Dangerous Goods Transport
AP 400
Procedures concerning IT security

transport logistic 2011

München, 11.05.2011 v. 1.0

|otten|software|

Content

- Requirements for IT safety and IT security
- Boundary conditions
- Security procedures within the generic process modell
- Access Control List „Who sees what“
- Modelling IT security procedures
  - Creating DG transport data during loading
  - Update of DG transport data during transport
  - Access to DG transport data with differnent scenarios for communication infrastructure
- Extensions of the communication modell

|otten|software|

Requirements for IT safety and IT security

- Unique mapping of vehicle, DG data and transport meta data to originators
- Confidentiality of data, access to data strictly according to access control lists
- Separation of vehicle data, DG loading data and transport meta data (e. g. starting point, route, target)
- Prevention of deducing load and routing profiles
- Short term storage of data
  - (automatic) deletion of data after transport
  - No data warehouse
- Availability of data access must be ensured according to ACL
- Tamper detection: Tampering data without appropriate rights by any third party must be detectable

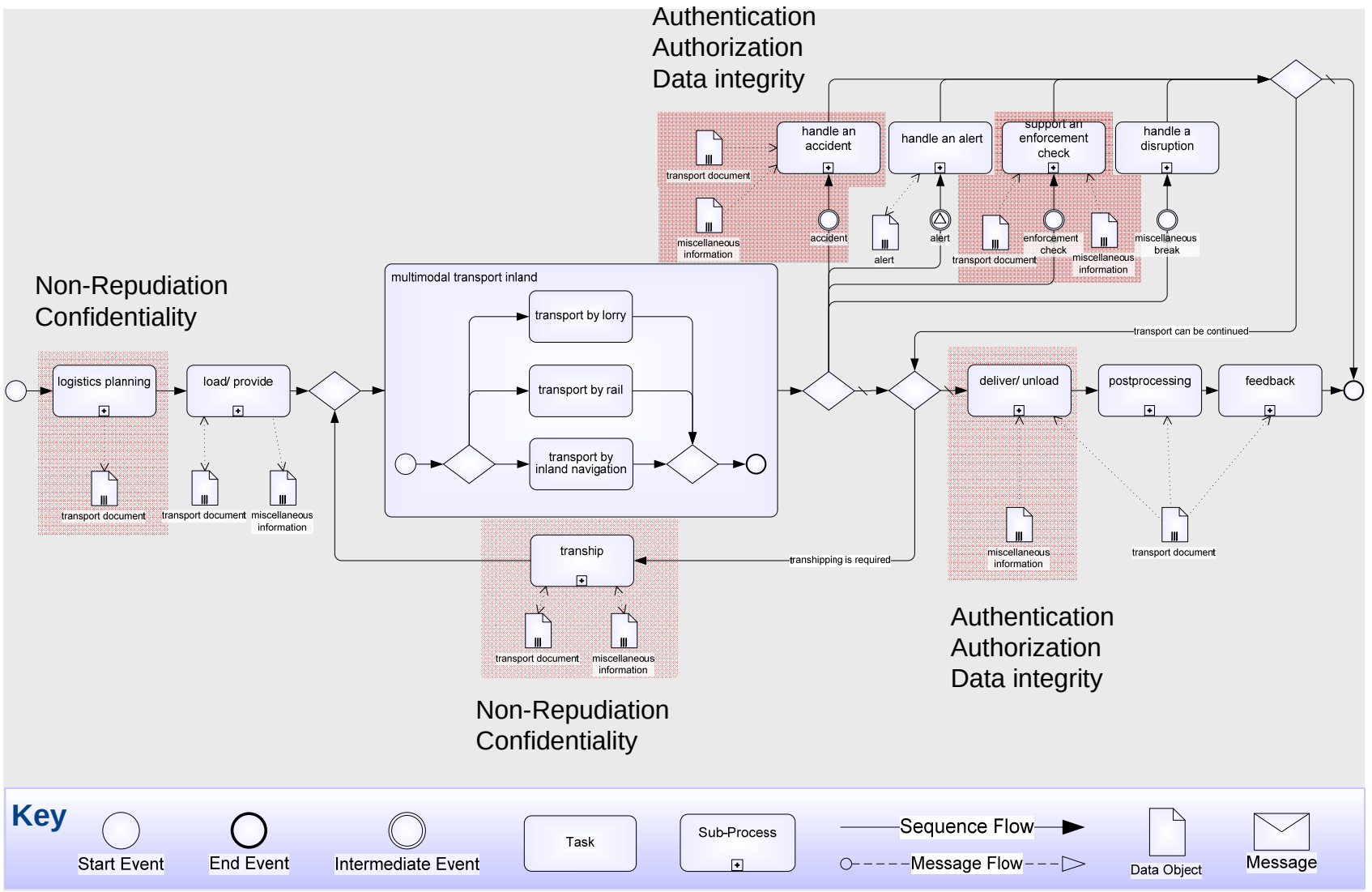
|otten|software|

Boundary conditions

- Communication scenarios presented here focus on accidents and enforcement checks
  - Scenarios can be easily adopted to end2end communication between sender and recepient of DGs
- DG data must not be changed during the entire transport process
  - Information about changes (eg. load additional DGs, unload parts of DGs) are stored in additional DG data documents
- Therefore more than one document with DG and transport related data may exists
- Transshipping processes are treated as normal transport processes
  - End of transport A / transshipping / begin of transport B
  - New DG transport informations are created before transport B starts

|otten|software|

Process Dangerous Goods Transport (from WP500 Data Process Modelling)

