Info brochure

SIGNiT® provides data integrity for multi-party IoT ecosystems

The Internet of Things (IoT) is increasingly prevalent in our daily lives within new areas such as smart cities, autonomous cars, industry 4.0 and products as a service, where sensors and remotely controlled systems are becoming a standard. In most cases, the question whether the sensor data can be trusted is core to the business model. If the data to operate is not trustworthy the entire application is at risk. The overall functionality of SIGNiT® is to provide data integrity within the IoT ecosystem via digital signing of data generated by an IoT device. The signed data is placed in a blockchain for a posterior data integrity verification for any third party involved in the IoT application ecosystem.

IoT security today

"State of the art" IoT security does not ensure trustworthy data & integrity. Only the data transmission is protected. Typically there is no protection against where and how data is generated. Therefore, data can easily be manipulated or deleted before it reaches the backend server.

Out-of-the-box security is not enough

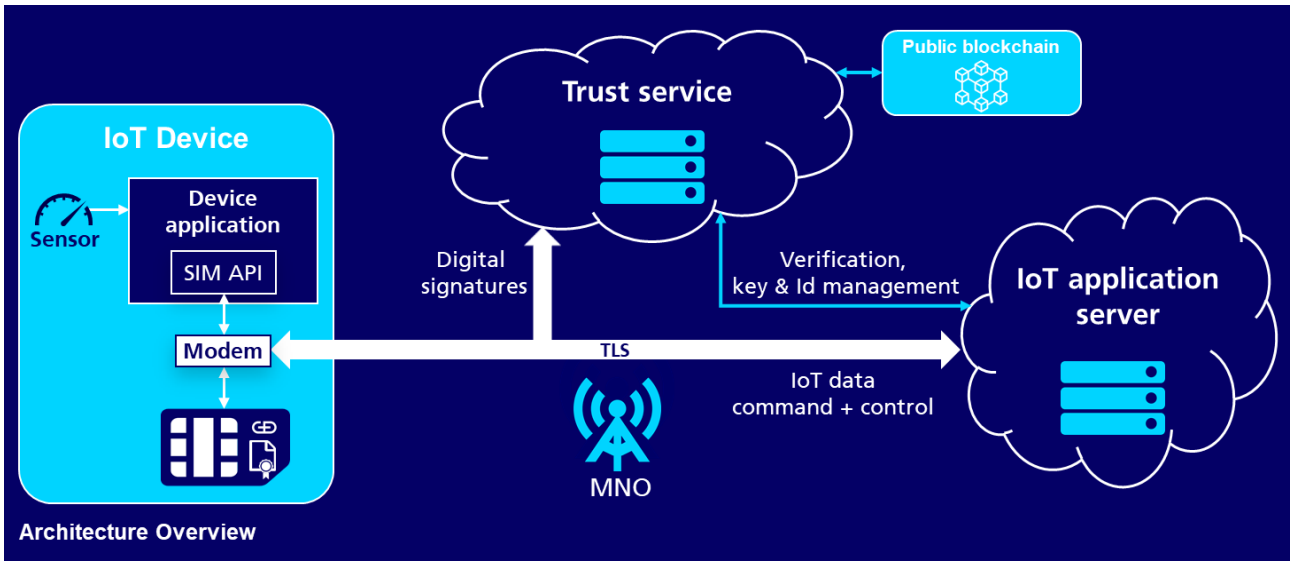
IoT devices communicate to the server application via Transport Layer Security (TLS). Therefore the communication channels are secured by encryption. However, this does not protect the data outside the communication channel, at the IoT device or at the backend and the data could be manipulated.

SIGNiT® uses blockchain technology to ensure data integrity

The solution works like a blockchain that starts right from the source of data-creation – the IoT sensor. IoT data is sealed by a private key that sits on the G+D SIM-Card. In the backend these micro-certificates are then stored and anchored in public blockchains, thus creating an immutable and irrefutable record of that sensor. The benefits for clients are huge – as IoT data can be verified whenever it is processed or new data-driven business models like smart contract insurances can be deployed. A prevention for major hacking attacks like "man in the middle" or packet duplication / suppression is also a built-in feature, as only verifiable packets are processed.

SIGNiT® uses elliptic curves (ECC) as a means for resource optimized asymmetric cryptography. This process is far superior regarding speed and resources compared to traditional RSA based cryptography without any significant drawbacks in security.

The data is sealed by the SIM directly at the time of creation



Value proposition – Use cases

The SIGNiT® solution can be used for multiple use cases not limited to the list below:

- **Proof of origin** for manufactured parts e.g. by storing serial number or other identifiers of the used components and parts
- **Digital twin** production related data can be shipped with the product. Different production sites can rely on data and fully automize production across the chain i.e. final product assembly can be based on trustworthy information about parts
- **Proof of work** – to guaranty that e.g. a critical production step has been performed correctly i.e. reduced liability
- **Predictive maintenance** – to verify reliable data on machine status i.e. increased uptime, decreased efforts
- **Tracking and tracing** of data about handling and treatment during transport and storage
- **Smart insurance** e.g. by automated regulation of insurance cases

SIGNiT® is winner of the IoT GLOBAL AWARDS 2020

IoT GLOBAL AWARDS 2020 WINNER

SIGNiT®: "Innovative and solving real IoT issues."

SIGNiT® provides data reliability in an IoT ecosystem where multiple parties must rely of the data. It ensures there is no possibility of data manipulation or deletion by storing digital signatures of the data in a public blockchain.

The solution is simple to integrate in a IoT end-to-end application where data integrity is important for the success of the business application.

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

mobilesecurity@gi-de.com
www.gi-de.com

Follow us on: