Formal Verification of a V2X Privacy-Preserving Scheme using Proverif

Simone Bussa, Riccardo Sisto, Fulvio Valenza
DAUIN, Politecnico di Torino

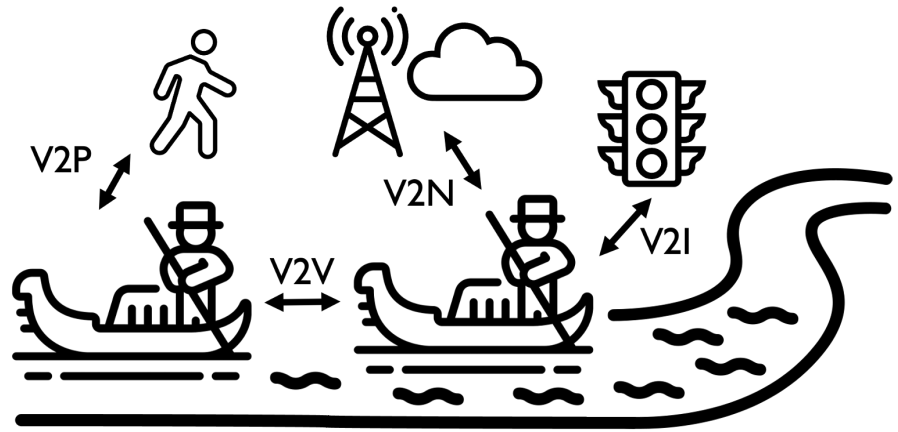
{first}.{last}@polito.it

netgroup

1859

V2X Introduction

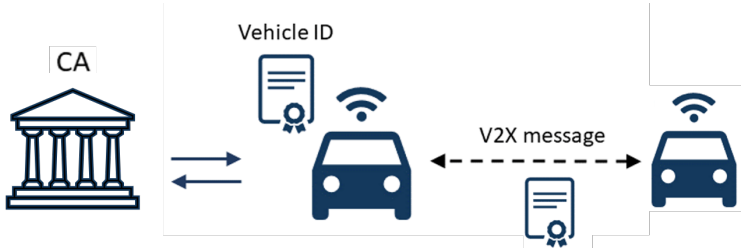
- **V2X** – Vehicle to Everything
- **Broadcast messages** sent to surrounding neighbours
- … vehicle **speed, position, direction** …
- Applications = Road safety and Traffic flow optimization
- Being sensitive, a compromise of this data can impact the **safety** of involved actors
- Mechanisms are needed to protect it



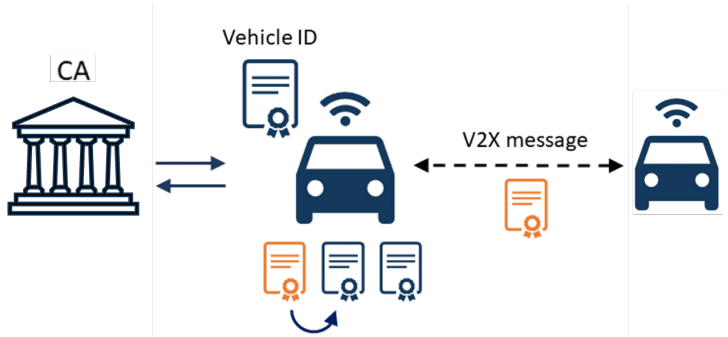
In particular, message authentication and integrity

V2X Privacy Issues

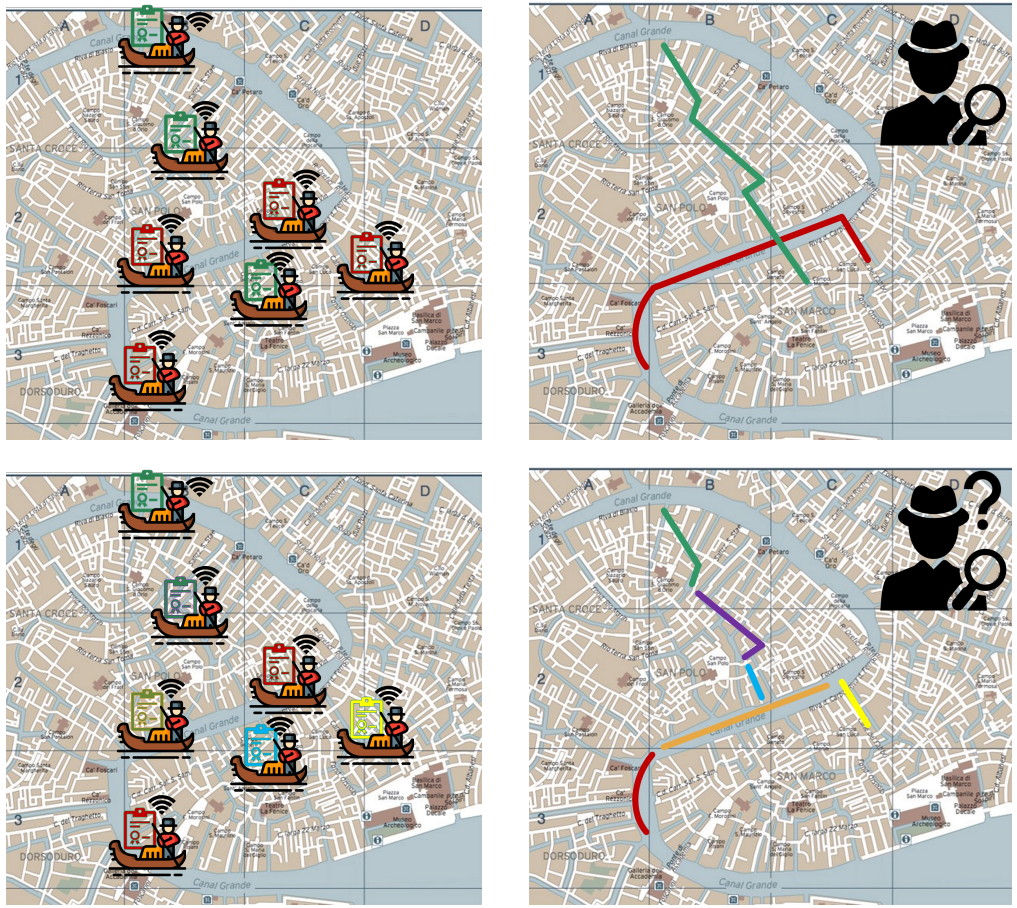
- Traditional network protocols use **Digital signatures** and **certificates**



- **Privacy** issues! Easy to **track** vehicle position
- **Anonymity** is needed



- Solution with **Pseudonymous certificates**
- Still some **problems**: Refill problem, Pseudonyms revocation …



