The Vertical Cybersecurity Platform

Smart City Expo World Congress

WISeKey Geneva

November 2016

sales@wisekey.com

WISeKey

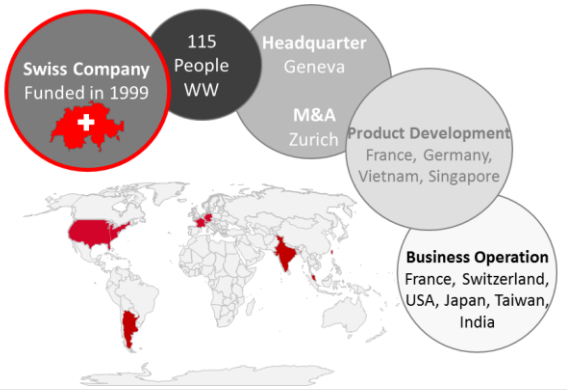
www.wisekey.com

WISEKEY – VISION AND MISSION

Vision

- **Technology allows to connected People-to-Machines and Machine-to-Machines, creating new opportunities to:**
  - improve people life, Optimize Processes and resources, Reduce Risk toward end users, Improve Processes and end-user experience, Create new businesses and Improve existing business
- **Companies and customers can realize value and enable monetization when they can certify that they are receiving authenticated and secure device data**
- Gain insight from it, and propose appropriate actions as needed (applications)

Company Overview



Mission

- **WISeKey's mission is to offers clients a Vertical Cybersecurity Platform integrating Root of Trust to Chip, empowering the Personal to be the Center of Gravity of the Internet.**

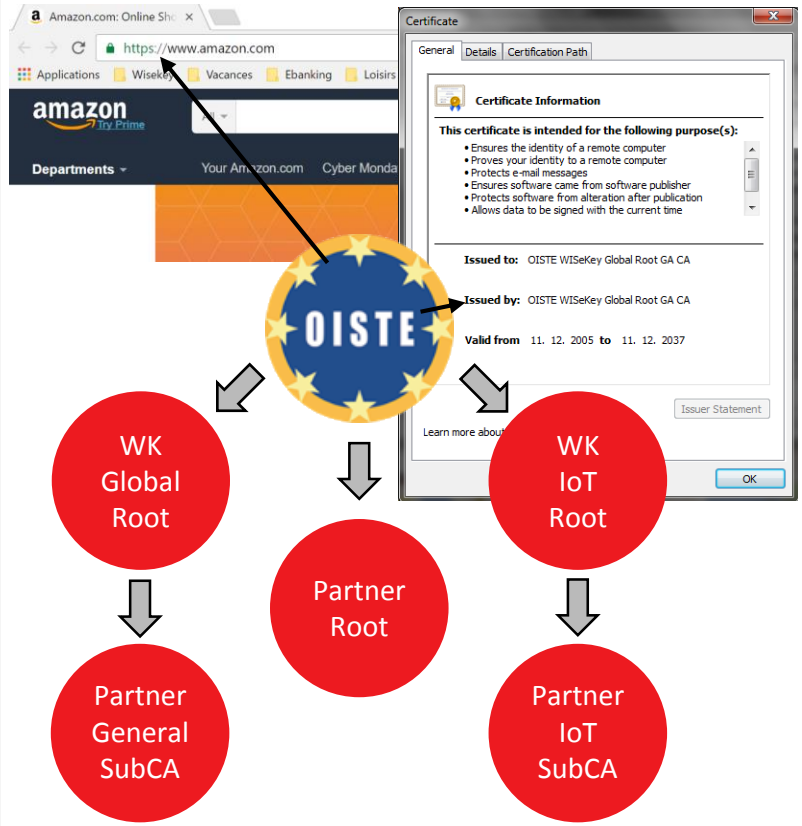
- **WISeKey is bringing trust and security through identity, confidentiality and integrity based on trusted cryptographic root keys.**

Why Switzerland ?

