Secure V2X Communications
- According ETSI (Europe) -

Markus Ullmann
Outline

- Secure Vehicle-2-Vehicle Communication (V2V) according to ETSI
  - Communication Model
  - Security - and Privacy Requirements
  - Shortcomings of the existing ETSI Specifications
    - Security, Privacy
- Secure Vehicle-2-Infrastructure Communication (V2X)
  - V2X Pilot Projects in Europe
    - Cooperative Intelligent Transport System (C-ITS) Corridor Project Rotterdam-Frankfurt-Vienna
  - Secure V2X Communication
  - Secure ITS Roadside Station (IRS) messages (DENM)
  - Multi Domain PKI Architecture
- Conclusion/Future Work
Vehicle-2-Vehicle Communication (V2V)

- Aim: Enhance Traffic Safety
Status V2V Communication

- ~ 2005 – 2010: Prototyping
- ~ 2010 – 2015: Standardization
  Europe: ETSI
  US: IEEE, SAE
- 2018/19: Start Deployment Vehicles with V2V interface in Europe
Vehicle-2-Vehicle Communication

- Broadcast Communication
- IEEE 802.11p
- 5,9 GHz ("G5")
Security and Privacy Requirements for the V2V Communication

- Security Requirements
  - Message Integrity
  - Message Authenticity

- (Location) Privacy
  - Sender Anonymity
  - Message Unlinkability (~ “over longer time periods“)
ETSI ITS Architecture

- ITS roadside stations
- ITS vehicle stations
- ITS central stations
- ITS personal stations
Secure Vehicle-2-Vehicle Communication

- **ETSI ITS Specifications**
  - **TS 102 637-2 V 1.2.1**: Cooperative Awareness Message (CAM): Location, Speed, Time, ... Send Frequency: 100ms
    - Header | CAM Information | ECDSA Signature | Certificate
  - **TS 102 637-3 V 1.1.1**: Decentralized Environmental Notification Basis Services (DENM): Warning
    - Header | DENM Information | ECDSA Signature | Certificate
  - **TS 103 097 V 1.1.1**: Security header and Certificate formats
ECDSA

- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Digital Signature is a “Cryptographic Fingerprint“
- In general: Use of Asymmetric Cryptography
  - Here: Elliptic Curve Cryptography (ECC)
- Entities need:
  - Key Pair: (public key | private key)
  - Certificate (formal attestation of a key pair)
- Sender: Calculates signature (ECDSA)
- Receiver: Verifies signature (ECDSA)

Elliptic Curves Cryptography
- Calculation in specific cyclic finite groups (Discret Logarithm Problem on ECC is hard)
- Elliptic Curve Domain Parameter (according to NIST, Brainpool, …)
  - NIST P-256 (NSA/NIST does not recommend to use this curve any longer)
  - BrainpoolP256r1
  - ...

Tutorial InfoWare: Secure V2X November 13, 2016 Folie 9
Cooperative Awareness Message (CAM)
- "~ Beacon Message" -

