INTERNATIONAL DATA SPACES ASSOCIATION

INTERNATIONAL DATA SPACES
FACT SHEET UND KERNAUSSAGEN

Version 1.0 | August 2019

STRATEGISCHE POSITIONIERUNG

- Ziel: Das Ziel der International Data Spaces Association (IDSA) ist die Etablierung eines Standards für Datensouveränität – für den vertrauenswürdigen, selbstbestimmten Austausch von Daten.
- Werte: Die Spezifikation der IDSA bildet die Basis für Datenökosysteme und Marktplätze, die auf europäischen Werten basieren, d. h. Datenschutz und Sicherheit, Chancengleichheit durch ein föderiertes Design und die Gewährleistung der Datensouveränität für den Urheber der Daten und das Vertrauen zwischen den Teilnehmern.
- International Data Spaces Association: Die IDSA ist ein gemeinnütziger Verein und nonprofit. Alle Mitglieder haben die gleichen Rechte, die Ergebnisse zu nutzen. In drei Stufen erfolgt die Adoption der Idee der International Data Spaces (IDS) im Markt:
  1) Forschung, um bisher ungelöste Fragen zu lösen (Fraunhofer, TNO, vtt u. a.)
  2) Konsensbildung zu Architektur, Implementierungsoptionen und Standardisierung in den Gremien des Vereins
  3) Überführung der Konzepte aus der Vereinsarbeit in marktfähige Produkte und Services durch Unternehmen aus dem Verein und auch außerhalb.

  Die IDSA steht an der Schwelle von 2) zu 3).
- International: IDS ist eine internationale Initiative. Die IDSA hat 100 Mitglieder aus 19 Ländern (EU plus Brasilien, China, Indien, Japan, Kanada und die USA) und formale Kooperationen mit internationalen Initiativen (Plattform Industrie 4.0, IIC, IVI, DTA, RRI, OPC-F, Fiware, DMA, iShare).
- Datensouveränität: IDS liefert mit dem Konzept der Datensouveränität einen wichtigen Beitrag digitaler Infrastrukturen und damit eine Antwort auf markthemmende Effekte der Datenökonomie im Allgemeinen, insbesondere für das Industrial IoT, für Künstliche Intelligenz (KI) und jede Art von Smart Service Scenarios. IDS bietet die Möglichkeit, das zentrale Objekt dieser Ökosysteme (das Wirtschaftsgut Daten) zu beschreiben, zu handeln und zu schützen. Einen globalen Standard dafür gibt es derzeit nicht.
- IDS und EU: IDS ist Bestandteil der zukünftigen Strategie der Europäischen Kommission im Rahmen der Strategic Value Chain des Indusrial IoT sowie bei der Strategie der Digitsing European Industry (DEI).
- IDS und GAIA: Vorarbeiten des IDS sind mehrwertig für GAIA und sollten unbedingt aufgegriffen werden, da sie direkt auf die Ziele von GAIA einzahlen und damit den Time to Market für GAIA erheblich verkürzen. Auf dem Weg zu einer florierenden Datenökonomie sind dennoch viele Herausforderungen offen, denen mit GAIA konsequent begegnet werden muss.
- IDS und KI: IDS liefert mit dem Konzept der Datensouveränität die Grundlage für erfolgreiche KI, indem wesentlich mehr Datenquellen zugänglich gemacht werden.

GENERELLES KONZEPT

- IDS liefert eine Referenzarchitektur, einen formalen Standard und Referenzimplementierungen einschließlich Sample Code.
- IDS ist ein Konzept analog dem Internet auf Basis von Peer-to-peer-Kommunikation. IDS ist keine Plattform.
- Intern/extern: IDS adressiert Ökosysteme und Unternehmensnetzwerke. Anwendungsfälle innerhalb einer Fabrik bzw. innerhalb einer Firewall brauchen keinen IDS.
- Zertifizierung: Mit dem Zertifizierungskonzept wird die Konformität von Komponenten (Connector) und Organisationen zur IDS-Architektur von unabhängigen Organisationen (PwC, TÜV, Fraunhofer) bestätigt. So ist sichergestellt, dass die Organisationen alle notwendigen Maßnahmen für eine IDS-konforme Betriebsumgebung getroffen haben und auch Komponenten einsetzen, die entsprechend der Connector-Variante realisiert sind.

CONNECTOR UND IMPLEMENTIERUNG

- IDS Connector: Der IDS Connector fungiert als Gateway. Er kann je nach Szenario unterschiedlich implementiert werden: auf Mikrocontroller, Sensoren, mobilen Devices, auf Server, in der Cloud. Aufgrund der Container-Architektur erlaubt der IDS Connector auch Trusted Exection von Apps – und zwar solchen, die Daten aus verschiedenen Quellen souverän analysieren. Diese Softwareservices werden nicht in einem ERP-System hinter der Firewall laufen, sondern auf Cloud-Plattformen, also „in der Mitte“

von Ökosystemen. Daher ist der Connector eine passende Ausführungskomponente für Amazon Web Services (AWS), Digital Innovation Hubs (DIH), SAP HANA, etc., weil dadurch die Plattformen eine sichere Umgebung anbieten können, in der Datensouveränität gewahrt bleibt. Domänenspezifische Einsatzprofile ermöglichen die Einbettung in Fachdomänen mit verschiedenen Anforderungen (siehe DIN SPEC 27070).

