Prerequisites for cross-border internet-based use of the electronic Transport Document

Christian Lüpges

AlbrechtConsult GmbH

transport logistic - 05. Juni 2019

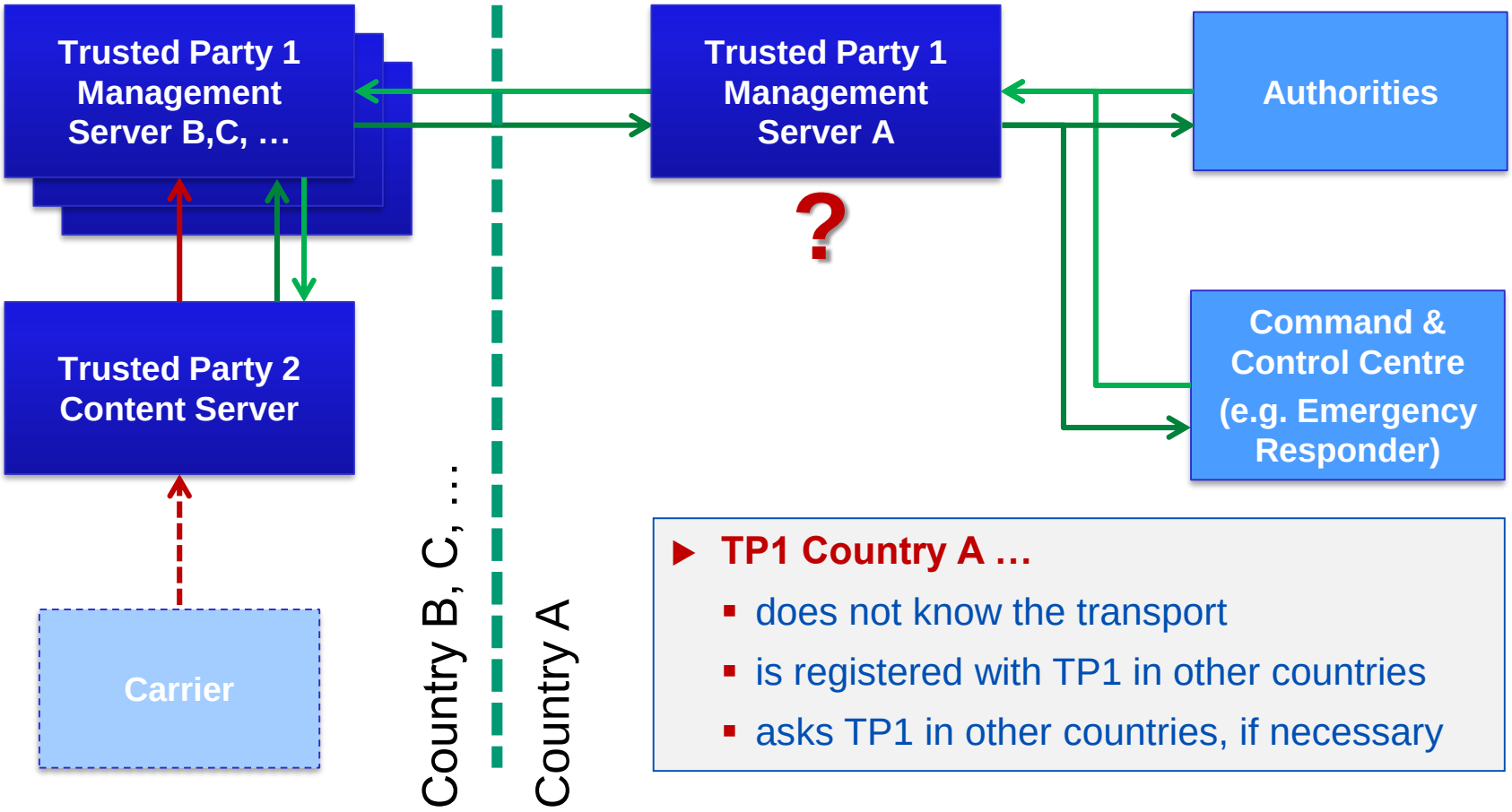
Overview

- **Basic principles – a short recap**
- **Requirements related to**
  - secure communication
  - interfaces
  - data
  - organisation
- **Impact on the federated system network**
- **Outlook: desired impact of the eFTI initiative**

