HOCHSCHULE HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Fahrzeugvernetzung – V2X

Lecture 6: Security and Privacy

Hugues Tchouankem, 03.11.2021

Lecture 6
Previous Lecture

- ► Overview Physical Layer
  - ► IEEE 802.11p
- ► Propagation Characteristics
- ► Multipath Propagation
- ► Orthogonal Frequency-Division Multiplexing
- ► Channel Propagation Models

Lecture 6
Outline

- Part 1: Security
  - Objectives
  - Threats
  - Algorithms
  - Public Key Infrastructure

- Part 2: Privacy
  - Location Privacy
  - Pseudonymity
  - Pseudonym Switching Strategies

Lecture 6

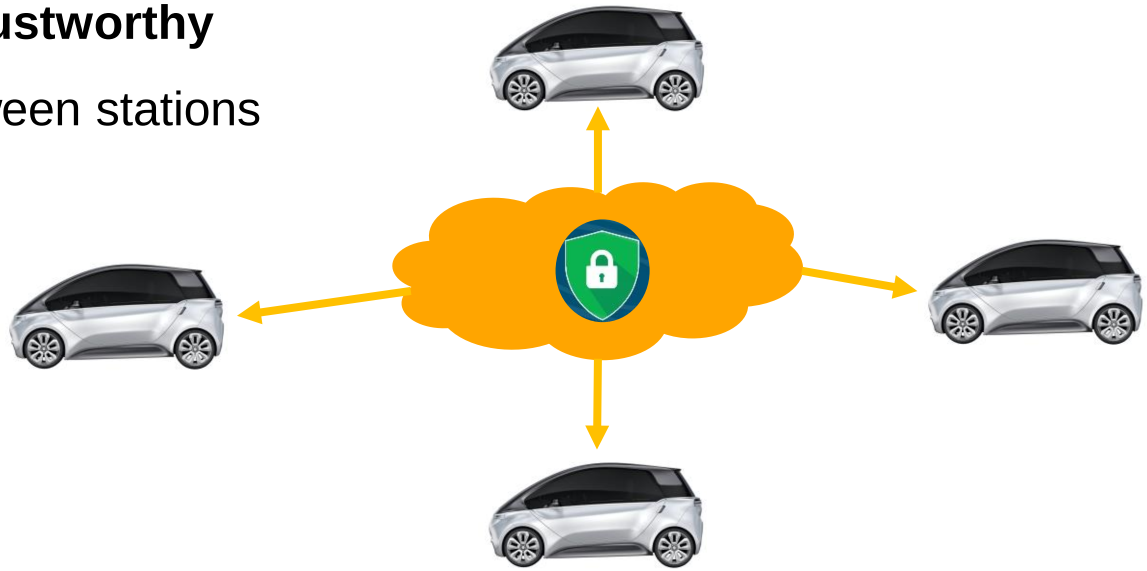
Security and Privacy more than just a Feature

► **Security** and **privacy** in V2X communication is a major aspect that affects all **applications** used in the network

► **Attacks** are likely and not detectable by central entities due to the **wireless communication** and the **decentralized character** of the V2X-network

► Road safety **critical applications** that rely on data received from other network entities must be **trustworthy**

→ **Secure** and **trusted** awareness between stations



Lecture 6

Hackers Remotely Kill a Jeep on the Highway

- ► In late 2015 two cybersecurity researchers, Charlie Miller and Chris Valasek, remotely compromised a Jeep Cherokee (source: www.theverge.com)
  - ► The hackers **remotely send commands** through the Jeep’s entertainment system to its dashboard functions, steering, brakes, and transmission

Lecture 6

Security Objectives – Authentication (1/2)

- ► Vehicles must be able to establish a **high level of trust** in the messages they use to **make** safety-related **decisions**

- ► Broadcast message authentication:
  - ► **First** and **most fundamental** security function for cooperative awareness
  - ► Ability for vehicles to determine whether a broadcasted CAM is from a **vehicle/RSU authorized** to send such messages
  - ► It is sufficient to determine that the message originator belongs to a **group** of entities (Vehicles or RSUs)
    - ► Uniquely identifying the message-originating vehicle is **not implicitly required**

Lecture 6

Security Objectives – Authentication (2/2)

- Broadcast message authentication:
  - **Authentication** can be achieved using digital **signatures** with digital **certificates**
    - **Digital signature** allows a vehicle to determine that a message originating knows a **secret**
    - **Certificate** attests that this **secret** is possessed **only by a vehicle authorized** to broadcast safety messages

Lecture 6

Security Objectives – Data Integrity

- **Data integrity** means that data have not been **altered** in an **unauthorized manner** since it was created
- Data can be altered **accidently** or **deliberately**
  - During transmission over network or while stored in databases
- Prevent an attacker from **modifying messages** or provide the possibility to detect such changes
- It is the **most important security objective** in the **V2X network domain**
  - Potential scenario: **Falsified messages** might make **other drivers** leave a freeway because of an **imaginary traffic jam**

Lecture 6

Security Objectives – Data Confidentiality

- **Data confidentiality** is the ability to prevent **unauthorized** parties from knowing the **content of the message**
- Following aspects are to consider:
  - Every vehicle must protect the confidentiality of security-related data stored in the vehicle including cryptographic keys and certificates
  - Vehicles must be able to protect the confidentiality of data exchanged with security servers
    - Data exchanged with a security server to acquire cryptographic keys and certificates
- BUT **data confidentiality is not required for CAMs** because **their contents are meant to be viewed by all vehicles in the vicinity**

- Confidentiality **is not the most critical security objective** due to the broadcast nature of V2X

Lecture 6

Security Objectives – Misbehavior Detection and Revocation

- **Ability** to detect **misused certificates** and **misbehaving** vehicles and the ability to **revoke misbehaving vehicles' privileges** to send messages that other will trust

- Prevent misbehaving vehicles to harm the transportation system endlessly

- Without revocation of misbehaving vehicles, they would **accumulate** in the network and could **cause severe disruptions** to the system

- **Ability of detect** and **revoke misbehaving vehicles** is the **prerequisite** for real-world deployment of V2X of a nation-wide network

