UNIVERSITY OF SURREY

Formal Analysis and Applications of Direct Anonymous Attestation

14th November 2018

RISE Annual Conference

Jorden Whitefield

sudo_jorden

j.whitefield@surrey.ac.uk

Intelligent Transportation Systems: Security & Privacy Challenges

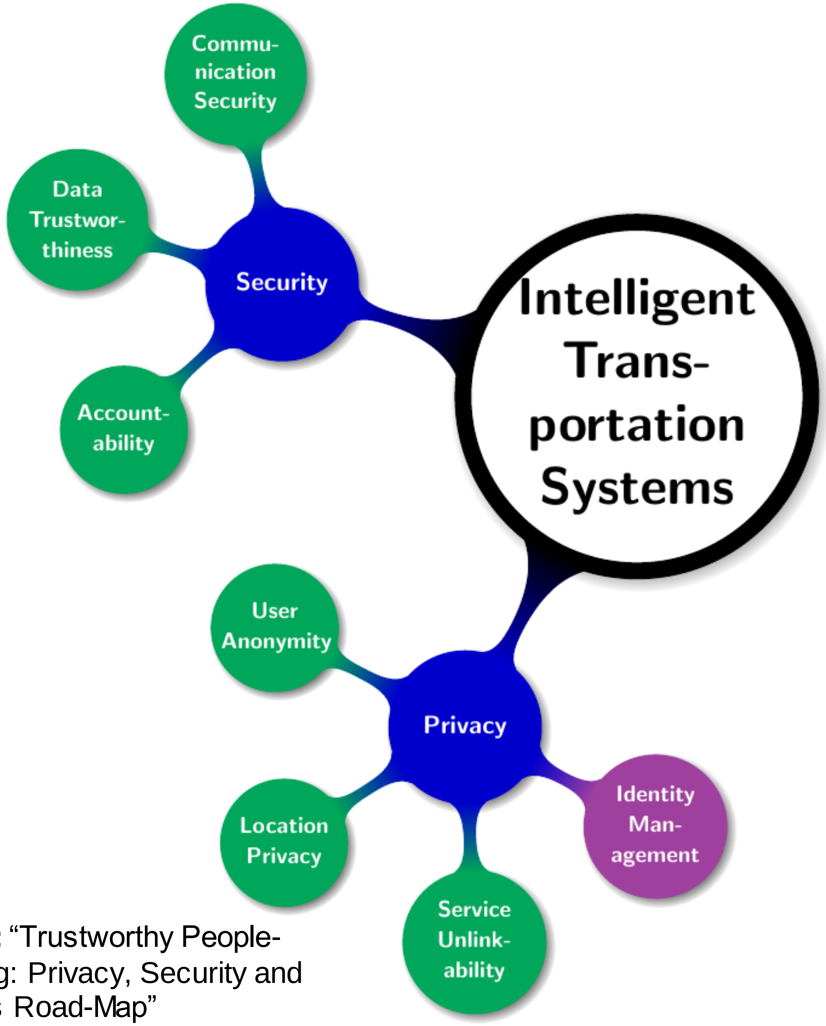


Image source: "Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-Map"

- Protect the users from the System (i.e., privacy)
  - Anonymity (conditional)
  - Pseudonymity
  - Unlinkability
  - Unobservability
- Protect System from the Users
  - Authentication & Authorisation
  - Accountability
  - Data Trustworthiness
- *Contradictory position between users and infrastructure*

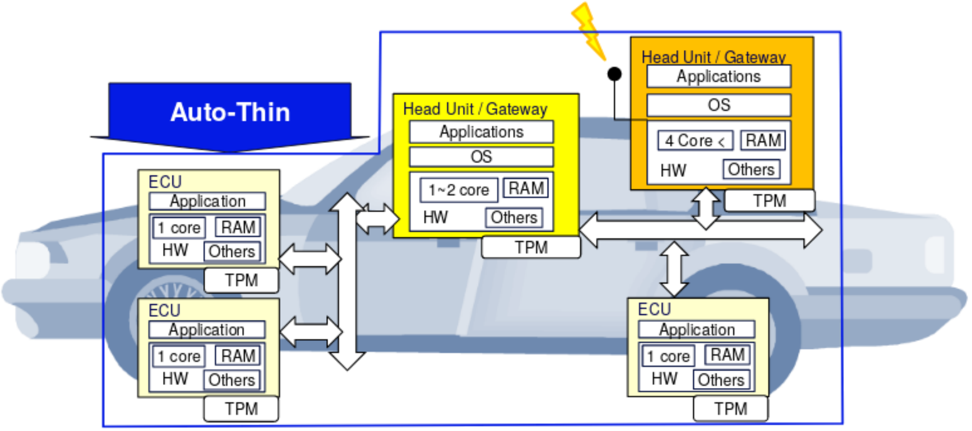
Direct Anonymous Attestation

- Anonymous Digital Signature scheme
  - Strong but privacy-preserving authentication

