filancore

Identity Gateway – Decentralized Identity and Access Management for IoT

Whitepaper

Version 1.2, March 2023

www.filancore.com

info@filancore.com

Table of contents

Abstract

The filancore Identity Gateway is an Identity and Access Management (IAM) platform for the Internet of Things (IoT) based on **Self-Sovereign Identity (SSI)**.

The goal of filancore is to make both the management of digital identities - over their entire lifecycle - and (access) policies for these identities simple to use and secure at the same time.

The target group and focus of the platform are organizations that potentially need to issue and manage a significant amount of these identities and related credentials. Manufacturers of Internet of Things (IoT) devices - smart sensors and actuators - who want to give each of their devices its own identity and need a scalable and efficient solution to do so, are a case in point.

The foundation on which filancore is built consists of highly innovative technologies such as the **W3C standard** for **decentralized identifiers (DIDs)**, **verifiable credentials (VCs)**, and **distributed ledger technology (DLT)**. The identities are agnostic with regard to their subjects and can accordingly be used to authenticate and authorize organizations, people, machines, devices, services, applications and much more. These technologies thus enable a highly interoperable next-generation digital ecosystem.

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

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

With the rise of the Internet of Things, organizations operating in this space are facing new challenges. Identity and access management (IAM) for IoT becomes a fundamentally critical component of IT security for these organizations and is inextricably linked to digital efficiency. In this context, the aspects of security, scalability, openness and simplicity can no longer be fully managed with traditional systems and procedures in the context of IoT.

Self-Sovereign Identity (SSI) is a holistic problem solver in the field of digital identities and offers numerous advantages that filancore is able to apply to the challenges of the Internet of Things (IoT). On the basis of the standard for self-sovereign identities published by the World Wide Web Consortium (W3C), we are seeing the emergence of a digital, decentralized ecosystem inspired by the ideas of a „Web of Trust“, in which the owner of a digital identity - whether human, machine or organization - is given full ownership and control over the use of this identity and any associated personal data. Furthermore, filancore sees SSI as a secure and interoperable way to realize decentralized identity and access management for use cases in the IoT and to create new business models in which networked systems, machines, devices and sensors play an increasingly important role.

filancore‘s vision is to overcome these challenges and unfold the potential of IoT for organizations using SSI. The team around filancore has therefore set itself the goal of making SSI and the underlying highly innovative technologies such as the W3C standard for Decentralized Identifiers (DIDs), Verifiable Credentials (VCs) and Distributed Ledger Technology (DLT) easily retrievable and usable for organizations in the field of IoT. Therefore, since 2019, the filancore Identity Gateway - an SSI-based Identity and Access Management (IAM) platform - has been developed and refined with selected test and pilot customers to ensure that the needs of the industry and its security requirements are met for enterprise as well as cross-enterprise IoT use cases.

The filancore Identity Gateway facilitates the creation and management of trusted IoT ecosystems along the security lifecycle by providing participants, whether a few or hundreds of thousands of organizations, people, machines, devices, services, applications, etc., a public and decentralized identity, as well as controllable permissions or credentials. In this process, an advantageous emergent identity layer is established, which leads to the fact that traditional, centralized authentication and authorization mechanisms are increasingly supplemented and prospectively replaced by decentralized methodologies. The advantage of these decentralized authentication and authorization mechanisms is that they can operate a heterogeneous environment and enable an open IoT ecosystem by protecting against compromise, misuse as well as single-point-of-failures. At the same time, these technologies also offer brokering properties that lead to network effects for organizations

and the IoT ecosystem, by allowing a large number of new participants, e.g., additional partners or external devices and services, to be integrated for mutual benefit in a controlled manner and more effective interactions.

These properties can be achieved and managed along the entire life cycle of identities, from the registration process and on-boarding, e.g. in end-of-line production for devices, through controlled operation in the desired target environment with a wide range of stakeholders, to end-of-life. The filancore Identity Gateway acts as a trusted ecosystem enabler for use cases where, for use cases where

- evidence or proof of authenticity is required, for example, to establish that a device is an original from the manufacturer;
- an IoT device or participant in the IoT ecosystem must be verified to ensure that the device or participant is who it says it is;
- Access or authorizations for devices and systems must be set and controlled to ensure only authorized interactions, even across companies;
- the generation, exchange, and verification of trusted data is necessary, e.g., when a recipient wants to verify the authenticity and data integrity of a sensor data point within a data marketplace.