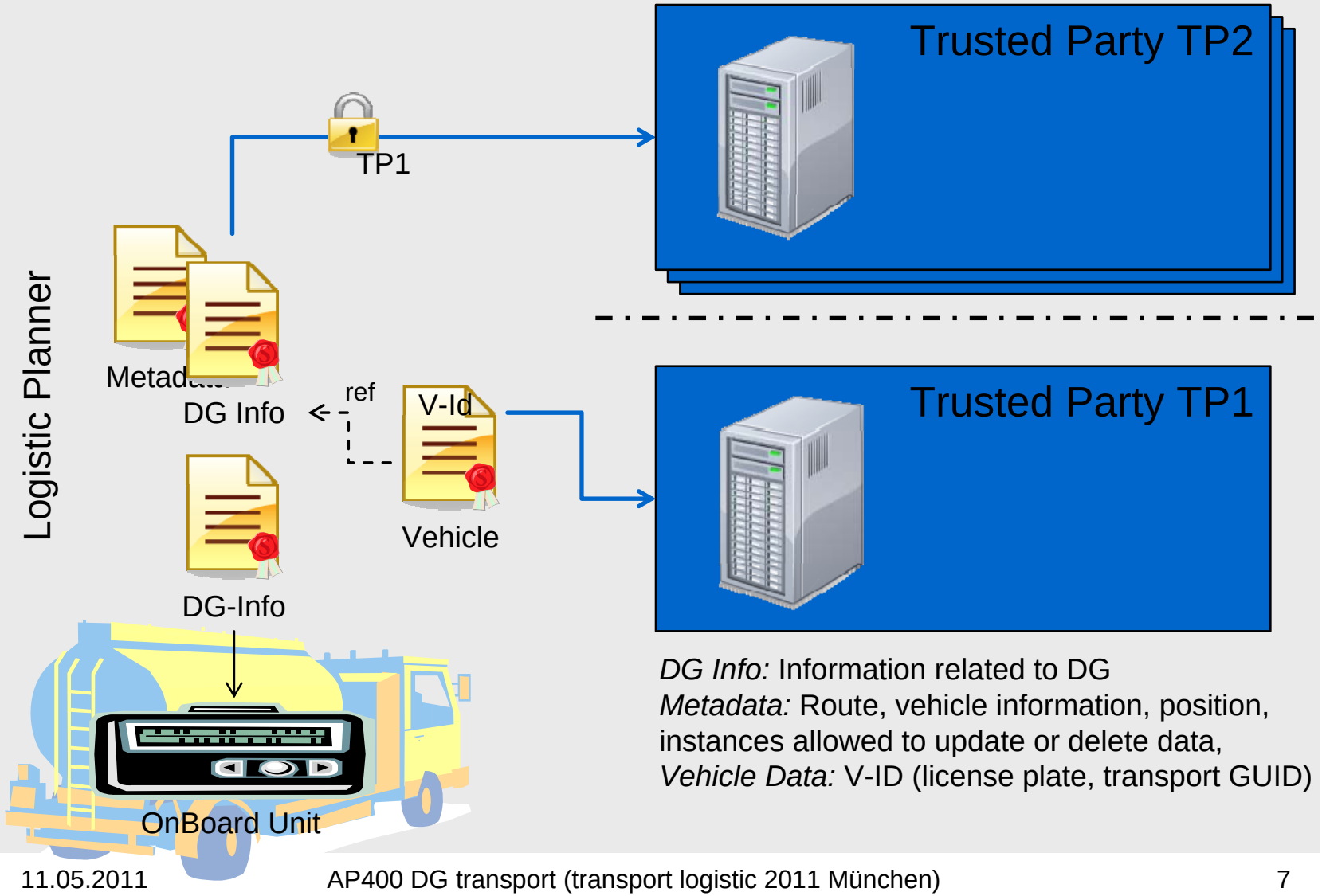


Access Control List „Who sees what“

- An access control list (ACL) fixes the conditions for creating, reading, (updating) and deleting DG data
- The ACL depends on roles (who wants to access data), type of data and type of access
- Roles under consideration
  - Carrier / logistic planner
  - Recipient
  - Inspector for enforcement checks
  - Fire Service / Rescue Service
  - Control Centers
  - Administrators
- Data types
  - DG information
    - static
    - dynamic
  - Routing information
  - Vehicle information
- Acces type
  - Create information
  - Update information
  - Emergancy access
  - Enforcement check access
  - Delete Information

|otten|software|

Modelling IT security procedures
Creating DG transport informations



DG Info: Information related to DG
Metadata: Route, vehicle information, position, instances allowed to update or delete data,
Vehicle Data: V-ID (license plate, transport GUID)

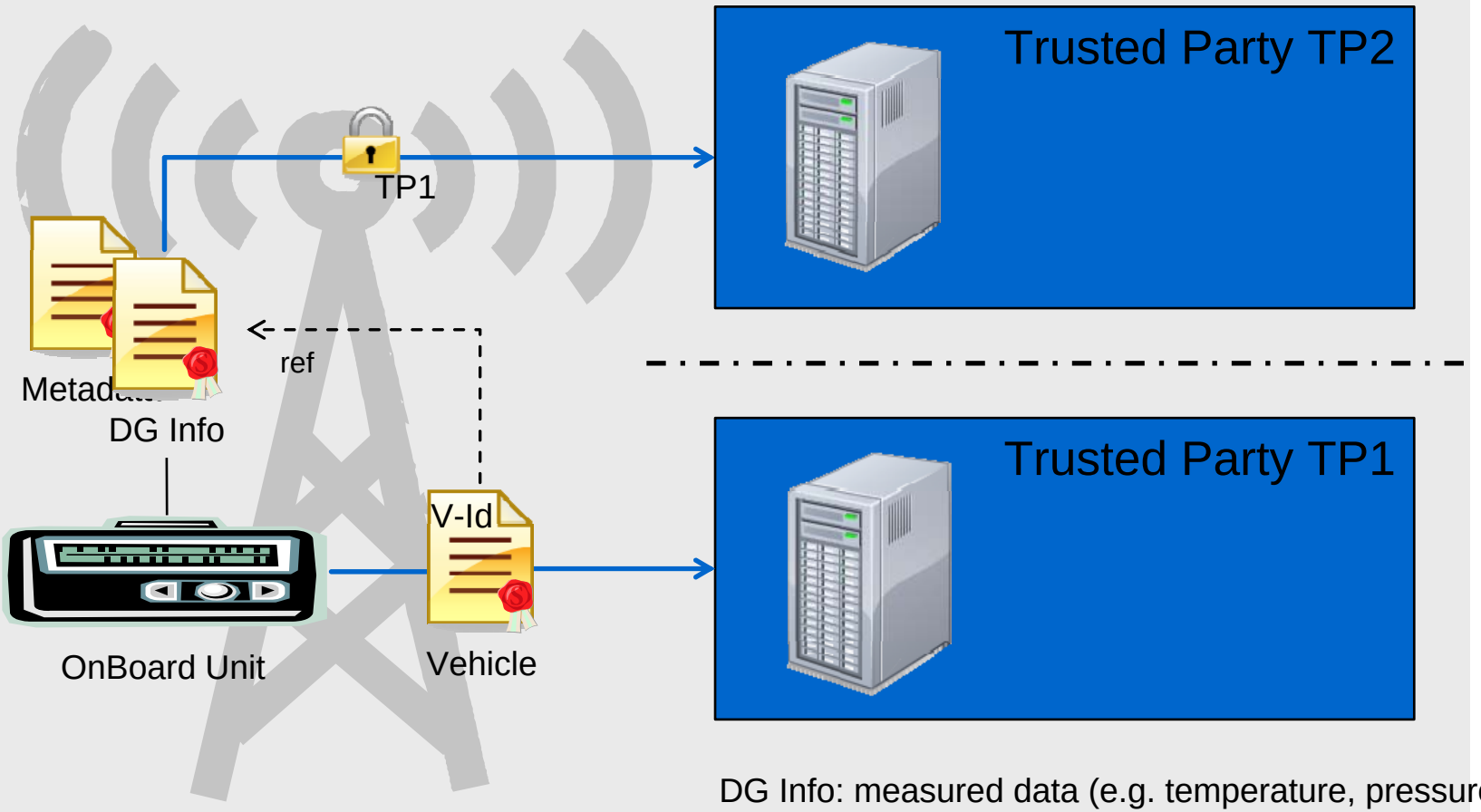
|otten|software|

Advantages of separating IDs and Payload Data

- Trusted Party 1 administers only transport / vehicle Ids without any payload
  - Access on payload is only possible in cooperation with TP 2
  - Data access can be monitored and logged/journalized both at TP1 and TP2
  - Data separation grants access to data in cleartext only by pre-definded access structures
- Trusted Party 2 does not gain clear text information about DG data
  - Data is encrypted für TP 1
  - Profiling impossible
- Trusted Party 2 can be set up manifold at different physical locations
  - e.g. implemented with defined service levels in the data center of the logistic planner, the manifacturer or other 3rd parties
- Separation of data makes it difficult to get access to clear text informationen for any aggressor
  - Aggressor has to succesfully attack both Trusted Party 1 (to get the key) and Trusted Party 2 (to get the encrypted data)

|otten|software|

Modelling IT security procedures
Adding DG Data by OnBoardUnit



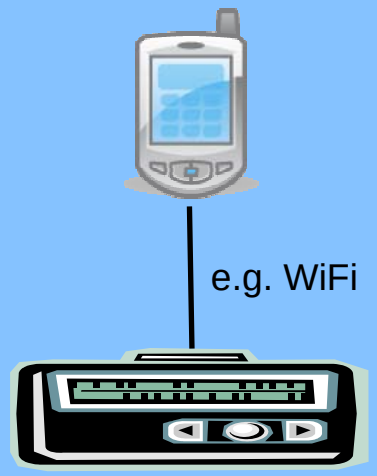
DG Info: measured data (e.g. temperature, pressure)
Metadata: Routing-Information, Position
Vehicle Data: V-ID

|otten|software|

Getting Access to Data (emergency, enforcement) Communication Infrastructure

Scenario 1

Local Interaktion between Vehicle and Handheld without any WAN

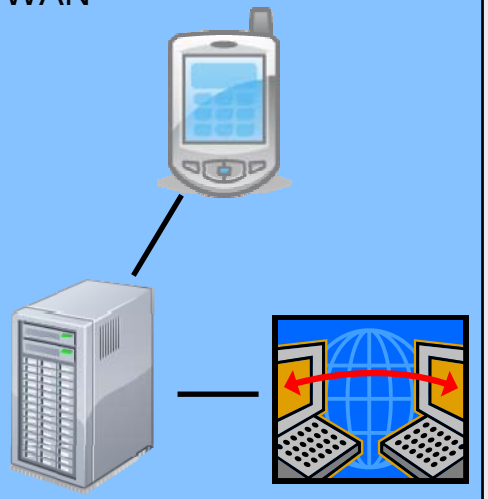


Scenario 2

IP-Communication from Handheld to WAN

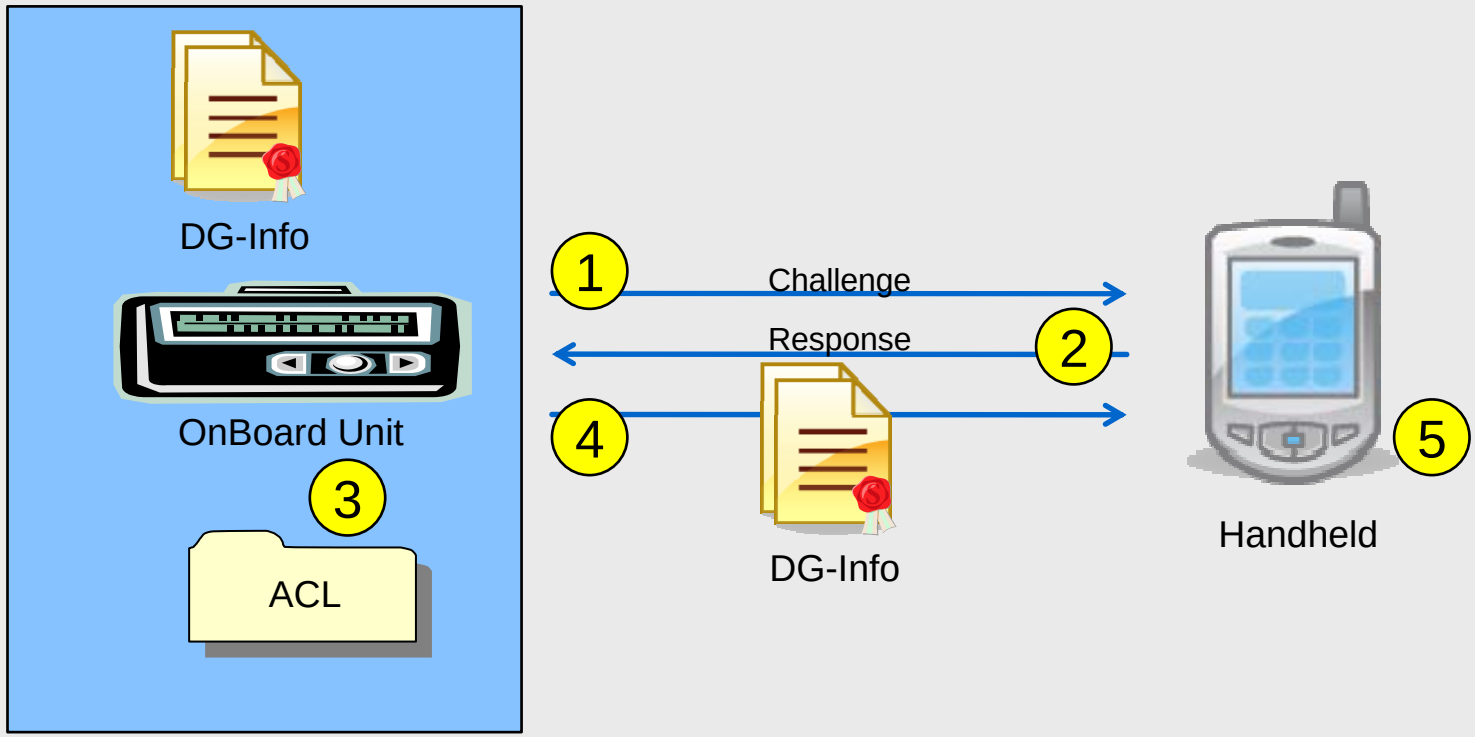
Scenario 3

(Proprietary) Communication from Handheld to Control Center, IP-Communication from Control Center to WAN



Parallel Setup of all scenarios possible.

Getting Access to Data:
Local Interface between OBU and Handheld



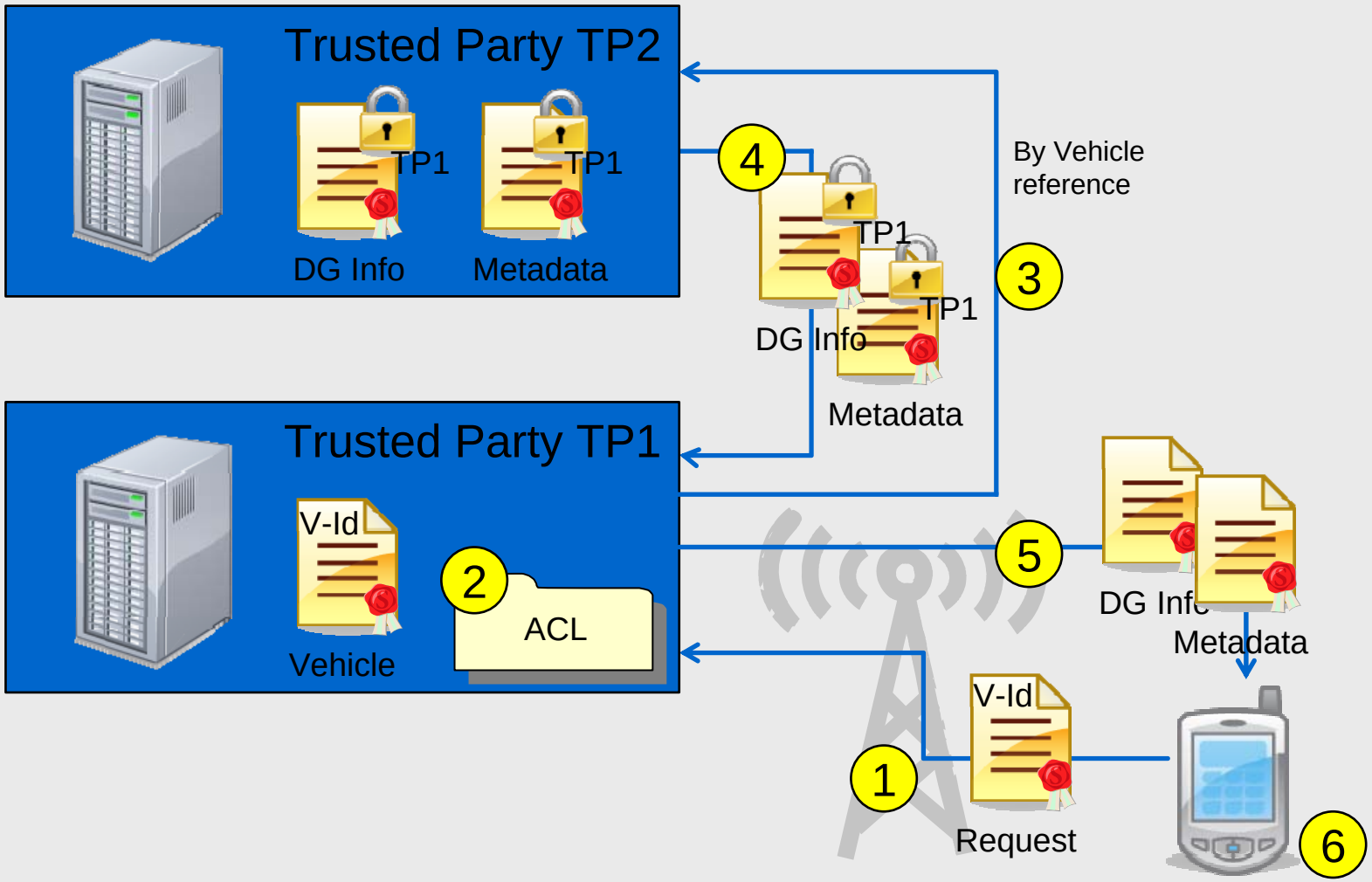
Explanations
Local Interface between OBU and Handheld