Formal Verification gap and Objective of the work

- Many **v2x schemes** have been proposed over the years
- Also, many definitions of **properties** that these schemes must satisfy

To our knowledge, a formal analysis of the security of these schemes is missing

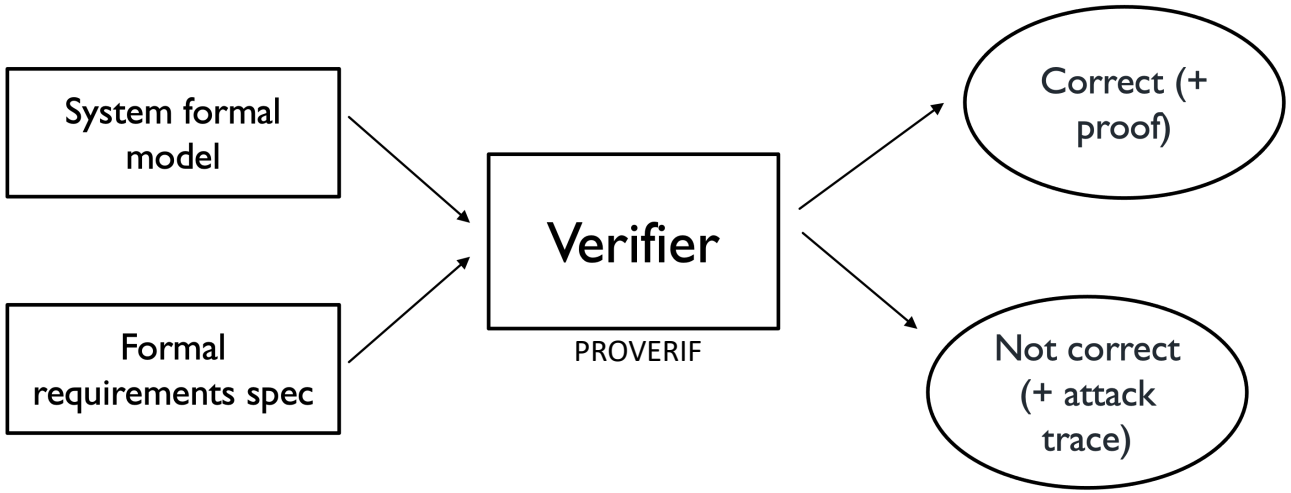
- **Objective** of the work:
  - Consider **one** of the proposed schemes existing in the literature
  - **Complete** the scheme to get a **formal specification** of the protocol
  - **Formally** define the security/privacy **properties** it must enforce
  - Run the **formal verification** using **Proverif**

The verification revealed some issues. Some of them are well-known in the literature and common to other schemes; other specific to the modeled protocol.

Formal Verification

- Static **analysis** of a system **formal model**

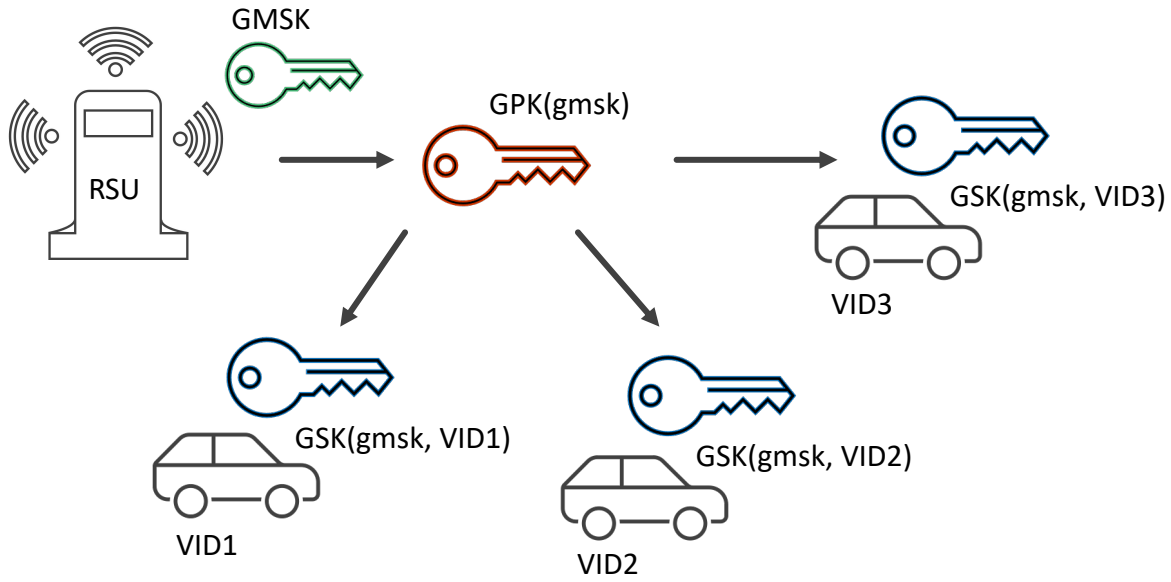
1. **Formal Specification**: from the real system to its formal abstract model
2. **Formal Verification**: check if the model satisfies some formal properties (e.g., its security requirements)



- Why formal verification?
- Designing security protocols is error prone
- Several flaws are constantly being found
- Formal verification today is required to submit most protocols
- Formal methods **increase the confidence** in the security by giving high assurance

