Enhanced Security, Privacy & Trust in Connected Cars

Technologies for Establishing & Managing Trust in CCAM

Thanassis Giannetsos

UBITECH Research Institute
Digital Security & Trusted Computing Group

Dagstuhl Seminar, January 27^{th}, 2022

Key Messages as we are moving forward

- Importance of Trust in the **data sharing** economy
- Data sharing between Autonomous Vehicles
  - ⇒ *Which is considered personal data or that can impede different privacy aspects of the users?*
  - ⇒ AVs have sensors and collect massive amounts of data
  - ⇒ Such data constitute the corner-stone for most of the safety-critical applications; e.g., collision avoidance
- Trust through Connected Car Technology
  - ⇒ Don't forget the additional entities of the backend (e.g., MEC, 5G)
  - ⇒ **Trust to the EDGE** - *Do I trust the EDGE device to calculate on my behalf?*
  - ⇒ **Trust to the NETWORK** - *Do I trust the input given by other platforms? Compromise or malfunction*
- Tension between **trust-building** and **privacy protection**

Principles of Evolving Complex Ecosystems

BUT IoT is really about the "DATA" and closing the loop:

⇒ **Users are the focal point of the sensing infrastructure**

- ⋆ "*Data lives forever...*" - When does this become user personal data?

⇒ **Security & Privacy are needed to protect the loop!**

- ⋆ S&P requirements for core IoT end points - *Mobile devices, Vehicles and Sensors*

Software eats the world...and what's left is data

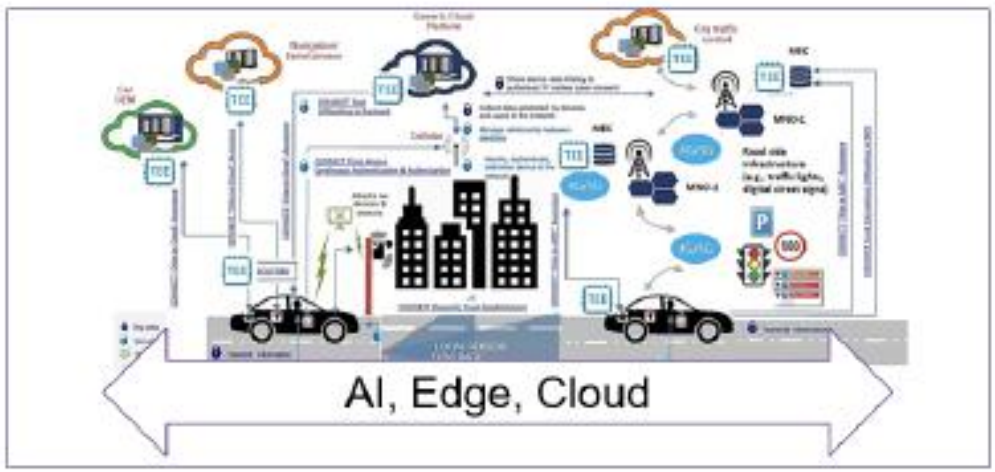
- ⇒ Telemetry data which can be used for maintenance
- ⇒ Data transmitted by connected components need to be authenticated
- ⇒ Data protection is essential
- ⇒ Safeguards code updates against tampering
- ⇒ Ensure that firmware and software code comply with internal policies
- ⇒ Over-the-air reprogramming

Digital Trust Requirements

Orchestrating resources to form a "secure computing continuum"

Quality

Ethics



Reliability

Privacy

Resilience

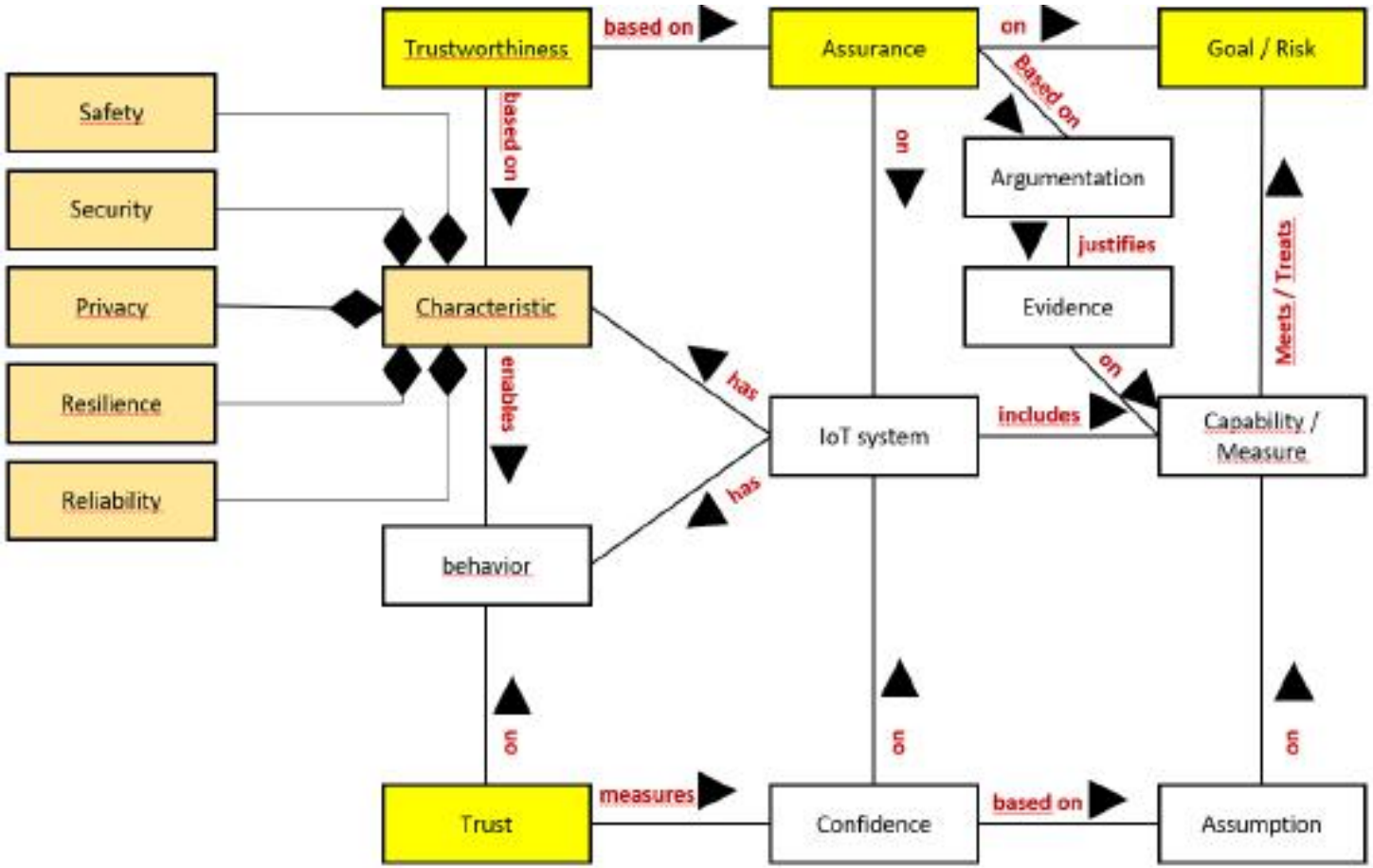
Security

Safety

Liability

Conceptual Model of Trustworthiness

Putting all trust requirements together... (JTC 1 - SC41)



Security & Privacy Challenges

Contradictory positions between vehicles and infrastructure entities. . .

