Certificate-based access to the vehicle and its data
Report on ISO work (G. Feiter)

Gangolf Feiter - Concepts & Services Consulting
Ostpromenade 107 (City Center)
52525 Heinsberg, Germany
Ph.: +49 (2452) 96 484 0
info@csc-online.eu
www.concepts-services-consulting.de

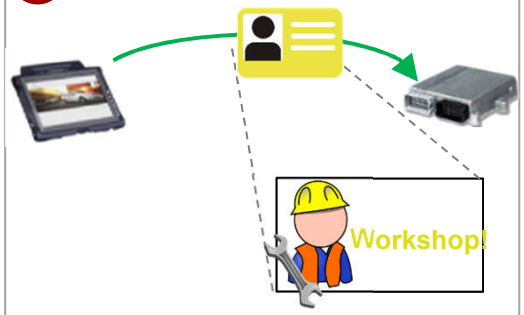
Meeting @EGEA Office in Bruessels
Sept. 05, 2017

How to ensure security of the OBD port?

- Except for the ISO 15031 / SAE J1979 emissions-related protocol all enhanced diagnostic communication services might require (due to the decision of the VM) authentication and authorization via certificate
- In addition, due to the decision of the VM, messages might be encrypted (secured DataTransmission, service 0x84 in ISO 14229-1)

Secure Diagnosis has three main components

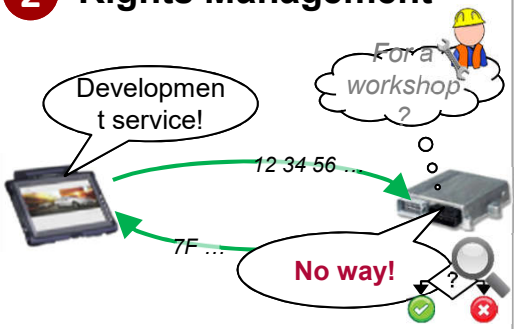
1 Tester Authentication



Tester shows Authentication to ECU. Now, ECU knows whom it is talking to.

+

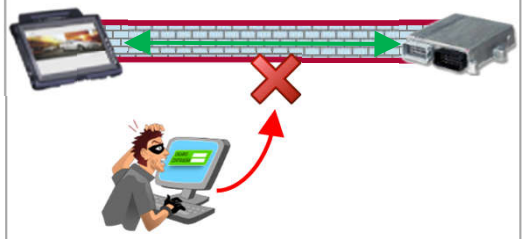
2 Rights Management



ECU grants the specific rights for diagnostic services and access to data.

+

3 Secure Communication



Communication is secure against manipulation.

… is the base for Rights Management and Secure Communication.

… is the base for controlling access rights.

… is the base for a secure rights management.

This service uses two security concepts:

— Concept #1 is based on PKI certificate exchange procedures using asymmetric cryptography (see 10.6.2). As certificate format CVC or X.509 shall be used.

— Concept #2 is based on challenge-response procedure without PKI certificates using either asymmetric cryptography with software authentication tokens (see 10.6.3) or symmetric cryptography (see 10.6.3).

NOTE The generation, distribution and storage of cryptographic material is out of scope for this specification.

Figure 1 gives an overview over the Authentication service security concepts.

