

Zeitschrift für
Zahlungsverkehr und Kartendienstleistungen



D 25079
Fritz Knapp Verlag
Frankfurt am Main
29. Jahrgang
10. Mai 2018
ISSN 0937-597 X

2-2018

**Digitaler
Sonderdruck**



**PSD2-Umsetzung –
noch ein weiter Weg**



**Technik und Prozesse
für ein Internet of Payments**

Von Joachim Dorschel und David Karlin

Technik und Prozesse für ein Internet of Payments

Von Joachim Dorschel und David Karlin



Die Entwicklung des Internet of Payments steht erst ganz am Anfang. Dabei muss das Rad nicht neu erfunden werden, so Joachim Dorschel und David Karlin, sondern etablierte Anwendungen bringen viele der benötigten Funktionen mit. Für die Skalierung auf Millionen beteiligter Endgeräte werden diese jedoch angepasst werden müssen. Hierbei raten die Autoren den Banken, beizeiten entscheidende Impulse zu setzen. Denn in der digitalen Welt werden Marktanteile verteilt, bevor die Technologie den Reifegrad erreicht. Red.

Das Internet of Things (IoT) ist ein wesentliches Element der Digitalisierung. Die Vernetzung schafft Möglichkeiten der maschinellen Steuerung und Optimierung der physischen Lebensumgebung. Die denkbaren Anwendungen reichen von Wearables über Smart Homes bis zu Smart Cities.

Eng verbunden mit dem Begriff IoT ist jener der Industrie 4.0, der Digitalisierung und Vernetzung von Produktionsstätten und -prozessen, von Komponenten und Produkten entlang von Wertschöpfungsketten und der digitalen Optimierung von Dienstleistungen. Das Konzept einer solchen „smarten“ Umwelt basiert auf der autonomen Kommunikation und Interak-

tion der Elemente der unbelebten Welt miteinander und, über ubiquitäre Schnittstellen, mit dem Menschen als Nutzer und letztverantwortlichem Entscheider.

Kommerzielle Nutzung von IoT braucht Payment-Lösungen

Dient IoT kommerziellen Zwecken, stellt sich die Frage der Vergütung. Kommerzielle IoT benötigt effiziente Möglichkeiten, Leistungen zu bezahlen. Überlegungen zur Erweiterung von IoT um Payments-Funktionalitäten haben bereits vor einiger Zeit den Begriff „Internet of Payments (IoP)“ geprägt, welcher die spezifischen Eigenschaften digital vernetzter, hochautomatisierter Leistungsbeziehungen zwischen Maschinen einschließlich der Abrechnung dieser Leistungen kennzeichnet.

Die Anwendung von IoT in der industriellen Produktion hat zwei wesentliche Stoßrichtungen: Einerseits geht es darum, Produktionsprozesse zu optimieren und mit der Logistik zu verzahnen, andererseits um die Möglichkeiten der Individualisierung und Personalisierung der Produkte selbst.

Zum Autor

Joachim Dorschel, Managing Partner, **Dr. David Karlin**, CTO, beide DPS Group, Leinfelden-Echterdingen

Bestehende IoT-Lösungen stammen vor allem von etablierten Softwareunternehmen und folgen dem Plattformgedanken. Ziel ist, unterschiedliche IoT-Komponenten sicher zu integrieren und zu managen und mit anderen Datenquellen und Applikationen so zu verbinden, dass der Gesamtnutzen für alle Stakeholder optimiert werden kann. Dabei ist auch bei Software-Anbietern, die in der Vergangenheit eher auf proprietäre Systeme gesetzt hatten, eine Tendenz zu Offenheit und Kooperation zu erkennen. Dies erstaunt nur auf den ersten Blick: Der Mehrwert, den IoT-Plattformen zu stiften vermögen, hängt entscheidend von der Integrationsfähigkeit in die bestehende IT-Landschaft des Unternehmens ab.

Szenarien eines Internet of Payments

Um pragmatische und realistische Lösungen für eine Abrechnung von IoT-spezifischen Leistungen zu finden, bedarf es der Differenzierung der verschiedenen diskutierten oder bereits etablierten kommerziellen IoT-Anwendungsszenarien.