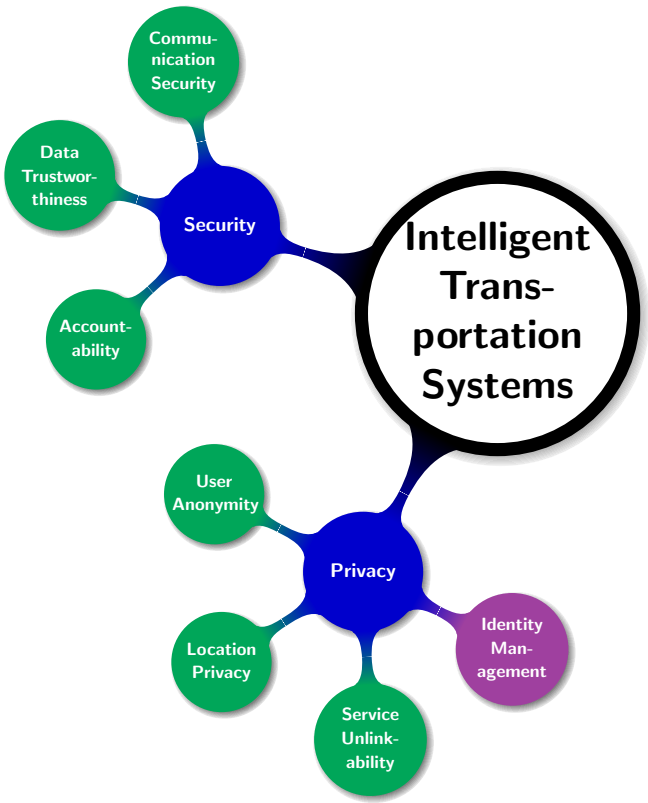
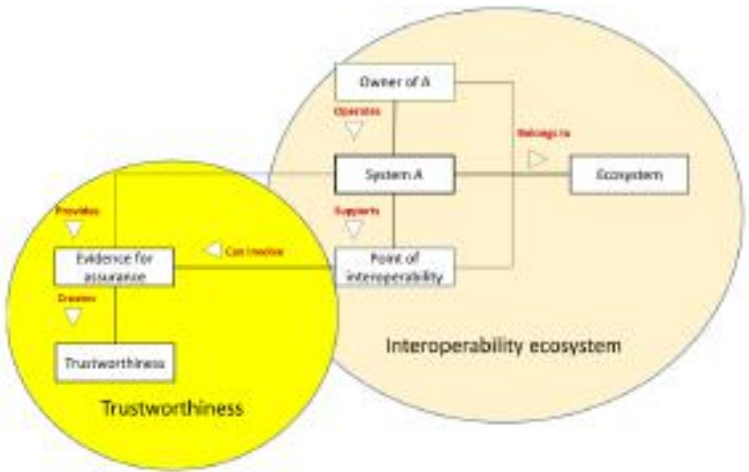


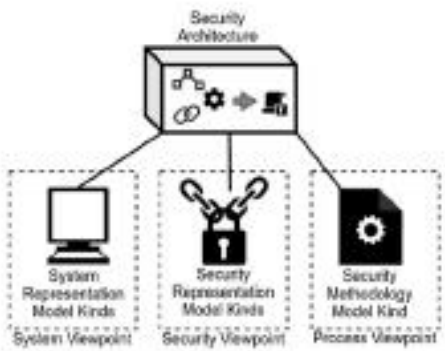
Image source: "Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-Map"

- Protect the Vehicles from the System (i.e., user privacy)
  - ⇒ Anonymity (conditional)
  - ⇒ Pseudonymity
  - ⇒ Unlinkability
  - ⇒ Unobservability
- Protect the System from the Vehicles (i.e., trustworthiness)
  - ⇒ Authentication & Authorization
  - ⇒ Accountability
  - ⇒ **Data Trustworthiness** linked with device integrity

Conceptual Model of Trustworthiness

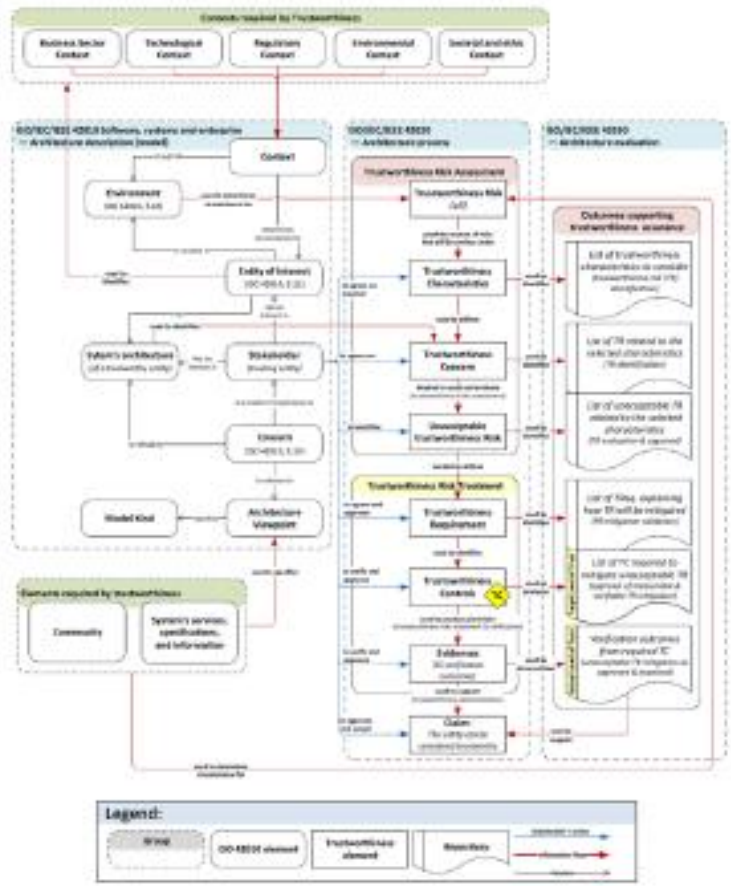
- The impact of **Interoperability**
- **Distributed**
  - ⇒ An Automotive System seen as inherently and increasingly a *federated safety critical system* which is not owned by a single entity
  - ⇒ Communication with multiple entities - beyond vehicles in vicinity BUT also backed infrastructure





