filancore

Identity Gateway – Decentralized Identity and Access Management for IoT

Whitepaper

Version 1.1, März 2023

www.filancore.com

info@filancore.com

Inhaltsverzeichnis

Kurzfassung

https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_Mythbusting_Self-Sovereign_Identity.pdf

Das filancore Identity Gateway ist eine Identity und Access Management (IAM) Plattform für das Internet der Dinge (IoT) auf Basis **selbstbestimmter Identitäten (Self-Sovereign Identity , SSI)**.

Ziel von filancore ist dabei sowohl das Management von digitalen Identitäten - über deren gesamten Lebenszyklus - als auch (Zugriffs-) Richtlinien für diese Identitäten einfach und zugleich sicher zu gestalten.

Hauptnutzer und Fokus der Plattform sind Organisationen, die potenziell eine erhebliche Menge dieser Identitäten ausstellen und verwalten müssen. Ein Beispiel hierzu sind Hersteller von Geräten für das Internet der Dinge (Internet of Things, IoT) - intelligente Sensoren und Aktoren – die jedes ihrer Geräte mit einer eigenen Identität ausstatten wollen und dafür eine skalierbare und effiziente Lösung benötigen.

https://www.w3.org/

https://www.w3.org/TR/did-core/

https://www.w3.org/TR/vc-data-model/

https://en.wikipedia.org/wiki/Distributed_ledger

Das Fundament, auf dem filancore aufsetzt, besteht aus hochinnovativen Technologien wie dem **W3C -Standard** für **Dezentralized Identifiers (DIDs)**, **Verifiable Credentials (VCs)** sowie der **Distributed Ledger Technologie (DLT)**. Die Identitäten sind dabei agnostisch hinsichtlich ihrer Subjekte und können dementsprechend zur Authentifizierung und Autorisierung von Organisationen, Menschen, Maschinen, Geräten, Services, Applikationen uvm. eingesetzt werden. Diese Technologien ermöglichen so ein hochinteroperables digitales Ökosystem der nächsten Generation.

Mit dem Aufkommen des Internets der Dinge stehen Organisation, die in diesem Bereich tätig sind, vor neuen Herausforderungen, da das Identitäts- und Zugangsmanagement (IAM) nun auch für IoT einen grundlegenden, kritischen Bestandteil der IT-Sicherheit dieser Unternehmen ausmacht und untrennbar mit der digitalen Effizienz verbunden ist. Dabei können die Aspekte Sicherheit, Skalierbarkeit, Offenheit und Einfachheit mit herkömmlichen Systemen und Verfahren im Kontext IoT nicht mehr vollumfänglich bewältigt werden.

Selbstbestimmte Identitäten (Self-Sovereign Identity, SSI) gelten dabei als ganzheitlicher Problemlöser im Bereich der digitalen Identitäten und bietet zahlreiche Vorteile, die sich für filancore auch auf die Herausforderungen des Internet der Dinge (IoT) übertragen lassen. Auf Basis des Standards zu Selbstbestimmten Identitäten des World Wide Web Consortiums (W3C) entsteht ein digitales, dezentrales Ökosystem nach den Vorstellungen eines „Web of Trust", bei dem der Inhaber einer digitalen Identität – gleich ob Mensch, Maschine oder Organisation – die volle Eigentümerschaft und Kontrolle über die Verwendung derselben sowie damit verknüpfter, gegebenenfalls persönlicher Daten erhält. Darüber hinaus sieht filancore in SSI eine sichere und interoperable Möglichkeit, eine dezentrale Identitäts- und Zugriffsverwaltung für Anwendungsfälle im Bereich IoT zu realisieren und neue Geschäftsmodelle zu schaffen in welcher vernetze Systeme, Maschinen, Geräte und Sensoren eine immer größere Rolle spielen.

Die Vision von filancore ist es, diese Herausforderungen zu bewältigen und das Potenzial des IoT für Organisationen mittels SSI entfalten zu können. Das Team rund um filancore hat sich daher zum Ziel gesetzt SSI und die zugrundeliegenden hochinnovativen Technologien wie dem W3C-Standard für Dezentralized Identifiers (DIDs), Verifiable Credentials (VCs) sowie der Distributed Ledger Technologie (DLT) für Organisationen im Bereich IoT leicht abruf- und nutzbar zu machen. Hierfür wird seit 2019 mit ausgewählten Test- und Pilotkunden das filancore Identity Gateway - eine auf SSI basierende Identity and Access Management (IAM) Plattform - ent- und weiterentwickelt, um sicherzustellen, dass die Bedürfnisse der Industrie und deren Anforderungen an die Sicherheit für unternehmenseigene sowie unternehmensübergreifende IoT-Anwendungsfälle gedeckt sind. Das filancore Identity Gateway erleichtert dabei den Aufbau und die Verwaltung von vertrauenswürdigen IoT-Ökosystemen entlang des Sicherheits-Lebenszyklus, indem den Teilnehmern, egal ob einige wenige oder hunderttausende von Organisationen, Personen, Maschinen, Geräten, Services, Applikationen, uvm. eine öffentliche und dezentrale Identität, sowie kontrollierbare Berechtigungen bzw. Nachweise verliehen werden. Es etabliert sich dabei eine vorteilhafte emergente Identitätsschicht, die dazu führt, dass traditionelle, zentrale Authentifizierungs- und Autorisierungsmechanismen zunehmend durch dezentrale Methodiken er-

gänzt und perspektivisch ersetzt werden. Der Vorteil dieser dezentralen Authentifizierungs- und Autorisierungsmechanismen liegt darin, dass sie einem heterogenen Umfeld agieren können und ein offenes IoT-Ökosystem ermöglichen, indem sie vor Kompromittierung, Missbrauch sowie vor Single-Point-of-Failures schützen. Dabei bieten sie auch vermittelnde Eigenschaften, die bei Organisationen bzw. im IoT-Ökosystem zu Netzwerkeffekten führt, indem eine große Menge an neuen Teilnehmern, z.B. weitere Partner bzw. externe Geräte und Services, zum gegenseitigen Nutzen kontrolliert zusammenführen werden können, um effektivere Interaktionen zu ermöglichen.