Basic principles – a short recap

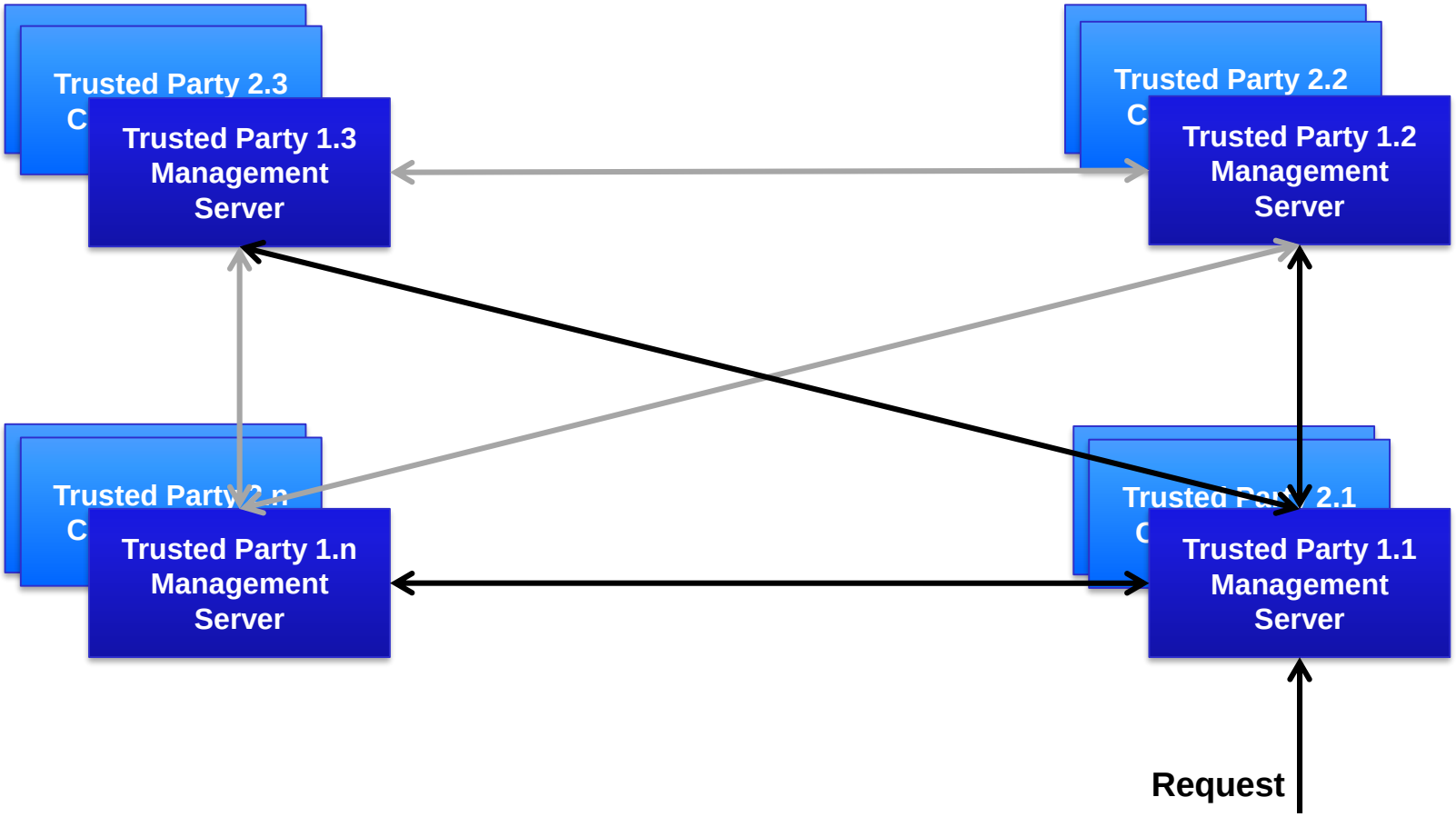
- **Regarding the implementation of the target architecture the question of the operator model of central management (TP1) arises.**
  - TP1 private or country driven / mixed forms
- **In the architectural concept, TP1 is logically a singular instance, but this does not mean that it must technically be implemented as a singular system with uniform operational sovereignty.**
- **It is also possible to implement central management as a federated (cross-border) service, where each TP2 is associated with exactly one TP1 instance**
- **The prerequisite, is that each instance of the service must know all other instances (for forwarding requests)**
- **Difference to central TP1 operation: The cooperation of many TP1 instances must be specified**

