ROLE OF ETSI AND OTHER SDOS IN MAKING ITS MARKET A REALITY

ETSI Security Workshop – ITS thread, 24th June 2015
Brigitte LONC, ETSI TC ITS WG 5 Chairman
Overview

Introduction
- C-ITS standardization & activities in EU

ETSI ITS standardisation
- ITS Security framework & services
- ETSI ITS Trust model (PKI)
- Single message services (TS 103 097)

Security association
- Draft RFC TLS extension

Validation and deployment roadmap

Next Steps & extensions

© ETSI 2014. All rights reserved
What is cooperative ITS?

- 5.875 – 5.905 GHz allocated by EU to road safety & traffic applis (ITS G5)
- C-ITS may use also other communication technologies, 3G/LTE, WLAN

**ITS G5 communication features:**
- Quick medium access (low latency)
- Allocation of frequencies to safety (high reliability)
- Ad hoc communication (no need of infrastructures)
- 200-800 m com range (extended vehicle sensor for assistance & autonomous vehicle)

**ITS G5 considered for Day1 road safety applications deployment by C2C Communication Consortium**

**V2V & V2I coordination will stimulate the C-ITS deployment & penetration rate**
- SCOOP@F pilot project in France
- Project Corridor, NL- Germany- Austria

© ETSI 2014. All rights reserved
ETSI ITS standardisation (ITS WG5)
C-ITS Security Framework

TR 102 893
Risk analysis TVRA

TS 102 731
Security services

TS 103 097
Security headers, Certificates

TS 102 940
ITS security architecture & sec management

TS 102 941
Trust & Privacy

TS 102 942
Access control

TS 102 943
Confidentiality

New version published (v1.2.1)

Under revision, extensions:
• scalability & extensibility (PKI entities)
• maintainability, crypto-agility
Security processing services
- Sign & verify Message, Encrypt & Decrypt data, manage security association (SA)

Security management
- Enrolment, Authorization, Identity management, report misbehaviour

HSM requirements
- Secure key storage
- Heavy computational operations (crypto)
- Trusted running environment
## Security & privacy services (ETSI TS 102 94x)

<table>
<thead>
<tr>
<th>Service category</th>
<th>Security service</th>
<th>Security Service Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Message Signature Service</td>
<td>Authorize Single Message</td>
<td>SIGN</td>
</tr>
<tr>
<td></td>
<td>Validate Authorization on Single Message</td>
<td></td>
</tr>
<tr>
<td>Data Encryption Service</td>
<td>Encrypt Single Message</td>
<td>ENCRYPT</td>
</tr>
<tr>
<td></td>
<td>Decrypt Single Message</td>
<td>DECRYPT</td>
</tr>
<tr>
<td>Replay Protection services</td>
<td>Replay Protection Based on Timestamp</td>
<td>used by SIGN, VERIFY</td>
</tr>
<tr>
<td>Plausibility service</td>
<td>Validate Data Plausibility</td>
<td>used by SIGN, VERIFY</td>
</tr>
<tr>
<td>Security Associations management</td>
<td>Establish Security Association</td>
<td>ref to IETF standards:</td>
</tr>
<tr>
<td></td>
<td>Update security association</td>
<td>e.g. Draft RFC</td>
</tr>
<tr>
<td></td>
<td>Send Secured Message</td>
<td>TLS extension</td>
</tr>
<tr>
<td></td>
<td>Receive Secured Message</td>
<td>for ITS</td>
</tr>
<tr>
<td></td>
<td>Remove Security association</td>
<td></td>
</tr>
</tbody>
</table>

Privacy concerns are introduced:
- by message content and by the message signature
- cryptographic certificate allows tracking

Privacy protection by changing frequently the pseudonymous certificates (ID change
ETSI ITS Trust model (PKI)

- Enrolment Authority (EA)
- Root CA
- Authorization Authority (AA)

ITS-S
(vehicle, road-side, personal)

Enrolment ID
Canonical ID & public key

Secured message
Bootstrap Certificate (self signed)

Pseudonymous Authorization Certificates

© ETSI 2014. All rights reserved
ITS Certifications authorities

Due to the broadcast nature of CAM and DENM, the trust relationship between ITS stations has to be:

- scalable (hundreds of millions of nodes)
- instantaneously verifiable.