Zone of Mobile Privacy Secured in The Swiss Alps

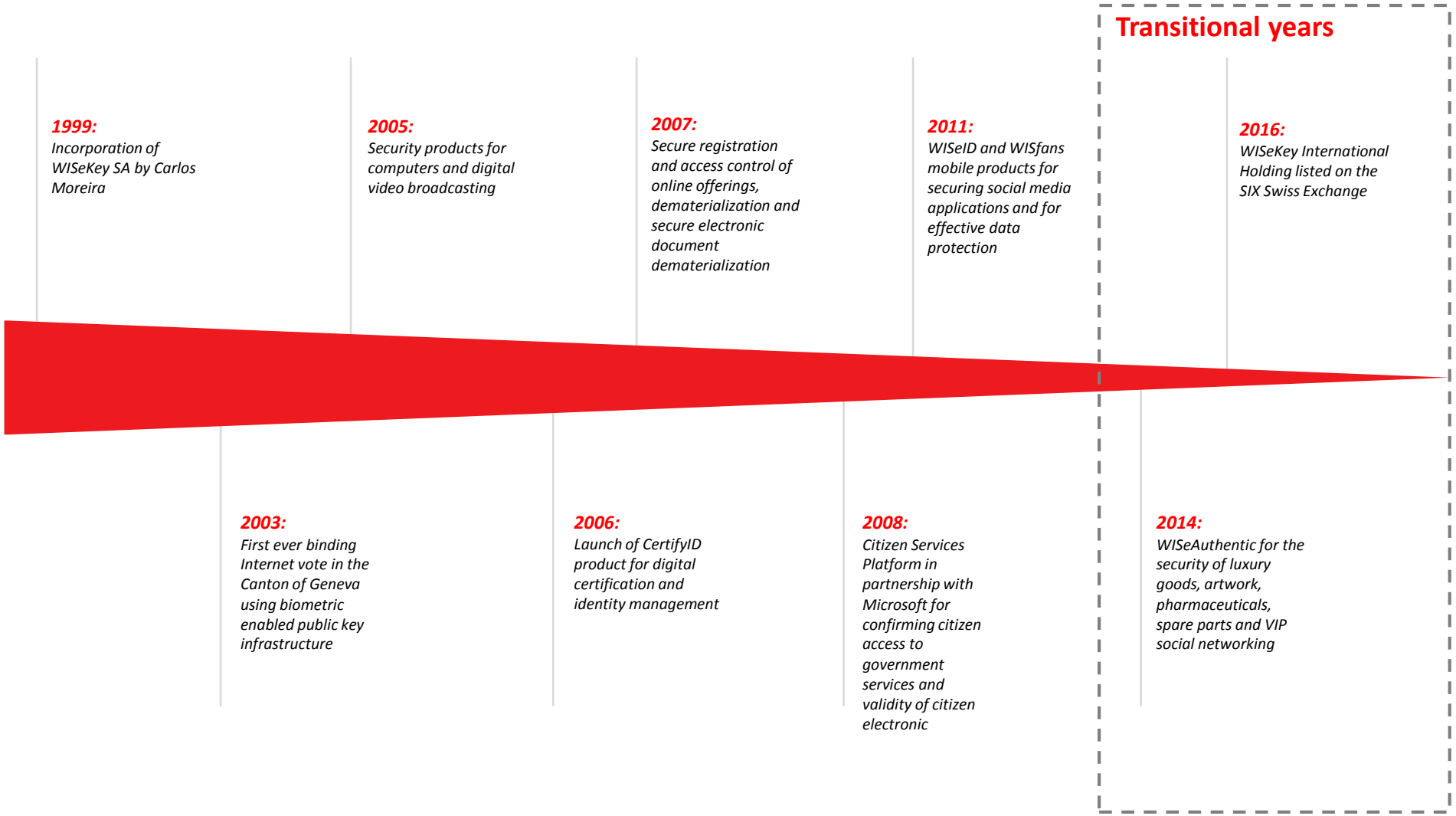
- Outstanding and unprecentend infrastructure
- Leading technology center
- Highly educated employees
- Intellectual property protection
- Most innovative economy according to the Global Innovation Index 2014
- Political and financial stability

ROOT OF TRUST: UNIQUE TRUST MODEL



- The OISTE Foundation was created by the WISeKey Founders to ensure the neutrality of the Trust Services
- The Foundation is regulated by the Swiss laws and enforces values to protect the Neutrality and Sovereignty of the data and identities
- WISeKey is nominated as the operator of the Trust Model, but the by-laws of the Foundation allow the participation of other players, operating their own Root of Trust
- The OISTE Foundation is recognized by the United Nation with an special ECOSOC consultative status, and participates in different initiatives promoted by UN to universalize the access to the electronic identities