CAM Send Frequency: 10 Hz

<table>
<thead>
<tr>
<th>Complete Message</th>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Signer Info</strong></td>
</tr>
<tr>
<td></td>
<td>Generation Time</td>
</tr>
<tr>
<td></td>
<td>its_aid ITS-AID for CAM</td>
</tr>
<tr>
<td></td>
<td><strong>Basis Container</strong></td>
</tr>
<tr>
<td></td>
<td>ITS-Station Type</td>
</tr>
<tr>
<td></td>
<td>Last Geographic Position</td>
</tr>
<tr>
<td></td>
<td>Speed</td>
</tr>
<tr>
<td></td>
<td>Driving Direction</td>
</tr>
<tr>
<td></td>
<td>Longitudinal Acceleration</td>
</tr>
<tr>
<td></td>
<td>Curvature</td>
</tr>
<tr>
<td></td>
<td>Vehicle Length</td>
</tr>
<tr>
<td></td>
<td>Vehicle Width</td>
</tr>
<tr>
<td></td>
<td>Steering Angle</td>
</tr>
<tr>
<td></td>
<td>Lane Number</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td><strong>High Frequency Container</strong></td>
</tr>
<tr>
<td></td>
<td>Vehicle Role</td>
</tr>
<tr>
<td></td>
<td>Lights</td>
</tr>
<tr>
<td></td>
<td>Trajectory</td>
</tr>
<tr>
<td></td>
<td>Emergency</td>
</tr>
<tr>
<td></td>
<td>Police</td>
</tr>
<tr>
<td></td>
<td>Fire Service</td>
</tr>
<tr>
<td></td>
<td>Road Works</td>
</tr>
<tr>
<td></td>
<td>Dangerous Goods</td>
</tr>
<tr>
<td></td>
<td>Safety Car</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td><strong>Special Container</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Signature</strong></td>
</tr>
<tr>
<td></td>
<td>ECDSA Signature of this Message</td>
</tr>
<tr>
<td></td>
<td><strong>Certificate</strong></td>
</tr>
<tr>
<td></td>
<td>According Certificate for Signature Verification</td>
</tr>
</tbody>
</table>
Privacy: Pseudonym Concept

- **Concept**
  - Pseudonymous key pairs / certificates

- **Privacy Requirements**
  - Sender Anonymity
  - Message unlinkability

**Privacy Requirements**
- Sender Anonymity
- Message unlinkability

**Time**
- \( t = t_0 \)
- \( t = t_1 \)
**CAM Data Volume**

- **Basis Container + High Frequency Container + Low Frequency Container:** \(~200\) bits
- **Header + Signature:** \(~750\) bits
- **Certificate:** \(~1000\) bits

<table>
<thead>
<tr>
<th>Complete Message</th>
<th>Header</th>
<th>CAM Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Basis Container</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ITS-Station Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last Geographic Position</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Speed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Driving Direction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Longitudinal Acceleration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Curvature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vehicle Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vehicle Width</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Steering Angle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lane Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>High Frequency Container</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vehicle Role</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trajectory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Police</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fire Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Road Works</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dangerous Goods</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safety Car</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Low Frequency Container</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Special Container</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Signature</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ECDSA Signature of this Message</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Certificate</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>According Certificate for Signature Verification</td>
</tr>
</tbody>
</table>
Decentralized Environmental Notification

Basis Services (DENM)

- **Warning (event driven)** -

<table>
<thead>
<tr>
<th>Complete Message</th>
<th>Header</th>
<th>Management Container</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Signer_INFO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Generation_Time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>its_aid ITS-AID for DENM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Vehicle Position (GPS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Event Identifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time of Detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time of Message Transmission</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Event Position (GPS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Validity Period</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Station Type (Motor Cycle, Vehicle, Truck)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Message Update / Removal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant Local Message Area (geographic)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic Direction (forward, backwards, both)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transmission Interval</td>
<td></td>
</tr>
</tbody>
</table>

|                  | Information Quality (low - high, tbd) |          |
|                  | Event Type (Number)                  |          |
|                  | Linked Events                        |          |
|                  | Event Route (geographical)           |          |
|                  | Event Path                           |          |
|                  | Event Speed                          |          |
|                  | Event Direction                       |          |
|                  | Road Type                             |          |
|                  | Road Works (Speed Limit, Lane Blockage …) |   |

| A la carte Container | Road Works (Speed Limit, Lane Blockage …) |          |

<table>
<thead>
<tr>
<th>Signature</th>
<th>ECDSA Signature of this message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>According Certificate for Signature Verification</td>
</tr>
</tbody>
</table>
# Comparison V2X in Europe / US

