PLATTFORM INDUSTRIE 4.0

Secure Retrieval of CAE-Data

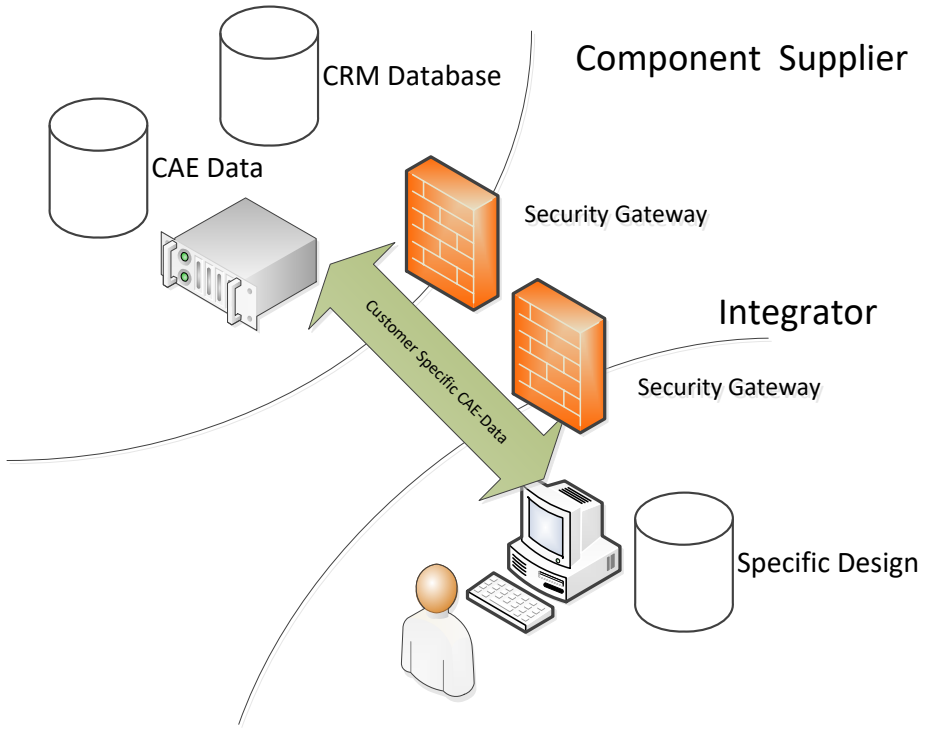
Dr. Lutz Jänicke

Phoenix Contact and Member of the German Plattform Industrie 4.0

January 27, 2021

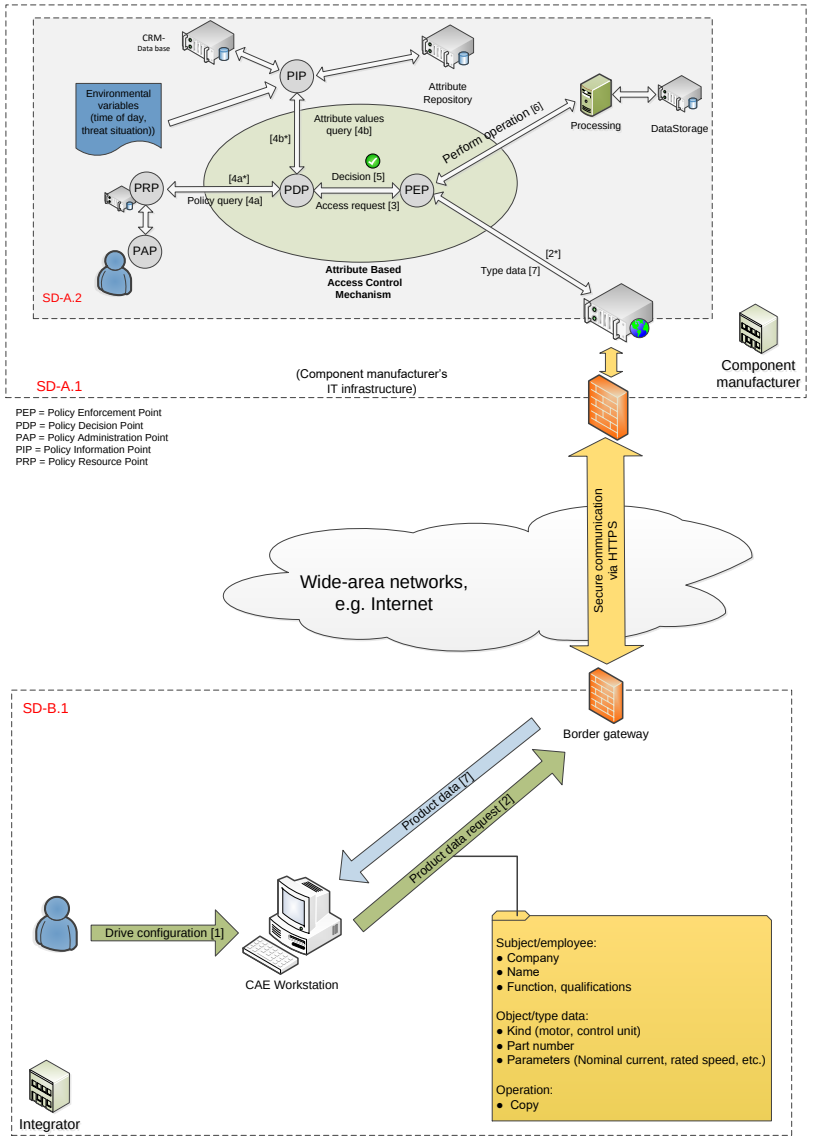
Introduction: The Challenge

- Today CAE-Data
  - are provided as part of a collection or by download
- In the future CAE-Data
  - will be retrieved on demand
  - will be retrieved automatically by tools
  - will need to be provided such that integrity and authenticity can be verified
  - may need to be provided on a per-customer base
- Therefore
  - Communication protocols need to be secure
  - Authentication needs to be automatic and scalable
  - Data in transit and at rest need to be protected against manipulation (and disclosure if needed)



