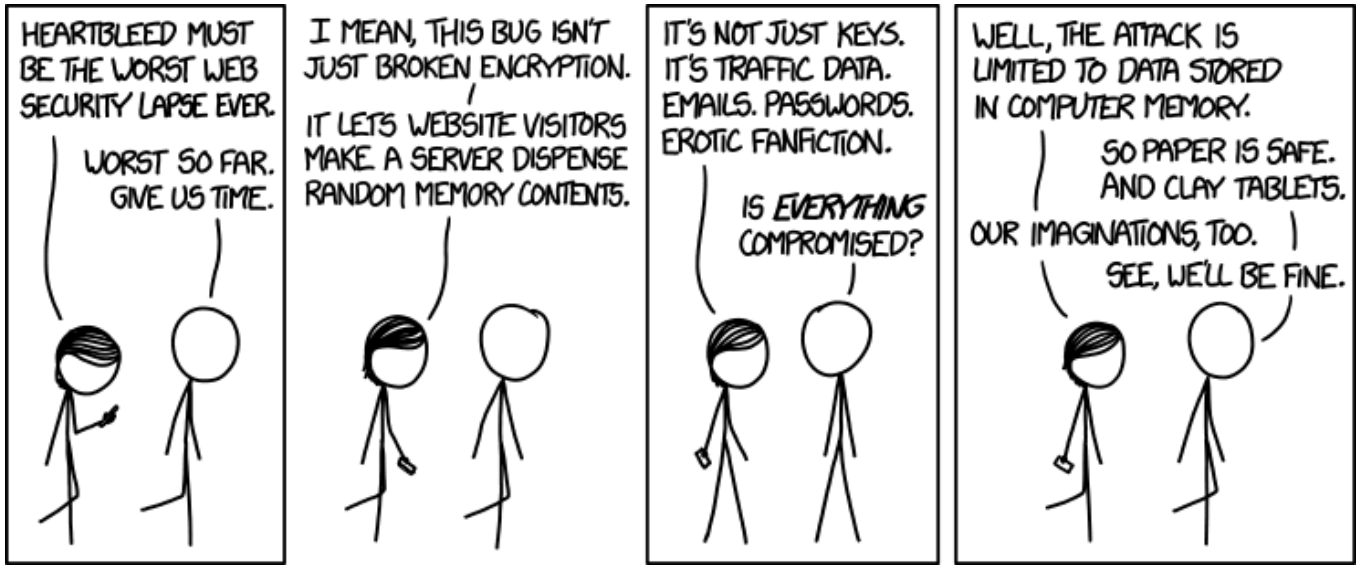


ETSI ITS Security Assessment

Alexandru C. Serban[1,2]
Erik Poll[1]
Joost Visser[2]

[1]Digital Security - Radboud University, Nijmegen

[2]Research Team - Software Improvement Group, Amsterdam

Contents

Outline of ETSI ITS

Security in ETSI ITS

Security Issues

Conclusions

A word about ETSI ITS

- ETSI ITS standardises V2V & V2X in Europe

"Does your car have any idea why my car pulled it over?"

A word about ETSI ITS

- ETSI ITS standardises V2V & V2X in Europe
- Defines C-ITS and its evolution to support full autonomous driving (including wireless communications dedicated to automotive ITS and road transport and traffic telematics)

