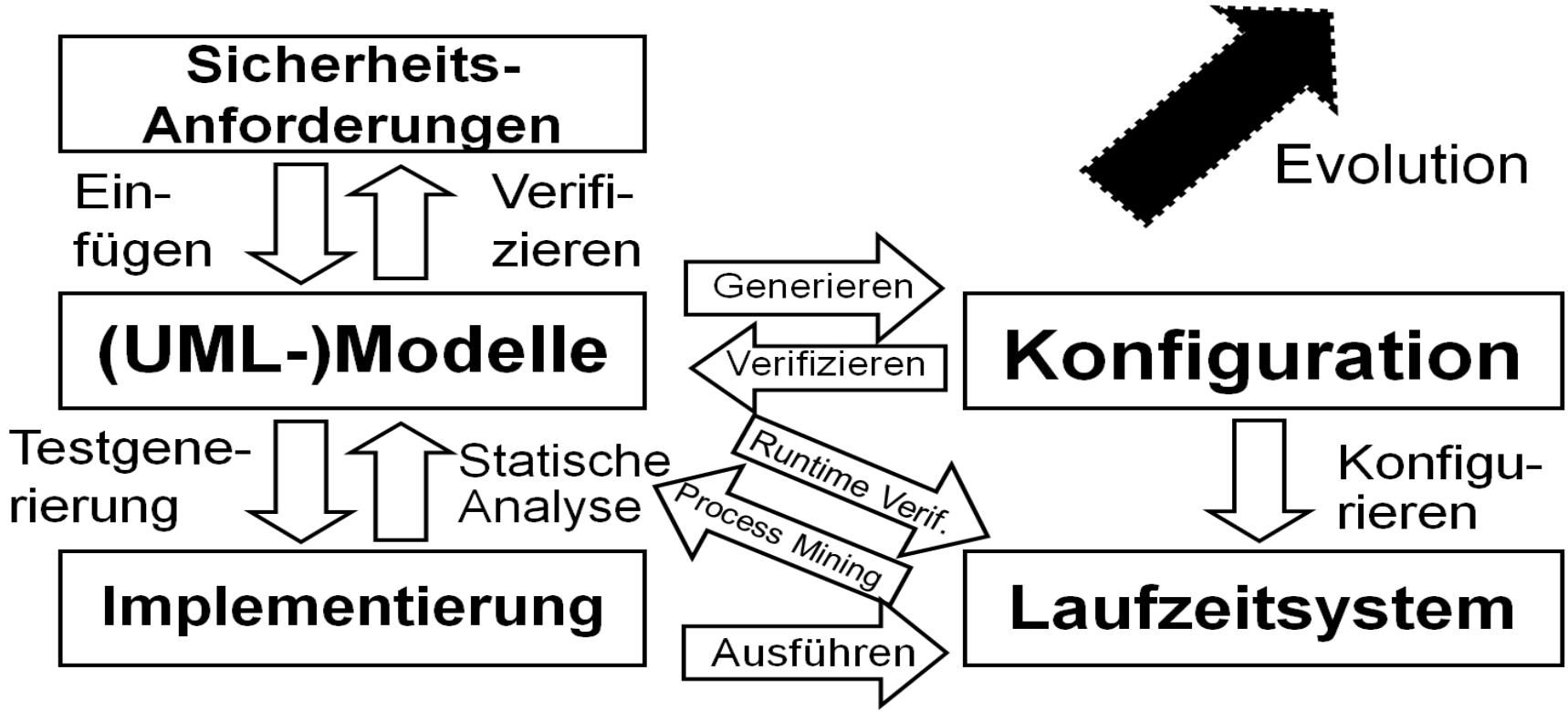
SECURITY BY DESIGN FÜR CLOUD-BASIERTE DATENAUSTAUSCHPLATTFORMEN: DER INDUSTRIAL DATA SPACE

Prof. Dr. Jan Jürjens

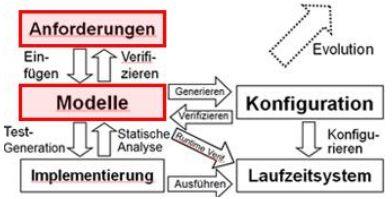
Director Research Projects, Fraunhofer-Institute for Software and Systems Engineering ISST (Dortmund)
Compliance Innovation Lab, Fraunhofer Innovation Center for Logistics & IT FILIT (Dortmund)
Director, Institute for Software Engineering IST, University Koblenz-Landau (Koblenz), Germany