- Mutual authentication between OBU and Handheld
- Authentication procedure is neccessary to avoid any improper use of data stored in the OBU, e g. by

1. Challenge-Response protocol between OBU and Handheld.
2. Handheld respondes to challenge by using its handheld ID & an individual security token (e.g. a digital certificate)
3. OBU verifies whether or not the handheld is allowed to access the DG data (testing against the locally stored access control list)
4. If test is successful the OBU transmits DG Data (or parts of it according to the ACL) to the handheld
5. Handheld checks integrity and authenticity of transmitted data and displays relevant Informationen

|otten|software|

Getting Access to Data
Direct Communication between Handheld and TP 1

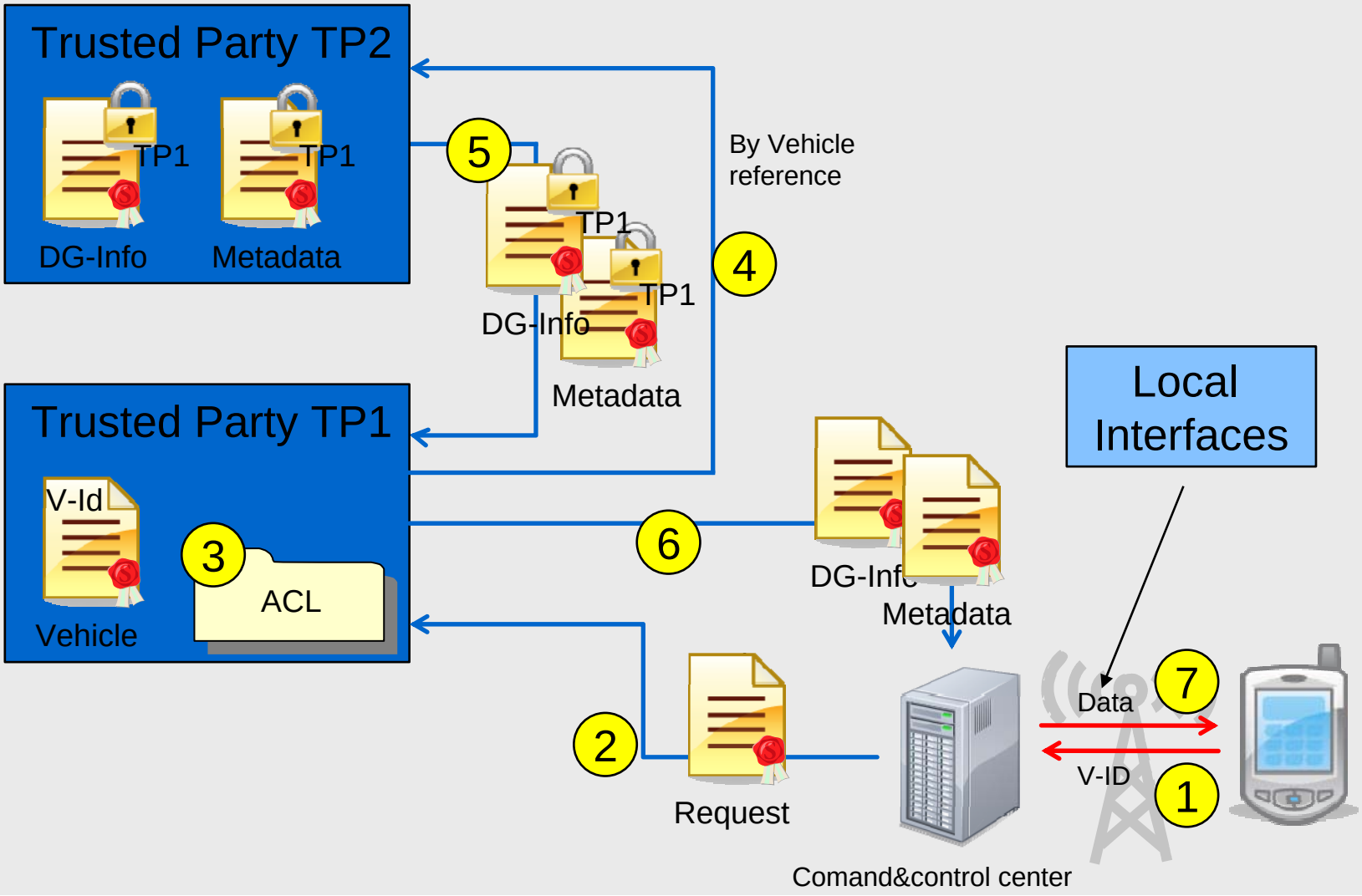


Explanation
Direct Communication between Handheld and TP 1

1. After entering the vehicle ID Handheld sends a signed message with this ID to Trusted Party 1 over a secure channel
2. Trusted Party 1 checks the validity of the signature and proves by means of ACL the authorization of the handheld.
3. In case of a valid request TP1 sends a data request to Trusted Party 2 via an authentic channel
4. TP 2 responses by sending the encrypted documents (DG data and metadata, if available) via an authentic channel to TP 2.
5. Trusted Party 1 decrypts the messages with its private key, checks the validity of the document signatures (which have been originated by the logistic planner) and submits data to the handhelp.
