PLATTFORM INDUSTRIE 4.0

DISKUSSIONSPAPIER

Vertrauensinfrastrukturen im Kontext von Industrie 4.0 – Anforderungen und Lösungsbausteine

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Stand
März 2021

Diese Publikation wird ausschließlich als Download angeboten.

Gestaltung
PRpetuum GmbH, 80801 München

Bildnachweis
koto_feja / istockphoto / Titel
Plattform Industrie 4.0

Zentraler Bestellservice für Publikationen der Bundesregierung:
E-Mail: publikationen@bundesregierung.de
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Executive Summary

Das Diskussionspapier „Vertrauensinfrastrukturen im Kontext von Industrie 4.0 – Anforderungen und Lösungsbausteine“ beschreibt Anforderungen für die Gestaltung digitaler und automatisierter Geschäftsbeziehungen zwischen zwei oder mehr Unternehmen entlang der Supply Chain und diskutiert ausgewählte Lösungsbausteine zu deren Erfüllung.

Eine wesentliche Herausforderung der Digitalisierung entlang von Versorgungsketten (engl. Supply Chains) ist die Etablierung von vertrauensvollen Lieferbeziehungen. Jedes beteiligte Unternehmen bildet dabei eine „Insel“, in der Maßnahmen ergriffen werden, um innerhalb des eigenen Unternehmens Vertrauen in die eigenen Prozesse und Produkte zu haben. Innerhalb einer Versorgungskette ist es aber entscheidend zu wissen, ob die zugelieferten Produkte die vertraglich vereinbarte Qualität aufweisen, z. B. hinsichtlich Funktionalität und Verlässlichkeit. In nicht digitalen Anwendungsfällen (z. B. klassische mechanisch-/elektrische Bauteile) kann die Qualitätsprüfung im Rahmen der Wareneingangsprüfung erfolgen. Bei Produkten, die umfangreich IT nutzen (z. B. komplexe, programmierte Steuergeräte), reicht eine Wareneingangsprüfung allein nicht mehr aus. Bei diesen Produkten muss der Empfänger i. d. R. wissen, von wem das Produkt hergestellt wurde und welche Qualitätssicherungsmaßnahmen vom Hersteller umgesetzt wurden. Die Beantwortung folgender Fragen ist entscheidend: Wer hat das Produkt hergestellt? Wie schließe ich aus, dass das Produkt eine Fälschung ist? Hat der Hersteller alle aus meiner Sicht erforderlichen Maßnahmen ergriffen, um die von mir erwartete Produktqualität zu gewährleisten? Hat der Lieferant gleichwertige Anforderungen an seine Zulieferer gestellt?

Dazu ist Transparenz über die gegenseitigen Anforderungen wesentlich. Es muss Einigkeit bestehen, wie diese gemäß einheitlicher Standards erfüllbar sind. Ist dies nicht möglich, muss zumindest Einvernehmen darüber hergestellt werden, wie diese vergleichbar gemacht werden können. Die „Vertrauensinseln“ der Unternehmen müssen in diesem Sinne zu einem „Vertrauensraum“ der Versorgungskette zusammenwachsen. **Das Diskussionspapier entwirft einen Vertrauensraum, einen virtuellen, digitalen Raum, in dem sich Industrie 4.0-Teilnehmer auf gemeinsame Vertrauensanforderungen geeinigt haben.** In einem Vertrauensraum müssen potenzielle Geschäftspartner ihre Erwartungen und Fähigkeiten verständlich beschreiben und austauschen können. Dabei ist es essenziell, dass die Unternehmen dem Ursprung und der Unveränderbarkeit von Erwartungen und Nachweisen über Fähigkeiten vertrauen können.

Das Diskussionspapier beschränkt sich zunächst auf den Aspekt der IT-Sicherheit und die Verwendung von Sicheren Digitalen Identitäten entlang der Supply Chain. Speziell beschreibt dieses Diskussionspapier Anforderungen für Nachweise, die sich auf die Identifizierung und Authentifizierung von Geschäftspartnern sowie die Qualität ihrer Produkte, Prozesse und Dienste beziehen. In diesem Zusammenhang wird auch auf den Klärungsbedarf in der Industrie 4.0 in Bezug auf dezentrale Ansätze zur Verwaltung von Identitäten hingewiesen. Zudem werden erste Lösungsansätze zur Erfüllung von Vertrauensanforderungen als eine Art modularer Baukasten beschrieben. Diese erfüllen aber weder den Anspruch auf Vollständigkeit noch liefern sie konkrete Umsetzungsempfehlungen.

Weiterhin beschreibt dieses Dokument Anforderungen und Herausforderungen an bestehende Public Key Infrastrukturen als Grundlage für den Aufbau von Vertrauensbeziehungen in der industriellen Produktion. Insbesondere müssen in der Industrie 4.0 (internationale) unternehmensübergreifende Konstrukte, die unterschiedliche Vertrauensanforderungen haben können, mit bestehenden Verfahren und Konzepten verknüpft werden.

Eine zentrale Erkenntnis dieses Dokuments ist, dass Vertrauenslisten, engl. Trusted Lists, dazu beitragen können, eine Übersicht darüber zu liefern, welche Industrie 4.0-Teilnehmer gemeinsame Vertrauensanforderungen erfüllen oder nicht.

1. Präambel

Das vorliegende Papier soll eine Diskussionsgrundlage für die Umsetzung von Vertrauensinfrastrukturen im Kontext von Industrie 4.0 liefern. Dabei sollen dem Leser die Anforderungen an solche Vertrauensinfrastrukturen nähergebracht werden. Darüber hinaus werden Lösungsbausteine vorgestellt, die sich für eine Verknüpfung mit bestehenden Systemen eignen.

Zielgruppe sind alle Unternehmen, die an (internationaler) Industrie 4.0-Kommunikation teilnehmen möchten und innerhalb dieser Kooperation entsprechende IT-Sicherheitsanforderungen erfüllen und ggf. aufbauen müssen. Speziell richtet sich das Dokument an technisch Verantwortliche im IT- und Security-Umfeld.

Die folgenden Dokumente dienen als Verständnisgrundlage:

- Internationales Papier „IIoT Value Chain Security – The Role of Trustworthiness“ (1)
- Ergebnispapier „Technischer Überblick: Sichere Identitäten“ (2)

1.1 Struktur des Dokuments

Der Text gliedert sich in die folgenden Bereiche: Zunächst werden relevante Begriffe erläutert sowie deren Bezug zur Industrie 4.0 hergestellt. Als nächstes wird auf die Erfordernisse und die Zielsetzung einer Vertrauensinfrastruktur eingegangen. Im Hauptteil werden grundsätzliche Anforderungen an eine Vertrauensinfrastruktur sowie erste Lösungsbausteine zur Konzeption beschrieben. Im abschließenden Ausblick wird auf den Klärungsbedarf bezüglich dezentraler Identitätssysteme hingewiesen.

1.2 Begriffsklärungen

Unter „Industrie 4.0“ begreifen wir alle Geschäftsprozesse, die durch die Vernetzung von Wertschöpfungsketten sowie von Maschinen und Abläufen mit Hilfe von Informations- und Kommunikationstechnologie möglich werden.[1] Beispielsweise sollen so Produktionsanlagen kooperieren, die auf unterschiedliche Standorte weltweit verteilt sind. Weitere Beispiele sind, dass Monitoring- und Wartungsprozesse zu einem optimierten Einsatz von Ressourcen und damit zur verbesserten Wertschöpfung und Qualitätsverbesserung beitragen und auch Clouddienste an Bedeutung gewinnen.

Wertschöpfungsnetzwerke der Industrie 4.0 beruhen auf smarten Produktionsanlagen, die ad hoc neue Geschäftsbeziehungen eingehen und Verträge abschließen – mehr oder minder autonom. Doch auf welcher Grundlage steht diese Vision?

Damit sich ein Geschäftspartner ausweisen kann und beispielsweise von einer Produktionsanlage als geeignet eingestuft wird oder gültige firmenübergreifende Verträge in der digitalen Welt abgeschlossen werden können, muss Vertrauenswürdigkeit, wie bspw. im internationalen Papier „IIoT Value Chain Security – The Role of Trustworthiness“ (1) beschrieben, etabliert werden. Eine Vertrauensinfrastruktur im Kontext von Industrie 4.0 ist also ein Rahmen, in dem Nachweise für die Vertrauenswürdigkeit in einem Wertschöpfungsnetzwerk unternehmensübergreifend ausgetauscht werden können. Eine angemessene Vertrauenswürdigkeit von Sicheren Digitalen Identitäten, vgl. Ergebnispapier „Technischer Überblick: Sichere Identitäten“ (2), ist eine essenzielle Voraussetzung für multilaterale und unternehmensübergreifende Wertschöpfungsnetzwerke bzw. Supply Chains.

Der Begriff „Entität“ wird in diesem Dokument entsprechend des Standards „ISO/IEC 24760“ (3) verwendet, um Teilnehmer der Industrie 4.0 zu bezeichnen, beispielsweise Unternehmen (Betreiber, Hersteller, Integrator), Systeme, Maschinen, Komponenten, Produkte, Beschäftigte in ihrer Rolle und nichtphysische Objekte (Software, digitale Zwillinge, Prozesse).

Für das Security- und Risikomanagement von Value/Supply Chains bezieht sich der Begriff **„Vertrauenswürdigkeit“** auf die Fähigkeit eines Suppliers, die Erwartungen eines potenziellen Vertragspartners in einer verifizierbaren Weise zu erfüllen. (1)

Eine **„Sichere Identität“** ist eine eindeutige Identität mit zusätzlichen Sicherheitseigenschaften für eine belastbar vertrauenswürdige Authentifizierung der Entität (d.h. mit angemessenen Maßnahmen zur Verhinderung der Vortäuschung einer falschen Identität). (2)

Jedes Unternehmen sollte seine Anforderungen an vertrauenswürdige Wertschöpfungsnetzwerke festlegen. Damit Vertrauenswürdigkeitsanforderungen organisationsübergreifend erreicht und interpretiert werden können, müssen diese Anforderungen sowie entsprechende Prüfvorgaben durch eine übergreifend gültige Vertrauensinfrastruktur erfüllt werden. Unternehmen mit gemeinsamen Vertrauensanforderungen können einen Vertrauensraum bilden. **Ein Vertrauensraum ist also ein virtueller, digitaler Raum, in dem sich Industrie 4.0-Teilnehmer auf gemeinsame Vertrauensanforderungen geeinigt haben.**

1 Vgl. https://www.plattform-i40.de/PI40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html

1.3 Chancen und Herausforderungen einer Vertrauensinfrastruktur

Industrie 4.0 verspricht Chancen auf neue Geschäftsmodelle und ein hohes Maß an Effizienzsteigerungen, die mit der Digitalisierung der industriellen Produktion einhergehen. Kleine und mittlere Unternehmen (KMU) müssen hierbei genauso wie Großunternehmen an Industrie 4.0-Geschäftsmodellen partizipieren können. Die Voraussetzungen und Bedingungen, unter denen sie die neuen Dienste und Geschäftsmodelle nutzen oder eigene Dienste und Geschäftsideen anbieten können, müssen transparent und interoperabel gestaltet werden. Hierfür wird eine Vertrauensinfrastruktur benötigt.

Im Kontext von Industrie 4.0 ergibt sich für Unternehmen die Herausforderung, unternehmensübergreifende Wertschöpfungsnetzwerke sowie einen multilateralen Datenaustausch zu etablieren und hierbei interoperable, verlässliche Anforderungen bezüglich der Korrektheit und Art der Identifizierung und Authentifizierung zu erreichen.

1.4 Anwendungsszenario

Für das Anwendungsszenario werden Unternehmen betrachtet, die in der Ausgangslage keine vertrauenswürdigen und belastbaren Informationen übereinander haben. Sie müssen sich diese erst beschaffen, bevor sie eine Geschäftsbeziehung miteinander eingehen. In der Industrie 4.0 soll es möglich sein, dass der Austausch dieser Informationen vollständig digital und automatisiert abläuft.

Um sich gegenseitig vertrauen zu können, müssen Unternehmen untereinander Dokumente, z. B. Qualifizierungszertifikate, Referenzen oder Bescheinigungen, austauschen und diese beurteilen. Neben der Identifizierung der Unternehmen selbst, muss die Qualität des Geschäftsgegenstands oder der Dienstleistung, also das Ergebnis der angestrebten Transaktion in Form von Informationen und/oder Produkten, einschätzbar sein. Dies geschieht auf Basis vertrauenswürdiger Informationen.

Das Vertrauen in den Informationsaustausch innerhalb eines Unternehmens wird durch das Unternehmen selbst festgelegt. Für den multilateralen Austausch über Unternehmensgrenzen hinweg sind weitere organisatorische und technische Prozesse sowie Maßnahmen erforderlich, da unterschiedliche Zuständigkeiten gegeben sind. Die Unternehmen können dabei auch aus unterschiedlichen Ländern oder Wirtschaftsräumen stammen. Um darauf zu vertrauen, dass anforderungsspezifische Eigenschaften eines Geschäftspartners korrekt sind, wird eine Möglichkeit benötigt, „übergreifendes Vertrauen“ aufzubauen. Die Anwendungsszenarien der Industrie 4.0 sehen darüber hinaus Kooperationen und Interaktionen zwischen Entitäten (Maschinen, Produkte, Menschen etc.) unterschiedlicher Unternehmen vor. Unterschiedliche Entitäten sollen in der Lage sein, unabhängig von einem Wirtschaftsraum vertrauensvoll miteinander zu agieren.