Representation of Trustworthiness

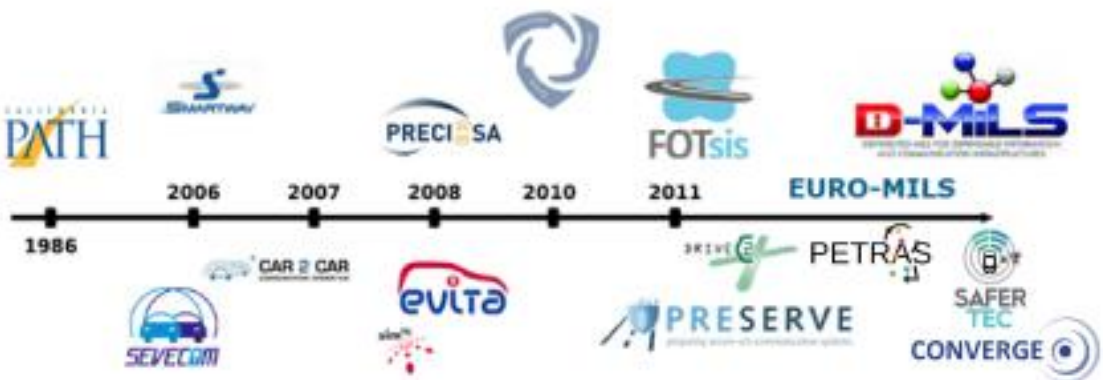
- **Concerns**
  - ⇒ **Characterization** - What are the trustworthiness characteristics? What information do we need to build trust?
  - ⇒ **Measurement** - What are the measurement means for trustworthiness?
  - ⇒ **Impact** - What is the impact for nor addressing sufficiently a charcteristic?
  - ⇒ **Operation** - What are the means to ensure trustworthiness during operation? *Is it possible to build trust without invading privacy?*



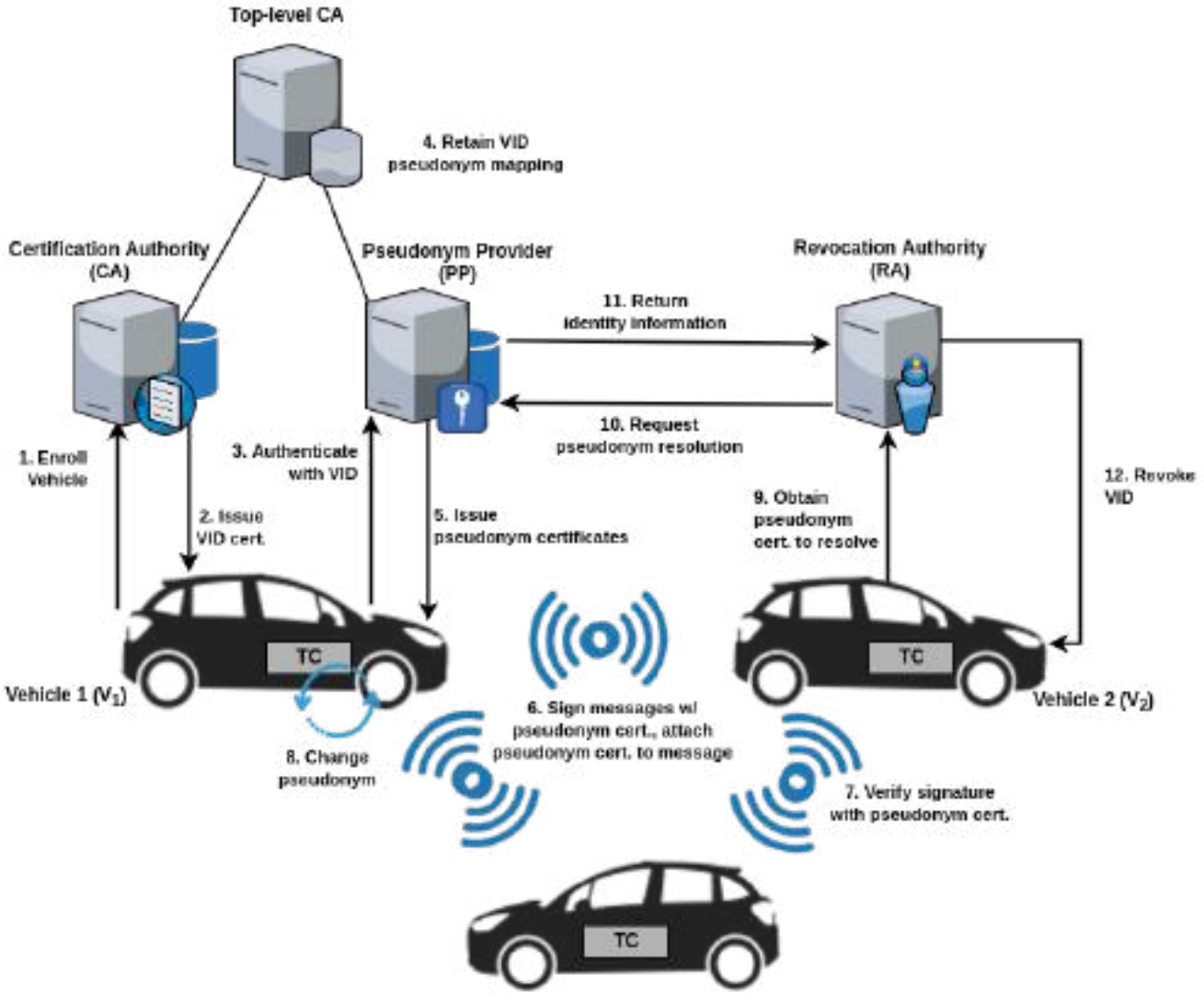
- **Models for Privacy Enhancement:** PKIs vs. Decentralized Roots of Trust

Security & Privacy Architectures - Close to deployment

- IEEE & ETSI standard specifications:
  - ⇒ Each vehicle has a unique LT_{id}; a public key (LK) and the corresponding private key (Lk)
  - ⇒ For privacy protection vehicles receive ephemeral, anonymous credentials (pseudonyms)
- Credential Management is performed by the VPKI:
  - ⇒ LTCAs manage LT_{id}
  - ⇒ PCAs issue pseudonyms
  - ⇒ RAs resolve pseudonyms



