

gi
GELDINSTITUTE

+++ SPECIAL +++
**Security for Finance
and Insurance**

GELDINSTITUTE

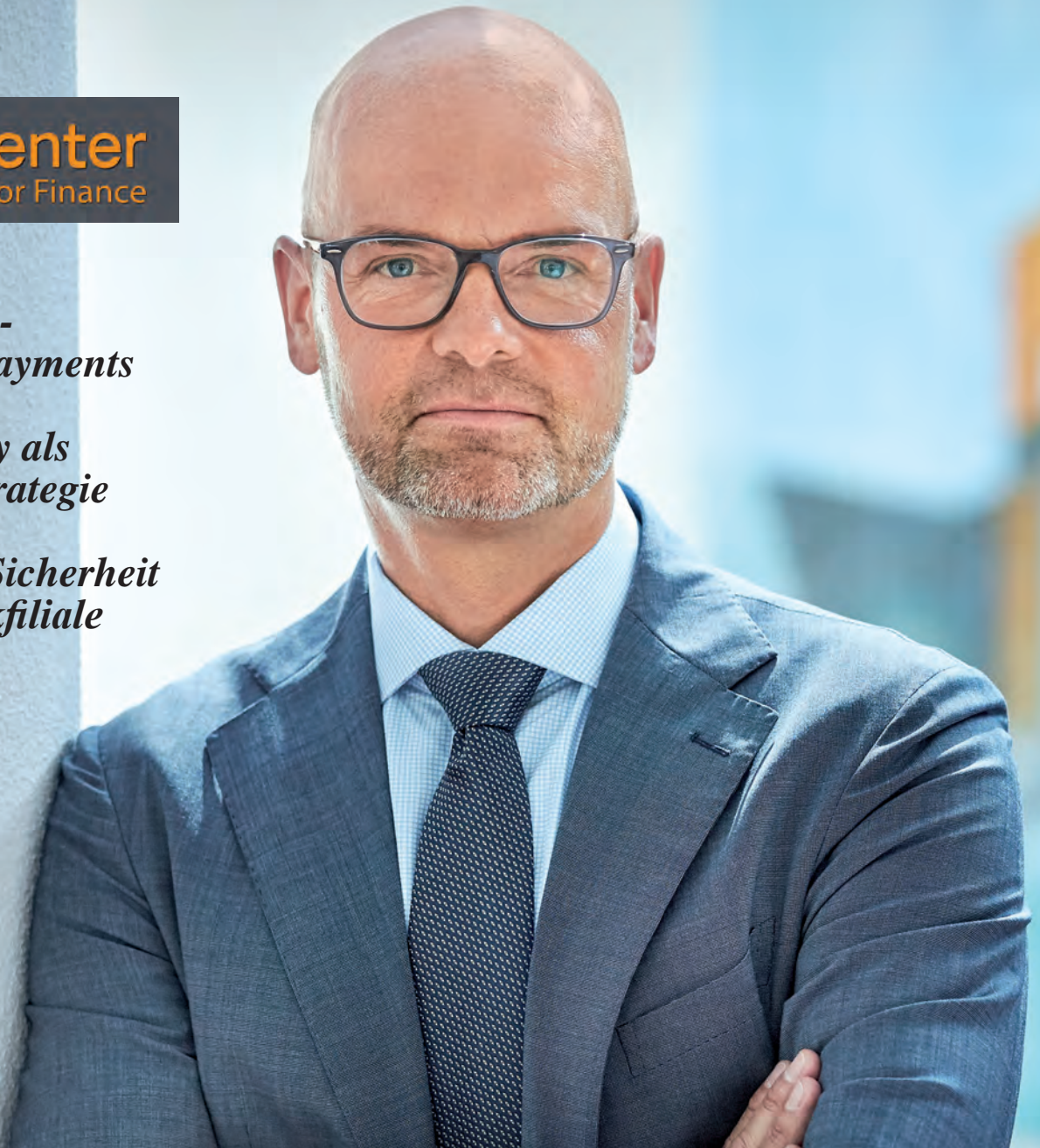
Fachzeitschrift für IT-Entscheider und Manager

CallCenter
Ausgabe 2/2020 for Finance

*Machine-to-
Machine-Payments*

*Bug-Bounty als
Security-Strategie*

*Physische Sicherheit
in der Bankfiliale*



Daten treiben Kosteneffizienz

Ansgar Steden, Vice President Banking DACH bei Diebold Nixdorf, spricht im Interview über Vorbilder, partnerschaftliche Kooperationen und Zukunftsszenarien.

