



Vertrauensinfrastrukturen im Kontext von Industrie 4.0 Anforderungen und Lösungsbausteine

23.06.2022

Vanessa Bellinghausen – BSI Referat DI23 – Cyber-Sicherheit für intelligente Transportsysteme und Industrie 4.0
(Leitung der Unterarbeitsgruppe Sichere Digitale Identitäten und Vertrauensinfrastrukturen)

1

Agenda

Vertrauensinfrastrukturen im Kontext von Industrie 4.0

Nachweise für die Vertrauenswürdigkeit

Lösungsbausteine

Fazit

2

2

Vertrauensinfrastrukturen im Kontext von Industrie 4.0 Beweggründe

- ▶ **Verbesserung bestehender Prozesse und Produkte**
 - ▶ Potentiale für Kosteneinsparungen können durch Lieferkettentransparenz offengelegt, quantifiziert und ausgeschöpft werden.
 - ▶ Qualitätskosten können durch Informationen über die Fertigungshistorie von Produktbestandteilen und einer datengetriebenen Fehlerursachenanalyse signifikant reduziert werden.

- ▶ **Weiterentwicklung bestehender oder Entwicklung neuer Geschäftsmodelle**
 - ▶ Pay-per-Use
 - ▶ Maschinenhersteller vermietet dem Maschinenbetreiber die Fertigungseinrichtung

- ▶ **Erfüllung aktueller und zukünftiger regulatorischer Vorgaben/Rahmenbedingungen**
 - ▶ Lieferkettensorgfaltspflichtengesetz
 - ▶ CO2-Bepreisung
 - ▶ Berücksichtigung ökologischer und sozialer Kriterien (z.B. Nachhaltigkeit)

3

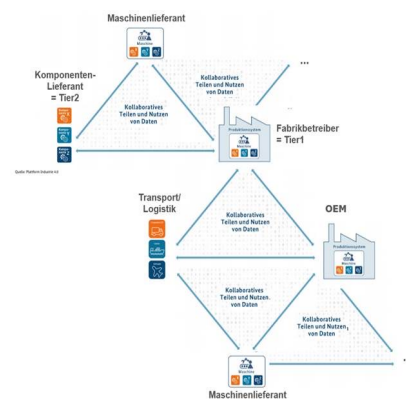
3

Vertrauensinfrastrukturen im Kontext von Industrie 4.0 Collaborative Condition Monitoring als Referenzmodell

- ▶ Ein Komponentenhersteller möchte Zugriff zu den Lebensdauer-Daten seiner Komponenten im Betrieb erhalten.
- ▶ Die Komponenten wurden von verschiedenen Maschinenlieferanten in unterschiedliche Maschinen integriert.
- ▶ Die Maschinen laufen bei unterschiedlichen Fabrikbetreibern



Produktions-Wertschöpfungsnetzwerk auf Basis des skalierten Referenzmodells



Quelle: Plattform Industrie 4.0 – Multilaterales Datenteilen in der Industrie (2022)

4

4

P L A T T F O R M
INDUSTRIE 4.0

Vertrauensinfrastrukturen im Kontext von Industrie 4.0 Drei Betrachtungsebenen

- ▶ Data Set
 - ▶ **Kapselt die Daten**
(z.B. Lebensdauerdaten, Temperaturdaten oder CO2-Footprint) für die multilaterale Nutzung
- ▶ Data Business Policy
 - ▶ **Essenzielle Eigenschaften der Daten wie z.B. Nutzung oder Verwendung**, deckt sowohl technische, rechtliche und ökonomische Gesichtspunkte ab, z.B.
 - ▶ Zugriffsberechtigung, -zweck, -dauer, -modus
 - ▶ Lizenz, Preis
- ▶ Data Exchange Framework
 - ▶ Etablierung **der rechtlichen, technischen und ökonomischen** Rahmenbedingungen für das unternehmensübergreifende Datenteilen

Quelle: Plattform Industrie 4.0 – Multilaterales Datenteilen in der Industrie (2022)

5

P L A T T F O R M
INDUSTRIE 4.0

Vertrauensinfrastrukturen im Kontext von Industrie 4.0 Drei Gestaltungsdimensionen

Gestaltungsdimensionen des Data Exchange Framework

- ▶ **Technisch**
 - ▶ Technische Interoperabilität z.B. Verwaltungsschale als Single Point of Entry, Technologie für die Verifizierung
- ▶ **Rechtlich**
 - ▶ Erfüllung rechtlicher Vorgaben und Bereitstellung juristisch belastbarer Daten z.B. Datenschutzrecht, Kartellverbot, AGB's der Unternehmen
- ▶ **Ökonomisch**
 - ▶ Ökonomische Interoperabilität z.B. firmenübergreifendes Controlling