KEY MILESTONES – PROVEN TRACK RECORD SINCE THE INCORPORATION IN 1999



WISEKEY'S CERTIFYID: OUR PKI TECHNOLOGY

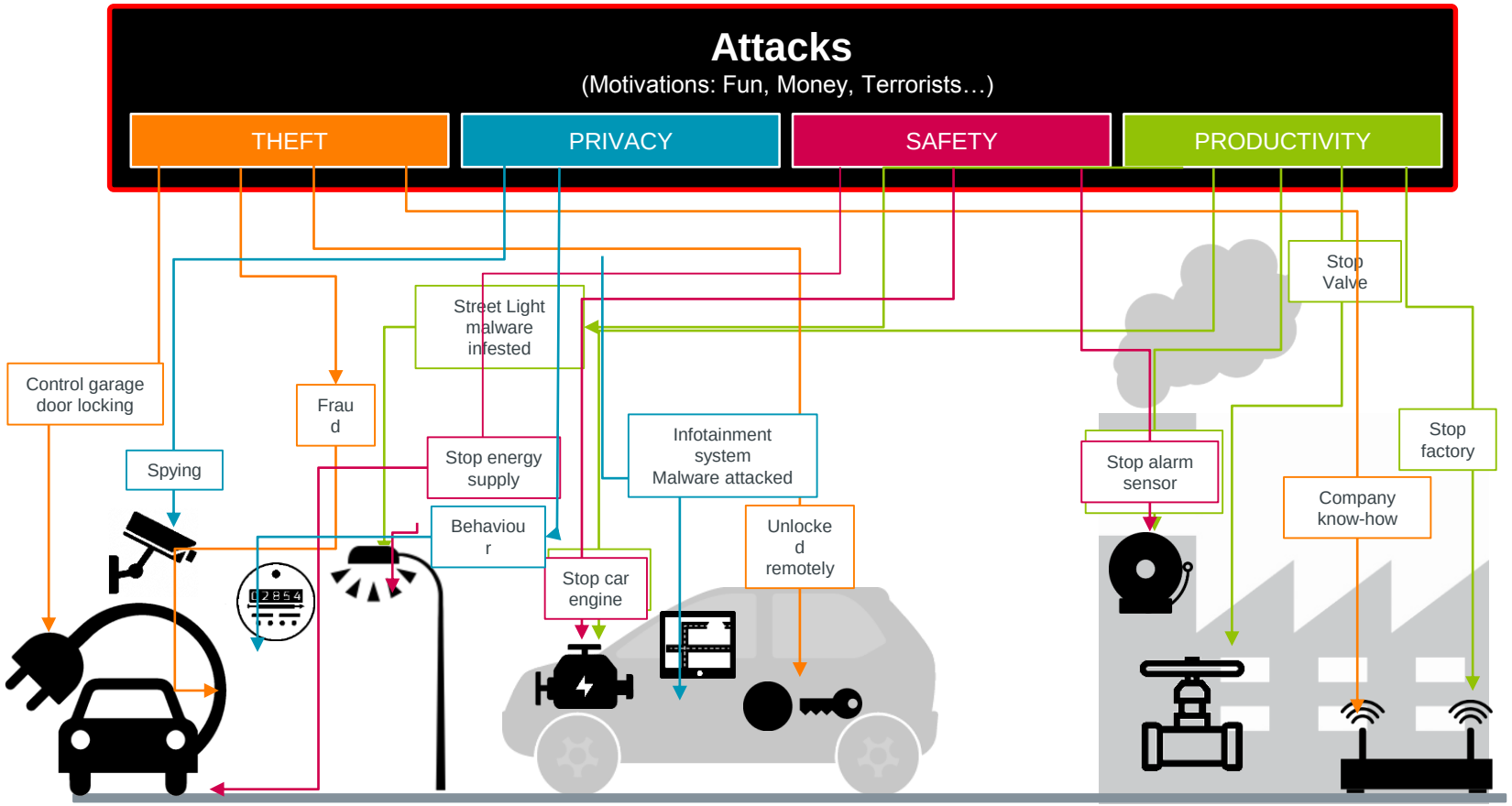
- **Complete suite of PKI Products:**
  - Advanced Certificate Management solution
  - Fully integrated with Microsoft Certification Services and Active Directory
  - Open interfaces for custom integrations
  - Unique Mobile Device Strategy
- **TrustCenter License: Adherence to OISTE Trust Model:**
  - Corporate CAs are signed by the WISeKey Trusted Root CA
  - Certificates issued by the Corporate PKI are automatically recognized as trusted for third parties
  - Reduces dramatically costs and time-to-market
- **Professional Services:**
  - Deep understanding and experience in the technical, legal and operational implications of running trusted Certification Authorities
  - Full range of PS offering, from senior consultancy to software integr services