State-of-the-art VPKI



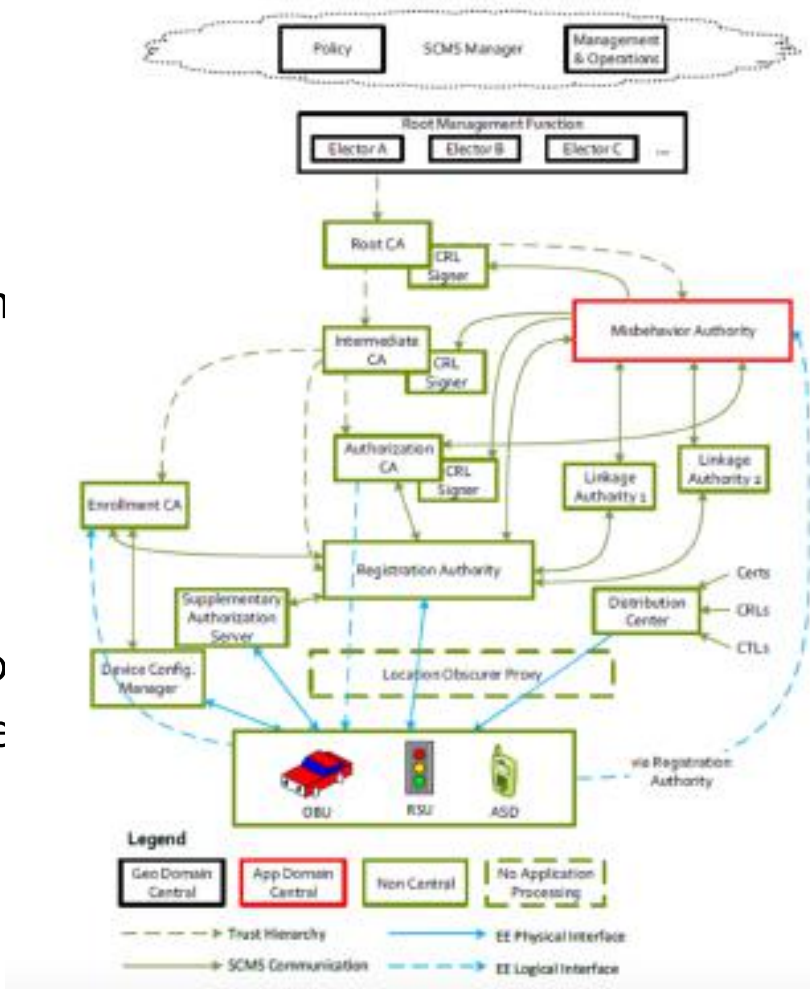
Vehicular PKI for V2X

Concept

- Provide pseudonym certificates such that "no single entity" can relate two certificates

Solution

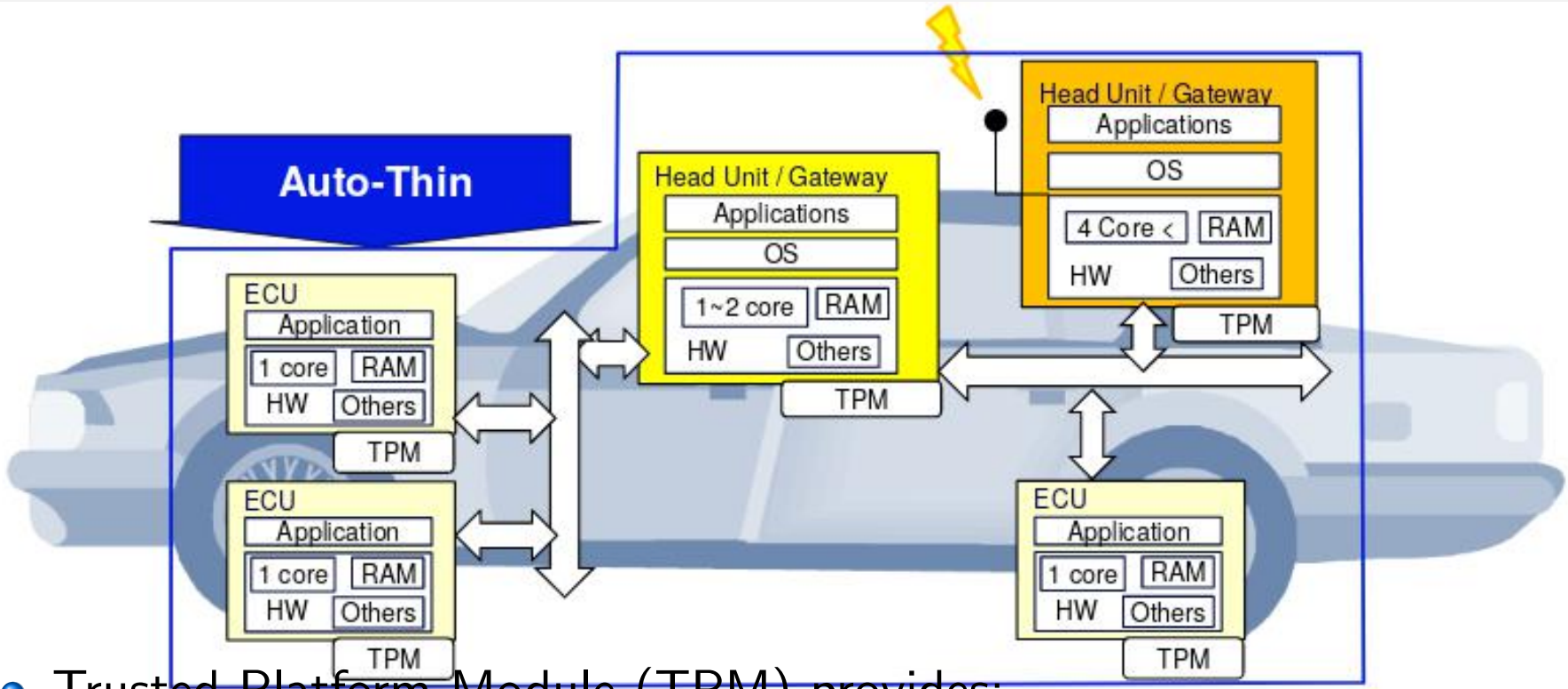
- A very complex architecture with technical and organizational separation Can we simplify this?
- Shift of onus to the SCMS operator. Including MNO in the ecosystem can further justify this
- SCMS operator decides on the rules fo governance and establishes appropriate policies
- Check it out: 5GAA Efficient Security Provisioning System (ESPS)



Challenges...An Alternative Research Avenue

- **Scalability:**
  - ⇒ Many infrastructure entities - *Not clear yet who will operate the identity and credential provision?*
  - ⇒ Connectivity & Bandwidth
- **Privacy & Trust:**
  - ⇒ Protection against "Honest-but-curious" infrastructure entities?
  - ⇒ Separation of duties - *But what happens when we have colluding entities*
- **Revocation:**
  - ⇒ CRLs assumes enhanced connectivity
- **Toward decentralized Roots-of-Trust**
  - ⇒ Shifting trust from the infrastructure to the edge devices
  - ⇒ *Direct Anonymous Attestation*