Lecture 6
Security Adversaries

- Individuals or organizations that would make use of communication capabilities to mount security and/or privacy attacks to the network
  - **Individuals** operating on their own with limited resources (e.g. monetary): Computer hackers, electronics hobbyists
  - **Loosely coordinated groups** with more resource than each individual: Sharing private keys with collaborators to collectively multiply the damages
  - **Insiders** owning sensitive information about security protection system for an organization
  - **Adversary organizations** with abundant resources and sophisticated technologies
  - **Foreign governments** interested in mounting security attacks to nation's vehicle networks
  - **Government agencies** permitted to breach driver privacy

Lecture 6

Security Threats

- ► Send false safety messages using valid security credentials
- ► Falsely accuse innocent vehicles
- ► Impersonate vehicles or network entities
- ► Denial-of Service attacks

Lecture 6

Security Threats: Send false safety messages

- An **adversary** could cause some vehicles to send **false safety messages** to other vehicles or the roadside unit
  - Counterfeit CAMs carrying bogus information on vehicle positions and speeds
  - False emergency electronic brake lights
  - Fake traffic information messages
- False safety messages **could cause vehicle to issue unnecessary warnings** to drivers
- Multiple ways to alter the input data
  - A malicious device connected to the **CAN bus** can insert extra **erroneous packets** onto the CAN bus
  - A malicious could tamper with **vehicle onboard sensors** to cause them to generate false inputs
  - **Malfunction of onboard communication unit** or hardware could cause the vehicle to send false or erroneous messages

Lecture 6

Security Threats: Falsely accuse innocent Vehicles

- ► Vehicles may be required to report **misbehaviors** helping to detect misbehaving vehicles
- ► **Global misbehavior detection system** can used information collected from multiple vehicles to make **better** and **accurate judgments**

- ► BUT misbehavior could abuse this reporting process
  - ► By sending reports to **falsely accuse innocent vehicles** as misbehaving vehicles
  - ► Impact the **misbehavior detection system's ability** to detect misbehaving vehicles

Lecture 6

Security Threats: Impersonate Vehicles/Network Entities (1/2)

- ► Malicious vehicle could pose as **a different vehicle** by using another vehicle's credentials

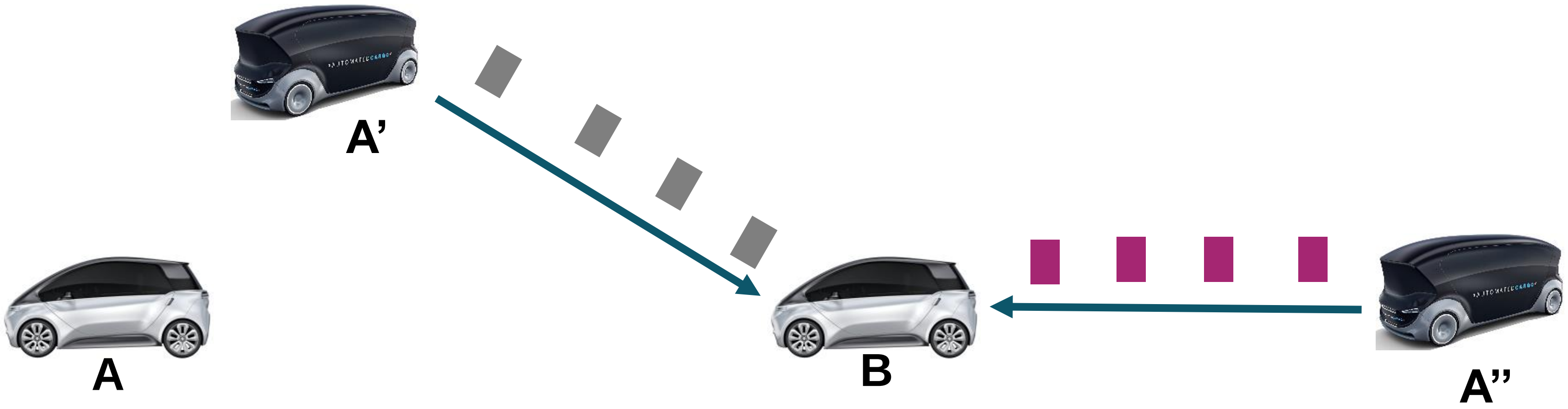
- ► **Sybil Attack**:
  - ► Malicious vehicle sends safety message to attempt to **convince** other vehicles that **more vehicles are present** than there actually are
  - ► Most dangerous form of impersonate attacks

Lecture 6

Security Threats: Impersonate Vehicles/Network Entities (2/2)

► Malicious vehicle A sends **two message streams** with different certificates carrying fake positioning and speed information

► Innocent vehicle B **thinks** there are two different vehicles A’ and A’’ that do not exist



Lecture 6

Security Threats: Denial-of-Service Attacks (DoS)

- ► Goal of these attacks is to **disable**, **degrade** or **disturb** the functionality, capability and performance of vehicle communication
- ► Well known DoS attacks:
  - ► **Jam** the radio waves
  - ► **Flood** the vehicle network with wasteful messages to overload the radio communication channel
  - ► **Compromise** RSUs to disable their services
- ► Most dangerous attack specific for V2X
  - ► Attacker's vehicles is used to cause the security credential management system, e.g. certificate management system
  - ► To **overload** the network with credential management messages
  - ► To cause a large number of vehicles **to lose their security credentials**

Lecture 6
Basic Security Algorithms

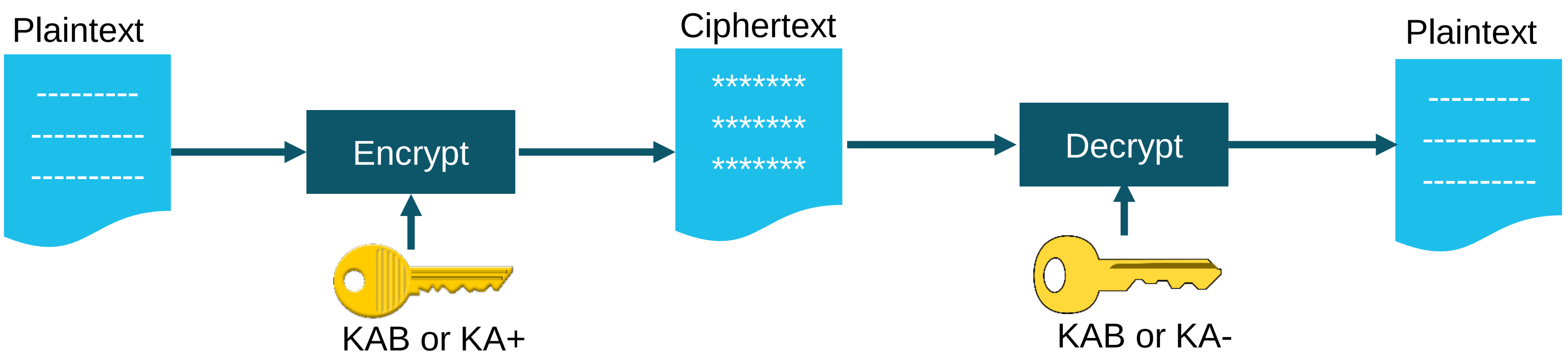
- Three classes of security techniques in the field of network security:
  - **Cryptographic algorithms**
    - Mathematical transformation of input data (data and keys) to output data. It is used in cryptographic protocols
  - **Cryptographic protocols**
    - Series of steps and message exchange between multiples entities to achieve a specific security objective
  - **Security-supporting mechanisms**
    - Provide security-relevant functionalities as a part of a cryptographic protocol