SECURITY FOR SMART CITIES

Offering

SECURITY REQUIREMENTS FOR SMART CITIES

IoT Requires Scalable Security Solutions (Different needs that may evolve)



TECHNOLOGY ALLOWS TO CONNECTED PEOPLE-TO-MACHINES AND MACHINE-TO-MACHINES

Gather and Analyze data

Offer new products and services

Improve Life quality

Optimize Processes and resources, Reduce Risk toward end users, Improve Processes

Possible only if data can be trusted:
- Source: authentication
- Integrity

(at rest and in transit)

New Threats: Attacks

DDoS, Men in the middle…)

Motivations: Fun, Money, Terrorists…

- THEFT (data, IP, objects..)
- PRIVACY
- SAFETY
- PRODUCTIVITY (Quality of Service)

A vertically integrated digital identity platform interconnecting its cybersecurity offering and IoT ecosystem.

WISeKey

WISeKey is bringing trust and security through identity, confidentiality and integrity based on trusted cryptographic root keys.

WISEKEY'S IOT SECURITY PLATFORM

Identity Management

Trusted Identities for Objects, Applications and Users:

- Root of Trust
- Standards-based Certificate Management solution
- Open and scalable identity distribution

Transaction Assurance

Using PKI technology to ensure authenticity, integrity and confidentiality of the transaction:

- Only trusted entities can connect and transact in the IoT platform
- Data managed by the platform is protected

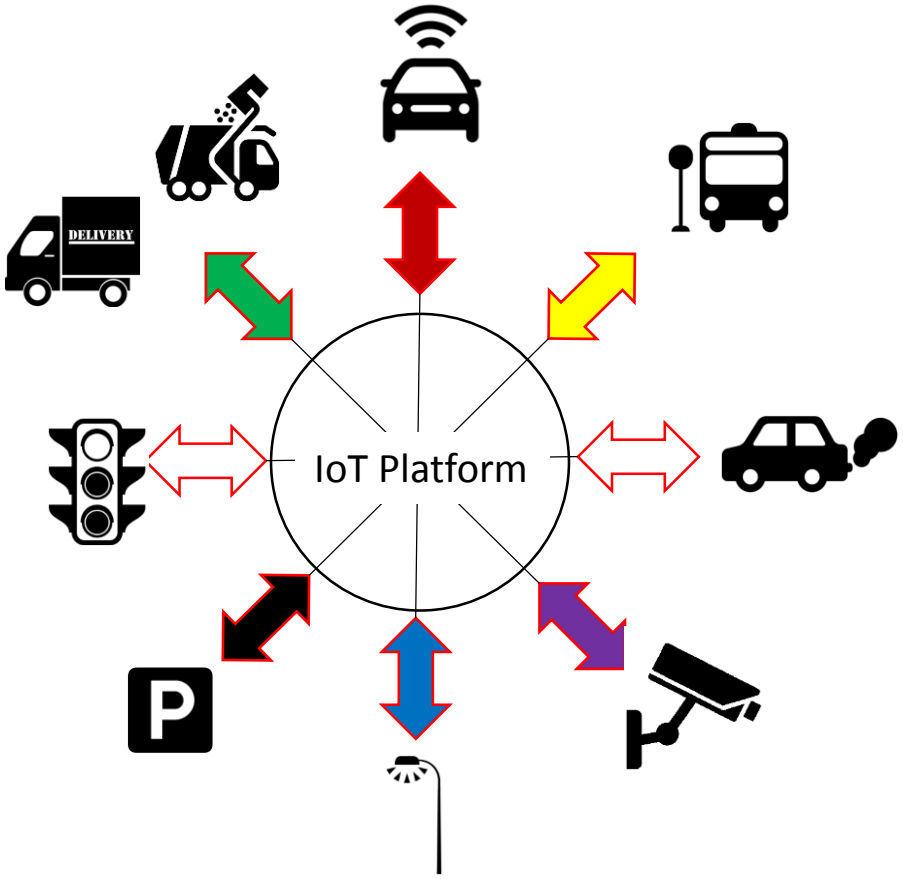
Process Integration

Open API to integrate the IoT platform with the business processes:

- Automation of identity management tasks
- Object's attributes and lifecycle assurance
- Custom connectors can be easily built for business applications

A CONNECTED WORLD THROUGH AN IOT PLATFORM – WISEKEY

- **Create an identity on a single format for each connected object**
  - Identity based on Digital Certificate is a proven standard solution
  - Identity store in a tamper prof secure element for critical use cases
- **Secure messaging**
  - Use one or a few message format for device to talk securely to the network
- **WISeKey Framework hosted an IoT Platform**
  - Control the identity
    - Identity provisioning
  - Interconnect the devices
  - Control back-end applications

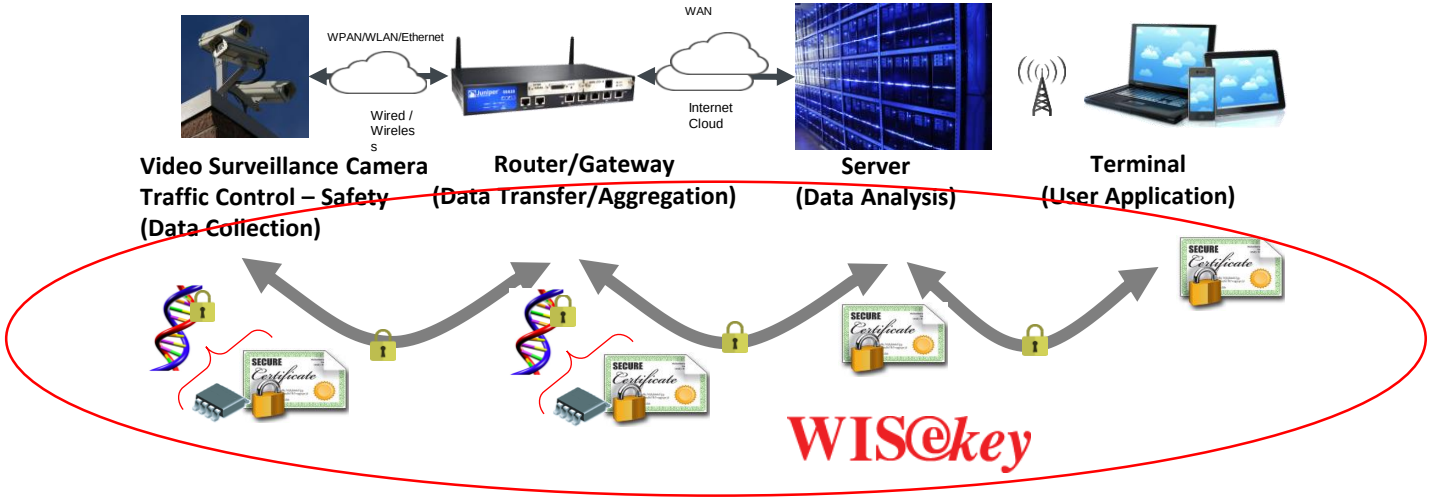


SAP HANA

Microsoft Azure

WISEKEY OFFERING FOR IOT SUMMARY – TOP VIEW

End to End Scalable and Flexible Security Solution



End-to-end security:

In Operation:

Identification, secure communication and Integrity through digital certificate and PKI technology
Storage of critical asset in tamper resistant chip (Secure Element) - Optional
Certificate Generation and Management tools and services
Certificate Authority
Data Management Solutions

During Manufacturing /Maintenance

Device configuration, software upgrade late in the manufacturing process, operated in a non-secure environment

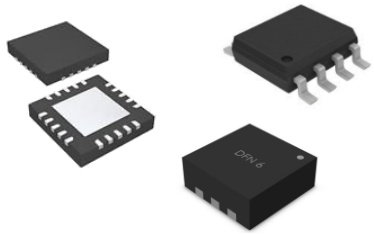
VAULTIC: TAMPER RESISTANT CHIP (SECURITY MODULE/ELEMENT)