Diese Eigenschaften können entlang des gesamten Lebenszyklus der Identitäten, vom Registrierungsprozess und Onboarding, z.B. in der End-of-Line-Produktion für Geräte, über einen kontrollierten Betrieb in der gewünschten Zielumgebung mit verschiedensten Stakeholdern, bis hin zum End-of-Life erreicht und verwalten werden. Das filancore Identity Gateway agiert als ein Trusted-Ecosystem-Enabler, für Anwendungsfälle in denen

- Nachweise bzw. Echtheitsbeweise erforderlich sind, um z.B. feststellen zu können, dass es sich bei einem Gerät um ein Original des Herstellers handelt;
- ein IoT-Gerät bzw. ein Teilnehmer im IoT Ökosystem verifiziert werden muss, um sicherstellen zu können, dass das Gerät bzw. der Teilnehmer auch wirklich derjenige ist, für den er sich ausgibt;
- Zugriffe bzw. Berechtigungen für Geräte und Systeme gesetzt und gesteuert werden müssen, um nur autorisierte Interaktionen auch unternehmensübergreifend zu gewährleisten;
- die Erzeugung, der Austausch und die Überprüfung von vertrauenswürdigen Daten notwendig ist, z.B. wenn ein Empfänger die Authentizität und Datenintegrität eines Sensor-Datenpunktes innerhalb eines Datenmarktplatzes überprüfen möchte.

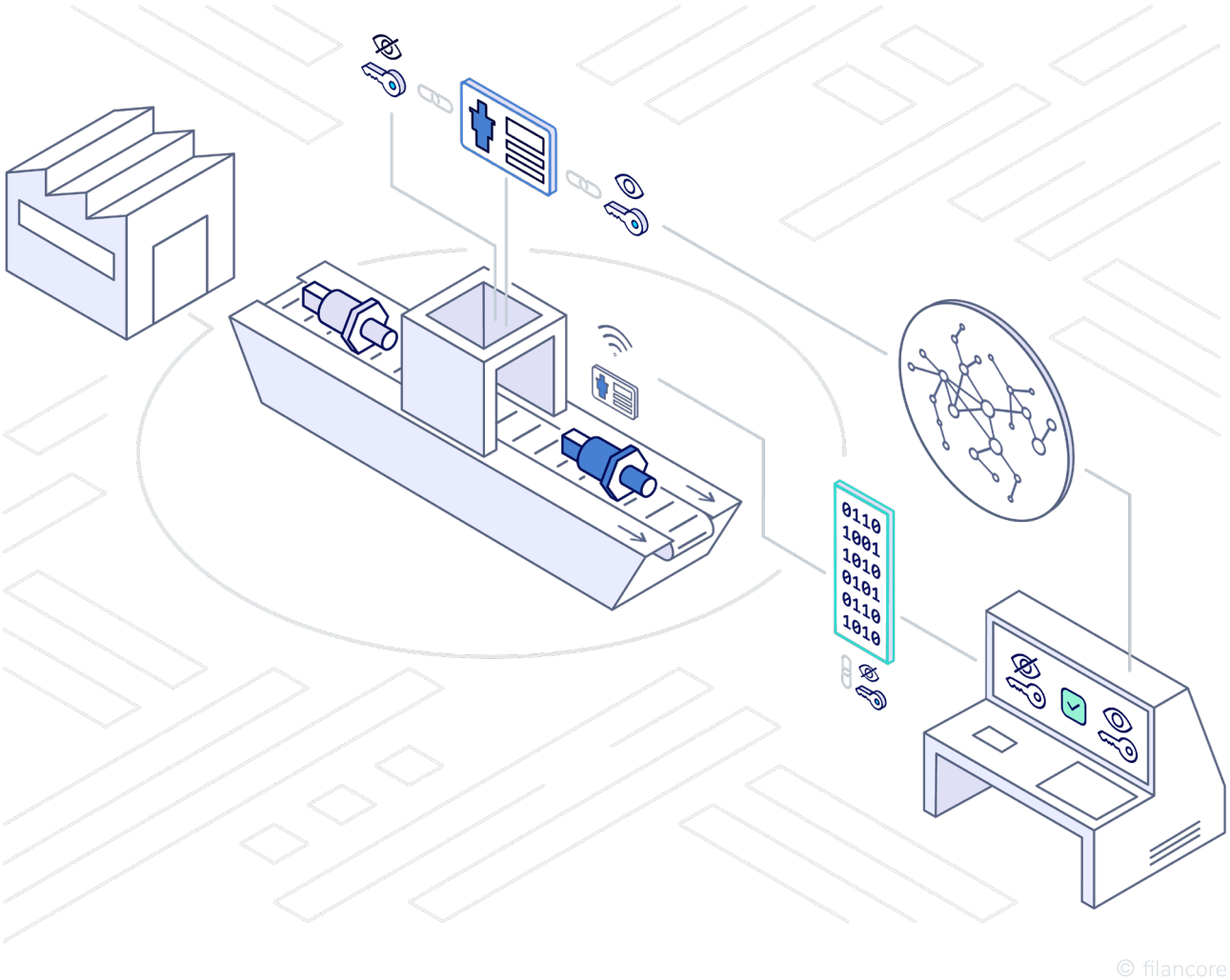
Kurzum, Nutzer des filancore Identity Gateway können somit

- mit geringem Aufwand auch große Mengen selbstsouveräner Identitäten erstellen oder bereits erstellte Identitäten in der Plattform registrieren;
- automatisch oder manuell kontrollierte Identitäten in verschiedenen DLTs oder anderen Netzwerken verankern, um sie global nutzbar zu machen;
- Identitäten verwalten, durchsuchen, sortieren und gruppieren, mit anderen Entitäten verknüpfen sowie Aliase vergeben;
- andere Identitäten bzw. Teilnehmer (z.B. IoT-Geräte) im Ökosystem verifizieren, um sicherzustellen, dass die Teilnehmer auch wirklich derjenige sind, für die sie sich ausgeben;
- Nachweise bzw. Echtheitsbeweise (VCs) auf Basis eines praktischen Vorlagensystems ausstellen und ebenso wie Identitäten verwalten, durchsuchen, (um-) benennen, sortieren und gruppieren;
- Nachweise Dritter verifizieren, um z.B. feststellen zu können, dass es sich bei einem Gerät um ein Original des Herstellers handelt;
- die Erzeugung und den Austausch von vertrauenswürdigen IoT-Daten ermöglichen, z.B. wenn ein Empfänger die Authentizität und Datenintegrität von Daten anhand der Identität des Erzeugers der Daten (z.B. einem Sensor) überprüfen möchte;
- Zugriffe bzw. Berechtigungen für Teilnehmer und Zielsysteme aufsetzen und verwalten, um nur autorisierte Interaktionen im Ökosystem (auch unternehmensübergreifend) zu erlauben;
- Vorlagen erstellen und verwalten, die das massenhafte Erstellen von Identitäten und Nachweisen erleichtern und eine Standardisierung von Prozessen erlauben;
- automatisiert, simpel und ohne Programmierkenntnisse die gesamte Hintergrundinfrastruktur wie DLT-Knoten zur Verankerung von Identitäten, Sicherheitsmodulanbindungen wie Hardware Security Module zur Speicherung von privatem Schlüsselmaterial und Dateisystem- bzw. Datenbankknoten zur Ablage von Identitätsdokumenten verwalten und überwachen.

Das filancore Identity Gateway als Identity und Access Management (IAM) Plattform unterstützt IoT-Ökosysteme als sicheres Fundament für kollaborative Anwendungsfälle, indem eine durchgängige Identifizierung jedes Beteiligten, Zugangsregeln und Richtlinien, benötigte Nachweise, sowie eine vertrauenswürdige Datenübertragung ermöglicht, etabliert und gewährleistet werden.

(1) Trusted IoT Data & Data Integrity

Mit dem Identity Gateway können IoT-Anwendungsfälle realisiert werden, bei denen die Unveränderbarkeit und Gültigkeit von IoT-Daten über den gesamten Lebenszyklus zu gewährleisten ist, insbesondere wenn diese Daten sensibel oder für eine Weiterverwendung erforderlich sind, beispielsweise für einen Verkauf in einem Datenmarktplatz. Die Plattform stellt hierfür Mechanismen zur Etablierung und Überprüfung der Authentizität und Integrität von Daten bereit, was deren Wert und das Vertrauen in diese Daten erhöht.



Wie kann das erreicht werden?

Technisch wird dies erreicht, indem das IoT-Gerät über das filancore Identity Gateway, im besten Fall aus Sicherheitsgründen bereits in der Produktion (End-of-Line), eine eigene selbstbestimmte Identität erhält. Optimalerweise geschieht dies, indem der mit der Identität korrelierende geheime Schlüssel auf einem geeigneten Sicherheitschip (z.B. HSM oder TPM) fest „verdrahtet“ wird. Alternativ kann dieser auch, z.B. bei leistungsschwachen Geräten, von der nächstbesten Einheit (bspw. ein IoT Gateway) oder bei weniger kritischen IoT-Geräten in einem Software Security Modul bzw. Secure Software Environment gehalten werden. Der korrelierende öffentliche Schlüssel wird vom Identity Gateway automatisiert auf dem öffentlichen Distributed Ledger verankert.

Das IoT Gerät kann nun mit dieser Identität autonom und nachweisbar die von ihm ausgehenden Daten mit dem privaten Schlüssel der Identität signieren. Die Signierfunktion wird in der Regel von dem Sicherheitschip nativ unterstützt, alternativ kann dies durch Software auf dem IoT-Gerät nachgebildet werden.

Der Empfänger, egal ob eine Person, eine Organisation oder ein anderes IoT-Gerät, ist nun in der Lage die Unverfälschtheit und Herkunft der Daten zu verifizieren, indem diese mit dem öffentlich einsehbaren Teil der Identität des IoT-Gerätes auf dem Distributed Ledger (bzw. dem überprüfbaren Datenregister) in Punkto Gültigkeit überprüft werden. Hierfür wird die Signatur der empfangenen Daten, also die Unterschrift mit dem die IoT-Geräte die gesendeten Daten versehen haben, kryprografisch abgeglichen. Bei einer Übereinstimmung kann sich der Empfänger sicher sein, dass die empfangen Daten von besagtem IoT-Gerät stammen und die Daten nicht manipuliert wurden. Die Daten erhalten somit eine nachweisliche Wertigkeit für den Empfänger.