International data exchange



- **TP1 Country A …**
  - does not know the transport
  - is registered with TP1 in other countries
  - asks TP1 in other countries, if necessary

Federated management
TP1 instances are known to each other



Requirements on secure communication (I)

- **Existing PKIs can be (re)used**
  - This implies a (logical) central registration of certificates and the roles/rights assigned to them
- **Access rights are managed explicitly as meta data and are not dependent on the content of the record (e.g. class)**
- **Certificates are used to encode the End-to-End transmission and to digitally sign the content**
- **Certificates are assigned to organizations, not individuals**
  - This has an impact on organizational processes and aspects, such as non-repudiation

Requirements on secure communication (II)

- **Elaboration of a Certificate and Security Policy**
  - Implementing a Trust List Manager (TLM) is a common IT security procedure for building trust systems.
    - As a central trusted instance, the TLM manages the list of qualified TP1 instances (Trust List) which are registered by the countries.
  - Definition of requirements on the accreditation of Root Certification Authorities
  - Operation of TP1 e.g. according to ISO/IEC 27001 and ISO/IEC 27005
- **Example:**
  - Delegated Act (to be adopted) for the deployment and operation of cooperative Intelligent Transport Systems and Services (C-ITS)

Requirements on interfaces

- **The service interfaces are formally specified (e.g. WSDL & XSD) to support the development of interoperable software components**
  - In the case of Web Service development, it means "WSDL-first"
- **In terms of interfaces specification, interfaces for self-inspection are provided, which enable migration paths for future extensions / changes**

