Formal Analysis of V2X Revocation Protocols

Jorden Whitefield, Liqun Chen, Frank Kargl, Andrew Paverd, Steve Schneider, *Helen Treharne* and Stephan Wesemeyer

University of Surrey, UK

Ulm University, Germany

Aalto University, Finland

STM 2017, Oslo, Norway

Outline

- Security challenges of Intelligent Transportation Systems
- Revocation in Vehicle-to-Anything (V2X) communication
- Formal Verification of REWIRE Protocols: PLAIN and R-TOKEN
- O-TOKEN: Addressing the issues found

Intelligent Transport Systems (ITS)

What are they?

ITS's are the combination of transport and ICT Systems to enable safer, coordinated, environmentally friendly, and smarter transportation networks.

ITS's use Pseudonyms (short-lived certificates) for authenticated message exchange. Pseudonyms change frequently to protect privacy of vehicles.

Standards

- ISO15408-2
- ETSI 102-941 and;
- IEEE WAVE

Overview of V2X Security

UNIVERSITY OF SURREY

Trust
Architecture
Attestation
Assurance

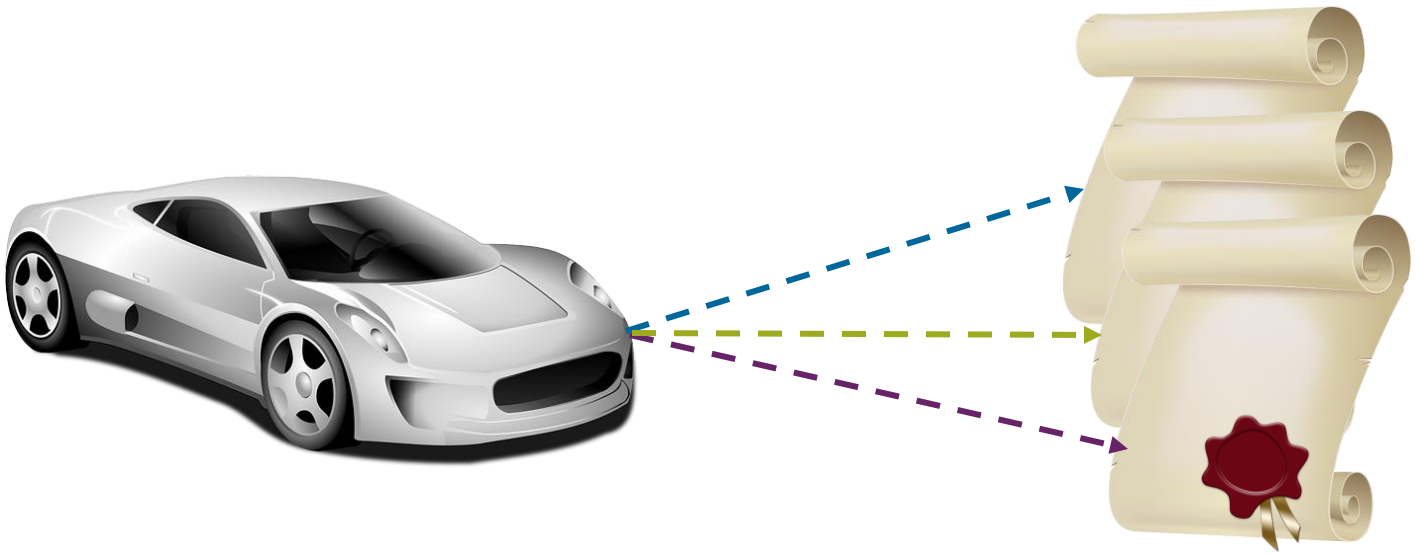
Privacy
Anonymity
Pseudonymity
Unlinkability
Unobservability