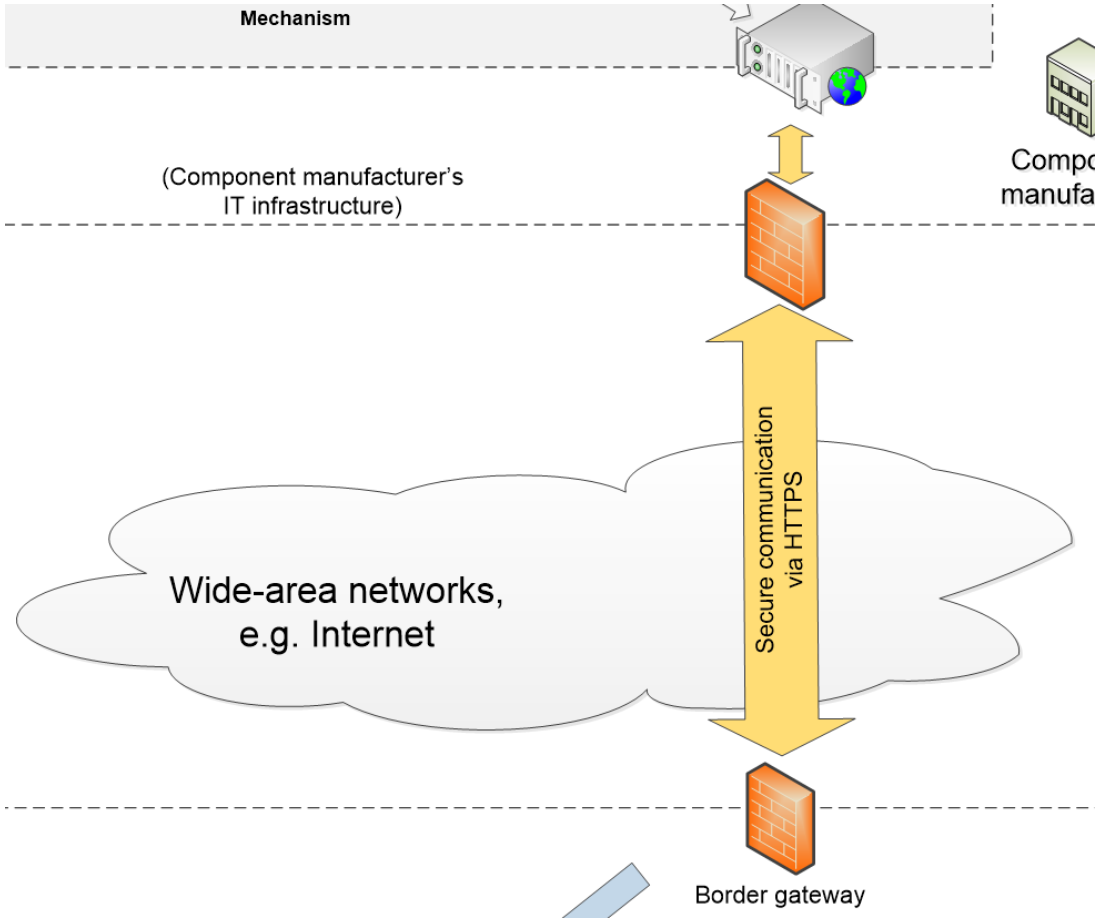
Deeper View into Security Domains

- Multiple stakeholders are involved
  - Component supplier (SD-A)
    - IT-Infrastructure services (SD-A.2)
    - CAE-data provider (SD-A.1)
  - Integrator (SD-B)
    - IT-Infrastructure services (SD-B.1)
    - CAE-user and workstation
- Each security domain is intended to protect its own assets
  - Security measures are limiting communication protocols including filtering web-gateways
    - End-to-end security may be blocked