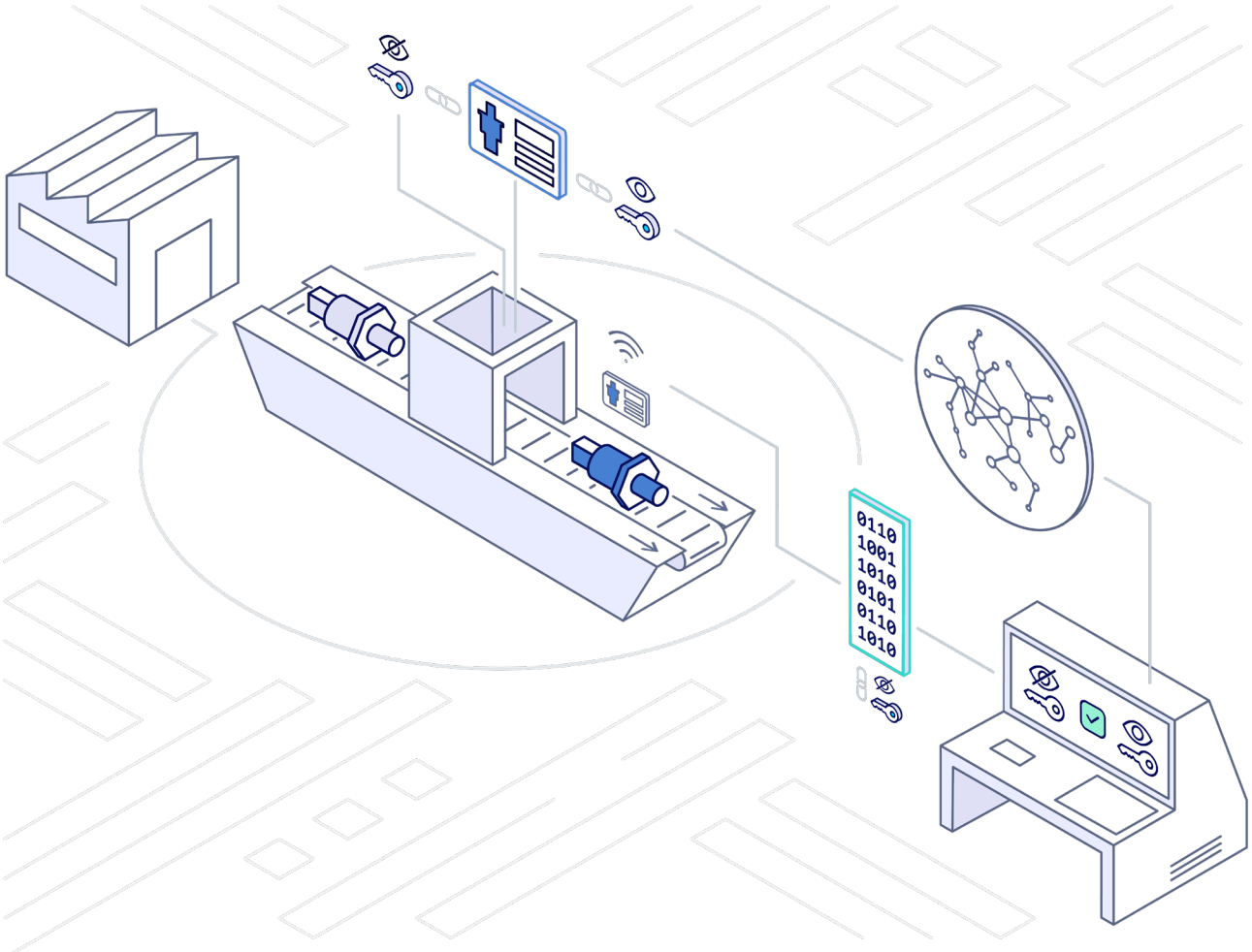
In short, users of the filancore Identity Gateway can thus