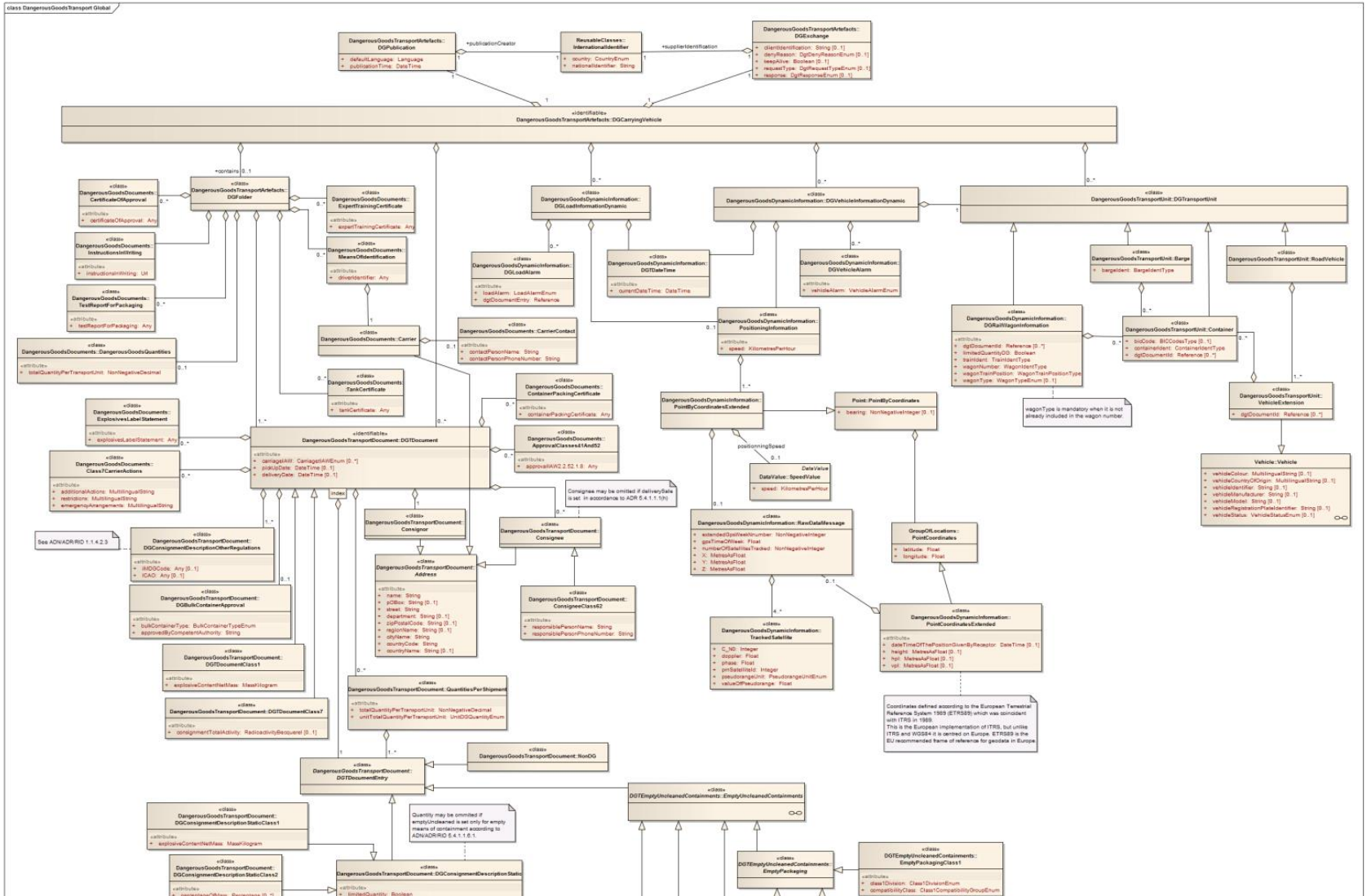
- **Expansion of interface specifications by federated TP1 services**
  - Distribution of a request to all other TP1 instances (broadcast), if the transport on the first requested TP1 is not known.
  - Acceptance and Processing of the Response

Data requirements (I)

- **Access only with contextual information (e.g. license plate, ...) - " random Observer“**
- **Access with the Vehicle Identification Number (VIN) - e.g. electronic Emergency Call**
- **Access to the Backoffice-System should provide the full dangerous goods data record**
  - In particular, it is not sufficient to build reference chains to other Systems
- **The data record should apply the (carrier-specific) structural principles that are currently also used for paper documents**

- **Validation of the previously submitted dangerous goods data model**
  - Transform the DATEX II DG data model into the new Version 3
- **Knowledge of the service access points of the other TP1 instances in the federal system network**

Data requirements (II)
Dangerous goods data model



Requirements on the organisation (I)