Authentication
Authorisation
Revocation

Software
Safety / Run time
Verification
Assurance

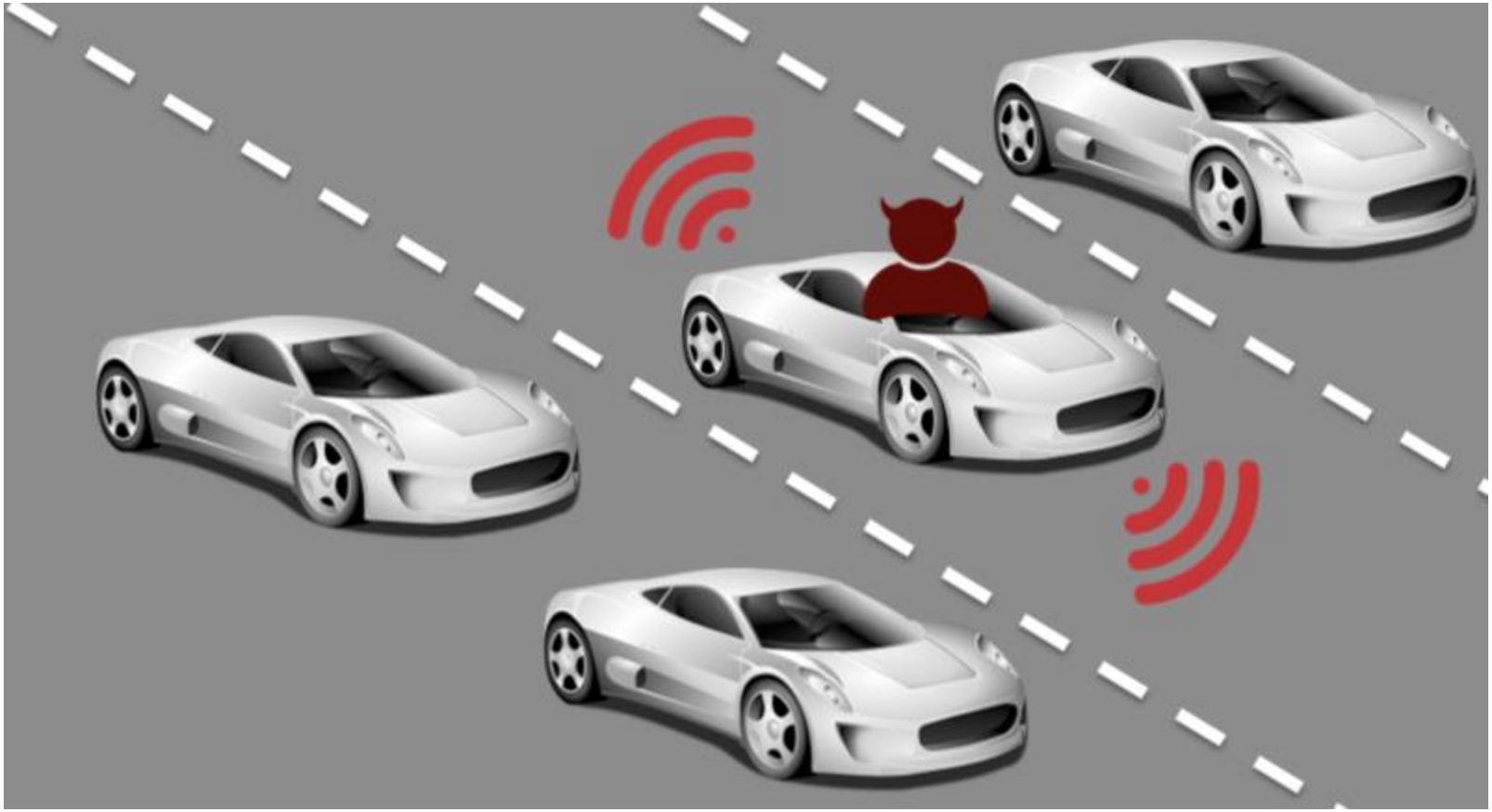
Pseudonyms in V2X

Pseudonyms can enable:



- Anonymity
- Pseudonymity
- Unlinkability
- Unobserveability

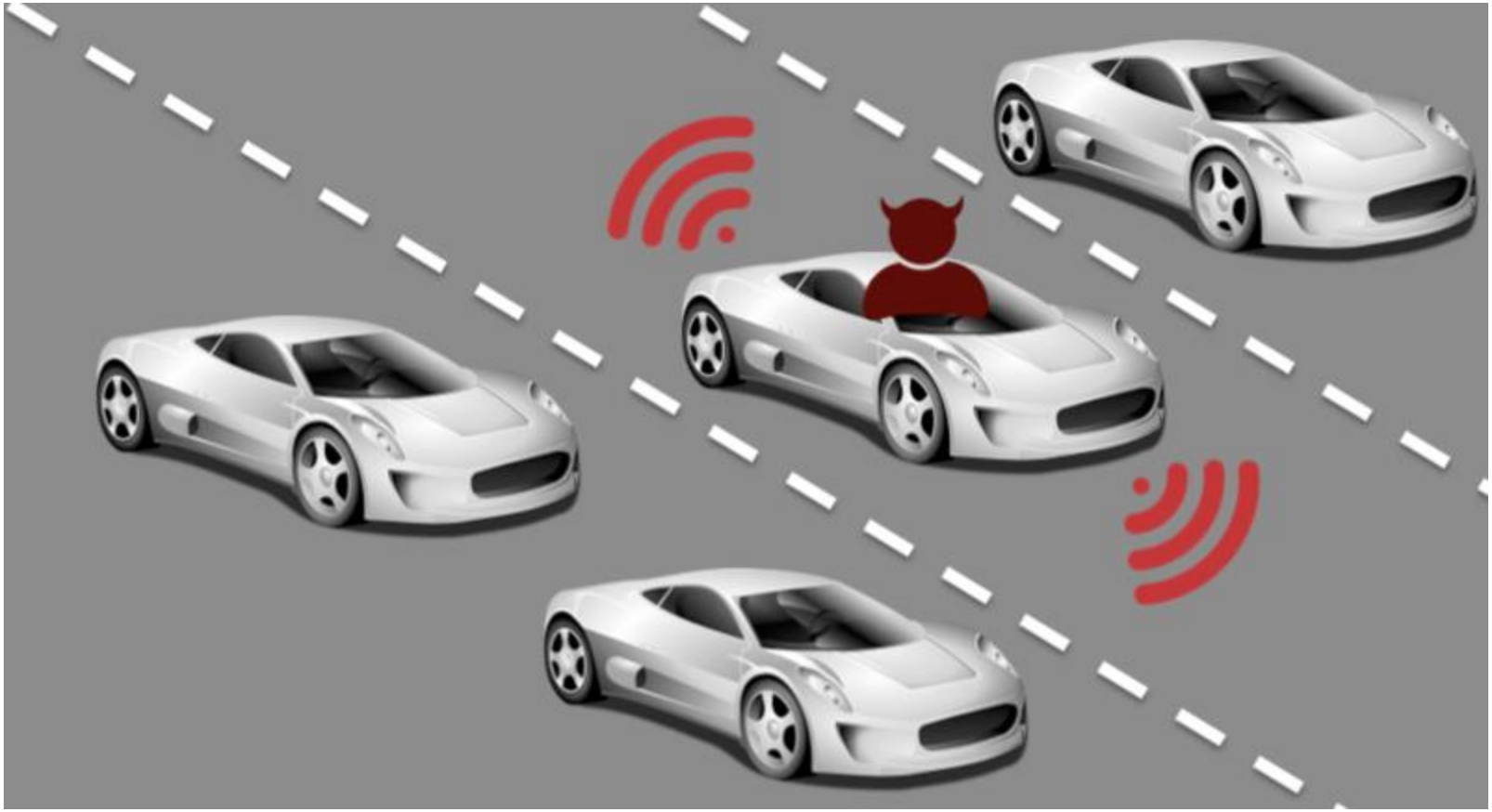
How do you remove a rogue vehicle?