- create large numbers of self-sovereign identities with little effort or register already existing identities in the platform;
- automatically or manually anchor controlled identities in various DLTs or other networks to make them globally usable;
- manage, search, sort, and group identities, link them to other entities, and assign aliases;
- verify other identities or participants (e.g., IoT devices) in the ecosystem to ensure that the participants are who they say they are;
- issue evidence or proofs of authenticity (VCs) on the basis of a practical template system and manage, search, (re)name, sort and group them in the same way as identities.
- verify third-party proofs, e.g., to determine that a device is original to the manufacturer;
- enable the generation and exchange of trusted IoT data, e.g., when a receiver wants to verify the authenticity and data integrity of data based on the identity of the creator of the data (e.g., a specific sensor);
- set up and manage access or permissions for participants and target systems to allow only authorized interactions in the ecosystem (even across organizations);
- create and manage templates that facilitate mass creation of identities and proofs and allow standardization of processes;
- manage and monitor the entire underlying infrastructure such as DLT nodes for anchoring identities, hardware security modules for storing private key material, and file system and database nodes for storing identity documents in an automated, simple manner and without any programming knowledge;

The filancore Identity Gateway as an Identity and Access Management (IAM) platform supports IoT ecosystems as a secure foundation for collaborative use cases by establishing and ensuring end-to-end identification of each participant, access rules and policies, required credentials, and trusted data transmission.

(1) Trusted IoT Data & Data Integrity

With the Identity Gateway, IoT use cases can be realized where the immutability and validity of IoT data must be ensured over the entire lifecycle, especially if this data is sensitive or required for further use, for example for a sale in a data marketplace. The platform provides mechanisms for establishing and verifying the authenticity and integrity of data for this purpose, which increases its value and trust in relevant data.



How can this be achieved?

Technically, this is achieved by giving the IoT device its own self-sovereign identity via the filancore Identity Gateway, in the best case already in production (end-of-line) for security reasons. Optimally, this is done by “hardwiring” the secret key corresponding to the identity on a suitable security chip (e.g. HSM or TPM). Alternatively, e.g. for low-power devices, this can be held by the next closest unit (e.g., an IoT gateway) or, for less critical IoT devices, in a software security module or secure software environment. The correlating public key is automatically anchored on the public distributed ledger by the Identity Gateway.

The IoT device can now use this identity to autonomously and verifiably sign the data it sends out with the identity’s private key. The signing function is usually supported natively by the security chip, alternatively this can be replicated by software on the IoT device.

The recipient, whether a person, an organization or another IoT device, is now able to verify the authenticity and origin of the data by checking its validity against the publicly visible part of the IoT device’s identity on the distributed ledger (or the verifiable data register). For this purpose, the signature of the received data, i.e. the signature with which the IoT devices have signed the sent data, is cryptographically matched. If there is a match, the recipient can be sure that the data received originates from the IoT device in question and that the data has not been manipulated. This gives the data a verifiable value for the recipient.