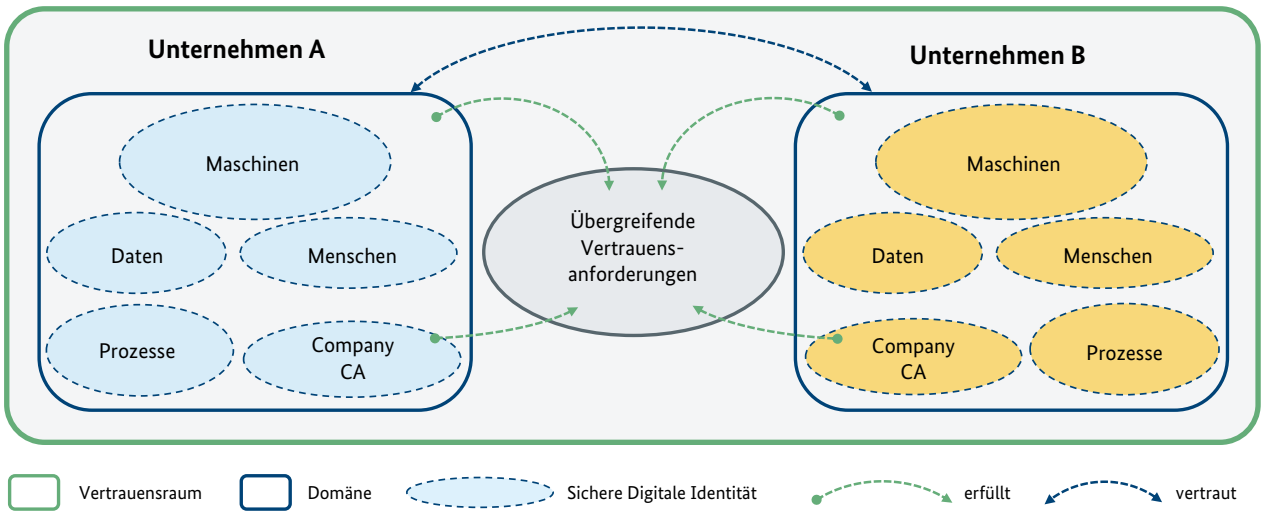
1.5 Zielsetzung

Das Ziel dieses Dokuments ist es, eine Vertrauensinfrastruktur zu beschreiben, die eine vertrauenswürdige Identifikation und Authentifikation in unternehmensübergreifenden Industrie 4.0-Wertschöpfungsnetzwerken ermöglicht sowie eine Grundlage für die Nutzung von Sicheren Digitalen Identitäten im unternehmensübergreifenden Kontext schafft. Eine vertrauenswürdige Infrastruktur ist hiervon abzugrenzen. Sie bezieht sich nicht auf Sichere Digitale Identitäten, sondern auf die technischen Möglichkeiten zum Informationsaustausch. Die vertrauenswürdige Infrastruktur wird in diesem Dokument nicht betrachtet.

Eine Vertrauensinfrastruktur hat zum Ziel, eine angemessene, unternehmensübergreifende Belastbarkeit in Bezug auf Sichere Digitale Identitäten zu erreichen. Identifikatoren haben dabei eine zentrale Bedeutung. Sie ermöglichen eine eindeutige Bezeichnung der Entität.

Abbildung 1 beschreibt das Konzept des von der Infrastruktur geschaffenen Vertrauensraums mit potenziellen Sicheren Digitalen Identitäten. Zur Vereinfachung und Übersichtlichkeit wird der Vertrauensraum durch zwei Domänen bzw. Unternehmen dargestellt. Im unternehmensübergreifenden und multilateralen Kontext müssen sich mehrere Vertrauensräume vertrauen können. Hierfür müssen sich die Unternehmen auf gemeinsame Anforderungen einigen. Diese übergreifenden Vertrauensanforderungen bilden den Anknüpfungspunkt für das wechselseitige Vertrauen der jeweiligen Domänen in die Identitäten der Menschen, Daten und Maschinen sowie die Nachvollziehbarkeit der Prozesse. Eine zentrale Voraussetzung für das Vertrauen ist eine unternehmensintern genutzte Company-Certification Authority (CA; im Eigenbetrieb oder als Dienst) für die Ausstellung von Sicheren Digitalen Identitäten in den Unternehmen, wobei die übergreifenden Vertrauensanforderungen erfüllt werden müssen. Nur auf Grundlage einer unternehmensübergreifenden Identifizierung und Authentifizierung kann die Vertrauenswürdigkeit von Informationen automatisiert geprüft werden.

Abbildung 1: Konzept des von der Infrastruktur geschaffenen Vertrauensraums



Quelle: Plattform Industrie 4.0

2. Grundsätzliche Anforderungen an eine Vertrauensinfrastruktur

Im Folgenden wird auf die grundsätzlichen Anforderungen an eine Vertrauensinfrastruktur eingegangen. Dazu werden zunächst Anforderungen beschrieben, welche eine Identifizierung und Authentifizierung innerhalb eines Vertrauensraums bzw. eine Integritätssicherung von Dokumenten und Systemen ermöglichen. Als nächstes wird die Validierung von Prozessen und Attributen sowie die Vertrauensbildung bei Produkten, Diensten und Prozessen beschrieben. Zuletzt wird der Zusammenhang zwischen der Identifizierung und Authentifizierung bzw. Integritätssicherung und dem Vertrauen in Prüfnachweise hergestellt.

2.1 Identitätsinfrastrukturen

Im Folgenden wird ein mögliches Schema für eine Identitätsinfrastruktur beschrieben. Diese stellt Sichere Digitale Identitäten für Unternehmen zur Verfügung. Mit Sicheren Digitalen Identitäten können sich Unternehmen gegenseitig authentifizieren bzw. die Integrität und Authentizität von Dokumenten validieren.

Dazu ist es erforderlich, dass sich Unternehmen ihre Identität durch eine unabhängige Stelle bestätigen lassen. Im Folgenden wird für diese Stelle der Begriff **Identity Authenticating Certificate Provider (IACP)** verwendet. Diese neutrale Stelle identifiziert die beteiligten Unternehmen, verifiziert ggf. zusätzliche Informationen und bestätigt die Identität (z. B. Name, Adresse). Dabei ist durch die unabhängige Stelle nachvollziehbar darzulegen, wie und wann die Informationen verifiziert wurden. Dies ist notwendig, damit sich andere Domänen im Vertrauensraum auf die Korrektheit verlassen können. Auf Basis dieser Prüfung wird durch den IACP ein **Identity Authenticating Certificate (IAC)** ausgestellt. Bei beiden Begriffen wird an die Begriffsbildung angeknüpft, die bereits in dem internationalen Papier „IIoT Value Chain Security – The Role of Trustworthiness“ (1) vorgenommen wurde.

IACs enthalten einen Identifikator, weitere relevante Identitätsdaten und einen öffentlichen kryptographischen Schlüssel. Der zugehörige private Schlüssel befindet sich im Besitz des Unternehmens. Bei der Signatur eines Dokuments mit dem privaten Schlüssel kann die Signatur mittels des im IAC enthaltenen öffentlichen Schlüssels geprüft werden. Da nur das Unternehmen im Besitz des privaten Schlüssels ist, wird auf diese Weise die Herkunft bestätigt. Durch die Inhalte des IACs wird eine Zuordnung zu dem Unternehmen möglich, und die Bestätigung der Inhalte durch den IACP garantiert, dass diese auch korrekt sind. Technologisch bieten sich aufgrund der bisherigen Verbreitung X.509-Zertifikate der 3. Version des Standards „ISO/IEC 9594-8“ (4) an. Neuere Entwicklungen können ebenfalls genutzt werden.

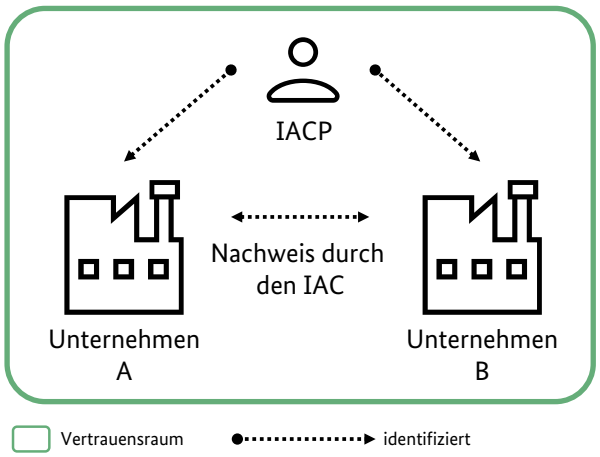
Unternehmen können in unterschiedlichen Vertrauensräumen agieren. Ein Vertrauensraum kann gebildet werden, indem bspw. ein Land, eine Wirtschaftsregion oder eine Branche gemeinsame Anforderungen aufstellt. Innerhalb jedes Vertrauensraums müssen sich alle Teilnehmer auf Anforderungen für IACPs einigen. IACs dienen dabei erst einmal der vertrauenswürdigen Identifikation der Unternehmen untereinander.

Mit den IACs werden noch keine weiteren Aussagen über die Fähigkeiten (z. B. hinsichtlich eines Security Managements oder eines Secure Development Lifecycles) der Unternehmen getroffen. Vertrauensanforderungen an IACs müssen regelmäßig überprüft und aktualisiert werden.

2.1.1 Zentrale und dezentrale IACP

In Vertrauensräumen gibt es jeweils mindestens einen IACP. Dabei kann strukturell zwischen einem zentralen Szenario mit einem zentralen IACP und einem Szenario mit mehreren parallel agierenden IACP unterschieden werden.

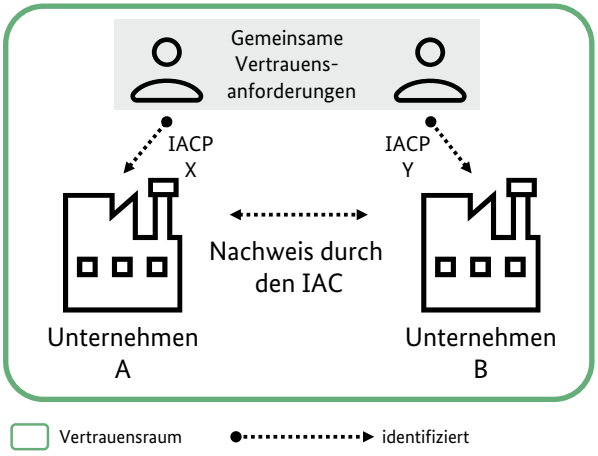
Abbildung 2: Zentrale IACP



Quelle: Plattform Industrie 4.0

Abbildung 2 stellt einen zentralen IACP dar. In diesem Fall haben sich alle Unternehmen in dem Vertrauensraum darauf verständigt, dass die Anforderungen an die Identifizierung, Verwaltung und Vergabe der IACs ausreichen, welche der zentrale IACP zusichert. Alle Unternehmen sind überzeugt, dass sie den Zusicherungen des zentralen IACP hinsichtlich den Inhalten des IACs vertrauen können. Diese Überzeugung bildet sich aufgrund organisatorischer und technischer Maßnahmen, welche der IACP umsetzt. Dies kann durch Audits und vertragliche Regelungen sichergestellt werden.

Abbildung 3: Dezentrale IACP



Quelle: Plattform Industrie 4.0

Das Szenario eines zentralen IACP ist in der Praxis für einzelne Bereiche oder Branchen denkbar. Wahrscheinlicher ist jedoch, dass es mehrere IACP gibt, um eine Monopolstellung eines IACP zu verhindern. Abbildung 3 zeigt dies. In diesem Fall werden Unternehmen A und B durch IACP X und Y identifiziert und auf dieser Basis die jeweiligen IACs ausgestellt. Unternehmen B vertraut den Zusicherungen von IACP X sowie Unternehmen A von IACP Y.

Um die Zusicherungen zu gewährleisten, ist es notwendig, dass beide IACP in dem Vertrauensraum gemeinsame Vertrauensanforderungen erfüllen. Diese müssen transparent offengelegt sowie deren Einhaltung und Umsetzung durch unabhängige Stellen bestätigt werden. In jedem Fall muss es möglich sein, zu prüfen, ob ein IACP die Anforderungen an den Vertrauensraum erfüllt und in diesem anerkannt ist. Ansonsten ergeben sich Probleme hinsichtlich der Zugehörigkeit. Bei eIDAS (siehe Kapitel 3.1) wird dies zum Beispiel durch sogenannte Trusted Lists realisiert, die von einer zentralen Stelle ausgestellt werden und Vertrauensdiensteanbieter auflisten.

2.1.2 Unterschiedliche Vertrauensanforderungen von Vertrauensräumen

Die Anforderungen an die IACP können sich von Vertrauensraum zu Vertrauensraum unterscheiden. Je nach Anwendungsfall oder Branche kann es unterschiedliche Anforderungen an die zu bestätigenden Informationen geben. Beispielsweise kann es in einem Vertrauensraum ausreichen, dass die Informationen bzgl. der Identifikation lediglich für fünf Jahre aufbewahrt werden. In einem zweiten Vertrauensraum ist es aufgrund von gesetzlichen Vorgaben unter Umständen notwendig, auch nach 20 Jahren über einen Online-Dienst noch auf die Informationen zugreifen zu können.

Ein anderes Beispiel sind unterschiedliche Anforderungen an die Prozesse des IACP, die als Nachweis dienen.

Aus den Anforderungen hinsichtlich der Prozesse, Nachweise, Speicherfristen und Verfügbarkeiten der Dienste ergeben sich unterschiedliche Aufwände. Diese führen zu unterschiedlichen Kosten.

Diese Qualitätsunterschiede zwischen den Vertrauensräumen müssen erkennbar und nachvollziehbar sein. Es ist darzulegen, welche Anforderungen an die Qualitäten hinsichtlich der verwalteten Identitäten und Überprüfungen durch IACP erfüllt sind. Dazu kann auf Konzepte aus Kapitel 2.2 zurückgegriffen werden. Wenn ein IACP die Anforderungen aus verschiedenen Vertrauensräumen erfüllt, können seine IACs in verschiedenen Vertrauensräumen durch die Unternehmen genutzt werden.