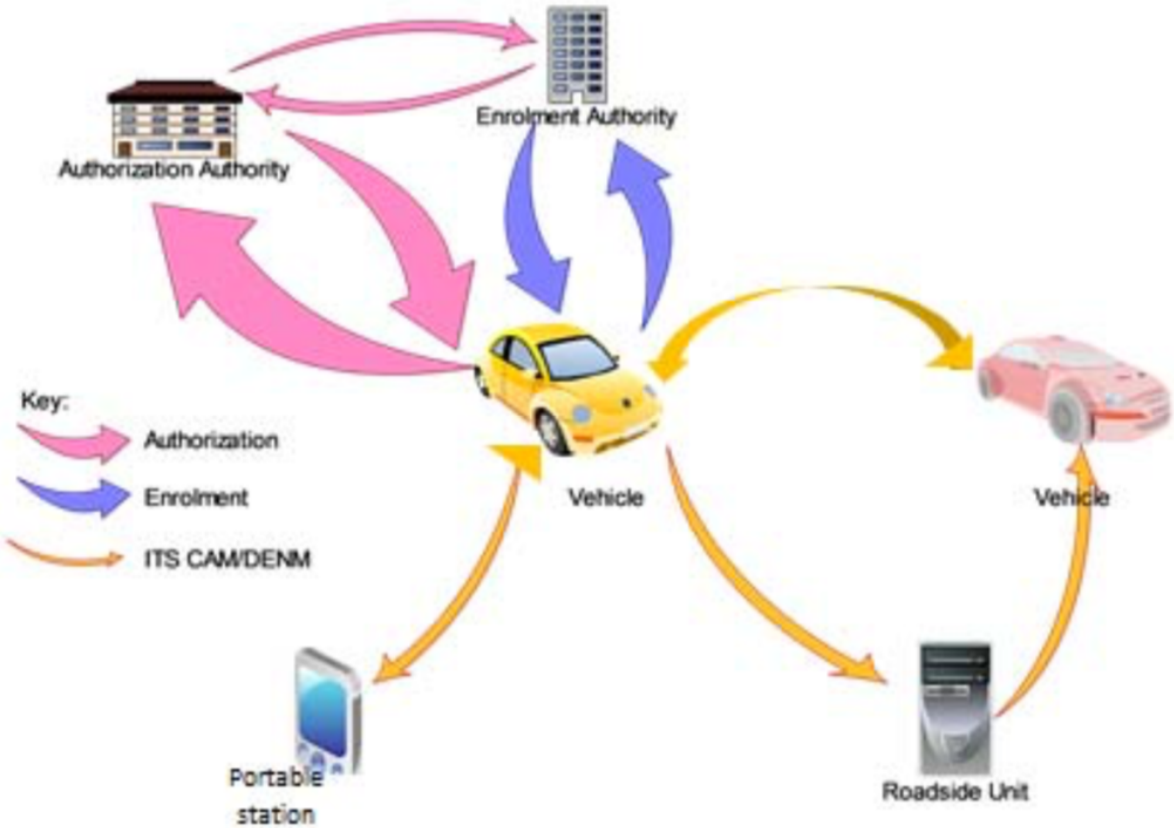
"Does your car have any idea why my car pulled it over?"