(2) Authentication

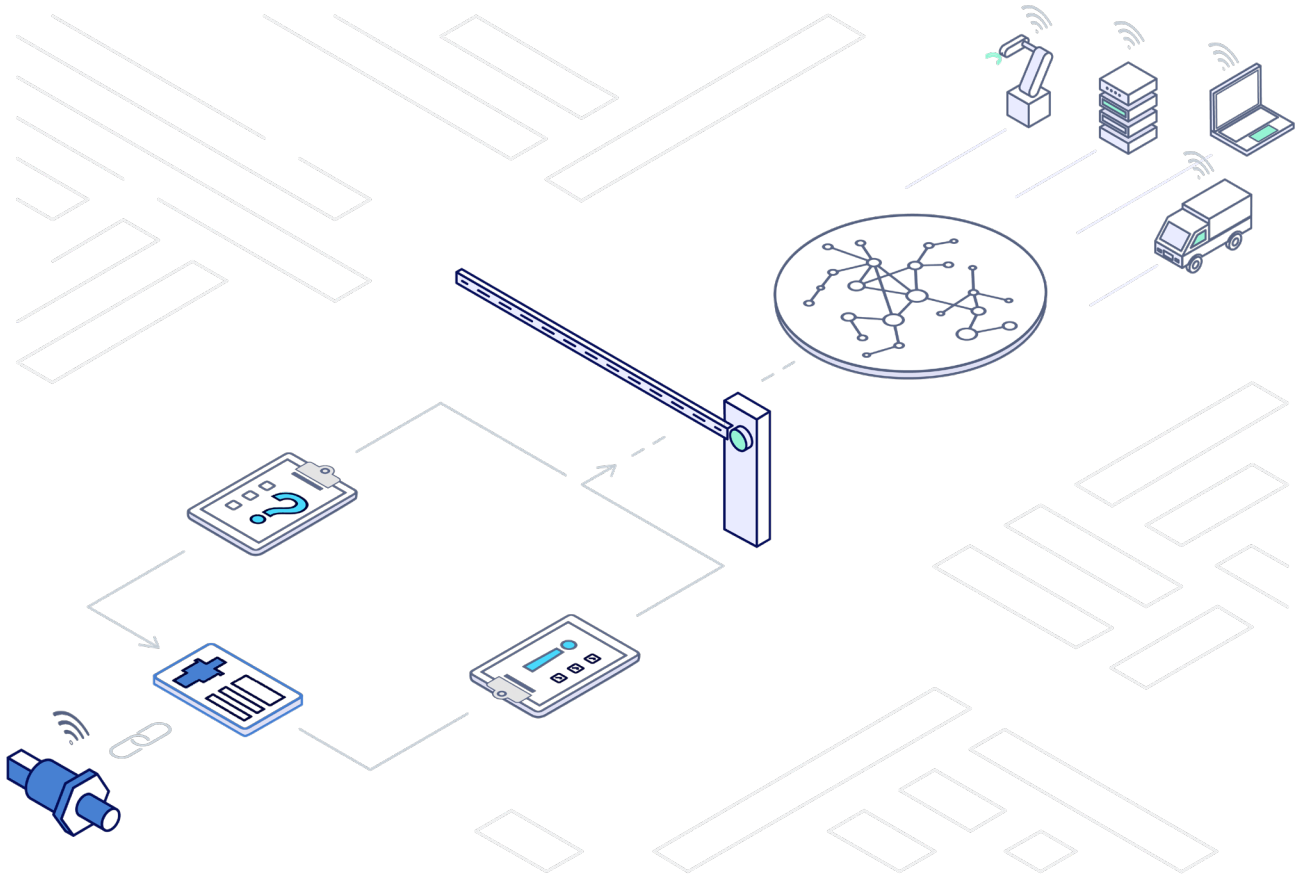
In (IoT) ecosystems, it is necessary for participants (persons, organizations, or such as IoT devices) to be able to authenticate each other for specific use cases (e.g. an IoT device at a specific service point) in order to enable trustworthy multilateral interaction or communication. Authentication is used to prevent unauthorized third parties from gaining access to the (IoT) ecosystem and its data or functions. This is also relevant for the zero trust concept, in which every data access is initially classified as untrustworthy, regardless of whether the request is made inside or outside the company network.

How can this be achieved?

Authentication represents the actual verification of the identity claimed by the counterpart, checking whether the participant is really in possession of the identity or communicated characteristics. The filancore Identity Gateway

supports this procedure by giving a participant an identity that can be verified by third parties, e.g. if an (IoT) ecosystem participant in the form of an IoT device wants access at a service point, the verifier, within the ecosystem.

Authentication is performed using a challenge-response procedure in which the verifier presents the participant with a task that only the owner of the identity is capable of solving. If the participant successfully solves the challenge, they are considered authenticated by the verifier. Since this procedure is based on established cryptographic standards, it offers a high degree of security against unauthorized access.