2.1.3 Attribute der Unternehmen

Für den Aufbau von Geschäftsbeziehungen spielt nicht nur allein der Name des Unternehmens eine Rolle. Es sind ggf. weitere Informationen von Relevanz. Beispiele hierfür können sein:

- Zeichnungsberechtigte Personen,
- Zertifizierungen von Prozessen,
- Verweise auf unternehmenseigene PKIs, die für Produktidentitäten genutzt werden.

Ein IAC muss die Möglichkeit bieten, weitere Informationen zu beinhalten bzw. zu referenzieren, um weitere Nachweise direkt mit dem IAC zu verbinden.

Zudem sollte ein Unternehmen, das unterschiedliche IACs verwendet, jeweils den gleichen eindeutigen Identifikator nutzen, um eine Referenz über Vertrauensräume hinweg zu ermöglichen.

2.1.4 Maschinenverarbeitbare Formate und transparente Dokumentation

Für eine Nutzung von IACs im Kontext von Industrie 4.0 ist eine weitestgehende Automation erforderlich. Gleichzeitig ist eine transparente, verständliche und nachvollziehbare Dokumentation erforderlich, um auch eine Prüfung durch Menschen zu ermöglichen. IACs müssen daher in maschinenverarbeitbaren und interoperablen Formaten vorliegen. Gleiches gilt für die Attribute und die Anforderungen.

Um eine Auswertung durch Menschen zu ermöglichen, müssen entsprechende Werkzeuge verfügbar sein, um die Lesbarkeit und Verständlichkeit zu gewährleisten.

2.2 Vertrauen in Fähigkeiten, Prozesse, Dienste und Produkte

Das gegenseitige Vertrauen der Unternehmen kann sich auf zusätzliche Nachweise stützen. Diese dienen dazu, die Fähigkeiten der Unternehmen zu bestätigen. Nachweise können sich beispielsweise auf verschiedene Prozesse, Dienste oder Produkte beziehen:

- Bei den Prozessen kann es sich um die Umsetzung eines Informationssicherheitsmanagementsystems nach „ISO 27001“ (5) bzw. dem IT-Grundschutz des BSI[2] oder auch um einen sicheren Entwicklungszyklus für Produkte nach der „IEC 62443-4-1“ (6) handeln. Auch andere Unternehmensprozesse könnten von Bedeutung sein.

- Bei den Produkten kann es sich beispielsweise um Produktfunktionalitäten hinsichtlich IT-Sicherheit nach „IEC 62443-4-2“ (7) oder Common Criteria „ISO/IEC 15408“ (8) handeln. Weiterhin besteht die Möglichkeit, Produktidentitäten zu prüfen und so die Herkunft und Integrität des Produktes zu validieren.

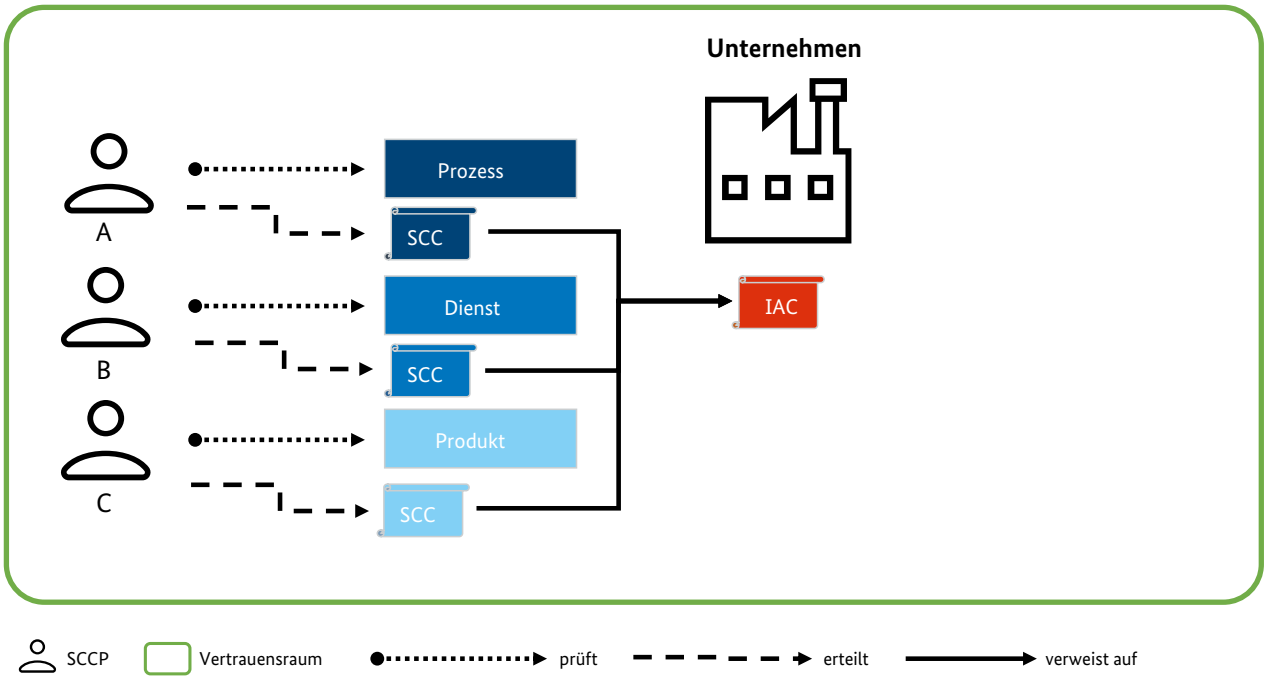
Ein **Security Certification Certificate Provider (SCCP)** prüft anhand definierter Kriterien und stellt im Anschluss einen Bericht sowie bei positivem Prüfergebnis ein **Security Certification Certificate (SCC)** aus. Abbildung 4 soll die Prüfung unterschiedlicher Eigenschaften von Unternehmen verdeutlichen. Beispielhaft wird hier dargestellt, dass im Industrie 4.0-Kontext SCCs für Prozesse, Dienste oder Produkte ausgestellt werden können, die auf das IAC des Unternehmens referenzieren, für das sie ausgestellt wurden.

2.2.1 Gegenseitige Anerkennung von SCCs

Es muss transparent und nachvollziehbar sein, was, wie, wann geprüft wurde. Die Kriterien für die SCCs müssen daher im Vertrauensraum einheitlich festgelegt sein. Als Grundlage kommen gegenseitig anerkannte Standards sowie dazugehörige Prüfvorschriften und -schemata zum Einsatz. Auf diese Weise können SCCs unterschiedlicher SCCP anerkannt werden.

Beispielsweise kann hierbei künftig ein Zertifizierungsschema des „Cyber Security Act“ (CSA) (9) der EU eine Rolle spielen. Ebenso kommt das „System für Konformitätsbewertungssysteme elektrotechnischer Betriebsmittel und Komponenten der International Commission on the Rules for the Approval of Electrical Equipment“ (IECEE)[3] in Frage.

Abbildung 4: Prüfung unterschiedlicher Eigenschaften von Unternehmen



Quelle: Plattform Industrie 4.0

2 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html

3 https://www.iecee.org

Als Standard können beispielsweise ISO- und IEC-Normen, wie unter Abschnitt 2.2 erwähnt, verwendet werden.

Wenn innerhalb des Vertrauensraums unterschiedliche Kriterienkataloge angewendet werden, weil es beispielsweise mehrere ähnliche Standards für den gleichen Beschreibungsgegenstand gibt, müssen sich die Unternehmen darauf einigen, wie die Gleichwertigkeit hergestellt werden kann. Damit soll sichergestellt werden, dass trotz der Verwendung unterschiedlicher Standards ein einheitliches Anforderungsniveau erreicht wird.

Ein Beispiel dafür sind die „ISO 27001“ (5), die „IEC 62443-2-1“ (10), das NIST Cybersecurity Framework[4] und der IT-Grundschutz des BSI[5]. Alle beschreiben den Aufbau eines Informationssicherheitsmanagementsystems. Beim IT-Grundschutz des BSI wird mit der Erteilung des Zertifikats für das „Standard“-Niveau gleichzeitig bescheinigt, dass die Anforderungen aus der ISO 27001 erfüllt werden.

2.2.2 Zuordnungen der SCCs zu einem IAC

Die SCCs sind direkt einem Unternehmen zuzuordnen. Es darf nicht möglich sein, dass ein SCC von einem anderen Unternehmen genutzt, missbraucht oder gefälscht wird. Es handelt sich grundsätzlich um ein zusätzliches Attribut eines Unternehmens (wie in Kapitel 2.1.3 beschrieben).

Es muss immer eine vertrauenswürdige Verbindung zwischen den IACs und den SCCs hergestellt werden. Dabei ist zu beachten, dass sowohl IACs als auch SCCs nur eine begrenzte Gültigkeitsdauer besitzen und die Erneuerung vorgesehen werden muss.

2.2.3 Unterschiedliche Aussteller

Innerhalb eines Vertrauensraums kann es unterschiedliche Anforderungen der Unternehmen an die Unabhängigkeit der Prüfung geben. So ist in manchen Fällen eine Herstellerselbsterklärung ausreichend. Der Hersteller agiert in diesen Fällen selbst als SCCP. In anderen Fällen ist eine unabhängige Prüfstelle zu involvieren, die die Rolle des SCCP übernimmt.

Im SCC muss daher erkennbar sein, wer die Prüfung wie und wann durchgeführt hat. Dies wird durch ein IAC der Prüfstelle (SCCP) ermöglicht.

Bei mehreren SCCP kann ähnlich wie bei den IACP innerhalb des Vertrauensraums auf eine Liste zurückgegriffen werden. Diese listet alle akzeptierten SCCP auf und wird von einer zentralen Stelle ausgegeben.

2.2.4 Maschinenverarbeitbare Formate

Derzeit werden SCCs üblicherweise in Form eines händisch unterschriebenen und gesiegelten Papierdokuments ausgestellt. Wie bereits in Kapitel 2.1.4 beschrieben, müssen die SCCs für einen automatisierten Austausch in maschinenlesbaren und interoperablen Formaten vorliegen. Darin müssen unter anderem Prüfvorschriften, -tiefe, -ergebnisse und -organisation erkennbar sein. Für diese Beschreibung fehlen momentan noch Standards.

Gleichzeitig ist eine transparente, verständliche und nachvollziehbare Dokumentation erforderlich, um auch eine Prüfung durch Menschen zu ermöglichen.

2.2.5 Bereiche für SCCs

Die SCCs müssen unterschiedliche Eigenschaften, Informationen und Nachweise abdecken, die zwischen den Unternehmen ausgetauscht werden. Einige Beispiele hierfür sind:

SCCs für Prozesse und Dienste

Hierbei geht es um die Prozesse und Dienste eines Unternehmens. Dies betrifft unter anderem das Informationssicherheitsmanagement, die sichere Entwicklung sowie den sicheren Betrieb von Diensten. Um diese zu prüfen, wird bspw. auf die IEC 62443, ISO 27001 oder BSI IT-Grundschutz zurückgegriffen. Weitere unternehmensinterne Prozesse können ggf. ähnlich geprüft und bestätigt werden.

SCCs für Produkte

Bei Produkten werden die (Sicherheits-)Eigenschaften eines Produktes bestätigt. Hierzu kommen bspw. die „ISO/IEC 15408“ (8) und die „IEC 62443-4-2“ (7) in Frage.

4 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

5 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html

2.3 Zusammenspiel der genannten Rollen für die Industrie 4.0

Um eine automatisierte Vertrauensinfrastruktur zu ermöglichen, müssen die bisher genannten Anforderungen kombiniert werden. In Abbildung 5 wird das Zusammenwirken der vorgestellten Konzepte dargestellt.

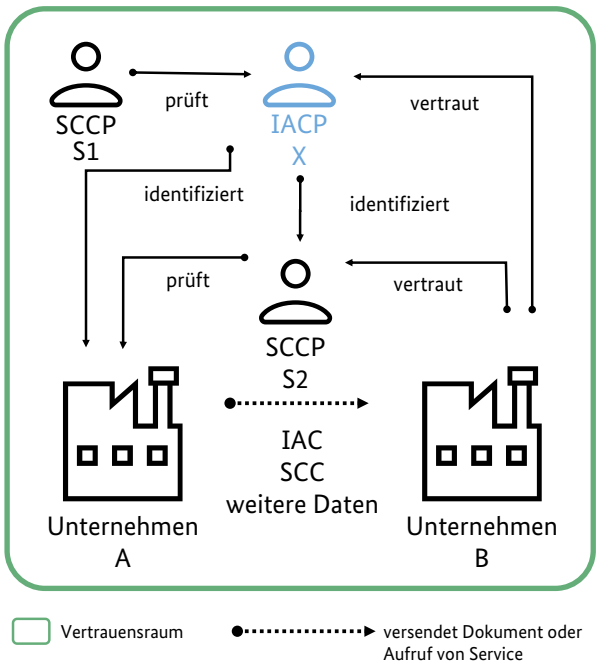
Alle beteiligten Parteien in dem Beispiel befinden sich in einem gemeinsamen Vertrauensraum. IACP X hat definierte Prozesse für die Identifizierung von Unternehmen. Diese sind durch SCCP S1 geprüft und mittels SCCs bestätigt. Dem IACP (in diesem Beispiel X) wird durch den Beitritt in den Vertrauensraum und die Akzeptanz der entsprechenden Anforderungen vertraut.