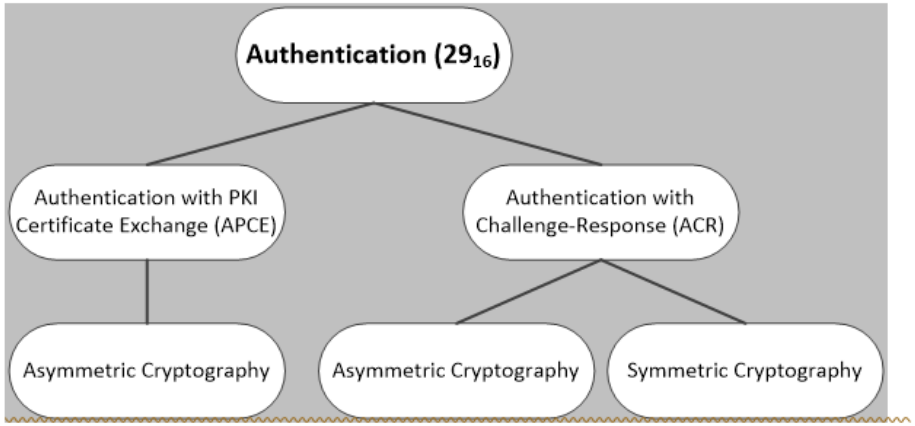
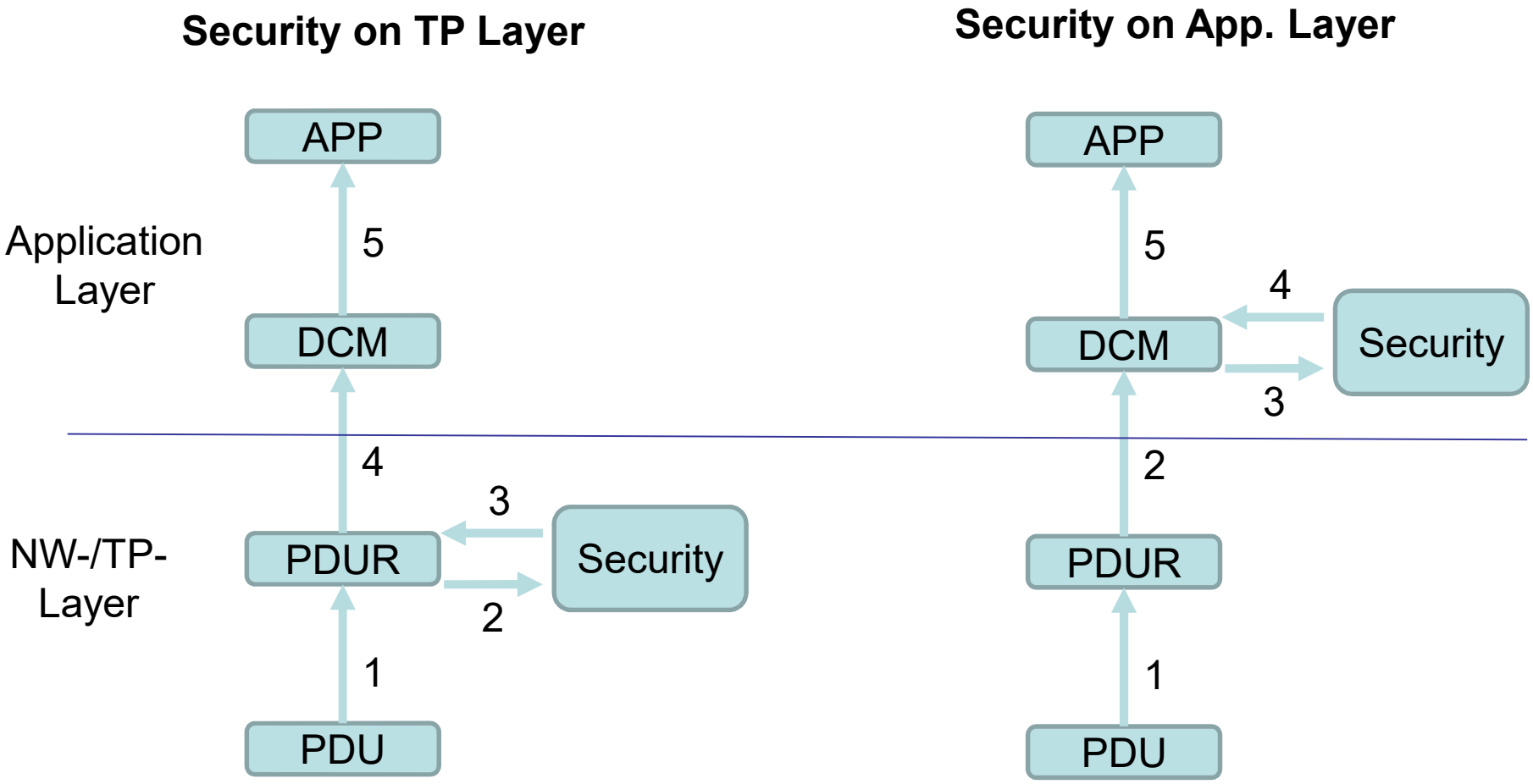


Figure 1 — Overview over the Authentication service security concepts

To identify the supported concept in the server, the client can send this service with the sub-function parameter 'authenticationConfiguration'.

Introduction - Schematic Security on TP vs. App Layer



For who?

- Workshops: YES
- Technicans: Possible, not defined
- Tool manufacturers: Possible, not defined
- Dedicated tool functions: Possible, not yet defined

For what services?

- Workshop use:
  - Yes - Flash programming
  - Yes – Safety-relevant systems/functions
- Legislative testing (e.g. PTI, emissions, ….):
  - No – Emissions-related systems
  - Maybe – ePTI
- Security-related information only:
  - Yes – Active driving assistance systems/functions
- Remote services (e.g. RDS, …) when the vehicle is moving:
  - Yes – Only via VM's ExVe
- Re-programming, reconfiguration, recording, software changes,…:
  - Most likely
- Read-only data and/or writing data?
  - Writing data
- Stationary or vehicle moving?
  - Vehicle moving

What data access and scope?

- Should the certificate be related to the access only, the function or to the data?
  - Certificate is needed for tester authentication;
    - ❖ See new ISO 14229-1 UDS Service 0x29 Authentication
  - Certificate is also used for tester Authorization
    - ❖ Functionality and/or Data

Validity duration?

- Certificate use only once
  - My best guess is that this use case applies to safety critical functions e.g. flash programming
- Certificate limited per day/hours
  - VM decision, no longer than 6 months
- Certificate limited to system/function
  - VM decision, however current status is that a certificate will be per vehicle type
- Certificate extended validity
  - ???
- How to avoid requesting certificates constantly, whilst ensuring security (vs. exposed to cyber-attacks)?
  - Certificate life time needs to be time limited to ensure security

Process of accessing and using certificates?

- Process structure?
  - Not defined anywhere
  - ISO will not define
  - Agreement between VMs and Aftermarket?
- Costs?
  - To avoid cost duplication when repairing and testing (e.g. PTI information is a subset of RMI)
    - ❖ Yes, if workshop is authorized for PTI
- Legislation?
  - Legislation will be needed, SERMI can be an existing solution (cf. Euro 5 legislation)
    - ❖ A modified version of SERMI might be possible. However, within ISO this is NOT discussed. The VMs plan to have their own Trust Center to allow access to the vehicle ECUs.

Draft proposal for discussion

Trust Centre

Independent Operator verification

PTI certificate

Independent Operator and tool certificates

Conformity assessment body

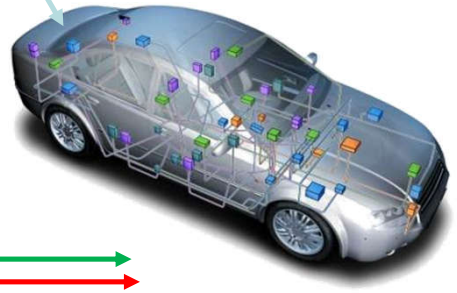
Vehicle Manufacturer

Independent workshop

PTI credentials

PTI test centre

PTI inspector



PTI certificates

PTI test tool