TLS Certificate Types" (IEEE/ETSI references).
Thank You!