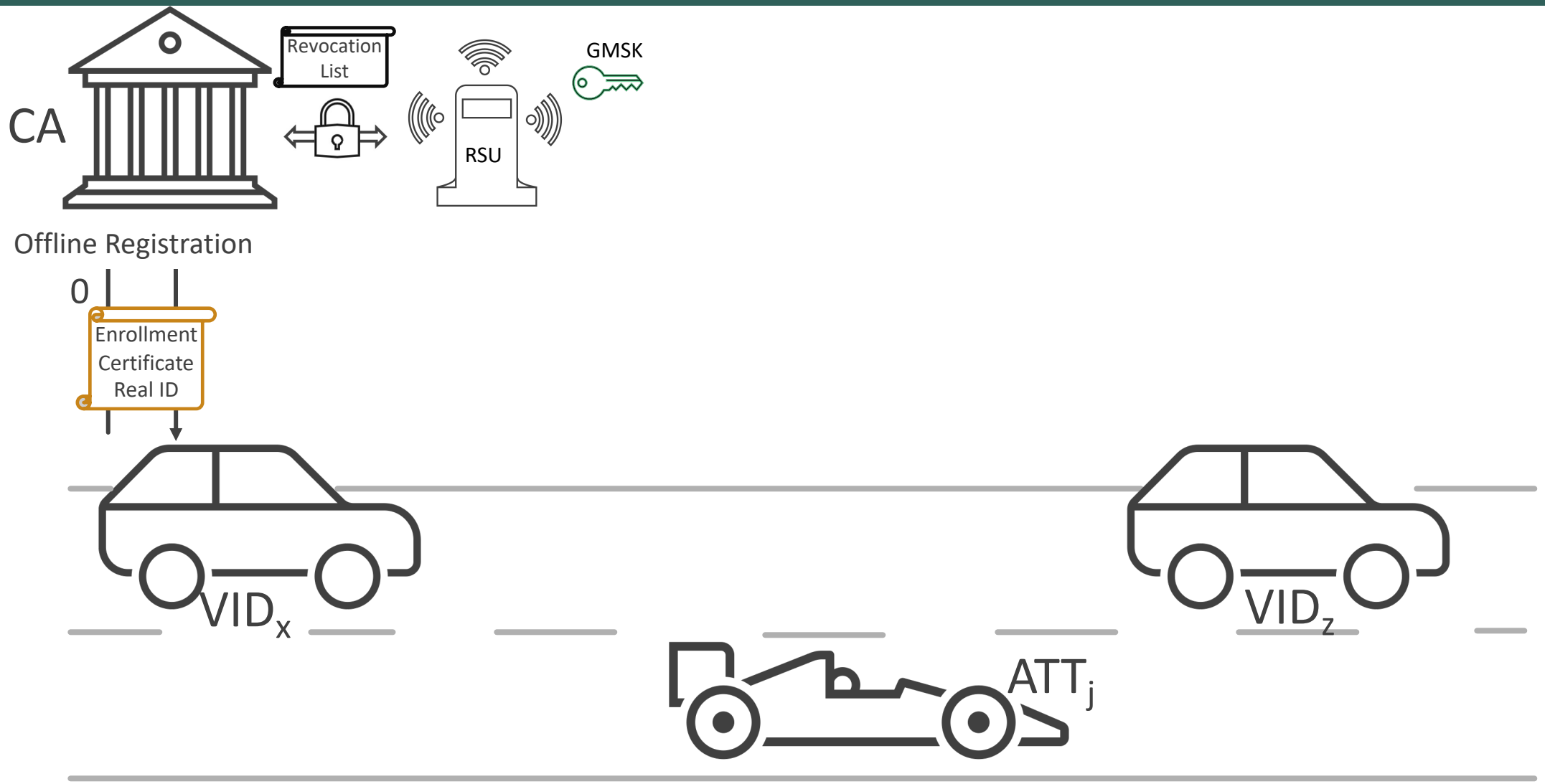
The Verified Scheme

- "Efficient and robust pseudonymous authentication in vanet" (reference paper)
- **Pseudonymous certificates** (Asymmetric encryption and Digital signatures)
- Pseudonyms are **generated** and **self-certified** by each vehicle using **group signatures**
  - Avoid the refill problem !
  - Groups are managed by a **RSU** (group master)

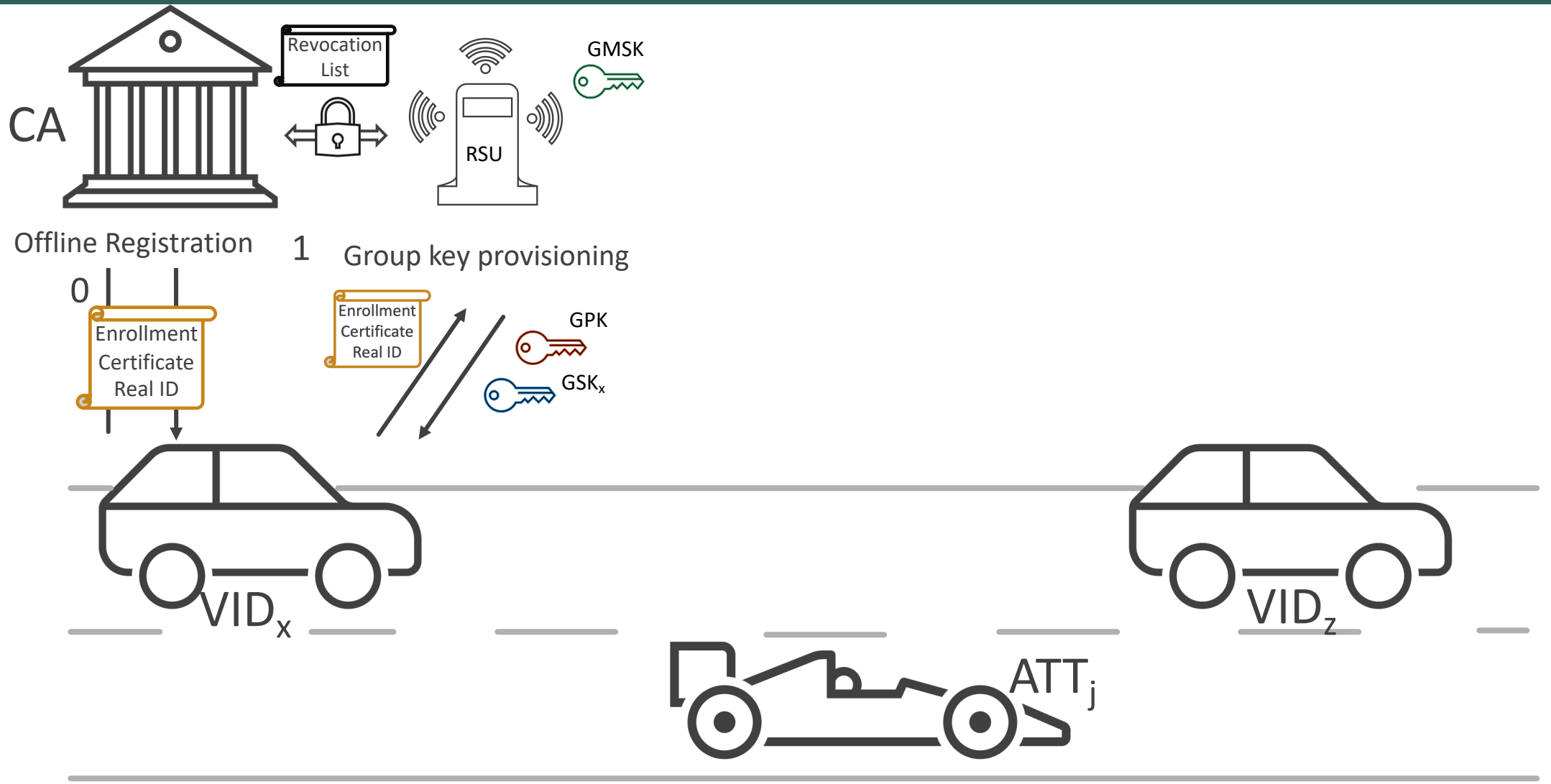


- Group signature properties
- A single signature is anonymous within the group (**anonymity**)
- Multiple signatures cannot be linked (**unlinkability**)
- Only the group master can reveal the group private key that performed a signature (**conditional accountability**)
- Unfortunately, complex and expensive operations