Trusted Computing for Automotive



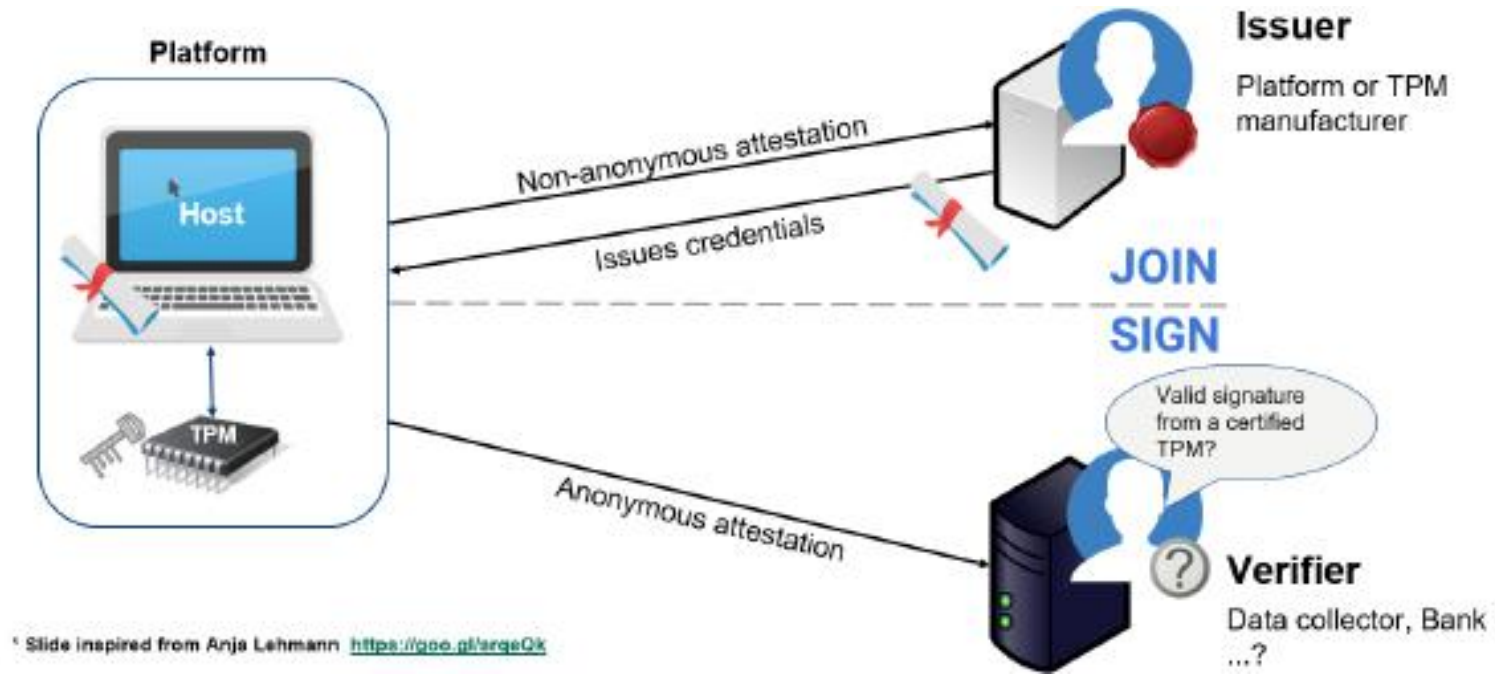
- Trusted Platform Module (TPM) provides:
  - ⇒ Isolation
  - ⇒ Protected Execution
  - ⇒ Shielded Storage
- Secure crypto processor: creates, stores, uses crypto keys
- TCG developing TPM for "Automotive Thin Profile"*

*https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM_2.0_Automotive_Thin_Profile_v1.1-r15.pdf

Direct Anonymous Attestation

- Anonymous digital signature scheme
  - ⇒ Strong, but privacy preserving authentication.
- Hardware-based attestation using TPMs
- Properties of DAA include:
  - ⇒ **Correctness:**
    - → Valid signatures only producible by honest platforms, and are verifiable and linkable when specified.
  - ⇒ **User-controlled Anonymity:**
    - → Identity of user cannot be revealed.
  - ⇒ **User-controlled Traceability:**
    - → The host controls whether signatures can be linked.
  - ⇒ **Non-Frameability:**
    - → Adversary should not be able to impersonate honest platforms.
- Standardised in ISO/IEC 20008-2 & 11889

Overview of DAA

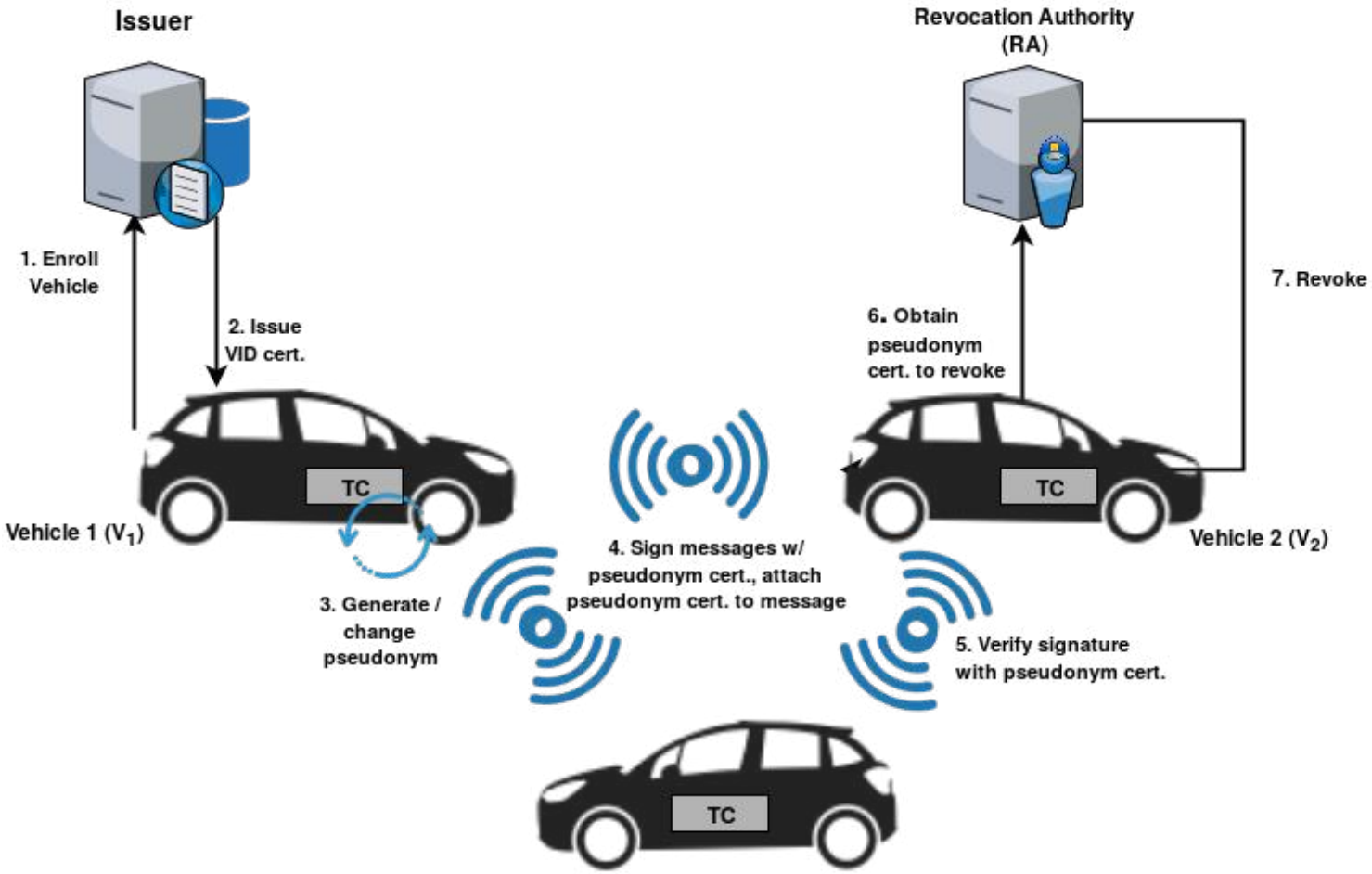


DAA Pseudonym Scheme - Overview

- Simplified VPKI Architecture
  - ⇒ **Issuer:** Authenticates vehicles' to ITS and issues DAA credential
  - ⇒ **Revocation Authority:** Removes misbehaving / malfunctioning vehicles'
- Decentralised ITS allows a shift-of-trust into vehicles.
  - ⇒ Vehicles responsible for self-signing pseudonyms
  - ⇒ Promotes scalability - *Certificate Revocation Lists* not required
- Timely and "*in the moment*" revocation
- Vehicles in control of privacy
- Utilises trusted hardware and uses DAA for hardware-based attestation

Trusted third parties gain no knowledge of ITS entities from colluding with one another.