1. Maschineninduzierte Beschaffung: Wo Geräte über Sensoren selbstständig erkennen können, dass Verbrauchsmaterial, Ersatzteile oder Serviceleistungen bezogen werden müssen, liegt es nahe, neben der Bestellung auch die Bezahlung ohne menschliche Interaktion zu ermöglichen. Es handelt sich hierbei um nicht mehr als eine Erweiterung der für Smartphones und Wea-

ables etablierten Bezahlfunktionen auf weitere smarte Devices: Leistung und Gegenleistung müssen so erfolgen, dass das Ausfallrisiko für beide Parteien vertretbar ist. Es ist eine Frage der Vertragsgestaltung, welche Partei in Vorleistung geht. Anbieter von Zahlungsdiensten wie Paypal oder Paydirekt bieten bereits Lösungen, das wechselseitige Risiko zu reduzieren. Technische Anforderungen beschränken sich hier auf die Frage, welche Services und Anwendungen benötigt werden, um Maschinen in die Lage zu versetzen, Zahlungen sicher und rechtskonform auszulösen.

2. Komplexe Modelle, insbesondere Per-Use: Spezifischere Anforderungen stellen Modelle, bei denen eine Pay-per-Use-Abrechnung über mehrere Ebenen der Supply Chain eingerichtet wird.¹⁾ Einfache Beispiele finden sich in etablierten Servicemodellen der Shareconomy: Will ein Anbieter Drittleistungen in sein Serviceangebot integrieren (beispielsweise Parkgebühren in die Fahrzeugmiete), bedarf es geeigneter Abrechnungsverfahren. Flatrate-Vereinbarungen sind wirtschaftlich häufig nicht optimal. Ein Verfahren, bei dem der Kunde Belege sammelt und sich beim Anbieter erstatten lässt, entspricht nicht dem heute erwarteten Nutzungserlebnis. Gefordert ist eine Lösung, bei der das gemietete Fahrzeug die Parkgebühren selbst und automatisch bezahlt. Der Kunde ist an diesem Vorgang nicht beteiligt, die Abrechnung erfolgt zwischen Anbieter und Parkplatzbetreiber.²⁾

Möglich scheinen auch sehr viel komplexere Anwendungsszenarien, etwa wenn Komponenten einer Maschine nutzungsabhängig bezahlt werden und der Betreiber der Anlage, in welche die Maschine verbaut ist, seinerseits nutzungsabhängige Entgelte erhebt. In einem solchen Szenario bezahlen sich technische Komponenten untereinander für die jeweils in Anspruch genommene Leistung. Dies geschieht ohne menschliche Interaktion.

Bei der Abrechnung solcher Leistungen stellen sich Fragen auf rechtlich-wirt-

schaftlicher und technischer Ebene: Rechtlich-wirtschaftlich lassen sich Leistung und Gegenleistung in diesen Szenarien anders als bei bloßen Beschaffungsvorgängen nicht durch bloße Vereinbarung risikoadäquat verzahnen. Der Nutzungsvorgang findet zunächst unabhängig von der Bezahlung statt, die genutzte Leistung kann im Falle eines Zahlungsausfalls nicht zurückgeholt werden. Ein IoP-System muss daher neue rechtliche, wirtschaftliche oder technische Lösungen für einen adäquaten Risikoausgleich finden.

Bei der Entwicklung von IoP-Lösungen ist zwischen den notwendigen Schnittstellen von IoT-Plattformen zu den bestehenden Zahlungsverkehrssystemen und der Abrechnung von IoT-Komponenten innerhalb eines Netzwerks untereinander zu differenzieren. Eine Abrechnung im Sinne eines Transfers von Buchgeld durch Überweisung oder Lastschrift setzt, gegebenenfalls über Zwischeninstanzen, eine Anbindung an die bestehenden Clearing- und Settlement-Systeme sowie an die kontenführenden Systeme der Banken voraus. Will man vermeiden, dass jede Einzeltransaktion zwischen zwei Komponenten innerhalb eines IoT-Netzwerks unmittelbar zu einer Zahlungsverkehrstransaktion führt, muss innerhalb des Netzwerks ein eigener Mechanismus der Binnenabrechnung geschaffen werden, der für sich genommen ohne Anbindung an den klassischen Zahlungsverkehr funktioniert.

Regelwerke für die Authentifizierung nicht ohne weiteres übertragbar

Im Folgenden werden, ohne Anspruch auf Vollständigkeit, einige wesentliche Unterschiede behandelt zwischen Zahlungen, die unmittelbar oder mittelbar von Personen ausgelöst werden, und jenen, deren Initiierung ohne menschliches Zutun durch Maschinen erfolgt.

