Maschinenidentitäten

Schlüssel zum Internet der Dinge

(Studie)

Mit freundlicher Unterstützung von

Autor: Ralf Keuper

September 2019

Inhaltsverzeichnis

Zusammenfassung

Das Identitätsmanagement war in der Vergangenheit eher eine lästige Pflicht in den Unternehmen. Wichtig war und ist auch noch, nur zugangsberechtigten Personen oder Organisationen Zugang zum Unternehmen und seinen IT-Systemen zu gestatten. Die Produktion war von der Außenwelt, sprich dem Internet weitestgehend abgeschlossen. Mit dem Aufkommen von Industrie 4.0, dem Internet der Dinge und dem Industriellen Internet der Dinge ändert sich das. In der vernetzten Produktion kommunizieren und interagieren die Unternehmen mehr oder weniger direkt miteinander. In ihrem Auftrag agieren nicht selten Maschinen und Geräte, die, so jedenfalls sieht es die Machine Economy vor, selbständig Aufträge erteilen und Rechnungen bezahlen können.

Unternehmen und Kunden müssen sich darauf verlassen können, dass die Maschinen auch nur das tun, wofür sie berechtigt sind, und sich nicht als jemand anderes ausgeben. Aufgrund der Komplexität wäre jedes Unternehmen damit überfordert, die Identitäten der Maschinen, Komponenten und Prozesse zu verifizieren. Diese Aufgabe übernehmen häufig Certificate Authorities (CA), die Maschinenzertifikate bereitstellen. Dennoch bleiben Sicherheitslücken. Die Daten, die zwischen den Maschinen ausgetauscht werden, müssen ebenfalls validiert werden. Das nötige Vertrauensniveau kann entweder durch spezielle Institutionen, integrierte Lösungen (Identity of Things - Plattformen), Standards oder durch die Blockchain-Technologie hergestellt werden.

In den letzten zwei bis drei Jahren sind zahlreiche Startups entstanden, die für das nötige Vertrauenslevel in der Machine Economy sorgen wollen. Die meisten von ihnen setzen dabei auf die Blockchain-Technologie. Einige kooperieren. So kommt es vor, dass ein Startup sich auf die Integrität der IoT-Daten und die Bereitstellung der nötigen technischen und organisatorischen Infrastruktur konzentriert, während das andere Startup sichere Digitale Identitäten für Maschinen und Digitale Zwillinge beisteuert. Andere wiederum haben sich auf das Management von Maschinenzertifikaten spezialisiert und treiben parallel den Aufbau eines entsprechenden Ökosystems voran.

Im Hintergrund sind die großen Technologiekonzerne dabei, das Identitätsmanagement für die Unternehmen zu übernehmen. Daneben drängen die Anbieter von Procurement-Lösungen in den Markt.

Das Identitätsmanagement bekommt für die Unternehmen, ja sogar für ganze Volkswirtschaften eine hohe strategische Bedeutung. Die Unternehmen werden versuchen, eine zu große Abhängigkeit von einem Anbieter zu vermeiden und bei der Wahl der geeigneten Lösung zum Management der Maschinenidentitäten flexibel zu bleiben. Diesem Wunsch steht der Mangel an anerkannten Standards für sichere Maschinenidentitäten jedoch entgegen.

Zwar fehlt es nicht an Initiativen – gleichwohl erreicht bislang keine von ihnen die kritische Größe.

In der Wirtschaft der Zukunft verliert das fertige Produkt an Bedeutung – Lieferanten werden zu Betreibern, die keine Produkte mehr, sondern Services verkaufen. Banken und Versicherer müssen sich ebenfalls auf diesen Wandel einstellen. Parallel dazu werden sich die Informationstechnologie und die Operational Technology annähern, womöglich sogar verschmelzen.
Erfolgskritisch, so ein weiteres Ergebnis dieser Studie, wird die Beherrschung der Kombination von Hardware und Software sein. Eine wichtige Rolle übernehmen dabei Chips. Die Kombination aus Blockchain, Künstlicher Intelligenz und Graphentechnologie könnte der „Missing Link“ sein, der die verschiedenen Teile technologisch zusammenbringt. Eine entscheidende Rolle übernimmt dabei, so ein weiteres Ergebnis, das Identity Relationship Management (IRM).

Das IRM wird einen wichtigen Beitrag bei der Bewältigung der Komplexität in der vernetzten Wirtschaft und Gesellschaft zu übernehmen haben. Die Komplexität allein wird dafür sorgen, dass kein Unternehmen, sei es auch noch so groß, den Markt für Maschinenidentitäten bzw. für Identity of Things beherrschen wird. Wirtschaft und Gesellschaft werden zwangsläufig dezentraler – Ökosysteme lösen zentrale Systeme in vielen Bereichen ab; das gilt in besonderer Weise für die Maschinenidentitäten.

Der Markt für Maschinenidentitäten oder allgemeiner der für Identity of Things (IDoT) birgt großes Wachstumspotenzial. Noch befindet sich der Markt in der Findungsphase. Viel hängt davon ab, ob es in absehbarer Zeit einen anerkannten Standard für Maschinenidentitäten geben wird und es in Europa gelingt, die verschiedenen Akteure von der Bedeutung des Themas zu überzeugen. Hierzu einen Beitrag zu leisten, ist das Ziel der vorliegenden Studie.

Einleitung

Eine zunehmend vernetzte Wirtschaft erfordert von den Maschinen ein bestimmtes Maß an Autonomie. Wenn jedesmal, bevor eine Maschine einen Auftrag ausführt, von Menschen geprüft werden müsste, ob sie dazu berechtigt ist, brächte das einen enormen Aufwand mit sich. Die Effizienz würde ebenso darunter leiden wie die Reaktionsgeschwindigkeit auf sich ändernde Markt- und Kundenbedürfnisse. Die Kommunikation zwischen Maschinen über Unternehmensgrenzen hinweg ist ohne entsprechende Sicherheitsstandards riskant. Eine wesentliche Rolle übernehmen dabei Maschinenidentitäten. Sie geben der Maschine eine unverwechselbare, sichere Identität, mit der sie sich in der vernetzten Produktion anderen Maschinen, Instanzen und Akteuren gegenüber ausweisen kann.

Im Internet der Dinge (IoT) ebenso wie im Industriellen Internet der Dinge (IIoT) tauschen Maschinen, Prozesse und Komponenten Daten untereinander aus. Für die sichere Identifizierung der Maschinen und für die Validierung der Daten stehen mittlerweile verschiedene Verfahren und Standards zur Verfügung. Häufig übernehmen zentrale Plattformen wie AWS oder Predix das Identitätsmanagement. Ein dezentrales Identitätsmanagement könnte mit der Blockchain-Technologie Wirklichkeit werden. Zahlreiche Startups arbeiten derzeit intensiv an der Verknüpfung zwischen der Blockchain und dem Internet der Dinge.

Ähnlich wie die Nutzer heute im Internet von den großen Datenkonzernen mit einem Profil und damit mit einem digitalen Doppelgänger versehen werden, bekommen Maschinen einen digitalen Zwilling. Der Zwilling beinhaltet die wesentlichen Merkmale und Eigenschaften der Maschine. Er tritt als ihr Stellvertreter mit den Digitalen Zwillingen der anderen Maschinen in Interaktion und Kommunikation.

In der Machine Economy ist es demnächst selbstverständlich, dass Maschinen sich gegenseitig beauftragen und bezahlen können. Eine wichtige Rolle soll dabei die Blockchain-Technologie übernehmen. Angedacht ist, dass sog. Smart Contracts, sobald bestimmte Bedingungen erfüllt und Ereignisse eingetreten sind, automatisch Transaktionen oder Produktionsprozesse auslösen. Die Zahlungsabwicklung übernehmen u.a. sog. IoT- und M2M-Payments Lösungen. Bislang sind die Projekte jedoch noch nicht über die PoC-Phase hinausgekommen.

Überhaupt deutet sich an, dass der Finanzsektor und das Internet der Dinge künftig nahe zusammenrücken. Banken und Versicherungen könnten für das nötige Vertrauen zwischen den beteiligten Personen, Unternehmen und Maschinen sorgen und dabei als eine Art Clearingstelle für sichere Digitale Identitäten und valide Daten fungieren. Oder aber neue Technologien, wie die

Blockchain in Kombination mit den Verfahren der Künstlichen Intelligenz, sind in der Lage, dieses Vertrauen ohne weitere externe Instanz herzustellen. Jedenfalls können Banken und Versicherungen einen erheblichen Beitrag dazu leisten, das Potenzial des Internet der Dinge zu heben, wie etwa mit dem Digital Twin Financing.

Digitale Identitäten, so der Tenor eines Beitrags vor einigen Monaten, sind die Dampfmaschinen der digitalen Ökonomie [1] . Die Bedeutung sicherer Maschinenidentitäten kann daher kaum überschätzt werden, zumal die Zahl der Geräte, Komponenten und Prozesse in den nächsten Jahren exponentiell steigen wird. Neue Formen der Finanzierung wie auch der Zahlungsabwicklung ebenso wie das Object oder Identity Marketing sind denkbar. Allein, der Weg bis dahin ist noch lang. Ohne ein Mindestmaß an Sicherheit, sowohl was die Hardware- als auch die Software-Seite betrifft, werden viele Szenarien hypothetischer Natur bleiben.

Ziel der vorliegenden Studie ist es, das Potenzial, welches durch sichere Maschinenidentitäten gehoben werden kann, zu verdeutlichen, ohne die Risiken dabei auszublenden. Es ist dringend nötig, dass die Diskussion um die Rolle der Maschinenidentitäten wie überhaupt der sicheren Identifizierung im Internet der Dinge den Weg in die interessierte Öffentlichkeit findet. Das um so mehr, als die Zukunft der Wirtschaft in Europa eng mit diesem Thema verbunden ist. Wer die digitalen Identitäten kontrolliert, das zeigt das Beispiel des kommerziellen Internets mit Google, facebook und Apple, hat den Hebel in der Hand, um weiteres Geschäft an sich zu ziehen. Sollte sich diese Entwicklung im Internet der Dinge bzw. im Industriellen Internet der Dinge wiederholen, d.h. die Amazonifikation auch die Industrie erreichen[2], sieht es für die Zukunft der Wirtschaft in Europa nicht sonderlich gut aus. Europas wirtschaftlicher Erfolg gründet zum einen auf seiner dezentralen Struktur, die dem Wettbewerb um die besten Ideen förderlich ist, verdankt sich zum anderen aber auch der Fähigkeit, sich dort zusammen zu tun, wo es sinnvoll ist und nur alle zusammen das nötige Mindestgewicht auf die Waage bringen, wie seinerzeit im Europäischen Währungssystem und in jüngerer Zeit in Form des digitalen Binnenmarktes.

