Securing the Internet of Things

IoT: Internet of Threats?

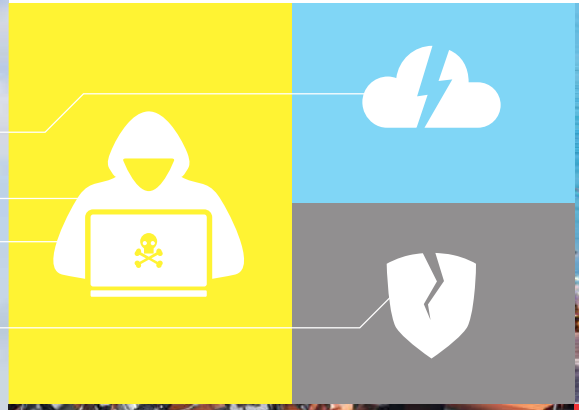
The Internet of Things will only stand up to its promise if it can be trusted.

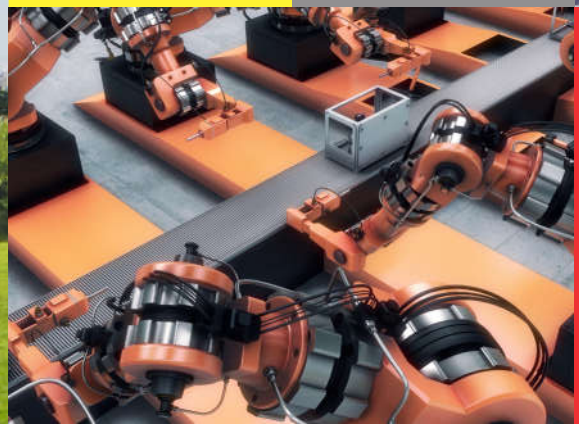
The steady development of IoT based applications goes in pace with the development of more and more sophisticated cyber attacks.
Distributed Denial of Services (DDoS), ransomware, data theft and other attacks are becoming increasingly ubiquitous and dangerous, causing billion dollar losses; Man-in-the-middle attacks on video surveillance cameras are almost common ground. These are just some examples of threats faced by IoT systems.

Consequences can be heavy:

- > disrupted services
- > theft of intellectual property
- > loss of revenue
- > liability claims
- > intrusion on users' privacy and safety
- > damaged brand reputation
- > job destruction
- > and more..

Stand up to the challenge of defying the increasing threat of attacks with a company that earned its spurs for more than twenty years.





WISeKey

Your 360° Best Practice Partner for Secure IoT

wisekey.com
info@wisekey.com

WISeKey IoT framework

Device Identity provisioning thanks to WISeKey's advanced PKI solutions

The security framework WISeKey IoT brings trust to your IoT applications by applying device authentication through the use of digital certificates and building message protection through the use of standards proven secure messaging schemes.

The digital certificate and related private key are stored in your devices with the use of the optional tamper resistant secure elements **VaultIC**.

The Security Broker INeS connected to your IoT platform performs the authentication and validation of the messages coming from the different IoT devices and transfers only trusted messages to the background applications.

It can be easily customized to integrate IoT platforms such as:

> IBM Watson*
> Amazon Web Services*

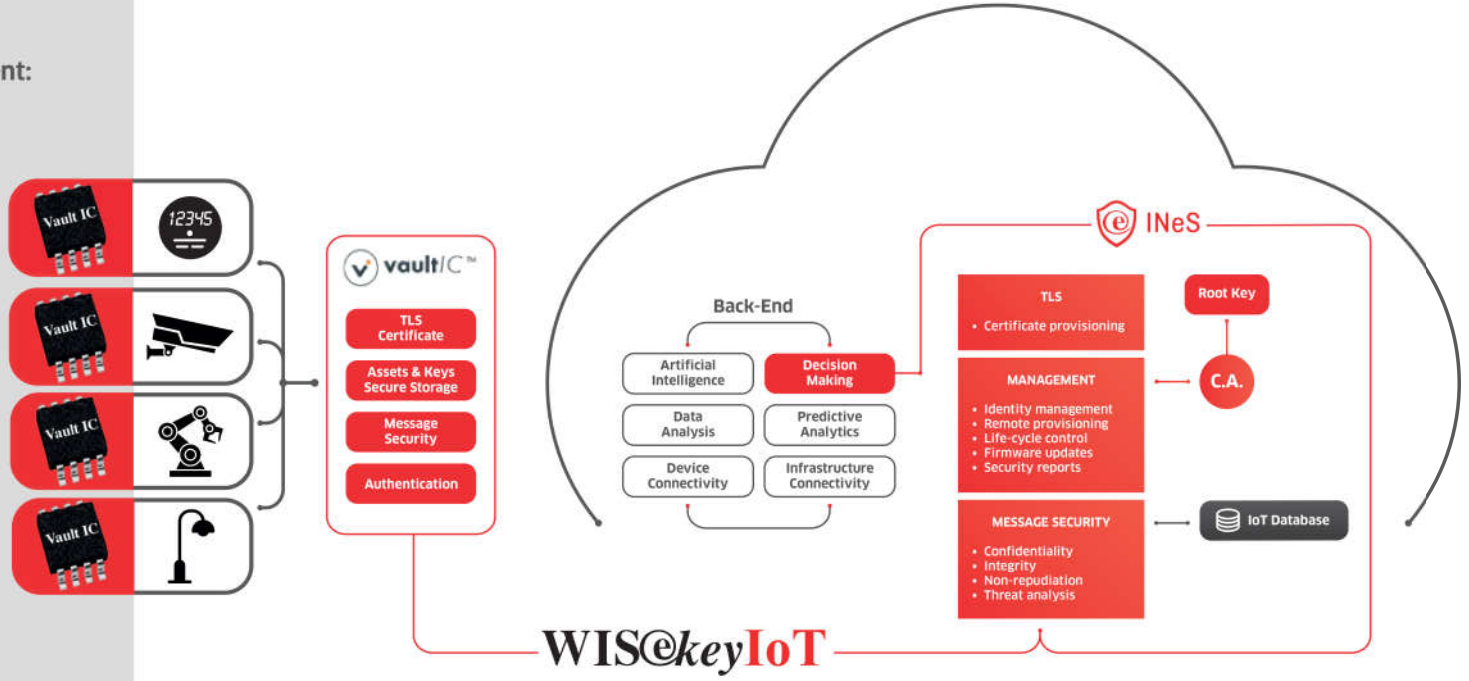
It offers best in class entity life cycle management for a secure remote device deployment, control, update and deprecation, including remote secure certificate renewal and revocation.

The system 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.

*Trademarks are property of their respective owners

Characteristics

> **Easy to integrate into IoT platform**
> **Remote Device & Application life cycle management:**
  > Identities
  > Software/Security updates
  > Ownership changes
> **Message security**
  > **Connection security**
> **Device to Business End to End security:**
  > VPN like (Global Platform SCP11)
  > Digital certificates
  > Root of Trust
> **Features:**
  > SCP11 certificate provisioned into devices and Applications
  > Publish-Subscribe messaging
  > X509 certificates for TLS authentication
  > Large scale PKI
  > Webtrust Digital Certificates
  > Long Validity Digital Certificates
  > Multiple CAs: RSA, several Elliptic curves
  > RESTful API



