L3Pilot
Driving Automation

Data Privacy for Automation:

Leveraging Privacy Enhancing Technologies

Virtual, 9 -10 September

SUMMER SCHOOL 2020

Jesus Diaz Vico
IBM Research GmbH

IBM Research

Outline

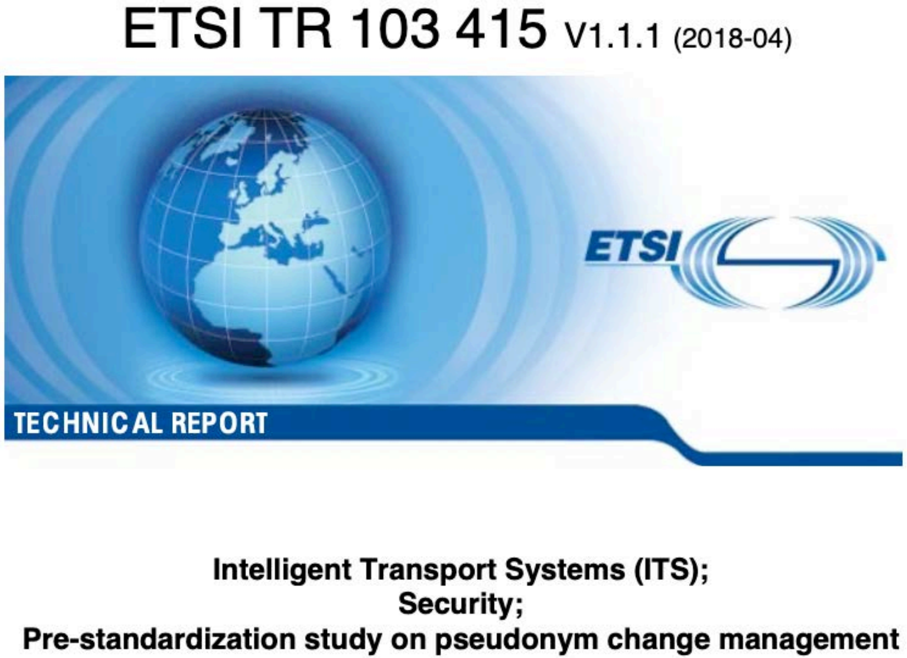
- The Challenge.
- Data privacy (in automation) at present.
- Leveraging PETs.
- Demo.

The Challenge

- Connected vehicles continuously report to the cloud and among them.
- Only authenticated vehicles can submit data.
- Not anonymized data can be used to track vehicles.
- Anonymized data reduces utility.

We need anonymously authenticated messages that still allows some processing.

Data Privacy (in automation) at Present



ETSI TR 103 415 V1.1.1 (2018-04)

TECHNICAL REPORT

Intelligent Transport Systems (ITS);
Security;
Pre-standardization study on pseudonym change management

Data Privacy (in automation) at Present

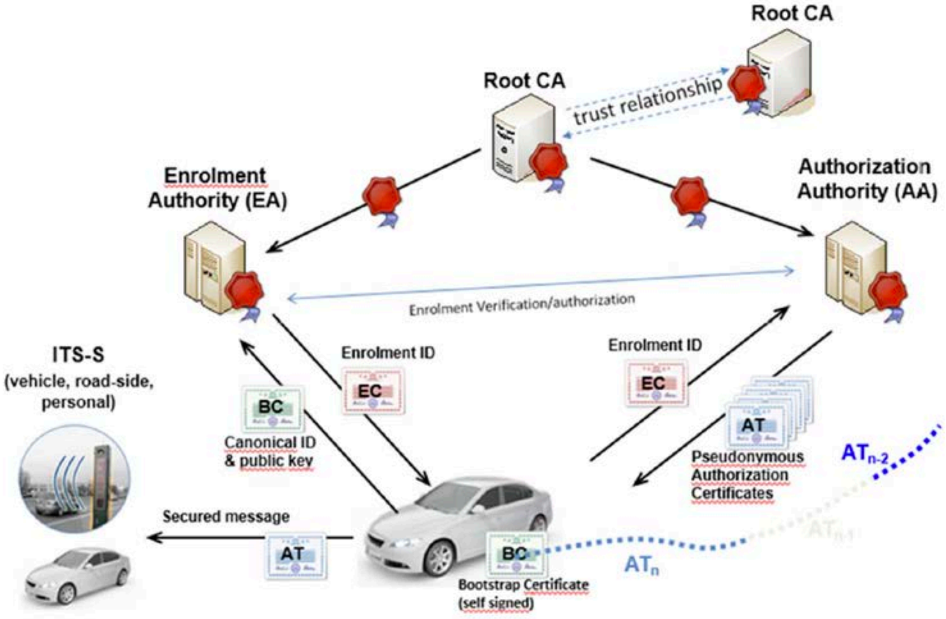

Root CA
Root CA
trust relationship
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
ITS-S (vehicle, road-side, personal)
Enrolment ID
EC
Enrolment ID
EC
BC
Canonical ID & public key
AT
Pseudonymous Authorization Certificates
AT_{n-2}
AT_{n-1}
Secured message
AT
BC
Bootstrap Certificate (self signed)
AT_n