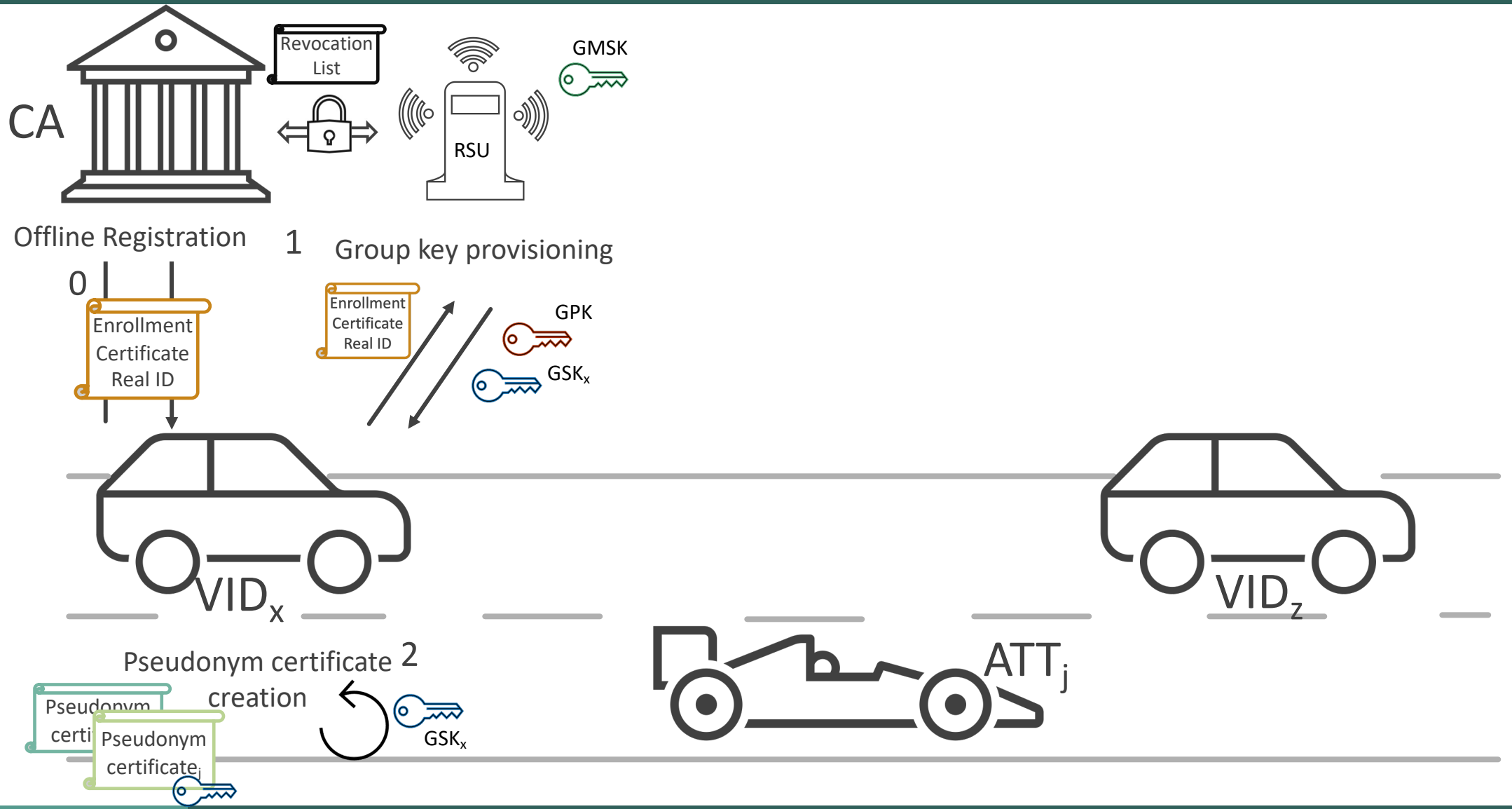
The Verified Scheme (in more details)



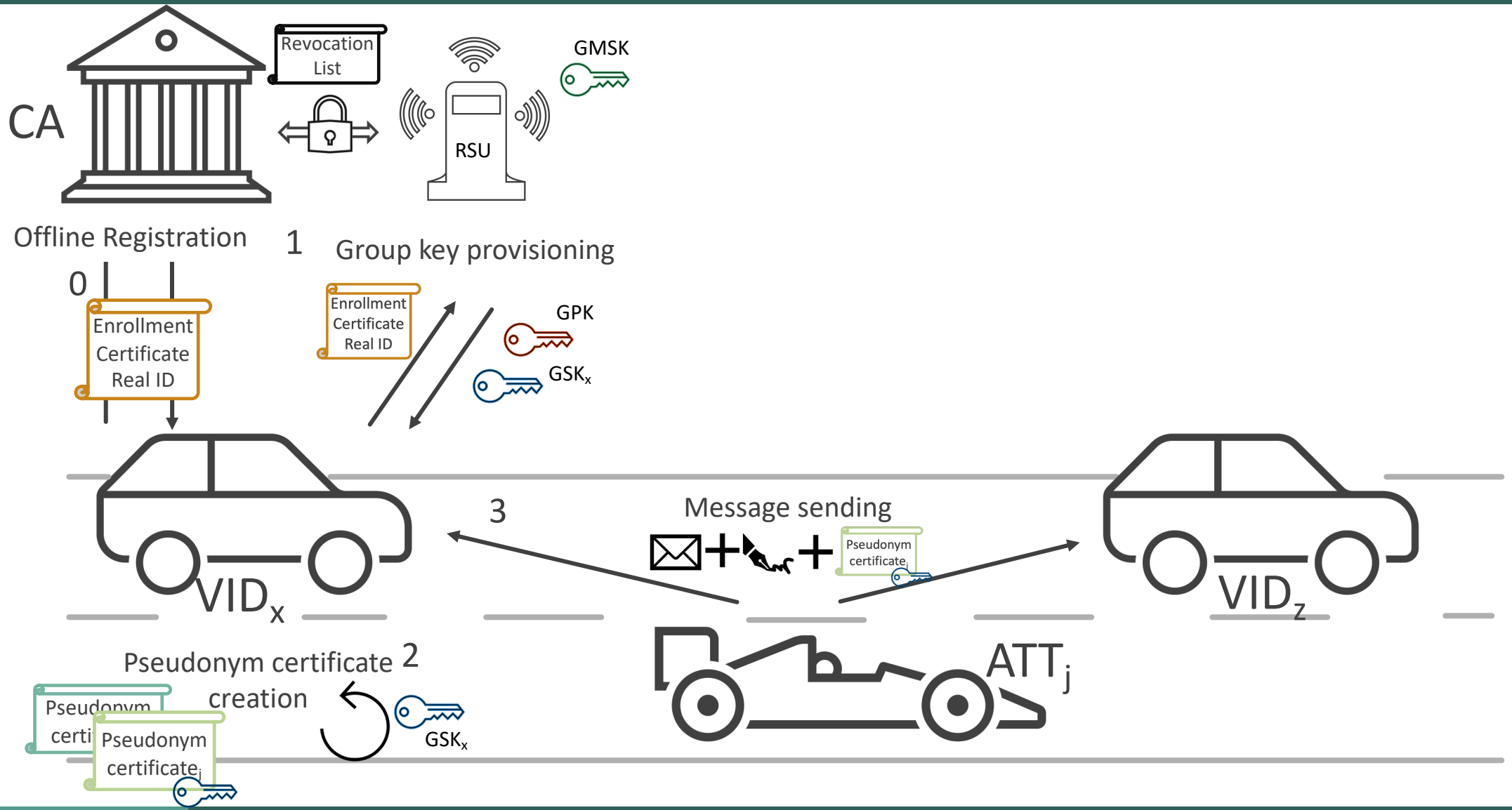
The Verified Scheme (in more details)