- Main applications of cryptographic algorithms
  - **Encryption of data**
  - **Signing of data**

Lecture 6

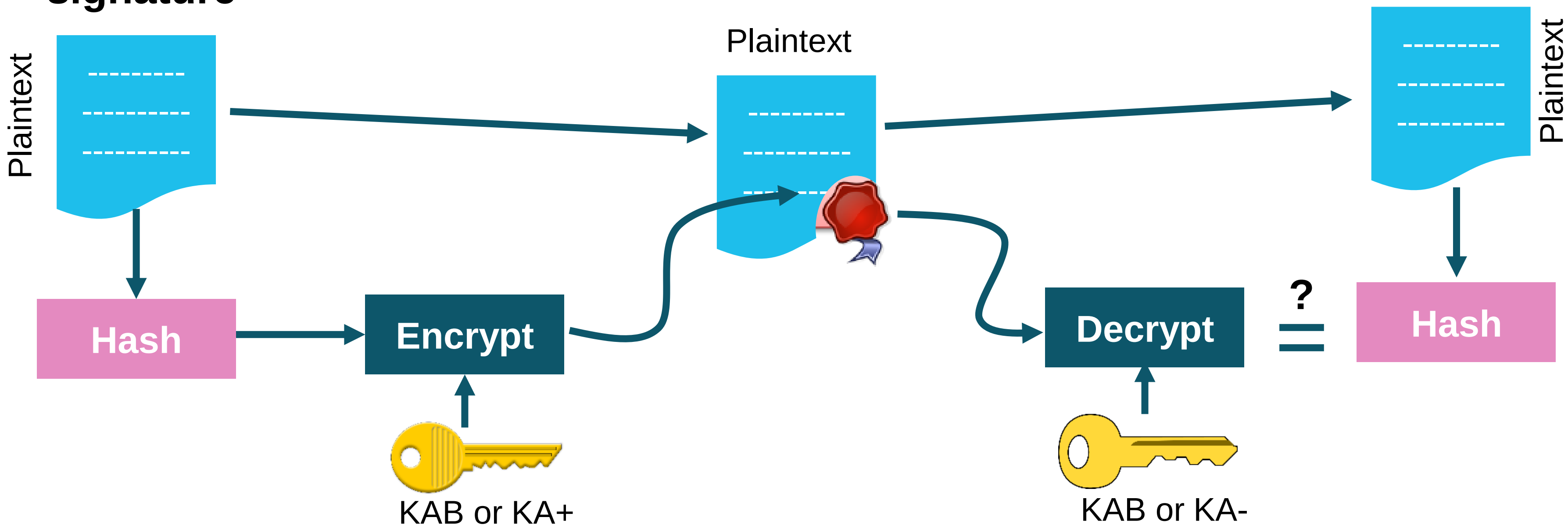
Encryption of Data

- Transformation of **plaintext** data into **ciphertext** in order to conceal its meaning
- Cryptographic encryption algorithm is used in combination with a **key**
  - **Symmetric encryption**
    - Single **shared key** is used for encryption and decryption, eg. K_{AB}, both node A an B have to be in possession with the key but not other entity
  - **Asymmetric cryptography**
    - Two different keys for encryption and decryption: Public key KA+ of the receiving node A is used to encrypt the data. Whereas A uses it own private key KA- to decrypt the data



Lecture 6
Signing of Data

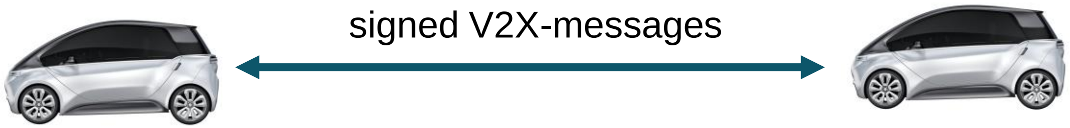
- **Computation of a check value** or an assignment of a digital signature to a given plain text or ciphertext
- **Signature** is based on a cryptographic **hash function** in combination with a cryptographic encryption algorithm
  - **Hash function** is used to calculate a **hash value** of the original text
  - **Hash value** is encrypted (symmetric or asymmetric algo.) to calculate **digital signature**



Lecture 6
Certificate

- Kind of **ID card** providing information describing the owner such as its **name** and its public key
- Allow a secure transfer of the **public key** to the sender
- The **Certificate Authority (CA)** secures the certificate itself by signing it with his private key
  - **Public key of the CA** must be known in advance to receivers of a signed message
    - Preinstalled in the local system