  - User and system authentication between security domains is not synchronized



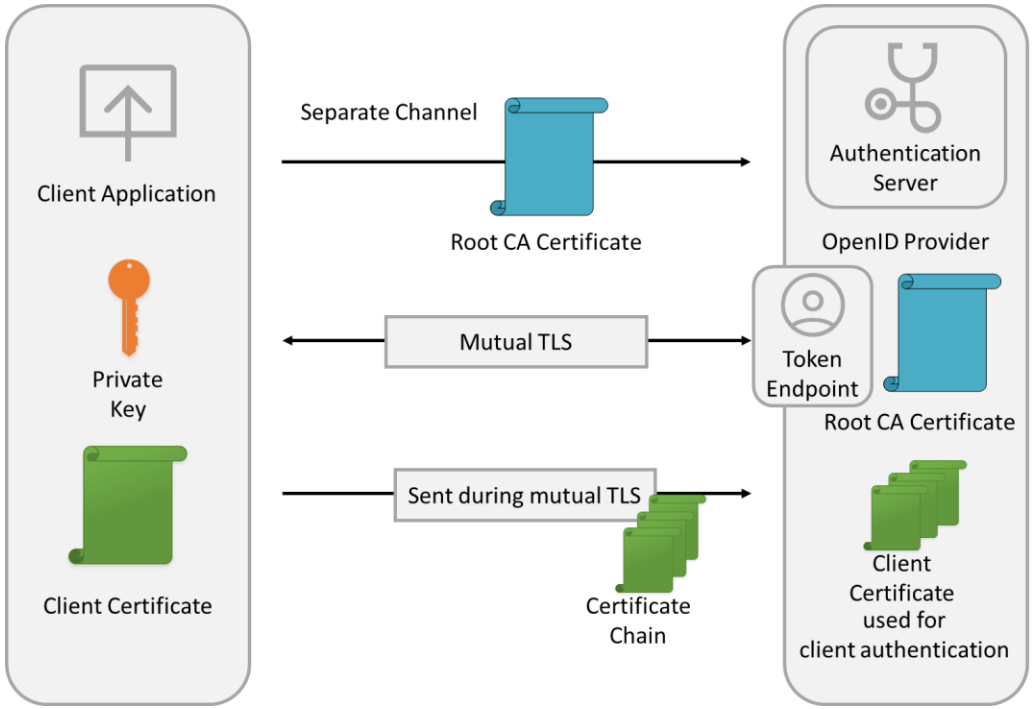
Discussion of Solution Proposal: HTTPS/REST

- Communication shall use the most interoperable protocol
  - HTTP(S) is the most supported protocol in the Internet
  - HTTPS/REST is established providing Web-services
  - HTTPS/REST is often used with authentication tokens
- Limitations
  - TLS (as basis of HTTPS) is often broken in security gateways
    - No mutual TLS authentication possible
    - End-to-end security not provided