[1] Identity is the Steam Engine of the Digital Economy
[2] Auf der Suche nach dem Amazon für Investitionsgüter Made in Germany

Definition Maschinenidentität

Das Wort „Maschinenidentität“ geht einem relativ leicht über die Lippen - nur, was hat man unter einer Maschinenidentität zu verstehen? Selbst unter einer Maschine stellt sich wohl jeder etwas anderes vor. Allgemein formuliert sind Maschinenidentitäten wie beim Menschen individuelle Merkmale, die sie von anderen unterscheiden. Eine sichere Maschinenidentität kann nicht manipuliert, gefälscht oder missbraucht werden. Die Identität einer Maschine wird in der Regel durch ein digitales Zertifikat bestätigt. Damit kann sich eine Maschine gegenüber anderen ausweisen[3]. Bei einem digitalen Zertifikat handelt es sich um einen elektronischen Datensatz, der die Identitätsinformationen der Anlage enthält, wobei die Angaben mit kryptografischen Verschlüsselungsmechanismen geschützt sind[4]. Zwar können Unternehmen selber Zertifikate für ihre Maschinen ausstellen, jedoch werden diese dann von anderen Maschinen als unsicher eingestuft, da die Beglaubigung durch eine dritte Instanz fehlt. Diese Aufgabe übernehmen Dienstleister wie die Bundesdruckerei oder GlobalSign. Damit ein Unternehmen ein Zertifikat für seine Maschinen bekommen kann, muss es sich zunächst gegenüber dem VDA ausweisen, z.B. mit dem Handelsregisterauszug. Da es sich bei digitalen Zertifikaten um Software handelt, benötigen sie die Verbindung mit Hardware. Beispielsweise können die Zertifikate auf einer Chipkarte oder einem sogenannten Hardware-Sicherheitsmodul gespeichert werden[5].

Eine potenzielle Schwachstelle stellen die Code Signature bzw. die betrügerische Verwendung der Code Signing Credentials dar[6]. Verschiedene Studien[7] kamen zu dem Ergebnis, dass es für Hacker relativ leicht ist, Code Signing Zertifikate zu erhalten und damit schadhaften Code zu verbreiten. Es sei dringend geboten, die Identität der Käufer digitaler Zertifikate genauer zu überprüfen, etwa durch Due Dilligence – Prozesse.

In der Industrie 4.0 bekommt jede Maschine nach Möglichkeit einen digitalen Zwilling zur Seite gestellt. Der digitale Zwilling enthält die wesentlichen Merkmale der Maschine, des Prozesses oder der gesamten Infrastruktur. Dabei kann ein Digitaler Zwilling aus mehreren anderen digitalen Zwillingen bestehen. Jeder Digitaler Zwilling kann mit einer eigenen Identität ausgestattet werden[8].

[3] Digitale Zertifikate: Die sichere Identität einwandfrei nachweisen
[4] „Jedes vernetzte Geräte benötigt eine sichere Identität“
[5] Maschinenzertifikate – Sichere M2M-Kommunikation
[6] Code Signing Credentials Are Machine Identities and Need to Be Protected
[7] Attackers Are Signing Malware With Valid Certificates
[8] How do you create a digital twin?

Methodisches Vorgehen

Die vorliegende Studie erhebt keinen Anspruch auf Vollständigkeit. Als Informationsgrundlage dient u.a. die auf dem Blog Identity Economy, wie in den Wochenrückblicken, dokumentierten Meldungen sowie die dort veröffentlichen Analysen. Weitere Quellen sind persönliche Gespräche wie auch Interviews der letzten Jahre mit den diversen Akteuren in der deutschen Identity-Szene. Abgerundet wird das Bild durch die Beschäftigung mit den diversen Studien und Veröffentlichungen auf dem Gebiet Cybersecurity/Identity.

Wenngleich die Studie keine Vollständigkeit anstrebt und auch nicht anstreben kann, so besteht das Ziel dennoch darin, ein möglichst vollständiges und kohärentes Bild zu zeichnen. Die Methodik folgt einerseits den Prinzipien der evidenzbasierten Wissenschaft, d.h. die Hypothesen werden anhand der Anzahl stützender Belege geprüft, um daraus vorläufige Schlussfolgerungen ableiten zu können. Auf der anderen Seite werden Analogien dazu verwendet, Ähnlichkeiten mit anderen Bereich, die nicht sofort auf der Hand liegen, herauszustreichen, um im Anschluss daran zu prüfen, inwieweit sich die Erkenntnisse/Muster der einen Domäne auf die andere übertragen lassen.

Marktübersicht

Die Aussichten auf dem Markt für Identity of Things – Lösungen für die nächsten Jahre sind rosig. Laut dem Marktforschungsunternehmen ABIresearch erreicht der Markt für IoT Identity und Management – Lösungen bis 2022 ein Volumen von 21,5 Mrd. US-Dollar[9]. Davon profitieren die Anbieter von Identity of Things – Plattformen ebenso wie IoT-Startups, Certificate Authorities (CA) und Procurement-Plattformen. Nimmt man den Markt für IoT Security als weiteren Referenzpunkt hinzu, dann steht hier bis 2023 ein Volumen von 35,2 Mrd. US-Dollar im Raum[10]. Soviel ist sicher: Der Markt für Identity of Things und IoT-Security – Lösungen ist in den nächsten Jahren von hohen Wachstumsraten geprägt, wie sie nur wenige andere Segmente in dem Zeitraum erreichen werden.

Eine aktuelle Studie von Data Bridge schätzt die jährliche Wachstumsrate (CAGR) für den europäischen Markt für Blockchain Identity – Lösungen für die Jahre von 2019 – 2026 auf 51,7 Prozent[11].

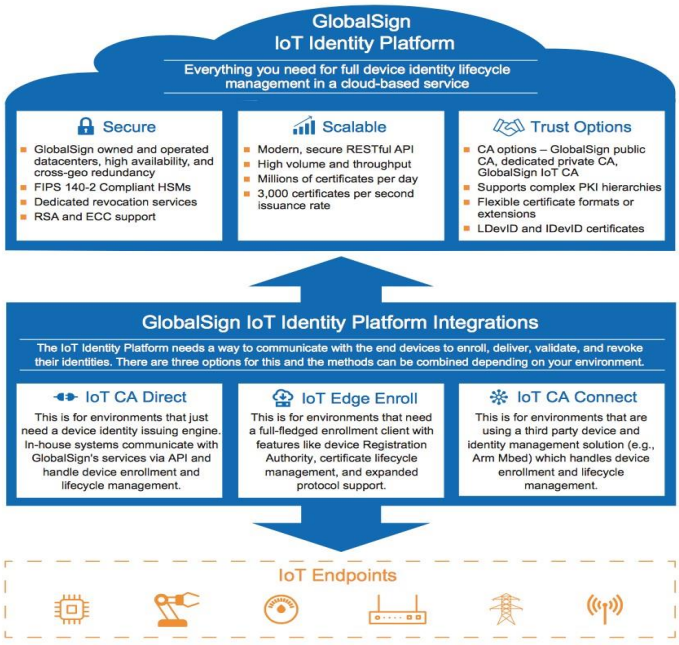
[9] Identity and Management of Things in the IoT a US$ 21,5 Billion Opportunity
[10] IoT Security Market worth $35,2 billion by 2023
[11] Europe Blockchain Identity Management Market 2019: Growth, Emerging Trend And Forecast to 2026

Identity of Things – Plattformen

Integrierte Lösungen für das Management der Identitäten im Internet der Dinge haben in den letzten Jahren in den Unternehmen wie überhaupt in der Industrie an Aufmerksamkeit gewonnen. Nachfolgend eine kurze Vorstellung der wichtigsten Anbieter.

GlobalSign

GobalSign verfügt mit seiner IoT Identity Platform über eine Lösung, an deren Leistungsumfang nur wenige Mitbewerber heranreichen. Kernelement ist die PKI-Infrastruktur. Die Plattform ist branchenübergreifend ausgelegt. Mit ihr kann der komplette Lebenszyklus einer Maschinenidentität verwaltet werden (siehe Abbildung).



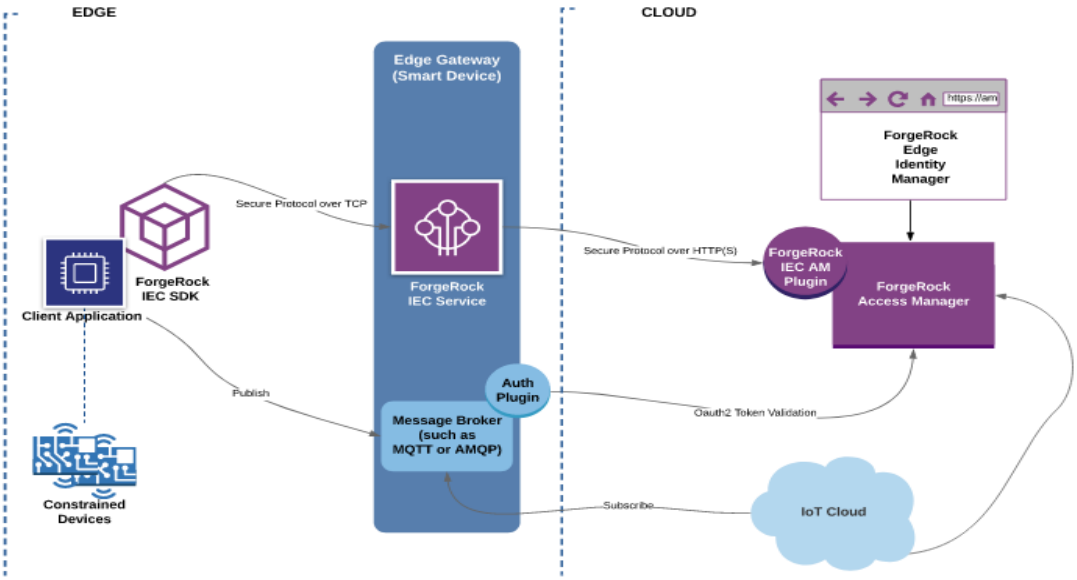
GlobalSign IoT Identity Platform

ForgeRock IoT Edge Controller

Der ForgeRock IoT Edge Controller ist eine komplette End-to-End-Sicherheitslösung für IoT-Implementierungen. Er läuft auf Smart-Edge-Geräten und bietet die Privatsphäre, Integrität und Sicherheit[12]. Er ist , die Geräte benötigen, um sich als Identitäten in der ForgeRock Identity Platform zu registrieren. Mit dem Open-Source-Edge-Controller können die Unternehmen,

[12] IoT Identity Management: Build Better Connected Products and Services Into Your Ecosystem

ihren Produkten digitale Identitäten geben und die Markteinführung neuer IoT-Lösungen deutlich beschleunigen[13].



Komponenten des Identity Edge Controller

OpenText

Ein weiterer Anbieter ist der kanadische Hersteller von Enterprise Information Management – Systemen OpenText. Mit der Übernahme von Covisint[14], der zu dem Zeitpunkt führenden Cloud-Plattform für die Anwendungsentwicklung in den Bereichen Identity, Automotive und Internet of Things, ist OpenText ein wichtiger Anbieter im Identity of Things Segment.