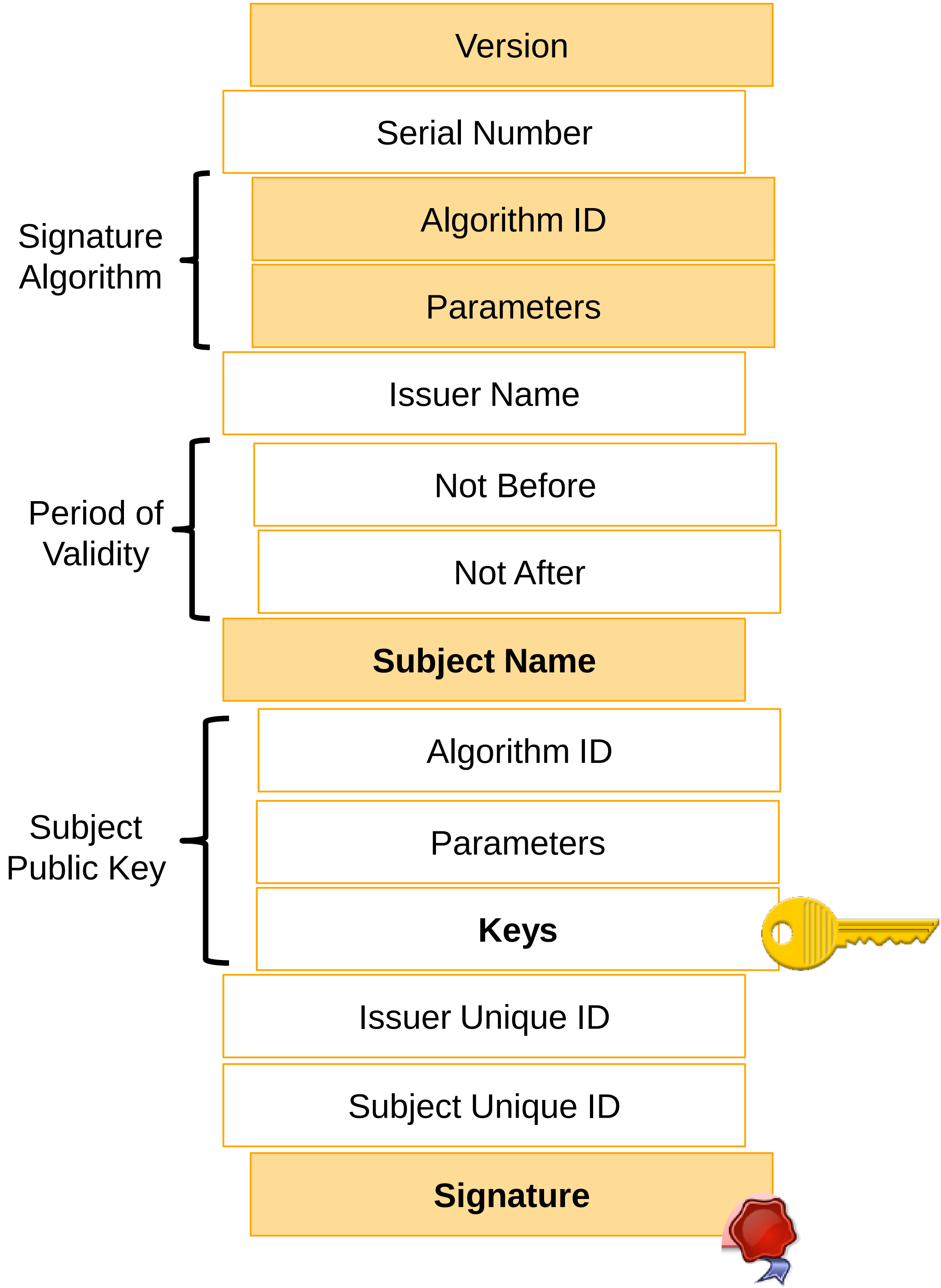
- **X.509 certificate** is used for signing **V2X-messages**



Lecture 6

X.509 Certificate

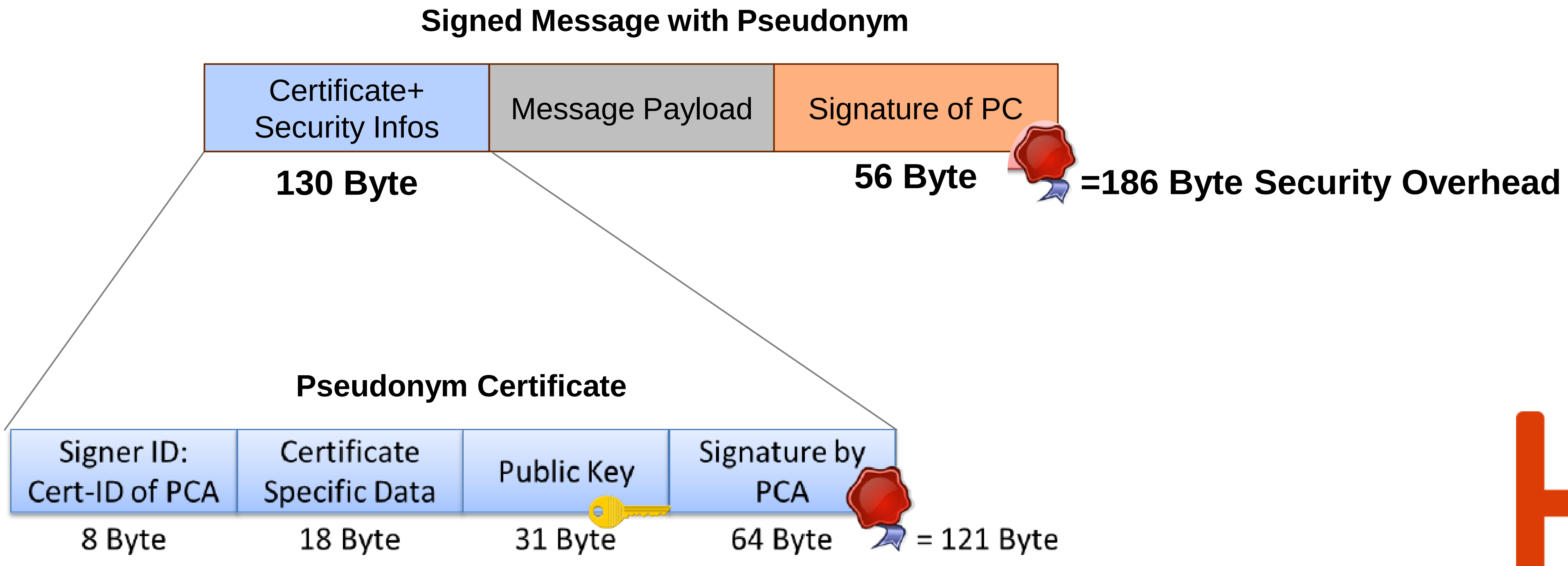
- Defines a complete security framework focusing on authentication services
- De **facto standard** for almost all area of computer networking where **digital signatures** are required
- Contains at least the **name** of its **owner** and its **public key**
  - Protocol version, certificate serial number and validity-period
  - ID of the issuing CA
  - Signature containing an encrypted hash of the whole certificate
  - Signature algorithm to identify crypto. hash and encryption algo. as well as their configurations