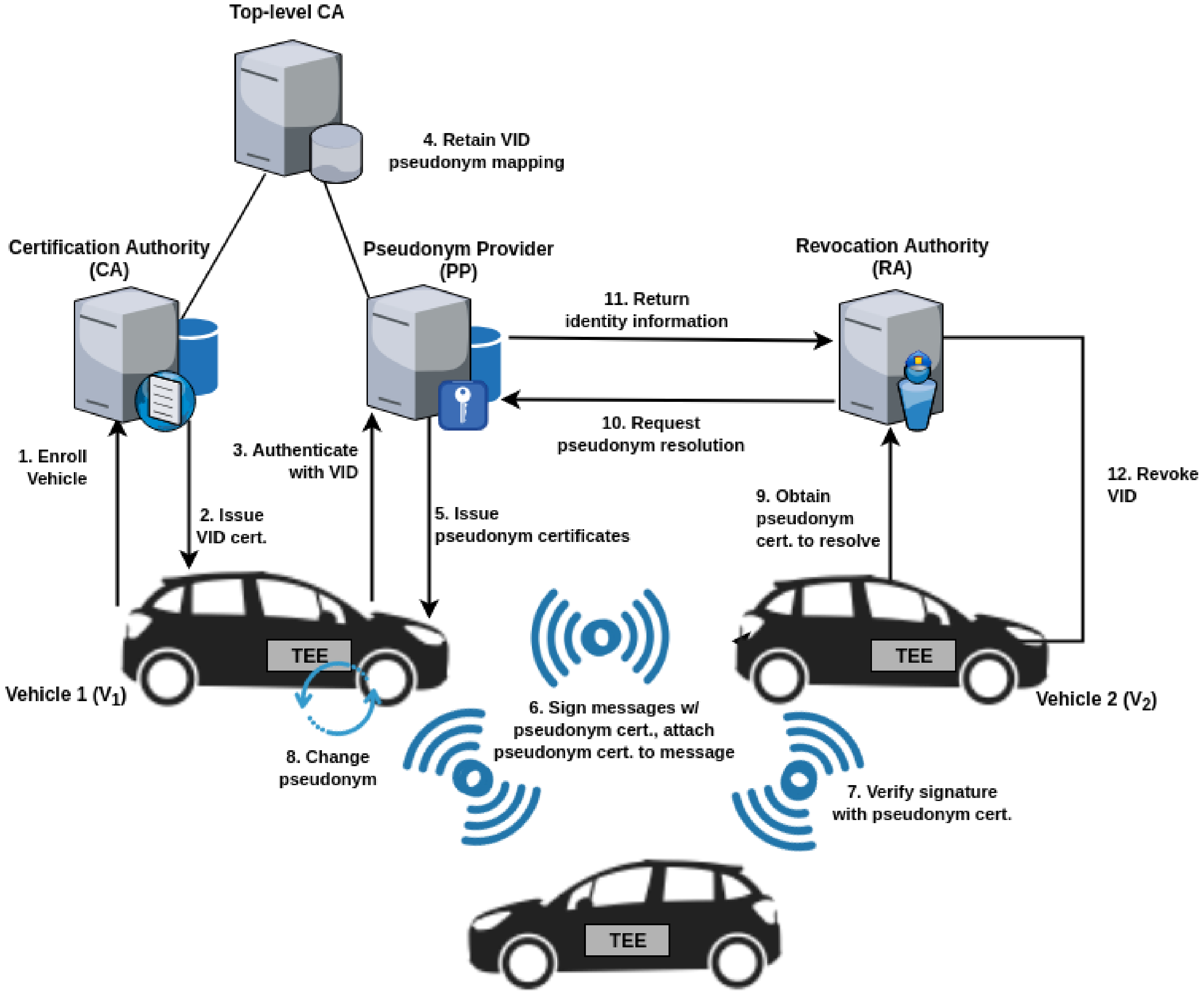
- Hardware-backed attestation using Trusted Platform Modules (TPM)

- Properties of DAA:
  - **Correctness**
    - Valid signatures only producible by honest platforms, and are verifiable and linkable where specified.
  - **User-controlled Anonymity**
    - Identity of a user cannot be revealed from signature.
  - **User-controlled Traceability**
    - Host controls whether signatures can be linked.