Quelle: Plattform Industrie 4.0 – Multilaterales Datenteilen in der Industrie (2022)

6

Vertrauensinfrastrukturen im Kontext von Industrie 4.0

Kernmerkmale

- ▶ Herstellung der Vertrauenswürdigkeit in der Industrie 4.0-Wertschöpfungskette
- ▶ Berücksichtigung der drei Gestaltungsdimensionen
- ▶ Etablierung von Rahmenbedingungen, die es allen Teilnehmern ermöglicht Daten zu teilen und zu nutzen
- ▶ Digitale und automatisierte Abbildung von Vertrauensmechanismen
 - ▶ Identifizierung z.B. Wer hat die Komponente hergestellt?
 - ▶ Authentifizierung z.B. Ist der Maschinenhersteller auch der, für den er sich ausgibt?
 - ▶ Autorisierung z.B. Was darf der Komponentenhersteller?
 - ▶ Verhandlung von Nutzungsbedingungen
 - ▶ Überprüfung von Security Eigenschaften z.B. ISO 27001 oder IEC 62443
 - ▶ Kataloge und Mechanismen zum Suchen und Finden der DataSets

7

7

Vertrauensinfrastrukturen im Kontext von Industrie 4.0

Definition eines Vertrauensraums Industrie 4.0

„Ein Vertrauensraum Industrie 4.0 legt die **Governance für die Anforderungen an eine vertrauenswürdige Zusammenarbeit** für einen **Zweck im Rahmen von Industrie 4.0 Szenarien** fest. Die Governance wird von den Teilnehmern verwendet, um ihre Vertrauensbeziehung zu etablieren und aufrecht zu erhalten. Auf Basis der Governance und der Vertrauensbeziehung infolge des Trustworthinessprofil-Abgleichs wird sicher und vertragskonform zusammengearbeitet.“

Note 1: Der Vertrauensraum Industrie 4.0 stellt die Anforderungen für die vertrauenswürdige Identifikation der Unternehmen und die Verknüpfung mit entsprechenden Credentials bereit.

Note 2: Der Vertrauensraum Industrie 4.0 stellt Anforderungen an die Nachweisführung für die Qualitäten, z.B. ISO 9000, ISO 27000 Zertifikate der Kooperationspartner bereit.

Note 3: Akteure im Vertrauensraum umfassen alle Entitäten, z.B. Personen, Unternehmen, Maschinen, industrielle Komponenten, Prozesse, digitale Zwillinge/Verwaltungsschalen

8

8

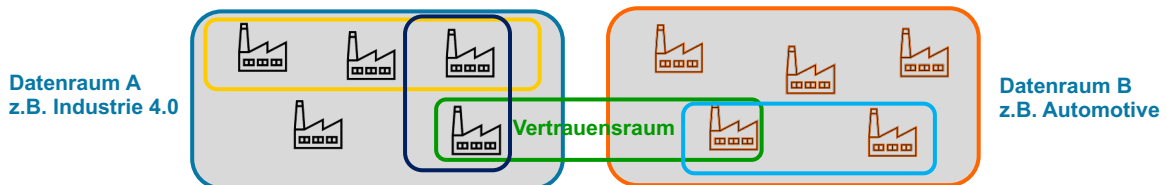
Vertrauensinfrastrukturen im Kontext von Industrie 4.0
Die Bedeutung von Vertrauensprofilen


- ▶ Matching von Fähigkeiten und Erwartungen der Geschäftspartner
- ▶ Prüftiefe des Lieferanten hängt von dem Risiko des jeweiligen Business Cases ab und kann bis zum Audit vor Ort gehen
- ▶ Attribute eines Vertrauensprofils können in Klassen eingestuft werden (bspw. eIDAS Einstufung low, substantial, high)

Quelle: Plattform Industrie 4.0 und Robot Revolution & Industrial IoT Initiative: "IIoT Value Chain Security – The Role of Trustworthiness". Berlin: Federal Ministry for Economic Affairs and Energy (BMWi), 2020.