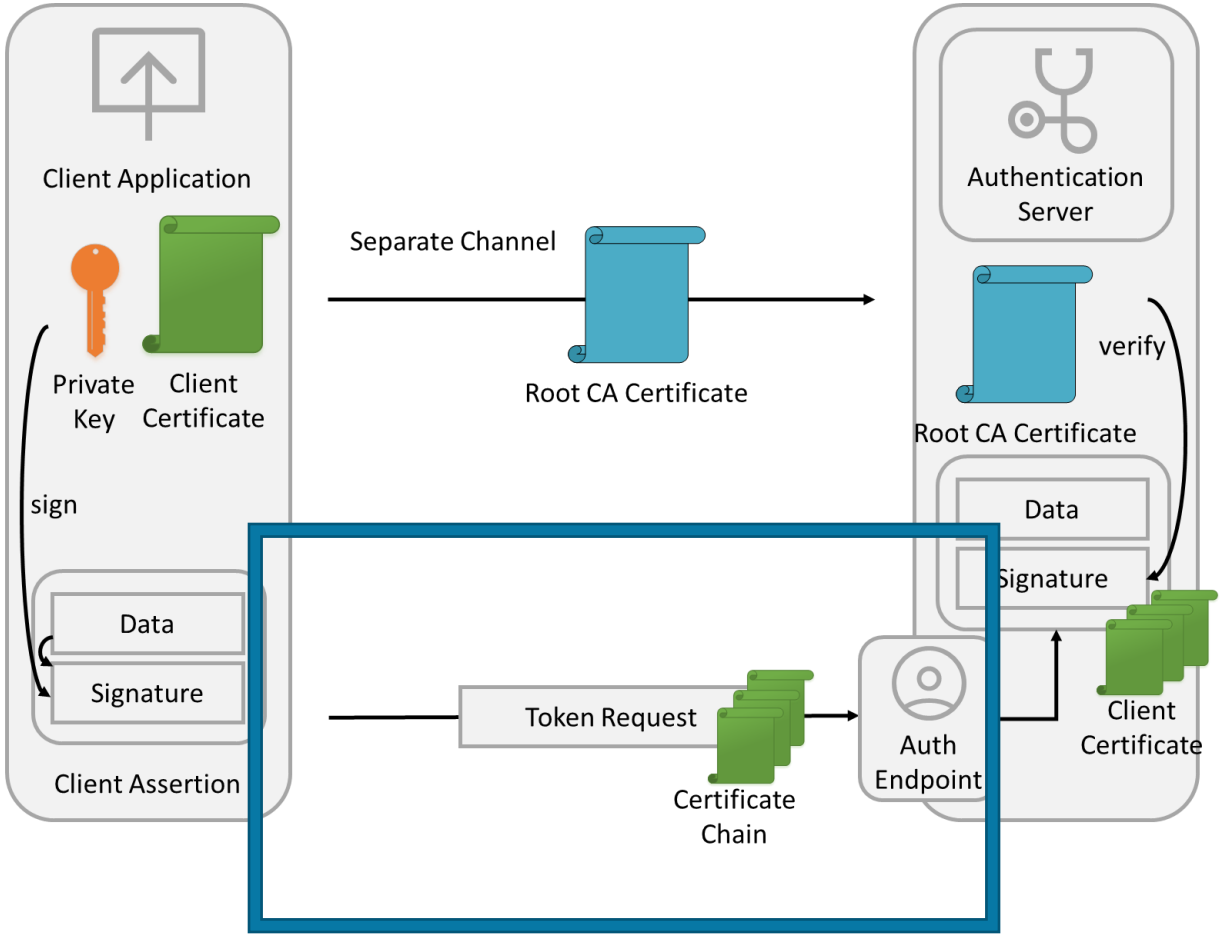
Discussion of Solution Proposal: Authentication via X.509 certificates

- B2B: Proper identification of peers is needed
- Password based authentication is neither secure nor scalable
- Authentication via X.509 certificates is scalable
- Mutual TLS authentication using X.509 certificates cannot be used with filtering Web-gateways