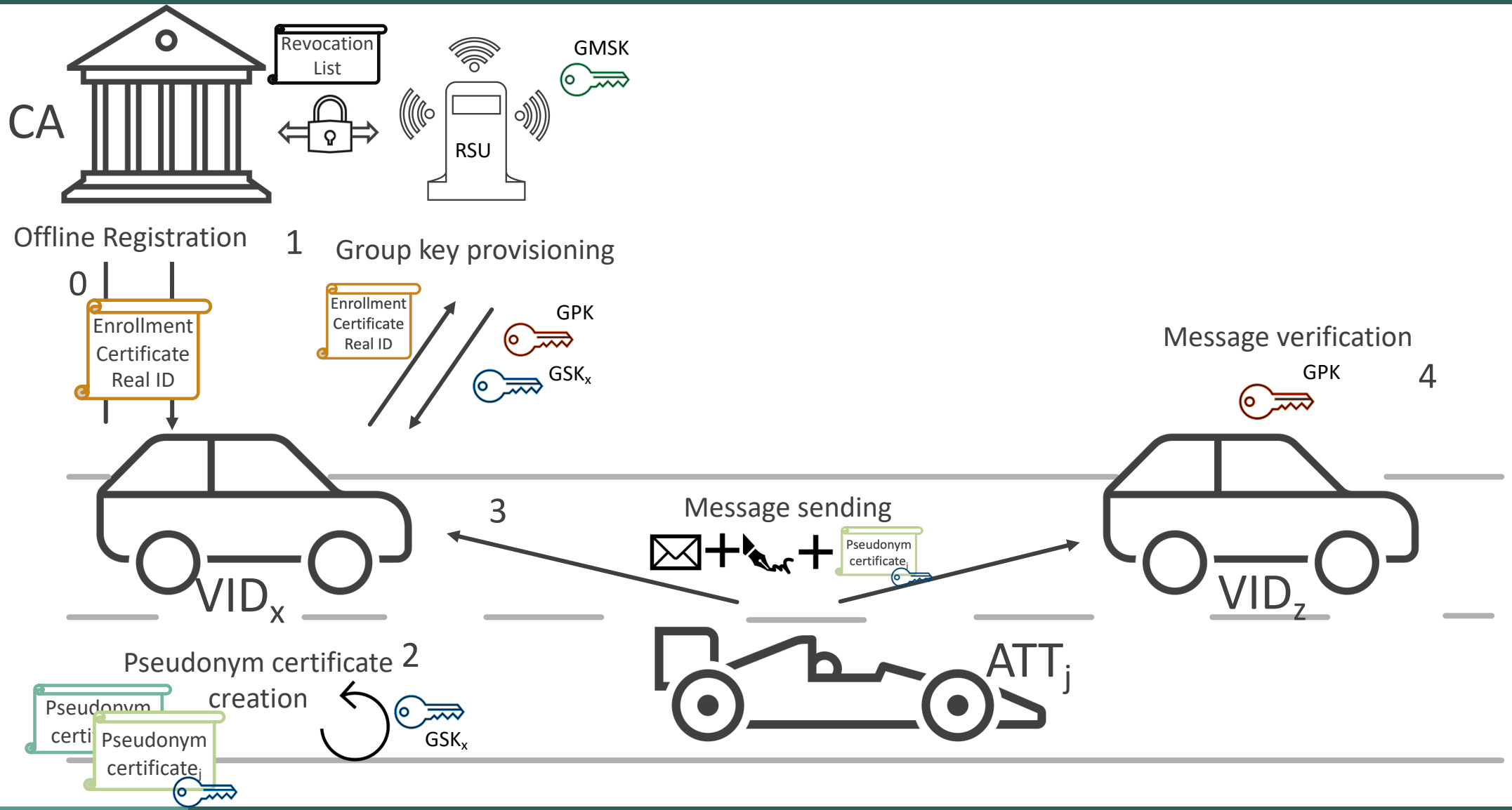
The Verified Scheme (in more details)