6. Optionally the signatures are validated by the handhelp also. Finally the handheld displays the relevant informations in a suitable manner.

|otten|software|

Getting Access to Data
Communication between Control Center and TP 1

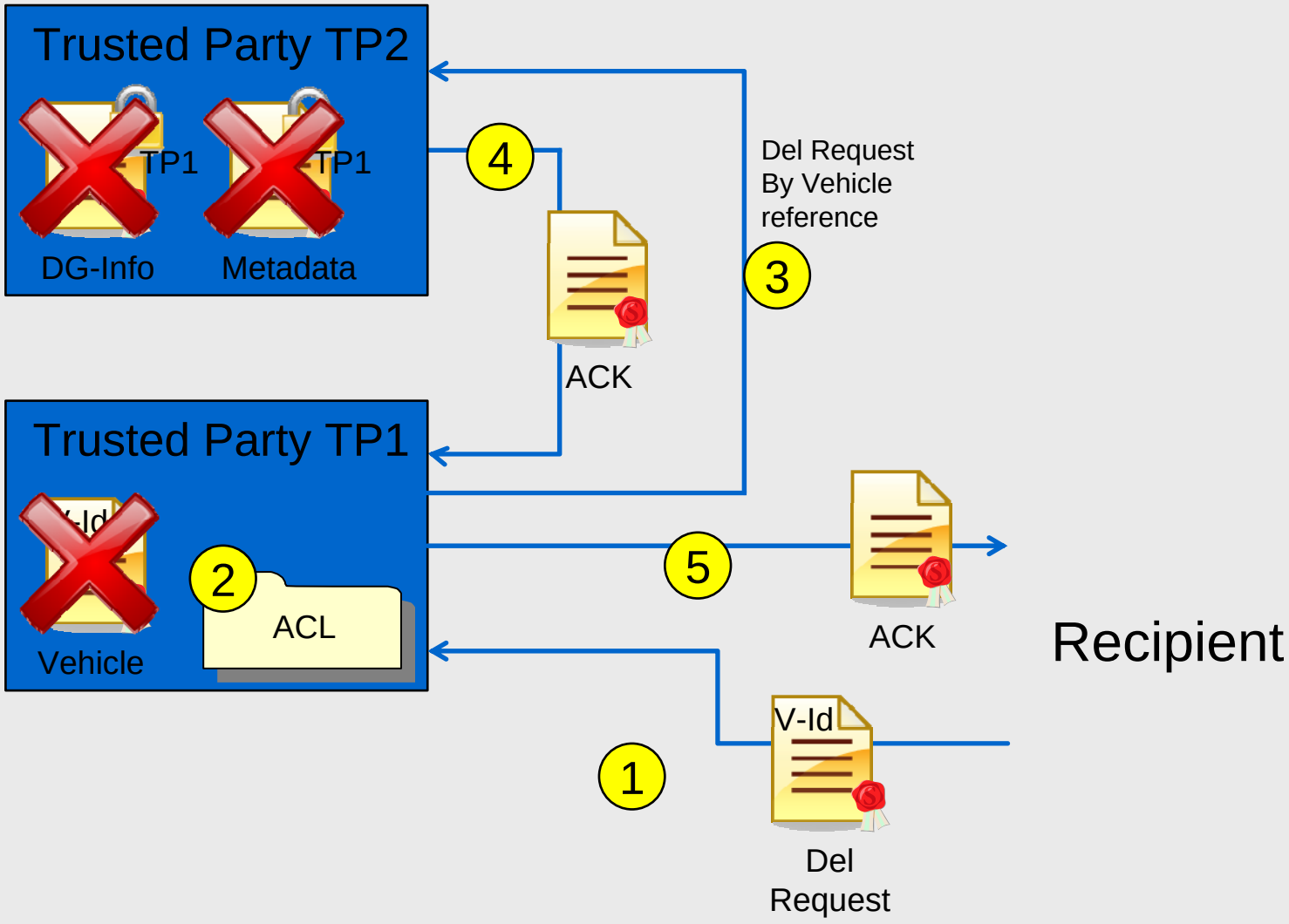


Data access via command&control center

1. After entering the vehicle ID Handheld sends a message with this ID to Control Center over an proprietry interface (no standardisation required!)
2. The Control Center sends a signed message to Trusted Party 1 over a secure channel.
3. Trusted Party 1 checks the validity of the signature and proves by means of ACL the authorization of the Control Center.
4. In case of a valid request TP1 sends a data request to Trusted Party 2 via an authentic channel
5. TP 2 responses by sending the encrypted documents (DG data and metadata, if available) via an authentic channel to TP 2.
6. Trusted Party 1 decrypts the messages with its private key, checks the validity of the document signatures (which have been originated by the logistic planner) and submits data to the Control Center.
7. Optionally the signatures are validated by the Control Center. The Control Center submits the data to the handheld by proprietary formats and/or interfaces. Finally the handheld displays the relevant information in a suitable manner.