A word about ETSI ITS

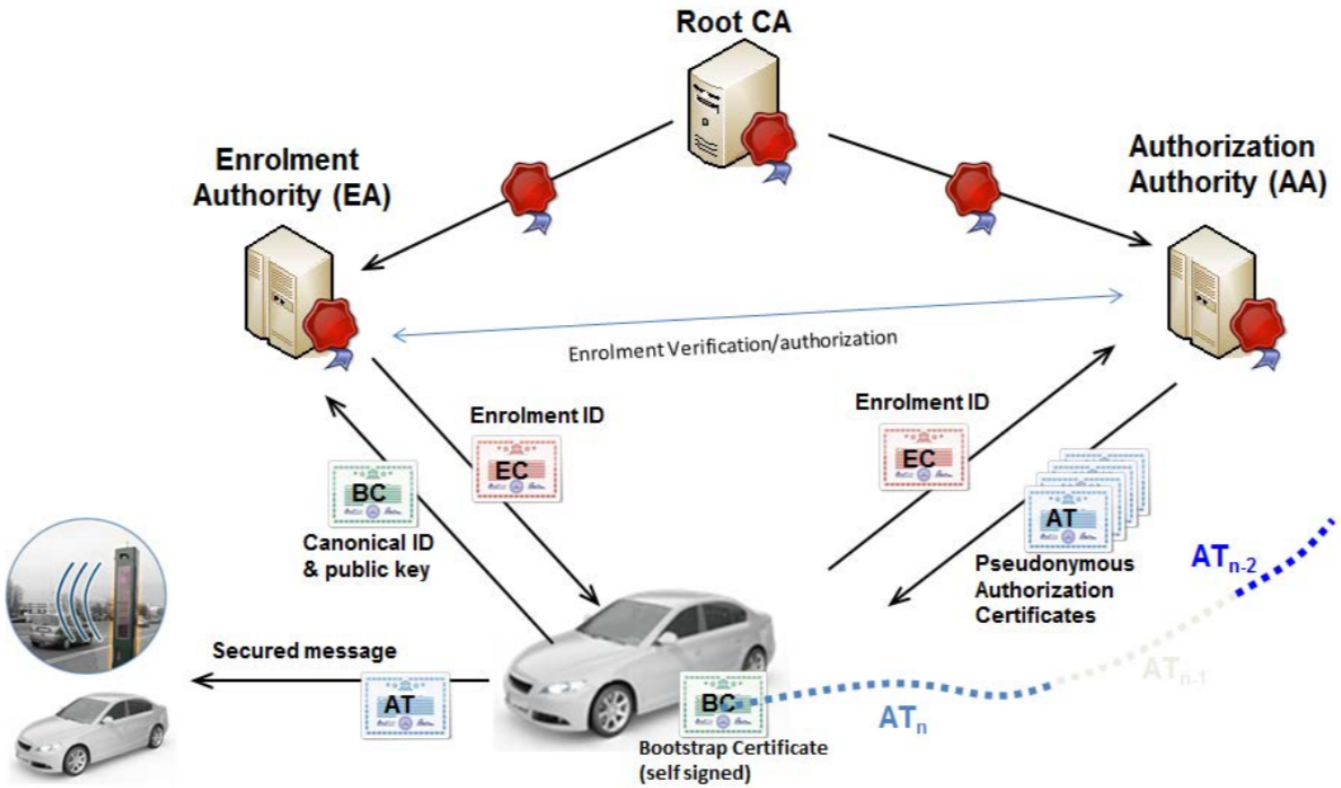
- ETSI ITS standardises V2V & V2X in Europe
- Defines C-ITS and its evolution to support full autonomous driving (including wireless communications dedicated to automotive ITS and road transport and traffic telematics)
- Defines 'Automotive Security'

"Does your car have any idea why my car pulled it over?"