Unternehmen A wird durch den IACP X bestätigt und erhält ein entsprechendes IAC. Zudem prüft SCCP S2 beispielsweise das Vorhandensein und die Wirksamkeit eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001 (5) oder eines Cybersicherheitsmanagementsystems (CSMS) nach IEC 62443-2-1 (10). Der SCCP stellt ein SCC aus, das den Geltungsbereich des ISMS bzw. des CSMS beschreibt.

Im Rahmen eines Geschäfts übermittelt Unternehmen A das SCC sowie weitere Daten an Unternehmen B. Diese Übertragung wird durch das IAC bzw. durch die Nutzung der enthaltenen Schlüssel von Unternehmen A authentisiert. Bei den weiteren Daten kann es sich beispielsweise um ein Angebot auf eine Ausschreibung handeln oder auch um zusätzliche Attribute wie Bonitätsinformationen.

Unternehmen B wertet das SCC und die weiteren Daten aus. Dabei kann ein Abgleich mit internen Vorgaben erfolgen. Es wird somit ermittelt, ob auf dieser Basis eine Geschäftsbeziehung zustande kommt oder weitere Aktionen initiiert werden können. Aufgrund des Vertrauens in das IAC und die SCCs ist eine Grundlage für weitere geschäftliche Transaktionen gelegt worden.

Abbildung 5: Zusammenwirken der bisher beschriebenen Rollen



Quelle: Plattform Industrie 4.0

3. Lösungsbausteine

Die Lösungsbausteine zeigen eine Auswahl an konkreten Möglichkeiten auf, wie die in Kapitel 2 genannten Anforderungen erfüllt werden können. Dabei wird zunächst die EU-Verordnung „electronic identification and trust services for electronic transactions in the internal market" („eIDAS-VO") (11) als zentrales Trust Framework vorgestellt. Weiterhin werden globale Identitätsattribute aufgelistet, die beispielhaft zur übergreifenden Identifizierung und Authentifizierung genutzt werden können. Zuletzt wird gezeigt, wie eine Verknüpfung von bestehenden Public Key Infrastrukturen hergestellt werden kann.

3.1 eIDAS als Teil des zentralen Trust Framework

Der folgende Abschnitt geht darauf ein, wie in Europa eIDAS eingesetzt werden kann, um die grundsätzlichen Anforderungen aus Kapitel 2 zu erfüllen. Dazu wird eine kurze Einführung in die eIDAS-Verordnung gegeben und dargestellt, wie die Beziehung zu einer Vertrauensinfrastruktur ist.

3.1.1 Gesetzliche Grundlagen

Die eIDAS-Verordnung regelt seit 2014 den Einsatz von Identifikations- und Vertrauensdiensten im europäischen Wirtschaftsraum (EWR). Spezifische Durchführungsakte konkretisieren die eIDAS-Verordnung[6].

Durch eIDAS wird dabei keine Vereinheitlichung von elektronischen Identifizierungssystemen und Lösungen, bzw. von Identifikationsmitteln und -prozessen zur Verwaltung digitaler Identitäten forciert. Vielmehr wird durch eIDAS eine Regelung geschaffen, auf deren Basis eine gegenseitige Anerkennung verschiedener Verfahren innerhalb des EWR übergreifend gewährleistet wird. Dies wird durch eine freiwillige Notifizierung der nationalen eID-Systeme ermöglicht.

Vertrauensdienstegesetz

Die Umsetzung der Anforderungen aus der eIDAS-Verordnung erfolgt in Deutschland nach dem Vertrauensdienstegesetz (VDG)[7]. Das Gesetz regelt die wirksame Durchführung der Vorschriften über Vertrauensdienste in der eIDAS-Verordnung auf nationaler Ebene.

Das VDG ersetzt mit der am 29. Juli 2017 erfolgten Inkraftsetzung das Signaturgesetz aus dem Jahr 1999 und schließt in der eIDAS-Verordnung enthaltene Regelungslücken, wie zum Beispiel:

- Definition von Zuständigkeiten für die Zertifizierung von qualifizierten Signaturerstellungseinheiten und die Verwaltung der Liste von deutschen Vertrauensdiensten
- Stärkere Berücksichtigung von barrierefreien Diensten von Trust Service Providern (TSP) für schwerbehinderte Personen
- Berücksichtigung von datenschutzrechtlichen Problemstellungen bei der Verarbeitung und Speicherung von personenbezogenen Daten
- Definition einer Mindestsumme für die Deckungsvorsorge von qualifizierten TSP im Falle von Haftungsansprüchen
- Bußgeldvorschriften im Falle eines ordnungswidrigen Handelns durch die qualifizierten TSP

Bezüglich der zuletzt genannten Punkte der Deckungsvorsorge und Bußgelder bestehen Unterschiede zwischen den EU-Mitgliedsstaaten, wodurch ungleiche wettbewerbliche Bedingungen für die TSP entstehen können.

Weiterhin aktualisiert das VDG den rechtlichen Rahmen für die Verwendung von qualifizierten elektronischen Signaturen und Siegeln. So wurde beispielsweise die Bundesnetzagentur zur Aufsichtsbehörde für elektronische Signaturen und Siegel ernannt.

Aufbau der eIDAS-Verordnung

Die eIDAS-Verordnung regelt im Wesentlichen in Kapitel II die Mittel zur elektronischen Identifizierung und in Kapitel III die Vertrauensdienste.

6 Durchführungsakte zur Konkretisierung der eIDAS-Verordnung:
- Die Durchführungsverordnung (EU) 2015/806, welche die Form eines visuellen EU-Vertrauenssiegels für qualifizierte Vertrauensdienste spezifiziert,
- der Durchführungsbeschluss (EU) 2015/1505 zu Formaten für Vertrauenslisten, in denen Informationen über Vertrauensdienstanbieter (VDA) und die von ihnen erbrachten Vertrauensdienste von der zuständigen Stelle jedes Mitgliedsstaates bereitgestellt werden,
- der Durchführungsbeschluss (EU) 2015/1506, welcher Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel festlegt, die von öffentlichen Stellen anerkannt werden, und
- der Durchführungsbeschluss (EU) 2016/650, welcher Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten festlegt.

7 https://www.gesetze-im-internet.de/vdg/BJNR274510017.html

Grundsätzlich wird für elektronische Identifizierungsmittel im Rahmen eines elektronischen Identifizierungssystems das Maß an Vertrauen an eine behauptete Identität einer Person durch eIDAS Kapitel II wie folgt unterschieden:

„Niedrig“: Begrenztes Maß an Vertrauen in die beanspruchte oder behauptete Identität

„Substanziell“: Substanzielles Maß an Vertrauen in die beanspruchte oder behauptete Identität

„Hoch“: Höheres Maß an Vertrauen in die beanspruchte oder behauptete Identität

Kapitel III beschreibt elektronische Signaturen, Siegel und TSP. Ein qualifiziertes elektronisches Siegel bzw. eine Signatur bestätigt stets die Herkunft und die Unversehrtheit eines Dokuments oder Datensatzes. Die vollständige Verwaltung, von der Beantragung und Ausstellung über die Verwendung bis hin zum Widerruf beziehungsweise Ablauf, ist so in eIDAS geregelt, dass im Vertrauensraum eine gegenseitige und verlässliche Anerkennung für qualifizierte elektronische Signaturen und Siegel gewährleistet wird.

Die elektronische Signatur wird von natürlichen Personen verwendet und ist einer Willenserklärung gleichgestellt. Elektronische Siegel beziehen sich auf juristische Personen, wie beispielsweise Organisationen. Beide bestätigen die Unversehrtheit und Herkunft von Dokumenten.

Es wird dabei zwischen den folgenden Sicherheitsniveaus unterschieden:

Elektronische Signaturen und Siegel: Elektronische Signaturen und Siegel gemäß eIDAS Artikel 3 Absatz 10 und Absatz 25 sind „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden“ und zur Authentifizierung dienen. Diese zeichnen sich durch eine niedrige Verbindlichkeit aus und werden häufig für unternehmensinterne Abstimmungsprozesse, wie zum Beispiel Bescheinigungen, Protokolle oder Genehmigungen, verwendet. Eine zusätzliche Evidenz entsteht hierbei durch den Transportweg. Die praktische Anwendung einer einfachen elektronischen Signatur erfolgt beispielsweise anhand eines Touchscreens, über den sich eine Unterschrift an entsprechende Informationen anhängen lässt.

Fortgeschrittene elektronische Signaturen und Siegel: Fortgeschrittene elektronische Signaturen und Siegel stellen Software-Zertifikate dar, die eine Überprüfung der Integrität von Informationen ermöglichen. Gemäß eIDAS Artikel 26 und Artikel 36 liegen fortgeschrittene elektronische Signaturen beziehungsweise Siegel vor, wenn folgende Anforderungen erfüllt werden:

- Sie ist eindeutig dem Unterzeichner beziehungsweise Siegelersteller zugeordnet.
- Sie ermöglicht die Identifizierung des Unterzeichners beziehungsweise Siegelerstellers.
- Sie wird unter Verwendung elektronischer Signaturerstellungsdaten beziehungsweise Siegelerstellungsdaten erstellt, die der Unterzeichner beziehungsweise Siegelersteller mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.
- Sie ist so mit den Daten, auf die sie sich bezieht, verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Die praktische Anwendung kann beispielsweise über eine asymmetrische Verschlüsselung unter Verwendung von einer zentralen Public Key Infrastruktur (PKI) oder einem dezentralen Web of Trust erfolgen. Wird die fortgeschrittene elektronische Signatur im Rahmen einer asymmetrischen Verschlüsselung implementiert, spricht man auch von einer „digitalen Signatur“.

Die Nutzung von nicht-qualifizierten elektronischen Siegeln und Signaturen ist in Deutschland gemäß BGB § 126 zulässig, soweit keine abweichende gesetzliche Regelung besteht. Es ist hierbei zu beachten, dass rechtlich fortgeschrittene elektronische Siegel und Signaturen als Objekte des „Augenscheins“ behandelt werden und somit nur eine eingeschränkte Verlässlichkeit besteht. Die Korrektheit der Angaben muss stets durch diejenige Partei nachgewiesen werden, die sich auf die Identität der fortgeschrittenen elektronischen Signatur beziehungsweise Siegel bezieht.

Qualifizierte elektronische Signaturen und Siegel: Qualifizierte elektronische Signaturen und Siegel unterliegen strengeren Anforderungen als fortgeschrittene elektronische Signaturen und Siegel. Gemäß eIDAS Artikel 3 Absatz 12 liegt eine qualifizierte elektronische Signatur/Siegel vor, wenn es sich um eine fortgeschrittene elektronische Signatur beziehungsweise Siegel handelt, die

- von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und
- auf einem qualifizierten Zertifikat für elektronische Signaturen beziehungsweise Siegel beruht.

Gegenüber den fortgeschrittenen elektronischen Signaturen und Siegeln benötigen die Teilnehmer eine zertifikatsbasierte Identität, die von einem akkreditierten EU-Vertrauensdienst erzeugt und auf einer qualifizierten Signaturerstellungseinheit, zum Beispiel Chip-Karten oder Hardware Security Module, gespeichert wird, wobei letztere auch von einem qualifizierten Vertrauensdienst betrieben werden müssen.

In Kombination mit einer Passworteingabe kann der Teilnehmer die qualifizierte elektronische Signatur beziehungsweise das Siegel erstellen und an die entsprechenden Informationen anhängen.

Signatur- bzw. Siegelerstellungseinheiten können sich auch auf einem Server eines Vertrauensdienstanbieters befinden. Dadurch lassen sich nach vorheriger Authentifizierung elektronische Signaturen und Siegel mobil, beispielsweise durch ein Smartphone, generieren. Fernsignaturen ermöglichen Flexibilität und eigenen sich für Remote-Anwendungen. So können sie beispielsweise durch eine API einfach in bestehende Workflows oder Portale eingebunden werden.

Durch eIDAS Kapitel III werden Vertrauensdienste in folgenden Bereichen definiert:

1. Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln

2. Zustellung elektronischer Einschreiben

3. Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung

4. Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten

Elektronische Zeitstempel

Gemäß eIDAS Präambel Absatz 33 sind elektronische Zeitstempel „Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren."

Elektronische Zeitstempel sind demnach ein geeignetes Verfahren, um zu bestätigen, dass die vorliegenden Informationen zu einem bestimmten Zeitpunkt existiert haben beziehungsweise nach dem Datum des Zeitstempels nicht verändert worden sind. Entsprechende Anwendungsgebiete ergeben sich beispielsweise bei personenbezogenen Informationen wie Patientenakten, Personenstammdaten oder zahlungsrelevanten Belegen bei Sozialversicherungsträgern, deren zeitliche Zuordnung von hoher Relevanz ist.

Die praktische Umsetzung erfolgt analog zu den elektronischen Signaturen und Siegeln über TSP. Beispielsweise kann für ein Dokument zu einem bestimmten Zeitpunkt ein Hash-Wert erstellt werden, der vom TSP im Rahmen eines Zeitstempel-Zertifikats signiert und mit dem Dokument verbunden wird. Eine nachträgliche Änderung des Dokuments würde zu einem veränderten Hash-Wert führen, was durch einen Abgleich mit dem Hash-Wert des Zeitstempel-Zertifikats auffallen würde.

Wie auch bei den elektronischen Signaturen und Siegeln definiert eIDAS Anforderungen, damit ein qualifizierter elektronischer Zeitstempel vorliegt. Gemäß eIDAS Artikel 42 Absatz 1 müssen demnach elektronische Zeitstempel

- Datum und Zeit so mit Daten verknüpfen, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist,

- auf einer korrekten Zeitquelle beruhen, die mit der koordinierten Weltzeit verknüpft ist, und

- mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel eines qualifizierten Vertrauensdienstanbieters gesiegelt werden oder ein gleichwertiges Verfahren verwenden.