1. Using Pseudonym Certificate Revocation Lists (does not scale)

2. Prevent vehicle from broadcasting network messages, by deleting its issued pseudonyms

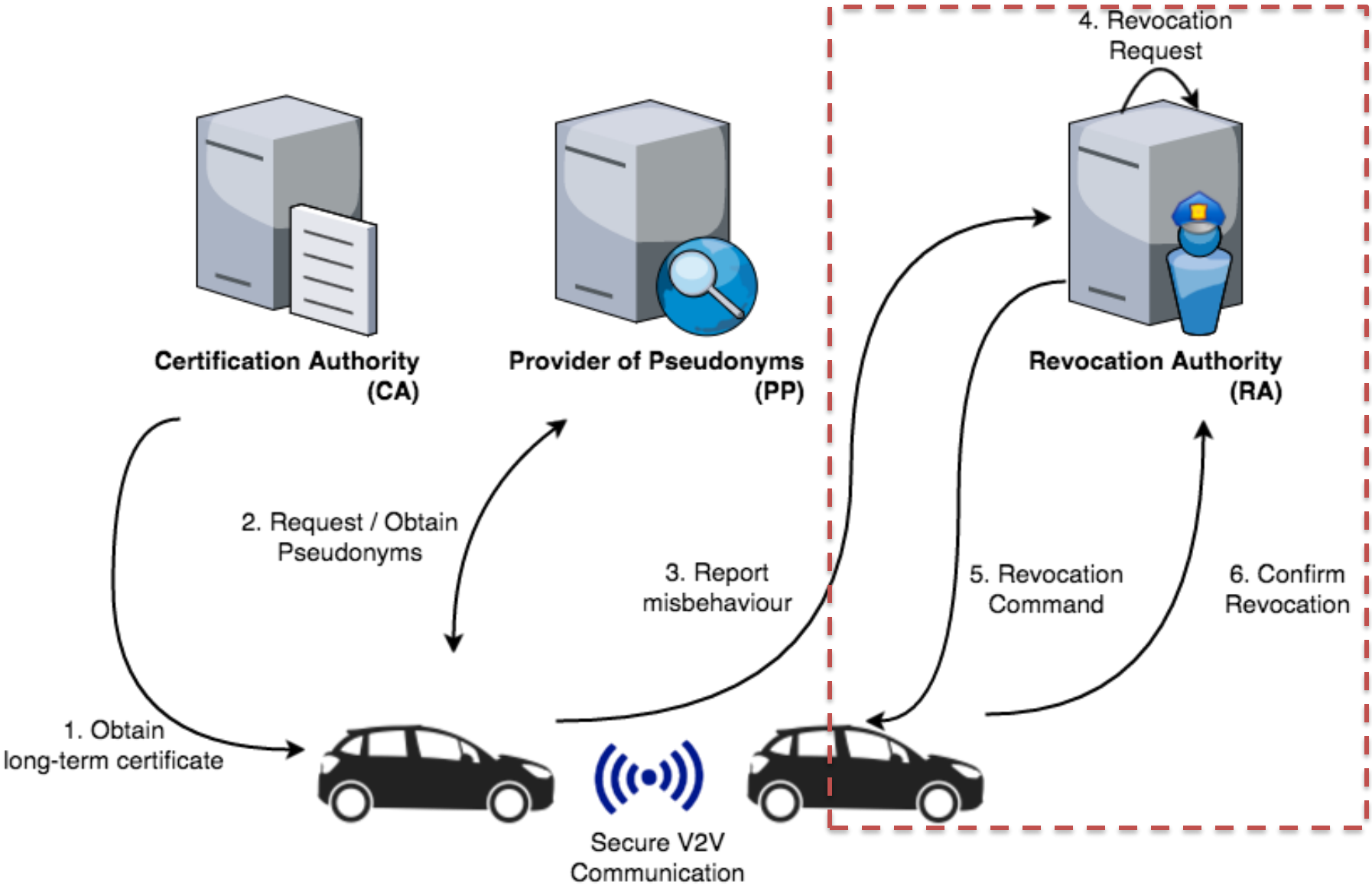
How do you remove a rogue vehicle?



