EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

IAM für Internet-Dinge (IoT)

Fachartikel von Peter Weierich, Managing Director, IPG GmbH Deutschland

Ist ein moderner PKW noch ein „Auto“ wie wir es früher kannten? Oder ist es ein komplexes Internet-Ding mit ein wenig Physik zur Fortbewegung? In jedem Fall ist das ein gutes Beispiel, um auch folgende Fragen zu bearbeiten: Welche Auswirkungen haben Internet of Things Projekte auf die IAM-Prozesse? Sind oder haben IoT-Devices eine Identität? In diesem Artikel versuchen wir auf diese Fragen eine Antwort zu geben, indem wir eine Systematik für IoT-Einsatzfälle einführen. Daraus können wir dann Anforderungen an IAM-Projekte ableiten.

Von „dumm“ bis intelligent und autonom

Zuerst muss geklärt werden, welche Typen von IoT-Devices im Fokus stehen:

- Einfache Geräte, beispielsweise Sensoren (Temperatur, Bewegungsdetektion, Geschwindigkeitsmesser)
- Komplexe Devices, die typischerweise eine Komposition einfacher Geräte sind
- Intelligente Geräte, bis hin zu autonomen Plattformen: Beispielsweise Serviceroboter, autonome Fahrzeuge

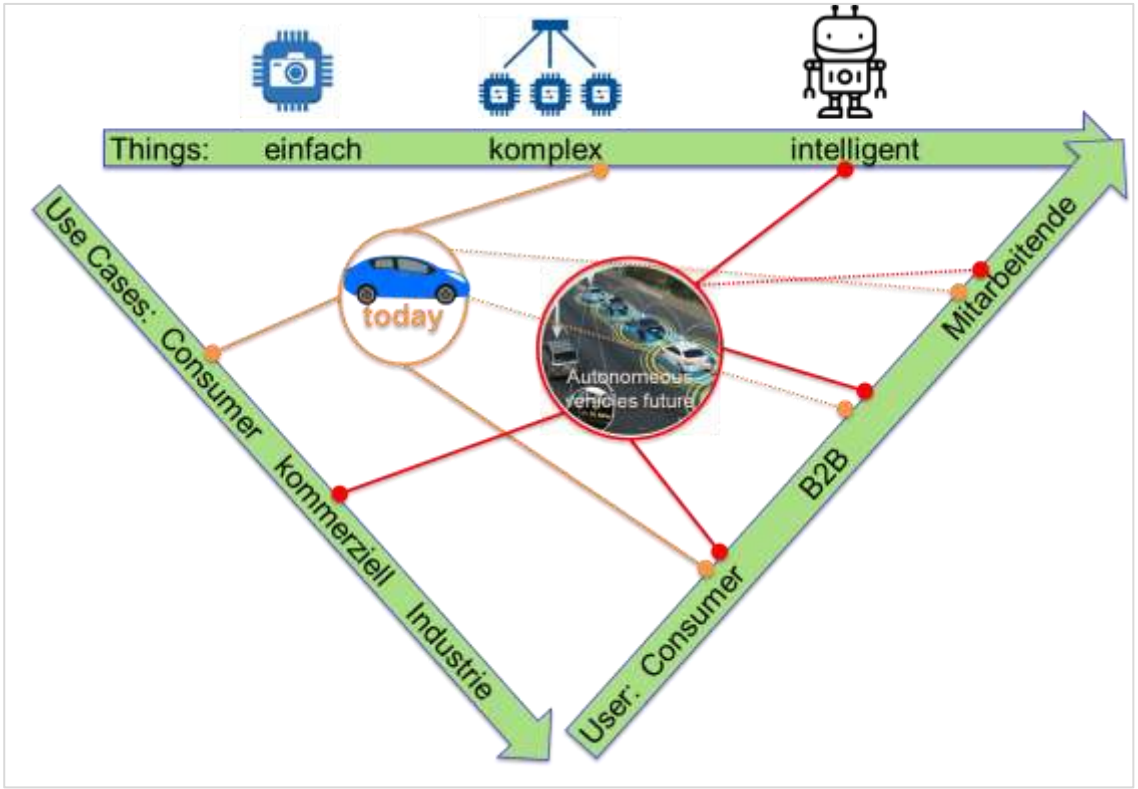

Abbildung1: Klassifizierung von IoT-Szenarien

Tatsächlich läuft es darauf hinaus: Je intelligenter und autonomer die «Internet-Dinge» werden, desto mehr müssen sie aus der Sicht des Identity- und Accessmanagements wie menschliche Identitäten behandelt werden: Ihre Rechte zum Zugriff auf Daten und Ressourcen müssen unter Umständen genauso gemanagt werden, wie jene natürlicher Personen.

Dabei ist eine wichtige Randbedingung zu beachten: Die Steuerung und Kommunikation sehr komplexer Geräte erfolgt nicht direkt, sondern in der Regel über IoT-Plattformen, in denen ein «digital twin» abgebildet ist. Das heißt: Die Interaktion findet primär mit dem digitalen Zwilling statt und die IoT-Plattform ist – nicht zuletzt aus Sicherheitsgründen – der exklusive Kommunikationspartner des Geräts. Insofern hängt die Umsetzung von IAM-Prozessen davon ab, welche Mechanismen die IoT-Plattform bereitstellt. Die heute weit verbreiteten Produkte agieren noch weitgehend IAM-agnostisch. Einige wenige bieten immerhin LDAP-basierende Zugriffsteuerungen zur Verfügung.

Benötige ich überhaupt IAM für Internet-Dinge?

Bevor die Frage beantwortet wird, ob und welche IAM-Prozesse benötigt werden, müssen neben der Klassifizierung der Geräte selbst noch weitere Dimensionen unterschieden werden:

- Welche Personen bzw. Interaktionspartner sind involviert?
- Welche Geschäftsprozesse werden abgedeckt?