Der zentrale Vorteil von qualifizierten elektronischen Zeitstempeln besteht in ihrer gegenseitigen Anerkennung innerhalb aller Mitgliedsstaaten der Europäischen Union.

Weiterhin bieten qualifizierte elektronische Zeitstempel gemäß eIDAS Artikel 41 Absatz 2 den Vorteil, dass im Rahmen der Rechtswirkung die „Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten" gilt.

Einem elektronischen Zeitstempel darf jedoch gemäß eIDAS Artikel 41 Absatz 1 die „Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt."

Anforderungen an TSP

Durch Artikel 19 werden folgende Sicherheitsanforderungen an qualifizierte und nichtqualifizierte TSP aufgelistet:

- Es müssen „geeignete technische und organisatorische Maßnahmen" ergriffen werden, um die Sicherheitsrisiken, welche im Zusammenhang mit den jeweiligen Vertrauensdiensten stehen, zu minimieren. Die Maßnahmen müssen dem Stand der Technik entsprechen. Außerdem müssen geeignete Maßnahmen getroffen werden, um potenzielle „Auswirkungen von Sicherheitsverletzungen zu vermeiden bzw. so gering wie möglich zu halten und die Beteiligten über die nachteiligen Folgen solcher Vorfälle zu informieren".

- Weiterhin müssen TSP „unverzüglich, in jedem Fall aber innerhalb von 24h nach Kenntnisnahme von dem betreffenden Vorfall, jede Sicherheitsverletzung oder jeden Integritätsverlust, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt“, melden.

Für TSP, die IACs ausstellen, ist der Stand der Technik hinsichtlich der Policy- und Sicherheitsanforderungen in der „ETSI EN 319 411“ (12) beschrieben. Dabei sind die ETSI-Anforderungen nicht verpflichtend. Auch ISO-Standards oder die Technische Richtlinie „BSI-TR 03145“ (13) des BSI können herangezogen werden, um die Anforderungen der eIDAS-Verordnung zu erfüllen.

Qualifizierte TSP werden zudem alle 24 Monate von einer Konformitätsbewertungsstelle geprüft (Artikel 20). Darüber hinaus können die jeweiligen Aufsichtsstellen der Mitgliedsstaaten jederzeit

- eine Überprüfung vornehmen oder durch die Konformitätsbewertungsstellen vornehmen lassen
- bei Nichteinhaltung der Anforderungen eine Frist zur Ausbesserung stellen
- bei andauernder Nichteinhaltung begründet den Qualifikationsstatus entziehen sowie eine Aktualisierung der Vertrauenslisten (engl. Trusted Lists) bewirken

Vertrauenslisten

Der wesentliche Charme der eIDAS-Verordnung liegt in der Schaffung von Vertrauenslisten (Artikel 22), gegen die qualifizierte Signaturzertifikate, qualifizierte Siegelzertifikate, qualifizierte Zeitstempel und qualifizierte Website-Zertifikate automatisch und kostenlos kryptographisch geprüft werden können.

Die „National Trust List“[8] stellt eine öffentlich zugängliche Auflistung von nationalen TSP der Bundesrepublik Deutschland dar, die gemäß der eIDAS-Verordnung eine Zulassung zur Erstellung von qualifizierten Signaturzertifikaten, qualifizierten Siegelzertifikaten, qualifizierten Zeitstempeln und qualifizierten Website-Zertifikaten besitzen[9]. Weiterhin besitzen alle anderen Mitgliedsstaaten der Europäischen Union eine eigene National Trust List mit entsprechenden zugelassenen TSP. Eine Übersicht aller internationalen Trust Lists der Europäischen Union ist der List of Trusted Lists oder EU Trusted List (im Folgenden „LOTL“ genannt) zu entnehmen.

Für jeden Mitgliedsstaat beaufsichtigt eine individuelle Organisation die dort ansässigen TSP. Beispielsweise stellt die Bundesnetzagentur die deutsche Aufsichtsstelle für die National Trust List dar. Dies impliziert jedoch nicht, dass der nationale TSP nur in dem ihm zugeordneten Mitgliedsstaat in Anspruch genommen werden darf. Wird ein TSP in einer National Trust List und demzufolge auch der LOTL aufgenommen, sind die entsprechenden Vertrauensdienste in allen Mitgliedsstaaten der Europäischen Union anzuerkennen.[10] Die National Trust List beziehungsweise LOTL unterstützt somit eine im EWR länderübergreifende gegenseitige Anerkennung durch qualifizierte elektronische Signaturen, Siegel und Zeitstempel.

Der Ort der übergeordneten Vertrauensliste (LOTL), die auf die nationalen Trusted Lists verweist, wird im Europäischen Gesetzblatt veröffentlicht und wird sowohl in einer menschen- als auch maschinenlesbaren Form bereitgestellt. Durch die jeweiligen nationalen Aufsichtsbehörden werden die Vertrauensanker (Root CAs) der Vertrauensdienste auf die Listen aufgenommen, die eine entsprechende nachgewiesene und überprüfte Qualität aufweisen und somit ein hohes Vertrauen genießen können.

Durch dieses Verfahren einer Produktzulassung wird gewährleistet, dass ein einheitliches Niveau der Vertrauensdienste in Europa zur Verfügung steht. Im EWR stehen heute ca. 172 TSP in 29 Ländern mit unterschiedlichen Vertrauensdiensten zur Verfügung. Aktuell existieren rund 200 europäische TSP zur Erstellung von qualifizierten Zertifikaten für elektronische Signaturen sowie knapp 100 TSP zur Erstellung von qualifizierten elektronischen Zeitstempeln.[11]

3.1.2 Anwendung in einer Vertrauensinfrastruktur für I4.0

Mit eIDAS und den TSP ist in Europa bereits die Grundlage für eine einheitliche grenzübergreifende Identitätsinfrastruktur gegeben.

TSP erfüllen die für die IACP formulierten Anforderungen. Es handelt sich um eine dezentrale Variante der IACP. Dabei erfüllen die TSP für den Bereich der qualifizierten

8 Für eine Auflistung der deutschen TSP siehe https://webgate.ec.europa.eu/tl-browser/#/tl/DE
9 Viele TSP der National Trust Lists bieten qualifizierte elektronische Signaturen, Siegel und Zeitstempel nicht gleichzeitig an, sondern spezialisieren sich auf eine oder mehrere Vertrauensdienste.
10 Mitgliedsstaaten können in die eigene National Trust List theoretisch auch Vertrauensdienste aufnehmen, die nicht den Vorgaben von qualifizierten Vertrauensdiensten gemäß eIDAS entsprechen. Diese müssen jedoch entsprechend gekennzeichnet sein und unterstützen keine automatische internationale Anerkennung.
11 https://blog.eid.as/de/tag/vertrauensdiensteanbieter

Siegel und Signaturen alle ein gemeinsames Sicherheitsniveau. Es wird somit ein gemeinsamer Vertrauensraum aufgespannt, der bereits eine rechtliche Gültigkeit bietet.

Gleichzeitig bietet eIDAS mit den drei unterschiedlichen Sicherheitsniveaus (bei der Identifizierung und den Signaturen/Siegeln) die Möglichkeit, auf unterschiedliche Anforderungsbereiche angewendet zu werden.

Durch die „ETSI EN 319 412“ (14) werden zudem, basierend auf dem Standard „ISO/IEC 9594-8“ (4), Empfehlungen für Zertifikatsprofile gegeben, die unter anderem technische Spezifikationen für maschinenverarbeitbare und interoperable Formate für qualifizierte und nichtqualifizierte Zertifikate bereitstellen.

Für Industrie 4.0 lassen sich folgende Vorteile herausarbeiten. Bei der Verwendung von eIDAS-Mitteln sind:

1. die handelnden juristischen Personen automatisierbar und revisionssicher erkennbar,

2. keine weiteren Onboarding-Kosten vorhanden, da die verlässliche Identifikation automatisch durch das Zertifikat möglich ist,

3. die Identifikation der juristischen Person (qualifizierte Siegel) – revisionssicher – und GDPR-konforme Absicherung der Kommunikationsschicht durch qualifizierte Website-Zertifikate möglich sowie

4. eine kostenlose, automatische Validierbarkeit (der Verbindung und der Herkunft der Daten) durch die Verwendung der EU Trusted List möglich, daher sind keine separaten kostenintensiven Policy-Erarbeitungen notwendig.

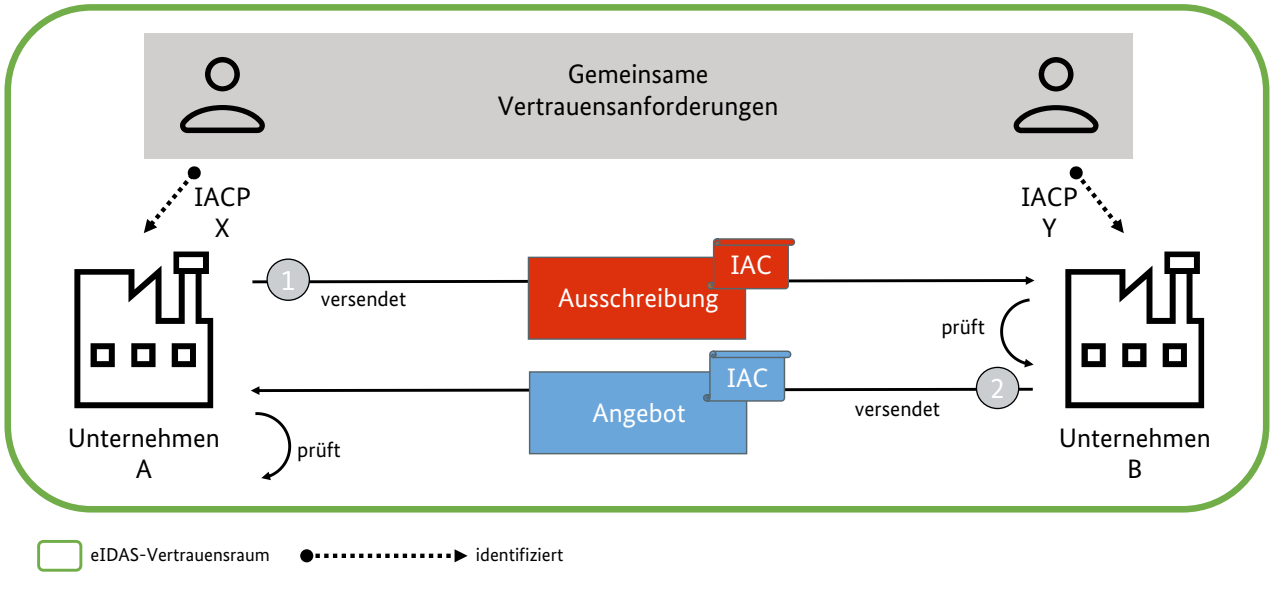
Beispiel für Industrie 4.0

Ziel der Industrie 4.0 sind unter anderem elektronische und automatisierte Vertragsverhandlungen, wie bereits in Kap. 1.4 beschrieben wurde. Dafür bietet eIDAS eine gute Grundlage. Im Folgenden soll dies, wie auch in Abbildung 6 dargestellt wird, anhand eines Beispiels für einen Ausschreibungs- und Angebotsprozess erläutert werden.

Unternehmen A und B beantragen bei einem TSP ein qualifiziertes Siegel-Zertifikat, bevor sie die Geschäftsbeziehung für den Ausschreibungsprozess miteinander eingehen. Der TSP übernimmt die in Kapitel 2.1 beschriebene Rolle des IACP, wobei es sich bei dem Siegel-Zertifikat, welches nach Beantragung und Prüfung ausgestellt wird, um ein IAC handelt. Dabei gelten für die Beantragung der IACs die in Kapitel 3.1.1 beschriebenen Anforderungen.

Unternehmen A verwendet das Siegel-Zertifikat, um eine Ausschreibung elektronisch zu unterschreiben, bzw. zu „siegeln“. Unternehmen B prüft die Ausschreibung. Durch die Verifizierung wird sichergestellt, dass die Herkunftsinformationen sowohl in der Ausschreibung als auch im Siegel stehen. Damit ist sichergestellt, dass die Ausschreibung unverändert ist und auch von Unternehmen A veröffentlicht wurde.

Abbildung 6: Beispiel für einen Ausschreibungs- und Angebotsprozess



Quelle: Plattform Industrie 4.0

Unternehmen B erstellt daraufhin ein Angebot, siegelt dieses ebenfalls mit seinem Siegel-Zertifikat und sendet es an Unternehmen A. Unternehmen A kann somit das Angebot prüfen und sich von der Korrektheit und Herkunft überzeugen. Das Angebot kann darüber hinaus die in Kapitel 2.2 beschriebenen SCCs enthalten, um die Qualität eines Produktes, eines Dienstes oder eines Fertigungsprozesses nachzuweisen.

Bei der Prüfung der IAC greifen Unternehmen A und B auf die durch eIDAS bereitgestellten Mittel und Wege zurück.

- Es kann mittels der Vertrauensliste (NTL) überprüft werden, ob das Siegel-Zertifikat von einem TSP ausgegeben wurde (in diesem Sinne ein IACP aus dem gemeinsamen Vertrauensraum beider Unternehmen).
- Durch das IAC kann auf den Namen bzw. die Identität des unterzeichnenden Unternehmens geschlossen werden.
- Durch die Unterschrift wird eine potenzielle Manipulation des Dokuments erkennbar. Zudem ist es nicht mehr möglich, die Herkunft abzustreiten.

Der Vorteil für Unternehmen A und B liegt darin, dass sie durch den gemeinsamen Vertrauensraum davon ausgehen können, dass eine gegenseitige sichere Identifizierung und Authentifizierung erfolgt ist, auch wenn sie ihre IACs bei unterschiedlichen IACP beantragt haben. Da das Format des Vertrags nicht festgelegt ist, können dort weitere Nachweise oder Ähnliches hinterlegt werden.