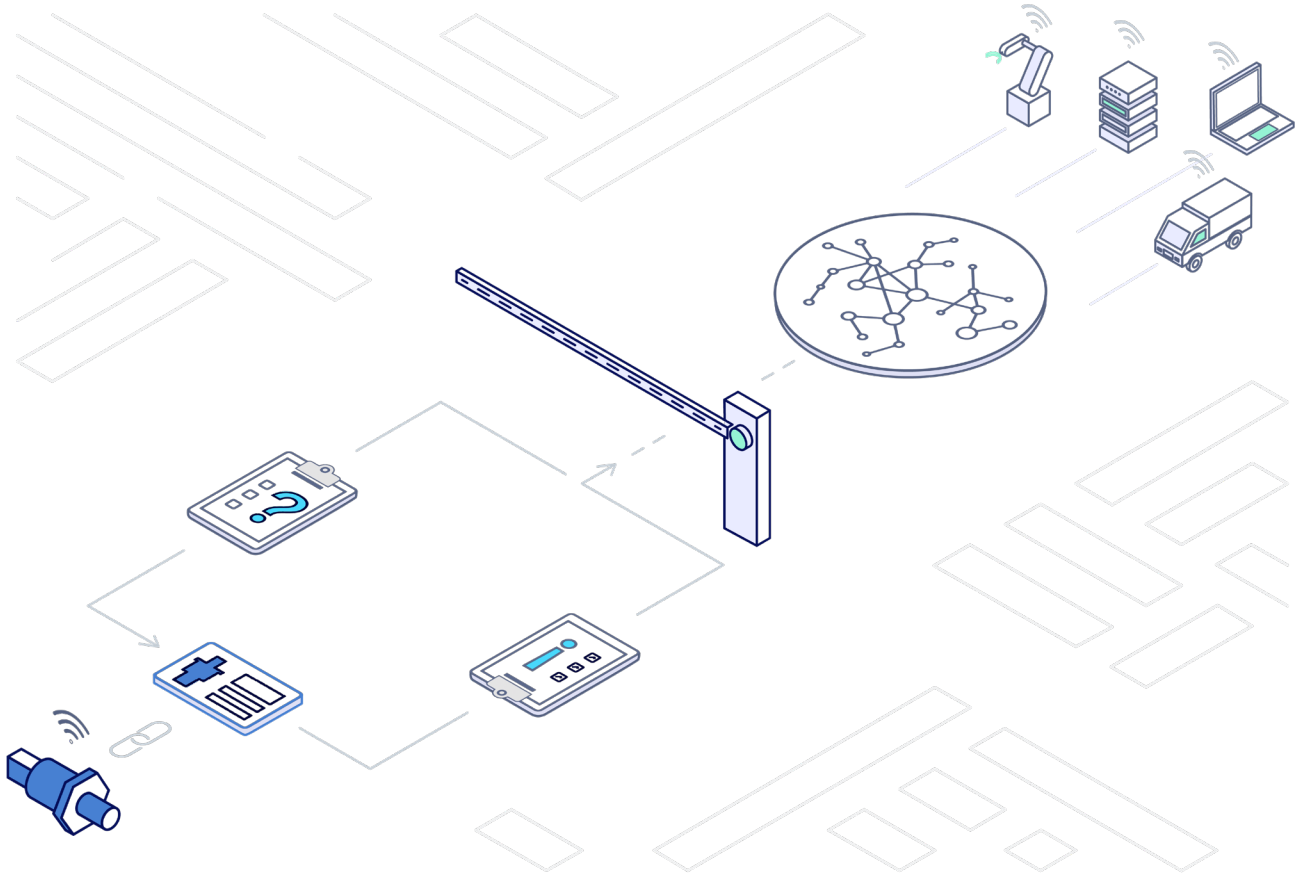
(2) Authentifizierung

In (IoT-)Ökosystemen ist es notwendig, dass sich die Teilnehmer (Personen, Organisationen oder z.B. IoT-Geräte) gegenseitig für bestimmte Anwendungsfälle authentifizieren können (z.B. ein IoT-Gerät an einem bestimmten Service Point), um eine vertrauenswürdige mehrseitige Interaktion bzw. Kommunikation zu ermöglichen. Mittels Authentifizierung wird verhindert, dass unbefugte Dritte einen Zugang zum (IoT-)Ökosystem und dessen Daten oder Funktionen erhalten. Dies ist ebenfalls für das Zero-Trust-Konzept relevant, bei dem jeder Datenzugriff zunächst als nicht vertrauenswürdig eingestuft wird, egal ob die Anfrage innerhalb oder außerhalb des Firmennetzwerkes erfolgt.

Wie kann das erreicht werden?

Die Authentifizierung stellt die eigentliche Prüfung der vom Gegenüber behaupteten Identität dar, bei der geprüft wird, ob der Teilnehmer auch wirklich im Besitz der Identität bzw. mitgeteilter Merkmale ist. Das filancore Identity Gateway unterstützt dieses Verfahren, indem einem Teilnehmer eine Identität verliehen wird, die von Dritten verifiziert werden kann, z.B. wenn ein (IoT-) Ökosystemteilnehmer in Form eines IoT-Gerätes Zugang an einem Service Punkt, dem Verifizierer, im Ökosystem haben möchte.

Die Authentifizierung erfolgt dabei durch ein Challenge-Response-Verfahren, bei dem der Verifizierer dem Teilnehmer eine Aufgabe stellt, die nur der Besitzer der Identität zu lösen imstande ist. Wird die Aufgabe vom Teilnehmer erfolgreich gelöst, so gilt er gegenüber dem Verifizierer als authentifiziert. Da dieses Verfahren auf etablierten kryptographischen Standards aufsetzt, ist ein hoher Grad an Sicherheit gegenüber unautorisiertem Zugriff gegeben.