Den Einkauf zahlt die Maschine

Ohne Machine-to-Machine-Payments (M2M-Payments), also autonom zwischen Maschinen getätigten Zahlungstransaktionen, wird das Internet of Things Stückwerk bleiben. Damit das nicht passiert arbeiten Politik und Wirtschaft daran, rechtliche und technische Hindernisse aus dem Weg zu räumen. Zahlungsdienstleister tun gut daran, sich bereits jetzt Gedanken über die Implementierung zu machen.



Autor:
Michael Titsch,
Managing
Consultant und
Experte für Pro-
jektmanagement,
Payments und
Banking

Das Internet of Things (IoT) ist auf dem besten Weg, die Welt zu verändern. Ein Blick auf die Zahlen verdeutlicht die Dimensionen: Aktuell sind etwa 27 Milliarden vernetzte Geräte im Einsatz, Experten rechnen bis 2025 mit einer Verdreifachung. Die zu erwartenden Benefits sind vielfältig. So ist eine höhere Wertschöpfung durch präziseres Prozesswissen möglich, ebenso genauere Lagebilder, Reaktionen in Echtzeit, neue Fähigkeiten von Systemen und vieles mehr. Das Wissen um Vorgänge und Interaktionen verbessert die Entscheidungsgrundlage für künftiges Handeln, senkt Kosten und erlaubt die Konzeption individuellerer Problemlösungen. Auch müssen Geräte für bestimmte Leistungen nicht mehr gekauft, geleast oder gemietet werden. Stattdessen wird die Nutzung abgerechnet.



Bei der Implementierung von M2M-Payments sind vielfältige Fragestellungen zu klären, mit deren Beantwortung möglichst bald begonnen werden sollte

IoT braucht autonome Bezahlverfahren

Aber wer bezahlt wie und wann eben diese Abrechnung? Die Frage ist zu klären, wenn das IoT seine Wertschöpfungskraft heben soll. Denn bislang lassen sich Zahlungen für erbrachte Leistungen zwar automatisiert einfordern, für die Bezahlung aber muss der Mensch selbst handeln, indem er die Transaktion autorisiert. Das kostet Zeit, ist fehleranfällig und

bringt so den Gesamtprozess ins Stocken. Beispielsweise wäre ein intelligenter Kühlschrank in der Lage festzustellen, dass die Milch aufgebraucht ist. Auch die Nachbestellung würde funktionieren. Aber der Onlinehändler müsste auf die Zahlung solange warten, bis der Kühlschrankbesitzer die Summe freigibt.

Die Lösung: vollkommen autonome Zahlungsströme zwischen Geräten, sogenannte Machine-to-Machine-Payments.

Nur damit werden alle Vorteile des IoT nutzbar sein. Das Marktpotenzial ist enorm, denn es ist mit bis zu 85 Milliarden Transaktionen bis 2027 alleine im Euroraum zu rechnen. Diese Dimension zeigt, warum Zahlungsdienstleister sich möglichst bald auf den Markt der M2M-Payments vorbereiten sollten.

Rechtliche Voraussetzungen

Zunächst einmal müssen die rechtlichen Grundlagen vorhanden sein. So fehlt es Maschinen bisher an einer eigenen Rechtspersönlichkeit, was Regelungen zu Haftung und Authentifizierung verhindert. Entsprechende Vorschriften sind national und international in Arbeit.

Die zweite Schwierigkeit liegt in der Schaffung rechtsverbindlicher Maschinenidentitäten. Schließlich muss jede Handlung eindeutig einer bestimmten Maschine zuzuschreiben sein. Hier wird vermutlich alles auf die Verwendung digitaler Zertifikate hinauslaufen. Für deren universelle Gültigkeit bedarf es der Einschaltung neutraler Instanzen, beispielsweise der Bundesdruckerei oder GlobalSign.

Grundlegende Handlungsfelder

Sind diese Herausforderungen zufriedenstellend bewältigt, steht der Implementierung von M2M-Payments an sich nichts

mehr im Wege. Da es aber eine ganze Reihe unterschiedlicher praktischer Aspekte gibt, zu denen Standards und Handlungsempfehlungen zu entwickeln sind, sollten Finanzdienstleister mit den Vorarbeiten beginnen.