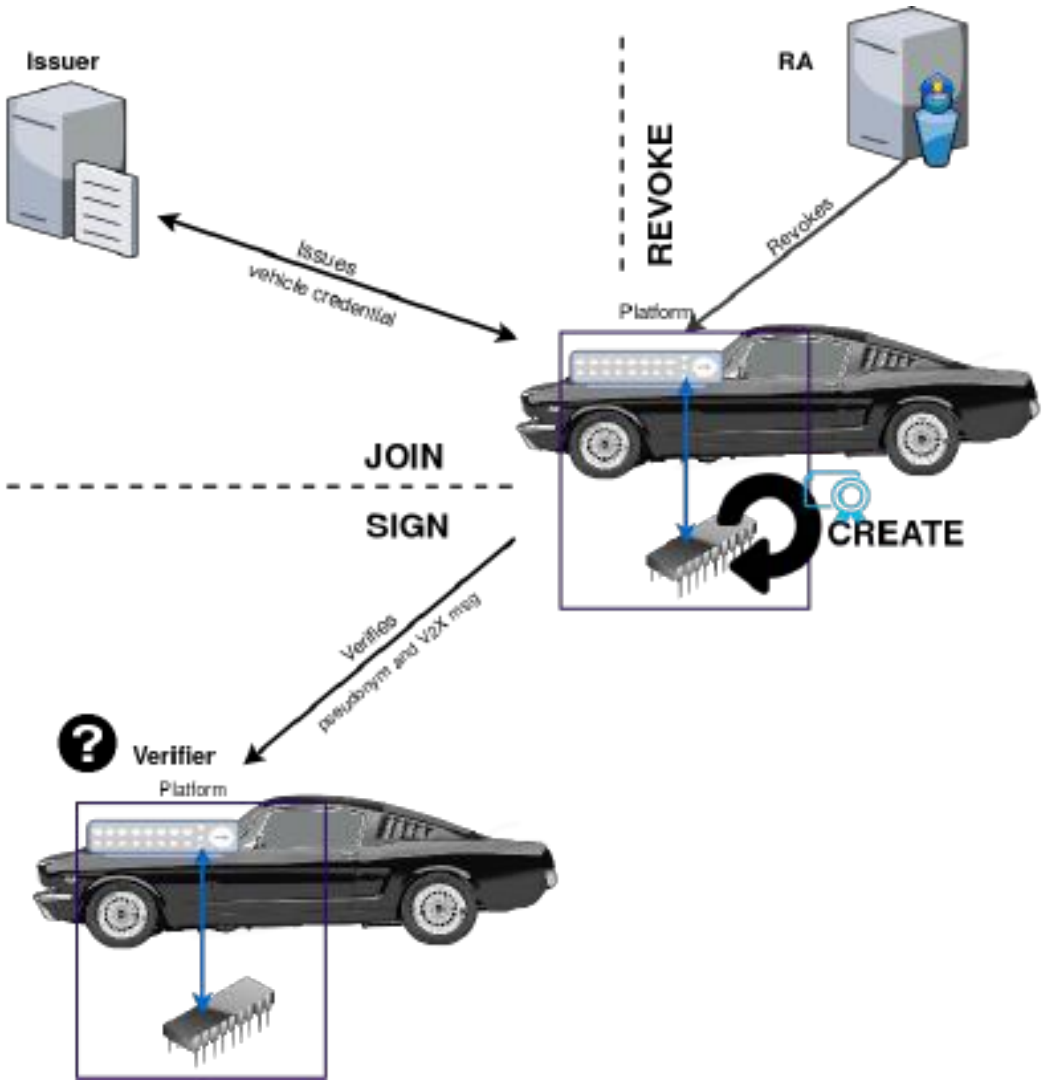
DAA Pseudonym Scheme - Architecture



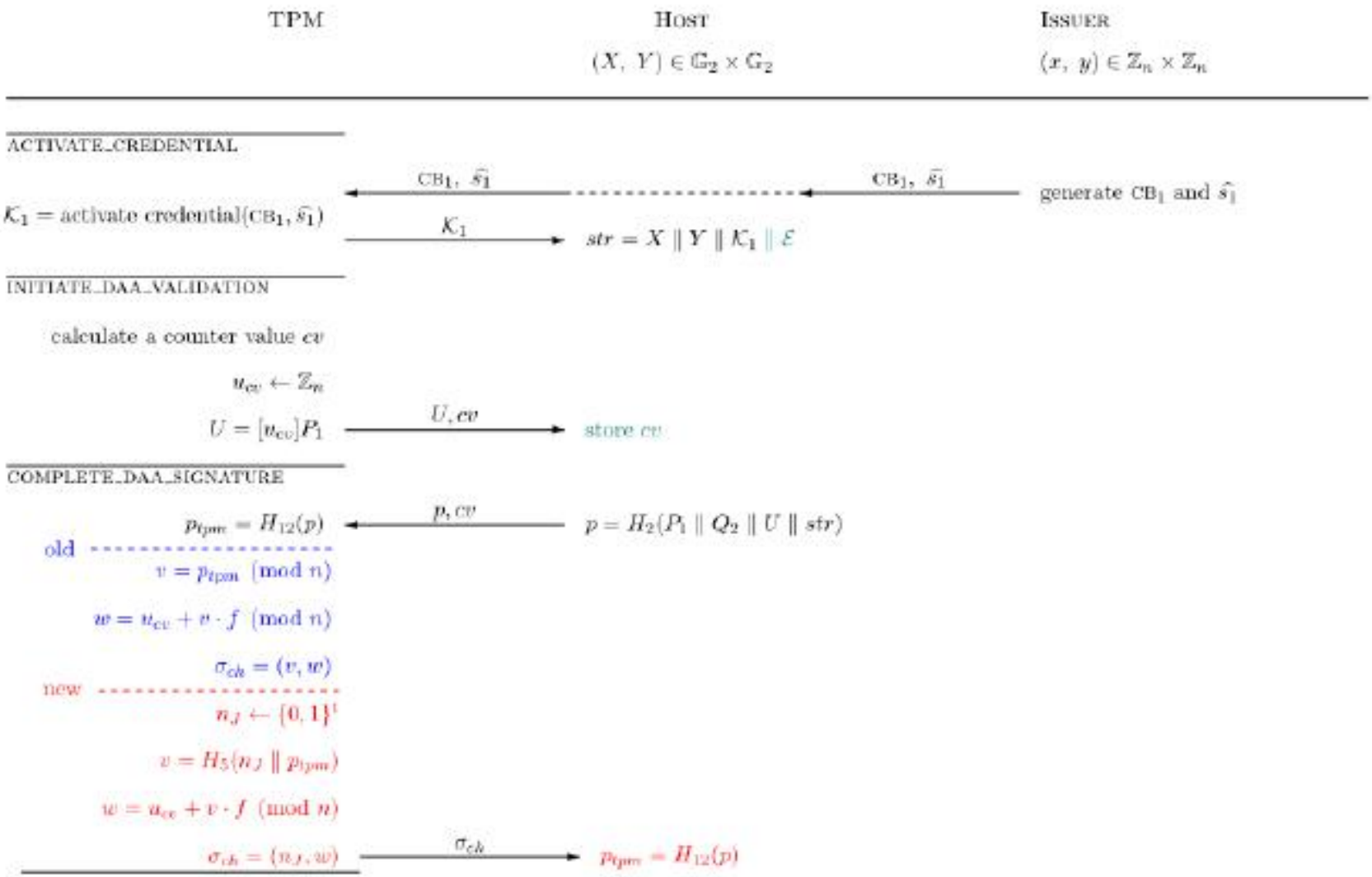
DAA Protocols for VANETs

- SETUP: TC generates fresh DAA key-pair from Issuers security parameters.
- JOIN: Attests that a vehicle has a valid TC, and produces the DAA credential from Issuer $\Rightarrow$ authenticated member of ITS.
- CREATE: Fresh self-signed pseudonyms created by TC using credential.
- SIGN/VERIFY: Authenticated V2X communication that verifies pseudonym is valid.
- REVOKE: Verifiable revocation that a vehicle has been removed from ITS. Performed without pseudonym resolution.

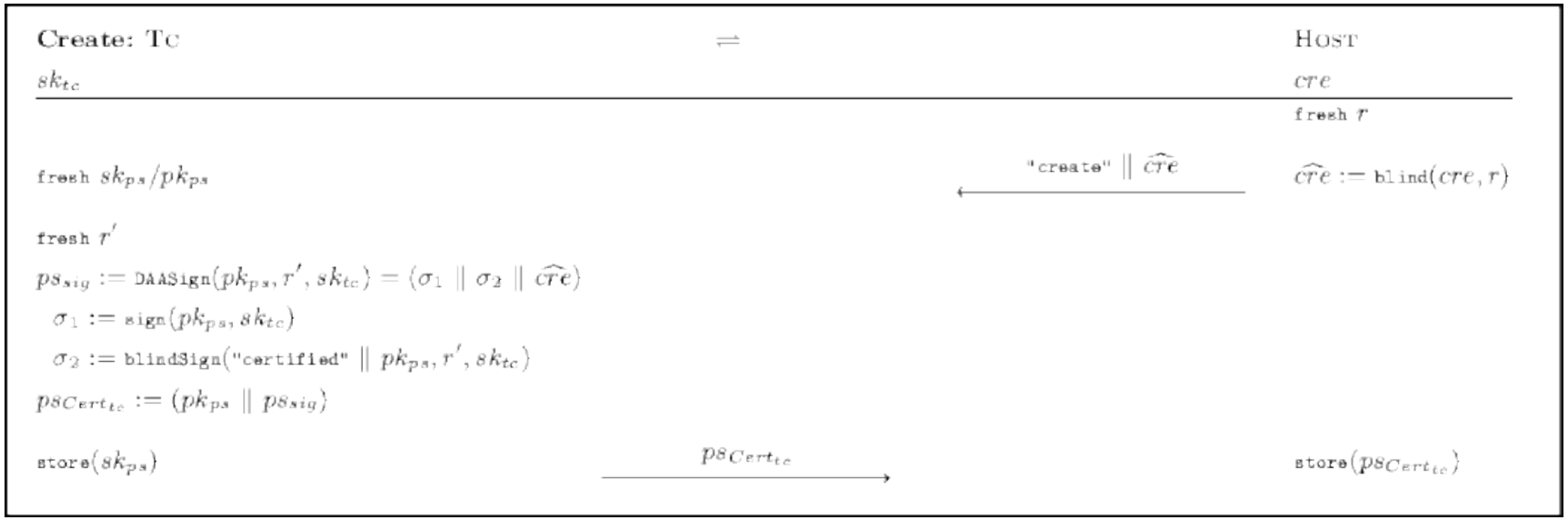
DAA Protocols for VANETs