Fraunhofer

Security-by-Design



Security-by-Design mit UMLsec



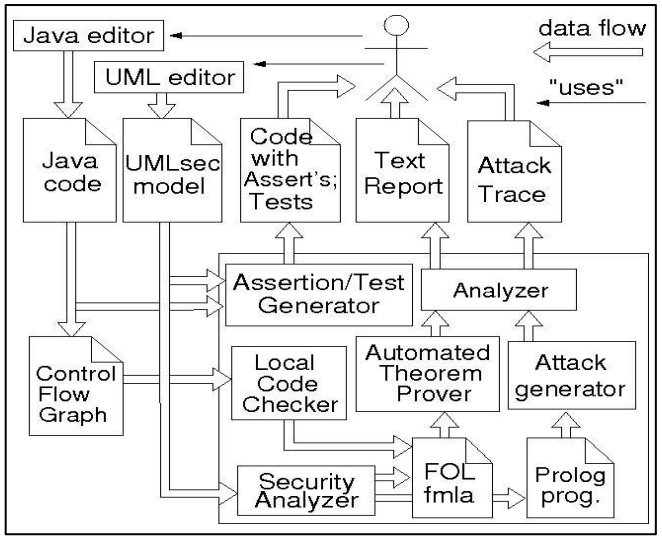
UMLsec: UML-Erweiterung für **Dokumentation** und **automatische Überprüfung** von Sicherheitsanforderungen.

[http://carisma.umlsec.de]

Anforderungen als **Annotationen** in UML-Modell.

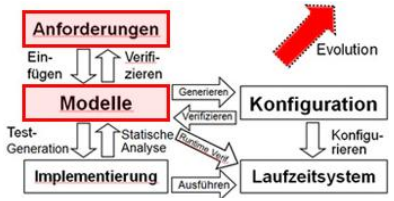
Automatische Überprüfung der Modelle und Implementierungen gegen Anforderungen.

Werkzeugplattform CARiSMA (open-source, integriert in Eclipse).



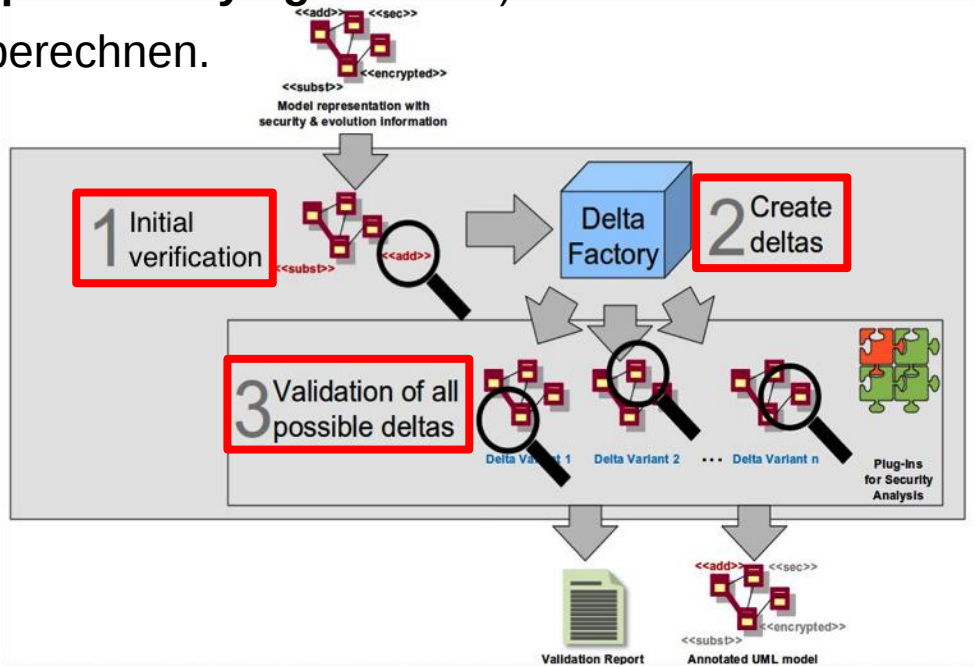
[Jürjens: **Secure systems development with UML**. Springer 2005. Chines. Übers. 2009]

Evolutions-basierte Sicherheitszertifizierung



- Erstmalige Analyse: Registrieren, welche **Softwareteile relevant**.
- Teilresultate in Modell speichern („**proof-carrying models**“).
- **Differenz**: altes zu neues Modell berechnen.
- Nur die **Systemteile reverifizieren**, die
  1) in der initialen Analyse relevant,
  2) **geändert** wurden, sodass
  3) o.g. Bedingungen **nicht erfüllt**.

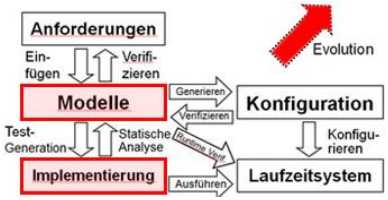
➔ Erheblich **weniger Aufwand** als komplette Reverifikation.