<table>
<thead>
<tr>
<th></th>
<th>Europe</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standards:</strong></td>
<td>ETSI 102637 1-3</td>
<td>SAE J 2735</td>
</tr>
<tr>
<td></td>
<td>ETSI 102 943</td>
<td>IEEE 1609.2</td>
</tr>
<tr>
<td></td>
<td>ETSI 103 097 (Naming derived from IEE 1609.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>further ETSI standards possible</td>
<td></td>
</tr>
<tr>
<td><strong>Accepted ECC Curves:</strong></td>
<td>NIST P-256r1</td>
<td>NIST P-256r1</td>
</tr>
<tr>
<td></td>
<td>BrainpoolP256r1 (in discussion)</td>
<td>BrainpoolP256r1 (in discussion)</td>
</tr>
<tr>
<td><strong>Message Types:</strong></td>
<td>CAM</td>
<td>BSM</td>
</tr>
<tr>
<td></td>
<td>DENM</td>
<td>RSA</td>
</tr>
<tr>
<td></td>
<td>EVA</td>
<td>EVA</td>
</tr>
<tr>
<td></td>
<td>“unlimited” number of types possible</td>
<td>limited number of types</td>
</tr>
<tr>
<td><strong>Minimal Message Size without Signature and Certificate:</strong></td>
<td>186 bit</td>
<td>275 bit</td>
</tr>
<tr>
<td><strong>Minimal Message Size with Signature and Certificate:</strong></td>
<td>~2 Kbit</td>
<td>~2 Kbit</td>
</tr>
</tbody>
</table>
Secure Vehicular Communication  
- Keys, Certificates, PKI

- Identification and Authentication of Vehicles
  - Long term cryptographic key pair (certificate) based on Elliptic Curves (NIST P-256)
    - ETSI Certificate format (not widely used)
  - Issued by Long Term Certification Authority (LTCA)
    [ETSI]: Enrolement CA

- Message Security / Location Privacy
  - Pseudonymous key pairs (certificates) (ECC NIST P-256)
    - ETSI Certificate Format
  - Issued by Pseudonym Certification Authority (PCA)
    [ETSI]: Authorization CA
Secure Vehicular Communication
- Key Generation, Key Storage -

- Private keys are generated at random (within the order of the ECC group)
  - Long term -, pseudonymous keys are distinct
  - No key duplicates
- Typically secret keys will be generated and stored within secure elements in the vehicle
Outline

- Secure Vehicle-2-Vehicle Communication (V2V) according to ETSI
  - Communication Model
  - Security - and Privacy Requirements
  - Shortcomings of the existing ETSI Specifications
    - Security, Privacy
- Secure Vehicle-2-Infrastructure Communication (V2X)
  - V2X Pilot Projects in Europe
    - Cooperative Intelligent Transport System (C-ITS) Corridor Project Rotterdam-Frankfurt-Vienna
  - Secure V2X Communication
  - Secure ITS Roadside Station (IRS) messages (DENM)
  - Multi Domain PKI Architecture
- Conclusion/Future Work
Shortcomings of the ETSI specifications

- **Cryptographic Setting**
  - Cryptography *ages over time* (e.g., due to better computer attack capabilities)
  - Missing mechanism for *cryptographic update* (crypto agility)
    - Elliptic Curve Domain Parameter
    - Hash Function, Signature Algorithms, ...

- **Adapations**
  - Crypto agility concept is needed
## Linkability of CAMs (BSMs)

- **Static Information**
  - Certificate
  - Length/Width
  - Confidence Level
  - (Geographic position)

- **Linkability based on the Pseudonym Certificate**

- **Linkability based on CAM data**
  - Length / Width
  - Confidence Level
  - (Geographic position)