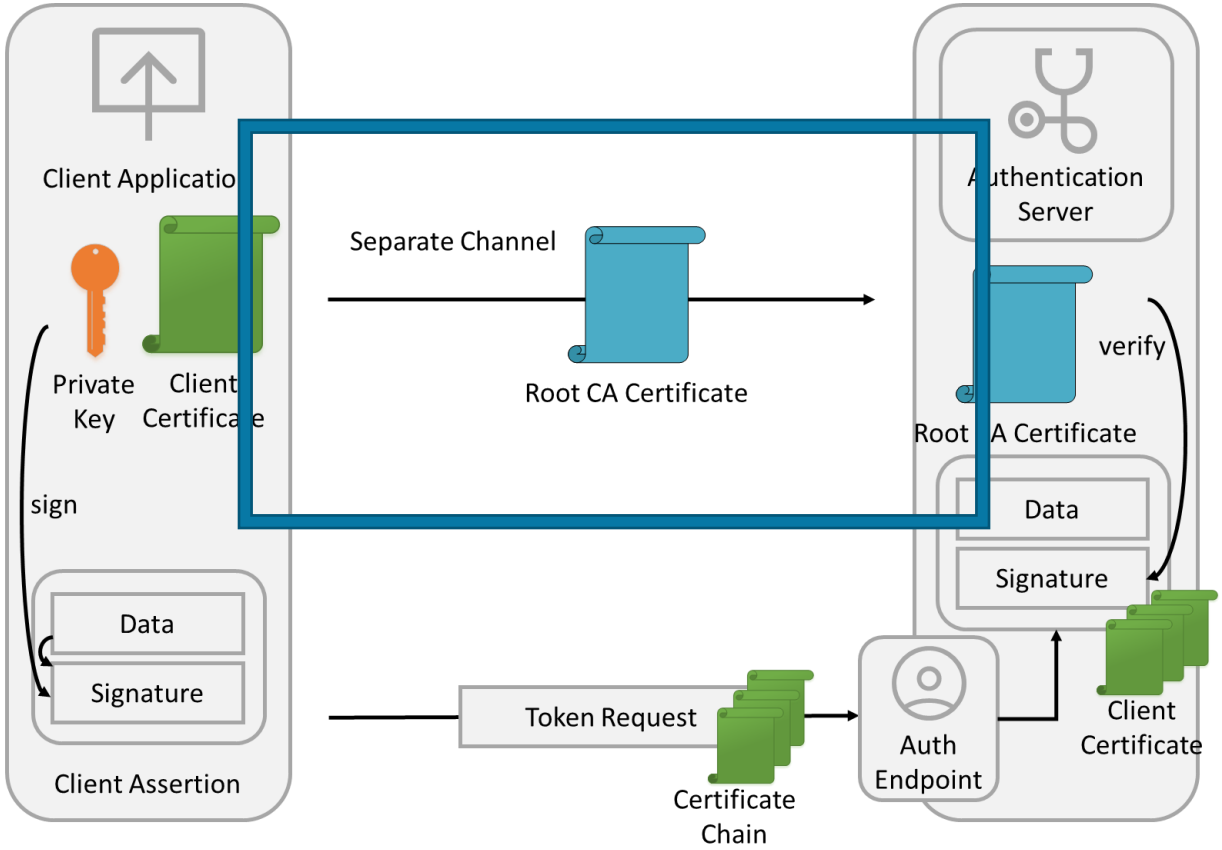
Discussion of Solution Proposal: Authentication at Application Level

- Authentication via X.509 certificates should be performed at application level
- Cryptographic handshake might be performed with JSON Web Tokens (JWT) that support all mechanisms needed
- This solution is compatible with filtering web proxies