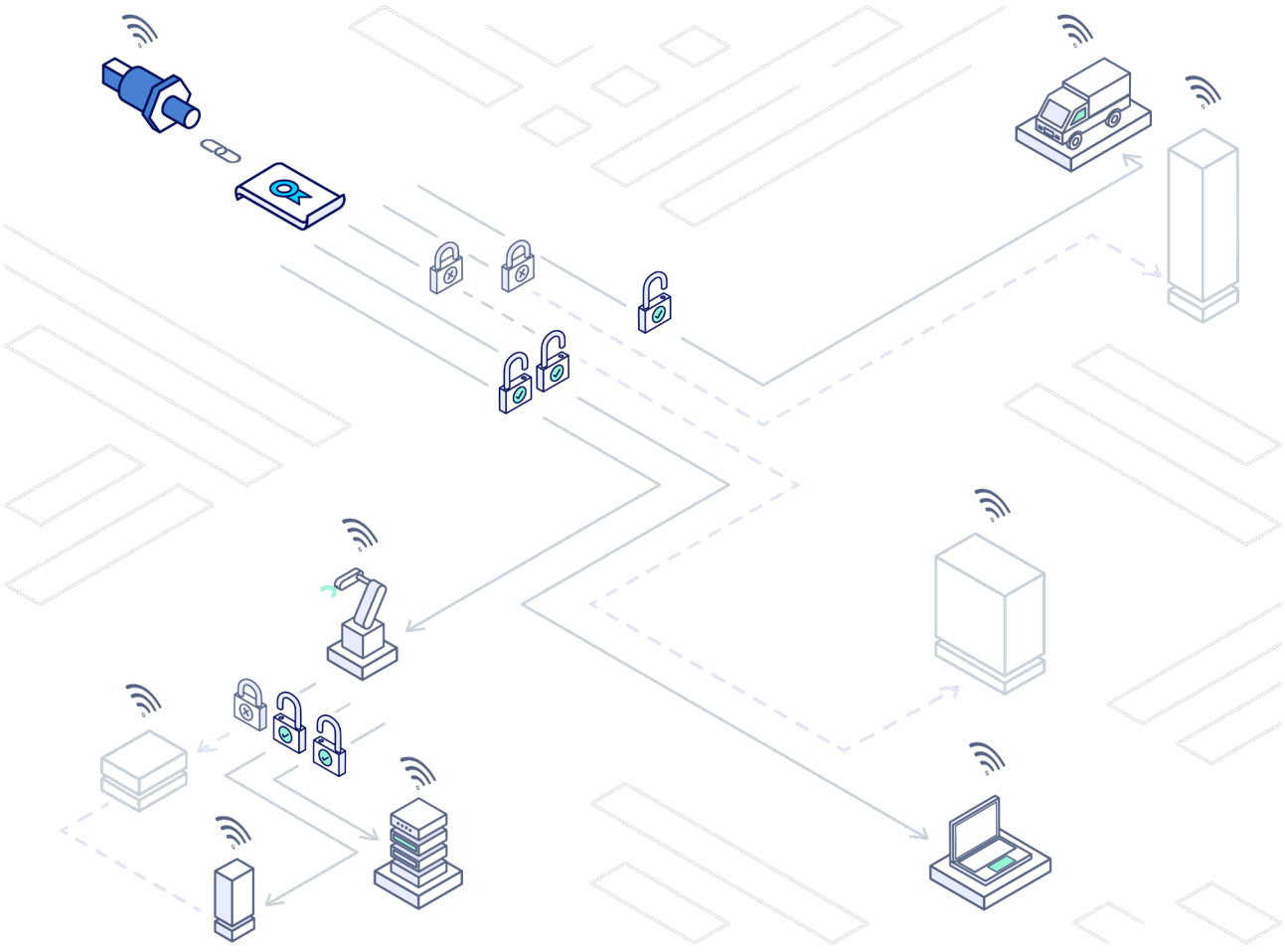
(3) Autorisierung

Mit Autorisierung können nach einer erfolgreichen Authentifizierung zusätzlich bestimmte Zugriffe bzw. Berechtigungen und Privilegien im (IoT-)Ökosystem überprüft und gewährt bzw. verweigert werden, wenn bestimmte Zugangspunkte, Daten und Funktionen ein separates Sicherheitsniveau benötigen.

Wie kann das erreicht werden?

Mittels des Identity Gateway können Richtlinien bestimmt und erteilt werden, die im IoT-Ökosystem für kontrollierte Zugriffe auf Anwendungen, Systemen oder Daten-Ressourcen oder gar anderen IoT-Geräten sorgen. So wird beispielsweise festgelegt, auf welche Ressourcen, Funktionen oder andere IoT-Systeme ein Teilnehmer, z.B. ein IoT-Gerät selbst Zugriff hat.

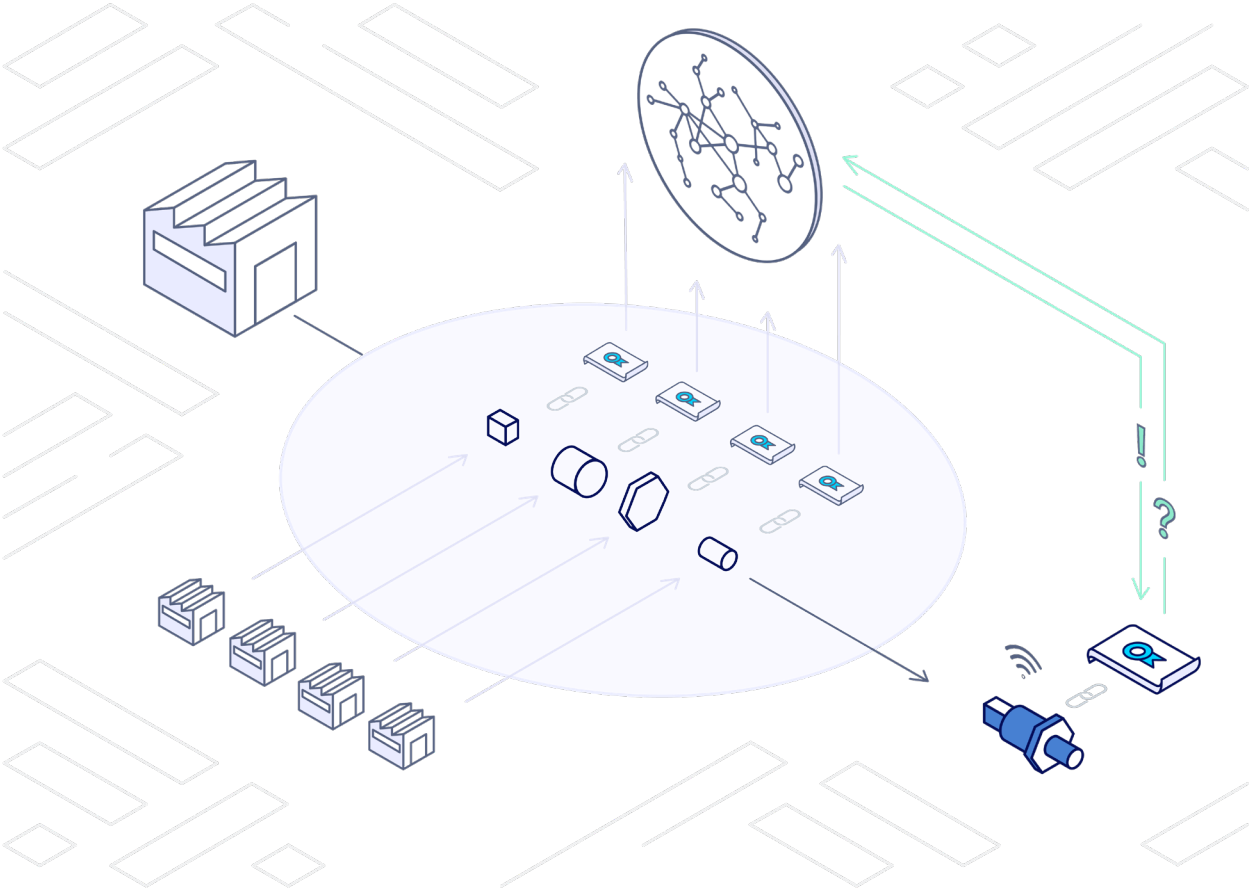
Hierbei können in Form von Verifiable Credentials sowie Vorlagen Berechtigungen standardisiert, definiert und ausgegeben werden. Einem Ökosystemteilnehmer werden somit, auch unternehmensübergreifend, bestimmte Privilegien und Zugriffe gewährt.