[Wenzel, Warzecha, Jürjens, Ochoa. **Specifying Model Changes with UMLchange to Support Security Verification of Potential Evolution**. Journal of Computer Standards & Interfaces, 2014]

Fraunhofer

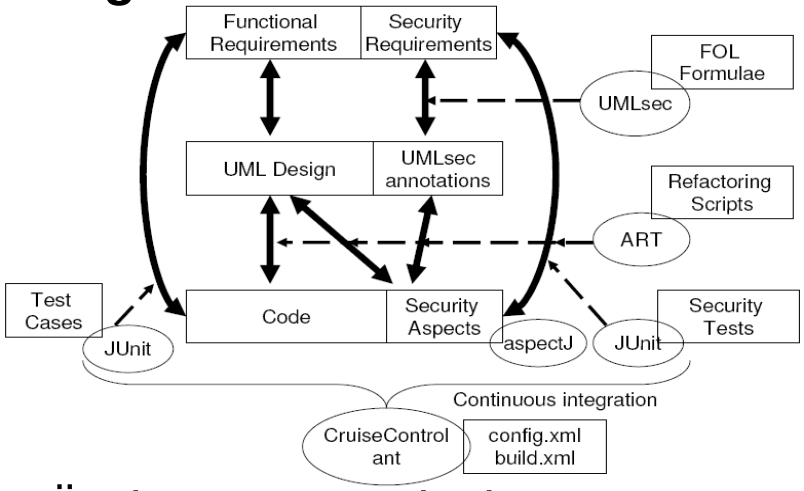
Nachverfolgbarkeit der Sicherheitsanforderungen bei Evolution



- **Ziel: Nachverfolgbarkeit** von **Anforderungen** vs. **Implementierung** bei **Evolution**.

Lösung: Änderungen reduzieren auf:

- Hinzufügen / Entfernen von Systemteilen.
- Grundlegende Refactoring-Operationen.



➔ **Automatische Nachverfolgbarkeit** der Änderungen zwischen Modell und Implementierung mit **Refactoring Scripts** (Eclipse).

[Bürger, Jürjens, Wenzel. **Restoring Security of Evolving Software Models using Graph-Transformation**. In: International Journal on Software Tools for Technology Transfer (STTT), 2015]

Notwendigkeit für Datenaustauschplattformen: Kombination von Daten im »Ecosystem«