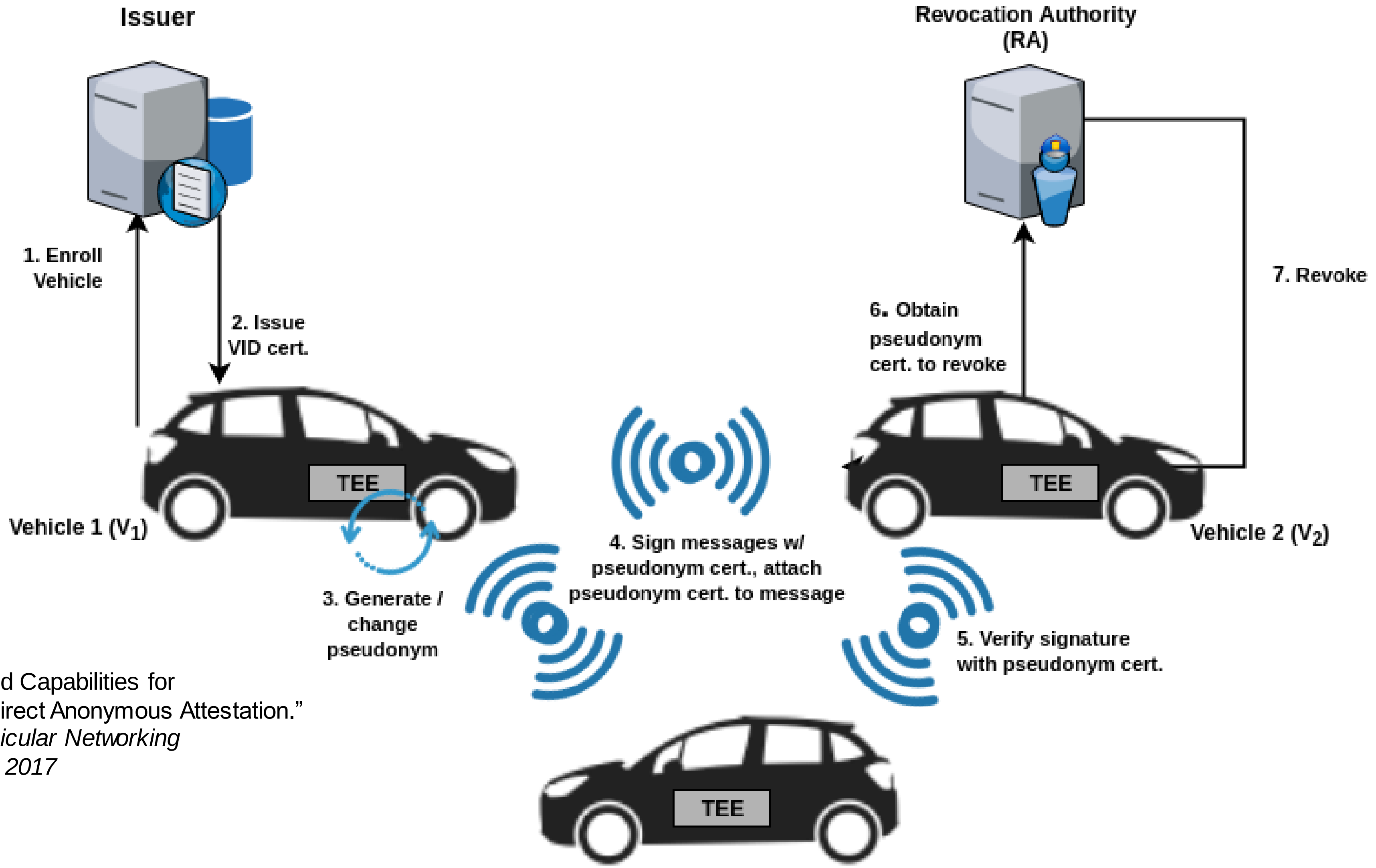
- Standardised in ISO/IEC 20008 2013



Vehicular Pseudonym System - VPKI

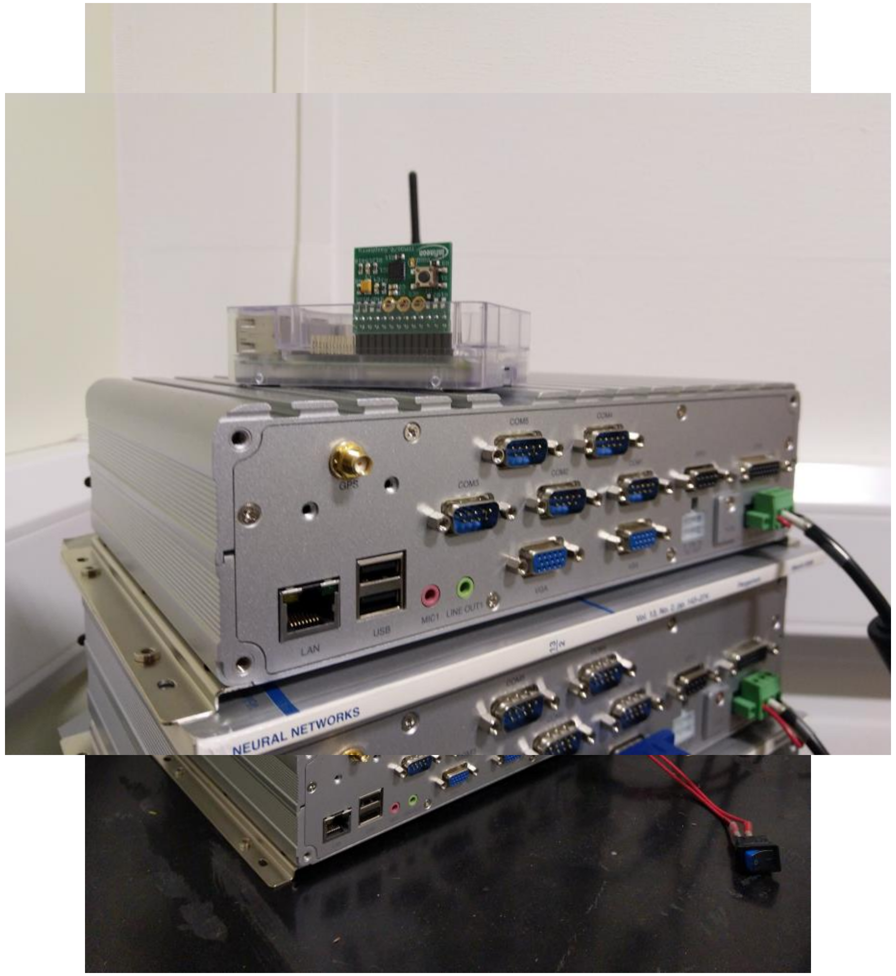

Top-level CA
4. Retain VID pseudonym mapping
Certification Authority (CA)
Pseudonym Provider (PP)
Revocation Authority (RA)
11. Return identity information
10. Request pseudonym resolution
1. Enroll Vehicle
2. Issue VID cert.
3. Authenticate with VID
5. Issue pseudonym certificates
9. Obtain pseudonym cert. to resolve
12. Revoke VID
TEE
TEE
Vehicle 1 (V_1)
Vehicle 2 (V_2)
6. Sign messages w/ pseudonym cert., attach pseudonym cert. to message
8. Change pseudonym
7. Verify signature with pseudonym cert.
TEE

Vehicular DAA Pseudonym System


Issuer
Revocation Authority (RA)
1. Enroll Vehicle
2. Issue VID cert.
6. Obtain pseudonym cert. to revoke
7. Revoke
TEE
Vehicle 1 (V_1)
TEE
Vehicle 2 (V_2)
3. Generate / change pseudonym
4. Sign messages w/ pseudonym cert., attach pseudonym cert. to message
5. Verify signature with pseudonym cert.