1. Using Pseudonym Certificate Revocation Lists (does not scale)

2. Prevent vehicle from broadcasting network messages, by deleting its issued pseudonyms

Pseudonym Lifecycle



Existing REWIRE Protocols

By D. Förster, H. Löhr, J. Zibuschka, F. Kargl at TRUST 2015

- Use of Trusted Components (TC) to support revocation
- TC = no Certificate Revocation Lists
- Two schemes identified in paper
  - PLAIN: Uses pseudonyms to sign "confirm revocation" messages
  - R-TOKEN: Link token scheme. Uses Long-term key pair for "confirm revocation" message signing

Formal Analysis of REWIRE Protocols

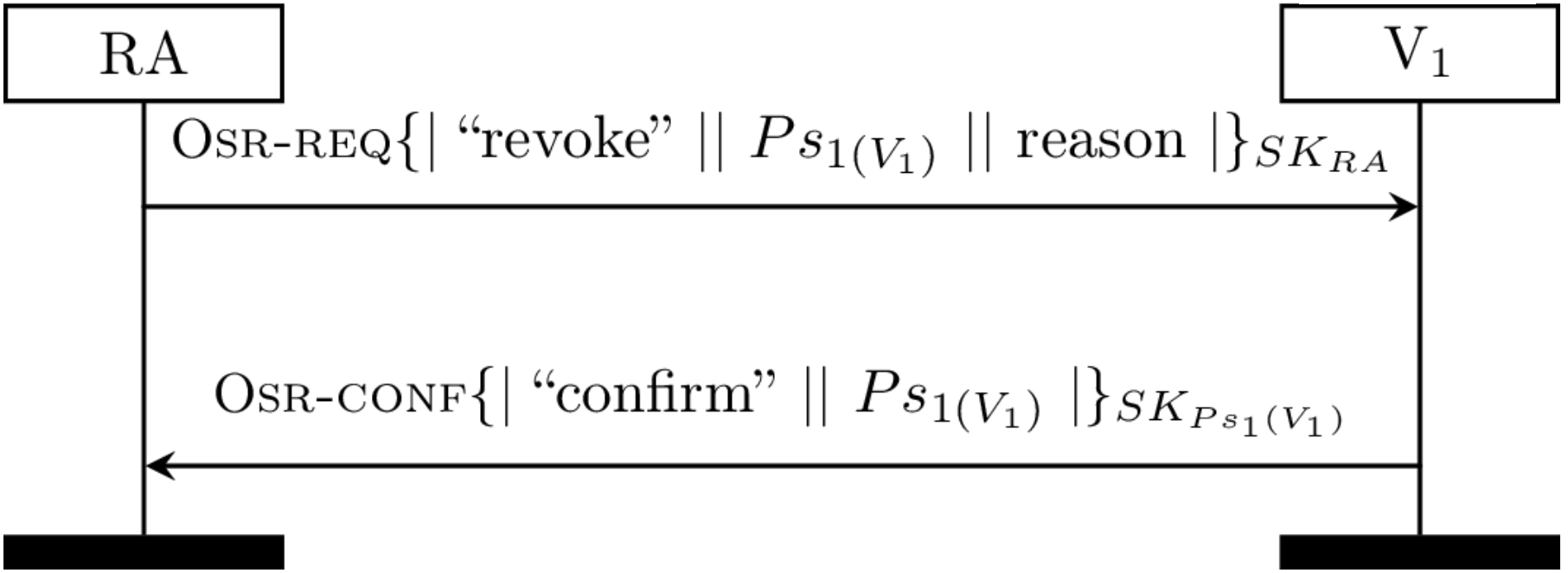
UNIVERSITY OF SURREY

- **Goals**
  - ***Authentication***: Completion of the protocol confirms the intended vehicle has been revoked
  - ***Functional Correctness***: revocation happens even in presence of a change of pseudonym
- Analysis performed using the TAMARIN Prover
  - Symbolic protocol analysis
  - Behavior defined as Multiset Rewrite rules
  - Properties expressed on traces using logic