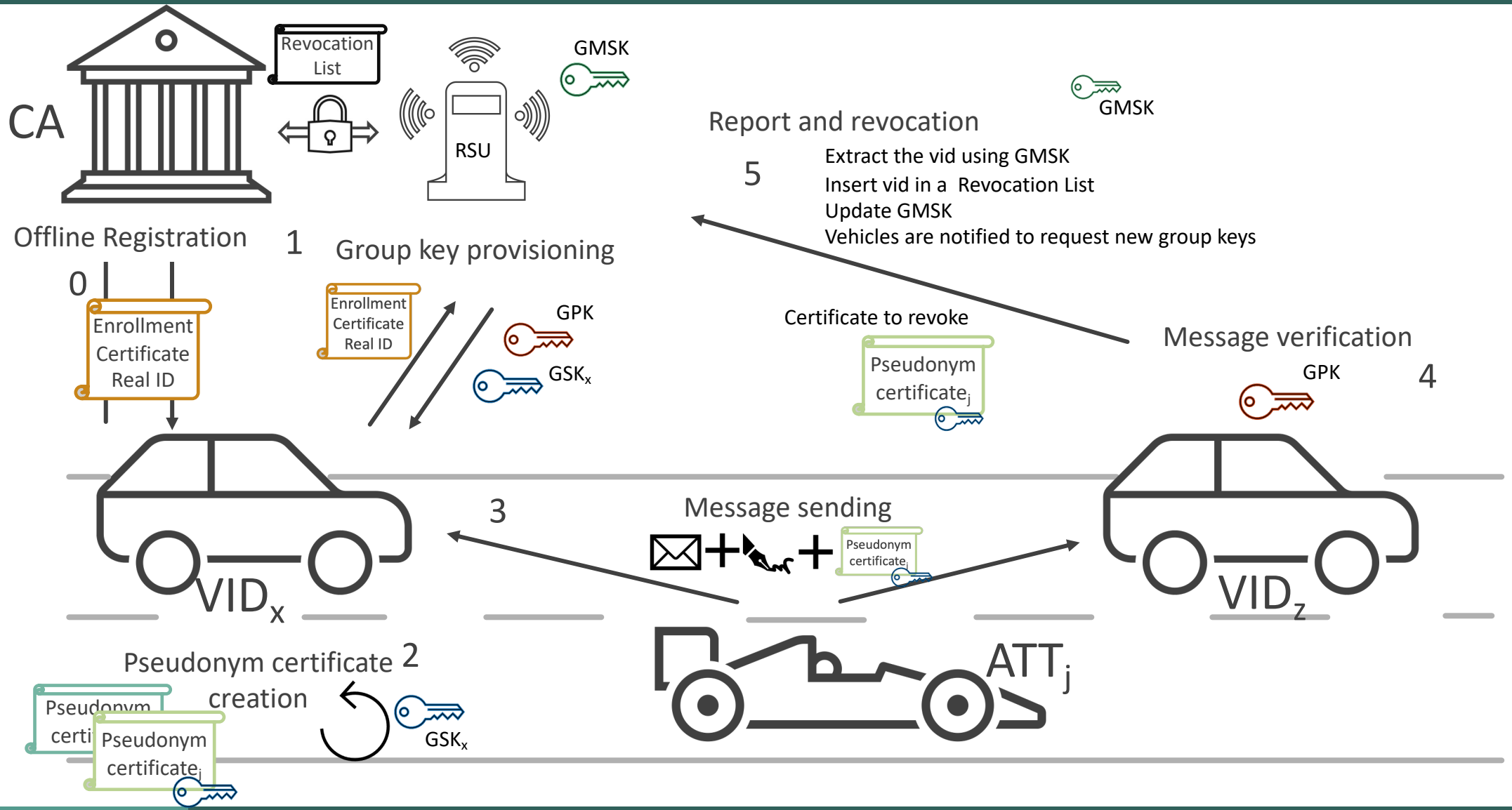
The Verified Scheme (in more details)



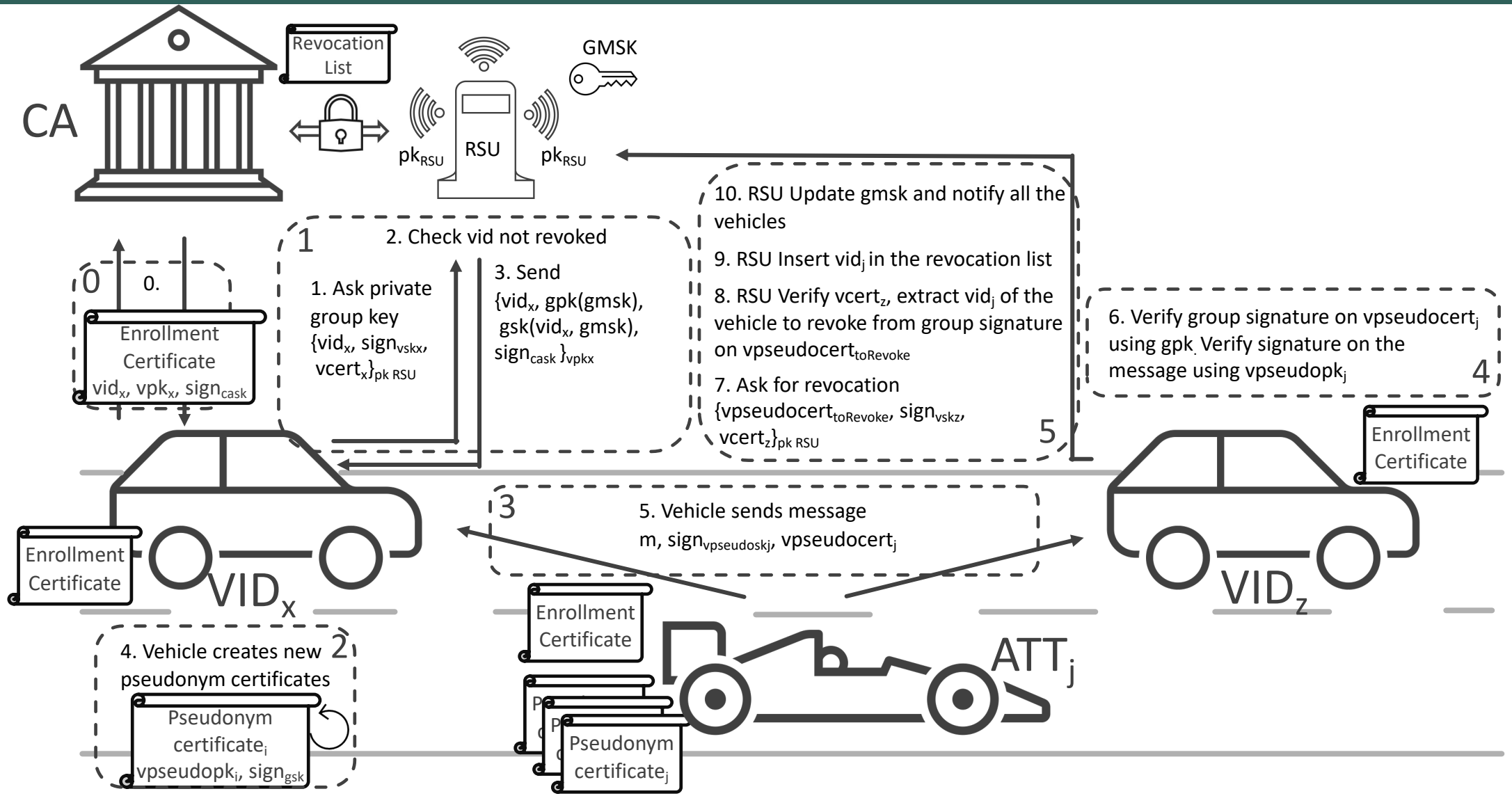
The Verified Scheme (in more details)



The Verified Scheme (in more details)