Figure 2: ETSI ITS trust model (PKI)

Data Privacy (in automation) at Present

- Pseudonyms are updated depending on:
  - Fixed parameters (time/distance/number of messages).
  - Silent periods.
  - Vehicle-centric parameters: speed/direction.
  - Vehicle density and mix-zones.
  - Combinations of the previous.

Data Privacy (in automation) at Present

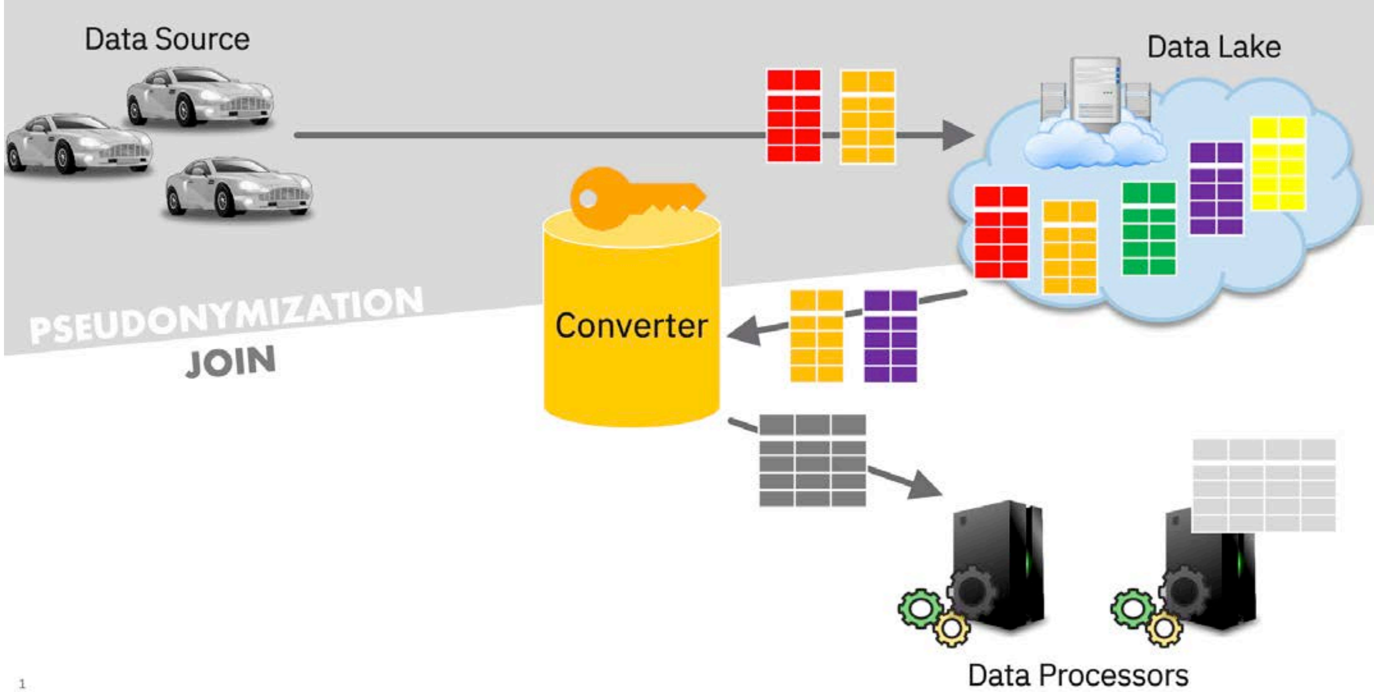
- **Pros**:
  - Simple.
  - Keeps utility.

- **Cons**:
  - Limited privacy.
    - Linkable (by anyone) during pseudonym lifetime.
  - Need to re-fetch pseudonyms.
  - Storage at the server side:
    - Needs to maintain a long-lived list of used pseudonyms.