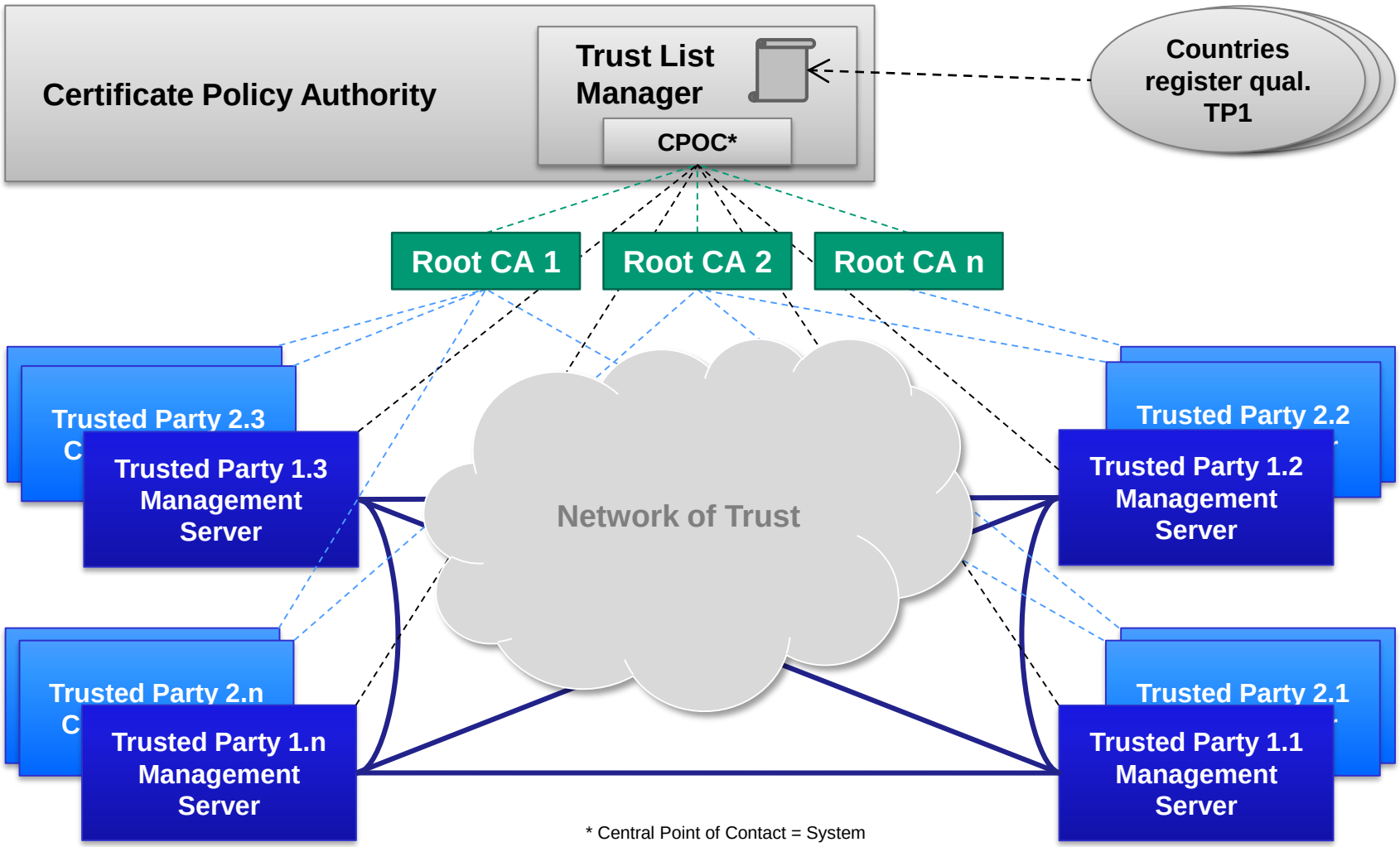
- **No requirements for authorities or emergency forces**
- **Special networks / VPNs (e.g. Testa) are not prescribed - the effects of communication via the general Internet are taken into account in the definition of the security architecture**
- **Interoperability of services should be certified to ensure successful access**
- **The service level of the TP2 services is not constantly monitored**
  - The legal situation remains the same as for the paper document
  - Irrespective of this, recommendations for meaningful service levels based on international standards are to be made

Requirements on the Organisation (II)

- **TP2 instances must be registered at the TP1 instances**
  - in the case of a federal management service, registration with one instance is sufficient