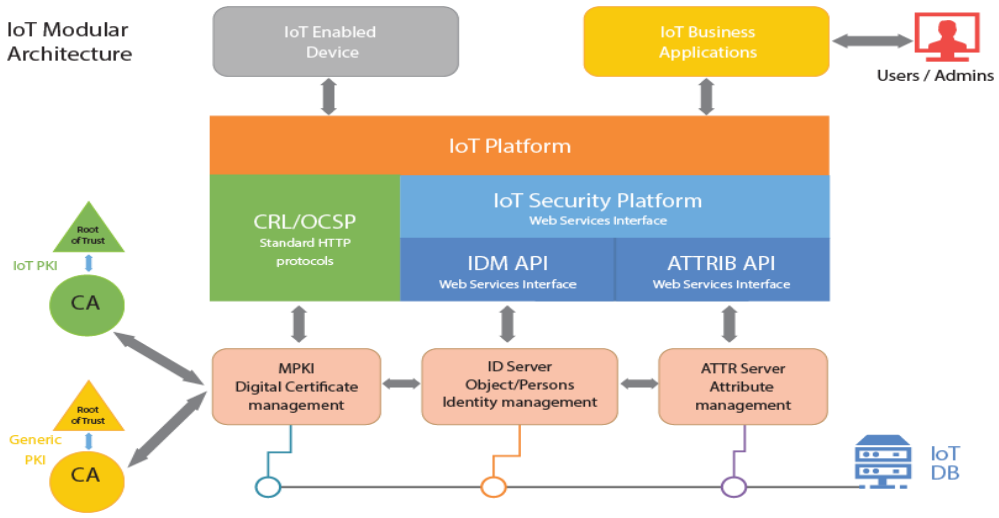
OpenText bietet als White Label Supply Chain – Portale an[15]. Viele namhafte Automobilhersteller wie Daimler zählen zu den Kunden. Zusammen mit den Lösungen zum IAM[16] und der IoT Security[17] verfügt das Unternehmen über eine hohe Bandbreite an Lösungen, die sich branchenübergreifend einsetzen lassen. Erst vor wenigen Wochen gab OpenText die Zusammenarbeit mit Mastercard und Microsoft im B2B-Banking bekannt[18]. Es zeichnet sich ab, dass die Bereiche Procurement, IoT, Identity und Banking näher zusammenrücken.

[13] ForgeRock liefert IoT Edge Controller-Lösung zur Sicherung von Geräteidentitäten
[14] OpenText übernimmt Covisint
[15] Supplier portal solution
[16] Identity and access management
[17] Secure IoT devices
[18] B2B Banking mit Mastercard, Microsoft und OpenText

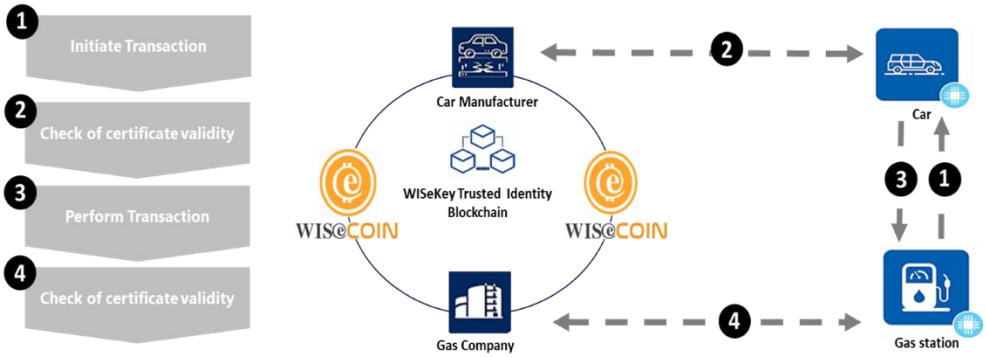
Parallel dazu steigt der Stellenwert der Operational Technology gegenüber der Information Technology[19].

WISeKey

Das Schweizer Unternehmen WiseKey verfolgt mit *Root for IoT* einen eigenen Ansatz. Dazu hat WISeKey die CertifyID IoT Platform[20] entwickelt.



Die Plattform bietet Zertifikate- und Identity-Management aus einer Hand. Zudem kann damit der komplette Lebenszyklus der Objekte, IDs und Daten verwaltet werden.
Eine weitere Lösung von WISeKey in dem Umfeld ist WISeCoin und die [WISeKey Trusted Blockchain Of Identities](#)[21]. Bei WISeCoin handelt es sich um einen tokenized service für die Authentifzierung von Menschen, Produkten und Maschinen gegen unberechtigte Zugriffe Dritter.



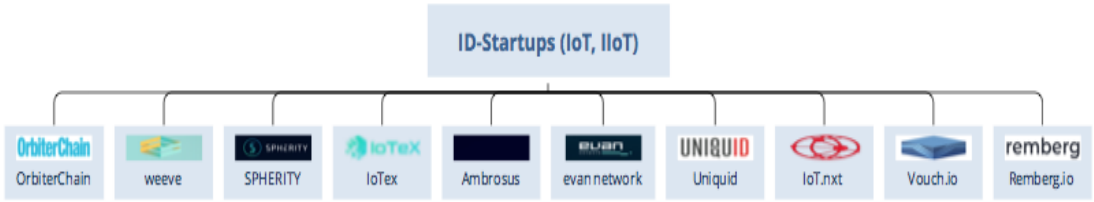
[19] Operational Technology wird die neue IT
[20] CertifyID IoT Platform
[21] The Trusted Blockchain

WISeKey versteht sich als Komplettanbieter von ID-Lösungen auf BlockchainBasis, sowohl für Geräte und Maschinen wie auch für natürliche Personen. Für Außenstehende geht ob der vergleichsweise hohen Anzahl von Lösungen schnell die Übersicht verloren. Es erschließt sich jedenfalls nicht auf den ersten Blick, worin sich die Lösungen im Bereich IoT-Identity unterscheiden und wo sie sich überlappen bzw. ergänzen.

ID-Startups (IoT und IIoT)

Das Internet der Dinge hat mit diversen Sicherheitslücken zu kämpfen. Es macht sich zunehmend bemerkbar, dass das Internet der Dinge entwickelt und ausgebaut wurde, ohne dabei dem Thema Sicherheit allzu große Bedeutung beizumessen. Diese Lücken zu schließen haben sich zahlreiche IoT-Startups zur Aufgabe gemacht. Digitale Identitäten für Maschinen haben dabei eine Schlüsselstellung. Die meisten von ihnen setzen dabei die BlockchainTechnologie ein.

Grafische Übersicht



OrbiterChain

Bei der OrbiterChain handelt es sich um eine HochgeschwindigkeitsBlockchain, die den sicheren Zugriff auf Objekte im IoT regelt. Ein erster Prototyp #theendofcarkey [22] wurde zusammen mit Infineon entwickelt. Sichere Aufsperrsysteme für Autos lassen sich durch eine Kombination aus einem digitalen Schlüssel, der mit dem Smartphone verwaltet werden kann, und der fälschungssicheren Protokollierung der einzelnen Zugriffe darauf in der Blockchain realisieren. Ein unerlaubter Zugriff auf das Öffnungs- und Startsystem des Autos ist damit ausgeschlossen. Sowohl dem Schlüssel wie auch dem Auto wird dabei eine sichere digitale Identität zugewiesen, die wiederum in der orbiterchain verwaltet werden. Vor jedem Zugriff werden die beiden Identitäten und die ihnen zugewiesenen Rechte in der Blockchain überprüft. Alle Interaktionen zwischen diesen digitalen Identitäten werden in der orbiterchain fälschungssicher abgelegt.

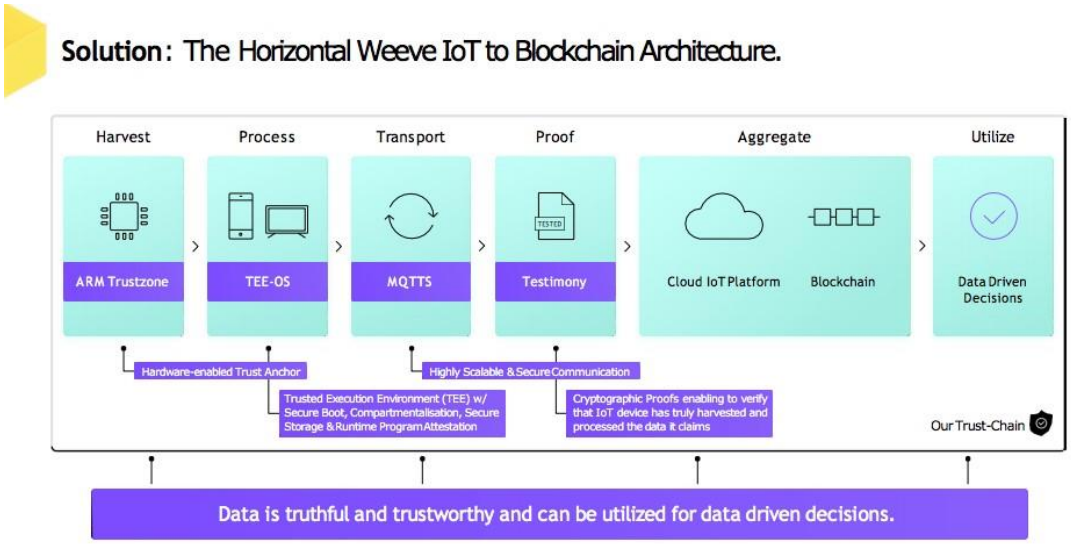
In der Referenzarchitektur der International Data Space Association (IDSA) übernimmt die OrbiterChain die Rolle des Indentity-Providers, der als Bindeglied zwischen der Blockchain und dem IDS-Connector[23] fungiert.

[22] Blockchain statt Autoschlüssel: Neue Technik löst Sicherheitsproblem
[23] Blockchain Technology in IDS

Die OrbiterChain ist ein Produkt von orbiter.de. Orbiter.de wiederum wurde von Hannes Bauer, dem Entwickler der ersten deutschen Suchmaschine, Kolibri[24], vor 25 Jahren gegründet.

Weeve-network

Das weeve-network verbindet das Internet der Dinge und die Blockchain mit dem Ziel, die Vertrauenswürdigkeit der IoT-Daten sicherzustellen. Dadurch werden die IoT-Daten handelbar. Kernstück des weeve-networks ist das eigene Betriebssystem, weeveOS[25]. WeeveOS verwendet neue Technologien, wie die ARM Trustzone extension, um auf diese Weise eine Trusted Execution Environment für die sicherheitskritischen Komponenten zu schaffen. Hacker haben keine Möglichkeit, auf die Trusted Execution Environment zuzugreifen und die IoT-Daten zu manipulieren. Die TEE schirmt die Geräte-Identitäten vor unerlaubten Zugriffen ab[26]. Vor wenigen Wochen wurde ein PoC mit Festo erfolgreich abgeschlossen[27].