Diese Zugriffssteuerung kann auch rollenbasiert nach einem sogenannten „Role Based Access Control (RBAC)“ Modell erfolgen: Hier wird dem Benutzer Rollen oder Gruppen zugewiesen, denen wiederum bestimmte Zugriffsarten und -beschränkungen zugeteilt werden.

(4) Proof of Origin

Überprüfbare Nachweise sind zunehmend in digitaler Form vor allem auch bei IoT-Komponenten notwendig. So ist es unter anderem wichtig für Hersteller dieser Komponenten, gegen gefälschte Produkte am Markt anzukommen, da Käufer von gefälschten IoT-Geräten häufig eine schlechtere vorhandene Qualität mit der Originalmarke bzw. dem Originalhersteller assoziieren. Dies hat unter anderem weitere negative Auswirkungen zur Folge, wenn diese schlechten Erfahrungen mit anderen geteilt werden und dadurch Umsatzeinbußen folgen.
Aber nicht nur der Imageschaden, sondern auch die Bekämpfung von Produktfälschungen ist kostspielig, insbesondere wenn Klagen abgewehrt werden müssen. Originalhersteller können die zuvor herausfordernde Erbringung eines nachvollziehbaren Beleges für eine im eigenen Werk produzierte IoT-Komponente, z.B. um Forderungen in Bezug auf Qualität- und Sicherheitsmängel besser abwehren zu können, einfach gewährleisten.



Wie kann das erreicht werden?

Hersteller von IoT-Komponenten können das Identity Gateway dafür nutzen, schon während der Produktion auf der Komponente ein vom Hersteller signiertes, verifizierbares Credential auszustellen und dieses automatisiert und sicher dort zu verankern. Dieses Credential bestätigt kryptographisch sicher die Herkunft und Authentizität der Komponente und kann je nach Anforderungen des Herstellers beliebige weitere Nachweise, sowie Kunden- oder produktspezifische Attribute enthalten, z.B. ein Nachweis zu welchem Zeitpunkt das Gerät erstellt wurde. Dritte und der Hersteller sind damit jederzeit und insbesondere im Falle einer Beanstandung in der Lage, die Echtheit der Komponente festzustellen.

Key Benefits

Die Anwendungsfälle rund um das Internet der Dinge bieten enorme Chancen für Unternehmen. Die Nutzung des IoT kann jedoch in vielen Fällen aufgrund von schwer zu erreichenden Anforderungen langsamer voranschreiten als erwartet. Hier schafft das filancore Identity Gateway für die Bereitstellung, Überwachung, Verwaltung und Steuerung von selbstbestimmten Identitäten für den Aufbau von IoT-Ökosystemen Abhilfe. Die Plattform hilft dabei, sich auf das wesentliche Geschäftsmodell eines Unternehmens fokussieren zu können und Probleme der Sicherheit bei IoT-Teilnehmern, egal ob Personen, Organisationen, Geräte, Systeme oder Dienste von einer potenziell großen Anzahl und Vielfalt bewältigen zu können.

(1) Sicher

Minimierung von Angriffsflächen, großer Datenverluste, Missbrauch von Daten, sowie Noncompliance im Bereich (IoT-)Security und Datenschutz (GDPR/ DSGVO).

Dezentralität

Weniger Abhängigkeiten, mehr Kontrolle und Resilienz

Hinter traditionellen Identitätslösungen und -Services stehen häufig zentralisierte Systeme unter der Kontrolle und Einflussnahme Dritter, was zu technischen Abhängigkeiten führt. Dies kann bei kritischen Anwendungsfällen zu einem sogenannten Single-Point-of-Failure führen, bei dem die Anwender der Willkür bzw. den un- oder absichtlichen Entscheidungen und Handlungen Dritter ausgesetzt sind.
Auch die Eigentümerschaft der Identitäten, Berechtigungen und zugrundeliegenden sensiblen Informationen verbleibt letztendlich bei diesen Dritten,

was diese zentralen Konstrukte prädestiniert für Angriffe und Missbrauch.

Das Identity Gateway und die zugrundeliegenden SSI-Prinzipen helfen Anwendern dabei, künftig Identitäts- und Zugriffssysteme zu dezentralisieren und demokratisieren, indem eine höhere Unabhängigkeit gegenüber zentralen Drittsystemen und -services geschaffen wird. Erreicht wird dies durch eine Verlagerung der Eigentümerschaft der Identitäten hin zum eigentlichen Identitätseigentümer und durch die Verwendung von dezentralen Identitätsregistern als Identitätsanker in Form von Distributed Ledgern. Hierdurch entsteht für den Anwender eine Zensurresistenz und Unabhängigkeit gegenüber Dritten, sowie eine sehr hohe Resilienz durch eine dezentrale Verankerung kritischer Identitäten und Credentials. (IoT-)Ökosystemteilnehmer können zudem auch in die Lage versetzt werden sich bidirektional und transparent zu authentifizieren, autorisieren bzw. übermittelte Daten von Dritten direkt auf ihre Integrität hin zu prüfen.