Vertrauensinfrastrukturen im Kontext von Industrie 4.0
Überlappung von Vertrauensräumen

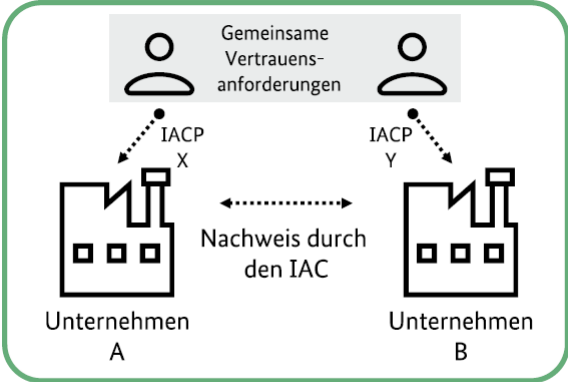
- ▶ Es können sich mehrere Vertrauensräume bilden.
- ▶ Vertrauensräume können beliebig überlappen.
- ▶ Eine Vertrauensbeziehung zwischen Partnern aus unterschiedlichen Vertrauensräumen kann durch die Vereinbarung eines neuen Vertrauensraumes etabliert werden.
- ▶ Eine Akkreditierung als Partner in einem Vertrauensraum könnte unter Berücksichtigung von potentiellen Delegationsprozessen, ohne neue Überprüfung, bei transparenten Vertrauensraum-Policies, zur Akkreditierung in einem anderen Vertrauensraum erfolgen.





Nachweise für die Vertrauenswürdigkeit Identity Authenticating Certificates (IACs)

- ▶ IACs können für eine gegenseitige Authentifizierung, sowie für die Bestätigung der Integrität und Authentizität von Dokumenten verwendet werden
- ▶ Ein IAC-Provider (IACP) prüft die Identität und stellt ein IAC aus




Vertrauensraum ●.....▶ identifiziert

Quelle: Plattform Industrie 4.0: „Vertrauensinfrastrukturen im Kontext von Industrie 4.0 – Anforderungen und Lösungsbausteine, 2021

11

11

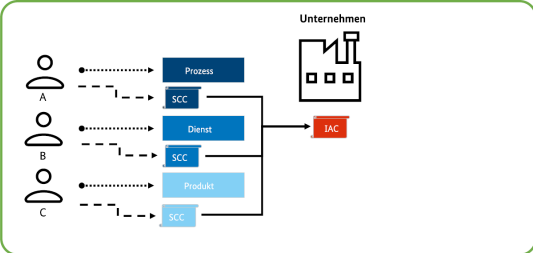


Nachweise für die Vertrauenswürdigkeit Security Certification Certificates (SCCs)

- ▶ SCCs können verwendet werden, um einen Nachweis für Fähigkeiten bereitzustellen
- ▶ Ein SCC-Provider (SCCP) prüft Fähigkeiten und stellt ein SCC aus

➔ Es muss immer eine vertrauenswürdige Verbindung zwischen den IACs und den SCCs hergestellt werden.

➔ IACs und SCCs besitzen eine begrenzte Gültigkeitsdauer, daher muss eine Erneuerung vorgesehen werden!



●.....▶ prüft - - - - -▶ erstellt —————▶ verweist auf

Quelle: Plattform Industrie 4.0: „Vertrauensinfrastrukturen im Kontext von Industrie 4.0 – Anforderungen und Lösungsbausteine, 2021

12

12

PLATTFORM
INDUSTRIE4.0

Lösungsbausteine

13

13

PLATTFORM
INDUSTRIE4.0

Lösungsbaustein 1

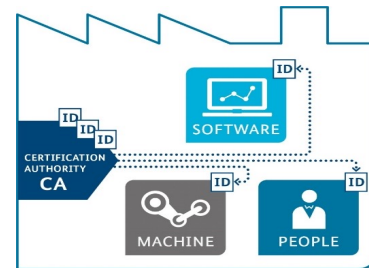
Verknüpfung von bestehenden Public Key Infrastrukturen

14

14

Lösungsbausteine Verknüpfung von bestehenden Public Key Infrastrukturen

- ▶ Funktionen von PKI-Architekturen können auch in Produktionsumgebungen zu einem Gewinn an Sicherheit beitragen.
- ▶ Sub Certification Authorities können durch eine zentrale Firmen-Root-CA oder einen Dienstleister verwaltet werden.
- ▶ PKI-Anwendungen dürfen den Produktionsfluss nicht in unvorhergesehener Weise unterbrechen.



Quelle: Plattform Industrie 4.0:
„Vertrauensinfrastrukturen im Kontext von Industrie 4.0 –
Anforderungen und Lösungsbausteine, 2021“

15

15

Lösungsbaustein 2

Electronic
Identification,
Authentication and
trust Services
„eIDAS“

16


16



Lösungsbausteine Electronic Identification, Authentication and trust Services „eIDAS“

eIDAS-Verordnung Nummer 910/2014 vom 23 Juli 2014


- ▶ **Gegenseitige Anerkennung von verschiedenen Vertrauensdiensten innerhalb des EWR**
- ▶ Keine Vereinheitlichung von technischen Identifizierungssystemen und Lösungen!