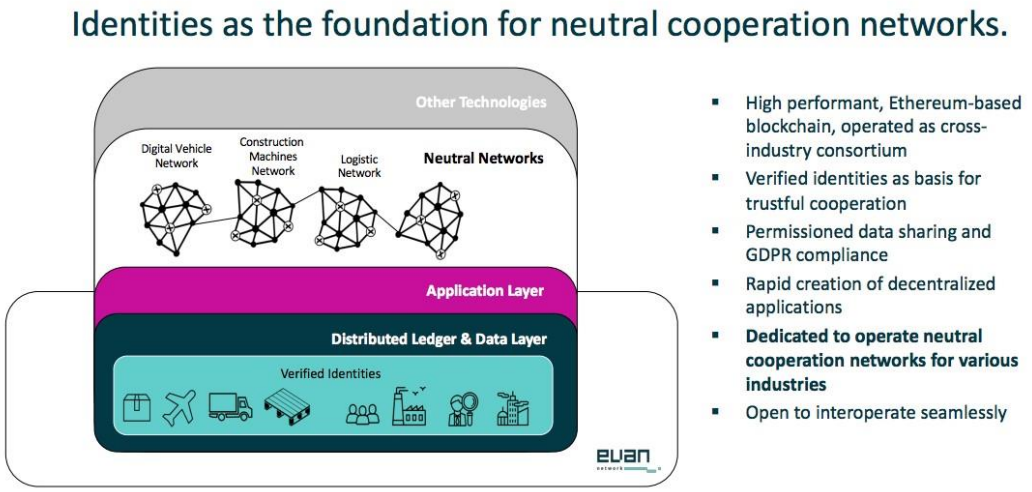


Im Bereich Identifizierung arbeitet weeve überdies eng mit Spherity zusammen[28]. Spherity steuert seine Identifizierungslösung für Digitale Zwillinge (Verifiable Digital Twin) bei.
Weeve hat nicht die Absicht, eine dominante Plattform wie Amazon zu werden, sondern versteht sein Geschäftsmodell als Plattform-as-a-Service. Ziel ist es, den Kunden dabei zu helfen, ihre eigenen Datenmarktplätze aufzubauen.

[24] Suchmaschine mit vielen Extras
[25] Introducing weeveOS – The first Operating System designed for Blockchain-enabled Internet of Things
[26] Empowering the Economy of Things
[27] Weeve and Festo complete a successful POC in the Industry 4.0 Domain
[28] Weeve partners with Spherity to bring digital twins of physical assets onto the digital blockchain-based Weeve ecosystem

evan.network

Das evan.network ist eine Business Blockchain, welche die Digitalisierung und Automatisierung von Geschäftsvorgängen auf Basis von digitalen Zwillingen ermöglicht. Betreiber der Blockchain ist die evan.network organization. Das evan.network ist laut eigener Aussage das erste unternehmensübergreifende öffentliche Blockchain-Netzwerk. Daneben bezeichnet sich das evan.network auch als „social network" of things. Um die Vertrauenswürdigkeit der Geschäftspartner und Transaktionen zu sichern, setzt das evan.network verfizierte Digitale Identitäten für Menschen, Geräte und Organisationen ein.



Unternehmen, die am evan.network teilnehmen, können durch einen Notar die Echtheit ihres Accounts bestätigen lassen. Der Notar erstellt eine entsprechende Urkunde, die eine Verknüpfung zwischen einer digitalen Identität im evan.network und einem in der realen Welt existierenden Unternehmen bestätigt. Diese Urkunde ist bei Bedarf von anderen Netzwerk-Mitgliedern einsehbar und schafft im evan.network ein Grundvertrauen. Außerdem können darauf aufbauend verlässliche Sub-Verifikationen von zugehörigen Maschinen, Produkten oder Mitarbeitern ausgestellt werden[29].

Kernelement des evan.network ist der Digitale Zwilling. Für jedes Produkt werden im evan.network verifizierte digitale Zwillinge erstellt. Jeder digitale Zwilling erhält eine eindeutige digitale Identität, mit der er sich gegenüber anderen digitalen Zwillingen ausweisen kann. Außerdem sorgt der Digitale Zwilling für die Dokumentation der Transaktionshistorie. Digitale Zwillinge können für verschiedene Anwendungsszenarien verwendet werden, wie für Vermietung, Sharing und Finanzierung (Digital Twin Financing). Im Bereich der

[29] evan.network – das erste unternehmensübergreifende öffentliche Blockchain-Netzwerk: Interview mit Thomas Müller

digitalen Identitäten für Personen arbeitet das evan.network mit BlockchainHelix zusammen. Weitere Kooperationen bestehen mit slock.it (Kommunikation mit IoT Devices) und Streamr (IoT-Datastreaming).

Spherity

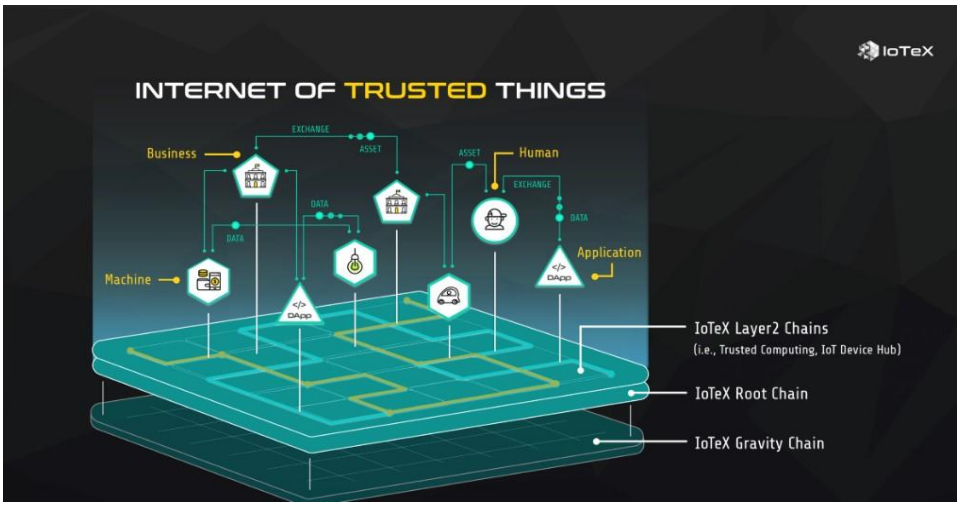
Spherity arbeitet an Lösungen für das dezentrale Identitätsmanagement, um damit die Grundlage für die 4. Industrielle Revolution zu schaffen. Hierfür setzt Spherity auf Sichere Digitale Identitäten und Digitale Zwillinge, sowohl für Maschinen, Algorithmen und andere technische Objekte (s Abbildung).

Wie bereits erwähnt, kooperiert Spherity mit weeve. Daneben ist Spherity im Bereich Mobility aktiv[30].

[30] Good bye monolithic platforms, welcome tot he future of dynamically defined mobility

IoTeX

Die Vision von IoTtex ist die Verwirklichung eines globalen Internet of Trusted Things. Zentraler Baustein ist Mainnet Alpha, bestehend aus der Root Chain, den Layer2 Chains und der Gravity Chain (s. Abbildung).IoTeX ist zu 100% Open Source.



IoTeX agiert als dezentrale Vertrauensstruktur für alle physischen und virtuellen Dinge und erhöht so das Vertrauen über den gesamten Lebenszyklus von Daten hinweg, einschließlich Erfassung, Transport, Speicherung und Nutzung. Das führt dazu, dass Daten und Assets von allen “Dingen” gemeinsam genutzt werden können, so dass aus dieser Verbindung von Menschen, Maschinen, Unternehmen und Anwendungen vollkommen neue dezentrale

Geschäftsmodelle möglich werden[31]. Der große Vorteil von IoTeX im Vergleich zu IOTA besteht laut IoTeX-Ambassador Simone Romano[32] in der Architektur, welche auf anpassbaren Subnetzwerken und einem schnellen, skalierbaren Konsensusmechanismus basiert [33]. Damit ist es möglich, nicht nur eine zuverlässige, netzwerkbasierte und gut getestete Blockchain bereitzustellen, sondern auch direkt Funktionen wie Smart-Contract, SPV und Privatsphäre zu integrieren, die in den meisten IoT-Szenarien notwendig sind. Anders als IOTA adressiert IoTeX das Thema Digitale Identitäten nur indirekt – über Privacy. Wie aus einer Diskussion auf Reddit hervorgeht, plant IoTeX auf dem Gebiet der digitalen Identifizierung Kooperationen[32].

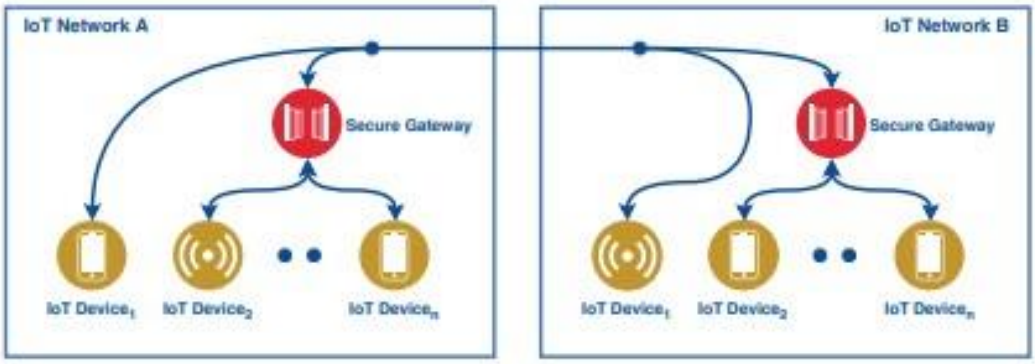
Partnerschaften bestehen mit Lineable (Tracking von Gesundheitsdaten, um so verschiedene Krankheiten vorab zu diagnostizieren) und SmartHab

[31] Alles, was man zum Mainnet Alpha wissen muss
[32] IoTeX – Interview mit IoTeX-Ambassador Simone Romano
[33] Everything You Need To know About The IoTeX Blockchain
[32] r/IoTeX

(dezentrales Register, das kritische Daten aus smarten Gebäuden und smarten Städten mit dem Ziel speichert, eine überprüfbare und zertifizierte Datenquelle zu schaffen). Neuer strategischer Investor ist HashKey Capital[34].

UniquID

UniquID bezeichnet sich als Identity Service für das dezentrale Internet of Things. Die Absicht ist, die traditionellen Identity Access Management Systeme durch flexiblere und leichter zu verwaltende zu ersetzen. Das geschieht dadurch, dass die Geräte sich direkt untereinander, ohne Zwischenschaltung einer dritten Partei, authentifizieren[35].



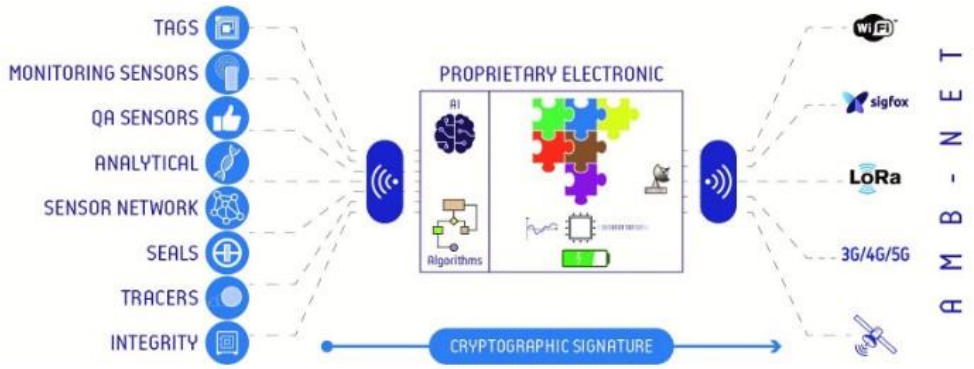
UniquID setzt auf dezentrale Digitale Identitäten für das IoT (Decentralized Public Key Infrastructure). UniquID stellt Werkzeuge zur Verfügung, um offen zugängliche Register von IoT-Maschinen und Services zu erstellen und zu verbreiten[36]. Technisch gesehen handelt es sich dabei um ein Werkzeug, das wie geschaffen ist für Edge Computing und Verteilte Geräte-Netzwerke, ähnlich den Infrastructure as a Code – Prinzipien. Sobald eine neue Zugangsregel in der Blockchain hinterlegt wird , wird sie automatisch an alle Systeme, die mit der Blockchain verbunden sind, weitergeleitet[37]. UniquID stellt einen digitalen Ausweis für IoT-Daten bereit. Damit können die Geräte über die verschiedenen Standards und Systeme hinweg Daten austauschen, ohne dabei auf individuelle Systemanpassungen angewiesen zu sein.

