We are the new secure communication mindset

SIKUR CONNECT

The Cybersecurity Market Size - IoT

Security breaches are a significant drawback to IoT. According to IEEE, over 80 percent of healthcare organizations that use IoT devices have suffered a security breach of their IoT devices or infrastructure.
Source: IEEE

Smart cities" are a major and emerging concept in IoT. Over one-fifth of all publicly announced IoT projects involve IoT-driven "smart cities" of some kind, with most of these "smart cities" (45 percent) announced in Europe.
Source: IoT Analytics, 2020

Gartner predicts a larger amount of "connected things" by 2020. According to Gartner, there will be over 14 billion connected devices by the end of 2019, and over 25 billion by the end of 2021
Source: Gartner, 2019

The global IoT market was worth over $150 billion in 2018 and is expected to exceed $1.5 trillion by 2025.
Source: IoT Analytics, 2020

The most common security threats to IoT were malware (49 percent), human error (39 percent) and DDoS attacks (22 percent).
Source: Aruba, 2019

Over a quarter of all cyber attacks against businesses will be IoT-based by 2025.
Source: Gartner

Gartner®

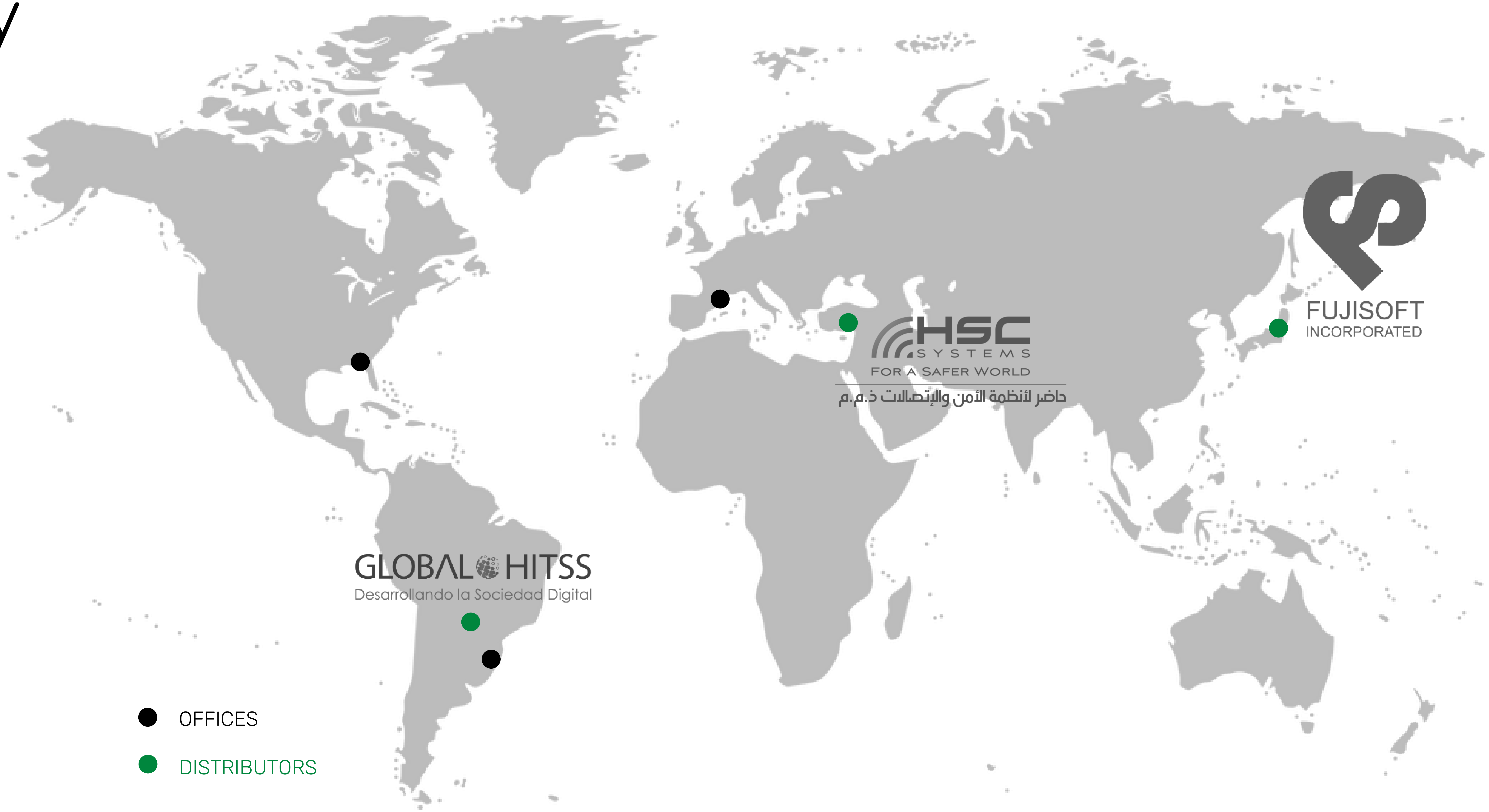
The systems and services in the IoT segment will allow authorized providers and customer administrators to establish and enforce the **privacy policy** for their devices, machines, and assets. Included in the scope of this service segment are **private Access Point Name (APN)** and **managed virtual private network (VPN)** services, services relating to **identity, credentialing, authentication** and establishment of **trust** between in-scope edge devices and the cloud, including **pre-integrated secure access** capabilities with public cloud providers. Source: Gartner, 2019

- By 2023, 10% of managed Internet of Things (IoT) worldwide connectivity will be provided through hyperscale cloud providers, up from less than 1% in 2019.
- By 2022 40% of global managed IoT connectivity vendors will offer worldwide 3rd Generation Partnership Project (3GPP) low-power wide-area (LPWA) networks (NarrowBand IoT [NB-IoT] and Long-Term Evolution for machine-type communications [LTE-M]) roaming coverage, up from 0% in 2019.
- By 2023, over 60% of all new connected vehicles produced will feature an embedded SIM (eSIM) for cellular connectivity, up from less than 5% in 2019.
- By 2023, 80% of manufacturers that embed 3GPP services will use a partner revenue share model, up from 20% in 2019.

Source: Gartner 2019

The Company

Sikur is defining the future of secure communication, operating globally, through its offices and Distributors in Brazil, the United States, Europe, the Middle East, and Japan. Sikur works alongside governments and corporations that believe security is fundamental to the integrity of their work. We believe that security is not only about platforms and digital systems but is a mindset that surrounds every aspect of a business.



SIKUR LAB

Sikur Lab is the brand new Sikur innovation and research laboratory located in Sophia Antipolis, France. Sikur is now a member of the Digital Security sector at Sophia Antipolis SCS Cluster (Secure Communicating Solutions), which is a Leading European Ecosystem in microelectronics, internet of things, digital security, artificial intelligence and big data. We established our research lab in this location because it is a fast-growing hub in advanced technologies. Now digitalization is the core for everything related to human development, and France is occupying a central role as we have noticed in the last few years. This is happening in parallel with Sikur's development as a company, and we want to take part on this, at the same quick pace.

SOPHIA ANTIPOLIS | SECURED COMMUNICATING SOLUTIONS A WORLD-CLASS CLUSTER | UNIVERSITÉ CÔTE D'AZUR | IMREDD INSTITUT D'INNOVATION ET DE PARTENARIATS

Global Exposure

SIKUR: “ONE OF THE MOST EXCITING PHONES AND GADGETS FROM **MWC 2018**”

WIRED

Gartner

According to Gartner, SIKUR is a vendor that has relevant solutions to this technological space

hackerone

Pushing its technology to the limit, SIKUR launched the safest smartphone ever in 2016. Not satisfied delivered it to the world best hackers, and gave them a mission: break it. They failed.

Mashable · cnet · Forbes · WSJ · TechCrunch

CNBC · engadget · CNN · REUTERS · Bloomberg

The Secure Foundation – H2H/ H2M/ H2M2M

Cloud

APPs

Endpoints

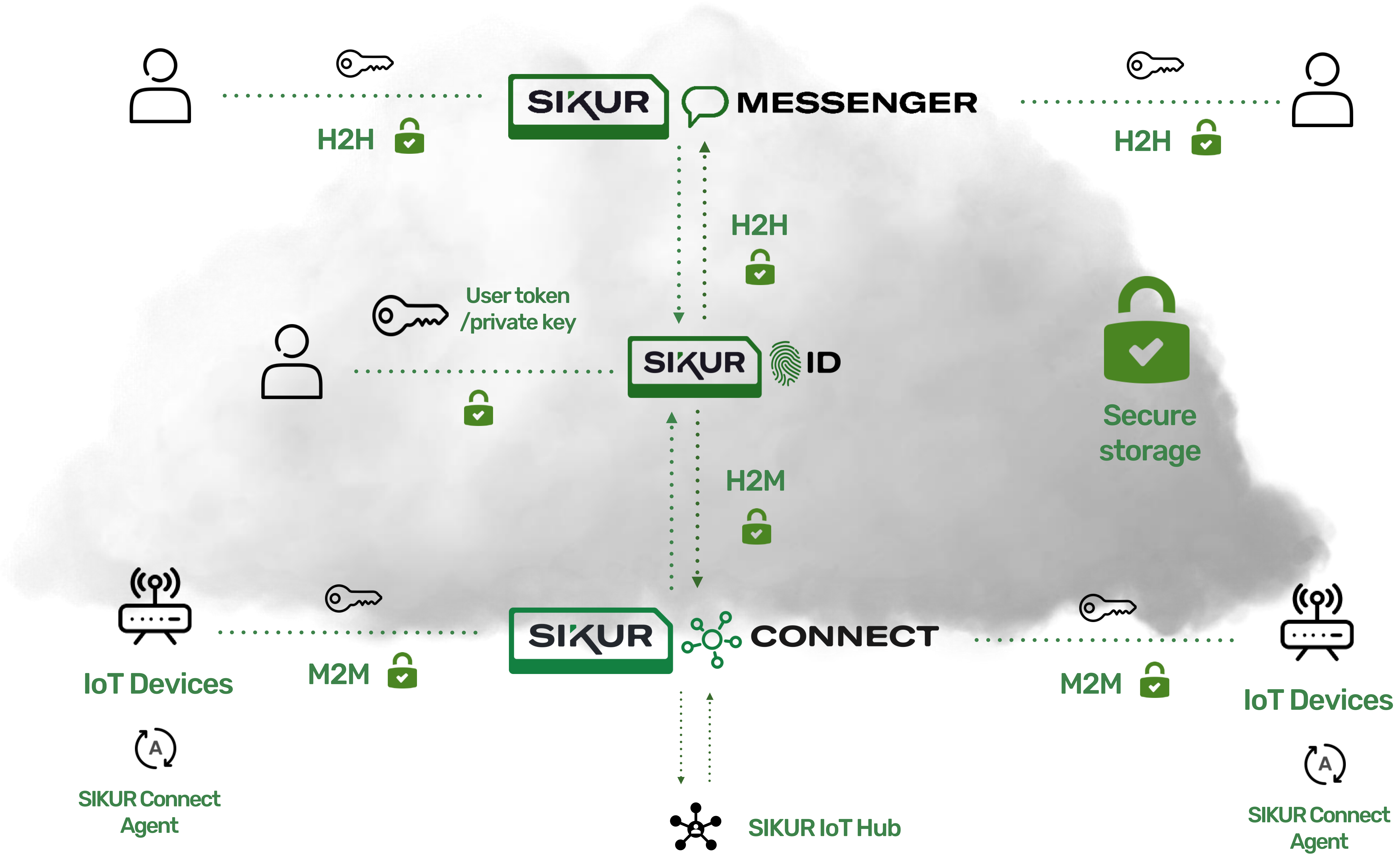
Tunneled Communication Solution

1 strong authentication

2 non-repudiation

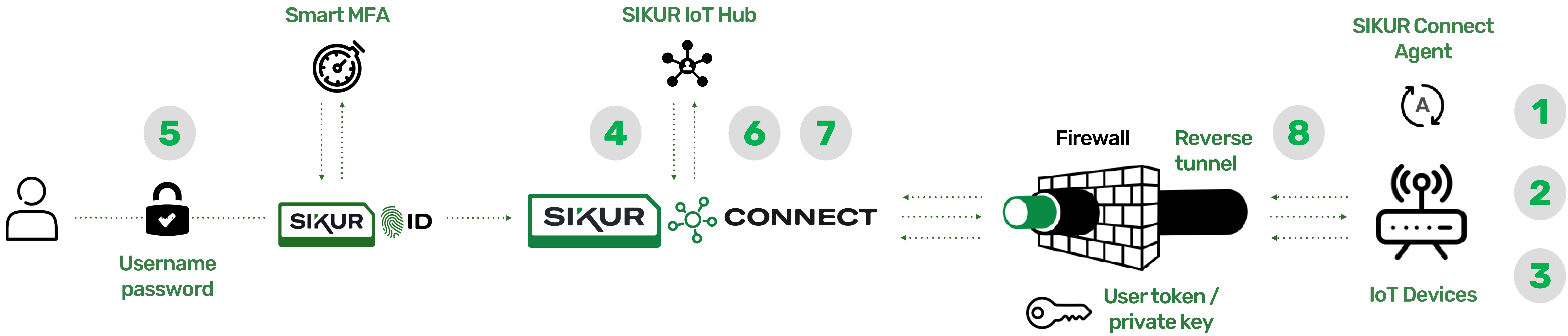
3 secure storage

4 secure communication



The Solution – H2M2M – step by step

Authentication and Control to protect assets and manage them remotely.



1 Device Agent installation

2 Hub definition

3 The agent generates the key pair (public and private), and authenticates on the destination Hub

4 The Admin enroll users on Sikur Connect, for device management

5 Users creates credentials in Sikur ID, generating their key pair (public and private)

6 The Admin defines user's access permissions to devices for each Hub, with no credentials previewing access

7 User ask permission for device connection

8 The Agent opens a reverse tunnel, starting a secure communication so that the user can manage the device

The Product – features

Identity Management

- Secure user access to any IoT system and application
- Stop default passwords

Authentication

- User and permission control within applications and systems
- Strong authentication, using encryption and automation keys

Auditing and Compliance

- Usage monitoring and security alerts
- Compliance with global regulations

Secure Storage

- Secure storage of data collected from devices

Secure Tunnel

- A secure device access tunnel, even on unstable networks
- Reverse access tunnel when firewall restrictions apply

Zero Touch

- Automatic deployment
- Remote provisioning of new devices
- Easy, no-touch registration

Device Management

- No device will be accessible anonymously
- Secure update and upgrade
- Protection against theft of equipment

Secure Data Collection

- Secure device data collection

The Product – Value Proposition for IoT Vendors

Security

- Deploy value through extra security layers
- Provide proper authentication and data protection
- Data Tunneling
- Data Encryption
- Messaging with the most up to date encryption algorithms
- Key protection, with hardware
- Layered protection against attacks
- Secure Storage
- Secure Data Collection

Comply with GDPR

Hybrid Cloud authentication

Data protection with strong Industry Encryption Standards

Remote access maintenance

- Manage devices remotely
- Optimized for low speed networks
- Real-time monitoring
- Device visibility
- Firmware upgrade and controlling

The Product – Value Proposition for Industry

Fast Management

- Manage devices remotely, no need for new network equipment
- Optimized for low speed networks
- Real-time monitoring

Hybrid Cloud authentication

Account lockout and behavioral monitoring

Single Sign-on

- Control who have access to devices, granularly and password-less
- Secure and flexible. No one else – than you – shall pass.

RBAC: Role Based Access Control

SIEM Integration: provide logging information for third-party systems

Security

- Data protection with powerful and light encryption
- Information protection for data in transit and at rest
- Multi-factor authentication
- Layered protection against attacks
- Secure Data Collection
- Secure Storage

Device visibility and control

Industry Standards

Business Model

White Label

Following a worldwide trend of micro private networks with usability

Hybrid Cloud

Sikur Cloud

Azure

Private Cloud

Azure or On-Premises

Product Differentials

1 **Zero Touch**
configuration made simple, remote and automatic

2 **Business Model**
Hybrid Cloud and White label solution

3 **Regulatory Compliance**
data protection with user keys, private

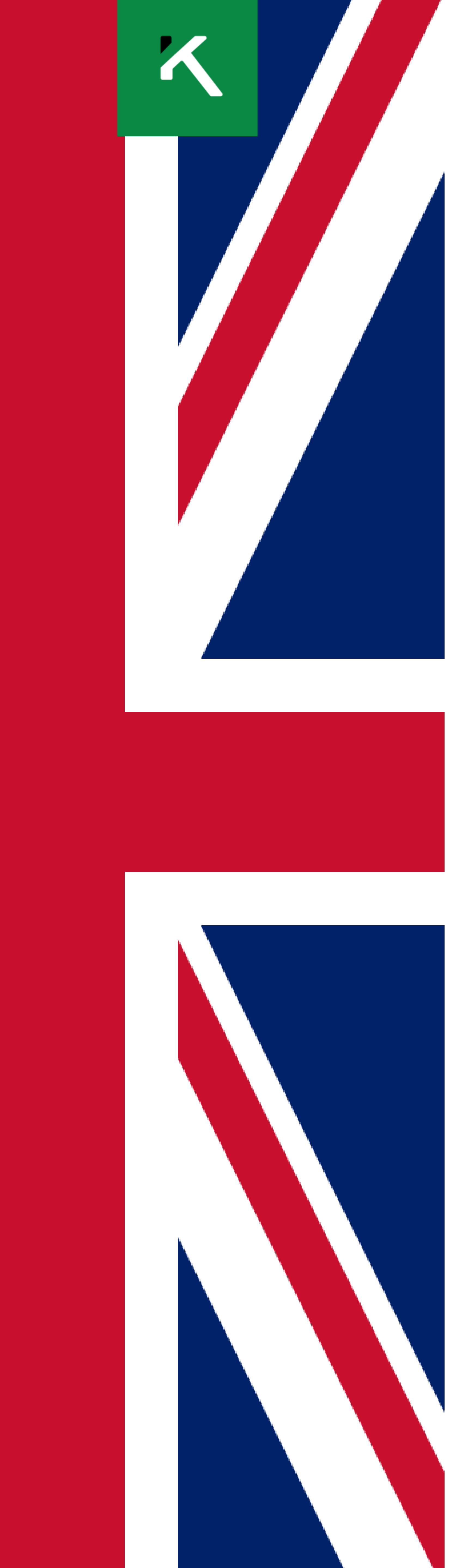
4 **Protected MFA**
strong and flexible

5 **Credential protection**
process automation, avoiding credentials misuse

6 **Secure from the start**
no default passwords, strong key generation

7 **Scalable and Manageable**
distributed architecture, grow consistently, manage and update software versions

8 **Secure Data Collection and Storage**
Safe storage and collection



IoT Regulatory – UK Governmental Proposal

1

IoT device passwords must not be default factory setting

2

Secure credentials storage and management

3

Software integrity

4

Access secure authentication

SIKUR Connect complies with (1), (2) and (4), the (3) is on the roadmap

Authentication and data protection are the center of existing data regulations and should be for the next ones. SIKUR Connect complies with most of them, delivering excellent management.

Where it can be applied

Industrial

IoT devices on the shop floor (automotive industry, agribusiness sensors, steel mills, mining companies, etc.)

Energy

Power systems and facilities infrastructure (smart meters, Programmable Logic Controllers, SCADA platforms, etc.).

Smart Cities

Vehicles and transportation (autonomous/driverless cars, urban traffic control systems, smart cities platforms, sensors, cameras and video monitoring systems etc.)

Healthcare

Health systems and appliances (hospital equipment, body sensors, e-Healthy devices, etc.)

Oil and Gas

Predictive and preventive maintenance, asset tracking and monitoring, data management

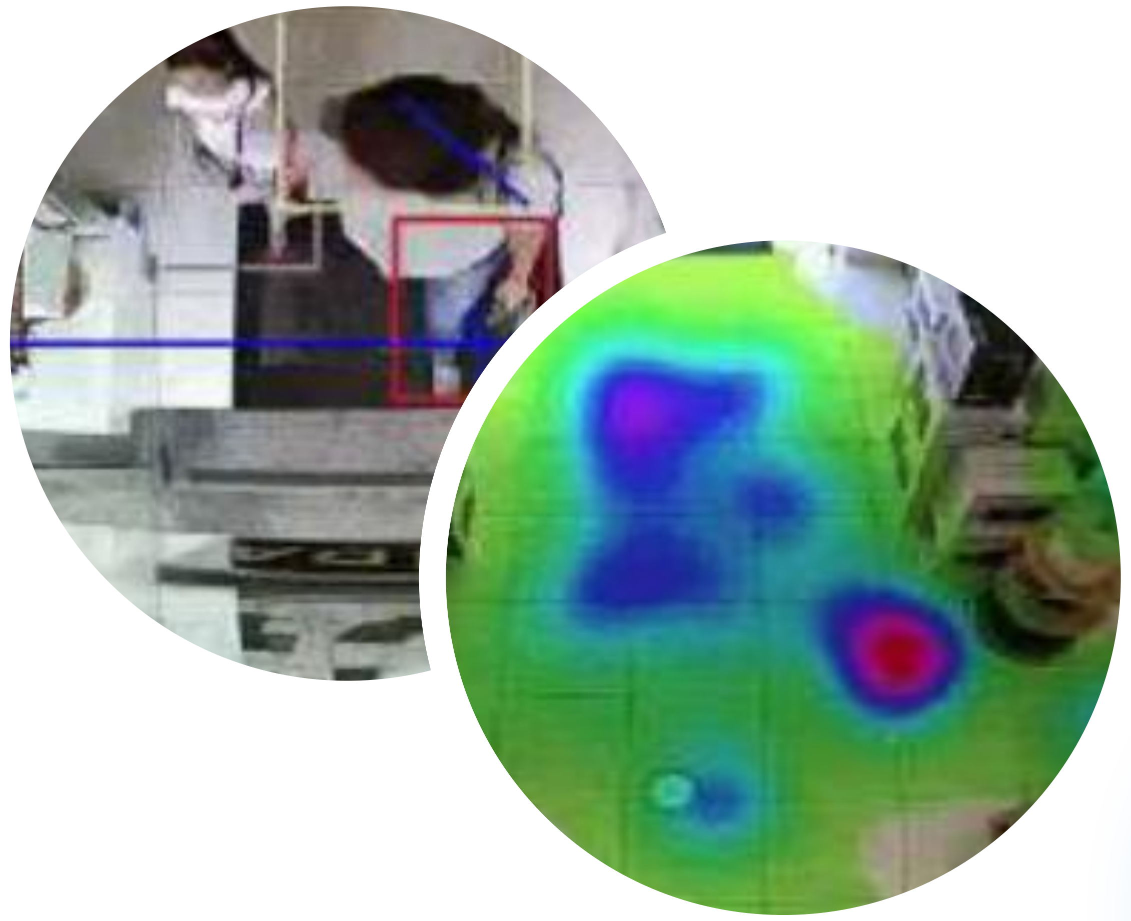
Smart Homes and Buildings

Home and building automation appliances (access control, CCTV cameras, general end point devices etc.)

Cases

AGVS

- Industrial, for automation and logistics
- Self-guided robots
- Better control and visibility



DOD Vision

- Camera management
- Distributed retail stores
- Real-time images for marketing campaign management

Appendix

Why our solution is disruptive?

Challenges for the IoT

SIKUR CONNECT

Why our solution is disruptive?

1 It guarantees security for IoT devices and IoT platforms

2 Market solutions rely on Firewalls, the Cloud and usual security solutions as passwords (these are old fashion, old-style security solutions for the "old" Internet)

3 It manages and controls IoT devices, leaving no breaches for external attackers

4 The solution inventories that key in an encrypted IoT Hub Management

5 Sikur Connect solution creates "exclusive secure tunnels" for communication between the IoT devices and the IoT Hub Management

6 It goes far beyond and rely on a unique identification key, created in each IoT device when turned on for the first time

7 It ensures secure end-to-end H2M (Human-to-Machine) connection and communication

Challenges for the IoT

		How to solve?
Impersonation/Identity Spoofing: this means that the attacker uses a false identity, communicating with the IoT device on behalf of a legitimate entity	SIKUR CONNECT →	• Only Users with Sikur ID can access the device
Eavesdropping: the interception of electronic communication, which happens because IoT devices often use public communication infrastructure	SIKUR CONNECT →	• Devices can be accessed only through the Secure Tunnel
Data tampering: the unauthorized alteration of data, which can occur in the IoT device or when it is exchanging data with the network	SIKUR CONNECT →	• Sikur ID plus Secure Tunnel guarantee no tampering.
Authorization and Control Access issues: the attacker gains access to the device and then manipulates the device itself and/or the network.	SIKUR CONNECT →	• Only Users with Sikur ID can access the device
Privacy: the attacker uses private data hosted in the IoT device to explore them for unknown/unauthorized reasons	SIKUR CONNECT →	• Sikur ID plus Secure Tunnel guarantee privacy
Interoperability and gateways: as several IoT devices don´t communicate using TCP/IP but other protocols, gateways, and other communication processes come to the network, and these are open-doors for attackers	SIKUR CONNECT →	• External gateways should be with Sikur Connect to be protected.

Challenges for the IoT

Compromising and Malicious code: the attackers can target the IoT devices with malicious code or software infection, since they usually are no tamper-resistant, and then physically compromising them.

SIKUR CONNECT

How to solve?

- We Funnel the access to the device using a single hub to avoid uncontrolled access.
- We Record access sessions to the device and log malicious activity.

What we don't do: avoid or prohibit installation of malicious code once the user is inside de device

Virtual Availability and DoS (Denial-of-Service) issues: the attackers can make IoT devices partially or unavailable as a result of the DoS attack. An example of this problem was described in, when a Distributed DoS attack targeted the east of USA internet through thousands of elementary IoT devices, like CCTV cameras and other home appliances, resulting in a vast communications blackout.

SIKUR CONNECT

- Devices on our hub don't need open ports that can be explored, because the connection flow in from inside out

What we don't do: avoid DDoS attacks on the device infrastructure, solutions designed for that purpose can be used together with ours

Physical availability: the attacker can target the physical characteristics of the IoT device to partially or destroy/alter it, aiming to send erroneous messages to the network.

SIKUR CONNECT

- We only allow authorized traffic to the device from the network

What we don't do: control access to the physical device and its ports

We are the new secure communication mindset

SIKUR CONNECT