Die bestehenden Regelwerke des Zahlungsverkehrs haben die Authentifizierung

durch Menschen im Blick. Diese sind nicht ohne weiteres auf die Authentifizierung durch Maschinen übertragbar. Die PSD2 als maßgebliches Regelwerk schreibt eine Zwei-Faktor-Authentifizierung vor. Diese Anforderung ist per se nicht leicht zu erfüllen, wenn sämtliche zur Authentifizierung zur Verfügung stehenden Faktoren durch ein und dasselbe Gerät und Betriebssystem verwaltet werden.³⁾

OPT-Verfahren als mögliche Blaupause

Ein Problem ist dies allerdings nur, wenn die von der Maschine initiierte Zahlungsinstruktion direkt an das Zahlungsverkehrssystem der Bank übergeben werden soll. Bietet das IoT/IoP-System die Möglichkeit, Zahlungen zu sammeln und gesammelt zu übergeben, so kann auf etablierte Verfahren wie EBICS zurückgegriffen werden. Entsprechende Funktionen sind in gängigen ERP-Systemen bereits implementiert.

Bei einer unmittelbaren Identifikation von Maschinen gegenüber einer Bank oder einem Zahlungsdienstleister bedarf es eines Verfahrens, welches eine eindeutige Identifikation des Geräts und der Transaktion sicherstellt. Nach heutigem Stand der Technik kann dies unter anderem durch den Austausch von Zertifikaten und Authentifizierungs-codes für einzelne Nachrichten zwischen den beteiligten Instanzen geschehen. Zum Schutz vor Manipulation sollte der Datenaustausch grundsätzlich verschlüsselt erfolgen. Als eine mögliche Blaupause mag hier das für Geldautomaten und PoS-Terminals etablierte OPT-Verfahren dienen.

Maschinen und Personen

Inhaber von Bankkonten und damit Teilnehmer am Zahlungsverkehr können nur natürliche oder juristische Personen sein. Maschinen besitzen keine eigene Rechtspersönlichkeit und scheiden als Kontoinhaber, Zahler oder Zahlungsempfänger

aus. Bei einer durch eine Maschine ausgelösten Zahlung muss daher stets klar sein, welcher Person diese Zahlung zuzuordnen ist. Unproblematisch ist dies, wenn die Eigentums- und Besitzverhältnisse an der beteiligten Komponente klar und in der Regel unveränderlich sind. In dem Beispiel, in dem ein Auto Parkgebühren oder Strom bezahlt, kann Zahler der Eigentümer oder der im Fahrzeugschein eingetragene Halter sein.

Schwieriger ist die Zuordnung, wenn Eigentums- und Besitzverhältnisse häufig wechseln, etwa, wenn eine Komponente einer Maschine in einer Supply Chain weiterveräußert wird. Welches Maß an Komplexität IoT-Anwendungsfälle in diesem Zusammenhang annehmen können, wird entscheidend auch davon abhängen, welche technischen Lösungen zur Abwicklung von Machine Payments mit wechselnder wirtschaftlicher und rechtlicher Zuordnung sich am Markt durchsetzen. Neben der technischen Abbildung werden zudem Fragen der Haftung und Verantwortung auch in Miet-, Kauf- und Serviceverträgen geklärt werden müssen.

Zahlungen über Instant Payments abwickeln

Im Zahlungsverkehr ist stets das Risiko zu beachten, dass eine Zahlung nicht ausgeführt werden kann, weil das Konto des Zahlers nicht existiert oder nicht die notwendige Deckung aufweist. Im Sepsa-Zahlungsverkehr besteht aus Sicht des Zahlungsempfängers erst dann Sicherheit, dass die Zahlung erfolgreich durchgeführt wird, wenn seine Bank ihm den Zahlungsbetrag gutschreibt. Bei Instant Payments ist dies innerhalb von höchstens 10 Sekunden nach Auslösung der Transaktion der Fall, sodass bei Zahlungen, die die als solche via Instant Payments abgewickelt werden, kein relevantes Ausfallrisiko besteht.

Voraussetzung ist, dass Instant Payments in der Lage ist, Zahlungsinstruk-

tionen von Maschinen unmittelbar zu verarbeiten.

Distributed-Ledger-Technologien und Kryptowährungen als Lösungsansätze

Für einige der dargestellten Problempunkte scheinen technische Lösungsansätze auf Basis von Distributed-Ledger-Technologien nahe liegend und sinnvoll. So ist denkbar, die Authentizität von Geräteidentifikationen über ein größeres Netzwerk zu verteilen und so Manipulationen durch Angriffe auf einzelne Geräte schwieriger zu machen. Denkbar ist auch hier, die Zuordnung zwischen Maschine und Zahler über dynamische Verzeichnisse in einem Distributed-Ledger zu verwalten. Gleiches gilt für die Zuordnung zwischen Maschine und Zahlungsempfänger.