Lecture 6

Structure of signed Message with Pseudonym

- Messages are **signed** with the **private key** of the sender
- Receiver needs the **public key** that is part of the **(Pseudonym) certificate**



Lecture 6

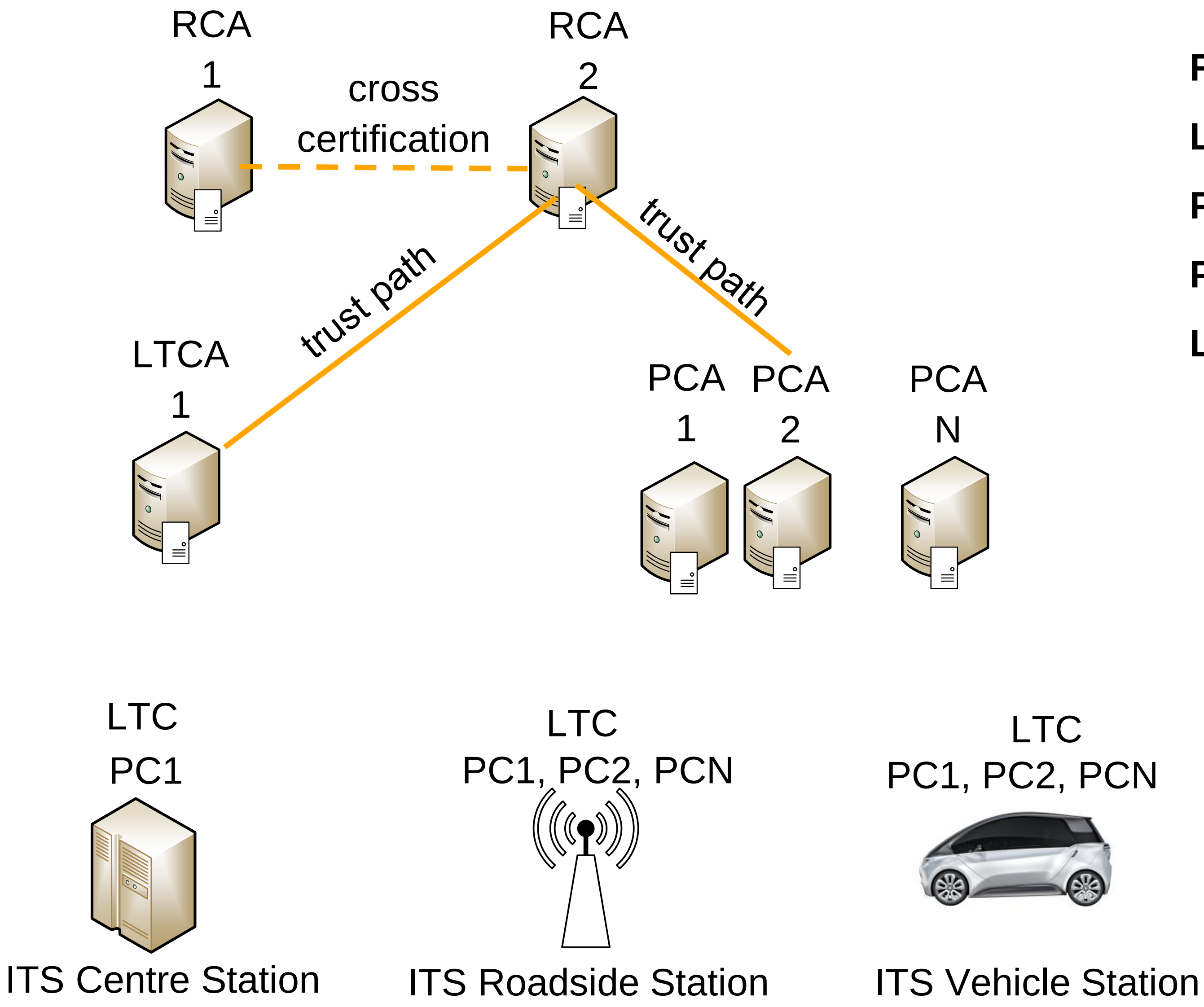
Public Key Infrastructure (PKI)

- **Central PKI** used to **distributes digital certificates** to all participating communication entities
  - For authenticating **valid** participants

- **Flexible** structure of the PKI for international integration as well as adaptations of processes to implement possible future requirements
  - **Message verification**
  - **Certificate updates**
  - **Entity revocation**

- Also known as **C-ITS Security Credential Management System (CCMS)**

Lecture 6
PKI Architecture



RCA: Root Certificate Authority

LTCA: Long Term Certificate Authority

PCA: Pseudonym Certificate Authority

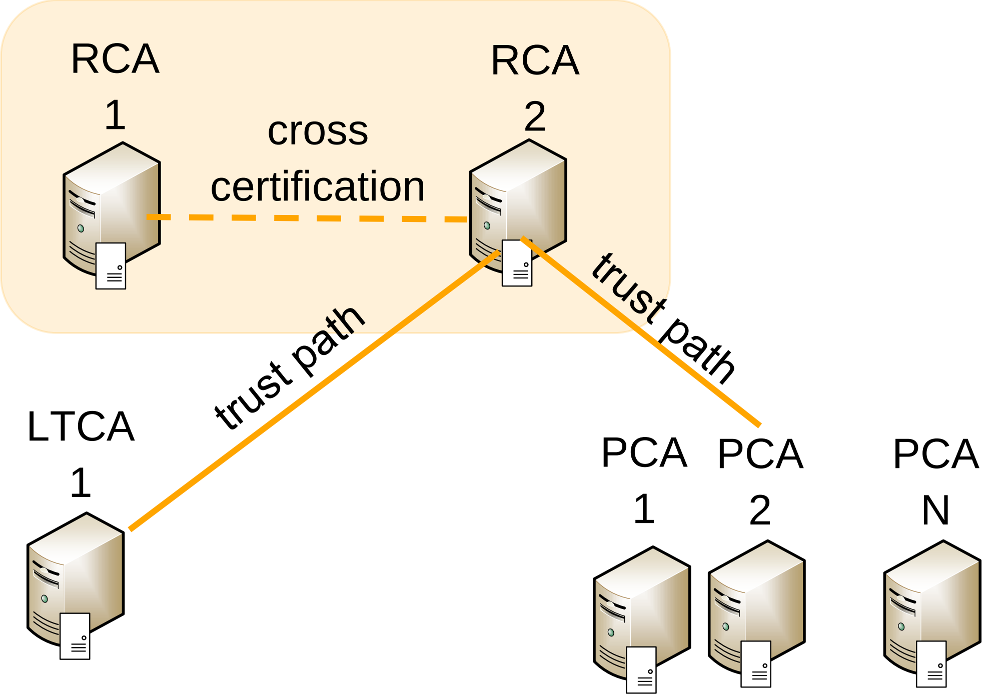
PC: Pseudonym Certificate

LTC: Long Term Certificate

Lecture 6

Root Certificate Authority (Root CA)