INDUSTRIAL DATA SPACE

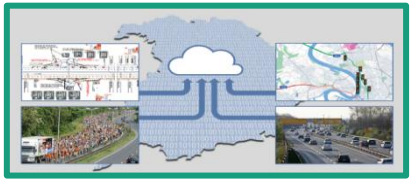
Pharma

Personalisierte Medizin

»Ökosystem«:
- Pharmazeutische Industrie
- Gesundheits-dienstleister
- Ärzte

Daten:
- Gesundheitsdaten
- Therapiedaten

Automobil



Verkehrsmanagement 2.0

»Ökosystem«:
- Automobilhersteller
- Verkehrszentralen
- Kommunen

Daten:
- Lokation, Ziel
- Fahrzeugdaten
- Verkehrsdaten

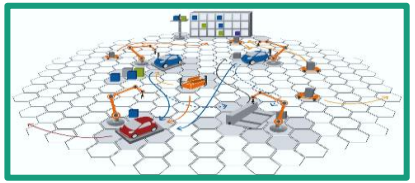
Handel

Transparente Lieferkette

»Ökosystem«:
- Einzelhandel
- Konsumgüter-industrie
- Logistikdienstleister

Daten:
- EPCIS-Ereignisse
- Transportdaten
- Zustandsdaten

Produktion



Industrie 4.0

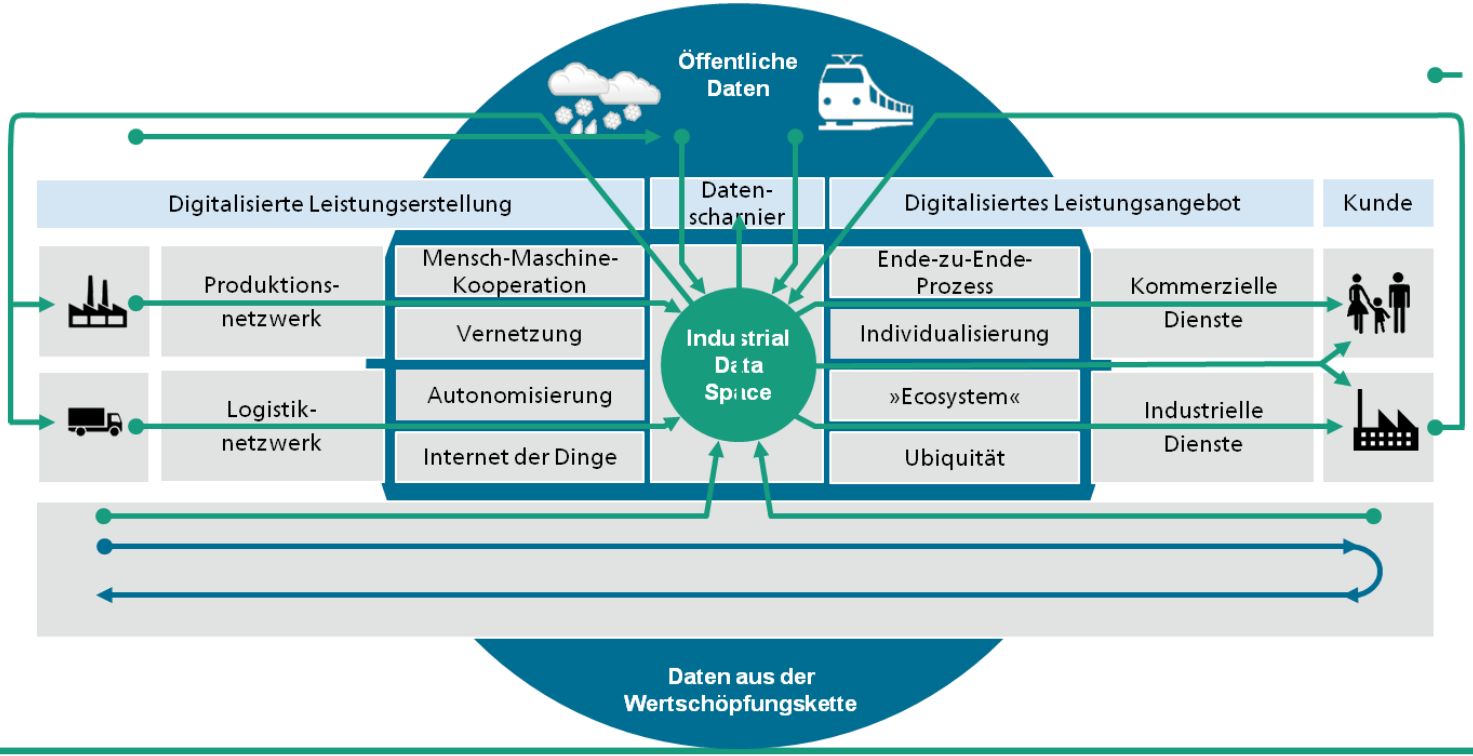
»Ökosystem«:
- Automobilhersteller
- Zulieferer
- Logistikdienstleister

Daten:
- Produktdaten
- Planungsdaten
- Zustandsdaten

Bildquellen: Microsoft, BMW, Databirds, SmartFace. Legende: EPCIS - Electronic Product Code Information Services.