Compliance

Einhaltung von Bestimmungen hinsichtlich des Datenschutzes, sowie IT- und IoT-Sicherheit.

Die Erreichung von Datenschutzvorgaben und Controls im Bereich IT- und IoT-Sicherheit Standards sind bzw. werden zunehmend für IoT-Produkte und IoT-Ökosysteme zur Pflicht. Das filancore Identity Gateway ermöglicht hierfür die Verwendung von selbstbestimmten Identitäten, welche durch ihre Datensparsamkeit und ihr Ownership-Prinzip als Datenschutzkonform gelten, da die Speicherung und Offenlegung sensibler Identitätsdaten und -Attribute dem Eigentümer der Identität obliegen. Zudem werden ausschließlich standardisierte kryptographische Verfahren und Protokolle auf Basis von öffentlichen und privaten Schlüsseln verwendet und bereitgestellt, die in der Regel bei typischen Control Domänen von Sicherheitsstandards wie „Identity and Access Management“ und Datenintegrität einen vollständigen oder hohen Abdeckungsgrad erreichen.

(2) Skalierbar

Das filancore Identity Gateway wurde so entwickelt, dass die Plattform den Anforderungen des IoT gerecht wird, was mit einer größtmöglichen Skalierbarkeit und Performance einhergeht.

Skalierung

Mit dem Identity Gateway können beträchtliche Mengen von Identitäten und Credentials bzw. Berechtigungen jederzeit und effektiv ausgestellt und verwaltet werden. Dafür sorgt die Auswahl der zugrundeliegenden Technologien und eine weitgehende Automatisierung. Ein weiterer Faktor ist die Wahl des

zugrundeliegenden Distributed Ledger als Indentitätsrepository. Dieser kann enorm große Transaktionsvolumina handhaben und ist in der Lage, Workloads parallel zu bearbeiten, was wesentlich zu einer horizontalen Skalierbarkeit beiträgt.

Auch bei der Entwicklung der Plattform wurde darauf geachtet, dass eine hohe Skalierbarkeit und ein Ressourcenschonender Umgang mit Speicher und Rechenkapazitäten durch die passende Wahl des Technologiestacks gewährleistet ist.

Perfomance

High-Performance bei steigenden Workloads

Von der Architektur bis hin zum Code und der Auswahl von geeigneten Sicherheitsverfahren sind alle Elemente so gewählt und umgesetzt worden, dass selbst bei hohen Workloads oder Leistungsspitzen die Lösung als Ganzes performant und schnell bleibt.

Die zugrunde liegenden Verfahren und Kryptografie sind auch für energieschwache IoT-Geräte bestens geeignet. Durch den bidirektionalen und standardisierten Austausch von (IoT-) Ökosystemteilnehmern sind die Prozesse rund um die Authentifizierung und Autorisierung sowie die der Datenintegrität verschlankt.

Wirtschaftlichkeit

Die filancore Plattform ermöglicht auch bei hoher Skalierung und Ausdehnung des IoT-Ökosystems Wirtschaftlichkeit.

Die Plattform wurde so entwickelt, dass sie ressourcenschonend eingesetzt und ausgebaut werden kann. Durch einen Plug and Play Ansatz weißt sie geringe Integrationsaufwände in jede IT-Landschaft auf, egal ob im Rechenzentrum oder in der Cloud. Darüber hinaus wurde die Plattform so konzipiert, dass die Verwaltung bzw. Aufrechterhaltung des Betriebs (inkl. Wartung) geringstmöglich ausfällt und automatisiert gestützt wird, was zu Personaleinsparungen führt.

(3) Offen

Das filancore Identity Gateway sorgt für Interoperabilität, Übertragbarkeit und die Verwendung der offenen SSI-Standards. Bei der Plattform entsteht kein Vendor Lock-in!

Interoperabel

filancore ermöglicht es, mit verschiedensten Arten von (IoT-)Ökosystemteilnehmern in Interaktionen und Austausch zu treten.

Hierfür bietet das Identity Gateway die Fähigkeit, verschiedenste Attribute, Datenquellen und Richtlinien aus diversen Quellen zu verwalten bzw. sich auf diese mit anderen Teilnehmern zu einigen. Somit ist gewährleistet, dass eine ausgestellte SSI und Credentials auch in verschiedenen domänenübergreifenden Anwendungsbereichen nutzbar ist und somit unabhängig ist von Grenzen existierender Systeme. Dies ermöglicht eine unternehmensübergreifende Verifizierung und Austausch bzw. Zugriffe im (IoT-)Ökosystem.

Portierbarkeit

Das filancore Identity Gateway ermöglicht eine Übertragbarkeit von Identitäten und Credentials auf die eigene, als auch auf andere Plattformen und Ökosystemen, was Informations- bzw. Identitätssilos (Fragmentierungen) und Datenqualitätsproblemen reduziert.

Mit diesem Ansatz können vormals begrenzte oder geschlossene Systeme, wie unternehmensbezogene IoT-Netze, Datenbanken oder anderweitige Cluster „aufgebrochen" werden, da Zugänge zu diesen nicht mehr in individuellen, proprietär verwalteten Lösungen residieren. Eine Ökosystemübergreifende Nutzung und Zusammenarbeit wird erleichtert und auch andere Identitätsverfahren bzw. Systeme können integriert werden.

Offen

Das Identity Gateway folgt der SSI-Standardisierung und ermöglicht ein agnostisches (IoT)-Ökosystem, das hersteller- und technologieunabhängig ist und sich in bestehende Unternehmenssysteme integrieren lässt und so die Grundlage für ein kollaboratives und digitales (IoT)-Ökosystem bildet.