Ambrosus

Bei Ambrosus handelt es sich um ein Blockchain-basiertes IoT-Neztwerk für die Lebensmittel- und Pharmabranche. Es ermöglicht die sichere und reibungslose Kommunikation zwischen Sensoren, verteilten Ledgern und Datenbanken, um dadurch die Transparenz von Versorgungsketten herzustellen und die Qualität zu sichern. Erklärtes Ziel von Ambrosius ist es, einen globalen Standard für dezentralisiertes Versorgungskettenmanagement zu setzen. Die

[34] IoTeX erhält strategische Investition von HashKey Capital
[35] UniquID: A Quest of Reconcile Identity Access Management and the Internet of Things
[36] The Quest of IoT Architects to Build Digital Identity Infrastructure for Machines
[37] Blockchain in Cybersecurity Use Case #5: UniquID

Kundenprodukte werden mit einer sicheren digitalen Identität ausgestattet. Herzstück von Ambrosus ist AMB-NET – ein dezentralisiertes Protokoll, das Daten über Lebensmittel, Pharmaka, die mittels Sensoren gesammelt werden, verfolgt, speichert und überträgt.



Kooperationen bestehen u.a. mit INATBA (International Association for Trusted Blockchain Applications)[38].

IoT.nxt

Das südafrikanische Startup IoT.nxt möchte den Unternehmen den Überblick aller Geräte und technischen Objekte verschaffen, um auf diese Weise tiefergehende und aussagekräftige Datenanalyen zu ermöglichen. Ein wichtiges Element ist dabei die Digitale Identität der Geräte und Maschinen. Dafür bietet IoT.nxt den Secure Device DNA Identity Service und den SIEM Connector an[39]. Vor einigen Wochen übernahm Vodacom, eine Tochter von Vodaphone, 51% von IoT.nxt. Der Gründer von IoT.nxt, Nico Steyn, sagte in einem Interview, dass er keine Nachteile durch die Übernahme, z.B. durch nachlassende Agilität, befürchte[38]. Stattdessen betont er die zusätzlichen Möglichkeiten, die Vodacom IoT.nxt im Geschäft mit Unternehmenskunden verschaffen könne. Nachdem IoT.nxt in den USA vertreten ist, strebt man nun auf den europäischen Markt.

[38] Ambrosus: Masternodes onboarding process, shaping of the EU blockchain initiatives via INTABA, ecosystem expansion and open-source code adoption
[39] IoT.nxt offers Secure Device DNA Identity Service & SIEM Connector
[38] Interview: IoT.nxt CEO Nico Steyn

Vouch.io

Vouch.io aus Atlanta verfolgt mit seiner Vouch Identity Trust Platform einen dezentralen, Blockchain-basierten Ansatz, um die Schwächen der herkömmlichen zentralisierten Lösungen für IDoT, wie CAs, zu umgehen[40]. Dabei wird die Identität der Maschine, des Geräts, des Prozesses oder der Person gegen eine chain of custody data geprüft [41] . Vouch.io greift auf die Firmware/Software zu. Die Audit-Daten werden mit dem Hersteller ausgetauscht.

Es besteht eine Kooperation mit ForgeRock[42].

Remberg

Das Münchener Startup Remberg.io will mit seinem cloud-basierten Asset-Relationship-System (ARM) das unternehmensübergreifende Management von Maschinen ermöglichen. Hersteller wie auch Dienstleister und Betreiber sind damit in der Lage, maschinenbezogene Informationen (Dokumentationen, Ersatzteile oder Servicefälle) auf einer Oberfläche zu managen. Maschinenidentitäten spielen dabei eine wichtige Rolle.

Durch diese Form der kollaborativen Zusammenarbeit haben Maschinenhersteller und Betreiber die Möglichkeit, Kundenbedarf frühzeitig zu erkennen und entsprechende Lösungen anzubieten[43].

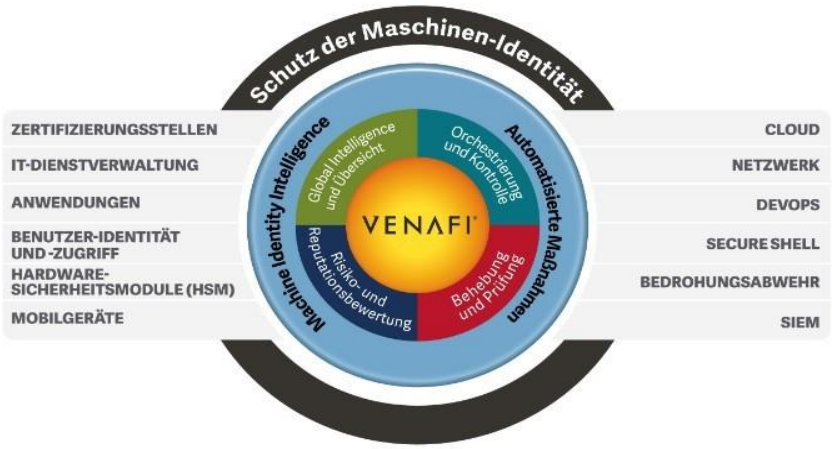
[40] IoT Identity Management
[41] IoT Device Authentication and Security
[42] ForgeRock Partners - Vouch
[43] 26 Tech-Start-ups mit Lösungen für Industrie

Identity Security

Die Sicherheit der Maschinenidentitäten zu gewährleisten, gehört zu den wichtigsten Aufgaben im Internet der Dinge und im Industriellen Internet der Dinge. Um die Übersicht der im Unternehmen verwendeten Digitalen Identitäten für Maschinen und Geräte zu behalten, bieten einige Unternehmen spezielle Lösungen für die Inventarisierung und Verwaltung der Maschinenzertifikate an. Nicht rechtzeitig erneuerte Zertifikate können in den Unternehmen zu hohen Ausfallszeiten führen. Ein weiteres Problem sind gefälschte Zertifikate.

Venafi

Venafi bietet eine Plattform für den Schutz der Maschinen-Identitäten in der gesamten erweiterten Infrastruktur[44]. Möglich wir das durch den Einsatz globaler Übersichten, detaillierter Informationen sowie Automatisierung aller Aspekte der Maschinen-Identitäten. Auf diese Weise können Schwachstellen in Schlüsseln und Zertifikaten schnell identifiziert und automatisch behoben werden. In dem Zusammenhang spricht Venafi auch von Machine Identity Intelligence[45]. Unter Machine Identity Intelligence versteht Venafi die Fähigkeit, Maßnahmen und Workflows zur Kontrolle der Schlüssel und Zertifikate automatisiert zur Verfügung zu stellen. Durch die Orchestrierung kann der gesamte Lebenszyklus der Maschinen-Identitäten automatisiert werden, was wiederum dazu führt, automatisch auf die sich ständig ändernde Bedrohungslage reagieren zu können. Die von Venafi beauftragte Studie von Forrester Securing The Enterprise With Machine Identity Protection kam u.a. zu dem Ergebnis, dass 80 Prozent der Unternehmen die nötigen Fähigkeiten und Werkzeuge zum Schutz der Maschinen-Identitäten fehlen.



[44] Die Venafi - Plattform
[45] Making a Business Case for Machine Identity Intelligence

Erst kürzlich hat Venafi Kooperationen mit nCipher [46], GlobalSign [47] und DigiCert [48] im Bereich Identity Protection bekannt gegeben. Als erstes und bislang einziges Unternehmen bietet Venafi eine Ausfallgarantie für zertifizierungsbedingte Ausfälle[49]. Im vergangenen Jahr konnte Venafi in einer Finanzierungsrunde 100 Millionen Dollar einsammeln[50]. Ein Teil des Geldes soll in einen Fonds fließen, der Dritte (Entwickler, Systemintegratoren, Beratungsgesellschaften, Startups) bei der Entwicklung ergänzender Produkte und Services unterstützt, um damit ein Maschinenidentität – Ökosystem aufzubauen.

Nexus

Ein ähnliches Spektrum an Lösungen wie Venafi bietet Nexus an. Ein Produkt ist die skalierbare Certificate Authority Software Smart ID IoT.

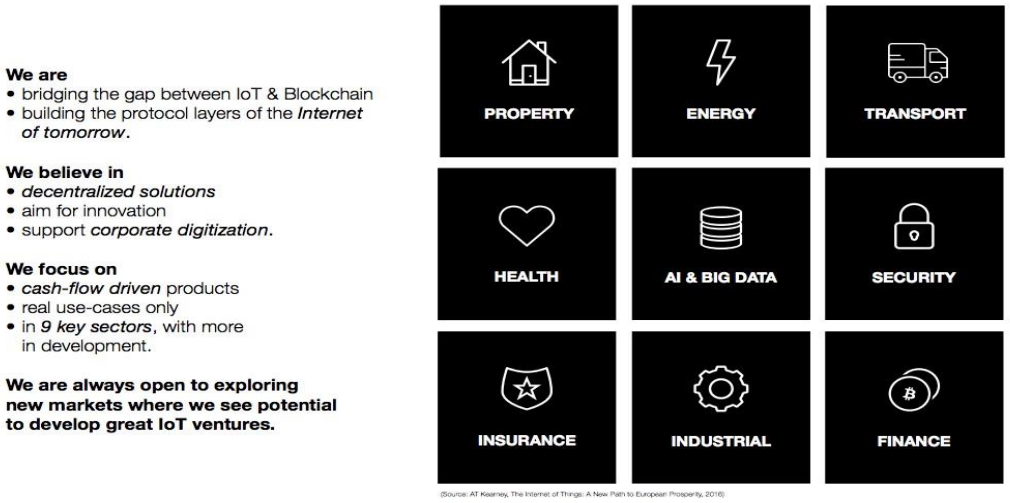
[46] Venafi and nCipher Security partner on machine identity protection
[47] Venafi and GlobalSign Partner to Expand Machine Identity Protection in DevOps Environments
[48] Venafi and DigiCert Machine Identity Protection Partnership Delivers New Solution for LargeScale Entperprise PKI
[49] Venafi mit erster Ausfallgarantie der Branche
[50] Venafi sichert sich ein Investment über 100 Millionen Dollar von TCV

Investoren / Inkubatoren

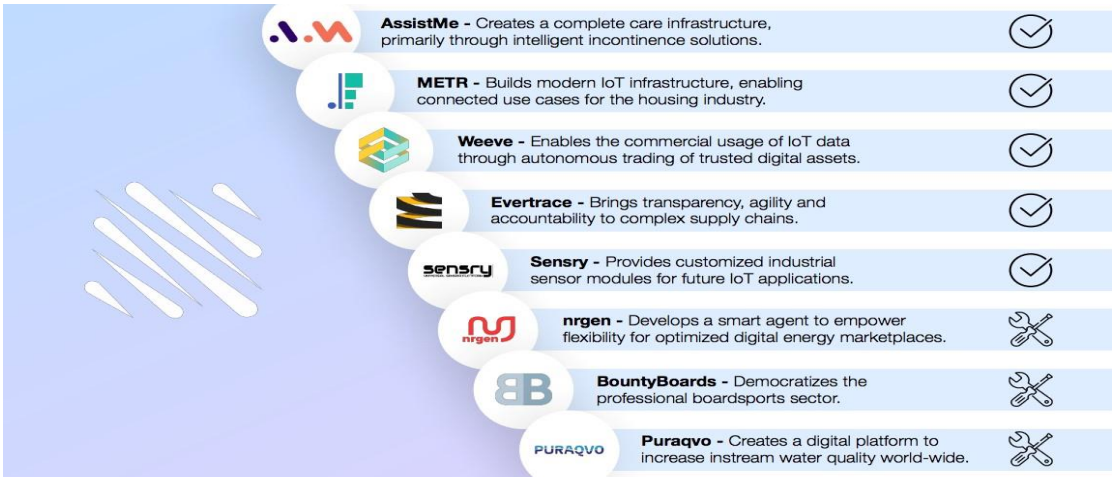
Investoren, die sich dezidiert mit Maschinen-Identitäten bzw. der Integrität der im IoT ausgetauschten Daten beschäftigen, gibt es nur sehr wenige. Im Anschluss sollen zwei davon vorgestellt werden.