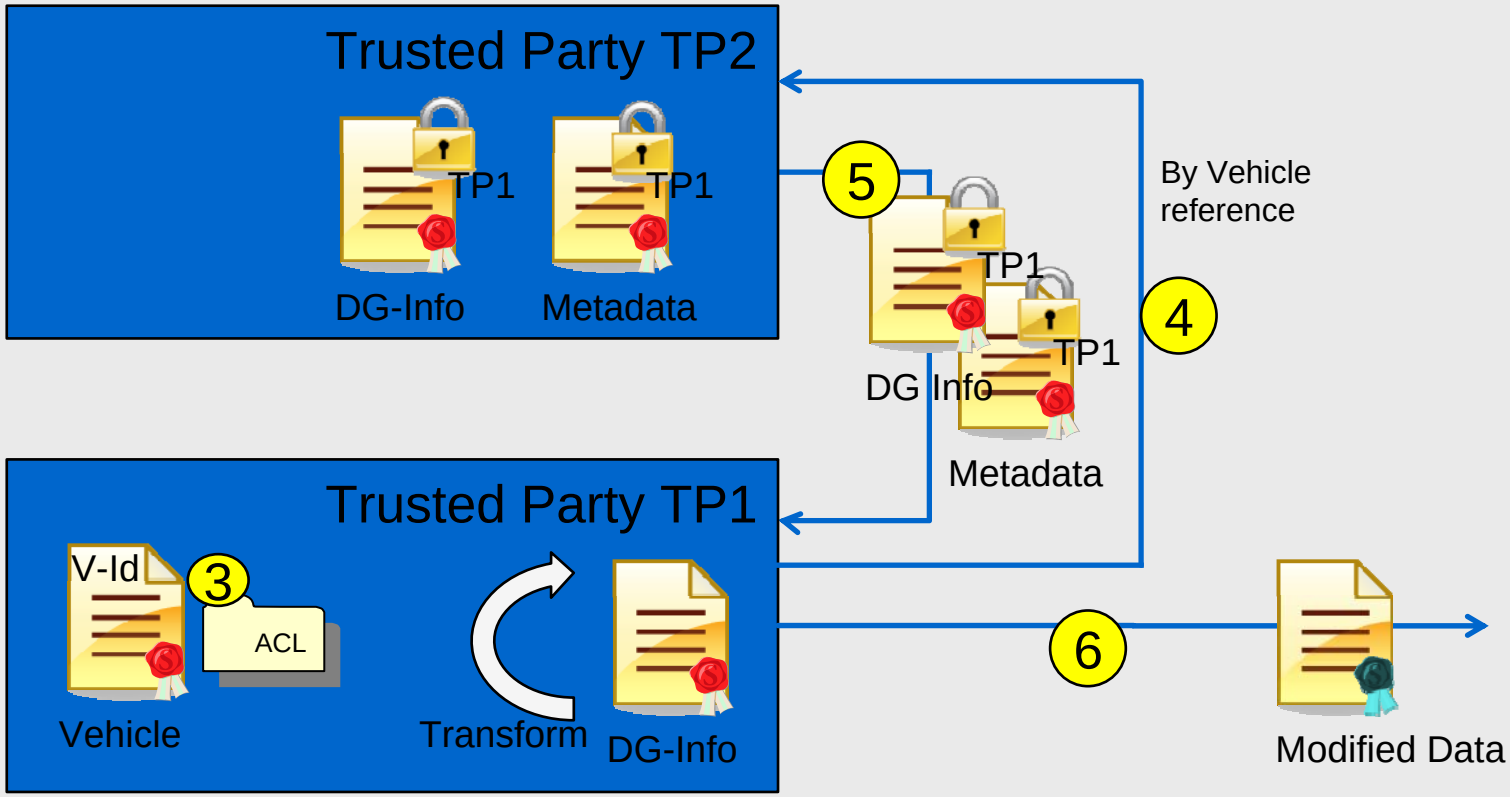
|otten|software|

Deletiing Data after Transport



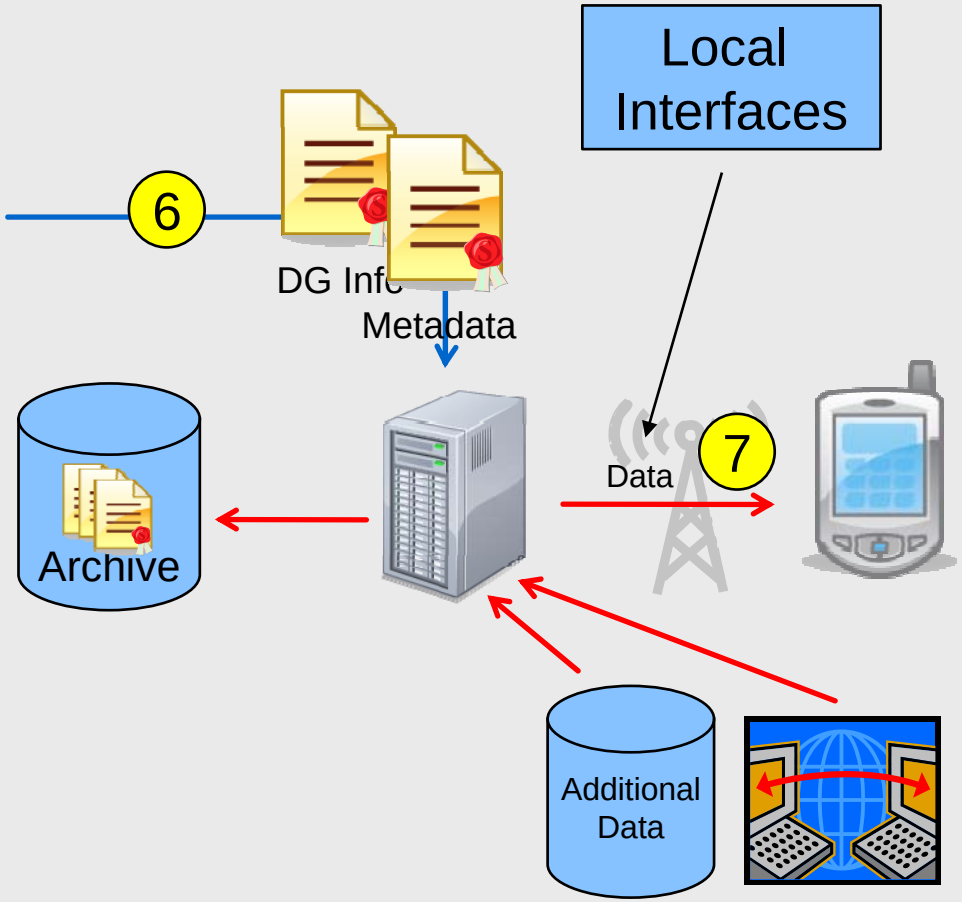
Extension of Scenarios 2 and 3

- Trusted Party 1 can transform (filter) the data delivered to handheld or control center, whenever the amount of information for a requesting party differs due to tthe ACL



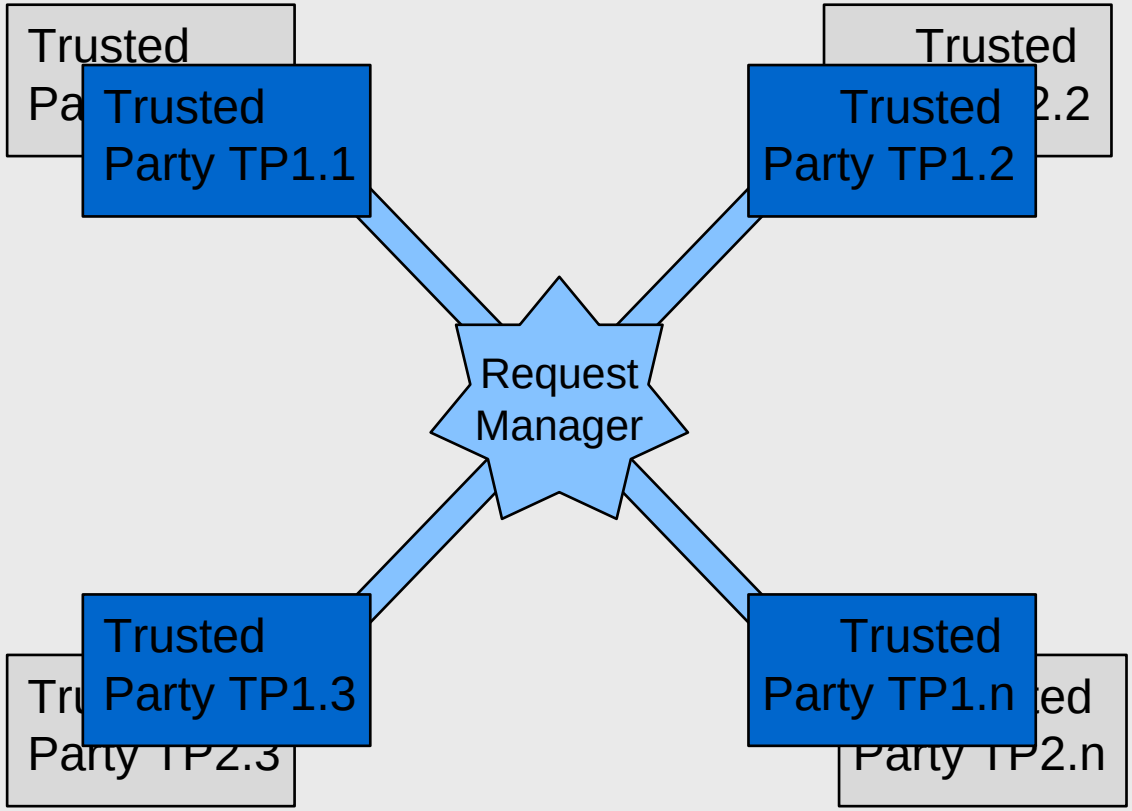
Extension of Scenario 3

- The Control Center can add further information to the DG Data (e. g. ERI Cards) before sending it to the handheld. Furthermore the data can be logged/archived for audits



Extensions of Scenarios 2 and 3

- As shown in other projects (e. g. EUCARIS) the Trusted Party 1 can be instatiated in several countries. Requests are distributed by a centralized Request Manager.



Extensions of Scenarios 2 and 3

- If desired data for tracking and tracing can be delivered by Trusted Party 2 (assuming the data is collected and sent by the OBU and data access is granted with respect to the ACL)