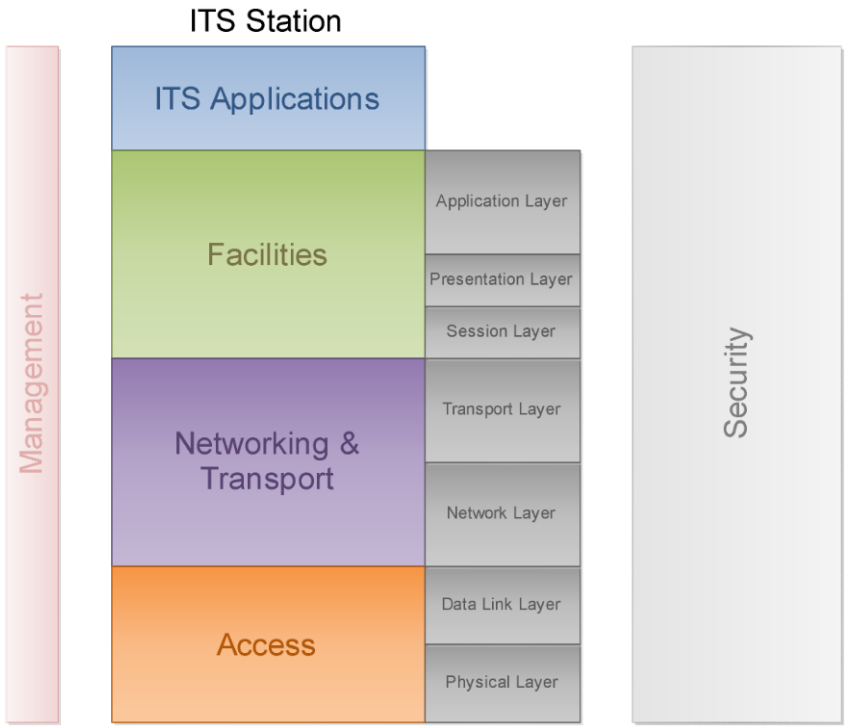
ETSI ITS Reference Model



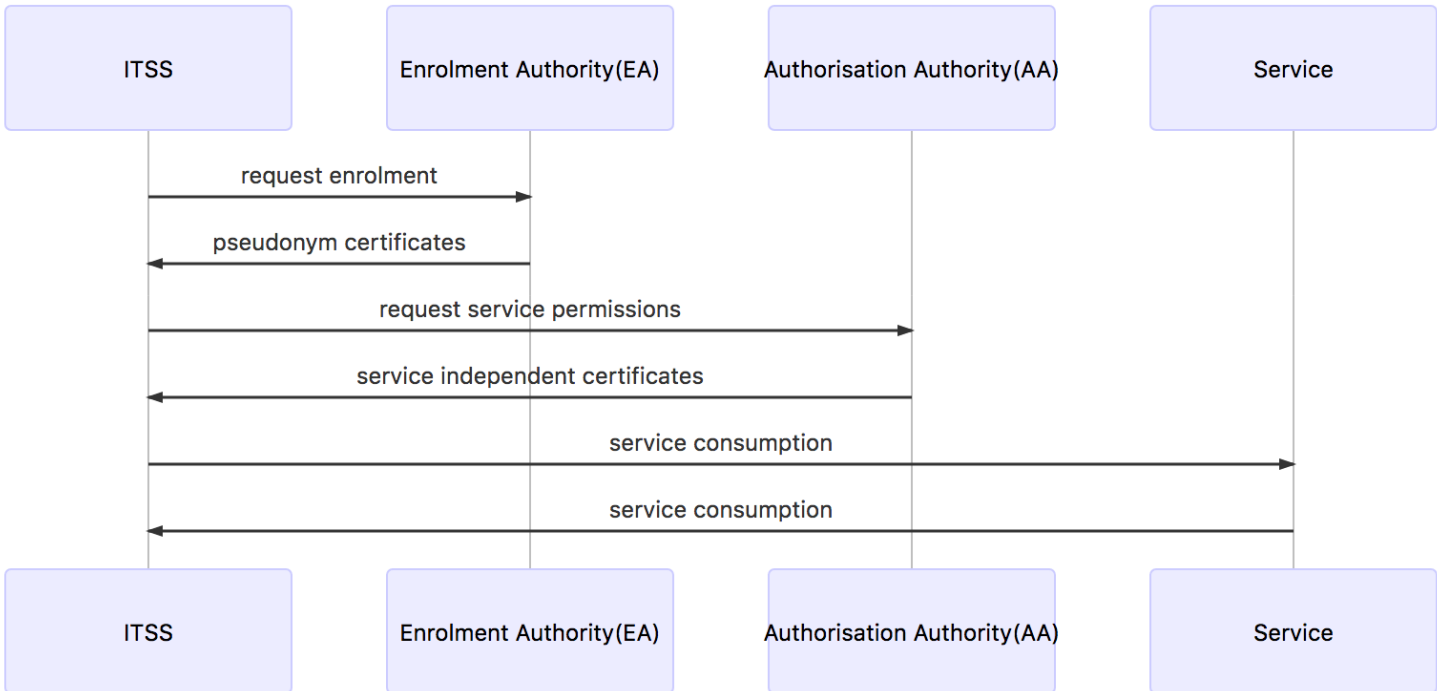
PKI Infrastructure in ETSI ITS



ETSI vs OSI


ITS Station
ITS Applications
Facilities
Networking & Transport
Access
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Management
Security

Authentication and Authorisation Flow

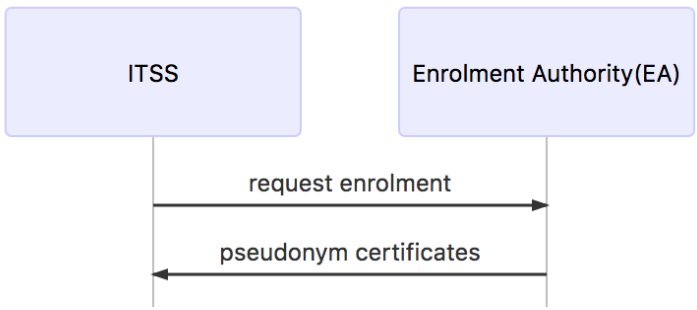


ITSS - EA

Requests:

- Create
- Update
- Remove

enrolment certificates.