Next Big Thing AG

Die Next Big Thing AG ist ein Inkubator, Operational VC und Company Builder auf den Gebieten IoT/IoS und Blockchain. Sich selbst bezeichnet NBT auch als das Rocket Internet of IoT.
Die Unternehmens- und Investmentphilosophie von NBT veranschaulicht die folgende Grafik.



Das folgende Schaubild gibt einen Überblick der Startups, die von NBT gefördert werden, darunter das bereits vorgestellte weeve-Netzwerk.



Die industrielle Expertise von NBT besteht aus der Kombination Retrofitting, DeepTech und neue Sensorik. Auf der Business-Seite konzentriert man sich auf datengetriebene Geschäftsmodelle. Einen weiteren Schwerpunkt bilden hardware-enabled business models bzw. Hardware-as-a-Service.
Kooperationen bestehen u.a. mit dem IoT Hub Berlin, der Frankfurt School of Finance, dem Cyberforum Karlsruhe und Fraunhofer Dresden. Bei letzterer handelt es sich um ein Joint Venture zur Entwicklung eines universellen IoT – Sensors (System auf einem Chip). Vor wenigen Monaten beteiligte sich die HDI Versicherung an NBT[51].

Riddle&Code

Riddle&Co bezeichnet sich als Blockchain Interface Company. Ähnlich wie NBT verbindet Riddle&Code Hardware und Software, um die Welt der Dinge, als Teil industrieller Wertschöpfungsketten, mit den Blockchains als digitale Plattformen zu verbinden[52]. Ziel ist es, Maschinen, Fahrzeuge oder Sensoren zu absolut vertrauenswürdigen Datenquellen zu machen. Hierfür werden eigens designte Crypto-Chips, die mittels der Software von Riddle&Code an beliebige Blockchains angebunden werden können und obendrein noch volle Wallet-Fähigkeit besitzen, eingesetzt. Auf diese Weise werden digitale und fälschungssichere Identitäten für Maschinen und andere physikalische Objekte kreiert, sodass man dann mit deren digitalem Zwilling oder der entsprechenden Maschinen-Wallet sichere Prozesse konstruieren kann. Ein Produkt ist das Universal Purpose Identity Gateway.

Gemeinsam mit dem bereits vorgestellten evan.network, dem Startup Blockchain Helix und Daimler hat Riddle&Code vor kurzem eine offene Mobility Blockchain Plattform präsentiert[53]

[51] HDI setzt Digitalisierungsstrategie durch Kooperation mit Next Big Thing fort
[52] Digitale und fälschungssichere Identitäten für Maschinen und andere physikalische Objekte durch eigens designte Crypto-Chips – Interview mit Sebastian Becker (Riddle&Code)
[53] Blockchain Use Cases: Daimler initiiert offene Mobility Plattform

Standards, Initiativen, Protokolle und Vereinigungen

Zahlreiche Standards, Protokolle und Initiativen beschäftigen sich im engeren und weiteren Sinne mit der Digitalen Identifizierung von Maschinen und Geräten. Bislang fehlt jedoch ein gültiger Standard für das IoT/IIoT und für Identity of Things[54]. Das bringt die Gefahr mit sich, dass große digitale Plattformen und Ökosysteme einen Quasi-Standard schaffen und damit einen Lock-In-Effekt erzeugen. Dem Ideal am nächsten kommt derzeit OPC-UA mit der TNS-Erweiterung. Eine ähnliche Bedeutung könnte im Bereich Werkzeugmaschinen Umati[55] erlangen, das auf OPC-UA aufsetzt.

Initiativen, Standards mit direktem Bezug zu Maschinenidentitäten

AIM (Advanced Identification Matters)	Industrieverband
AIOTI WG03 Reports – Identifiers in Internet of Things (IoT)	AIOTI – Alliance for Internet of Things Innovation
AutoID	Automatische Identifikation und Datenerfassung
Device Identifier Composition Engine (DICE).	Family of hardware and software techniques for hardware-based cryptographic device identity, attestation, and data encryption.
IDSA/IDS-Connector	Softwareplattform für vertrauenswürdige, sichere IIoT-Gateways
MOBI	Vehicle Identity Standard – Mobility Open Blockchain Initiative
Trusted IoT Alliance	Securing IoT With Blockchain (Open Source Software Foundation)

Bei Kantara gibt bzw. gab es eine Gruppe, die sich mit Identity of Things beschäftigt(e). Bei W3C spricht man generell von Decentralized Identifiers.

In Identity of Things (IDoT) stellt TechVision Research seine IDoTReferenzarchitektur vor.

Einen Überblick der IoT-Standards gibt der Beitrag IoT-Standards – eine Übersicht der wesentlichen Akteure. Über die Blockchain-relevanten Standards gibt IEEE SA - Internet of Things Related Standards Auskunft.

[54] Auf der Suche nach einem IoT-Standard
[55] Umati: Die universelle Schnittstelle für Werkzeugmaschinen

Ob und wann sich ein Standard für das IoT und das IDoT durchsetzt, steht derzeit noch in den Sternen. Es ist nicht auszuschließen, dass die verschiedenen Initiativen und Standards sich gegenseitig behindern.

Wissenschaftliche Projekte und Initiativen

Regierung, Wissenschaft und Wirtschaft haben in den letzten Jahren die Relevanz sicherer Maschinenidentitäten für das IoT und IIoT erkannt und entsprechende Projekte und Initiativen auf den Weg gebracht.

IUNO / IUNO InSec

Im Rahmen der Plattform Industrie 4.0 (PI4.0) ist die Sichere Identifizierung von Maschinen einer von vier als wichtig eingestuften Aspekte[56]. In dem Nationalen Referenzprojekt zur IT-Sicherheit in Industrie 4.0 – IUNO wurden die Einsatzmöglichkeiten Sicherer Digitaler Identitäten in Cyber-Physischen Produktionssystemen (CPPS) näher untersucht. Die Projektergebnisse wurden im September 2018 veröffentlicht[57]

In dem Folgeprojekt IUNO InSec geht es nun darum, die Möglichkeiten auszuloten, inwieweit sich sichere digitale Identitäten für Digitale Zwillinge mittels Distributed Ledger Technologies, in diesem Fall IOTA, erzeugen und verwalten lassen.

Problemstellung:

Im Vordergrund steht der Umgang mit Schlüsselmaterial, auf dessen Basis sich Maschinen und Geräte eine Identität erstellen lassen und im Nachgang authentisieren. Um die Anwendbarkeit in Produktionsstätten nachweisen zu können, haben zudem IT-Schutzziele bzw. eine sichere Kommunikation oberste Priorität.

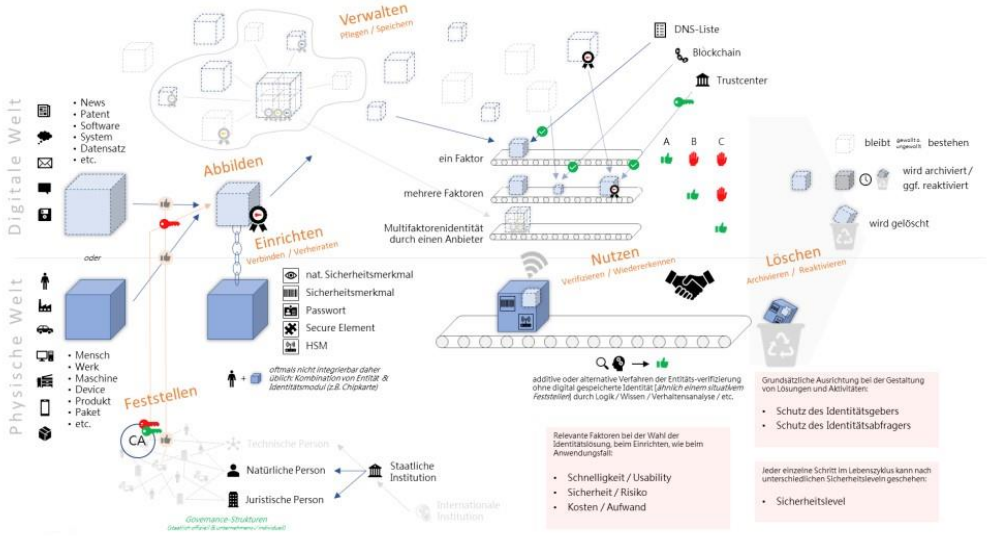
Im Industriellen Internet der Dinge könnte die deutsche Industrie mit weltweiten Registern für Maschinen oder Service-Schnittstellen [58] punkten. Sichere Digitale Identitäten sind hierfür unverzichtbar, sie sind der eigentliche Schlüssel.

DIN/DKE-Projekt „Sichere Digitale Identitäten“ (SDI)

In dem DIN/DKE-Projekt „Sichere Digitale Identitäten“ werden die bestehenden Normen und Standards sowie der Status-Quo zu Entwicklungen, Lösungen und marktüblichen Vorgehen in unterschiedlichen Branchen untersucht. Gefördert wird das Projekt durch das Bundesministerium für Wirtschaft und Energie mit

[56] Challenges of sescurity aspects of global industrial value chains
[57] Forschung für mehr IT-Sicherheit in Industrie 4.0 – Projektergebnisse
[58] Warum deutsche Fertiger „noch viel radikaler denken müssen“

dem Ziel, einen Prozess in die Wege zu leiten (Normungs-Roadmap und politische Maßnahmen), der hinsichtlich digitaler Identitäten das Bewusstsein, den Inhalt und die Rahmenbedingungen zu einer gemeinsamen Basis für eine interoperable, sichere und effiziente Infrastruktur schafft[59]. Im August 2018 legten DIN und DKE ihren Abschlussbericht vor[60]. Darin wird bemängelt, dass es derzeit noch keinen Standard gibt, der einen Rahmen liefert, der die Erfordernisse von Industrie 4.0 abdeckt. Dazu fehlen entsprechende Metastandards und Spezifikationen. Es fehlt ein roter Faden in Form eines internationalen Frameworks. Daraus könnte dann ein Standard entstehen, „der es Unternehmen, von Konzernen bis KMU, im Hinblick auf Industrie 4.0 ermöglicht eine SDI-Struktur aufzubauen, die interoperabel ist und Vertrauen schafft – zunächst vielleicht nur als Selbsterklärung, später ggf. als zertifiziertes Unternehmen. Nur ein solcher Standard vermag die Sicherheit zu schaffen, die zu entscheidenden Investitionen führt und das Zukunftsprojekt Industrie 4.0 real werden lässt“.