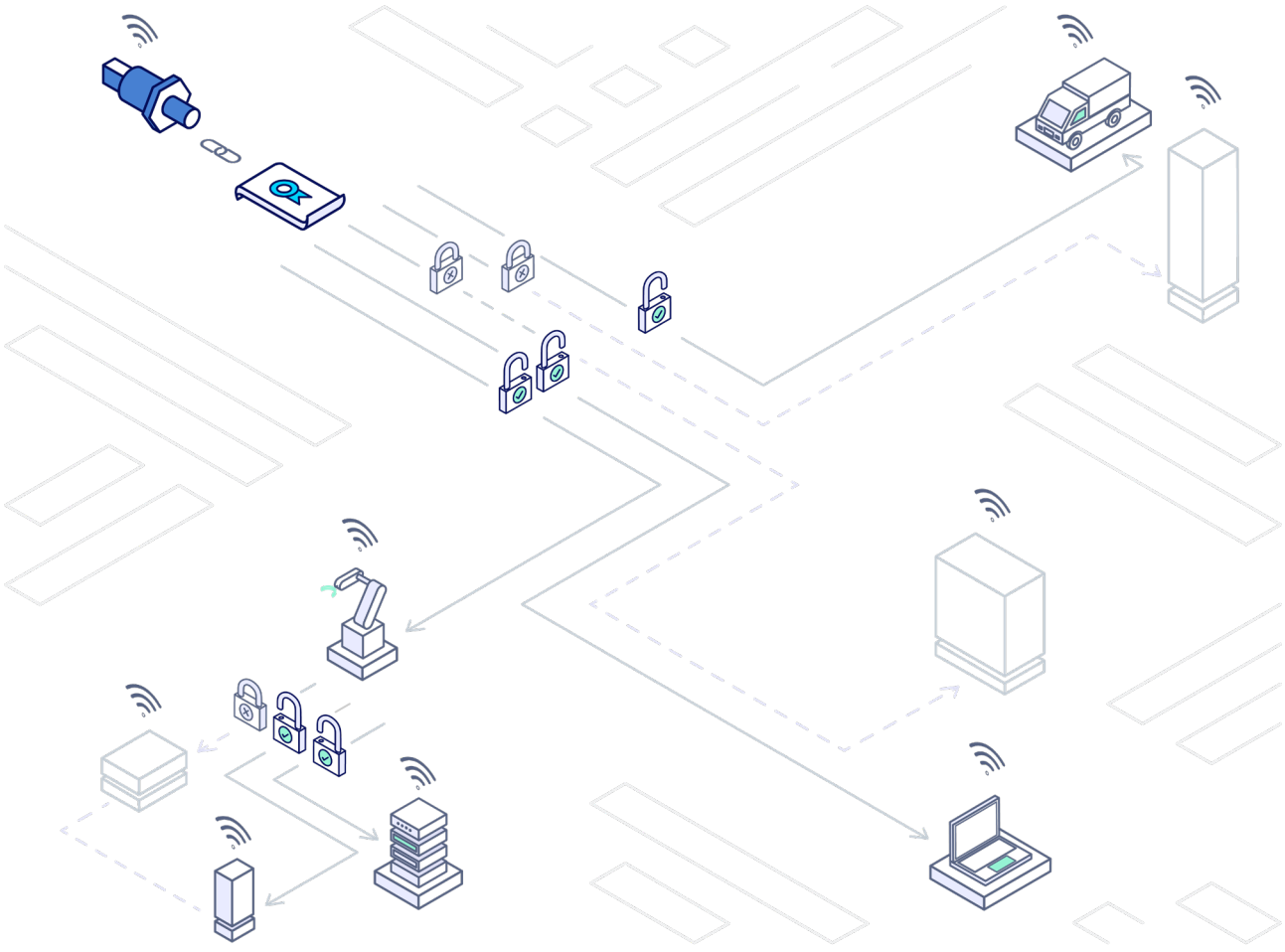
(3) Authorization

Authorization can be used to additionally check and grant or deny certain access rights and privileges in the (IoT) ecosystem after successful authentication, if certain access points, data and functions require a separate level of security.

How can this be achieved?

Using the Identity Gateway, policies can be created and issued to ensure controlled access to applications, systems or data resources or even other IoT devices in the IoT ecosystem. For example, the policies determine which resources, functions, or other IoT systems a participant (e.g., an IoT device itself) has access to.

Here, access rights can be standardized, defined, and issued in the form of verifiable credentials and templates, granting participants certain privileges and accesses, even across companies. This access management can also be role-based according to a so-called “Role-Based Access Control (RBAC)” model.