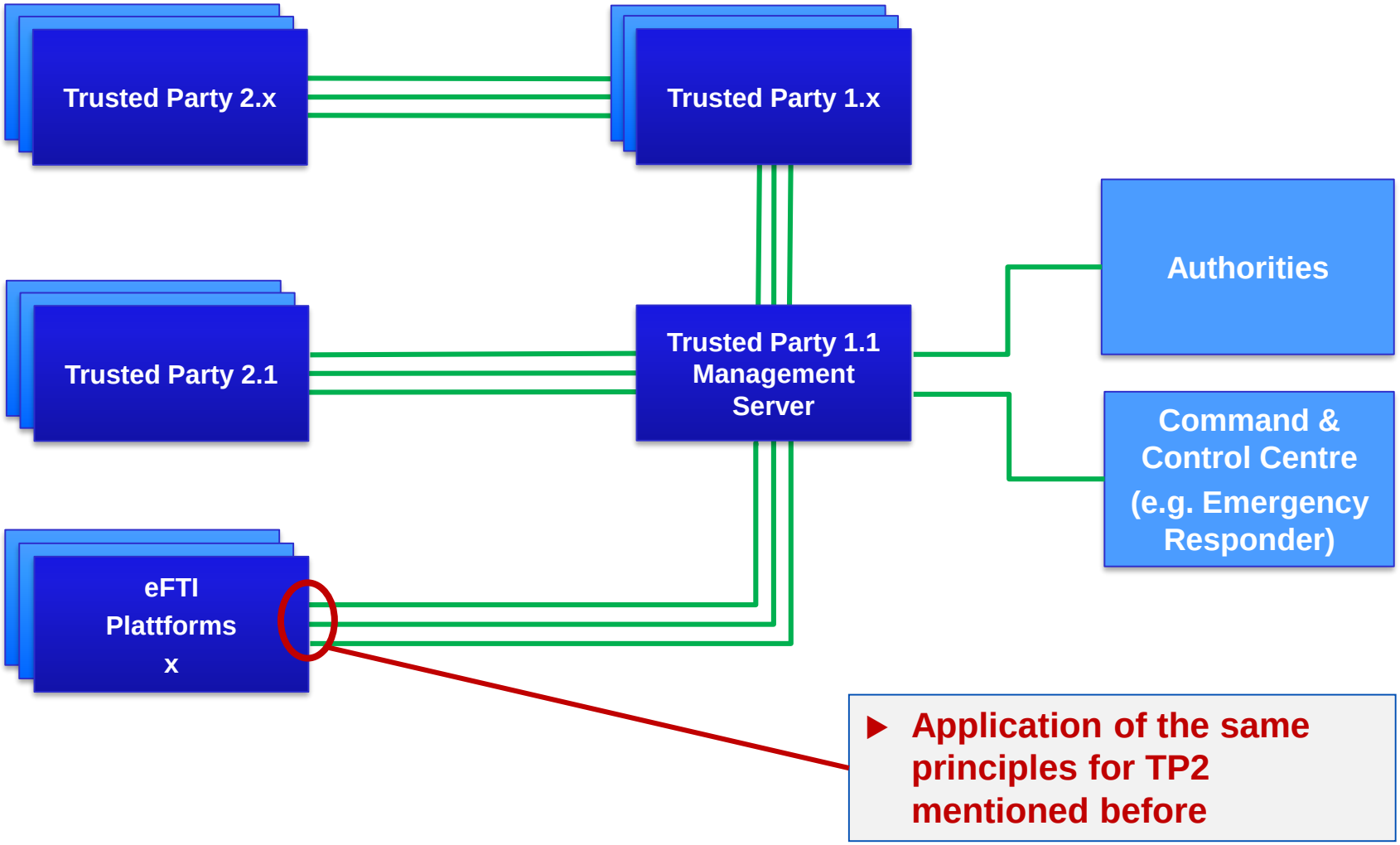
- **Establishment of a trust system of qualified TP1 instances**
  - Definition of a common method for the release of qualified TP1 instances
  - National release of qualified TP1 for federal operation
    - Certification e.g. of high availability, security, authenticity and interoperability
    - Observance of defined Service Level Argreements (SLA)
- **Establishment of a process for the maintenance of technical documentation**

Impact on the federated system network



* Central Point of Contact = System

Outlook: desired impact of the eFTI initiative



Thank you for your attention!

Christian Lüpges

AlbrechtConsult GmbH

Contact:

Tel: +49 241 446 89 708

Fax: +49 241 500 718

Christian.Luepges@albrechtconsult.com