Gesamtverhalt SDI mit seinen Handlungsschritten/ebenen

SAMPL – Secure 3D Printing

Das vom Bundesministerium für Wirtschaft und Energie geförderte Projekt SAMPL verfolgt als Ziel die Entwicklung einer durchgängigen Sicherheitslösung für additive Fertigungsverfahren. Dabei wird der komplette Prozess von der Entstehung der digitalen 3D-Druckdaten über den Austausch mit einem 3D-Druckdienstleister und seinen durch spezielle Secure Elements abgesicherten Trusted 3D-Druckern bis zur Kennzeichnung der gedruckten Bauteile mittels RFID-Chip betrachtet. Dafür soll ein digitales

[59] Forum Industrie 4.0 – Talk«1: Sichere Digitale Identitäten
[60] Projektbericht Sichere Digitale Identitäten (SDI)

Lizenzmanagement auf Basis der Blockchain-Technologie in die Datenaustauschlösung OpenDXM GlobalX der PROSTEP AG integriert werden. Als Schnittstelle für den Austausch der Zertifizierungs- und Lizenzdaten zwischen Rechteinhaber und Empfänger fungiert der Industrie 4.0 Standard OPC-UA.

Aktuelle Praxisbeispiele für Maschinenidentitäten

Obwohl, oder vielleicht auch gerade weil, bislang kein einheitlicher Standard für Maschinenidentitäten existiert, haben einige namhafte Unternehmen damit begonnen, auf diesem Gebiet erste Erfahrungen zu sammeln. Beispielhaft dafür sind Daimler und der Weltmarktführer für Autolackieranlagen, Dürr.

Daimler: TruckID

Grundlagen der TruckID in einem von Daimler und der Commerzbank durchgeführten Projekt sind das Truck Data Center sowie ein kryptographischer Prozessor des neuen Mercedes Actros. Damit wird der LKW mit einem Ausweis ausgestattet, der eindeutige Signaturen sowie die zweifelsfreie Identifizierung anderen Maschinen und Komponenten gegenüber übernimmt[61].

Künftig wird der LKW zu einer eigenständigen Geschäftseinheit mit eigener G+V. Dabei verfügt er über eigenes ZAG-konformes E-Geld. Im vorliegenden Fall hat die Commerzbank Euros in der Blockchain hinterlegt (Cash on Ledger) und den LKWs zur Verfügung gestellt. Dabei werden Zero Balance Accounts verwendet.

Nur Trucks, die sich eindeutig ausweisen können, sind berechtigt, M2M-Zahlungen durchzuführen. Auf diese Weise will man z.B. Tankkartenbetrug verhindern.

Auf den Einsatz von Smart Contracts hat man bewusst verzichtet. Vielmehr setzt man auf die Vorteile des klassischen Zug-um-Zug – Geschäfts. Vorstellbar ist die Einführung eines Reputation Layers, der für das nötige Vertrauens- und Sicherheitslevel sorgt[62].

Dürr: mySaveID

Der von Dürr und targens entwickelte Identservice mySaveID erlaubt das sichere Anlegen und Verwalten von vertrauenswürdigen digitalen Identitäten im Business-to-Business-Bereich. Damit können Identitätsdaten an Dritte freigeben, Unterschriftsberechtigungen hinterlegt und die Verträge mit einer rechtsgültigen elektronischen Unterschrift versehen werden. Neben geschäftlichen Transaktionen zwischen Personen kann mySaveID auch für die

[61] Daimler: Pilotprojekte Truck ID und Truck Wallet
[62] Wenn der LKW autonom bezahlt

sichere Maschinenidentität im Umfeld von Internet-of-Things-Anwendungen genutzt werden[63].

AvD: CarPass

Damit Autos sich künftig im Netz gegenüber Dritten (Werkstätten, Maut, Parkhäuser, Versicherungen, Leasing-Gesellschaften, Ladesäulen, Tankstellen, Car Sharing, Mehrwertdienste …) ausweisen können, benötigen sie eine verifizierte Digitale Identität. Wenn es nach dem AvD geht, dann erhält jedes Auto einen Pass, den CarPass[64], der als Digitale Identität fungiert.

Die digitale Identität des PKWs ist an die des Halters geknüpft. Wie die digitale Identität des Halters verifiziert wird, geht aus der aktuellen Meldung nicht hervor. Mit CarPass soll der Nutzer die Hoheit über die Fahrzeugdaten bekommen.

[63] DLT-Pilotprojekt: Identitätsservice mySaveID ermöglicht digitalen Abschluss eines Konsortialkredits
[64] AvD: CarPass als Basis für eine unabhängige Fahrzeugdaten-Plattform

Technische Umgebungen für die Verbreitung von Maschinenidentitäten

Damit Maschinenidentitäten die ihnen zugedachte Rolle übernehmen und ihre Wirkung entfalten können, sind auf unterstützende Systeme und Prozesse in den Unternehmen angewiesen. Eine Schlüsselfunktion übernehmen dabei Digitale Zwillinge, als Abbilder realer Maschinen, technischer Objekte und anderer Gegenstände.

Unterstützende Systeme und Prozesse

Das Internet der Dinge stellt an die bestehenden IT-Systeme in den Unternehmen, wie ERP, CRM und PLM, neue Herausforderungen. Zahlreiche Branchenbeobachter gehen davon aus, dass aufgrund der vielschichtigen Beziehungen und Abhängigkeiten von Personen, Geräte, Prozessen, Maschinen und Unternehmen die herkömmlichen IAM-Systeme nicht mehr ausreichen. Die Zukunft gehöre daher IoT-Identitätsplattformen[65]. Gleiches gilt für die Robotic Process Automation[66].

Generell lässt sich derzeit eine Konvergenz von ERP-, CRM-, MES- und PLMSystemen beobachten[6768]. Parallel dazu verläuft die Verschmelzung von bzw. Annäherung zwischen IT und OT[62].

Digitale Zwillinge – Know Your Object (KYO)

Um Maschinen über die gesamte Lebensdauer verwalten und Veränderungen simulieren zu können, werden Digitale Zwillinge eingesetzt. Dabei handelt es sich um digitale Abbilder realer, physischer Objekte. Der digitale Zwilling enthält die wesentlichen Merkmale einer Maschine, eines Geräts oder eines Prozesses. Sensoren, die an der Maschine angebracht werden, versorgen den digitalen Zwilling mit aktuellen Zustandsinformationen (Auslastung, Temperatur Standort etc.). Auch komplette technische Infrastrukturen und Anlagen lassen sich mit einem Digitalen Zwilling abbilden und steuern[69]. Ein digitaler Zwilling kann wiederum aus weiteren Zwillingen bestehen, die miteinander sowie mit externen Zwillingen kommunizieren und interagieren. Im Produktionsprozess muss daher zu jedem Zeitpunkt sichergestellt werden, dass die Daten, die von den Zwillingen gesendet und verarbeitet werden, valide sind und die Identität des Zwillings

[65] IoT erfordert ein neues Identitätsmanagement
[66] Identity Management in the Age of Robotics
[67] PLM, ERP und MES vernetzen
[68] Industrial connectivity trends driving the IT-OT convergence
[69] Digitaler Zwilling in der Produktentwicklung

zweifelsfrei feststeht[70]. Jeder digitale Zwilling bekommt eine eindeutige und sichere Identität zugewiesen.

Nach Lianne Kemp, CEO von Everledger, geht es im Supply Chain Finance Management weniger darum den Kunden zu kennen (KYC), sondern das jeweilige Objekt. Künftig gelte also Know Your Object – KYO. An anderer Stelle wird Kemp mit dem Satz zitiert “We focus on the identity of objects.” Pilotkunde von Everledger ist der weltweit größte Diamantenkonzern De Beers[71].

Mit der Verbreitung von Edge Computing und der Fähigkeit der Maschinen und Geräte, Informationen verarbeiten zu können, steigen die Anforderungen an das Identitätsmanagement Digitaler Zwillinge. Eine Folge davon könnte sein, dass intelligente elektrische Steckverbinder die Funktionen von Sensoren und von Schaltschränken übernehmen[72]. Steckverbinder könnten demnach in die Rolle übergeordneter Digitaler Zwillinge schlüpfen.

[70] How the Identity of Things underpins digital twin integration
[71] Ende der Blutdiamanten dank Blockchain
[72] Intelligente elektrische Steckverbinder für die dezentrale Datenverarbeitung

Neue Geschäftsmodelle

Das Internet der Dinge schafft die Basis für neuartige Geschäfts- und Servicemodelle. Sowohl im IoT wie auch IIoT werden Funktionen und Rollen benötigt, die in der „alten“ Wirtschaft zum Standardrepertoire gehören, wie das Bank- und Versicherungswesen und das Marketing.

Identity Banking as a Service

Das Internet der Dinge bietet nach Ansicht zahlreiche Branchenbeobachter für Banken ein weites Betätigungsfeld [73] . Banken könnten im IoT und IIoT Funktionen übernehmen, die sie in der realen Wirtschaft schon ausüben. Damit ist vor allem das Risikomanagement gemeint, d.h. der Schutz der Daten und Geräte vor unberechtigten Zugriffen. Ebenso die Lancierung neuer Finanzierungsmodelle, die sich am Verbrauch orientieren (Pay per use)[74]- auch datenbasierte Kredite genannt[75].

Eine weitere Möglichkeit besteht in der Organisation von Datenmarktplätzen.

Weiterhin denkbar ist die Wiederbelebung des Bankgeheimnisses in Form eines digitalen Bankgeheimnis 4.0[76]. Dabei übernimmt die Bank den Schutz der Identitäten der Kunden und deren technischer Objekte/Geräte (Smart Home, IoT). Zum Kundenkreis zählen vor allem Unternehmen, die für den betriebsübergreifenden Datenaustausch Trusted Advisors benötigen. Zugang zu den Maschinen bekommen nur vertrauenswürdige Personen oder Geräte. Von Nutzen können hierbei Score-Werte für Maschinen, Personen oder Unternehmen sein. Diese Score-Werte sind nicht unabänderlich und letztgültig. Es muss die Möglichkeit bestehen, Widerspruch einzulegen und andere Quellen zur Bewertung der Vertrauenswürdigkeit hinzu zu ziehen.

Ob für die Ausübung dieser Funktion Banken erforderlich sind oder ob diese Aufgabe nicht an spezialisierten Zulieferer (Identity Banking as a Service) delegiert werden, wird sich zeigen. Sicher ist aber schon jetzt, dass in der Serviceindustrie, auf die wir uns zubewegen, die Bereitstellung verifizierter Identitäten in Echtzeit erfolgen muss.