Quelle:
<https://webgate.ec.europa.eu/fribrowser/#/> (Stand: 10. Juni 2020)

17

17



Lösungsbausteine Electronic Identification, Authentication and trust Services „eIDAS“

Vorteile:

- ▶ Vertrauenslisten unterstützen einen gegenseitige Anerkennung unter allen Mitgliedstaaten
- ▶ Die Qualität von Vertrauensdiensten kann unterschieden werden
- ▶ Interoperabilität: Es existieren mehrere Standards hinsichtlich Anforderungen und der Zertifizierung von Stakeholdern, bspw. Vertrauensdiensteanbietern

➔ **Möglicher Ansatz für Industrie 4.0:**

- ▶ Gegenseitige Anerkennung von Sicheren Digitalen Identitäten für unternehmensübergreifende Geschäftsprozesse

Eine **'Sichere Identität'** ist eine eindeutige Identität mit zusätzlichen Sicherheitseigenschaften für eine belastbar vertrauenswürdige Authentifizierung der Entität (d.h. mit angemessenen Maßnahmen zur Verhinderung der Vortäuschung einer falschen Identität.)

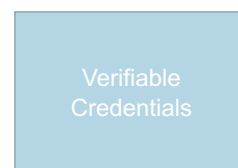
Quelle: Sichere Identitäten (Plattform Industrie 4.0, 2016)

- ▶ Es muss jedoch zwischen staatlichen und privatwirtschaftlichen Vertrauensräumen unterschieden werden

18

18

Lösungsbaustein 3

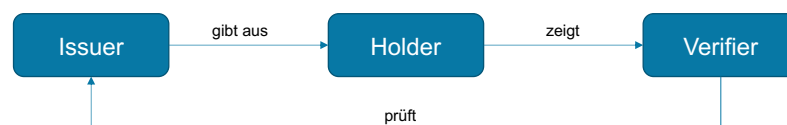


19

19

Lösungsbausteine Verifiable Credentials

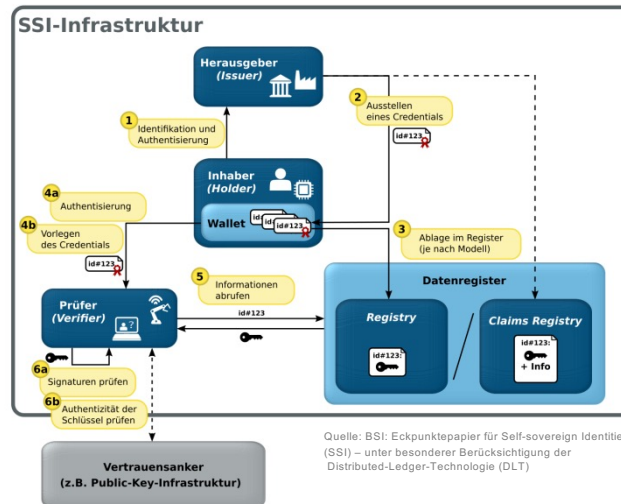
- ▶ Wunsch nach mehr Datensouveränität
- ▶ Verwaltung der Identitäten
- ▶ Entscheidung darüber, welche Informationen mit wem geteilt werden sollen
- ▶ Ein Nutzer (Holder) kann kryptografisch signierte Attribute (verifiable credentials), z.B. Hersteller-ID einer Maschine, verwalten und einem Dritten (Verifier) bei Bedarf zeigen.
- ▶ Attribute werden durch eine geeignete Ausgabestelle (Issuer) vergeben



20

20

Lösungsbausteine Verifiable Credentials Beispiel: Self-sovereign Identities



21

21

Fazit Zusammenfassende Herausforderungen

- ▶ Anschlussfähigkeit an Vertrauensräume muss ermöglicht werden
- ▶ Motivationen für Vertrauensräume sind unterschiedlich (z.B. Maschinenbau vs. Automobilindustrie)
- ▶ Charakteristika für verschiedene Vertrauensräume müssen identifiziert werden
- ▶ Stakeholder in der Supply Chain haben unterschiedliche Rollen inne z.B. Einkauf und Verkauf
- ▶ Dezentrale Ansätze zur Verwaltung von Identitäten für Industrie 4.0-Anwendungen müssen in Bezug auf Herausforderungen und Vorteile untersucht werden

22

22

Kontakt:

Vanessa Bellinghausen (Leitung der Unterarbeitsgruppe „Sichere digitale Identitäten und Vertrauensinfrastrukturen“)

Referat DI 23 - Cyber-Sicherheit für intelligente Transportsysteme und Industrie 4.0
Bundesamt für Sicherheit in der Informationstechnik

E-Mail: vanessa.bellinghausen@bsi.bund.de