LEGIC

White paper

Establishing Trust in the Industrial IoT – Security by Design

Authors: Anthony Fitze, Carl Fenger, LEGIC Identsystems

Trust in IIoT data relies on linking verified users with trusted sensors and objects so that their interactions are reliable, transparent and accountable.

Summary

Abstract: The IIoT promises to optimize processes, lower costs, enhance quality, safety, accountability and service availability. Achieving these goals depends on an IoT platform's ability to support user accountability by securing their interactions with sensors, assets and infrastructure. Only then can reliable, transparent and auditable business processes be achieved. "Security by Design" creates trust and can be established through Mobile Credentialing, Managed Encryption and Secure Element technologies.

Securing the Industrial Internet of Things

In industrial environments, mass deployment of sensors and the ability to gather and process data from fixed and mobile assets significantly increases efficiency and enables better business decisions. It makes it easier to streamline processes, reduce errors, support auditing and enforce quality control that would otherwise be carried out on an ad-hoc or statistical sampling basis.

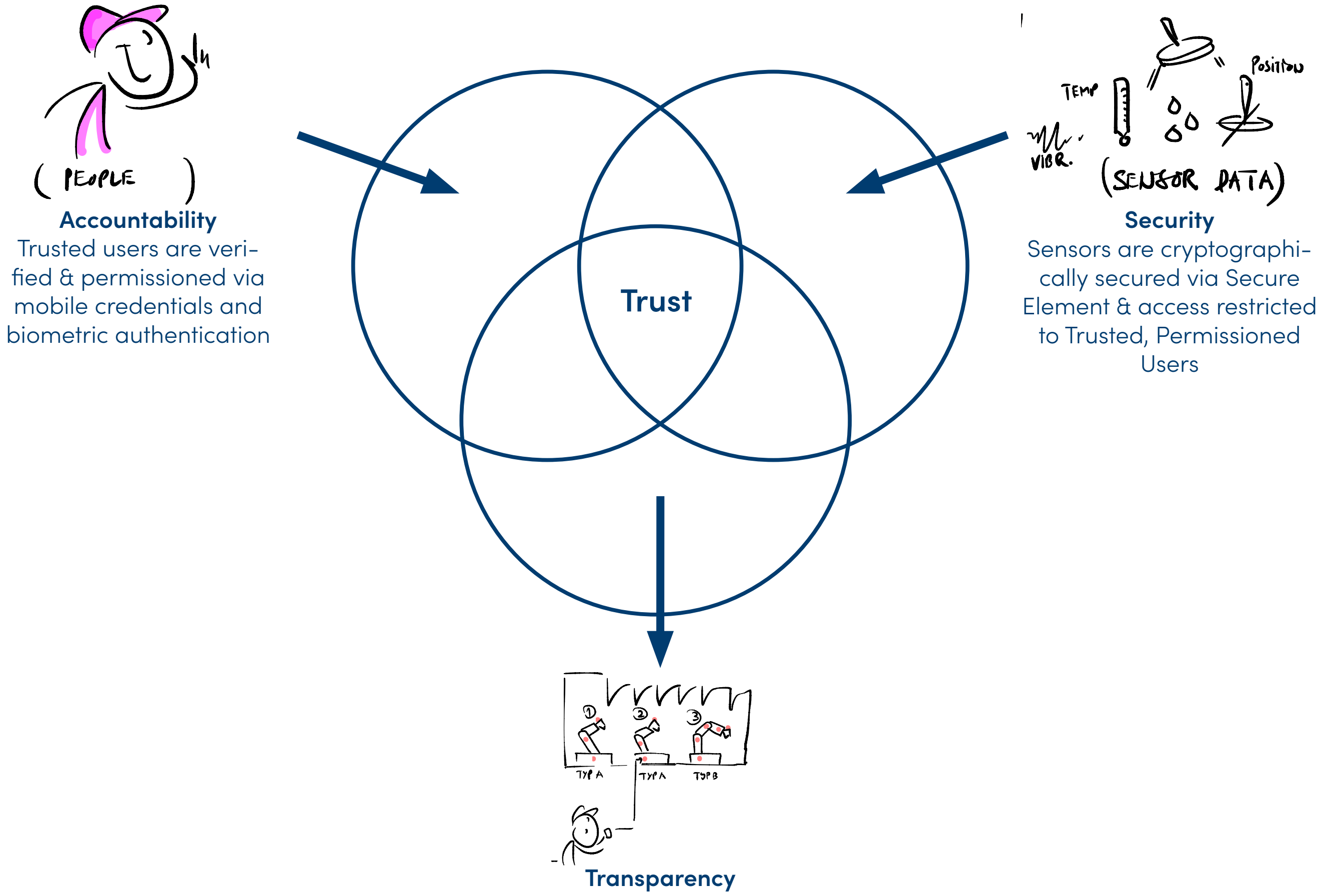
The common denominator: Trust
Simply connecting sensors to the internet is not enough. The viability of processes improved by the "Industrial Internet of Things" depends on a common denominator: Trust. Without the ability to trust data, sensors and the people who access, configure and service them, IIoT deployments lose their effectiveness. If users, sensors/objects and their interactions cannot be trusted, the results can be misleading, costly and even catastrophic, especially in environments where valuable or volatile assets and human safety are involved, which is often the case.