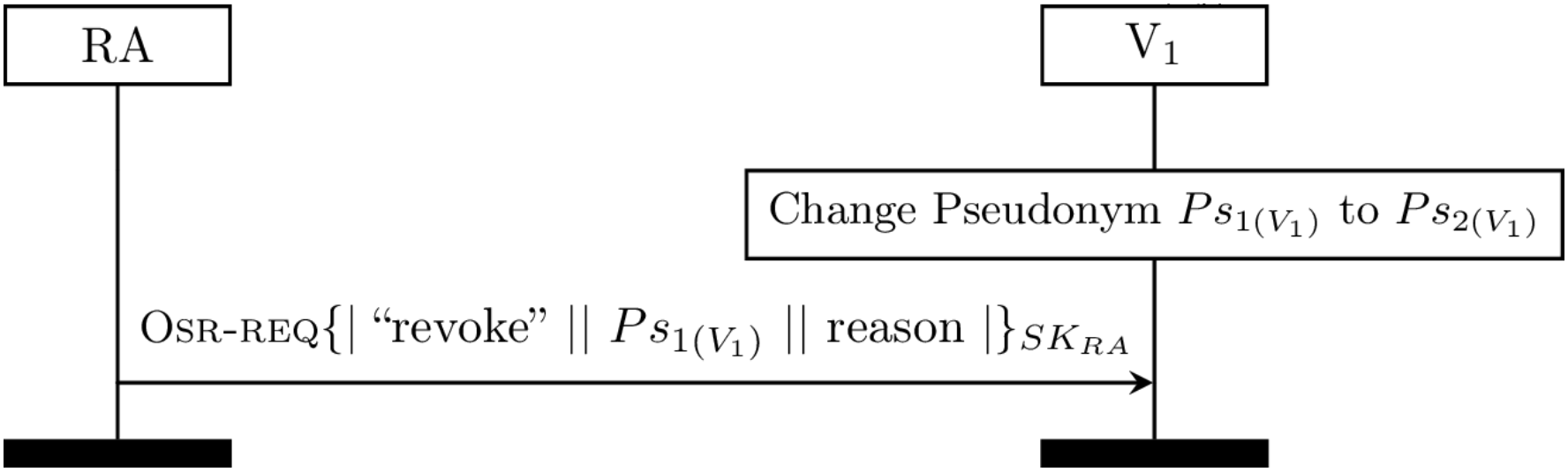
Summary of Results

- PLAIN: is not functionally correct
  - Revocation can only occur when there is no change of pseudonym
- R-TOKEN: has an authentication flaw
  - Revocation confirmation cannot be verified by the RA
- O-TOKEN:
  - Improvement to the REWIRE protocols that ensures correct revocation

PLAIN


RA
V1
OSR-REQ{| "revoke" || Ps1(V1) || reason |}SKRA
OSR-CONF{| "confirm" || Ps1(V1) |}SKPs1(V1)

PLAIN


RA
V1
Change Pseudonym $Ps_{1(V_1)}$ to $Ps_{2(V_1)}$
OSR-REQ{| "revoke" || $Ps_{1(V_1)}$ || reason |}$_{SK_{RA}}$