Die Themenfelder im Einzelnen:

• **Sicherheit von Maschinen**

Offene Schnittstellen, Datenaustausch mit Drittanbietern, ein hoher Vernetzungsgrad und vielfach einfache Software bieten Angriffsflächen für Cyberkriminelle. Der potenzielle Schaden durch unbefugt ausgelöste M2M-Zahlungsströme ist enorm. Hier sind vor allem die IoT-Betreiber gefragt, in enger Abstimmung mit den Zahlungsdienstleistern einer möglichen Vertrauenserosion vorzubeugen.

• **Digitales Onboarding**

Die Anmeldeverfahren zu M2M-Payments für eine erste Gerätegeneration ließen sich vielleicht noch manuell bewältigen. Bei einer millionenfachen Etablierung autonomer Maschinen ist dem aber nur noch digital und vollautomatisiert nachzukommen.

• **Compliance für Maschinen**

Hieß es bislang „Know your customer“ (KYC), wird zukünftig „Know your object“ (KYO) wichtig. Finanzdienstleister müssen Prüf- und Dokumentationsprozesse hinsichtlich der Vertrauens-

würdigkeit und wirtschaftlichen Zuordnung einer Maschine entwickeln.

• **Identifikation von Maschinenzahlungen**

Die Zahlungsverkehrssysteme müssen um Felder und Funktionen zur eindeutigen Zuordnung einer Maschine erweitert werden, etwa deren Autorisierungsmethode oder das Identitätszertifikat.

• **Verarbeitung von Rückinformationen**







Maschinen müssen – je nach genutztem Zahlverfahren – auch in der Lage sein, prozessuale und technische Störungen zu verarbeiten. Das umfasst insbesondere Fälle wie


- Dispositionsprüfung mit negativem Ergebnis,
- fehlende Zahlungseingangsbestätigungen,
- Widerruf von Zahlungen,
- technische Unterbrechungen in der Zahlungskette,
- Angriffe auf die Maschine und
- Erkennen von Betrugsfällen.

• **Komplexes Reporting**

Aufbereitung und Abrechnung von maschinellen Nutzungsdaten sowie zusätzlichen Informationen über die Maschinen müssen für unterschiedliche Reportings konfiguriert sein. Entsprechend hohen Anforderungen unterliegt die Datenstruktur.

Welche Bezahlverfahren am besten passen

| Elektronisches Bezahlverfahren | M2M-geeignet* | Herausforderungen |
|--|---------------|---|
|  Klassischer ZV „alt“ (SCT und SDD) | ☆☆☆ | <ul style="list-style-type: none"> • Erreichbarkeit • Geschwindigkeit • Skalierung |
|  Klassischer ZV „neu“ (SEPAInst und R2P) | ★★☆ | <ul style="list-style-type: none"> • Erreichbarkeit • Geschwindigkeit • Regulierung |
|  Kartengestützter ZV | ★☆☆ | <ul style="list-style-type: none"> • Kosten |
|  eGeld | ★★★ | <ul style="list-style-type: none"> • Regulierung |
|  Digitales Geld (stable Coin) | ★★★ | <ul style="list-style-type: none"> • Akzeptanz • Marktreife • Regulierung |
|  Digitales Geld (unbacked Coin) | ★☆☆ | <ul style="list-style-type: none"> • Akzeptanz • Skalierung • Regulierung • Starke Wertschwankungen |



Verlagerung vom Konto zur Wallet?

* Ausprägung in Abhängigkeit zu den Entwicklungsschritten: ○ = nicht geeignet, ★ = eingeschränkt geeignet, ★★ = gut geeignet, ★★★ = besonders gut geeignet.

Übersicht über die denkbaren Bezahlverfahren für M2M-Payments

Entscheidung für ein Bezahlverfahren

Wichtig ist auch die Wahl des geeigneten Verfahrens für intermaschinelles Bezahlen, gekoppelt mit der Überlegung, über welche Infrastrukturen die Abrechnung beim Kunden erfolgen soll:

- Klassischer Zahlungsverkehr – SEPA-Verfahren der Kreditwirtschaft
- Kartengestützter Zahlungsverkehr – Debit- und Kreditkarten
- E-Geld – geschlossene virtuelle Kontosysteme
- Digitales Geld – Unbacked Coins beziehungsweise Stable Coins

Da für das IoT mit vielen Transaktionen von Kleinstbeträgen zu rechnen ist, dürfen Kryptogeld- und E-Geld-Lösungen besonders attraktiv sein. Denn sie eröff-

nen die Möglichkeit, auch Dienstleistungen von nur geringem Wert – selbst unter einem Cent – wirtschaftlich abzurechnen, beispielsweise die Nutzung einer Glühbirne im Smart Home. Sie sind zudem unabhängig von klassischen Finanzdienstleistern integrierbar. Allerdings muss Kryptogeld die Fähigkeit zur Echtzeitverarbeitung großer Transaktionsmengen noch beweisen.