The Three Pillars of Trust in the Industrial IoT (IIoT)
Being able to trust in IIoT data relies on linking verified users with trusted sensors/objects so that their interactions are reliable, transparent and accountable. Accomplishing this relies on the following three principles:

1. Accountability: users in an IIoT environment must be identifiable and thereby accountable before gaining access to sensors or infrastructure. Access permissions must then be assigned based on a user's role, training and associated authorization as well as context-based criteria such as time, location, environmental data and other attributes required to support and secure operations . Permissions must be autonomously enforced, both online and offline, to minimize human error and support reliable 24/7 operation. All user activities must be transparent and auditable.

2. Security: equipment must only allow configuration and access by authorized permissioned users. Devices must also be immune to spoofing. As sensors are the most exposed, and hence vulnerable component of an IIoT system, physical hardware-level security must be implemented in the form of an embedded Secure Element for hosting of encryption keys and user permissions.

3. Transparency: interactions between users and devices and the data they generate must be trustable and transparent to validated users. They must not be visible to, nor subject to manipulation or interception by unauthorized parties either at the sensor, along local area networks, air interfaces or over the network, including the publicly available internet.



Accountability
Trusted users are verified & permissioned via mobile credentials and biometric authentication

Trust

Security
Sensors are cryptographically secured via Secure Element & access restricted to Trusted, Permissioned Users

Transparency
Sensor data and user interaction is trusted, transparent, reliable and secured through end-to-end managed encryption

Pillar 1: Accountability
To establish accountability, IIoT system users must be verified to establish trust. Permissions to access areas, machines, functionalities, vehicles, information and storage must be granted based on each trusted user's credential. Credentials can define where a user is allowed to go and when, what machines and their functionality are allowed to be used based on their training and function, which lockers and storage containers can be opened, etc.

Users change regularly – employees come and go, change job function or complete trainings on a daily basis. External staff such as auditors or contractors require ad-hoc credentials on a time-limited basis. Permissions must therefore be able to be created and re-configured in real-time and over-the-air. The permissioning system must function in both online and offline modes as network connections are not always available or reliable.

Important system requirements include real-time updating of credentials, as well as adding and removing staff at the touch of a button. These can all be supported by a mobile app on devices such as iOS/Android smartphones or tablets.

Pillar 2: Security
Trusted data can only come from trusted devices that are secured against manipulation. As typical IIoT deployments can result in thousands of devices spread out over large areas, deployment, configuration,

	Information Access				Infrastructure Access								Device Access				
	Logistics system	Administration records	Production line controll	Billing / Finance system	Factory main entrance	Production areas	Manufacturing machiens	Logistics / storage areas	Cantine	Administration office	Supply room	Server room	Production control	Logistics machines	Monitoring devices	Storage / shipping containers	HVAC
Plant manager	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
CFO	x	x		x	x	(x)		x	x	x	x						
Operators	(x)		x		(x)	x	x		x	x			(x)	(x)	(x)		
Service / IT Staff	x		(x)	(x)	x	(x)	(x)	(x)	x		(x)	x	(x)			(x)	x
Quality control	(x)		(x)		x	(x)	(x)	x	x		x	(x)	(x)	(x)	x		
Auditors*	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)		(x)	(x)	(x)	(x)	(x)	(x)	
Cleaning staff*					(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)				(x)	(x)

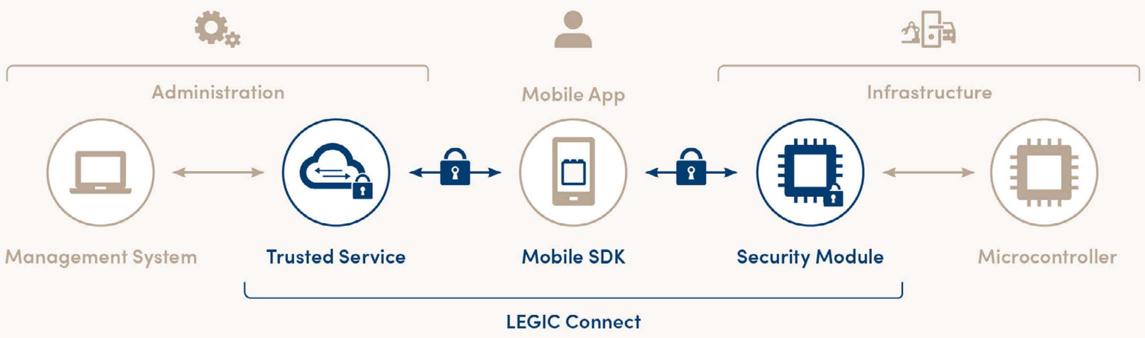
(x) = Conditional access (e.g. time of day, available functionality)
* = External service providers

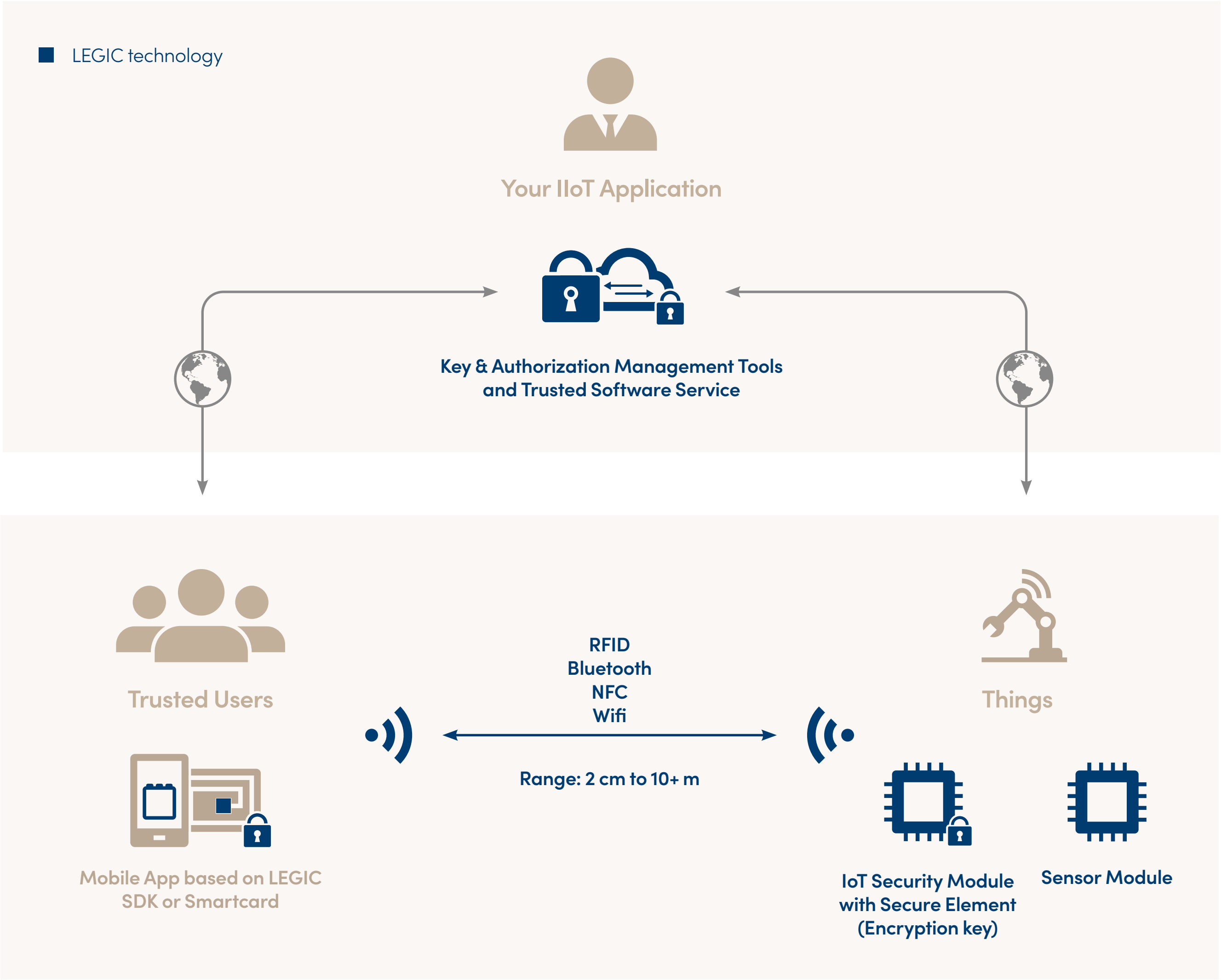
Trusted Users example: managing access to machines, infrastructure and information based on user credentials