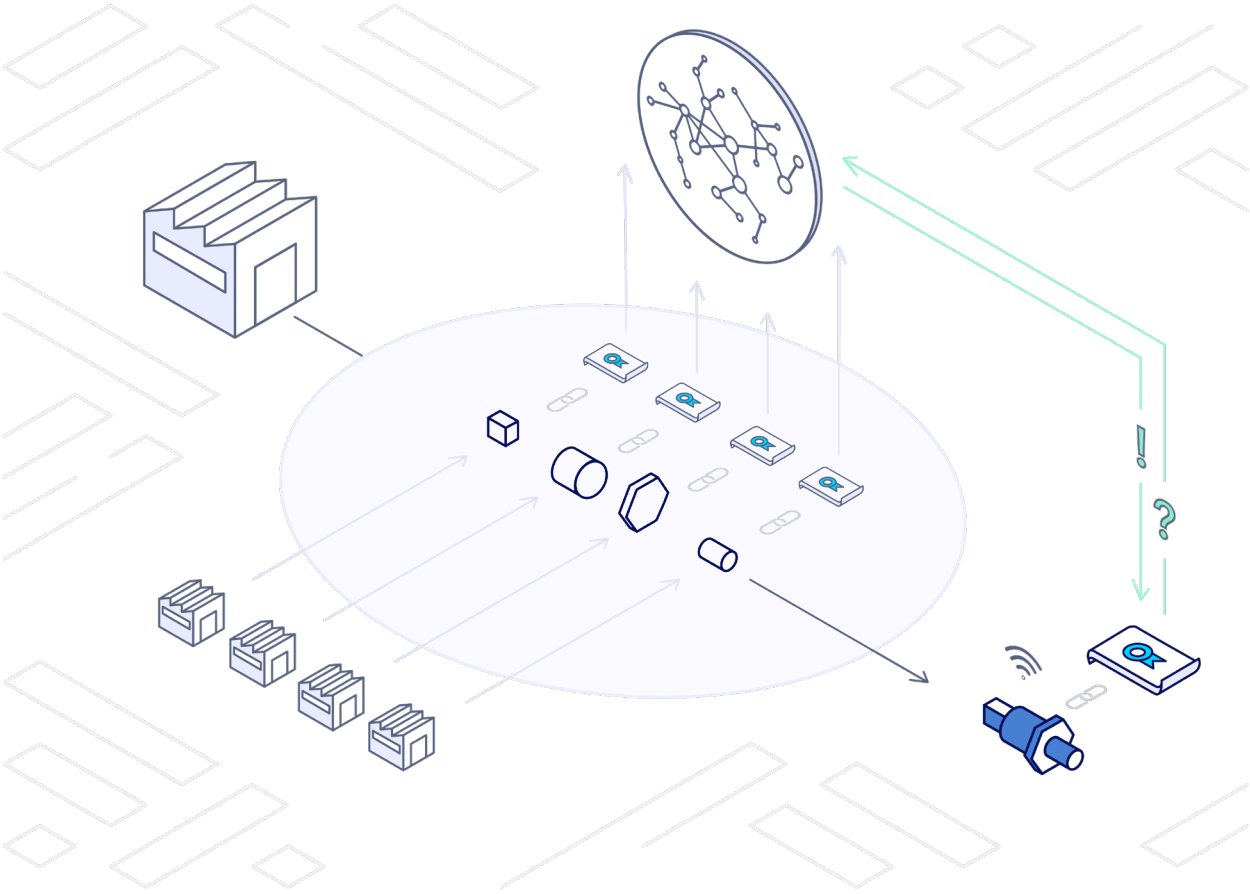


Here, users are assigned roles or groups, which in turn are assigned certain access types and restrictions.

(4) Proof of Origin

Verifiable evidence in digital form is increasingly necessary, especially to combat counterfeit products on the market for IoT components, as buyers of counterfeit devices often associate poorer quality with the original brand or manufacturer. This lower quality standard not only damages the brand image but also results in lost sales when bad experiences are shared with others.

However, the damage to the image is not the only concern; the fight against counterfeit products is also costly, especially when lawsuits have to be defended. Original equipment manufacturers can easily ensure providing traceable proof of an IoT component produced in their own factory, such as to better defend claims relating to quality and safety defects, which can be costly if lawsuits have to be defended.



How can this be achieved?

Manufacturers of IoT components can use the Identity Gateway to issue a verifiable credentials signed by the manufacturer and attached to the component during production, anchoring it there automatically and securely.

This verifiable credential cryptographically confirms the origin and authenticity of the component and can contain any other proof, as well as customer- or product-specific attributes, depending on the manufacturer's requirements. Third parties and the manufacturer can thus verify the authenticity of the component at any time, especially in the event of a complaint.