Ein entscheidender Aspekt der filancore-Plattform ist, dass es keine Herstellerbindung gibt, um dem IoT-Ökosystem beizutreten oder weiterhin daran teilzunehmen. Das bedeutet, dass keine spezifische Hardware oder Software eines bestimmten Anbieters erforderlich ist, um Teil des SSI-Ökosystems zu werden oder zu bleiben. Stattdessen basiert das Identity Gateway auf den W3C-Standards für Decentralized Identifiers (DID) und überprüfbare Verifiable Credentials (VC), um die Standardisierung von Datenformaten und Protokollen zu gewährleisten.

Diese Standardisierung ermöglicht es den Teilnehmern, ihre Identitätsdaten und Berechtigungsnachweise auf sichere und vertrauenswürdige Weise innerhalb des Ökosystems auszutauschen, ohne von einem bestimmten An-

bieter abhängig zu sein. So können die Teilnehmer ihre Identitätsdaten und Berechtigungsnachweise nahtlos nutzen und austauschen, unabhängig davon, welche Technologien oder Systeme sie verwenden. Die filancore-Plattform beinhaltet zudem eine No-Vendor-Lock-in-Politik, um Offenheit und Inklusivität zu fördern und die Zusammenarbeit und Innovation innerhalb der SSI-Community zu kultivieren, um innovative Lösungen zu entwickeln.

(4) Überraschend Einfach

Von der Integration über Betrieb und Wartung bis hin zur Anpassung an neue Bedürfnisse – das filancore Identity Gateway reduziert Komplexität und Aufwände in allen Belangen.

Flexibilität

Das Identity Gateway liefert eine leicht integrierbare und flexible Plattform für den Aufbau von IoT-Ökosystemen.

Sowohl bei klassischen Identitäts- und Zugangssystemen, als auch bei modernen SSI-gestützten Lösungen, die interne IT-Integration bis hin zum Status „Betriebsbereit“ kann schnell eine komplexe Aufgabe mit hohen Aufwänden werden. Die Plattform bietet hierfür einen flexiblen Plug and Play Ansatz, der geringe Integrationsaufwände in jegliche IT-Landschaft verspricht, egal ob im Rechenzentrum, in der Cloud oder anderen heterogenen Umgebungen wie bspw. einer Produktionslinie. Auch Anpassungen an sich ändernde Bedürfnisse der Endbenutzer oder IT-Anforderungen können schnell erreicht werden, wodurch geringere Aufwände sowie Personaleinsparungen entstehen. Erreicht wird dies durch die Trennung der Plattform in Funktionsblöcke, die modular entwickelt wurden.

Frictionality

Eine nahtlose und überzeugende Erfahrung für (Cybersecurity-)Administratoren und Anwender der Plattform.

Zeitaufwändige und manuelle Administrations- und Wartungsarbeiten zur Erreichung bzw. Aufrechterhaltung des Betriebs, sowie Funktionsfähigkeiten des IoT-Ökosystems sind typische Herausforderungen für die sogenannte „Plattform-Verantwortliche“. Um diesem Leidensdruck zu begegnen, unterstützt das Identity Gateway als Identität- und Zugangsplattform bei Serviceunterbrechungen, Technologieausfällen oder bei der Vermeidung von Cyber-Angriffen. Hierfür wurde die Plattform so konzipiert, dass der Administrations- und Wartungsaufwand kleinstmöglich gehalten wird, ohne den Betrieb dabei unterbrechen zu müssen. Die Verantwortlichen erhalten eine automatisiert gestützte und intuitive Konfiguration der Plattform, ein übersichtliches Live-Dashboard über den Status quo, als auch bei kritischen Er-

eignissen eine adäquate Fehlermeldung für eine zielgerichtet schnelle Ursachensondierung und Beseitigung der Störungsquellen.

Usability

Überraschend einfache, intuitive und übersichtliche Handhabung und Teilhabe für viele und diverse Arten von IoT-Ökosystemteilnehmern.

Herkömmliche Identitäts- und Zugriffssysteme weißen häufig eine schwierige Anwendung auf, da komplexe kryptografische oder IT-relevante Verfahren und Protokolle, sowie Berechtigungsregeln und Beziehungen nicht ausreichend genug für den Anwender abstrahiert und dargestellt werden. Es entsteht schnell ein unzureichendes Verständnis, eine Unübersichtlichkeit, und somit auch Fehlerquellen im Umgang mit sensiblen Daten, die schlimmstenfalls auch zu Angriffsflächen für Außenstehende werden können. Das filancore Identity Gateway ermöglicht ein selbstbestimmtes Identitätsmanagement verschiedener IoT-Ökosystemteilnehmer. Ein Alleinstellungsmerkmal ist jedoch auch die Ausrichtung auf eine enorm hohe Anzahl von IoT-Geräten und heterogener Systeme, die intelligent über ihren gesamten Lebenszyklus, von der Erstellung von Identitäten und Credentials bis hin zum End-of-Life, verwaltet werden können. Der Anwender erhält zu diesem Zweck automatisierte Funktionen, eine intuitive Bedienoberfläche und Führung in der Plattform für manuelle Tätigkeiten, damit jeder IoT-Ökosystemteilnehmer identifiziert, gruppiert, sowie für bestimmte Interaktionen berechtigt und überprüft werden kann.

Auch für die IoT-Ökosystemteilnehmer selbst können Vorteile im Umgang mit Identitäten und Credentials entstehen. So können insbesondere für Personen unbequeme Authentifizierungen abgelöst und (teil-)automatisiert werden, da diese nicht mehr gezwungen sind (meist schwache) Passwörter zu verwenden bzw. diese sich zu merken. Darüber hinaus können positive Erfahrungen im Zusammenhang mit dem IoT-Ökosystem entstehen, da die Prozesse zur Authentifizierung und Autorisierung für alle Teilnehmer transparent, vertraut und systemübergreifend „schlank“ bleiben und Identitäten in anderen Ökosystemen weiterhin genutzt werden können. Ein erneutes Onboarding bzw. eine ständige Identitätsprüfung, z.B. via Post-Ident, entfällt somit komplett.

Version 1.1, März 2023

www.filancore.com
info@filancore.com