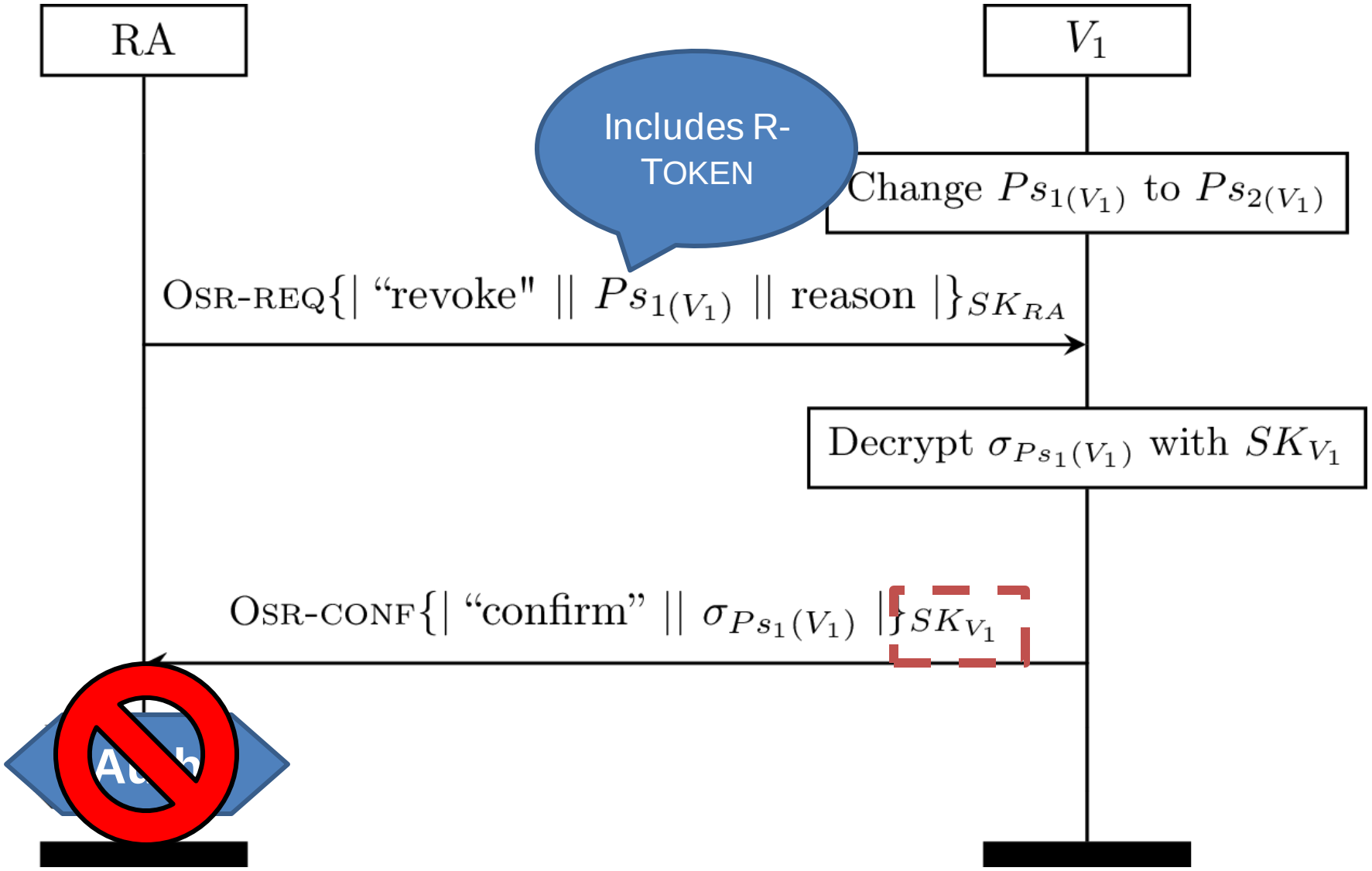
R-TOKEN

- Creates pseudo-linkability between pseudonyms
- Vehicles in this scheme have long term key-pair PK_{Vj} / SK_{Vj}
- Introduces extra field 'R-TOKEN' in pseudonyms

$$\sigma_{Ps_i(V_j)} := \{| V_j \,||\, PK_{V_j} \,||\, r \,|\}_{SK_{V_j}}$$

- Pseudonym now consists of a key-pair and R-TOKEN.

R-TOKEN


RA
V_1
Includes R-TOKEN
Change $Ps_{1(V_1)}$ to $Ps_{2(V_1)}$
OSR-REQ{| "revoke" || $Ps_{1(V_1)}$ || reason |}SK_{RA}
Decrypt $\sigma_{Ps_1(V_1)}$ with SK_{V_1}
OSR-CONF{| "confirm" || $\sigma_{Ps_1(V_1)}$ |}SK_{V_1}