Key Benefits

The use cases around the Internet of Things present tremendous opportunities for businesses. However, in many cases, the use of the IoT can be slower than anticipated due to requirements that are difficult to achieve. This is where the filancore Identity Gateway comes in, to provision, monitor, manage, and control self-sovereign identities for building IoT ecosystems. The platform helps focus on the essential business model of a company and address security issues among IoT participants, whether people, organizations, devices, systems, or services of a potentially large number and variety.

(1) Secure

Minimization of attack surfaces, data breaches, misuse of data, as well as non-compliance in the area of IoT security and data protection (e.g. GDPR).

Decentralization

Reduced dependencies, more control, and resilience.

Behind traditional identity solutions and services are often centralized systems under the control and influence of third parties, leading to technical dependencies. This can lead to a so-called "single point of failures" in critical use cases, where users are exposed to the arbitrary or unintentional decisions and actions of third parties. Ownership of identities, authorizations and underlying sensitive information also ultimately remains with these third parties, making these central constructs predestined for attack and misuse.

The Identity Gateway and the underlying SSI principles help users to decentralize and democratize identity and access systems in the future by creating greater independence from centralized third-party systems and services. This is achieved by shifting ownership of identities to the identity holders

and using decentralized identity registers as identity anchors in the form of distributed ledgers.

This creates censorship resistance and independence from third parties for the user, as well as highest levels of resilience through decentralized anchoring of critical identities and credentials. IoT ecosystem participants can also be enabled to authenticate and authorize themselves bidirectionally and transparently, or to directly check the integrity of transmitted data from third parties.

Compliance

Compliance with regulations regarding data protection, as well as IT and IoT security.

The achievement of data protection requirements and controls in the area of IT and IoT security standards are and will increasingly become mandatory for IoT products and IoT ecosystems. The Identity Gateway enables the use of self-sovereign identities for this purpose, which are considered data protection compliant due to their data minimization and ownership principle, as the storage and disclosure of sensitive identity data and attributes are the responsibility of the identity owner. In addition, only standardized cryptographic procedures and protocols based on public and private keys are used and provided, which generally achieve a complete or high degree of coverage in typical control domains of security standards such as “identity and access management” and data integrity.

(2) Scalable

The filancore Identity Gateway has been developed to meet the requirements of the IoT while also achieving the highest possible scalability and performance.

Scaling

With the Identity Gateway, large numbers of identities, credentials, or authorizations can be issued and managed effectively at any time.

This is ensured by the choice of underlying technologies and extensive automation. Another factor is the choice of the underlying distributed ledger as the identity repository. This can handle enormously large transaction volumes and is capable of processing workloads simultaneously, which contributes significantly to horizontal scalability.

During the development of the platform, attention was also paid to ensuring high scalability and resource-saving use of memory and computing capacity

through the suitable choice of technology stack.

Perfomance

High performance for increasing workloads.

From the architecture to the code and the selection of appropriate security procedures, all elements have been chosen and implemented in such a way that even with high workloads or performance peaks, the solution as a whole remains efficient and fast.
The underlying procedures and cryptography are also ideally suited for low-power IoT devices. The bidirectional and standardized exchange of IoT ecosystem participants streamlines the processes around authentication and authorization, as well as those of data integrity.

Economic efficiency

The filancore platform enables economic efficiency even with high scaling and expansion of the IoT ecosystem.

The platform was developed in such a way that it can be deployed and scaled in a resource-efficient manner. Thanks to a plug-and-play approach, it requires little integration effort in any IT landscape, whether in the data center or in the cloud. In addition, the platform has been designed in such a way that the administration, maintenance, and operations are kept to a minimum and supported automatically, resulting in personnel savings.

(3) Open

The filancore Identity Gateway ensures interoperability, portability and the use of open SSI standards. A vendor lock-in does not occur!

Interoperable

The platform makes it possible to interact and exchange data with various types of IoT ecosystem participants.

For this purpose, the Identity Gateway provides the ability to manage or agree on various attributes, data sources, and policies from diverse sources with other participants.
This ensures that issued SSIs and credentials can also be used in different application domains and are therefore independent of the boundaries of existing systems, enabling cross-enterprise verification and exchange or access in the IoT ecosystem.

