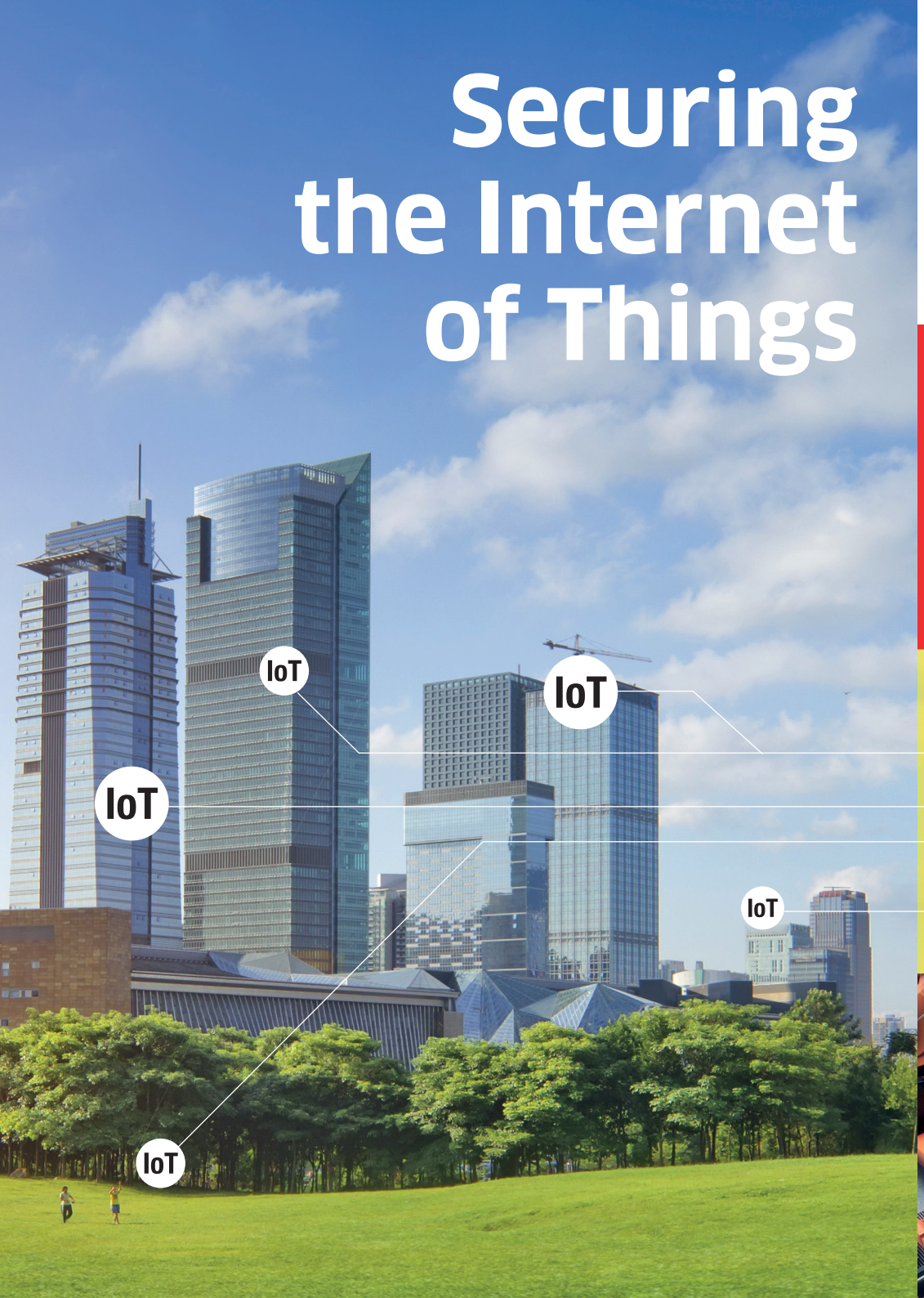
Securing the Internet of Things



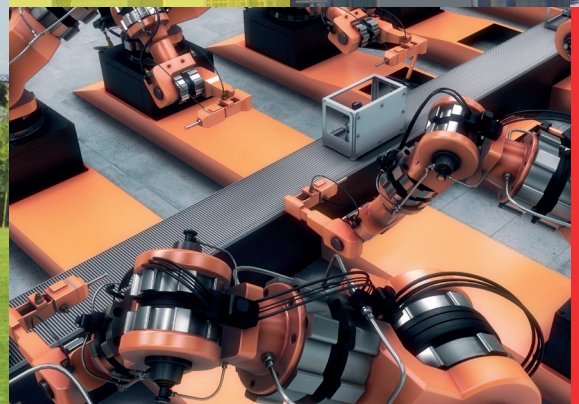
Technology allows people, objects and machines to connect to one another, creating new opportunities to improve people's lifes:

> Optimize processes and resources;
> Reduce risks;
> Improve end-user experience and
> Create or increase business.

IoT success can only happen if data can be trusted

WISeKey provides an end-to-end scalable security framework to be integrated into IoT platforms. Based on PKI Technology, it will protect the device and its data at rest or in transit.

WISeKey delivers cryptographic root keys and solutions to use and manage digital certificates and associated secure assets that protect otherwise vulnerable IoT devices in the field.



WISeKey

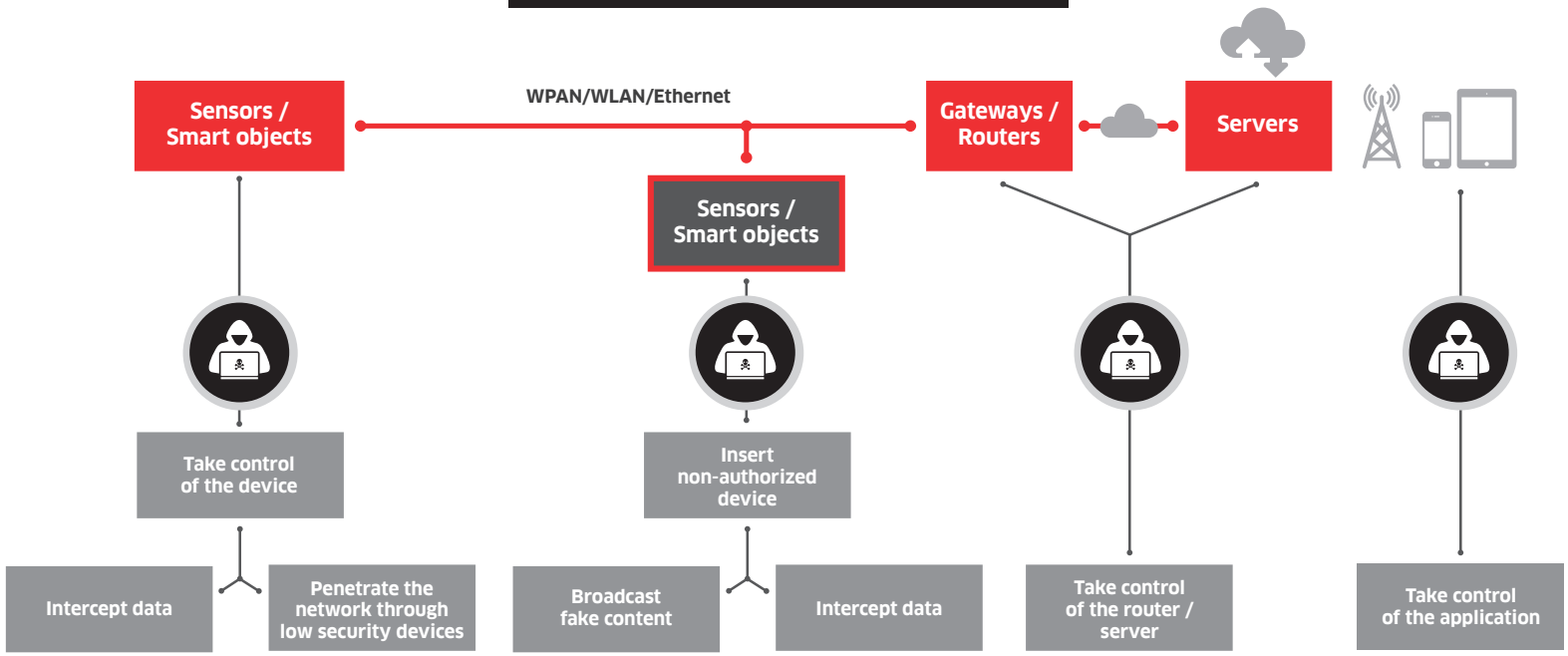
wisekey.com
info@wisekey.com

IoT:
Internet of Threats?

Distributed Denial of Services (DDoS) attacks are becoming increasingly ubiquitous and dangerous, causing organizations billion dollar losses; Man in the middle attacks on video surveillance cameras are almost common ground. These are just two examples of threats faced by IoT systems.

Hackers have different motivations (fun, money, terrorism...) and resources (material, collusion, expertise) to penetrate a system, but all IoT Systems will face hacking. Consequences can be heavy: disrupted services, intrusion on users' privacy and safety, theft of intellectual property, damaged brand reputation, loss of revenue, job destruction and more. WISeKey offers proven products and solutions to reduce the risk of IoT attacks.

Illustrating some potential attacks



WISeKey's Unique Root of Trust Model

A Root of Trust (RoT) is the basis for a global end-to-end security solution. A RoT serves as a common trust anchor, which is recognized by the operating system (OS) and applications, to ensure the authenticity, confidentiality and integrity of on-line transactions. With the certificates signed by this cryptographic RoT, embedded in the device, the IoT product manufacturers can use PKI (Public Key Infrastructure) technologies to secure interaction among objects and between objects and people.

WISeKey is the trusted operator of the International Organization for the Security of Electronic Transaction (OISTE) Global Root, which is widely distributed in commonly used software.

The OISTE Foundation is working with the United Nations and International Organizations. Swiss neutrality, security, and privacy laws allow operations without geo-political or governmental constraints. It Root of Trust is set in a military grade bunker located in the Swiss Alps.

OISTE

Secure Element: VaultIC

VaultIC is a product family, ranging from tamper-resistant Integrated Circuits to software vaults, to be used as a companion to the IoT-device host processor. VaultIC chips feature a configurable cryptographic tool box for authentication, confidentiality and integrity, executed in a secure environment.
VaultIC embeds on-chip non-volatile tamper resistant data storage capabilities for keys, certificates and customer data.

The VaultIC chips' low-power consumption profile make them a viable solution to meet the limited power budgets of IoT devices. VaultIC comes with middleware enabling secure boot, secure firmware update for IoT devices secure communication (SSL/TLS).

Common Criteria

FIPS 140-2 CRYPTOGRAPHY

https://www.wisekey.com/products/vaultic/secure-solutions

WISeKey

Certification Authorities

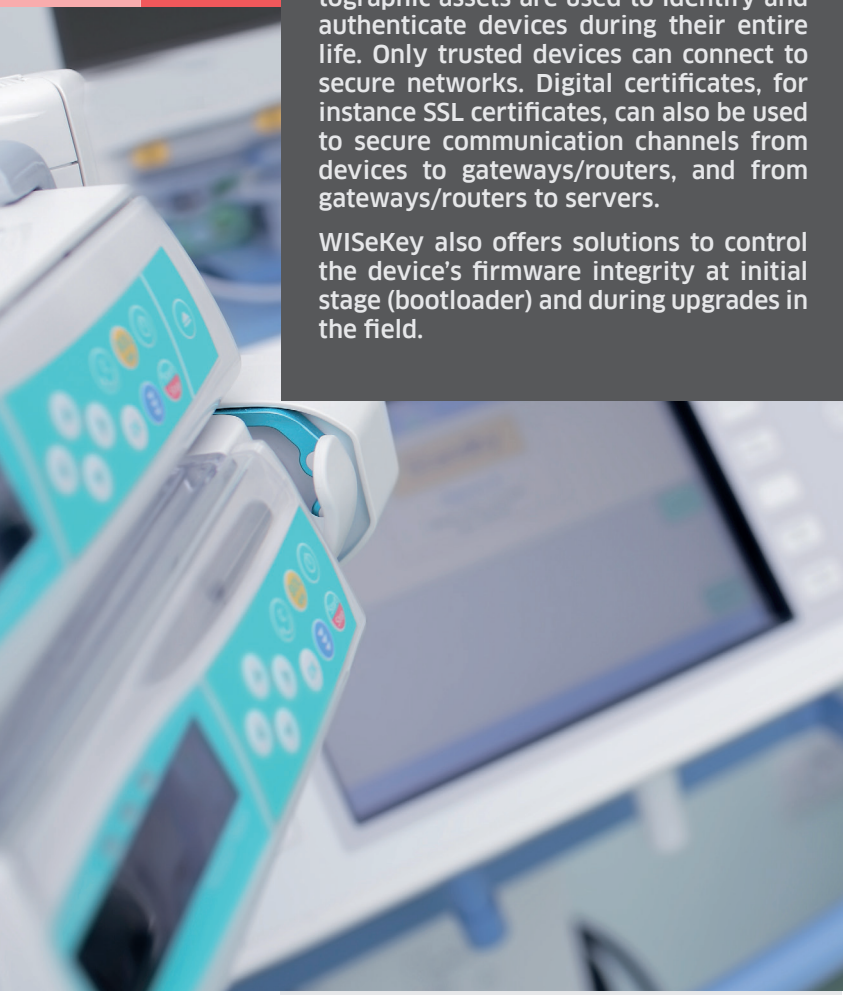
Certification Authorities

Certification Authorities

Use of Digital Certificates

Digital certificates and associated cryptographic assets are used to identify and authenticate devices during their entire life. Only trusted devices can connect to secure networks. Digital certificates, for instance SSL certificates, can also be used to secure communication channels from devices to gateways/routers, and from gateways/routers to servers.

WISeKey also offers solutions to control the device's firmware integrity at initial stage (bootloader) and during upgrades in the field.



WISeKey IoT framework

The WISeKey IoT Certificate Management System (CMS) is a software tool with a user-friendly interface and easy-to-integrate API that manages the life-cycle of devices and their digital certificates.

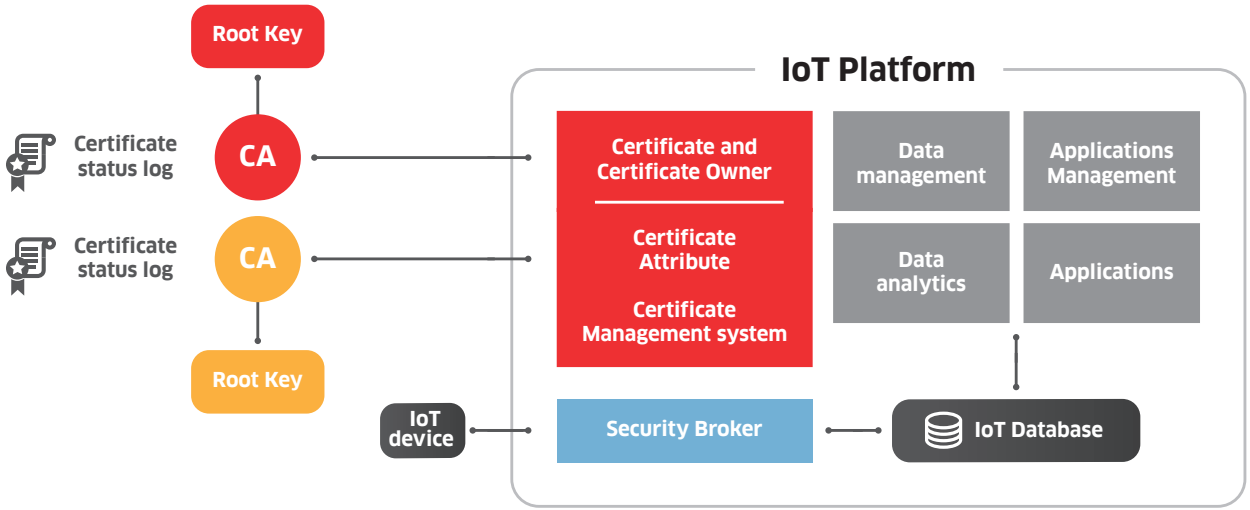
These certificates are signed by WISeKey's Certificate Authority and optionally the OISTE Root of Trust.

The optional security broker performs the authentication and validation of the messages coming from the different IoT devices and transfers only trusted messages to the IoT platform of our customer. The WISeKey IoT framework can easily be integrated into an IoT platform by our customers and no additional security mechanisms need to be implemented.

The WISeKey IoT framework also includes secure provisioning solutions to help maintain consistent high system security, even when the IoT device is in an unsecured environment (e.g. during production or in the field). Device configuration and firmware upgrades are made easy and secure at all times.

WISeKey IoT CMS can be installed on customer premises, or outsourced to WISeKey and located in one of our secure data centers in Switzerland, USA, India or China.

The managed platform can be accesses through a browser and a web-service API. The CMS and the framework are compatible with third party Certificate Authorities (CA), such as the Microsoft PKI or the Enterprise Java Beans Certificate Authority (EJCBA) open source CA.



WISeKey IoT

WISeKey IoT or 3rd Party

WISeKey IoT

- PKI based security, Swiss Root of Trust
- Software solution; optional use of tamper resistant chip
- Easy integration in IoT platform, and in devices
- Cost effective solution
- Security for device in operation and for provisioning
- Certified security
- WISeKey solid trusted partner

https://www.wisekey.com/solutions/secured-iot/

WISeKey

wisekey.com
info@wisekey.com