- Connector-Varianten: Je nach Nutzungsszenario und Umfang des Schutzbedürfnisses können Unternehmen aus vier Connector-Varianten wählen: Basefree, Base, Trust, Trust+. Das „Base"-Profil erfüllt grundlegende Sicherheitsanforderungen für die Kommunikation über Unternehmensgrenzen hinweg. Ein Connector, der nach dem „Trust"-Profil zertifiziert wurde, liefert darüber hinausgehende Sicherheitsmerkmale wie strikte Isolation der Dienstecontainer und gegenseitige Überprüfung der Integrität. Ein Connector nach dem „Trust+"-Profil ermöglicht sogar den Schutz vor Manipulation durch Administratoren.
- Implementierung und Produkte: Unternehmen entwickeln marktreife Lösungen (kommerziell, nicht-kommerziell) und stellen sie dem Markt über eigene Geschäftsmodelle zur Verfügung. Das Produkt muss zertifiziert werden, um mit anderen IDS Connectors interoperabel zu sein. IDSA ist gemeinnützig, hat keine Gewinnerzielungsabsicht.
- Plugfest und Developers Community: Die Umsetzung der erwähnten Dinge erfolgt im „Plugfest", wo sich alle drei Monate alle Entwickler (Forschungseinrichtungen und Unternehmen), im „IDS Lab" in Dortmund treffen. Derzeit existieren Implementierungen von Connector-Varianten von 15 Unternehmen und Forschungseinrichtungen sowie die der Services Broker, Appstore, Clearing House, Identity Management und Vocabulary Provider. Es existiert eine Entwicklungsroadmap, die von der Developers Community im Plugfest umgesetzt wird. Nutzbaren Code gibt es auf der vereinsinternen Kollaborationsplattform (nur den Vereinsmitgliedern zugänglich) und Teile davon in Git Repositories der Vereinsmitglieder.

INHALTLICHES KONZEPT

- Semantik: IDS standardisiert die Semantik des Datenaustauschs. IDS liefert in Form eines Informationsmodells die Semantik für die IDS-Architektur, beschreibt also bspw. was ein Broker ist, ein Connector, was überhaupt Datengüter sind, was Datengeber sind etc. Außerdem schlägt IDS eine Semantik für Datennutzungsbedingungen vor (Daten dürfen dreimal genutzt, gelesen, werden; Daten dürfen nicht weitergeleitet werden; dürfen weitergeleitet werden, aber nur gegen Gebühr etc.). IDS definiert nicht fachliche bzw. domänenspezfische Semantik. IDS sagt also nicht, welche Merkmale einen Schraubroboter etc. beschreiben bzw. wie ein „Industrie-4.0-Ding" aussieht – das macht die Verwaltungsschale, deren instanziierte Daten man allerdings mit Nutzungsbedingungen über IDS versehen kann, bevor man sie über einen IDS Connector austauscht.
- IDS und EDI: IDS ersetzt nicht EDI. EDIFACT-Nachrichten für Rechnungen, Lieferabrufe etc. wird es lange Zeit geben. Nur: EDI standardisiert keine Nutzungsbedingungen.
- IDS und standardisierte Nutzungsbedingungen. Das macht bisher noch kein Standard. Wir haben derzeit 14 Nutzungsbedingungsklassen spezifiziert, die über die Open Digital Rights Language Working Group an das World Wide Web Consortium getragen werden.
- Datengruppen: IDS ist für Ökosysteme, weil hier die Innovation stattfindet. Ökosysteme brauchen – aus Sicht eines Mitglieds des Ökosystems – eigene Daten, Daten von „Friends and Family" (langjährige, vertraute Lieferanten etc.) und Kontextdaten (Wetter, Verkehr etc.), häufig öffentliche.
- Policy Enforcement: Datensouveränität nicht nur deklarativ zu beschreiben und damit interpretierbar für einen Computer zu machen (was auch schon ein wichtiger Schritt ist), sondern Datensouveränität technisch durchsetzen zu können (Enforcement), ist ein zentraler Punkt der gesamten IDS-Initiative. Wir verfolgen dazu verschiedene Technologieentwicklungsstränge (die es schon vor IDS gab und die eigenständige Konzepte in sich sind): u. a. Distibuted Usage Control, Data Provenance Tracking und Sticky Policies.
- IDS und Cloud: Für die Integration der IDS-Komponenten in eine moderne Cloud-Plattform wie AWS, DIH etc., brauchen wir einmal ein Architekturbild, das als Reference Model typische Komponenten zeigt (u. a. auch den Connector, s.o.).

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Joseph-von-Fraunhofer-Str. 2–4
44227 Dortmund | Germany

phone: +49 231 9743 619
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

@ids_association

international-data-spaces-association