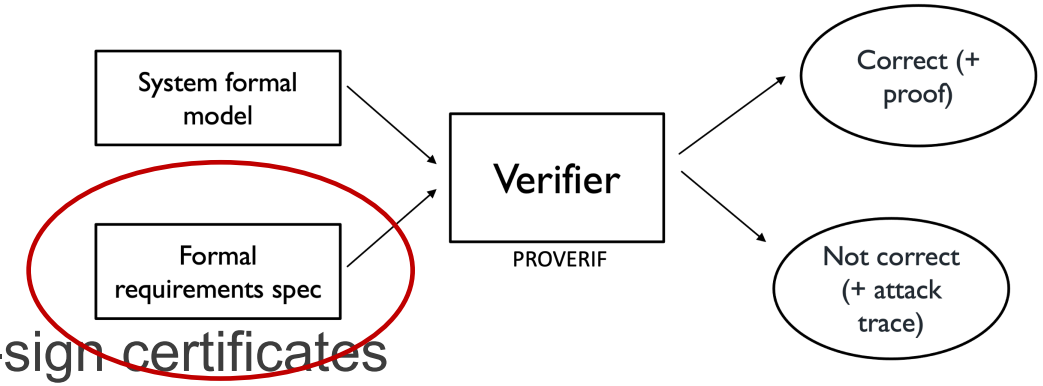


The Verified Scheme (in more and more details)



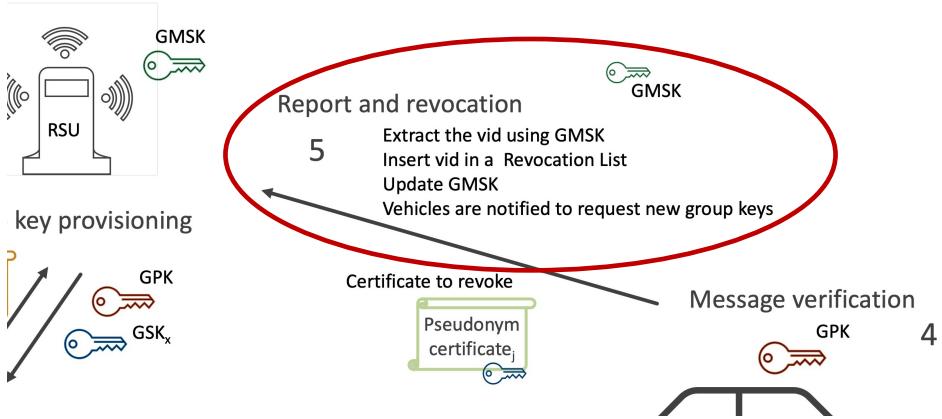
The Verified Properties

- **Confidentiality**
  - Of vehicle real identity and private keys
- **Anonymity**
  - When the vehicle uses group private keys to self-sign certificates and when it signs messages using pseudonymous certificates
- **Unlinkability**
  - In the use of different pseudo certificates to sign different messages and in the use of a single group key to certify multiple certificates



Verification results (i)

- **RESULT 1**: *Vehicle continues to be considered valid even after being removed*
  - After the RSU has added the revoked vid to the RL
    but before it updates the GMSK
  - OR after the RSU has updated the GMSK
    but before vehicles request new group keys



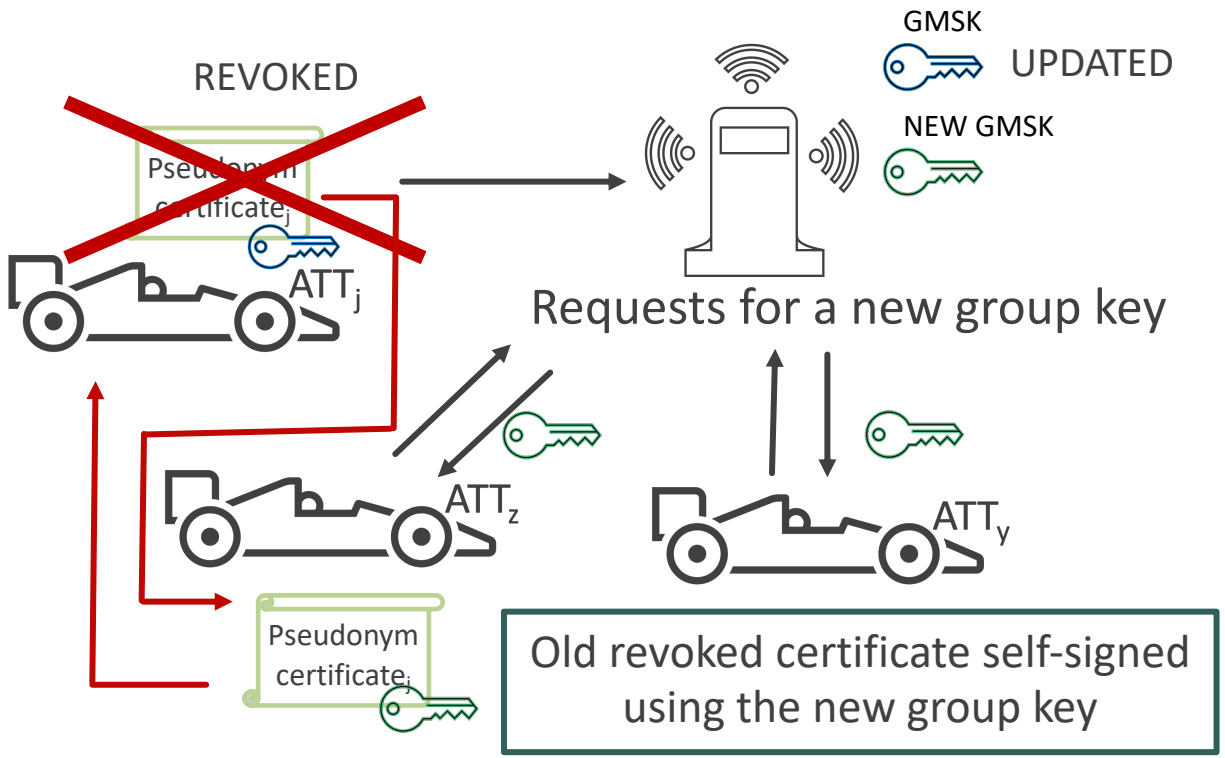
  - An attacker in this period can continue to use its old group key and vehicles would continue to accept it as a valid vehicle

Well-known Window of Exposure problem, common to other schemes

  - Adopted solutions: Group keys with short life (drawback of requiring more key updates and interactions with the RSU)

Verification results (ii)

- **RESULT 2**: *Pseudonymous certificate continues to be used even after the vehicle has been revoked*
  - When there are multiple attacker vehicles



- This process can continue as long as there are ”valid” attackers within the group
- Once all attackers are revoked one by one, the process ends
- No one can request and obtain updated group keys