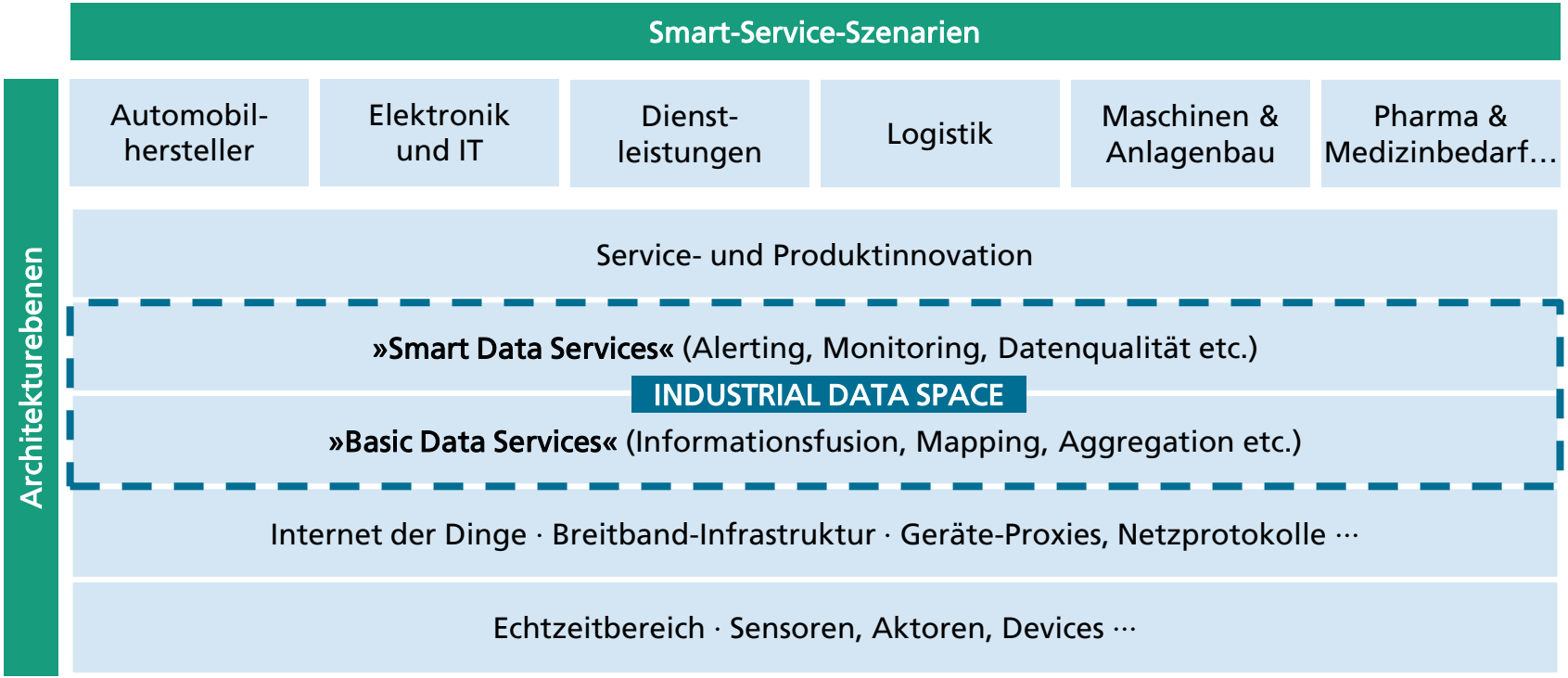
Fraunhofer

Der Industrial Data Space als Bindeglied zwischen digitaler Produktion / Logistik und Smart Services

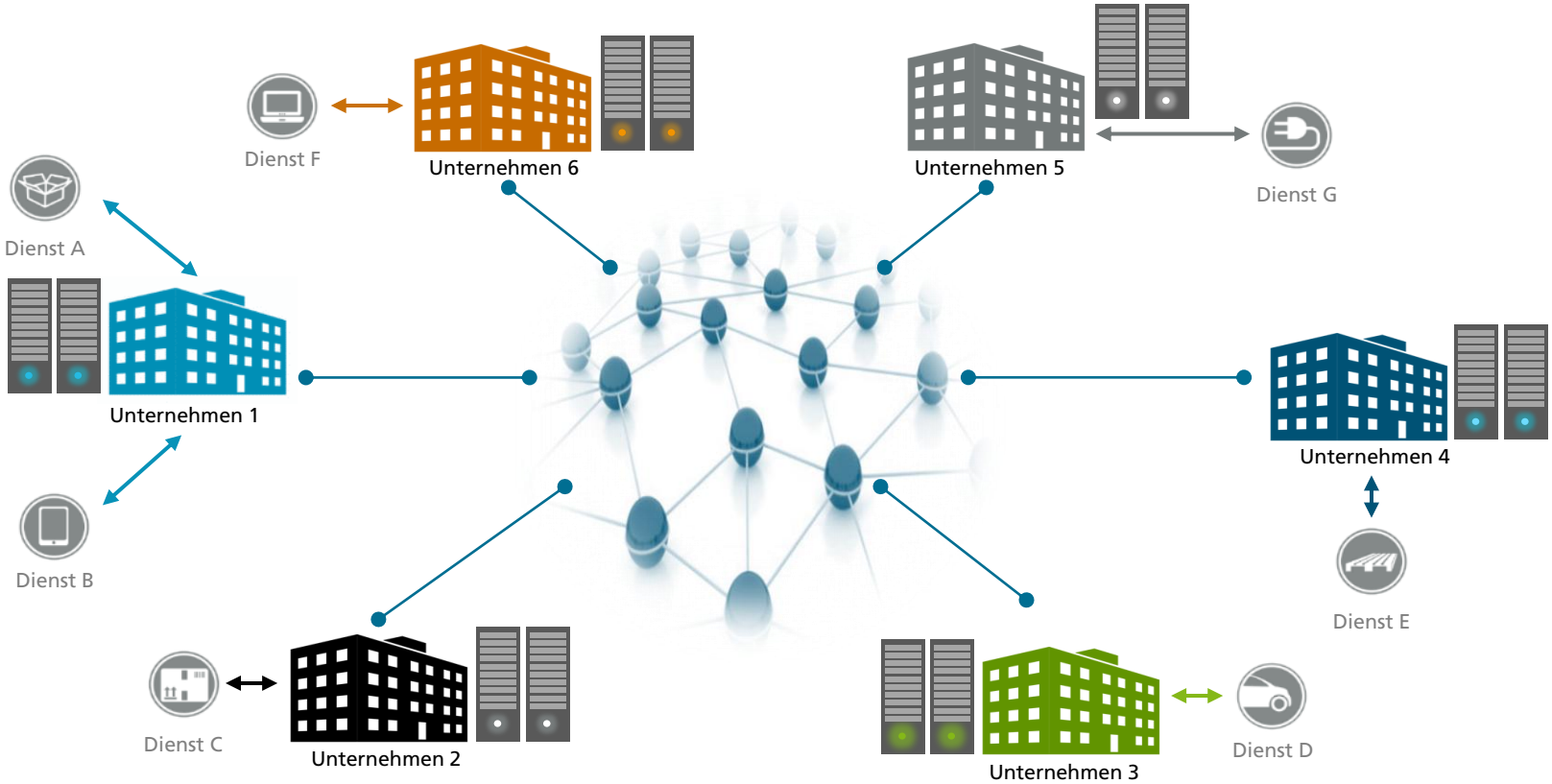


Legende: Informationsfluss Güterfluss.