TEE

"Privacy-Enhanced Capabilities for VANETS Using Direct Anonymous Attestation." In *2017 IEEE Vehicular Networking Conference, VNC 2017*

EPSRC UK Funded Project



- » Demonstrate the applicability of our DAA V2X architecture

- » Project in collaboration with
  - Thales UK
  - Thales eSecurity
  - Pervasive Intelligence

- » Nexcom VTC 6200
  - Intel Atom D510 Dual Core 1.6GHz
  - 2GB RAM

Preliminary Results

» CREATE: 10 ms

» SIGN: 84 ms

» VERIFY: 510 ms

Implementation details

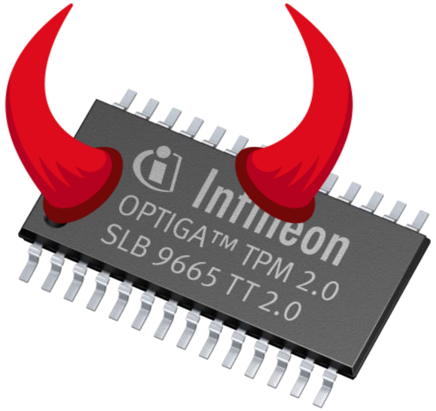
- **HOST:** Java
- **TPM:** Raspberry Pi Model B
  - Infineon development TPM
  - C with IBM TSS
- **ISSUER:** Java Spring

ETSI Standards 100 to 150 message per second

Formal Analysis Summary

Proofs and Disproofs obtained using the Tamarin Prover
https://tamarin-prover.github.io/

Found an attack when the integrity of one TPM is compromised, the security of all TPMs cannot be guaranteed.



UNIVERSITY OF SURREY

@sudo_jorden

jwhitefield.co.uk