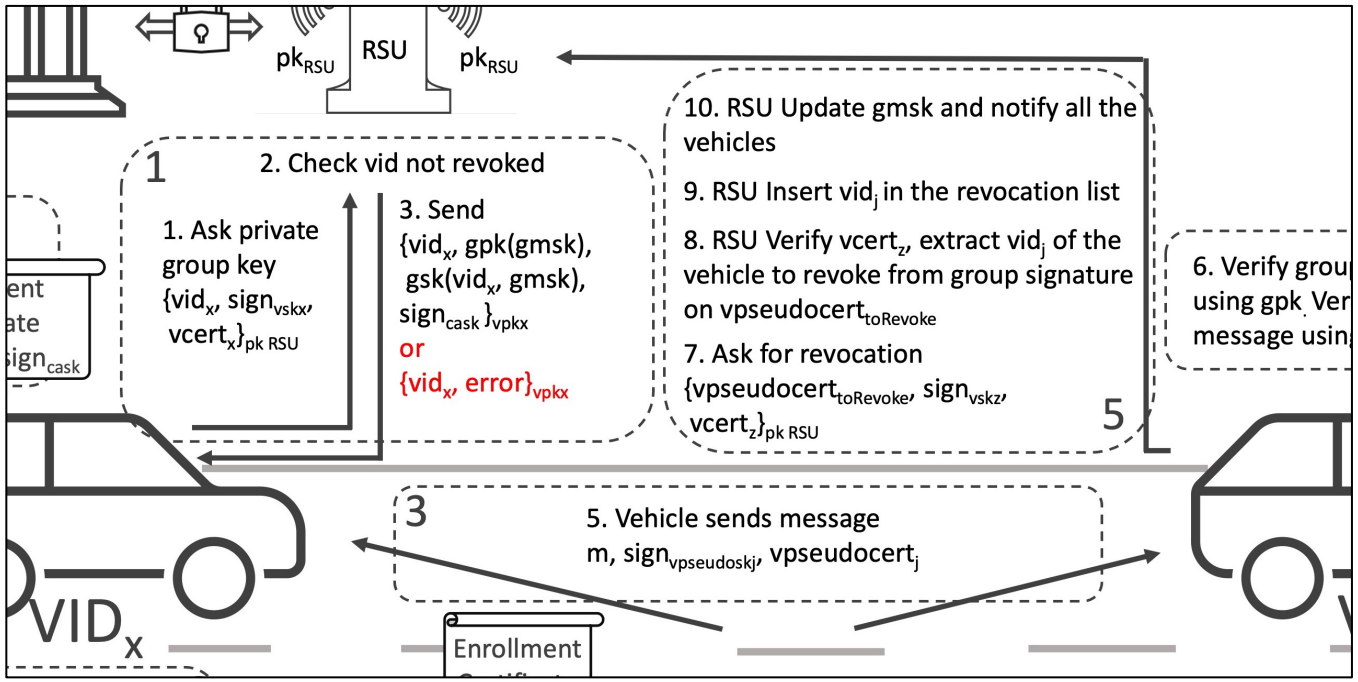
Verification results (iii)

- **RESULT 3**: *Anonymity issue in the revocation phase*
  - If the RSU receives a group key request from a revoked vehicle
  - It “should” reply with an error message and not simply ignore the request
  - ATTACK TRACE
    - Attacker intercepts and stores an initial request sent by a vehicle
    - Then, the vehicle is revoked
    - RSU notifies all vehicles to update their keys
    - By replying the initial request, attacker can understand if the revoked vehicle is the one it intercepted at the beginning

      based on whether it can get a response from the RSU

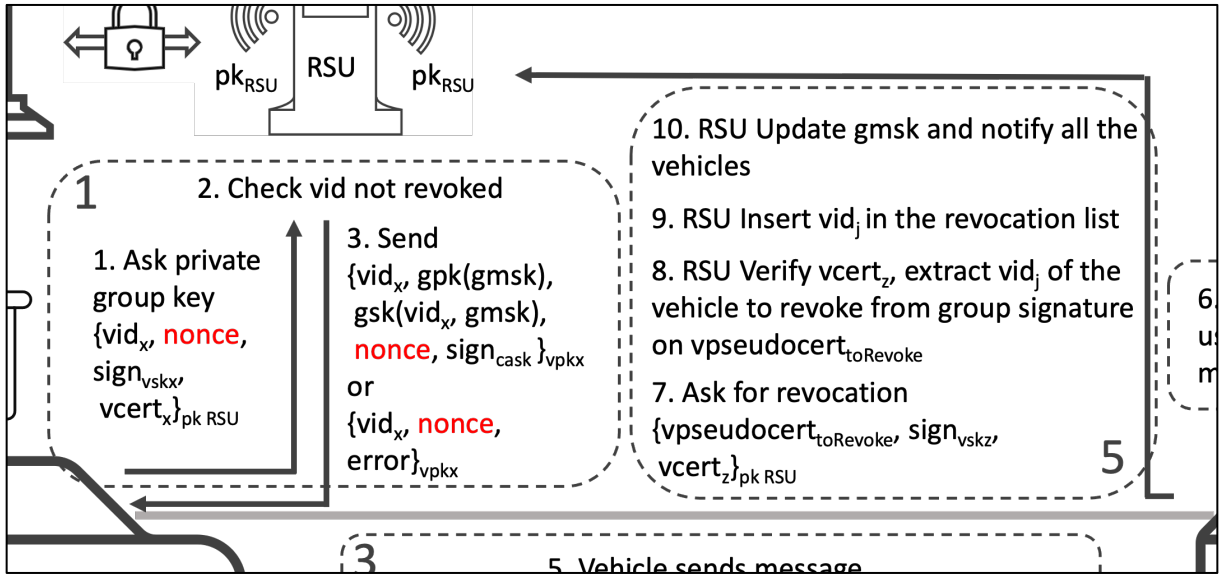
Verification results (iii)

- **RESULT 3**: *Anonymity issue in the revocation phase*
  - If attacker can link the initial intercepted request to the real identity of the vehicle (e.g., traffic-free road),
  - There is a violation of anonymity of the revoked vehicle
  - Solution



Verification results (iv)

- **RESULT 4**: *Linkability issue in the request for a group key*
  - Requests for a group key contain: vehicle id, enrollment certificate and signature using the enrollment certificate
  - These are all constant data
  - Two different requests are therefore identical and can be linked (tracking the vehicle through its requests to the RSU)
  - Solution



Conclusions

- We formally **modeled** and **analyzed** a v2x scheme existing in the literature
- The aim of the work is to show how **formal verification** can be used to analyze the **security** of a protocol
- The **model** we built for this protocol and the **related privacy properties** can be **adapted** to analyze other v2x protocols **as future work**

Thanks for your attention!

Simone Bussa
simone.bussa@polito.it

netgroup