Für die schnelle Abwicklung von Instant-Zahlungen können Kryptowährungen eine wichtige Rolle spielen. Denkbar sind in diesem Kontext auch hybride Lösungen. So kann der Zahlungsfluss zwischen einzelnen Komponenten in einer IoT-Kryptowährung erfolgen. Der Umtausch in Euro oder eine andere Fiat-Währung erfolgt dann durch die an das System angeschlossenen Banken.

Iota als Kryptowährung des Internet der Dinge

Hervorzuheben ist in diesem Zusammenhang Iota. Iota ist im Kern eine Kryptowährung auf Basis eines Distributed Ledger. Anders als bei Bitcoin kommt keine Blockchain-Technologie zum Einsatz. Die Vorteile von Iota sind eine hohe Abwicklungsgeschwindigkeit und Skalierbarkeit sowie geringe Transaktionskosten. Iota gilt daher allgemein als „Kryptowährung des Internet der Dinge“. Allerdings ist der Wechselkurs zu etablierten Fiat-Währungen wie Euro und US-Dollar wie bei allen frei handelbaren Kryptowährungen einer Marktpreisbildung unterworfen und daher volatil. Es bestehen Wechselkursrisiken,

die bei industriellen Anwendungen, bei denen virtuelle Recheneinheiten allein der technischen Abwicklung von Transaktionen dienen, unerwünscht sind.

Dieses Problem kann dadurch gelöst werden, dass für die Zahlungen zwischen den Komponenten keine Kryptowährung, sondern E-Geld zum Einsatz kommt, für welches der Emittent einen festen Umtauschkurs vorgibt. Möglicherweise tut sich hier ein neues Potenzial für Bankdienstleistungen im IoT-Umfeld auf. Banken können als Emittenten IoT-spezifischer Werteeinheiten die Basis für ein leistungsfähiges und kostengünstiges Internet of Payments schaffen.

Anforderungen an IoP-Software

Ein Internet of Payments benötigt Software zur sicheren Ausführung wie auch zum Clearing und Settlement der anfallenden Transaktionen. Dies gilt auf Ebene der einzelnen Komponenten, der IoT-/IoP-Plattformen und der beteiligten Banken. Relevante Faktoren sind neben der Komplexität des Gesamtsystems die gewünschte oder benötigte Autonomie und die zur Verfügung stehende Rechenleistung der einzelnen IoT-Komponenten.

Komponenten: Jede Komponente muss jedenfalls über die Fähigkeit verfügen, sich eindeutig gegenüber dem IoP-System zu authentifizieren. Es ist eine Frage des konkreten Anwendungsfalls, ob Komponenten Transaktionen untereinander unabhängig von einer zentralen Instanz ausführen. In einem auf Edge-Computing ausgerichteten Netzwerk ist durchaus denkbar, dass Komponenten IoT-spezifische Werteeinheiten unter Verwendung von Distributed-Ledger-Technologien rechtswirksam untereinander austauschen, ohne, dass jede Transaktion über einen zentralen Server autorisiert wird.

Eine solche Architektur ist insbesondere im Sinne der Offline-Fähigkeit der IoT-Komponenten sinnvoll. Heutige End-

geräte, bei denen die Autorisierung von Zahlungen über zentrale Server läuft (zum Beispiel Geldautomaten), gehen außer Betrieb, wenn die zentrale Instanz nicht erreichbar ist oder eine für die Zahlung relevante Komponente gestört ist. Bei einer Maschine, bei der die beteiligte Komponente für das Funktionieren eines technischen Gesamtsystems mitverantwortlich ist, kann ein solches Verhalten höchst unerwünscht sein. Gleichwohl ist zu definieren, wie die Maschine sich verhalten soll, wenn sie zwar technisch funktioniert, jedoch vorübergehend nicht in der Lage ist, die erbrachten Leistungen abzurechnen. Hier kann eine Verbindung von Edge-Computing und Distributed-Ledger-Technologien die benötigte Ausfallsicherheit schaffen.