Security by Design: LEGIC Connect mobile credentialing platform for IIoT system users

LEGIC Connect is a mobile credentialing platform that securely distributes mobile credentials or other data to registered smartphones or tablets anytime, anywhere and instantly at the touch of a button. The system provides a globally available, secure, end-to-end mobile credentialing service that is the backbone of establishing trust and accountability in user/device/infrastructure interactions. The system can be easily integrated into existing industrial infrastructure, giving IIoT service operators the ability to manage user permissions as well as send and receive data securely from smartphones and sensors.

LEGIC Connect protects infrastructure, data and credentials from manipulation, enables fully automated operation and provides transparency via transaction-based data that can be collected from trusted users, devices and infrastructure touchpoints. For details about LEGIC Connect mobile credentialing platform see www.legic.com/connect.




LEGIC technology
Your IIoT Application
Key & Authorization Management Tools and Trusted Software Service
Trusted Users
Things
RFID
Bluetooth
NFC
Wifi
Range: 2 cm to 10+ m
Mobile App based on LEGIC SDK or Smartcard
IoT Security Module with Secure Element (Encryption key)
Sensor Module

LEGIC IIoT Security Platform: auditable transparency via trusted users + trusted sensors

management and reading must be easy, quick and cost-effective. Ease of device retrofit is also important as many existing industrial installations need quick upgrading in-place. Establishing a trusted device network relies on several attributes:

- **All data coming from and going to devices must be protected.** The highest commercially available level of encryption such as AES (Advanced Encryption Standard) must be implemented.
- **Encryption keys must be invisible during initialization and inaccessible during operation.** As data is increasingly generated by devices at the network edge which are inherently physically vulnerable to manipulation, encryption keys and other sensitive data must be stored in a physically and electronically inaccessible secure element embedded in the device. During device initialization, encryption keys must never be human readable either at rest or in transit.
- **Infrastructure spoofing must be impossible** (e.g., a sensor which has been maliciously replaced with a manipulated sensor). A unique, invisible encryption key embedded in a secure element prohibits this from occurring: without the key, the sensor is unable to respond to external commands nor report erroneous data.
- **Wireless access is necessary.** Because devices are often installed in hard-to-reach areas, encrypted wireless configuration and reading is necessary over RFID, Bluetooth Low Energy or NFC via smartphone.
- **Firmware update over-the-air is required.** Configuration and updating of devices in the field including installation of encryption keys over the network or via smartphone must be possible; factory programming should be avoided to keep deployment and logistics costs down. This also increases security as third-party manufacturers are not involved.
- **Devices and access to them must operate both online and offline.** The system must function even with no network connection available to ensure robust and reliable operations.