### CAM Information

<table>
<thead>
<tr>
<th>Complete Message</th>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Signer Info</td>
</tr>
<tr>
<td></td>
<td>Generation Time</td>
</tr>
<tr>
<td></td>
<td>its_aid ITS-AID for CAM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAM Information</th>
<th>Basis Container</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ITS-Station Type</td>
</tr>
<tr>
<td></td>
<td>Last Geographic Position</td>
</tr>
<tr>
<td></td>
<td>Speed</td>
</tr>
<tr>
<td></td>
<td>Driving Direction</td>
</tr>
<tr>
<td></td>
<td>Longitudinal Acceleration</td>
</tr>
<tr>
<td></td>
<td>Curvature</td>
</tr>
<tr>
<td></td>
<td>Vehicle Length</td>
</tr>
<tr>
<td></td>
<td>Vehicle Width</td>
</tr>
<tr>
<td></td>
<td>Steering Angle</td>
</tr>
<tr>
<td></td>
<td>Lane Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAM Information</th>
<th>Low Frequency Container</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Vehicle Role</td>
</tr>
<tr>
<td></td>
<td>Lights</td>
</tr>
<tr>
<td></td>
<td>Trajectory</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAM Information</th>
<th>Special Container</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Emergency</td>
</tr>
<tr>
<td></td>
<td>Police</td>
</tr>
<tr>
<td></td>
<td>Fire Service</td>
</tr>
<tr>
<td></td>
<td>Road Works</td>
</tr>
<tr>
<td></td>
<td>Dangerous Goods</td>
</tr>
<tr>
<td></td>
<td>Safety Car</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAM Information</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ECDSA Signature of this Message</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAM Information</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>According Certificate for Signature Verification</td>
</tr>
</tbody>
</table>
CAM: Static Informations

- Vehicle Length  (CAM: in 10 cm intervals)
- Vehicle Width   (CAM: in 10 cm intervals)
- High Frequency Container: Confidence Level

<table>
<thead>
<tr>
<th></th>
<th>Value Range</th>
<th>Confidence Level Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heading</td>
<td>0, ..., 3601 (12 bit)</td>
<td>1, ..., 127 (7 bit)</td>
</tr>
<tr>
<td>Speed</td>
<td>0, ..., 16383 (14 bit)</td>
<td>1, ..., 127 (7 bit)</td>
</tr>
<tr>
<td>Acceleration</td>
<td>00000000, ..., 11111111 (7 bit)</td>
<td>0, ..., 102 (7 bit)</td>
</tr>
<tr>
<td>Curvature</td>
<td>-30000, ..., 30000 (16 bit)</td>
<td>0, ..., 7 (3 bit)</td>
</tr>
<tr>
<td>Yaw Rate</td>
<td>-32766, ..., 32767 (16 bit)</td>
<td>0, ..., 9 (4 bit)</td>
</tr>
</tbody>
</table>
Movement of the Geographic Position

Assumptions:
- Speed: 50 km / h
- CAM transmission frequency: 10 Hz

- Secondary vehicular identities: e.g., Bluetooth Device Address (48 bit), ...
- C-ITS Platform EC DG
  Move: „CAM / DENM: personal data“

Assumptions:
- Speed: 50 km / h
- CAM transmission frequency: 10 Hz

Diagram:
- Movement of geographic position over time
- Assumption: 
  - Speed: 50 km / h
  - CAM transmission frequency: 10 Hz

Summary:
- Movement of geographic position
- Assumptions for simulation
- C-ITS Platform EC DG Move: „CAM / DENM: personal data“
Location Privacy
- Attacker Models -

- „Big Brother“ Attacker
  - Monitoring traffic in a specific region
    - Static: e.g., roadside stations
    - Dynamic: class of vehicles (e.g., trucks)

- Local Attacker
  - Monitoring specific vehicle (driver)
Shortcomings of the Pseudonym Concept

Observation Device: e.g., Future Smart Phone

- IEEE 802.12 Interface (5G)
- Storage
- Prozessor
- GPS
- LTE

- Observation Device:
  - Stores „CAM Trace“ (location, time, speed, …)
  - Non-disputable observation

Due to the (ECDSA) Signature
Link a “CAM Trace“ to a Vehicle

Observation Device: e.g., Future Smart Phone
- IEEE 802.12 Interface (5G)
- Storage
- Prozessor
- GPS
- LTE
- WLAN/Bluetooth