ITSS - EA

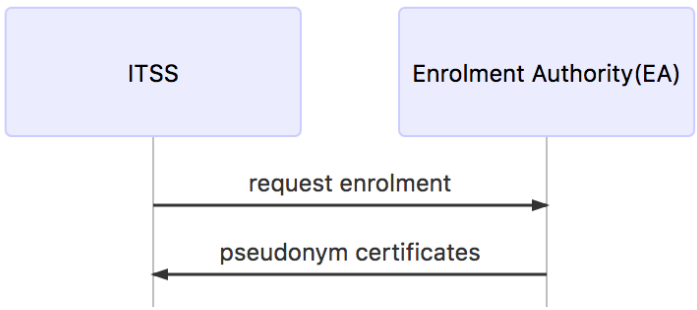
Requests:

- Create
- Update
- Remove

enrolment certificates.

Issues:

- Update & Remove requests can be replayed.



ITSS - EA

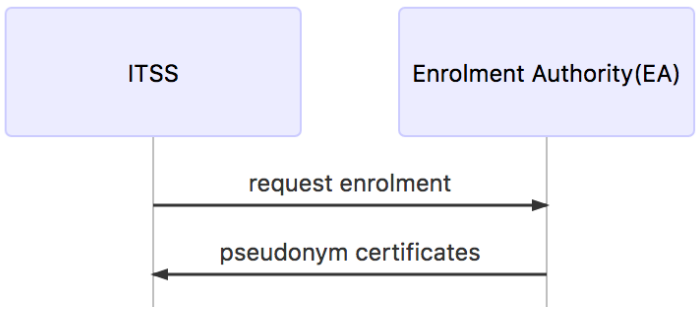
Requests:

- Create
- Update
- Remove

enrolment certificates.

Issues:

- Update & Remove requests can be replayed.



Attack economic factors:

ITSS - EA

Requests:

- Create
- Update
- Remove

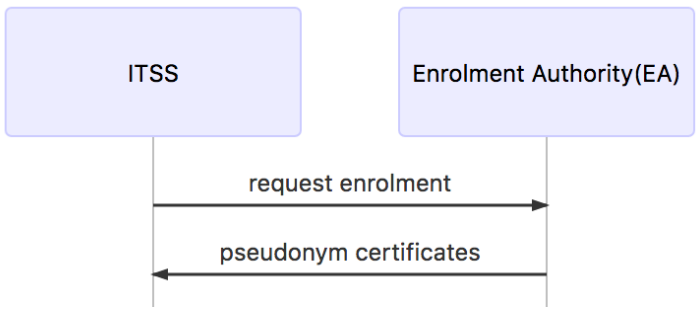
enrolment certificates.

Issues:

- Update & Remove requests can be replayed.

Attack economic factors:

- hard to mount because these requests are not frequent

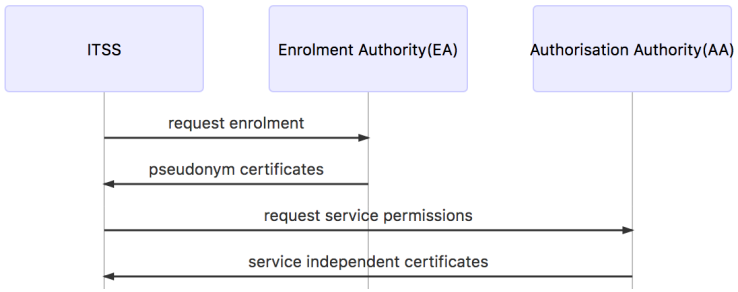


ITSS - AA

Requests:

- Create
- Update
- Remove

pseudonim certificates.