To meet these requirements, the ITS-S enrolment and authorization for different services is delegated to Trusted Third Parties (TTP), i.e. two types of Certification Authorities (CAs):

- **Enrolment Authority (EA)**: provides an ITS-S with an enrolment ID and related enrolment certificate (long term).
- **Authorization Authority (AA)**: provides the ITS-S with multiple pseudonyms and the related authorization certificates (short term), to be used in V2X communication.

Detection of Misbehaving and revocation of ITS stations

- Timely distribution of CRLs in ITS large scale system is challenging
- CRLs for revoked Enrolment certificates should be distributed to EA and AA (not all ITS stations)
- Authorisation certificates with short expiry periods is a good alternative to CRL distribution
Public Key Infrastructure
Authorization Tickets request to AA

V2X Security Infrastructure
- Root Certificate Authority
- Enrolment Authority (EA)
- Authorization Authority (AA)

ITS G5 Network
- IP
- ITS G5
- V2X message
- CA certs.
- LTC
- PC₁ … PCₙ

RSU
Vehicles

2015-06-18
3 Security profiles: CAM, DENM, generic certificates formats for ITS stations & CAs

Signed Message with Pseudonym Certificate

- Signed Message with certificate digest

<table>
<thead>
<tr>
<th>Header Fields</th>
<th>Payload</th>
<th>Trailer Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td></td>
<td>Signature</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Header Fields</th>
<th>Payload</th>
<th>Trailer Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td></td>
<td>Signature</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>security field</th>
<th>estimated size</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate (AT)</td>
<td>140 bytes</td>
</tr>
<tr>
<td>certificate digest</td>
<td>10 bytes</td>
</tr>
<tr>
<td>signature</td>
<td>69 bytes</td>
</tr>
<tr>
<td>header fields</td>
<td>variable</td>
</tr>
</tbody>
</table>
Digital signature ECDSA 256 for messages authenticity & integrity
- Public-key cryptography (PKI for management of certificates)
- ECDSA signature algorithm (harmonized with IEEE 1609.2)
- Nist P-256 curve
- Key size: 256 bits

Symmetric & asymmetric encryption for confidentiality
- ECIES: public-key encryption and key transport
- Encryption for data stream: AES CCM 128 bits
Reuse or adapt existing standards
e.g. draft RFC TLS extension for ITS certificate

• A new version is provided to IETF TLS group
• Submitted for next meeting (Prague 19-24/07/2015)
• **Objective:** extend TLS protocol such that clients and servers can be authenticated using C-ITS certificates (ETSI TS 103 097, IEEE 1609.2)
• **Use case:** secured communication between an ITS-S station and an ITS-S Center on the Internet
• Next: planned implementation in ISE project (SystemX)
For the extension ‘cert_type, new values have to be allocated by IANA
Plugtest validation of security standard

4th ITS CMS ETSI Plugtest, 17 – 27 March 2015
Security standard testing (TS 103 097)
Conformance and Interoperability testing
  • Extended number of tests based on ETSI TS 103 096-1, -2, -3
  • 64 test cases for conformance
  • More than 20 vendors, 8 different security implementations

Development of test will continue, new test sessions planned in next Plugtest in Fall 2016
C2C-CC Security roadmap

2013
- Basic System Profile
- Protection profile

2014
- Basic System Profile v2
- Certification Policy development
- Pilot PKI
- ETSI Plugtest
- Compliance assessment

2015
- ETSI Plugtest

2016
- Req. Quality & sync with PP
- Rewrite
- Option 1: C2C-CC founds LE
- Option 2: OEMs select other LE
- Root CA QA (C2C CC)
- LT/PS CA QA (OEM)
- Root CA prod (C2C CC)
- LT/PS CA prod (OEM)

Legal entity required!
Next Steps & extensions

Security maintainability

• Due to lifetime of ITS stations (vehicles, RSUs), security erosion will happen

• Crypto-agility is recommended
  • Key size, curve parameters, signature algorithm

• But issues for existing systems:
  • updatability in the field, limited HW (HSM, crypto accelerator), lower implementation performances
Roaming issues

- It would be easier with a single Root CA (Euro Root CA)
- but road authorities in EU countries may wish to operate their Root CA
- Multiple PKIs, multiple Root CAs must cooperate
- Standards extensions needed to support trust relationship between PKIs
  - New RCAs/EAs/AAs introduced using ‘over the air updates’ when endorsed by the (home) Root CA
  - Protocol to obtain enrolment and authorisation certificates