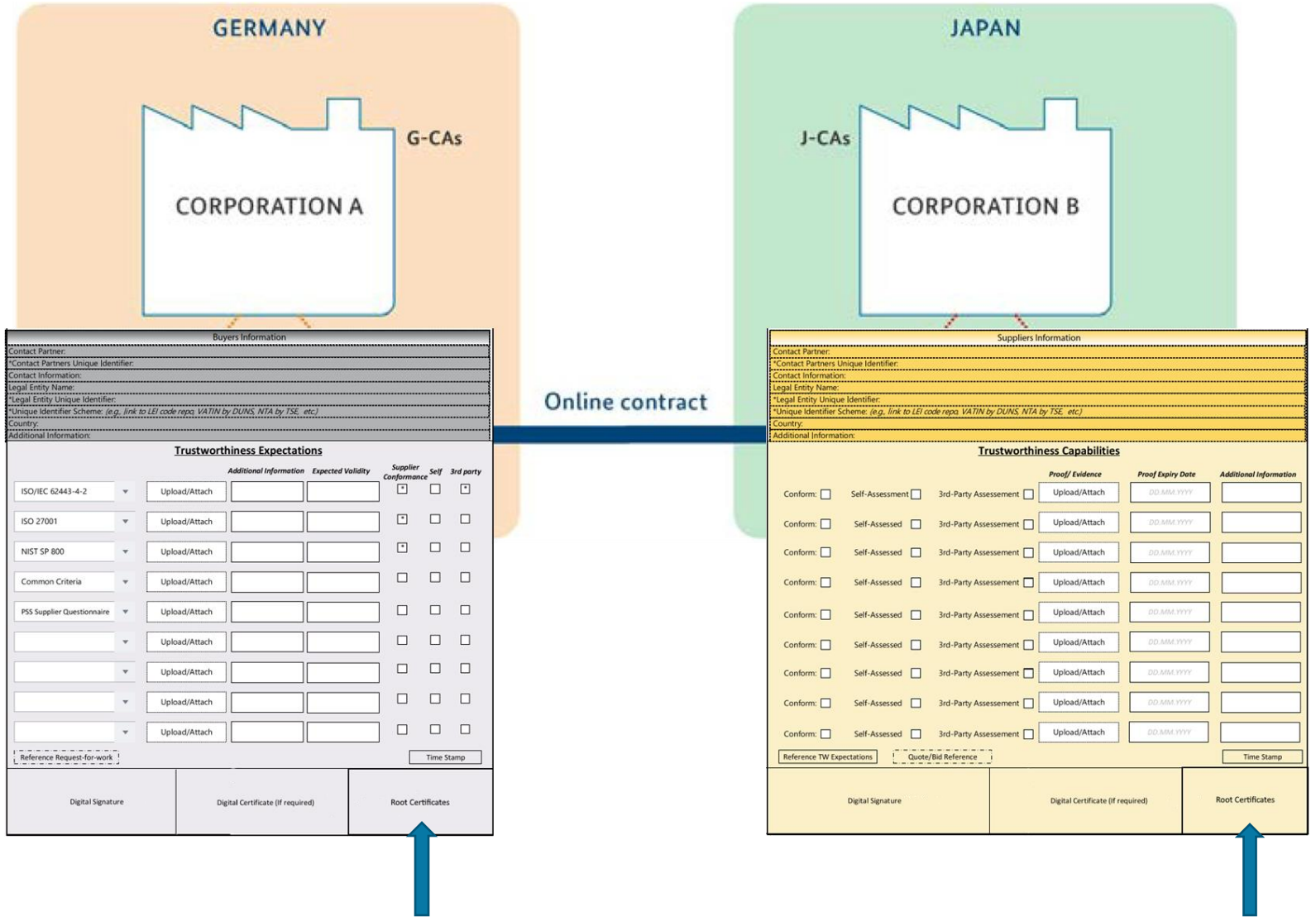


Discussion of Solution Proposal: Mutual Trust Relationship

- Authentication via X.509 certificates requires mutual trust of Certification Authorities
- Identity providers may issue X.509 certificates to partners for the purposes supported
  - E.g. download of CAE-data
- More scalable:
  - Companies trust each others' internal identity processes and infrastructure