JOIN Protocol - Update



CREATE Protocol



1. Credential (from JOIN) is blinded by the host for privacy
2. DAASign produces two signatures: σ_1 (*deterministic*) & σ_2
3. Pseudonym is a key-pair with a DAA signature associated with a blinded credential.

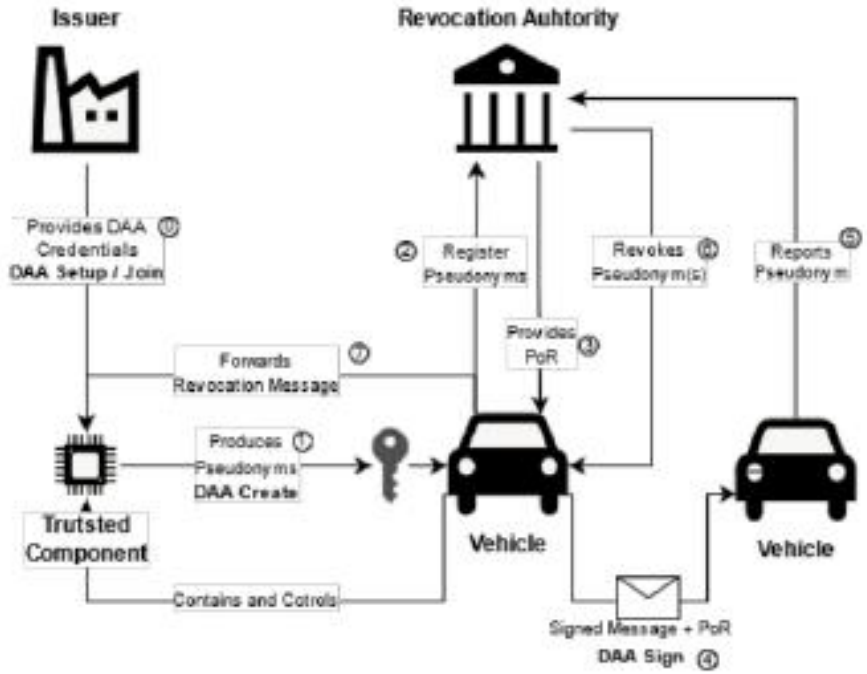
More Scalable Revocation Capabilities

Issuer provides the credentials needed for DAA (verifying the TPM)

Trusted component builds policy-protected pseudonyms

Vehicle registers pseudonyms with the **Revocation Authority**, who in turn provides proof of registration. The vehicle can now use the TC to sign messages and send anonymous, authenticated messages to other vehicles.