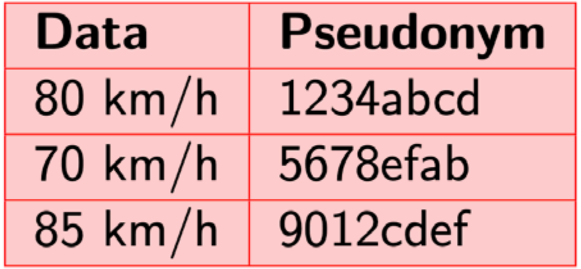
Leveraging PETs for Anomaly Detection

- **Scenario**:
  - Vehicles keep sending data to the cloud.
  - We need to support detection of anomalies.
  - … without identifying senders of non-anomalous messages.

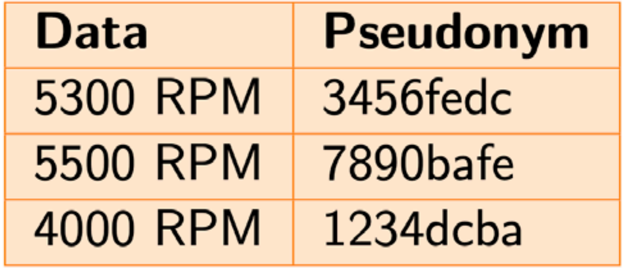
Leveraging PETs for Anomaly Detection



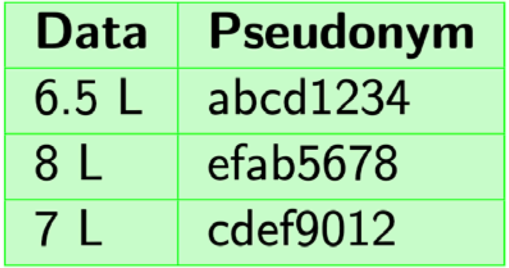
Leveraging PETs for Anomaly Detection



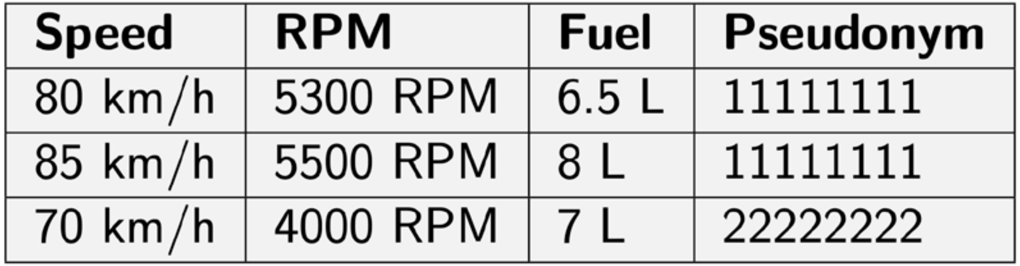
Data	Pseudonym
80 km/h	1234abcd
70 km/h	5678efab
85 km/h	9012cdef



Data	Pseudonym
5300 RPM	3456fedc
5500 RPM	7890bafe
4000 RPM	1234dcba



Data	Pseudonym
6.5 L	abcd1234
8 L	efab5678
7 L	cdef9012



Speed	RPM	Fuel	Pseudonym
80 km/h	5300 RPM	6.5 L	11111111
85 km/h	5500 RPM	8 L	11111111
70 km/h	4000 RPM	7 L	22222222

Leveraging PETs for Anomaly Detection

- Vehicles add a “single-use” pseudonym to authenticate each message.
- These “single-use” pseudonyms can be linked by a special entity.

How?

- Instead of conventional certificates (as in ETSI’s approach), we use a variant based on **group signatures**.

Convertably Linkable Signatures, from “*Group Signatures with Selective Linkability*”, by Garms and Lehmann, 2019.

Leveraging PETs for Anomaly Detection

Group signatures:

- Users (vehicles) can be added to the group.
  - When added, they receive a user private key.
- Users (vehicles) can create signatures on behalf of the group.
- Verifiers can check that such signatures come form “someone” within the group.

Convertably Linkable Signatures:

- Also, a special entity can (with limitations) link sets of these signatures.