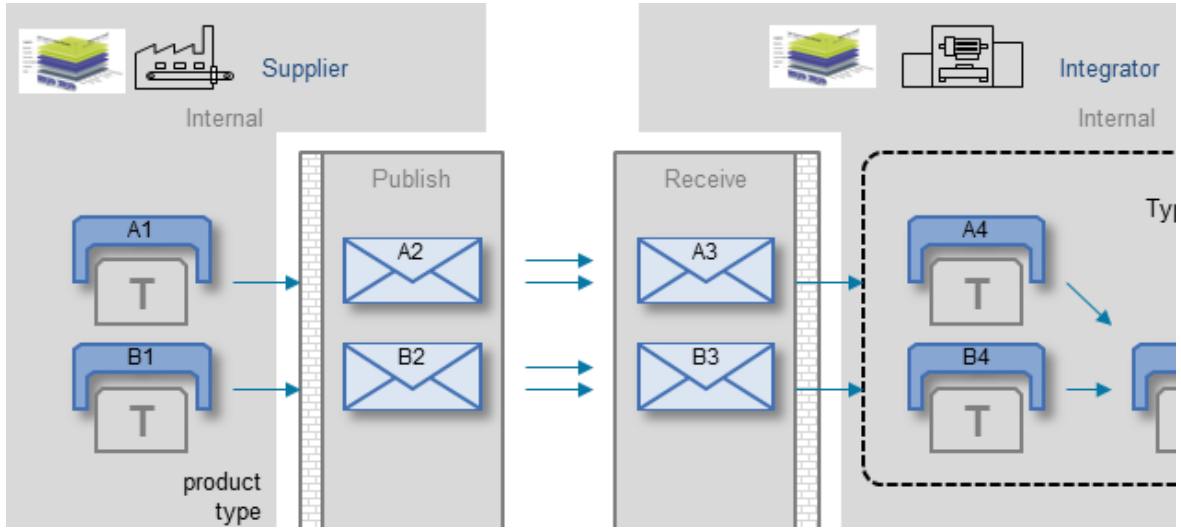


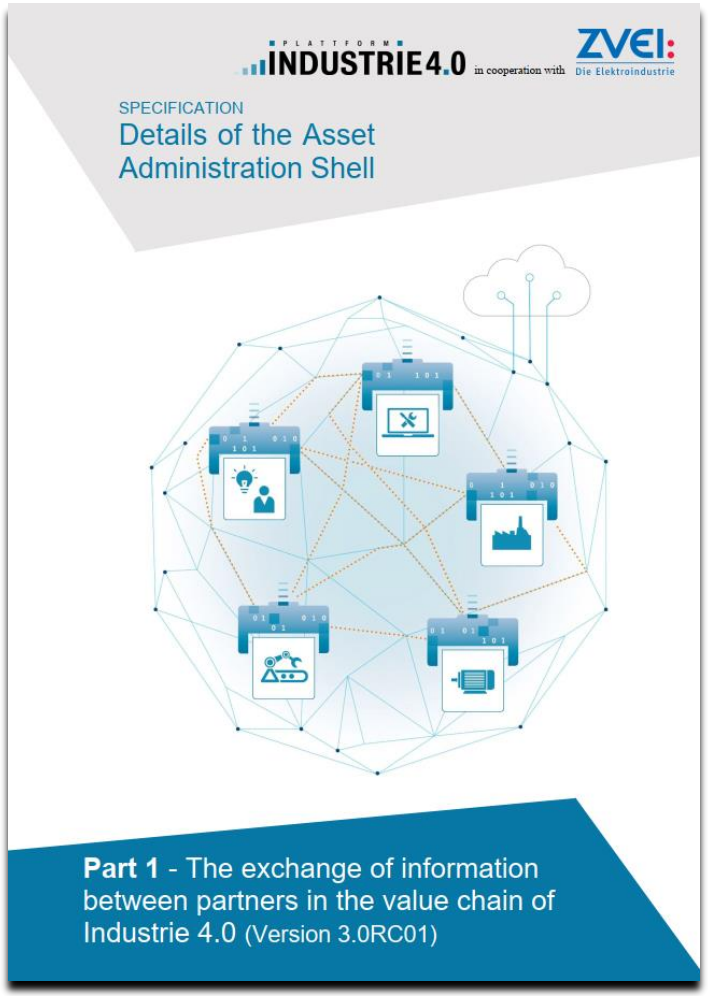
Discussion of Solution Proposal: Trustworthiness Protocol



Discussion of Solution Proposal: Data at Rest (File Formats)