- If one CAM of the whole “CAM Trace“ can be linked to a vehicle then the whole CAM Trace can be linked
- Linkability
  - Limited Vehicles with V2V Interface
  - Based on Second Level Vehicle Identifier
  - ...
Vehicle Identifier (1)

- First Level Identifier (formal/official)
  - Vehicle Identification Number (VIN)
- Licence plate
- Enrollement certificate (long term)
Vehicle Identifier (2)

- Second Level Identifier (arise with wireless vehicle communication interfaces)
  - Vehicular multimedia device:
    - 48 bit static Bluetooth MAC ID (24 bit manufacturer || 24 bit bluetooth device)
    - "User-friendly-name"
  - WiFi access point:
    - WLAN MAC ID
    - Service Set Identifier (SSID)
  - Active Tyre Pressure Monitoring System (TPMS):
    - RFID-ID
  - Mobile:
    - IMEI
Individual Driver Identification

- Do humans have individual driveability properties?
- Are driveability properties deducible from send CAM data?

Open Research Issues
- Driver identification based on a small driver set (1 : N)?
- Driveability Features?
- Matching Algorithm?
- …
Outline

- Secure Vehicle-2-Vehicle Communication (V2V) according to ETSI
  - Communication Model
  - Security - and Privacy Requirements
  - Shortcomings of the existing ETSI Specifications
    - Security, Privacy
- Secure Vehicle-2-Infrastructure Communication (V2X)
  - V2X Pilot Projects in Europe
    - Cooperative Intelligent Transport System (C-ITS) Corridor Project Rotterdam-Frankfurt-Vienna
  - Secure V2X Communication
  - Secure ITS Roadside Station (IRS) messages (DENM)
  - Multi Domain PKI Architecture
- Conclusion/Future Work
C-ITS Corridor Project
- Secure Vehicle-2-Infrastructure Communication

Attention: Short Term Site

Motorway Corridor
C-ITS Corridor Project
- Secure V2X Communication -

- Cooperative ITS Corridor Project Rotterdam-Frankfurt-Vienna (NL-G-AU)

- Joint Project of:
  - Austria: Federal Ministry of Transport, Innovation and Technology
  - Netherlands: Ministry of Infrastructure and the Environment
  - Germany: Federal Ministry of Transport and Digital Infrastructure

- Digitalization of Road Works Warning

- Use Cases (Broadcast Communication)
  - Send DENM messages to the crossing vehicles
  - Receive CAM / DENM messages of crossing vehicles

IEEE 802.11p

 arrows pointing from roadside to vehicles and vice versa.
Further V2X Pilot Projects in Europe

- France: Scoop@F

- Danmark, Finland, Norway, Sweden: NordicWay
Secure ITS Roadside Stations (1)
- Integration of an electronic gateway
- Threats to incoming/outgoing messages
  - Availability
    - Jamming, ...
  - Authenticity
    - Masquerading, ...
  - Integrity
    - Injection of forged messages, ...
  - Confidentiality
    - Extraction of sensitive information (e.g., cryptographic keys)
- Threats concerning the integrity of the electronic gateway itself
  - Malicious software
  - Extraction of cryptographic keys, ...
Secure ITS Roadside Stations (2)

- Location Privacy
  - ITS roadside stations are not controlled by a user
  - No Privacy Requirements ==> no pseudonym certificates are needed
  - Instead: Credential Certificate (short validity period [~ days] to avoid CRLs)

- Security Requirements
  - DENM-Security: Message integrity and authentication
  - „Protection of the gateways“ → Protection Profile (PP)
    - Identification and authentication (roles)
    - Access Control, …
    - Short time authorization (credential certificate)
    - ...