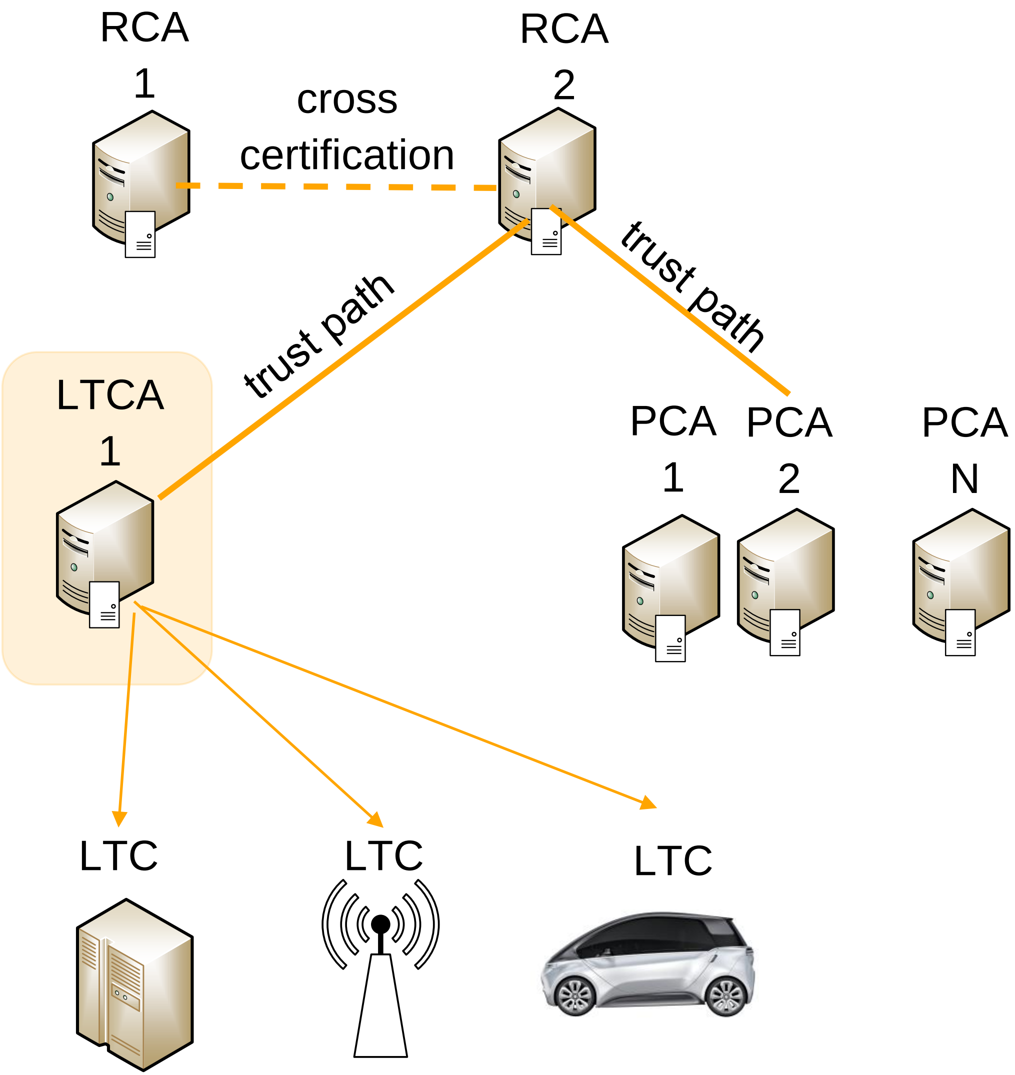
- The role is to define **common policies** among all subordinate LTCAs and PCAs
- It only issues certificates for **Long-Term CAs** and **Pseudonym CAs**, which are valid over long periods
- Interaction with LTCAs/PCAs is only required once a **new** LTCA or PCA is created, and when the **lifetime** of an LTCA/PCA certificate **expires**
- Multiple **RCAs** have to cross-certify each other
  - Root CA on a **European level**
  - Cross-certification between CAs and RCAs other than own RCA is **not allowed**



Lecture 6

Long-Term Certificate Authority (LTCA)