IoT/ IoP-Plattformen: Bestehende IoT-Systeme verfügen in aller Regel über zentrale Plattformen zum Management und zur Integration der angeschlossenen Komponenten. Für ein Internet of Payments ist es nicht ausreichend, solche Plattformen einfach um Bezahlfunktionen zu erweitern. Wenn ein Softwaresystem Zahlungsverkehrsfunktionen ausführt, gelten spezifische fachliche, technische und regulatorische Anforderungen. Eine Software-Applikation, die den Initiator einer Zahlung authentifiziert, Zahlungen autorisiert und ausführt, muss stets sicherstellen, dass der Status der Zahlung zu jedem Zeitpunkt und auch im Falle von Störungen bankfachlich und regulatorisch korrekt und revisionssicher dokumentiert ist. Entscheidende Bedeutung kommt hier dem Monitoring der beteiligten Komponenten zu, welches auch Grundlage für die Bearbeitung von Reklamationen ist. Die Tabelle gibt einen Überblick über wesentliche funktionale und nichtfunktionale Anforderungen, welche sich aus diesem Grundsatz ableiten.

Eine weitere wesentliche Anforderung an IoP-Plattformen ist die Offenheit gegenüber anderen Systemen. IoT trägt das Prinzip der Ubiquität und Vernetzung in sich. Proprietäre Abschottung wirkt diesem Prinzip

Wesentliche Anforderungen an IoP-Plattformen

Communication	Message Processing	Security	Management	Non-Functional
Format Validation	Format Mapping	Encryption/Key Management	Transaction Retrieval	24/7 Availability
Timeout Handling	Transaction Chaining	Authentication	Single Point of Truth	PCI Compliance
	Store and Forwarding	Anti-Fraud-Service	Statistik Data	Realtime
				Auditing Acceptability
				Scalability
				Multi-Client Capability

Quelle: DPS Engineering GmbH

entgegen. Es fällt auf, dass die Hersteller von IoT-Plattformen, auch solche, die sonst eine konsequent proprietäre Geschäftspolitik verfolgen, die Offenheit ihrer Lösungen betonen. Letztlich durchsetzen können sich nur solche Systeme, die zu einer selbstverständlichen Interoperabilität mit anderen IoP-Plattformen und konventionellen Payments-Systemen fähig sind.

Banksysteme: Banksysteme müssen in der Lage sein, durch ein IoP-System initiierte Transaktionen zu verarbeiten. Hier sind schon in der heutigen Sepa-Welt unterschiedlichste Konstellationen denkbar. Im einfachsten, unproblematischen Fall reicht das IoP-System Zahlungsstrukturen bei der Bank des Betreibers ein, wie dies heute ERP-Systeme tun. Der Betreiber eines IoP-Systems kann auch als Payment Initiation Service Provider gemäß den Vorgaben der PSD2 Zahlungen initiieren. Tritt die Bank selbst als Dienstleister für IoP-Infrastrukturen auf, werden für die neuen bankfachlichen Funktionalitäten entsprechende Software-Komponenten benötigt, welche dann sinnvollerweise direkt mit den Kernbanksystemen interagieren.

Rechtzeitig entscheidende Impulse setzen

Die Entwicklung eines spezifischen Internet of Payments hat noch nicht begonnen.

Markt, Teilnehmer, Geschäftsmodelle und regulatorische Rahmenbedingungen werden sich erst noch entwickeln. Banken wie Service Provider sind in einer digitalen Welt gleichwohl selten gut beraten, vor einer Entscheidung über die eigene Positionierung die allgemeine Entwicklung abzuwarten. In einer digitalen Welt werden Marktanteile verteilt, bevor Geschäftsmodelle und Technologien den erwarteten Reifegrad haben.

Festzuhalten ist, dass IoP das Rad nicht völlig neu erfinden muss. Etablierte Anwendungen etwa im Bereich Customer Self Service und Omnichannel Banking bringen viele der benötigten Funktionen bereits mit. Für die Skalierung in eine Welt auf Millionen beteiligter Endgeräte mit kleinen Chips und begrenzter Rechenleistungen werden diese um neue technische Fertigkeiten und Servicekonzepte zu erweitern sein. Hier können Banken wie Technologie-Provider entscheidende Impulse setzen.

Fußnoten

- 1) Vgl. hierzu Pähler und Rundshagen, Das Internet der Dinge erfordert neue Finanzdienstleistungen, in: Brühl, Dorschel, Praxishandbuch Digital Banking, 2018 S.344 ff.
- 2) Für weitere Beispiele vgl. auch Kamat, The „Internet of Payments“ is tech’s next hyper-growth sector, abrufbar unter www.paymentssource.com.
- 3) Diese Frage wird auch im Zusammenhang mit dem Mobile-TAN-Verfahren unter der PSD2 als kritisch diskutiert, vgl. hierzu Göbel, Chancen und Herausforderungen durch die PSD2 und Instant Payments, in: Hierl (Hrsg.) Mobile Payment, 2017, S. 167 ff.