3.2 Globale Identitätsattribute

Identitätsattribute spielen, wie in den Anforderungen bereits beschrieben, eine zentrale Rolle für Sichere Digitale Identitäten. Durch Identitätsattribute wird, wie auch in dem „Projektbericht Sichere Digitale Identitäten (SDI)“ (15) deutlich wird, eine Zurechenbarkeit, Verfolgbarkeit und Zuweisung bestimmter Eigenschaften möglich. Daher muss der IACP, wie in Kapitel 3.1.1 bereits beschrieben, eine eindeutige Identifizierung und Authentifizierung der Entität durchführen. Dafür muss der IACP Wege und Mittel finden, um zu überprüfen, dass die Bezeichnung des Antragstellers bzw. der Identifikator global eindeutig ist. Hierbei kann er sich mehrerer Möglichkeiten bedienen. Im Folgenden werden beispielhaft globale Lösungen beschrieben, die nicht den Anspruch auf Vollständigkeit erheben.

3.2.1 Firmenidentitäten durch Handelsregistereinträge

Als öffentliches Verzeichnis dokumentiert das Handelsregister Einträge über die registrierten Kaufleute im Bereich eines zuständigen Registergerichts. Es kann von jedem eingesehen werden und informiert über die wesentlichen wirtschaftlichen Bedingungen von Händlern und Unternehmen.

Dazu gehören beispielsweise Jahresabschlüsse und Bilanzen. Heute wird das Handelsregister nur noch elektronisch verwaltet, wobei die Registrierung und Eintragung ebenso ausschließlich auf diesem Weg erfolgt. Darüber hinaus wird eine notarielle Beglaubigung verlangt.

Im Handelsregister eingetragene Gewerbe werden in zwei Gruppen eingeteilt:

- Abteilung A (HRA): Registrierte Händler, Partnerschaften und rechtliche (wirtschaftliche) Vereinigungen
- Abteilung B (HRB): Unternehmen

Die folgenden Daten sind online, aber nicht kostenfrei unter der Handelsregisternummer sichtbar:

- Vorstand, Namen
- Aufsichtsrat, Namen
- Hauptsitz
- Steueridentifikationsnummer
- Anschrift
- Telefonnummer
- E-Mail

Mit der Handelsregisternummer können Geschäftspartner eindeutig identifiziert werden. Der Vorteil dieses Ansatzes ist das Vorhandensein einer zentralen und neutralen Instanz. Der Nachteil besteht in den geringen Daten zu Personen, die entsprechende Rollen und Rechte im Unternehmen besitzen. Auch mögliche Vertreterregelungen sind aus dem Handelsregistereintrag nicht einsehbar. Alle Daten beziehen sich nur auf Personen, nicht aber auf Maschinen, Produkte bzw. Objekte und Software. Darüber hinaus haben, wie in der „BSI-TR 01201“ (16) dargestellt, manche Unternehmen keinen Handelsregistereintrag. Daher kann der Identifikator nicht als allgemeingültige Lösung angenommen werden, sondern stellt eine Möglichkeit zur Identifizierung von Unternehmen dar.

Andere Wirtschaftsregionen, wie zum Beispiel China, Japan und USA, verwenden vergleichbare Unternehmensregistrierungssysteme.

- China: https://www.china-iprhelpdesk.eu/sites/all/docs/publications/How_to_search_for_company_information.pdf
- Japan: https://www.japanregistry.com
- USA: https://www.sec.gov/edgar/searchedgar/companysearch.html

3.2.2 International eindeutige Identifizierung

Es gibt privatwirtschaftlich organisierte, branchenübergreifend eindeutige Identifikationsschlüssel für nahezu alle Objekte, die im Business-to-Business-, im Business-to-Consumer- und im Business-to-Government-Geschäft relevant sind, beispielsweise für Produkte, Standorte, Unternehmen, Servicebeziehungen, Vermögensgegenstände oder Transaktionen.[12]

Weit verbreitet ist die Global Location Number (GLN), die von GS1[13] vergeben wird, womit Standorte, sogenannte Lokationen, beispielsweise Filialen, Lager, Liegeplätze etc., und juristische Einheiten sowie Funktionseinheiten, zum Beispiel Unternehmen, Abteilungen, auf Basis der „ISO/IEC 15459“ (17) und „ISO/IEC 6523“ (18) identifiziert werden können. Bei jeder Form der Kommunikation, sei es B2B oder B2C, Machine-to-Machine oder mit menschlicher Beteiligung, analog oder digital, ist es essenziell zu wissen, wer mit wem spricht und über welche Objekte. Eine eindeutige Lokationsidentifikation, zum Beispiel durch eine GLN, stellt eine Grundvoraussetzung für einen effizienten zwischenbetrieblichen elektronischen Informationsaustausch dar. Sie wird benötigt, um Güter, papiergebundene Informationen oder elektronische Daten an den gewünschten Ort beziehungsweise die richtige Adresse zu liefern. Mit Hilfe einer GLN können physische Adressen von Unternehmen, Tochterunternehmen, Niederlassungen und sogar Regionalbüros eines Unternehmens identifiziert werden, genauso wie funktionsorientierte Einheiten eines Unternehmens wie Lager, Abteilungen, Produktionsstraßen, Lieferpunkte sowie Netzwerk- und sonstige Kommunikationsknoten. Dabei wird die Nummer in allen Anwendungen als Zugriffsschlüssel für die im Computersystem hinter diesem Code abgelegten Stammdaten verwendet. Die GLN wird branchenübergreifend und global genutzt und ersetzt so an den Kommunikationsschnittstellen von Industrie, Handel und Dienstleistungssektor proprietäre und bilateral abzustimmende Kunden- und Lieferantennummern. Sie hilft den Verwaltungsaufwand zu verringern, den Informationsfluss zu vereinfachen und schafft zugleich die nötigen Voraussetzungen für ein effizientes Versenden, Sortieren und Verfolgen von Gütern und das Rückführen von Mehrweg-Transportverpackungen.

Zusätzlich ermöglicht die GLN über den Service GEPIR (Global GS1 Electronic Party Information Registry) die Suche nach Unternehmen, die die globalen GS1-Standards nutzen. Angezeigt werden die Unternehmensadresse sowie die Kontaktdaten zu einem Ansprechpartner, den das Unternehmen dafür benannt hat. Für häufige Anfragen bietet GEPIR die Möglichkeit, über eine automatisierte Abfrage mittels XML-basierten Webservice zuzugreifen.

Legal Entity Identifier (LEI)

Durch die Global Legal Entity Identifier Foundation (GLEIF) mit Sitz in der Schweiz wurde ein internationaler Identifikator, der so genannte „Legal Entity Identifier“ (LEI), auf Basis der ISO 17442 „Financial Services – Legal Entity Identifier (LEI)“ (19) veröffentlicht. Dieser regelt die Vergabe und Verwaltung von global eindeutigen LEI und zugehöriger Informationen für alle Rechtsträger im europäischen Finanzmarkt.

Geschäftspartner können zunächst als „Legal Entities“ (Juristische Personen) angenommen werden. Zur korrekten Identifikation müssen mindestens folgende Informationen eindeutig bestimmt werden:

- Vollständiger Name des Rechtsträgers, der innerhalb von offiziellen Registern verwendet wird
- Registrierte Anschrift des Rechtsträgers

Daneben können weitere Informationen für I4.0-Geschäftsprozesse benötigt werden, welche von der GLEIF ergänzend verwaltet und bereitgestellt werden. Hierbei sind insbesondere Rechtsanforderungen zu beachten, die sich aus dem Sitz des Geschäftspartners, seiner Rechtsform oder auch der Eigentümerstruktur ergeben.

Eine LEI ist innerhalb der EU für Derivatgeschäfte, gemäß „European Market Infrastructure Regulation, Artikel 9 Absatz 1“ (20), verbindlich zu verwenden. Für alle weiteren Unternehmen innerhalb der EU ist die Verwendung einer LEI optional. Für ein Siegel gemäß eIDAS-Verordnung kann die LEI als Identifier verwendet werden.

Die Vergabe und Verwaltung einer LEI geschieht durch sogenannte LEI-Vergabestellen (auch „Local Operating Units“ (LOU)). Die GLEIF bestimmt Vorgaben, die eine

12 Vgl. https://de.wikipedia.org/wiki/GS1
13 https://www.gs1-germany.de

LEI-Vergabestelle beachten muss. Das Vertrauen in die LEI wird somit durch die Vorgaben der GLEIF an die LEI-Vergabestellen unterstützt. Zu jeder LEI müssen sogenannte Level 1-Daten verpflichtend hinterlegt werden, zu diesen gehören:

- Der offizielle Name des Rechtsträgers, wie in offiziellen Registern verzeichnet
- Die registrierte Anschrift des Rechtsträgers
- Das Land der Gründung
- Die Codes für die Darstellung der Ländernamen und ihrer Unterbereiche
- Das Datum der ersten LEI-Zuweisung, das Datum der letzten Aktualisierung der LEI-Daten und, sofern zutreffend, der Ablauftermin

Die optionalen Level 2-Daten einer LEI erfassen solche Informationen, die Auskunft über die buchhalterisch direkt übergeordnete Muttergesellschaft und die ultimativ übergeordnete Muttergesellschaft geben.

Ergänzend können weitere Informationen in Absprache mit der zuständigen LEI-Vergabestelle vergeben werden.

Durch die GLEIF wird ebenso die Suche nach registrierten LEI beziehungsweise den zugeordneten Level 1- und Level 2-Daten ermöglicht. Die Suche wird unter anderem durch eine standardisierte Programmierschnittstelle (Application Programming Interface) unterstützt. Informationen werden in einem standardisierten Datenformat, dem sogenannten LEI-Common Data File (CDF) Format, bereitgestellt. Dies würde auch die automatisierte Verwendung von LEI-Daten im Umfeld von Industrie 4.0 ermöglichen.

3.2.3 Attribute für die Erstellung eines elektronischen Siegels im Rahmen von eIDAS

Für die Erstellung eines elektronischen Siegel-Zertifikats im Rahmen von eIDAS muss ein entsprechender Antrag bei einem TSP gestellt werden. Es gelten die jeweiligen Vorgaben des Zertifizierungskonzepts des TSP. Es können zusätzlich branchenspezifische Attribute festgelegt werden, die innerhalb einer Branche verpflichtend sind.

Grundsätzlich werden mindestens folgende Informationen benötigt:

1. Bezeichnung des Unternehmens
2. Rechtsform
3. Registernummer (wenn vorhanden)
4. Geschäftsanschrift gemäß Handelsregister beziehungsweise Hauptniederlassung
5. Namen der Mitglieder des Vertretungsorgans oder Namen der gesetzlichen Vertreter – sofern ein Vertretungsorgan oder der gesetzliche Vertreter eine juristische Person ist, jeweils die zugehörigen Informationen zu 1. bis 4.
6. Kontaktdaten zur Kontaktaufnahme durch den TSP

Die Antragsstellung muss durch einen Vertreter des Unternehmens erfolgen, der es gesetzlich vertreten darf oder für den eine entsprechende Vollmacht durch einen gesetzlichen Vertreter ausgestellt wurde.

Die Ausstellung eines elektronischen Siegel-Zertifikats umfasst mindestens die Prüfung

- der Angaben zur Bezeichnung und Adresse des Unternehmens,
- der Autorisierung des verantwortlichen Ansprechpartners des Unternehmens sowie
- die Prüfung einer Vollmacht, wenn die Antragsstellung im Auftrag erfolgt.

Die Ausstellung darf nur nach vollständiger und korrekter Prüfung durch einen TSP gemäß den Vorgaben der eIDAS-Verordnung erfolgen. In Abhängigkeit von den Geschäftsbedingungen des TSP können weitere Prüfungen erfolgen.

Ist die Antragsstellung erfolgreich, wird durch den TSP ein elektronisches X.509v3-Zertifikat auf Basis des Standards „ISO/IEC 9594-8“ (4) erstellt. Das Zertifikat muss durch den TSP unter Verwendung eines Hardware Security Moduls (HSM) signiert werden. Durch die Signatur des TSP wird die Authentizität des Zertifikats gewährleistet.

Die Informationen zu ausgestellten Zertifikaten müssen durch den TSP veröffentlicht werden. Die Gültigkeit eines Zertifikats kann in der Regel mittels des Online Certificate Status Protocol (OCSP) überprüft werden. Neben der Prüfung auf Widerruf wird insbesondere auch die Prüfung auf Korrektheit und Gültigkeit durch die TSP geboten.

X.509v3-Zertifikate

Der Aufbau der in X.509v3-Zertifikaten enthaltenen Informationen beziehungsweise Attribute stellt sich wie folgt dar:[14]

- Version
- Seriennummer
- Algorithmus
- Ausstellende Instanz (Angabe von Land, Bundesland, Ort, Organisation, Organisationseinheit, Name)
- Gültigkeitsdauer (Angabe von Start und Ende der Geltungsdauer)
- Name des Teilnehmers beziehungsweise Zertifikatinhabers
- Öffentlicher Schlüssel des Teilnehmers (inklusive der Angabe des zugehörigen kryptographischen Algorithmus)
- Eindeutige Identifikationsnummer der ausstellenden Instanz
- Eindeutige Identifikationsnummer des Teilnehmers beziehungsweise Zertifikatinhabers
- Erweiterungen (beispielsweise: Geschäftsbedingungen der Zertifizierungsstelle, Einschränkungen bezüglich des transitiven Vertrauens, Angabe der maximalen Länge der Zertifikatskette)
- Signatur der Zertifizierungsstelle (inklusive der Angabe des zugehörigen kryptographischen Algorithmus)

3.2.4 Übersicht der verschiedenen Lösungsansätze

In Tabelle 1 werden die verschiedenen Lösungsansätze, um die in Kapitel 2 genannten Anforderungen zu erfüllen, nochmals gegenübergestellt.