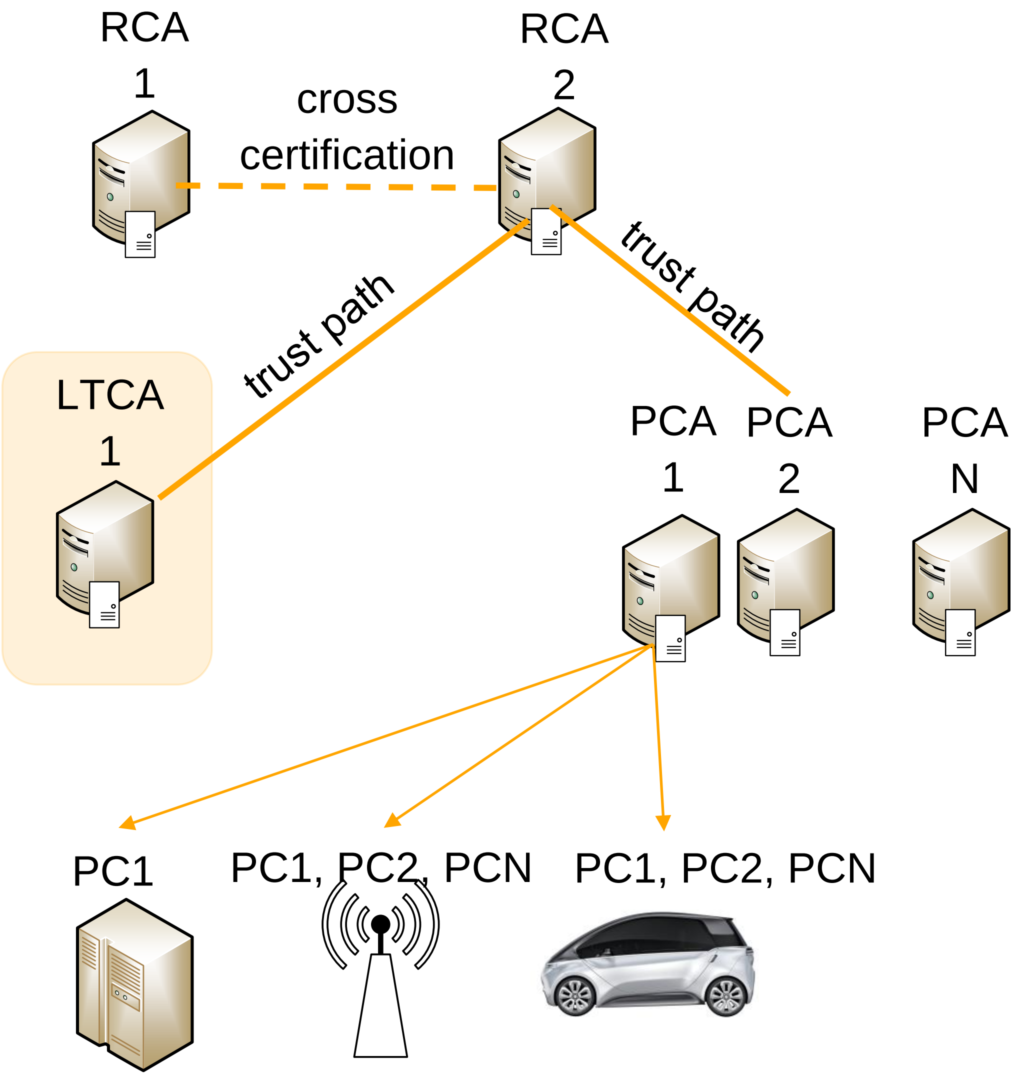
- ► Issues long-term certificates (LTCs) to **ITS stations**
- ► LTCs are valid for **a longer time period** and are dedicated to identify and authenticate ITS stations
  - ► Every LTCA has a Long-Term CA certificate that **is signed by** the **RCA**
  - ► Each ITS station has only **one valid LTC** at a time
- ► LTCAs are **operated** or at least **organized** by manufacturers (**VW, Toyota**), their suppliers or contractors
  - ► Due to their **close** relation to ITS stations



Lecture 6

Pseudonym Certificate Authority (PCA)

- Every PCA is are **directly authorized** by the **RCA**
- PCA issues pseudonym certificates (PCs) to **ITS stations**
  - **PCs** are used by ITS stations for communication purposes (G5A)
  - **PCs** are dedicated to have a short lifetime and shall be exchanged frequently
  - **PCs** shall include minimal information to preserve the privacy of the sender
  - An ITS station may be issued **a large number of PCs** valid in parallel



Lecture 6

Benefits of the PKI Architecture (1/2)

- ► **Trust uniformity and cost efficiency of a Root CA**
  - ► **Cost efficient** of registration of new Long-Term CAs and Pseudonym CAs when having a Root CA as central trust anchor
  - ► A new Pseudonym CA operator doesn’t have to make contractual relationships with all worldwide long-term CAs in order to be admitted
    - ► Increased number of contracts and costs between all involved authorities

- ► **Flexibility for process integration**
  - ► Separation between technical framework and operational instantiation options
  - ► An OEM (VW, Peugeot, Fiat) could operate a long-term CA under the European Root CA and an organization (C2C-Communication Consortium) provides a common PCA for all OEMs

Lecture 6

Benefits of the PKI Architecture (2/2)

- **Flat Structure**
  - **Keep overhead** of transmitting certificates over ITS-G5A **minimal**
  - Only one single certificate (source's Pseudonym Certificate) is attached to a message
  - Receivers must have the corresponding issuer certificate (of the PCA) available to be able to verify the message
  - All PCA certificates are preloaded or updated in an vehicle/ITS station
  - If not available the PCA certificate may be requested on demand from the sender

Lecture 6
PKI Requirements

- **Flexibility and extensibility** to support different regional and organizational environments. PKI must ensure that privacy of drivers cannot be broken
- **Low structural complexity** in order to keep trust effectively manageable
- Separation of basic technical framework, organizational implementation and policies/configuration
- **Modular architecture** to easily include or exclude extended features, e.g. separate authentication and function

Lecture 6
Aspects of Privacy

- **Privacy of location**
  - Where is the target individual?
  - Where was the target individual at a given time?
  - Where will the target individual likely be at a given time?

- **Privacy of interests**
  - Hobbies, services, news sources
- **Privacy of social standing**
  - Job, income, debt, home, contractual obligations
- **Privacy of social network**
  - Family, friends, friends-of-friends, acquaintances