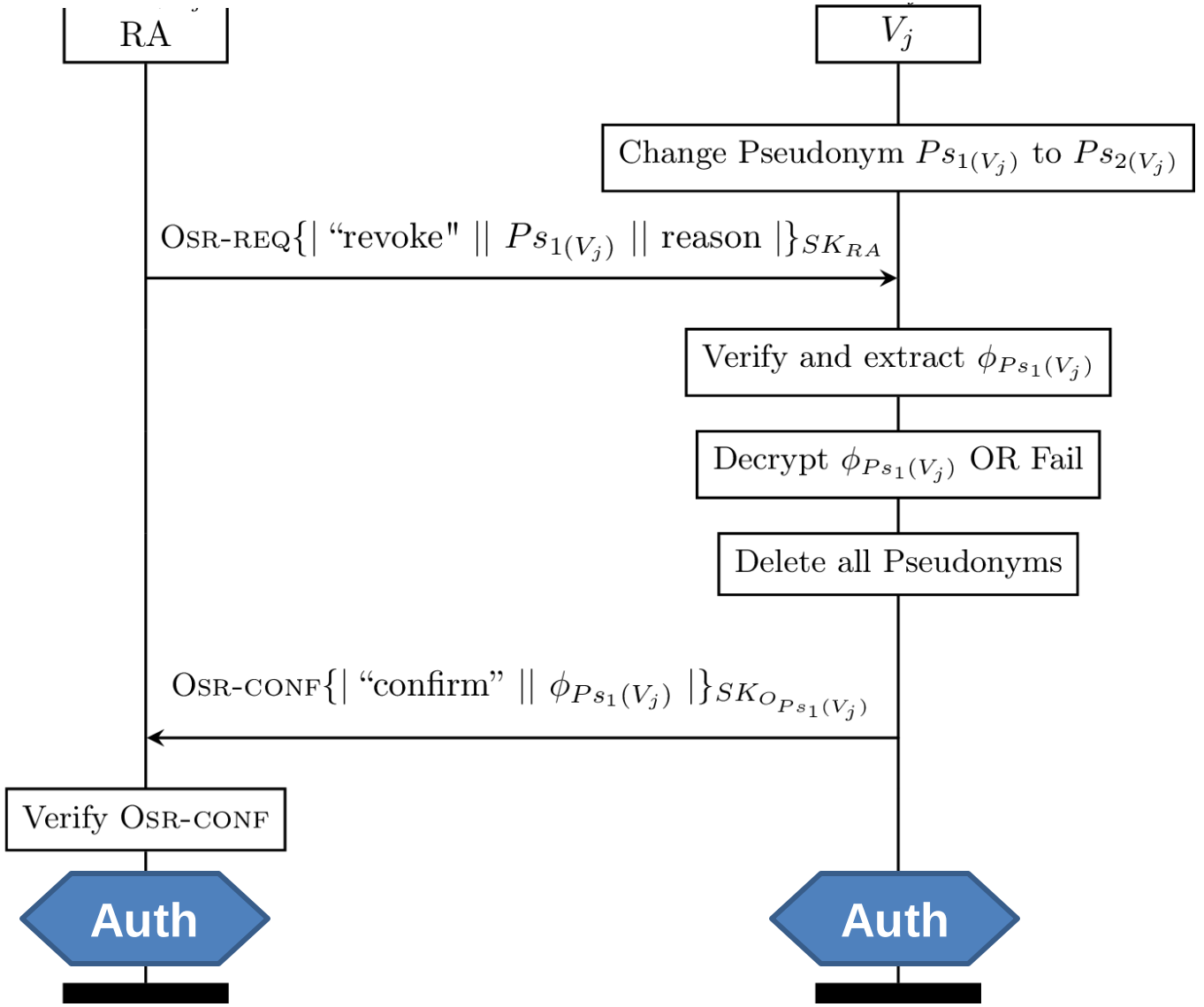
OBSCURE-TOKEN (O-TOKEN)

- New key-pair "O keys" SKO / PKO
- O-TOKEN is an encryption of SKO under vehicle long-term symmetric key:

$$\phi_{Ps_i(V_j)} := \{| SK_{O_{Ps_i(V_j)}} |\}_{LTK_{V_j}}$$

- Pseudonyms contain O-TOKEN and PKO

O-TOKEN


RA
V_j
Change Pseudonym $Ps_{1(V_j)}$ to $Ps_{2(V_j)}$
OSR-REQ{| "revoke" || $Ps_{1(V_j)}$ || reason |}$_{SK_{RA}}$
Verify and extract $\phi_{Ps_1(V_j)}$
Decrypt $\phi_{Ps_1(V_j)}$ OR Fail
Delete all Pseudonyms
OSR-CONF{| "confirm" || $\phi_{Ps_1(V_j)}$ |}$_{SK_{O_{Ps_1(V_j)}}}$
Verify OSR-CONF
Auth
Auth

Future research directions

UNIVERSITY OF SURREY

Finer grained model capture privacy

Use DAA to explore alternate architectures