Security by Design: LEGIC Trusted Sensors with Secure Element

The LEGIC XDK Secure Sensor Evaluation Kit is the "The Swiss army knife of IoT solutions". It is a universal programmable sensor device & prototyping platform for any IoT use case you can imagine.

Equipped with embedded security module with integrated Secure Element for storage of cryptographic keys/whitelists and wireless communications, it enables rapid prototyping of highly secure, touchless, sensor-based products and applications while offering developers the freedom to rapidly create basic to advanced IIoT solutions.

- All-in-one sensor kit: no need for component selection, hardware assembly, or deployment of a real-time operating system
- Readymade solutions for logging your data
- Includes accelerometer, gyroscope, magnetometer, environmental sensors (humidity, temperature, air pressure), ambient light and a microphone for noise detection, together with Wi-Fi, Bluetooth® Low Energy and an SD card slot
- Software examples and development APIs included

LEGIC XDK Secure Sensor Evaluation Kit with LEGIC Security Module and Secure Element

- **Devices must be modular, off-the-shelf, and easy-to-deploy without pre-configuration.** This streamlines device supply chains and minimizes opportunities for device manipulation or corruption during manufacturing. It also allows for easier application or customer specific configurations in the field while allowing the administrator of the IoT deployment to operate independently from device suppliers.

Pillar 3: Transparency
With trust in user accountability and device security established, system-wide transparency is achieved by verified users securely collecting or managing data from trusted devices over an encrypted network for processing by a management system. As IIoT deployments comprise devices distributed over a wide geographic area, or in mobile vehicles or containers that could be anywhere, being able to trust data as it traverses multiple wireless, cellular and internet links is crucial.

As no network, private or public can be 100% protected against data interception, end-to-end encryption must be employed. Using managed AES encryption, the most powerful commercially available encryption protocol, even networks susceptible to data interception cannot be meaningfully hacked as the payload in each data packet is impossible to read without the encryption key. Encryption keys must never be visible either in-transit or at rest.

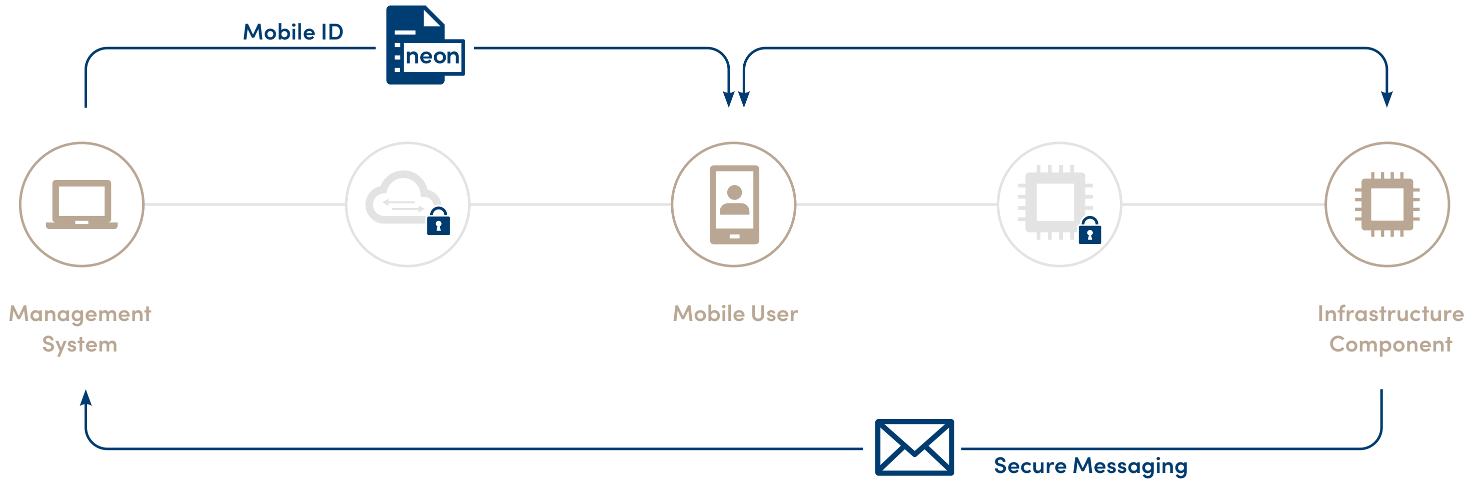
Secure gatekeeper at the IIoT edge
With a cryptographically secure, end-to-end IIoT platform based on Mobile Credentialing, Managed Encryption and Secure Element technologies, accountability, security and transparency can be achieved. Dynamically updateable user credentials combined with location and other context-based information such as sensor data makes tasks easier, more efficient and safer while improving process quality, integrity, accountability and convenience.