Industrial Data Space:
Von Internet of Things zu Smart Services



Industrial Data Space: Grundlegende Struktur



Der Industrial Data Space ermöglicht ein »Network of Trusted Data«

Dezentralität
Föderale Architektur

Souveränität
über Daten und Dienste

Vertrauensschutz
zertifizierte Teilnehmer

Sicherheit
Datenaustausch

Offenheit
Neutral und
anwendergetrieben

Governance
Gemeinschaftliche
Spielregeln

Skalierung
Netzwerkeffekte

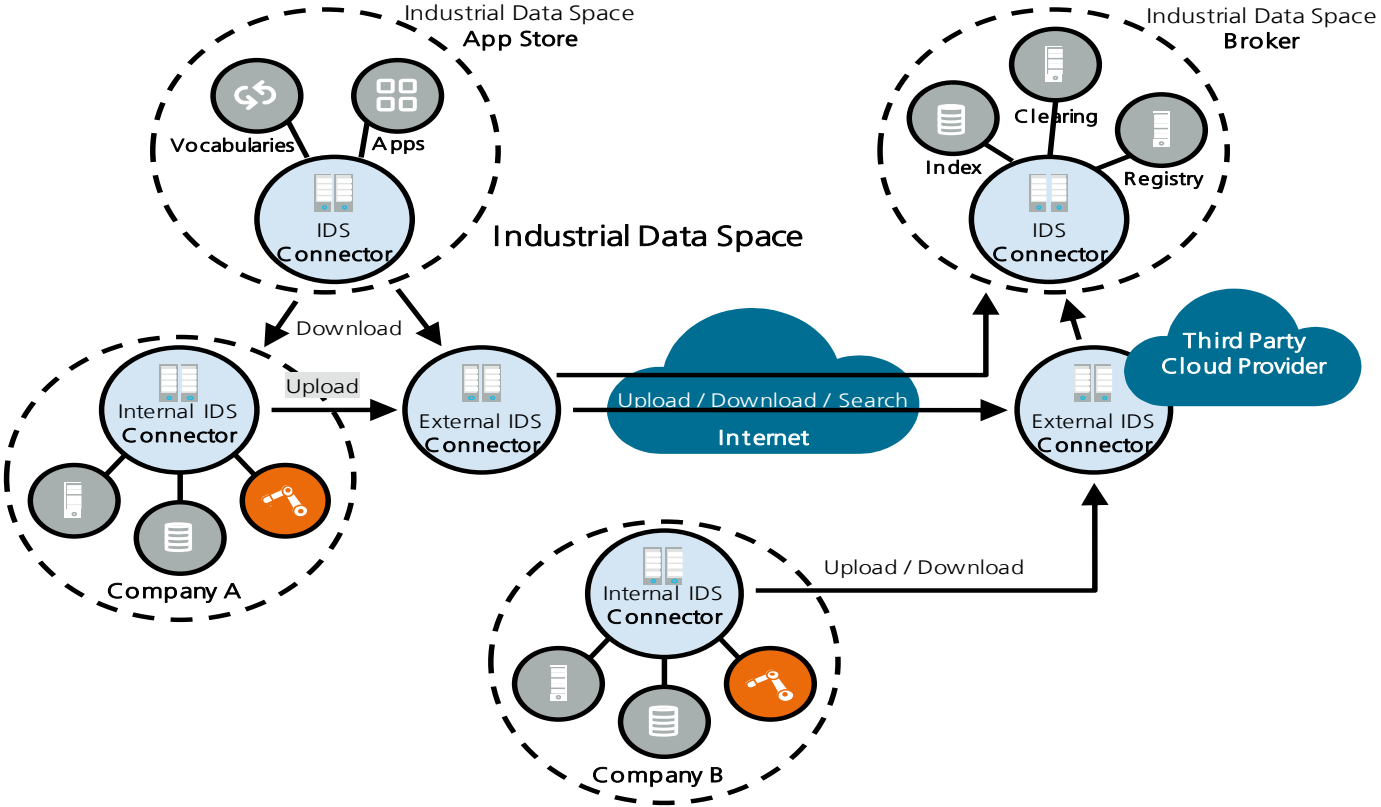
Netzwerk
Plattformen und Dienste

Industrial Data Space: Vier grundlegende Rollen

Daten-Geber	Daten-Nutzer	Broker	Zertifizierungsstelle
Stellt Daten zur Verfügung Eigener Betrieb eines Endpunkts im Industrial Data Space oder über Dienstleister Bestimmt Nutzungs-bedingungen und Preise für die Daten	**Nutzt Daten**, um **Dienste** anzubieten, oder für **interne Zwecke** Hält Nutzungs-bedingungen der Daten ein	**Bringt** Daten-Owner und -Nutzer **zusammen** Betreibt »Daten-verzeichnis« Übernimmt Monitoring- und Clearing-Aufgaben	**Zertifiziert Teilnehmer** auf die Standards des Industrial Data Space (u.a. Sicherheit, Nutzungs-bedingungen, Standards)