3.3 Verknüpfung von bestehenden Public Key Infrastrukturen

Eine PKI ermöglicht den Teilnehmern den gegenseitigen Austausch von öffentlichen Schlüsseln und setzt dafür definierte Prozesse und Policies um. Die PKI schafft so eine Sicherheitsbasis, die verhindert, dass sich unberechtigte Dritte an einer Kommunikation beteiligen, Informationen einsehen oder manipulieren.

Viele Hochtechnologiefirmen, z. B. in der Elektro- und Automobilbranche, nutzen weltweit PKIs zur Absicherung ihrer IT-Systeme, insbesondere in der Office-IT und zum Schutz vertraulich eingestufter Daten. Damit verbunden ist die Ausstellung, Verteilung und Prüfung von digitalen Zertifikaten. Die Hauptanwendung liegt heute in der Authentifizierung und der Autorisierung für den sicheren logischen Zugang (engl. logical access) zu PCs, IT-Systemen, Servern und Datenbanken sowie Steuerungssystemen, auch aus der Ferne (engl. remote). Häufig verwenden Mitarbeiter dieser Firmen elektronische Mitarbeiterausweise (Smartcards oder anderer Formfaktor) zur Speicherung und Verwendung der privaten Schlüssel. In Verbindung mit Passwörtern wird eine 2-Faktor-Authentisierung des Nutzers ermöglicht (Faktoren: Besitz und Wissen). Neben dem sicheren Zugang zur IT gibt es auch viele weitere Anwendungen, wie die elektronische Signierung und Verschlüsselung von E-Mails, aber auch die Signierung von Server-basierten PDF-Dokumenten oder elektronische Workflows, z. B. für Genehmigungsvorgänge, die vollständig auf dem digitalen Weg und damit papierlos erfolgen. Weitere Anwendungen können zum Beispiel Daten- und Festplattenverschlüsselungen in der Firma sein.

Tabelle 1: Übersicht über verschiedene Lösungsansätze

Verfahren/ Konzept	Wann wurde es eingeführt?	Haupttreiber/ Initiativgeber	Anwendungsbereich	Ursprüngliche Wirtschaftszone
Handelsregister	1820	(Finanz-)Behörde	Firma, Inhaber, Sitz	Deutschland
GS1	1973	Handel/Retail	Branchenübergreifend (bspw. Gesundheitswesen, Eisenbahnwesen, Automobilindustrie, Maschinen- und Anlagenbau, Logistik)	weltweit
LEI	2012	Finanzdienstleistungssektor	Finanztransaktionen, Wertpapierkauf etc. zwischen Finanzdienstleistern	weltweit
eIDAS	2014	(Digital-)Behörde	Elektronische Identität, elektronische Zustellung, elektronische Signaturen etc.	Europäischer Wirtschaftsraum

14 Bezieht sich auf X.509-Zertifikate der Version 3

Nicht selten werden diese Mitarbeiterausweise auch für den Zutritt (engl. physical access) zu Firmengeländen, Gebäuden und Räumen genutzt. Weitere Funktionen können die Zeiterfassung und das bargeldlose Bezahlen in Kantinen und an Getränkeautomaten sein.

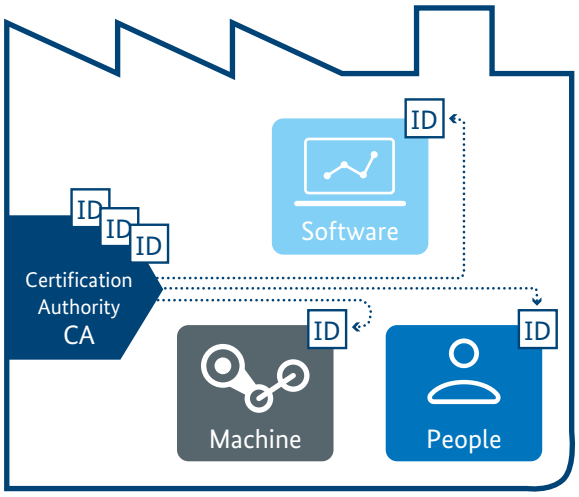
Übertragung von PKI-Architekturen in die Produktionswelt

Die Funktionen von PKI-Architekturen können auch in Produktionsumgebungen zu einem Gewinn an Sicherheit beitragen. Bei der Übertragung von PKI-Architekturen der „Office-Welt", wie sie heute bei einigen Firmen angewendet werden, in die „Produktionswelt" (engl. production oder Operational Technology (OT)) ergeben sich neue Fragen bezüglich der Umsetzung. Dabei ergeben sich auch Ansatzpunkte für zukünftige Anwendungen, wie in Kapitel 4.2 skizziert wird.

Innerhalb einer Firma oder Firmengruppe können Sub-CAs durch eine zentrale Firmen-Root-CA oder einen Dienstleister verwaltet werden. Andere Konfigurationen werden in der Praxis auch beobachtet. Dies ermöglicht eine Unterstützung von IT- und OT-PKI-Systemen mit unterschiedlichen Anwendungsanforderungen. Durch OT-PKI-Systeme können Sichere Digitale Identitäten an Personen, vernetzte Maschinen und eingesetzte Software ausgegeben und widerrufen werden, die auf die Anforderungen in OT-Umgebungen zugeschnitten sind. Abbildung 7 zeigt die Ausgabe von Identitäts-Zertifikaten an die drei genannten Anwendergruppen.

Fragen ergeben sich auch in Bezug darauf, wenn in einem kurzen Zeitfenster neue Identitäten hinzugefügt oder ältere Identitäten widerrufen werden. In der Industrie 4.0 müssen dynamische Änderungen, wie es bei solchen Beispielen der Fall wäre, den drei Anwendergruppen in Echtzeit mitgeteilt werden. Die Änderungen dürfen den Produktionsablauf nicht stören und müssen in zeitlicher Folge erfasst und gespeichert werden. Weitere technische Fragestellungen können sich auch aus der Verwendung von Zertifikaten für Produkte ergeben. So fordert bspw. die IEEE 802.1AR (Secure Device Identity) (21) die Verwendung von nicht ablaufenden Zertifikaten (realisiert durch einen Gültigkeitszeitraum bis zum Jahr 9999), was nicht mit den üblicherweise verwendeten CA-Policies kompatibel ist.

Abbildung 7: Smarte Produktion, basierend auf elektronischen Identitäten für Maschinen, Personen und SW



Quelle: Plattform Industrie 4.0

Um die durch interne PKIs erzeugten Zertifikate auch im unternehmensübergreifenden Kontext von Industrie 4.0-Wertschöpfungsnetzwerken einsetzen zu können, müssen die Anforderungen an die Vertrauenswürdigkeit im Vertrauensraum interoperabel und vergleichbar sein, wie dies in den vorhergehenden Kapiteln des Dokuments bereits beschrieben wurde.

Interoperabilität und Vergleichbarkeit zwischen verschiedenen CAs können sowohl über die auch bei eIDAS verwendeten Trusted Lists wie in der „ETSI TS 119 612" (22) spezifiziert, als auch über Cross-Zertifizierungen hergestellt werden. Wie bereits im Dokument dargestellt wurde, kann so Vertrauen kommuniziert und Transparenz über die Erfüllung gemeinsamer Anforderungen erreicht werden.

4. Ausblick und Zusammenfassung

Im Folgenden wird ein Ausblick auf weitere und zukünftige Anwendungen für Digitale Identitäten gegeben. Zum Schluss werden die wesentlichen Aspekte des Papiers noch einmal zusammengefasst.

4.1 Identitäten für Produkte und Systeme

Basierend auf einer übergreifenden Vertrauensinfrastruktur ergeben sich im Kontext von Industrie 4.0 weitere Anwendungen für Sichere Digitale Identitäten von Produkten und Systemen, bei denen Hersteller, Integratoren oder Betreiber als IACP fungieren. Für die sichere Interaktion zwischen technischen Komponenten müssen diese eindeutig und sicher identifizierbar sein. In Kommunikationsprotokollen wie HTTPS und OPC UA ist bspw. die Verwendung von elektronischen Zertifikaten im X.509v3-Format vorgesehen, die vom Betreiber anwendungsorientiert vergeben werden.

Für das initiale, automatisierte „Onboarding" von Produkten und Systemen werden aktuell Mechanismen diskutiert, die auf Geräteidentitäten nach IEEE 802.1AR (Secure Device Identity) (21) basieren, die ebenfalls X.509v3-Zertifikate verwenden. Die Einbettung entsprechender PKIs für Geräte in Identitätskonzepte, zum Beispiel zur Vergabe der initialen Geräteidentität (z. B. Hersteller, Typ und Seriennummer) „IDevID", ist zu betrachten.

Die Geräteidentität ist auch ein essenzieller Bestandteil des elektronischen Typenschilds, das in der DIN SPEC 91406 (23) beschrieben wird und langfristig physische Typenschilder ersetzen könnte. Auch hier besteht die Möglichkeit, das digitale Typenschild durch Sichere Identitäten und/oder Signaturen zu unterstützen.

4.2 Zukünftige Anwendungen in Bezug auf Identitäten

Aktuell existiert Klärungsbedarf für zukünftige Industrie 4.0-Anwendungen in Bezug auf dezentrale Ansätze zur Verwaltung von Identitäten. Dabei wird die Verantwortung für die Verwaltung von Identitäten auf die Entität selbst übertragen. Somit ermöglicht das Verfahren den Eigentümern eine alleinige Steuerung der Identität sowie die Verwaltung des Zugriffs auf zugehörige Informationen.

Ein im E-Commerce diskutierter Ansatz, der die dezentrale Verwaltung von Identitäten unterstützt, ist Self Sovereign Identity (SSI). Die dort verwendete Technik basiert unter anderem auch auf der Distributed Ledger Technologie (DLT)[15]. Für die Industrie 4.0 ergeben sich an dieser Stelle Anforderungen an eine interoperable Vertrauensbasis wie bspw. Authentizität, Skalierbarkeit, Langlebigkeit, Robustheit, Resilienz sowie Integrierbarkeit in industrielle Umgebungen (technisch sowie Use-Case-spezifisch). Daher müssen die Vorteile und noch ungelösten Herausforderungen im Zusammenhang mit einer Erweiterung von SSI auf Industrie 4.0-Wertschöpfungsnetzwerke und die Maschinenebene geklärt werden. Dies wird im Rahmen von weiteren Dokumenten erarbeitet.

4.3 Fazit

Zusammenfassend lässt sich festhalten, dass durch eine Vertrauensinfrastruktur ein Raum geschaffen wird, in dem sich mehrere Domänen vertrauensvoll und interoperabel austauschen können. Industrie 4.0-Wertschöpfungsnetzwerke bzw. multilateraler Austausch können auf Vertrauensräumen basieren. Dabei schafft eine Vertrauensinfrastruktur eine Grundlage für die Nutzung von Sicheren Digitalen Identitäten im unternehmensübergreifenden Kontext. In dem Vertrauensraum werden IACs und SCCs zwischen den Entitäten ausgetauscht. Diese wiederum können von unterschiedlichen IACP und SCCP ausgestellt werden, die gemeinsame Anforderungen erfüllen. Für die Ausstellung von IACs kann man zwischen einer zentralen und einer dezentralen Lösung unterscheiden, wohingegen sich SCCs auf nachgewiesene Eigenschaften von beispielsweise Prozessen, Diensten oder Produkten beziehen.

Im Kontext von Industrie 4.0 eignet sich die eIDAS-Verordnung als regulative Basis für einen übergreifenden Vertrauensraum auf hohem technischen sowie organisatorischen Anforderungsniveau und mit starker rechtlicher Wirkung. Die in der Verordnung beschriebenen Anforderungen bieten eine Möglichkeit, um eine verlässliche gegenseitige Anerkennung verschiedener Verfahren unternehmensübergreifend zu gewährleisten. Gleichzeitig bleibt für eine technische Umsetzung ausreichend Flexibilität, um Verknüpfungen mit bestehenden oder künftigen Anwendungen in Bezug auf Digitale Identitäten zu realisieren und damit die Vertrauensanforderungen auf allen Ebenen des Gesamtsystems zu erfüllen.

15 Für eine ausführliche Darstellung von DLT sei auf das Dokument „Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen" (24) des BSI verwiesen, das die dezentrale Speicherung und Verwaltung der Informationen in Distributed Ledgers analysiert.

5. Glossar

Attribut
Eigenschaft eines Unternehmens, welche für den Aufbau einer Geschäftsbeziehung von Bedeutung ist.

Authentifizierung
Prozess, der die Bestätigung der elektronischen Identifizierung einer Entität sowie Integrität (Herkunft und Unversehrtheit der Daten) ermöglicht.

Entität
Teilnehmer der Industrie 4.0, entsprechend des Standards „ISO/IEC 24760“ (3). Dies sind beispielsweise Unternehmen (Betreiber, Hersteller, Integrator), Systeme, Maschinen, Komponenten, Produkte, Beschäftigte in ihrer Rolle und nicht-physische Objekte (Software, digitale Zwillinge, Prozesse).

IAC
Digitale Identity Authenticating Certificates (IACs) werden oft nach dem X.509-Standard erstellt, welcher die Basis für viele Public Key Infrastrukturen (PKIs) darstellt. Ein IAC ist ein Zertifikat, welches verwendet wird, um einen öffentlichen Schlüssel zu authentifizieren, der in Zusammenhang mit asymmetrischer Kryptographie steht.