Daraus ist eine Risiko-Einschätzung abzuleiten, die dann die Notwendigkeit bzw. den Umfang der IAM-Prozesse begründet.

Interaktionspartner:

Hier kommen die klassischen IAM-Einstufungen zum Tragen, das heißt wir unterscheiden zwischen Mitarbeitenden im Unternehmen, Business-to-Business und Business-to-Consumer Szenarien. Zusätzlich können auch die IoT-Devices miteinander interagieren. Im Automobilbereich werden die folgenden zusätzlichen Interaktionsformen betrachtet:

- In-Vehicle: User (Fahrer) bzw. Fahrgäste kommunizieren mit dem Fahrzeug
- Vehicle-to-Vehicle: Fahrzeuge interagieren miteinander
- Vehicle-to-Enterprise: Die Fahrzeuge interagieren mit dem Hersteller bzw. einer anderen Partei, z.B. einem Mobilitätsdienstleister

Art der Geschäftsprozesse:

- Consumer-Prozesse haben häufig sehr niedrige Sicherheitsanforderungen bzw. Anforderungen an IAM-Prozesse, es sei denn es handelt sich um Finanztransaktionen oder um Szenarien, bei denen es um die Gesundheit von Menschen geht: Beispielsweise bei digitalen und vernetzen Blutzuckermessgeräten bzw. Insulinpumpen.
- «Commercial»-Prozesse, bei denen typischerweise Unternehmen involviert sind.
- Industrie-Prozesse: Hierunter werden die klassischen «Industrie 4.0»-Prozesse in der Produktion subsummiert, die oft besonders hohe Sicherheitsanforderungen haben.

Beispiel: Motorisierter Individualverkehr

Die heutigen Nutzungsszenarien erfordern oft keinerlei IAM-Mechanismen, allerdings bieten die Hersteller häufig digitale Dienste (Connected Drive, Audi Connect, me connect, OnStar etc.). Diese erfordern folgende IAM-Basisprozesse:

- Registrierung als User (typischerweise über die Homepage des Herstellers)
- Herstellen der logischen Verbindung zum PKW
- Anmeldevorgänge im PKW / per App

Zukünftig müssen detaillierte Konzepte entwickelt werden, um folgende Fragen zu beantworten: Welcher Prozessbeteiligter darf welche Daten von welchen Fahrzeugen wissen (Position, Route, Auslastung, Ladezustand)? Wie darf wer steuernd eingreifen, auch z.B. für Umfahrungsrouten etc.? Wer darf wissen, welche Person in welchem Fahrzeug wo unterwegs ist. Eine Gegenüberstellung wesentlicher Punkte findet sich in der folgenden Tabelle.

	Heute	Morgen
Szenario	1. Assistenzfunktionen im «eigenen» PKW 2. Abfrage von Fahrzeugdaten	Mobilitätsdienstleistungen mit autonomen Fahrzeugen
IoT-Klassifikation	Komplex, zum Teil intelligent (z.B. Mustererkennung, Spurhalteassistent, Abstandsregelung)	Intelligent, autonom
Use Cases	Consumer	Consumer und kommerziell (Mobilitätsverträge auch mit Unternehmen)
Interaktion	In-vehicle, Consumer mit rein physischer Zugangskontrolle V2E für Fahrzeugdaten (z.B. online Abfrage von Tankfüllung, GPS Position, Servicestatus)	- C-IAM für Bestell- und Abrechnungsvorgänge - Vehicle-to-Enterprise für die Flottenplanung und -steuerung - Vehicle-to-Vehicle für Optimierung der Fahrten
Geschäftsprozesse	Consumer mit bzw. ohne «digitale Identität»	Consumer, B2B
IAM-Anforderungen	Für 1: Praktisch nicht vorhanden, nur für zentrale Assistenzfunktionen erforderlich Für 2: C-IAM für Benutzerregistrierung, Login etc.	Hoch, insbesondere um Fremdeingriffe in das System zu verhindern

Tabelle 1: Beispiel für IoT-Szenarien

Wie unterstützt die IPG?

Sehr häufig erleben wir im Rahmen von IAM-Strategieprojekten, dass es nur diffuse Ideen dafür gibt, welche IoT-Szenarien in Zukunft relevant sein werden. Daher muss man im Rahmen dieser Vorhaben diejenigen Ansprechpartner im Unternehmen identifizieren, die in die Planungen involviert sind, typischerweise die Chief Digital Officers. Allerdings passiert es regelmäßig, dass aus der Produktentwicklung heraus eine Entscheidung für die Einführung einer IoT-Plattform von einem strategischen Lieferanten, z.B. von Microsoft (Azure IoT), ohne vorher die Szenarien zu entwickeln, die bedient werden sollen.

Daher ist es erforderlich, möglichst früh auch IAM-Spezialisten bei der Entwicklung der IoT-Szenarien zu involvieren, um im Vorfeld «die richtigen Fragen» zu stellen. Unter anderem können dann IAM-Anforderungen an eine zu beschaffende (oder zu mietende) IoT-Plattform abgeleitet werden, da etliche Produkte nur marginale oder gar keine IAM-Prozessunterstützung leisten können.

Kontaktieren Sie uns und erfahren Sie mehr über IAM für IoT.

Markus Blaha: Sales Manager Austria
markus.blaha@ipg-group.com; Telefon +43 676 734 23 00

Christian Rückert: Sales Manager Germany
christian.rueckert@ipg-group.com; Telefon +49 170 908 03 53

Marcel Weber: Sales Manager Switzerland
marcel.weber@ipg-group.com; Telefon +41 79 907 84 47