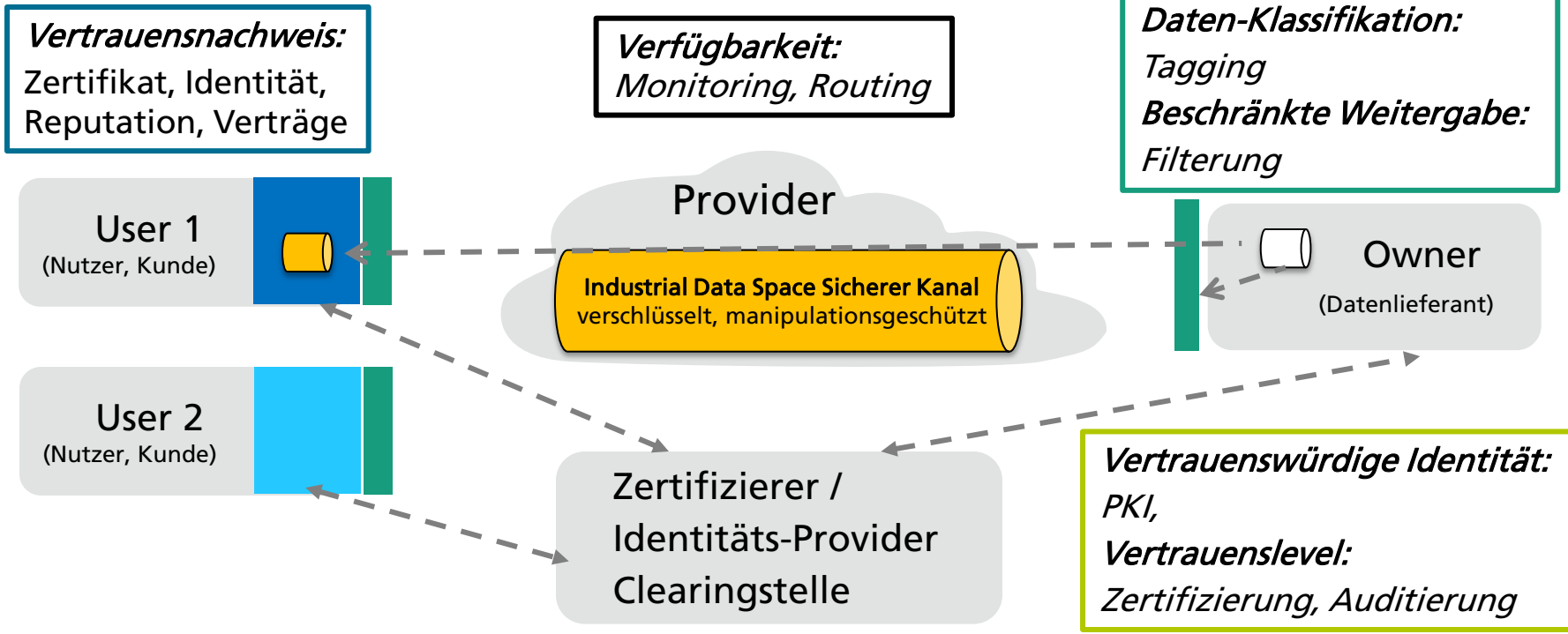
GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Industrial Data Space: Komponentenarchitektur