IACP
Ein Identity Authenticating Certificate Provider (IACP) identifiziert beteiligte Entitäten eines Industrie 4.0-Wertschöpfungsnetzwerks, verifiziert zusätzliche Informationen und bestätigt deren Korrektheit. Auf dieser Basis wird ein IAC ausgestellt.

Identifikator
Eindeutiges Merkmal, um eine Entität und die zugeordneten Eigenschaften im Kontext einer Handlung eindeutig zu bestimmen. Eine Identität kann im Kontext von Industrie 4.0 durch unterschiedliche Identifikatoren repräsentiert werden (globale Identifikatoren und herstellerspezifische Identifikatoren). Der Identifier gibt Auskunft über das zugrundeliegende Schema für die Authentifizierung.

Identifizierung
Prozess der Verwendung von elektronischen Identifizierungsdaten, die eine Entität eindeutig repräsentieren.

International Electrotechnical Commission for Electrical Equipment (IECEE)
Standardisierungsorgan der Internationalen Elektrotechnischen Kommission (IEC) für „IEC Conformity Assessments for Electrotechnical Equipment and Components | Multilateral certification system based on IEC International Standards“.[16]

Industrie 4.0
Alle Geschäftsprozesse, die durch die Vernetzung von Supply Chains sowie von Maschinen und Abläufen mit Hilfe von Informations- und Kommunikationstechnologie möglich werden.[17]

I4.0-Wertschöpfungsnetzwerke
Gesamtheit der I4.0-Teilnehmer, welche sich zusammenschließen um ein gemeinsames, wertschöpfendes Ziel zu erreichen.

SCC
Ein Security Certification Certificate (SCC) ist ein Zertifikat, welches als Nachweis verwendet wird, um die Qualität eines Produktes, eines Dienstes oder eines Fertigungsprozesses nach einem internationalen ISO- oder IEC-Standard zu verifizieren, wie bspw. ISO 27000x oder IEC 62443.

16 https://www.iecee.org
17 Vgl. https://www.plattform-i40.de/PI40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html

SCCP
Ein Security Certification Certificate Provider (SCCP) prüft anhand definierter Kriterien Produkte, Dienste oder Prozesse und stellt im Anschluss einen Bericht sowie bei positivem Prüfergebnis ein SCC aus.

Sichere Digitale Identität
Eine eindeutige Identität mit zusätzlichen Sicherheitseigenschaften für eine belastbar vertrauenswürdige Authentifizierung der Entität (d.h. mit angemessenen Maßnahmen zur Verhinderung der Vortäuschung einer falschen Identität).

Siegel
Artikel 3 der „eIDAS-VO“ (11) bezeichnet ein elektronisches Siegel als „Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen“. Elektronische Siegel beziehen sich auf juristische Personen.

Signatur
Artikel 3 der „eIDAS-VO“ (11) bezeichnet eine elektronische Signatur als „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet“. Die elektronische Signatur wird von natürlichen Personen verwendet und ist einer Willenserklärung gleichgestellt.

Signaturerstellungseinheit
Eine Signaturerstellungseinheit ist nach Artikel 3 der „eIDAS-VO“ (11) „konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird“.

Trust Service Provider (TSP)
Laut der „eIDAS-VO“ (11) ist ein TSP eine „natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt“.

Vertrauensinfrastruktur
Eine Vertrauensinfrastruktur im Kontext von Industrie 4.0 ist ein Rahmen, in dem Nachweise für die Vertrauenswürdigkeit in einem Wertschöpfungsnetzwerk unternehmensübergreifend ausgetauscht werden können.

Vertrauensraum
Raum, in dem Geschäftspartner gemeinsamen, übergreifenden Anforderungen für den Austausch von IACs und SCCs zwischen Entitäten vertrauen können.

Vertrauenswürdigkeit für das Security- und Risikomanagement
Die Fähigkeit eines Suppliers, die Erwartungen eines potenziellen Vertragspartners in einer verifizierbaren Weise zu erfüllen.

Zeitstempel
Zeitstempel werden im „RFC 3161“ (25) standardisiert und verknüpfen Daten mit einem bestimmten Zeitpunkt. Sie erbringen dadurch den Nachweis, dass diese Daten zu einem spezifischen Zeitpunkt vorhanden waren.

6. Abbildungsverzeichnis

7. Referenzen

(1) **Plattform Industrie 4.0 und Robot Revolution & Industrial IoT Initiative:** *„IIoT Value Chain Security – The Role of Trustworthiness“.* Berlin: Federal Ministry for Economic Affairs and Energy (BMWi), 2020.

(2) **Plattform Industrie 4.0:** *„Technischer Überblick: Sichere Identitäten“.* Berlin: Bundesministerium für Wirtschaft und Energie (BMWi), 2016.

(3) **ISO/IEC 24760-1:** *„IT Security and Privacy – A framework for identity management“ – Part 1: Terminology and concepts.* 2019.

(4) **Recommendation ITU-T X509 | ISO/IEC 9594-8 „Information Technology – Open Systems Interconnection – The Directory:** *Public-key and attribute certificate frameworks“.* 2019.

(5) **ISO/IEC 27001** *„Information technology – Security techniques – Information security management systems – Requirements“.* 2017.

(6) **IEC 62443** *„Industrial communication networks – Network and system security“ – Part 4-1: Secure product development lifecycle requirements.* 2018.

(7) **IEC 62443** *„Industrial communication networks – Network and system security“ – Part 4-2: Technical security requirements for IACS components.* 2019.

(8) **ISO/IEC 15408** *„Common Criteria for Information Technology Security Evaluation“*; 3.1.2009.

(9) **Regulation (EU) No 2019/881** of the European Parliament and of the Council of 17 April 2019 (*Cybersecurity Act*). 2019.

(10) **IEC 62443** *„Industrial communication networks – Network and system security“ – Part 2-1: Establishing an industrial automation and control system security program.* 2010.

(11) **EU-Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014** (*Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt*). 2014.

(12) **ETSI EN 319 411** *„Policy and security requirements for Trust Service Providers issuing certificates“.* 2017.

(13) **BSI TR 03145 „Secure CA Operation“ – Part 1:** *Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level ‚high‘.* 2017.

(14) **ETSI EN 319 412** *„Electronic Signatures and Infrastructures (ESI); Certificate Profiles“ – Part 1: Overview and common data structures.* 2020.

(15) **Projektbericht Sichere Digitale Identitäten (SDI)** – *Umsetzungsempfehlungen zur Definition und Etablierung Sicherer Digitaler Identiäten als Vertrauensanker in der digitalisierten Welt*. Berlin: DIN e.V., DKE, 2017.

(16) **BSI TR 01201 Teil 2.1** *„Accountmanagement Funktionalitätsspezifikation“.* 2019.

(17) **ISO/IEC 15459-1:** *„Information technology – Automatic identification and data capture techniques – Unique identification“ – Part 1: Individual transport units.* 2014.

(18) **ISO/IEC 6523-1:** *„Information technology – Structure for the identification of organizations and organization parts“ – Part 1: Identification of organization identification schemes*. 1998.

(19) **ISO 17442-1:** *„Financial services – Legal entity identifier (LEI)“ – Part 1: Assignment.* 2020.

(20) **Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 Juli 2012** (*European Market Infrastucture Regulation*). 2012.

(21) **IEEE 802.1AR** – *IEEE Standard for Local and Metropolitan Area Networks* – Secure Device Identity. 2018.

(22) **ETSI TS 119 612** *„Trusted Lists“.* 2015.

(23) **DIN SPEC 91406** – *Automatic identification of physical objects and information on physical objects in IT systems, particularly IoT systems.* 2019.

(24) **RFC 3161** – *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).* 2001.

(25) **Bundesamt für Sicherheit in der Informationstechnik:** *„Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen“.* 2019.

Elektronische Quellen:

https://www.plattform-i40.de/PI40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

https://www.iecee.org

https://webgate.ec.europa.eu/tl-browser/#/tl/DE

https://blog.eid.as/de/tag/vertrauensdiensteanbieter

https://www.china-iprhelpdesk.eu/sites/all/docs/publications/How_to_search_for_company_information.pdf

https://www.japanregistry.com

https://www.sec.gov/edgar/searchedgar/companysearch.html

https://de.wikipedia.org/wiki/GS1

https://www.gs1-germany.de

8. Anhang

Entwicklung der eIDAS-Verordnung

Der eIDAS-Verordnung voran gingen diverse Entwicklungen in Europa, welche von Sichtausweisen weg- und zu elektronischen Identitätsdokumenten hinführten, die u.a. für Online-Dienste genutzt werden können. Bereits 1998 erfolgte eine Machbarkeitsstudie in Finnland, um Bürgerdienste (e-Government) in das Web zu verlagern. Nicht der Bürger läuft ins Rathaus, sondern nur dessen Daten. Während Ende 2005 noch fünf Länder mit elektronischen Identitäten gezählt wurden, waren es fünf Jahre später bereits 17 Länder und 2015 sogar 29 Länder. Die überwiegende Zahl der Länder sind EU-Mitgliedsländer. Um „mehr Europa" zu schaffen und damit auch „mehr europäischen Binnenmarkt" zu generieren, wird „mehr länderübergreifendes Vertrauen" benötigt, was zur eIDAS-Verordnung geführt hat. Dabei steht nicht die Harmonisierung im Vordergrund, sondern die Interoperabilität bezogen auf das erzielte Sicherheitsniveau (Level of Assurance, abgekürzt LoA). Sowohl die Mindestanforderungen an Identifikationsmittel[18] als auch die Interoperabilität[19] wurden durch zwei weitere EU-Regulierungen für juristische wie auch natürliche Personen beschrieben.

Notifizierte Identitätssysteme eines EU-Mitgliedslandes müssen nach der eIDAS-Verordnung seit dem 29.09.2018 von allen anderen Mitgliedsländern verpflichtend anerkannt werden. Bis Ende Juni 2020 wurden elektronische ID-Systeme in Verbindung mit elektronischen Identitätsausweisen von elf Mitgliedsländern mit Niveau „hoch" notifiziert, teilweise sogar mit Mehrfach-Nennungen von Identifikationsmitteln, wie das Beispiel Estland zeigt, mit sechs Mitteln[20]. Zum Zeitpunkt der Erstellung dieses Dokuments hat Litauen den Notifizierungsprozess gestartet, und neun weitere Länder haben elektronische Identifikationsmittel in der Ausgabe, aber den Notifizierungsprozess noch nicht begonnen[21]. Drei Mitgliedsländer haben neben elektronischen Identitätsdokumenten auch mobile Identitäten mit Smart Phones als Identifikationsmittel mit Niveau „hoch" notifiziert. Dazu zählen Estland, Belgien und Portugal. Während dazu in Estland die SIM-Karte im Smart Phone durch eine PKI-SIM-Karte nach ETSI-Standards ersetzt werden muss, um bestimmte Identifikationsverfahren wie mit der estnischen ID-Karte zu ermöglichen, wurden für Belgien und Portugal Auflagen gemacht, die eine Zertifizierung, entweder eines vertrauenswürdigen Ausführungsumgebung (Trusted Execution Environment) oder eines Sicherheitselements (SE) erforderlich machen[22].

Da die eIDAS-Verordnung in der Architektur einen föderierten Identitätsansatz verfolgt, wurde 2019 von der EU-Kommission, Generaldirektion CONNECT, eine Studie in Auftrag gegeben, um eine technische Brücke vom eIDAS-Ansatz mit dezentralen Identitäten (DID) aufzubauen, zu denen die Self Sovereign Identity (SSI)-Technologie (siehe Kapitel 4.2) zählt. Dazu werden zwei Grundprinzipien verfolgt[23]:

- Verknüpfung der DID mit der Identität, die von einem notifizierten eID-Schema bereitgestellt wird
- Verknüpfung der DID mit der Identität eines elektronischen Zertifikats

Seit 2019 arbeitet die EU-Kommission an dem „Export" des eIDAS-Konzepts in andere Industrienationen. So wurden Workshops in Japan[24], Singapur, USA und Kanada und den dortigen Ministerien durchgeführt und Vorschläge zur Kooperation unterbreitet[25].

18 Mindestanforderungen an Identifikationsmittel (EU) 2015/1502
19 Interoperabilität (EU) 2015/1501
20 https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
21 Detlef Houdeau, Tina Hühnlein, Klaus Wolfenstetter, Digitale Identität als Fundament der vertrauenswürdigen Transformation, Zeitschrift DuD, Heft 4/2019
22 https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=148898042
23 https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI%20eIDAS%20Bridge_Flyer_1.pdf
24 https://www.a-trust.at/MediaProvider/2453/innovation-day-2019_jtsf_hamaguchi.pdf
25 https://www.enisa.europa.eu/events/tsforum-caday-2019/presentations/00-01-gjoen

AUTOREN

Aliza Maftun, Siemens | Dr. Detlef Houdeau, Infineon Technologies | Dr. Lutz Jänicke, Phoenix Contact GmbH & Co. KG | Dr. Andre Braunmandl, Bundesamt für Sicherheit in der Informationstechnik | Dr. Gerd Brost, Fraunhofer AISEC | Dr. Wolfgang Klasen, Siemens | Jan Grießbach, NXP | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Michael Jochem, Robert Bosch GmbH | Roman Winter, GS1 Germany GmbH | Sebastian Fandrich, Sick | Sebastian Oelmann, NCP Secure Communication | Tianzhe Yu, IFAK | Vanessa Bellinghausen, Bundesamt für Sicherheit in der Informationstechnik | Thomas Walloschke, secon trust consult | Björn Flubacher, Bundesamt für Sicherheit in der Informationstechnik

Diese Publikation ist ein Ergebnis der Arbeitsgruppe „Sicherheit vernetzter Systeme“ der Plattform Industrie 4.0.

www.plattform-i40.de