Portability

The filancore Identity Gateway enables the portability of identities and credentials across platforms and ecosystems, reducing fragmentation of information and identity silos and data quality issues.

With this approach, previously limited or closed systems, such as enterprise IoT networks, databases, or other clusters, can be "opened up" because access to them no longer resides in individual, proprietary managed solutions, facilitating cross-ecosystem use and collaboration and enabling integration with other identity methods.

Open

The Identity Gateway follows SSI standardization and enables an agnostic (IoT) ecosystem that is vendor-neutral, technology-independent, and integrates with existing enterprise systems, forming the foundation of a collaborative and digital (IoT) ecosystem.

A crucial aspect of the filancore platform is that there is no vendor lock-in to join or continue to participate in the IoT ecosystem. This means that no specific hardware or software from a particular vendor is required to become or remain part of the SSI ecosystem.
Instead, the Identity Gateway is based on the W3C standards for Decentralized Identifiers (DID) and Verifiable Credentials (VC) to ensure standardization of data formats and protocols. This standardization allows participants to share their identity data and credentials within the ecosystem, without depending on a particular vendor, enabling participants to seamlessly use and share their identity data and credentials regardless of which technologies or systems they use. The filancore platform also includes a no-vendor-lock-in policy to promote openness and inclusivity, and cultivate collaboration and innovation within the SSI community to develop innovative solutions.

(4) Surprisingly simple

From integration to operation and maintenance to adaptation to new needs - the filancore Identity Gateway reduces complexity and effort in all respects.

Flexibility

The Identity Gateway provides an easily integrated and flexible platform for building IoT ecosystems.

For classic identity and access systems as well as for modern SSI-based solutions, the internal IT integration up to the status "ready for operation" can quickly become a complex task with high expenses. The platform offers a

flexible plug and play approach that promises low integration efforts in any IT landscape, whether in the data center, in the cloud or other heterogeneous environments such as a production line. Adaptations to changing end-user needs or IT requirements can also be achieved quickly, resulting in lower effort as well as personnel savings. This is achieved by separating the platform into functional blocks that have been developed in a modular fashion.

Frictionality

A seamless and compelling experience for (cybersecurity) administrators and users of the platform.

Time-consuming and manual administration and maintenance work to achieve or maintain operation, as well as functional capabilities of the IoT ecosystem are typical challenges for responsible persons. To address this suffering, the Identity Gateway provides support as an identity and access platform in the event of service interruptions, technology failures or cyber-attack prevention. For this purpose, the platform was designed to keep administration and maintenance efforts to a minimum without having to interrupt operations. The responsible persons are provided with an automated and intuitive configuration of the platform, a clear live dashboard about the status quo, as well as an adequate error message in the case of critical events for a targeted, rapid investigation of the cause and elimination of the source of the malfunction.

Usability

Surprisingly simple, intuitive and clear handling as well as sharing for many and diverse types of IoT ecosystem participants.

Conventional identity and access systems are often difficult to use because complex cryptographic or IT-relevant procedures and protocols, as well as authorization rules and relationships, are not sufficiently abstracted and presented to the user. This quickly results in insufficient understanding, a lack of clarity, and thus also sources of error when dealing with sensitive data, which in the worst case can also become attack surfaces for outsiders. The filancore Identity Gateway enables self-sovereign identity management of various IoT ecosystem participants. However, a unique selling point is also the focus on an enormously high number of IoT devices and heterogeneous systems that can be intelligently managed throughout their lifecycle, from the creation of identities and credentials to end-of-life. To this end, users are provided with automated functionality, an intuitive user interface, and guidance in the platform for manual activities so that each IoT ecosystem participant can be identified, grouped, and authorized and verified for specific interactions.

There may also be advantages for the IoT ecosystem participants themselves in dealing with identities and credentials. For example, authentica-

tion processes that are inconvenient for people in particular can be replaced and (partially) automated, as they are no longer forced to use (usually weak) passwords or to remember them. In addition, positive experiences can arise in the context of the IoT ecosystem, as the processes for authentication and authorization remain transparent, familiar and “lean” across systems for all participants, and identities can continue to be used in other ecosystems. Re-boarding or constant identity verification, e.g., via know-your-customer-identification procedures, is thus completely eliminated.

Version 1.2, March 2023

www.filancore.com
info@filancore.com