Lecture 6

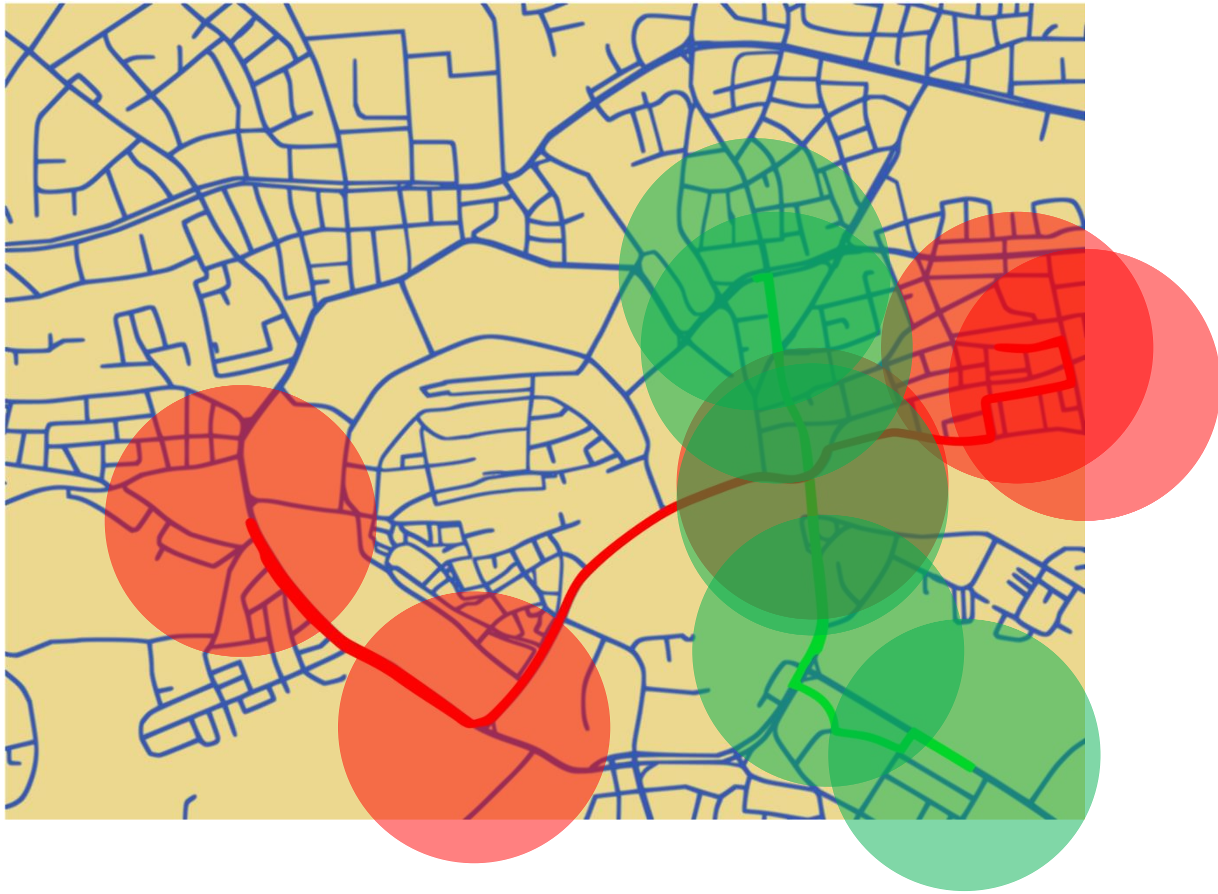
Location Privacy

- ► Most relevant aspect for V2X networks
- ► Ability to prevent third parties from **recording the current location** and location **changes** of a vehicle
- ► Location privacy seen as a security objective
- ► Security measures **reduce the level of privacy** because identities are strongly bound to the vehicles
  - ► Although each CAMs is secured using a digital signature, the vehicle **still reveals its identity** through the certificate used
- ► Anonymity → “being not identifiable within a set of subjects”
  - ► Not appropriate for V2X as vehicle at a certain location do not all share the same properties (vehicle type)
- ► **Challenge: How to increase vehicle privacy while maintaining a high level of security in V2X network?**

Lecture 6

Vehicle Tracking

- ► Possibility of following the trajectory of a vehicle by use of sample observations
  - ► CAMs/DENMs to track vehicles in a vehicular network
  - ► Camera-based tracking technique using vehicle-identification
    - ► Large base of installed infrastructure is required



Lecture 6
Pseudonymity

- ► Communication can be exploited to reveal the identity of each vehicle
  - ► **Physical layer information**
  - ► **MAC and network layer information**
    - ► Source MAC address (unique for each radio device)
      - ► *Big issue for V2X*
      - ► *Randomized MAC addressed as solution*
    - ► Network layer address information
      - ► *Not relevant for V2X as IP addressing is not used*
  - ► Application layer
    - ► Certificates can reveal the identity of the vehicle
- ► Pseudonym prevents **identification/re-identification** when using a certain **number of different identities** instead of using a **single identity**

Lecture 6

Generation of Pseudonyms

- ► Not possible to tell whether all transmissions have been sent by the same vehicle when **different pseudonyms** which cannot be linked to each other are used
- ► Concept of generation pseudonyms
  1. PCA assigns base identities for new vehicles to the automotive industry
  2. Manufacturer assigns a unique base identity to each new car
  3. Vehicle itself starts creating a pseudonym pool of p different pseudonyms
     - ► Each in form of a certificate request
  4. Vehicle requests the PCA to sign each of pseudonyms generated through an Internet connection
  5. PCA checks the validity of the signing requests using originally assigned based identity. When valid the PCA signs the pseudonyms and sends these signed certificates to the vehicle
- ► All **pseudonyms and certificates** are used to secure messages while not revealing the vehicle's identity

Lecture 6

Pseudonym Pools

- Create pool of pseudonyms (instead of **single one**)
- **Switch between different pseudonyms**
  - Validity
  - No restrictions
  - Spatial restrictions
  - Temporal restrictions

- **Switching strategies**
  - How to enhance anonymity?
  - **Tradeoff between safety and privacy**
    - Vehicle must have **static identifiers** for providing awareness, MUST NOT have for **privacy**

Lecture 6

Pseudonym Switching Strategies (1/2)

- **When to change pseudonym?**
  - **Fully random**
  - **Periodic**
    - Switch to another pseudonym every n seconds
  - **Geographical**
    - Switch to another pseudonym depending on region
  - **Vehicle dynamics and communication quality**
    - Use of position, speed, heading and number of cars in transmission range to trigger a pseudonym change
  - **Introducing silent periods**: After changing a pseudonym the vehicle stops emitting messages for a random amount of time → But lead to increase message latency

Lecture 6

Pseudonym Switching Strategies (2/2)

► Use of many pseudonymous identifiers to prevent tracking

Lecture 6

Security Challenges of V2X Network

- **Protocol overhead**
  - For each CAM, a signature as well as a certificate needs to be added to the original message
    - At least 150-160 Byte will be used for security measures
    - At CAM generation rate of 10 Hz → 1500 – 1600 B/s per vehicle
    - For a medium vehicle density of 100 vehicles in a communication range → **150 kB/s for security overhead**
- **Computational overhead**
  - For each CAM sent and received, complex asymmetric cryptographic algorithms need to be executed
    - One signature generation per beacon sent
    - Two verifications (signature + certificate) for each beacon received
    - **2000 operations/second** (100 vehicles@10Hz@2verifications)

Lecture 6
Literature

► Car2Car Communication Consortium, “Public Key Infrastructure”, 2012

► Luca Delgrossi and Tao Zhang: “Vehicle Safety Communications: Protocols, Security, and Privacy, Wiley, 2012

► Christoph Sommer and Falko Dressler: “Vehicular Networking”, Cambridge University Press, 2014