C-ITS Use Case: Sending DENM messages

- **Short Term Credential Certificate**

- **Usage**
  - Authorization of ITS roadside station
  - Message integrity and authentication of DENM messages

- **ETSI Certificate format**

---

**DENM Information**

- **Header**
  - Signer Info
  - Generation Time
  - its aid ITS-AID for DENM

- **Management Container**
  - Last Vehicle Position (GPS)
  - Event Identifier
  - Time of Detection
  - Time of Message Transmission
  - Event Position (GPS)
  - Event Position (GPS)
  - Validity Period
  - Station Type (Motor Cycle, Vehicle, Truck)
  - Message Update / Removal
  - Relevant Local Message Area (geographic)
  - Traffic Direction (forward, backwards, both)
  - Transmission Interval

- **DENM Information**
  - Event Type (Number)
  - Linked Events
  - Event Route (geographical)

- **Situation Container**
  - Information Quality (low - high, tbd)

- **Location Container**
  - Event Path
  - Event Speed
  - Event Direction
  - Road Type

- **A la carte Container**
  - Road Works (Speed Limit, Lane Blockage…)

- **Signature**
  - ECDSA Signature of this message

- **Certificate**
  - According Certificate for Signature Verification
IRS PKI Domain (Infrastructure)

- Identification and Authentication of ITS Roadside station
  - Long term key pair (certificate) based on Elliptic Curves
    - BrainpoolP256r1 curve
    - X.509 V3 certificate format
  - Issued by Long Term Certification Authority (LT-CA)
    [ETSI: Enrolement CA]

- Authorization and Message Authentication
  - Short term key pair (credential certificate) based on Elliptic Curves
    - BrainpoolP256r1 curve
    - ETSI Certificate format
  - Issued by Credential Certification Authority (C-CA)
    [ETSI: Authorization CA]
Certificate Shell Model

LT-RCA

LT-CA

0 I II

time

IRS-LT-RCA
IRS-C-RCA

LT(cert)
C(cert)
CRL

LT(cert) revoked?

Tutorial InfoWare: Secure V2X November 13, 2016 Folie 37
Crypto Agility

- Adaptation of Cryptographic Parameters
  - Key Length → ECC Domain Parameter
  - Crypto Algorithms
  - ...

- Performed by a IRS-LT-RCA link certificate (signed with the previous root key)
Multi Domain PKI Architecture

- Trust Relation
  - Local Trust Lists (LTL)
- Benefits
  - Flexibility (Requirements)
  - RSU under control of infrastructure authority
- Drawback
  - Managing of LTLs within each PKI
Outline

- Secure Vehicle-2-Vehicle Communication (V2V) according to ETSI
  - Communication Model
  - Security - and Privacy Requirements
  - Shortcomings of the existing ETSI Specifications
    - Security, Privacy
- Secure Vehicle-2-Infrastructure Communication (V2X)
  - V2X Pilot Projects in Europe
    - Cooperative Intelligent Transport System (C-ITS) Corridor Project Rotterdam-Frankfurt-Vienna
  - Secure V2X Communication
  - Secure ITS Roadside Station (IRS) messages (DENM)
  - Multi Domain PKI Architecture
- Conclusion/Future Work
Conclusion V2X

- Next steps C-ITS Corridor Project (2016)
  - Setup PKI for ITS roadside stations (RWWG)
  - Equip RWW gateway stations with keys/certificates
  - Test secure Vehicle-2-X communication with real vehicles within the C-ITS corridor
  - ...

- Secure V2X Communication
  - Security Concept for ITS Roadside stations and V2X is sound

- C-ITS Platform (EC DG MOVE): Common C-ITS PKI Policy in preparation for Europe
Thanks for listening?

**Kontakt**

Prof. Dipl.-Ing. Markus Ullmann  
Federal Office for Information Security (BSI)  
Head of Unit “Secure Identification and Hardware Security“  
Godesberger Allee 185-189  
D-53175 Bonn, Germany

Tel: ++49(0)22899-9582-5268

markus.ullmann@bsi.bund.de  
www.bsi.bund.de

Professor Bonn-Rhine-Sieg University of Applied Sciences