Zudem stellt sich bei Unbacked Coins die Frage nach dem Umgang mit starken Wertschwankungen. Zur Verwendung der Bezahlverfahren im IoT kommt insbesondere eine Wallet in Betracht, in der Zugangsdaten für verschiedene Zahlungsnetzwerke hinterlegt sind. Nutzt eine Maschine die Wallet, so wird die priorisierte Zahlungsmethode automatisch verwendet oder durch Auswahl ein alternatives Zahlungsverfahren bestimmt.

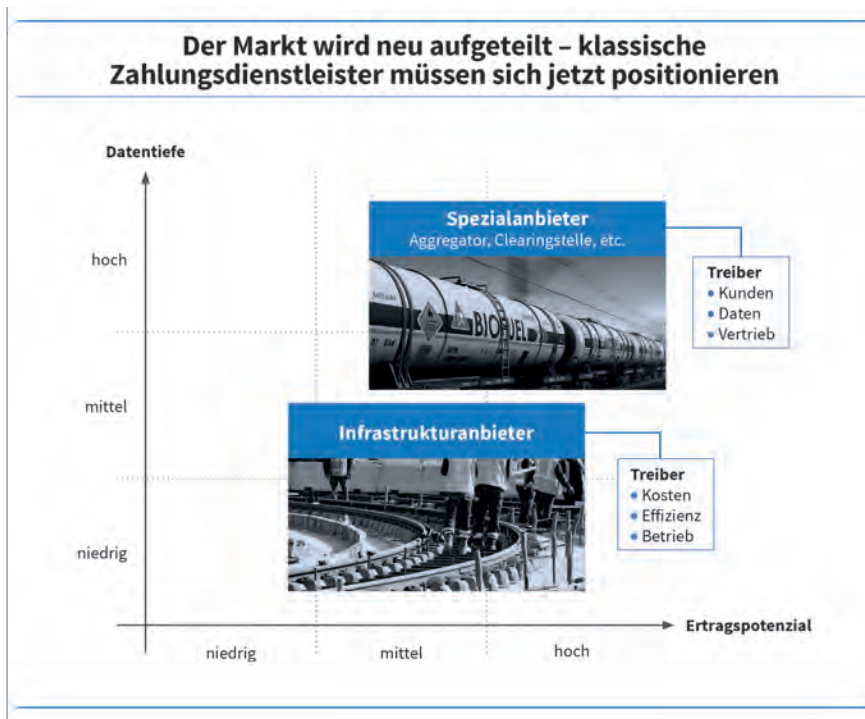
Darüber hinaus hat die Finanzindustrie mit ihren Bezahlverfahren Instant Payments und Request to Pay die Basis für die Nutzung im Internet of Things geschaffen.

Folgen für das Geschäftsmodell

Neben diesen eher technischen Angelegenheiten sollten sich Finanzdienstleister darüber klar werden, wie sie am künftigen Markt für M2M-Payments auftreten wollen. Bleiben sie reine Infrastrukturanbieter oder entwickeln sie selbst Kundenlösungen und datenbasierte Geschäftsmodelle? Für die zweite Strategie spricht die Tatsache, dass die Zahlungsdienstleister auf einem gewaltigen Datenschatz sitzen, der durch die Zunahme von IoT-Geräten noch weiter anwachsen dürfte – mit der Folge, dass sich zusätzliche Geschäftspotenziale beziehungsweise -modelle ergeben. So lassen sich zum Beispiel auf Basis detaillierter Verbrauchsdaten an diese angepasste Finanzierungsmodelle entwickeln. Finanzdienstleister könnten auch Datenmarktplätze organisieren oder als zentrale FX-Plattformen für digitale Währungen auftreten.

Aber dafür muss es den Anbietern gelingen, sich „auf“ den Maschinen zu platzieren, um sich diese Daten zu sichern. Zumindest aber müssen sie als Aggregator fungieren, der die Nutzungsdaten zu Zahldaten bündelt und diese transferiert. Denn der Wettbewerber, der über die primären Nutzungsdaten verfügt, wird am Ende demjenigen überlegen sein, der nur die sekundären, sprich abgeleiteten Zahldaten des Kunden kennt.