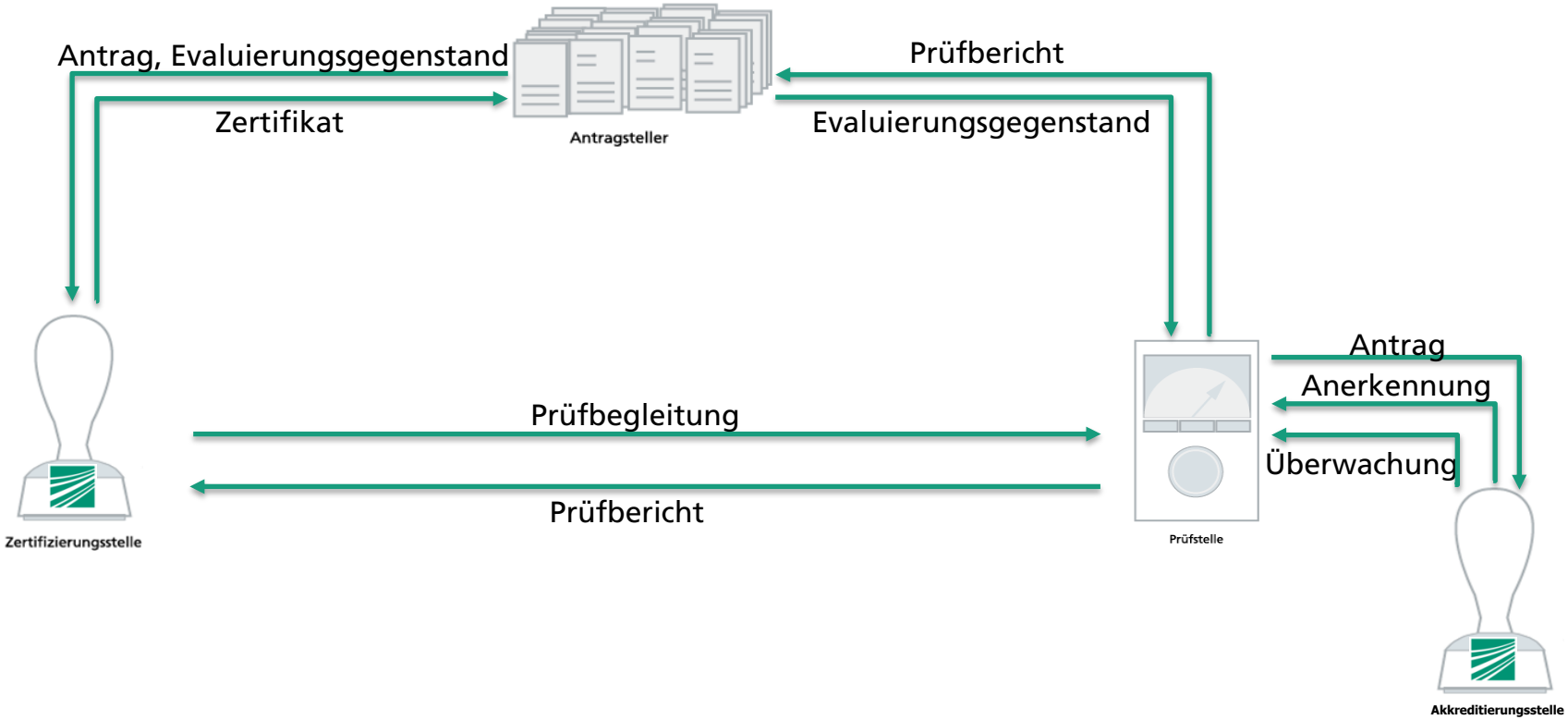


Industrial Data Space

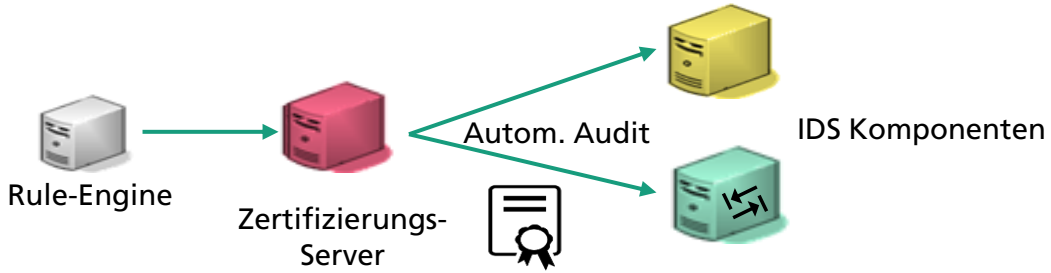
Top-Level Sicherheitsarchitektur



Zertifizierungsprozess im Industrial Data Space



Komponentensicherheit: Automatisierte (Re-) Zertifizierung



Initial werden Teilnehmer des Industrial Data Space **durch Zertifizierer auf Rollen zertifiziert**.

Technische, bzw. Sicherheitsanforderung an Diensteanbieter und – Nutzer können anschließend im Betrieb fortlaufend überwacht werden (**Verifizieren der Zertifizierungsvoraussetzungen**).

Einhaltung von SLAs kann somit automatisch überprüft werden.

- Verfügbarkeit, Datendurchsatz, Latenz

Industrial Data Space e.V.: Aktueller Stand

INDUSTRIAL DATA SPACE

Zusammenfassung
Security by Design für Cloud-basierte Datenaustauschplattformen: Der Industrial Data Space

Daten:

- … strategische Ressource, weil **wettbewerbsdifferenzierend,**
- … müssen als strategische Ressource **bewirtschaftet** werden.
- Ihr Wert steigt durch Austausch, Verknüpfung und Integration zu **Mehrwertdiensten.**
- **Netzwerkeffekte** in Markt zwischen Daten-Geber und –Nutzer.
- Nötig: **sicherer Raum**, der Souveränität wahrt und Vertrauen schützt

➔ **Industrial Data Space** deckt diesen Bedarf.

Kontakt: Jan.Juerjens@isst.fraunhofer.de

Ihr Ansprechpartner

Prof. Dr. Jan Jürjens

Director Research Projects,
Fraunhofer-Institut für Software- und Systemtechnik ISST (Dortmund)

Compliance Innovation Lab,
Fraunhofer Innovationszentrum für Logistik & IT FILIT (Dortmund)

Direktor, Institut für Softwaretechnik IST,
Universität Koblenz-Landau (Koblenz)

+49-172-255-2585

jan.juerjens@isst.fraunhofer.de