[73] Enabling the Internet of Things: Why Banks should be Part of the Fabric of The IoT
[74] Digitale Finanzierungsmodelle für Industrie 4.0
[75] Datenbasierte Kredite für Firmenkunden
[76] Digitales Bankgeheimnis 4.0 – ein neues Geschäftsfeld? Banken als Schutz vor der totalen Überwachung

Insurance as a Service

Von mindestens ebenso großer Bedeutung wie für die Banken sind vertrauenswürdige Identitäten und Daten für die Versicherungsbranche, und hier insbesondere für die Industrieversicherer. Verschiedene Publikationen haben das Potenzial von Insurance as a Service im IoT thematisiert[77]. Chancen für die Versicherer bestehen in der Vorhersage/Prävention (Predictive Maintenance) und Sicherheit[72]. Sofern es gelingt, Ausfallszeiten von Maschinen oder ganzer Fabriken im Vorfeld zu verhindern, können die Versicherer ihre Kosten reduzieren und den Kunden günstigere Konditionen anbieten. Versichern können sich die Unternehmen u.a. gegen Identitätsdiebstahl. Die Versicherer werden darauf achten, dass die Unternehmen geeignete Verfahren zum Schutz der Maschinenidentitäten installiert haben.

Object Marketing

Ein weiteres Geschäftsfeld ist das Objekt Marketing[78]. Durch ihre digitale Identität können digitale Zwillinge direkt angesprochen werden – wie für Marketing-Zwecke. Entscheidend sind damit die Objektdaten und nicht die Kundendaten. Es werden also nicht Kunden direkt angesprochen, sondern die Objekte, digitalen Zwillinge, mit denen sie kommunizieren und interagieren. Exemplarisch dafür ist die Nachverfolgung von Produkten in der Supply Chain. Der Käufer/Konsument erhält verifizierte Informationen zur Herkunft des Produktes. Auf diese Weise können im Idealfall das Markenerlebnis sowie das Vertrauen der Kunden in das Unternehmen gestärkt werden, wodurch die Kundenbindung erhöht wird[74].

[77] Digital Ecosystems for insurers: Opportunities through the Internet of Things
[72] The Internet of Things (IoT) and Cybersisk Insurance
[78] Mit dem Digital Twin zu Object Marketing: Nicht gesucht und doch gefunden
[74] Blockchain und Marketing

Identity Relationship Management (IRM)

Sichere Identitäten von Personen, Maschinen und Unternehmen sind kein Selbstzweck. Ihr Sinn und Zweck in der vernetzten Wirtschaft und Gesellschaft bestehen darin, das Management der Beziehungen zwischen den verschiedenen Identitäten zu vereinfachen und transparent zu machen[79]. Technologisch bieten sich dafür die Blockchain, die Verfahren der Künstlichen Intelligenz und Graphen-Datenbanken an[80]. So wie es schon heute Identity Graphen zu Personen gibt, wird das auch künftig für Maschinen der Fall sein[77]. Der Graph veranschaulicht die Beziehungen der Maschine mit anderen Maschinen, Geräten, Personen und Unternehmen. Weiterhin gibt er Auskunft über den jeweiligen Kontext, in dem sich die Beziehungen, d.h. die Identifizierung und der Austausch von Daten, vollzieht. Das ist sowohl für Marketingzwecke aber auch für das Risikomanagement von hohem Wert.

Das Management der Beziehungen der Identitäten wird damit zu einer wichtigen Aufgabe in den Unternehmen, aber auch, wenngleich in schwächer ausgeprägter Form, für den Endnutzer.

Identity Relationship Management ist daher eng mit CRM verbunden. IRMSysteme können einen standardisierten Identitätsansatz für alle Anwendungen bereit stellen[81]. IRM-Systeme stehen für der Übergang von punktuellen Lösungen zu strategischen Plattformen.

Die in dieser Studie vorgestellten Startups sowie Venafi verfolgen bereits diesen Ansatz, ohne ihn explizit beim Namen zu nennen. Jedes Unternehmen ist auf seine Weise dabei, über Kooperationen entsprechende Ökosysteme aufzubauen.

[79] The next generation of IAM: Identity Relationship Management
[80] Artificial Intelligence & Graphh Technology. Enhancing AI with Context & Connections
[77] ID Graph: What Is It and How Can It Benefit Cross-Device Tracking?
[81] Identitäten richtig handhaben – damit Ihre digitale Geschäftsstrategie erfolgreich wird

Maschinenidentitäten in einer selbstorganisierten Umgebung

Wenn Industrie 4.0, das IoT, IToT und IDoT Realität werden, dann entsteht dadurch eine Komplexität, welche die bisherigen Steuerungsmodelle an ihre Kapazitätsgrenzen und darüber hinaus führen wird. Unternehmen geben ein Stück weit Autonomie aus der Hand. Die Grenzen der Unternehmen werden noch durchlässiger. Die Kontrollillusion löst sich in Luft auf. Kein Unternehmen, ganz gleich welcher Größe, kann die wachsende Komplexität, die mit der vernetzten Produktion einher geht, alleine bewältigen. Selbstorganisation, repräsentiert durch digitale Ökosysteme und Plattformen, übernimmt in vielen Bereichen die Steuerung.

Fredmund Malik spricht in dem Zusammenhang davon, dass das ControlSystem mindestens ebenso viel Varietät haben muss, wie das zu kontrollierende System.

„ein System kann nur insoweit unter Kontrolle gebracht werden, als das Conrol-System Varietät aufbringt; .. Einfache Systeme haben wenig Varietät und sind daher leicht unter Kontrolle zu bringen; komplexe Systeme mit sehr grosser Varietät erfordern sehr hohe Varietät für ihre Regulierung – und dies ist exakt das Problem des Managements komplexer Systeme“. (in: Systemisches Management, Evolution, Selbstorganisation)

Wenn demnächst Milliarden und Billionen von Maschinen, Geräten und Prozessen selbständig agieren, dann kann man sich in etwa vorstellen, wie komplex das Control-System sein muss. Im Bereich Maschinenidentitäten und IDoT wird das Identity Relationship Management diese Rolle übernehmen. Dabei handelt es sich um eine Gemeinschaftsaufgabe vertrauenswürdiger z.T. übergeordneter Instanzen (u.a. Regulierung, Standards, Governance), dezentraler Systeme (Distributed Ledger, Blockchain), Startups sowie Unternehmen/Konzerne.

Ausblick

Sichere Maschinenidentitäten bekommen durch die Verbreitung des Internets der Dinge wie auch des Industriellen Internets der Dinge eine herausragende Bedeutung sowohl für Unternehmen wie auch für die (End-)Kunden. Obwohl allgemeine Standards für das IoT, IIoT und IDoT wie überhaupt eine „Killer Applikation“ bislang fehlen, lassen sich, wie vorliegende Studie zeigt, dennoch einige Trends erkennen, die sich in den nächsten Jahren verstärken werden.

Generell ist davon auszugehen, dass die großen Internet- und Technologiekonzerne wie Google, Amazon, Apple, Microsoft und Alibaba versuchen werden, im IoT, IIoT und IDoT eine ähnlich dominante Rolle einzunehmen, wie wir sie heute bereits im herkömmlichen Internet (Suchmaschinen, E-Commerce, Betriebssysteme) kennen. Solange in diesem Bereich keine einheitlichen, neutralen Standards existieren, haben Amazon & Co. die Chance, ihre eigenen Quasi-Standards durchzusetzen. Derzeit verfügt keiner der großen Technologiekonzerne über eine durchgängige Lösung für die Identifizierung von Personen, Geräten, Maschinen und Unternehmen.

Auf den ersten Blick könnte die Blockchain-Technologie die Unternehmen und Kunden vor der Abhängigkeit bzw. dem Lock-In-Effekt, wie er von den großen Technologiekonzernen ausgeht, bewahren. Die in dieser Studie vorgestellten Startups aus dem Umfeld zeigen, dass es durchaus möglich ist, neue, dezentrale Infrastrukturen für den Austausch und die Verwaltung verifizierter Daten und Identitäten zu schaffen. Sie verdeutlichen weiterhin, wie wichtig die Kombination von Software und Hardware ist. Inkubatoren wie Next Big Thing mit dem weeve Network , Lösungsanbieter wie orbiter.de mit der orbiterchain und Venafi können Wegbereiter eines digitalen Ökosystem für Identity of Things werden.

Ganz unabhängig davon, welche Technologie oder Kombination sich am Markt durchsetzen wird, werden wir die Entstehung einer neuen Kategorie von Unternehmenssoftware, eines neuen Layers sehen. Oder vielleicht anders: Das Identitätsmanagement von Maschinen, technischen Objekten, Prozessen und digitalen Zwillingen erhöht den Stellenwert dessen, was wir heute im weiteren Sinn unter IAM verstehen. Viele Anzeichen sprechen dafür, dass das IAM vom IRM abgelöst, zumindest aber ergänzt wird. Identity of Things- und IRM-Systeme erhalten eine strategische Bedeutung für die Unternehmen, die weit über die Verwaltung von Zugangsberechtigungen hinaus geht. Es handelt sich um ein Werkzeug, um die Risiken und Chancen, die durch die Vernetzung der digitalen Identitäten von Personen, Geräten, Maschinen und Prozessen entstehen, zu bewerten und zu managen. Es zeigt – zumindest in indirekter Form – die Art und Weise der Vernetzung eines Unternehmens mit seiner Außenwelt, den relevanten Ökosystemen an.

Die Entstehung neuer Geschäfts- und Rollenmodelle deutet sich an, wie die des Identity Banking. Damit sind Unternehmen gemeint, die, wie Venafi, die Risiken im Bereich Identity of Things managen, wie mit der bereits erwähnten Ausfallgarantie für zertifikatsbasierte Produktionsausfälle.

Zu den Profiteuren der Entwicklung zählen Anbieter, die im IAM-Umfeld bislang kaum bis gar nicht wahrgenommen wurden: Die Hersteller von Procurement-Lösungen wie OpenText und SAP. Auf eindrückliche Weise schildert das der Report Enabling and Securing the Digital Supply Chain Using IAM and IoT. Unternehmen wie OptenText mit Covisint sehen sich durchaus in der Lage, das Identitätsmanagement über die gesamte Supply Chain abzuwickeln – alles aus einer Hand. SAP ist mit Ariba und Gigya in einer ähnlichen Position.

Die Ebene, auf der sich alle die in dieser Studie genannten Anbieter zusammenfinden, ist das Identity Relationship Management. Das IRM wiederum kann nur dann seine Aufgabe erfüllen, d.h. Anwendungen für Unternehmen und Personen bereitstellen, wenn die Herkunft der Maschinenidentitäten und der ausgetauschten Daten zweifelsfrei geklärt ist. Kaum ein Unternehmen wird es schaffen, alles aus einer Hand anzubieten. Die größten Erfolgschancen hat der Anbieter, dem es gelingt, ein dynamisches Ökosystem aufzubauen und auf die richtigen Standards setzt.

Impressum

Kontakt

Ralf Keuper

Kolpingstr. 3

33428 Harsewinkel

E-Mail: ralf.keuper@bankstil.de

Autor: Ralf Keuper

V.i.S.d.P.:

Ralf Keuper

September 2019