ITSS - AA

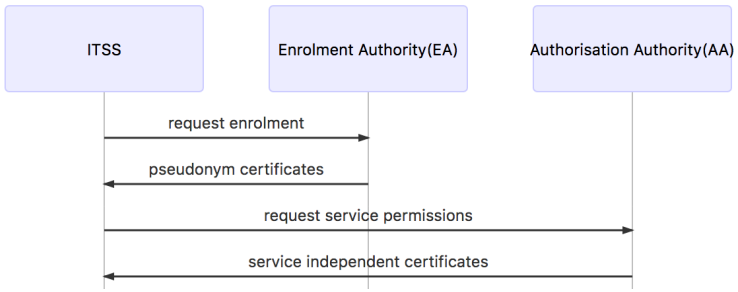
Requests:

- Create
- Update
- Remove

pseudonim certificates.

Issues:

- all requests can be replayed



ITSS - AA

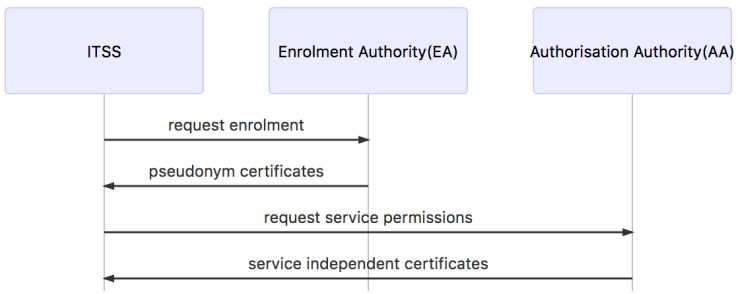
Requests:

- Create
- Update
- Remove

pseudonim certificates.

Issues:

- all requests can be replayed



Attack economic factors:

ITSS - AA

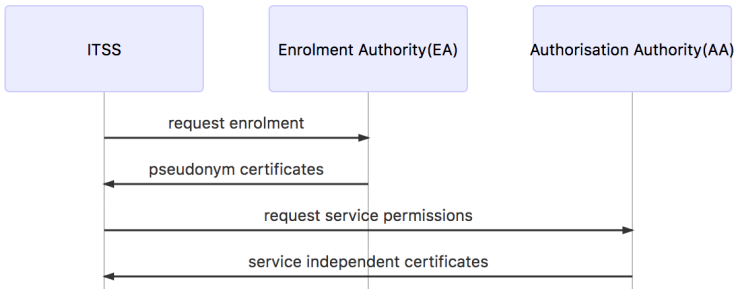
Requests:

- Create
- Update
- Remove

pseudonim certificates.

Issues:

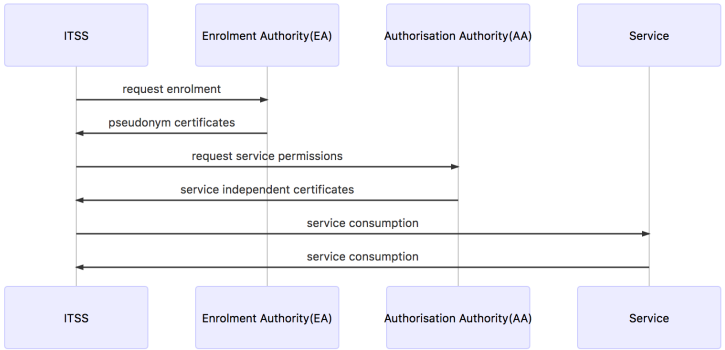
- all requests can be replayed



Attack economic factors:

- easier to mount because these requests are frequent

ITSS - Service



Take aways

- 1st versions of all security protocols will be broken (see TLS)

Take aways

- 1st versions of all security protocols will be broken (see TLS)
- ETSI ITS makes no exception

Take aways

- 1st versions of all security protocols will be broken (see TLS)
- ETSI ITS makes no exception
- Since security specs. are huge, first implementations will also be broken (see TLS)

Take aways

- 1st versions of all security protocols will be broken (see TLS)
- ETSI ITS makes no exception
- Since security specs. are huge, first implementations will also be broken (see TLS)
- Future research ranges from formal verification to conformance verifications (e.g. through SAT solvers, model learning, etc)