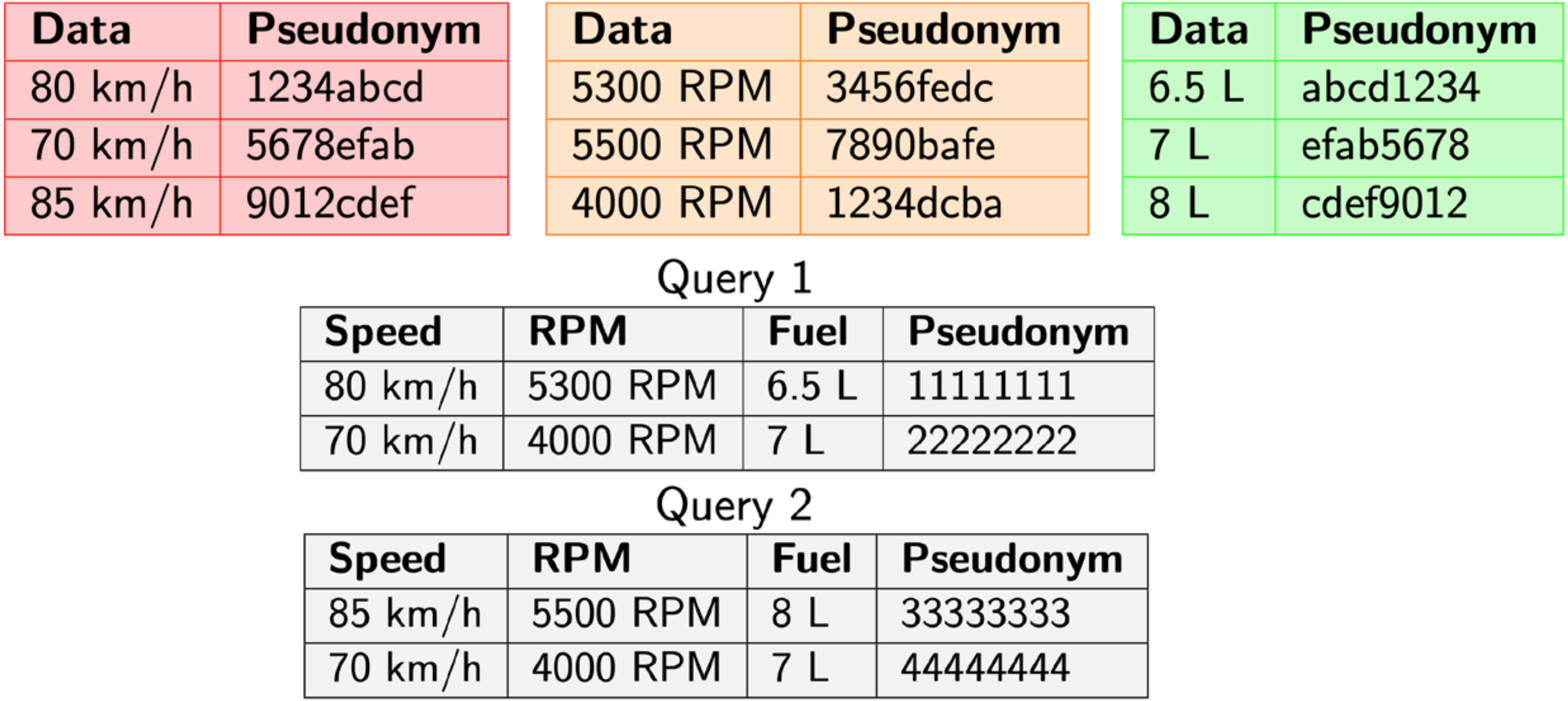
Leveraging PETs for Anomaly Detection

Approach:

1. Vehicles sign messages with CLS.
   - Each signature contains a “single-use” pseudonym.
2. The infrastructure verifies the signatures.
   - Receives assurance that signatures originate from valid vehicles.
3. When needed, the anomaly detection engine links sets of signed messages.
   - Without re-identifying the signer beyond the linkage.

Leveraging PETs for Anomaly Detection

CLS gives even more: **Non-Transitivity.**



Data	Pseudonym
80 km/h	1234abcd
70 km/h	5678efab
85 km/h	9012cdef

Data	Pseudonym
5300 RPM	3456fedc
5500 RPM	7890bafe
4000 RPM	1234dcba

Data	Pseudonym
6.5 L	abcd1234
7 L	efab5678
8 L	cdef9012

Query 1

Speed	RPM	Fuel	Pseudonym
80 km/h	5300 RPM	6.5 L	11111111
70 km/h	4000 RPM	7 L	22222222

Query 2

Speed	RPM	Fuel	Pseudonym
85 km/h	5500 RPM	8 L	33333333
70 km/h	4000 RPM	7 L	44444444

Leveraging PETs for Anomaly Detection

- **Pros**:
  - Keeps utility (suitable for most use cases).
  - Maximizes privacy (as much as data allows).
  - Reasonably efficient for high volumes of data.
  - Minimizes storage requirements by server and vehicles.

- **Cons**:
  - Utility restricted to “joins”.

Demo

Future Directions

- Evaluation in realistic settings.
- Compatibility with current infrastructures.
- Analysis of further functionality.

L3Pilot Driving Automation

Thank you for your kind attention.

Jesus Diaz Vico
jdv@zurich.ibm.com
@jesusdiazvico

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 723051.