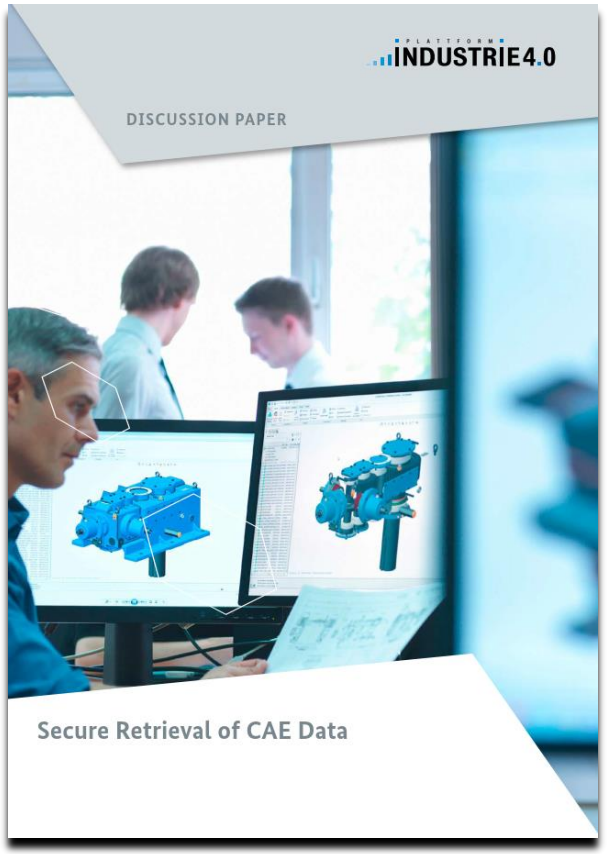
- The concept proposed addresses the communication process (data in transit)
- The security of the data at rest (file formats exchanged) will be addressed in future work
- The file format proposed (.AASX) is based on the Open Packaging Conventions (ISO 29500)

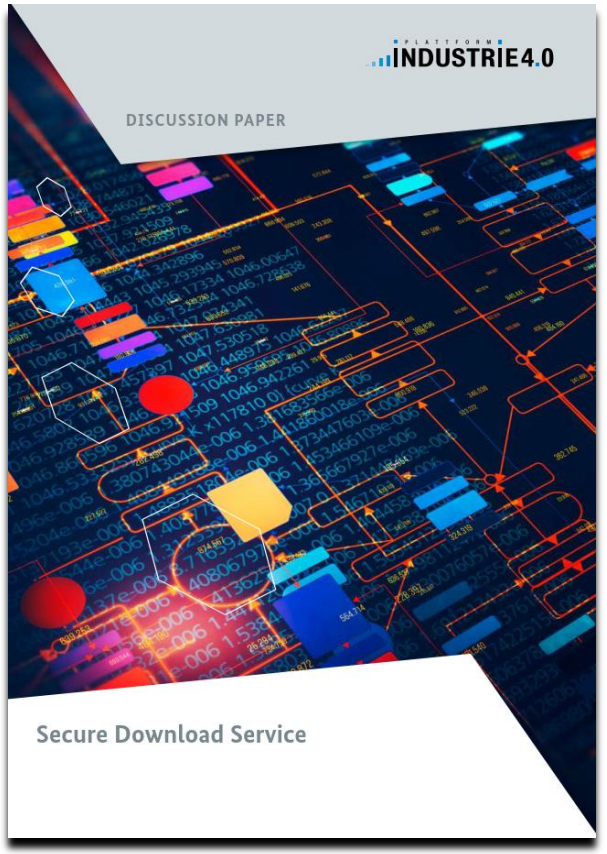




Summary and Outlook

- A secure concept for the retrieval of CAE-data “on demand” has been developed
- Scalable and usable authentication methods have been proposed
- Demonstrator available via AASX-Package-Explorer
  - https://admin-shell-io.com/screencasts/ Section “Security”
  - Technical Presentation “Implementing certificate based authentication on application level”
- Security concepts for the CAE-data at rest needs to be further developed





Plattform Industrie 4.0 - Secure Retrieval of CAE Data (plattform-i40.de)

Plattform Industrie 4.0 - Discussion Paper: Secure Downloadservice (plattform-i40.de)

Thank you very much!

Dr. Lutz Jänicke
Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg

ljaenicke@phoenixcontact.com

+49 1516 5213337

Plattform Industrie 4.0
Contact the Secretariat

Plattform Industrie 4.0
Secretariat

Bülowstraße 78, 10783 Berlin
Tel.: +49 30 2759 5066-50
geschaeftsstelle@plattform-i40.de
www.plattform-i40.de