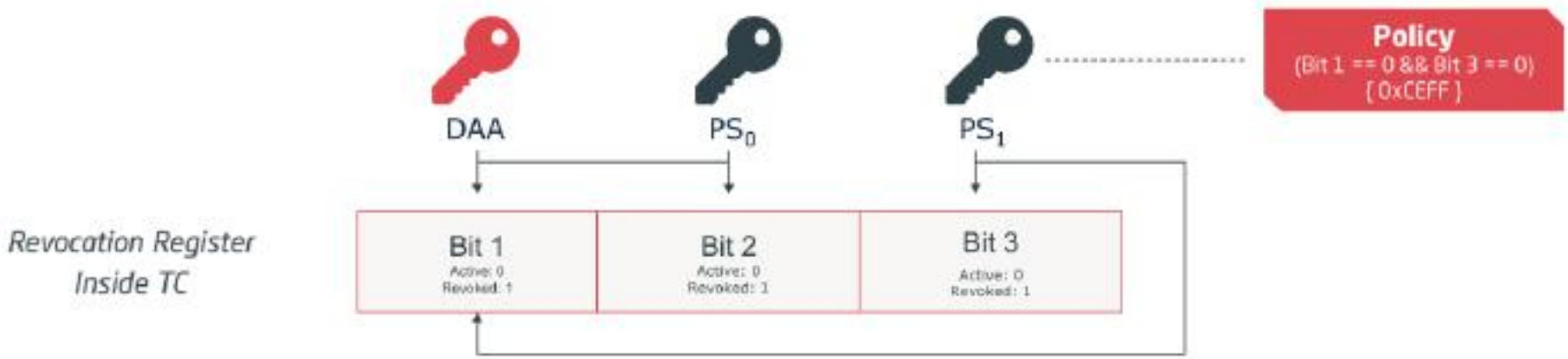
Revocation comes from the RA based on system policies.



How it works?

Goal 1: Pseudonyms can only work if they are not revoked.

Goal 2: If hard revocation is executed on *any* pseudonym, no pseudonyms can work



Each pseudonym is linked to individual revocation bits for Soft Revocation, but they share the DAA revocation bit for hard revocation.

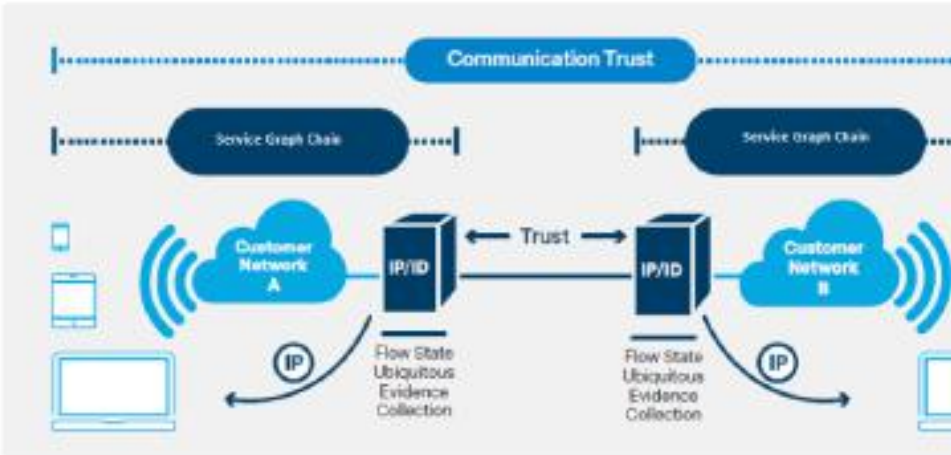
So is that all? Towards Trust Aware Service Graph Chains

Remember till now security and safety were two distinct goals BUT...

- **Industry is now interested in converging security and safety**
  - Contradicting requirements – *Security might impede safety*
  - *Strict requirements in terms of latency, reliability and seamless service delivery*

- **Fundamental issue of trust or trustworthiness**
  – *Remote platform behaves in a reliable and predictable manner*
  - **Trust to the EDGE** – *Do I trust the EDGE device to calculate on my behalf?*
  - **Trust the NETWORK** – *Do I trust the input given by other platforms? Compromise or malfunction*

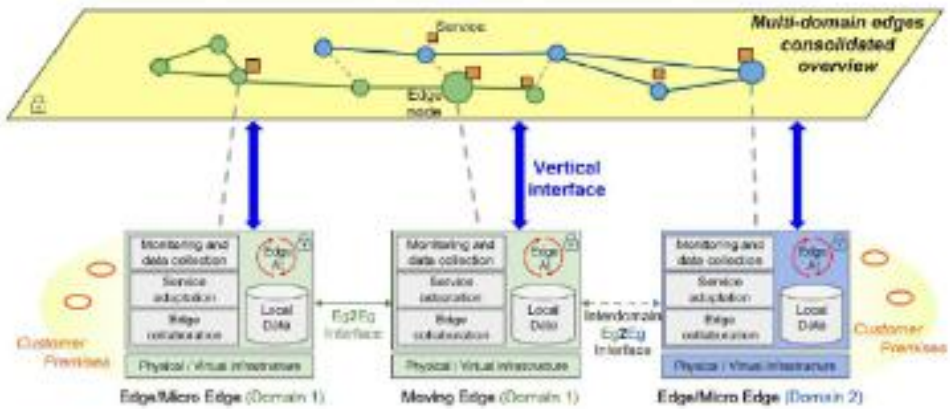
- **Trust Aware SGCs:** Platforms and their running services must be enabled to make and prove statements about their state and actions so that other component of a SGC can align their actions appropriately and an overall system state can be evaluated and enforced



So is that all? Towards Trust Aware Service Graph Chains

- **5G is the vehicle towards realizing next-generation smart-connectivity "Systems-of-Systems" (SoS)**
  - Managing service graph chains for highly distributed and heterogeneous services (cyber-physical end devices, to edge servers and cloud facilities and micro services)
  - Provision of **mixed-criticality services** in several vertical industries
    - Strict performance and security requirements

- **Goal**:
  - Enable high scalability by **decomposing a mixed-criticality application** into a set of **"cloud-native"** and **"edge-running"** micro services, with different trust considerations, and managing secure accelerated offloading capabilities for distributing the resource intensive processes to the backend, thus, limiting the workload that needs to be managed at the edge.



Wrapping it up...

Having connected the car to the external word creates new risks. **Security, Privacy and safety must converge for our best interest.**

The connection of the car leads to drastically influence safety & privacy. Privacy protection is not a burden but an enabler of trust and, thus, of business

Privacy protection is not only about protecting personal information but also about unlinkability, transparency, interveanability

- **Distributed:** An Automotive System must be seen as inherently and increasingly a Federated Safety Critical System which is not owned by a single entity.
- **Bottom Up:** Particularly with respect to Safety, data and system components must be in a position to make strong statements about their (run-time) integrity
- **Defensive:** Static defense techniques will not be enough in the face of a wide range of attack vectors

Future needs in Privacy-Enahcing Technologies

- **We need to capitalize on the shift of value creation to the edge**
  - $\Rightarrow$ Consideration of what trust calculations need to be done in the vehicle for protecting the privacy of data?
  - $\Rightarrow$ Better connection of the worlds of Trusted Computing and AVs
- Many more entities in the overall ecosystem than the Autnomous Vehicles themselves
  - $\Rightarrow$ Consideration of the MEC and the infrastructure. Privacy Implications?
  - $\Rightarrow$ Privacy By Design process needs to be reshaped

Thank You!
Q/A