Gerade im Hinblick auf eine Rolle als Datenaggregator könnten Zahlungsdienstleister zudem für das nötige Vertrauen bei allen Beteiligten sorgen. Denkbar wäre zum Beispiel die Funktion als eine Art Clearing-Stelle für sichere digitale Identitäten und valide Daten. Schließlich genießen sie ein hohes Vertrauen hinsichtlich Identitätsverwaltung, Datenschutz und auch IT-Security. Ein Aspekt dabei ist die Tatsache, dass – wie die Beispiele von Google, Facebook und Apple zeigen – derjenige Player den Hebel für weiteres Geschäft in der Hand hält, der die digitalen Identitäten kontrolliert.



Beim Eintritt in den Markt von M2M-Payments müssen Finanzdienstleister eine Grundsatzentscheidung treffen, deren Richtung von verschiedenen Treibern bestimmt wird

Veränderungen in der Kundenstruktur

Auch der Vertrieb der Zahlungsdienstleister wird sich mit steigender Bedeutung von IoT und M2M-Payments neu aufstellen müssen. Denn die Bedeutung von Ökosystemen wächst, etwa beim autonomen oder teilautonomen Fahren. Dann entscheidet nicht mehr der einzelne Wirtschaftsteilnehmer, über welche Bezahlfahrer Produkte oder Dienstleistungen abrechnet. Stattdessen muss er die Möglichkeiten des Ökosystems verwenden, innerhalb dessen er sich gerade bewegt. Beispielsweise gibt der Flottenanbieter vor, wie und womit Kraftstoffe beziehungsweise Energie für ein Fahrzeug zu bezahlen sind. Für die Vertriebsorganisationen bedeutet das einen – teilweisen – Abschied von der Betreuung einzelner Unternehmen oder Privatkunden hin zur Betreuung von Ökosystemen.

Systemlandschaften an der Belastungsgrenze

Bereits jetzt sollten Zahlungsdienstleister Investitionen in ihre IT-Infrastruktur planen. Denn: Die Anforderungen von M2M-Payments an die Lastfähigkeit, die Verfügbarkeit und die Skalierbarkeit sind

mit den historisch gewachsenen Systemlandschaften der europäischen Finanzdienstleister nicht auf Dauer zu erfüllen. Künftig müssen Zahlungsverkehrssysteme und ihre Umsysteme maschinelle von nicht-maschinellen Zahlungen unterscheiden können, da diese nach unterschiedlichen Regeln ablaufen. Sie müssen das Onboarding von Maschinen automatisiert durchführen sowie Identitäten und Zertifizierungen verifizieren. Das bereits beschriebene KYO muss in den Systemen abgebildet und organisiert sein. Hinzu kommen Rückinformationen aus System- und Prozessstörungen sowie deren Verarbeitung.

Zugleich sind künftig signifikant mehr Transaktionen zu bewältigen, bei paralleler Zunahme der Bedeutung von 24/7/365-Betriebsmodellen und Echtzeitfähigkeit. Zwar können auch im IoT Zah-

lungen mit einem zeitlichen Abstand zum Grundgeschäft akzeptabel sein. In vielen Fällen dürfte aber erwartet werden, dass auf den sofortigen Informationsaustausch beziehungsweise die sofortige Leistungserbringung oder Nutzung auch eine unmittelbare Zahlungsauslösung durch die Maschine folgt. Hostbasierte Lösungen oder Downtimes für das Einspielen neuer Releases werden damit immer inakzeptabler.

Die Zeit läuft

Angesichts des Klärungsbedarfs, der Infrastrukturarbeiten und Grundsatzentscheidungen wird klar, dass die Zeit gegen die Zahlungsdienstleister läuft. Eine prognostizierte Verdreifachung der IoT-Geräteanzahl innerhalb von gerade einmal fünf Jahren ist ein klares Signal zum Aufbruch in die neue Zeit eines Internet of Payments.

Aktuelle Studie

Details und weitere Informationen zu Herausforderungen und Chancen durch M2M-Payments für Zahlungsdienstleister sind in der unlängst erschienenen Studie „Internet of Payments“ des Hamburger Beratungs- und Softwarehauses PPI nachzulesen. Diese kann auf der Website von PPI kostenlos angefordert werden: www.ppi.de/studie-iop