Some specific use-cases:

- **Logistics automation:**
A trusted IIoT platform enables secure and transparent movement of goods within as well as between facilities by securing access and logging interactions and states during transportation. RFID or mobile/smartphone credentials can be used for authentication. Authorized transport of goods within a facility is further enhanced by indoor positioning systems (see use case "Combining UWB Real-Time Locating System with secure transporter authentication".)

- **Building management:**
Linking of persons with a verified identity enables trusted monitoring of building assets and interactions between users and doors, HVAC systems, security systems, fire alarms, indoor navigation systems, etc. Location-triggered automated processes can be implemented based on user identity and managed via centralized, digitally distributed access rights and permissions.

- **Industrial equipment:**
Linking of persons with a verified identity followed by dynamic permissioning and access to equipment ensures trusted interactions and accountability. Industrial equipment can be reliably located, identified and monitored. Protocolled equipment usage data can be collected per user. Granting and restriction of permissions can be performed in real-time and over-the-air.



LEGIC Orbit: Secure key and authorization management

Security by Design: LEGIC Orbit enabling system-wide data security and transparency

Based on managed end-to-end AES encryption, LEGIC Orbit enables you to securely configure your IIoT solutions. LEGIC Orbit secures LEGIC's credentialing technology which is at the heart of your mobile IIoT solution. It also protects messaging from your sensor modules back to your IIoT management system.

For details about secure deployment of encryption keys and configuration data to sensors and infrastructure, refer to LEGIC Orbit: Key and Authorization Management.

- **Hospitality**
  Hotel room booking and check-in via smartphone. Guests download virtual keys, bypass reception and go straight to their rooms. Indoor navigation via UWB guides guests to their destination. Customized offerings can be pushed to each guest's smartphone based on preferences stored in their digital credentials which are downloaded with the key (see use case "Smartphone-app Hotel Room Entry at Village Hotels UK").

Implemented as a trusted security platform which provides accountability, security and transparency, the LEGIC IIoT Security Platform can be integrated with any application and in any infrastructure. Providing secure, managed cryptography combined with secure element technology, mobile credentialing and Bluetooth, NFC, WiFi or RFID radio communications is a strong candidate to be the safest and most secure solution for life- and business-critical IIoT systems.

For more details about deploying trust based IIoT sensors and systems visit:

www.legic.com/iot

About LEGIC

For over 25 years, Swiss-based LEGIC Identsystems has enabled companies from around the world to deploy solutions with demanding security requirements. Based on key management, trusted services and secure, contactless semiconductors, the LEGIC Security Platform provides end-to-end security for smartphone- and smartcard-based access, mobility, shared resource and industrial IoT applications.

Juliy 2022   Authors: Anthony Fitze, Carl Fenger