Certification Authorities

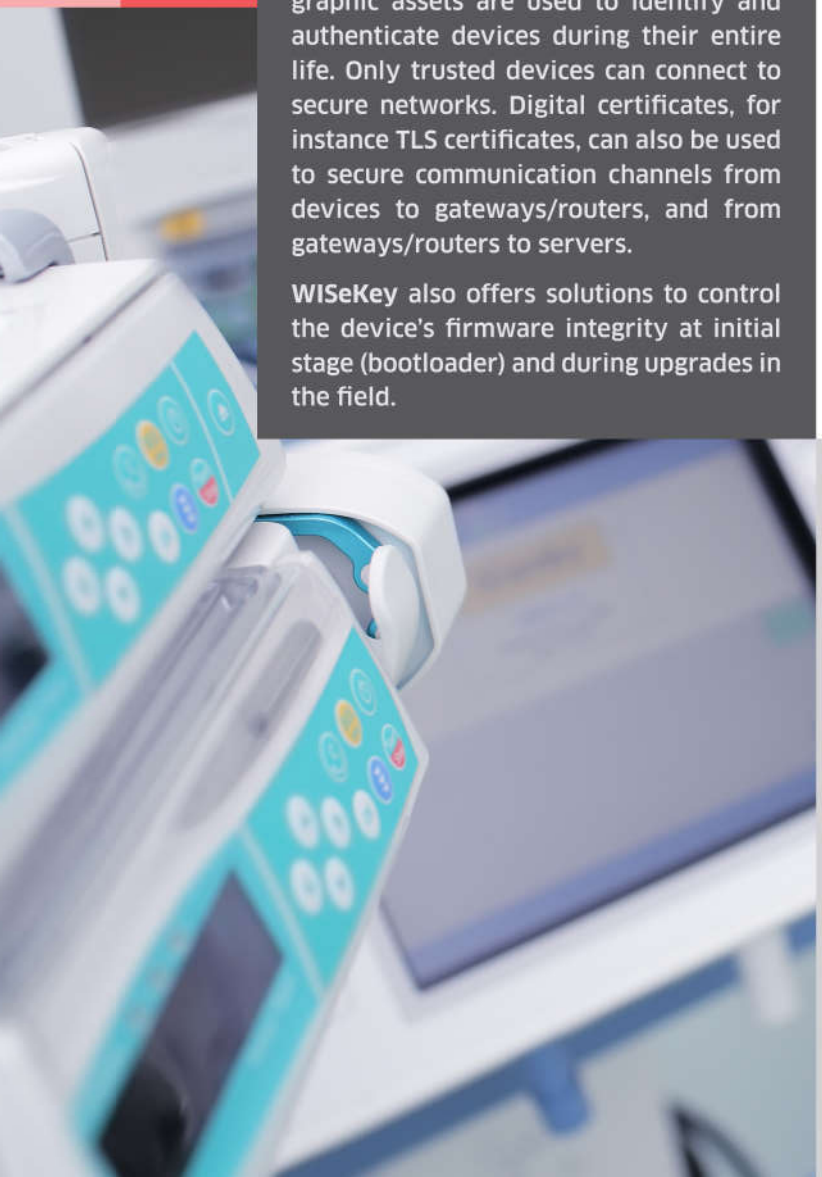
Certification Authorities

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 TLS 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.



Secure Element: VaultIC

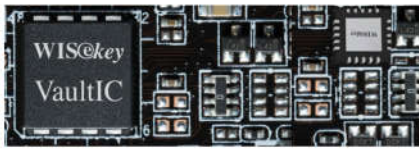
VaultIC is a product family, ranging from tamper-resistant Integrated Circuits to software vaults, to be used as a companion to the IoT-device host processor.

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 (TLS).



Why choose WISeKey?

WISeKey offers since more than 20 years tailor made security solutions for website, people, services and devices based on a scalable Public Key Infrastructure.

Our certificate Authorities, Security Brokers, management systems and tamper resistant secure microcontrollers are regularly audited and accredited with highest grade Webtrust and Common Criteria certifications.

You want Security? You need WISeKey.

WISeKey IoT

The single source turnkey security framework for your IoT system

Protect your revenue and brand image:

- Optimize processes and resources
  - Central, secure entity management
  - Life cycle control
  - Secure device boot and firmware update
  - Certificate renewal and control
- Reduce risks of the constant threat of large scale attacks and related loss of revenue
  - Device authentication
  - Uncompromised data communication
- Comply to regulations, standards and certifications

Building a solid security foundation with WISeKey is a starting point for a best in class IoT.

Common Criteria

FIPS 140-2 FIPS CRYPTOGRAPHY

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

WISeKey

WISeKey IoT

- **PKI based security, Swiss Root of Trust**
- **Off-the-shelf turnkey integration to tailor made end-to-end solutions**
- **Innovative approach towards entity management**
- **Integration with leading providers of cloud based IoT and AI platforms**
- **Entry Level approach with solution scalability**

WISeKey SA
Route de Pré-Bois 29
P.O. Box 853
CH-1215 Geneva 15
Switzerland

Phone: +41 22 594 3000
Fax: +41 22 594 3001

General information: info@wisekey.com
Sales: sales@wisekey.com
https://www.wisekey.com/solutions/secured-iot/

WISeKey

wisekey.com
info@wisekey.com