VaultIC is a tamper resistant chipset product family (companion chip to IoT device Host processor)

- Embedded configurable cryptographic tool boxes for Authentication, Confidentiality, Integrity* executed in a secure environment
- Embedded on-chip tamper resistant data storage capabilities (NVM) for keys, certificates, and customer data*
- Embed True Number Generator to guarantee the entropy needed for crypto
- Top security assessed through Certifications
  - VaultIC is FIPS 140-2 Level 3 certified
  - VaultIC is based on state of the art security chip: certified against Common Criteria EAL4+/5+
- Tiny industry standard packages and interfaces (I^2C, SPI, USB…)

VaultIC Middleware

- Drivers for interfaces (I^2C, SPI, USB…)
- EasyPlug Middleware (PKCS#11 Windows CSP) to redirect crypto function to the vaultIC
- Secure boot (under construction)
- Secure firmware update
- Secure Communication software (linked to VaultIC) (under construction)
  - MacSec, SSL (depending on the targeted communication layer)
- Secure Binding (establishing a strong link between a VaultIC with the device)



* Product dependent

WISEKEY CMS

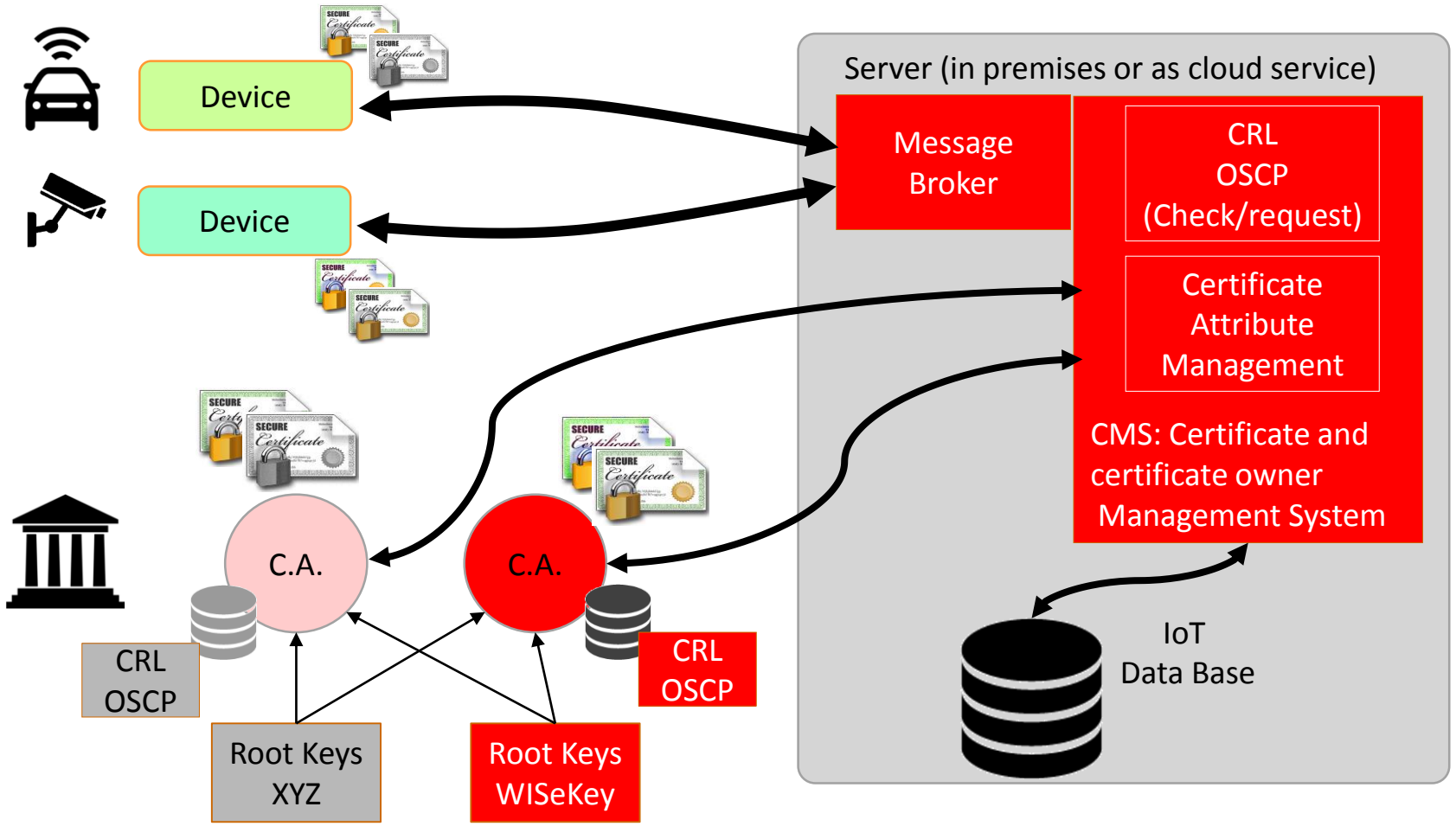
WISeKey supplies the PKI technology to provide the required services for the appropriate management of the life-cycle of identities (digital certificates) of persons, objects and applications:

- Multi-tenant CMS solution (developed by WISeKey) to manage the lifecycle of end-entities (persons, devices…) and their certificates (issuance, revocation...)
- Offers an administration browser interface and a web-services API that can be easily integrated to automate the certificate management tasks
- Can be deployed on-premises or provided as a service
- Compliant for chip based implementation and full software implmentation

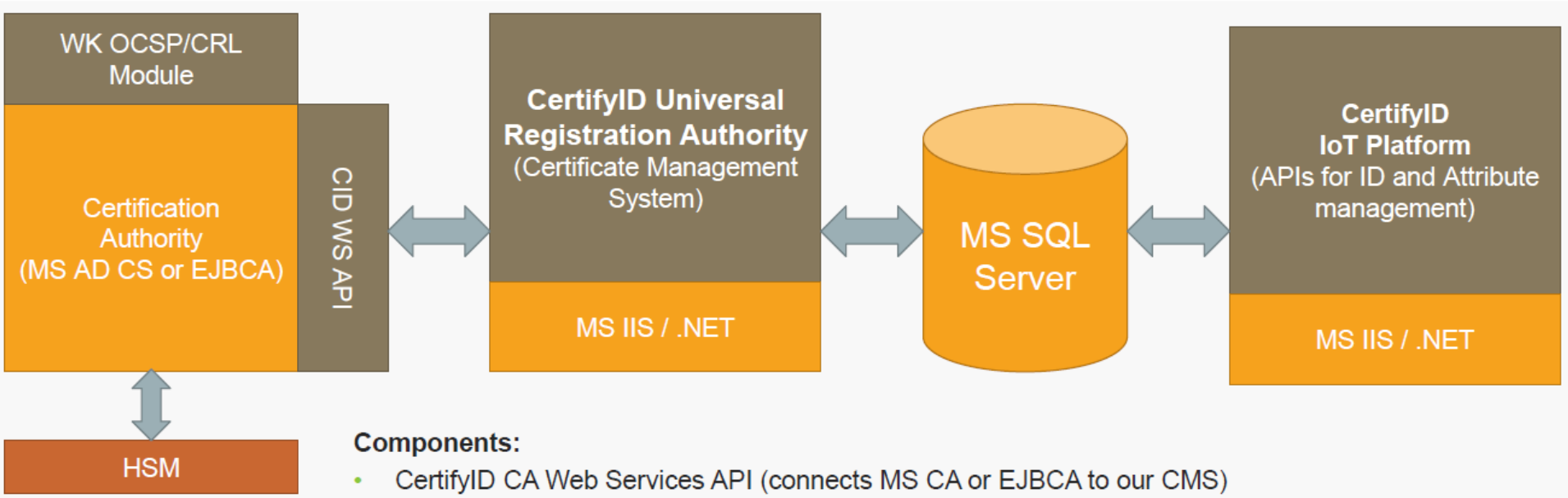
WISeKey also operates a Webtrust accredited Trust Model, so customers can **optionally** decide to have their certificates issued under a publicly trusted CA under our Root

IOT PLATFORM ARCHITECTURE

Delivered by WISeKey



IMPLEMENTATION EXAMPLE FOR IOT IN PREMISES

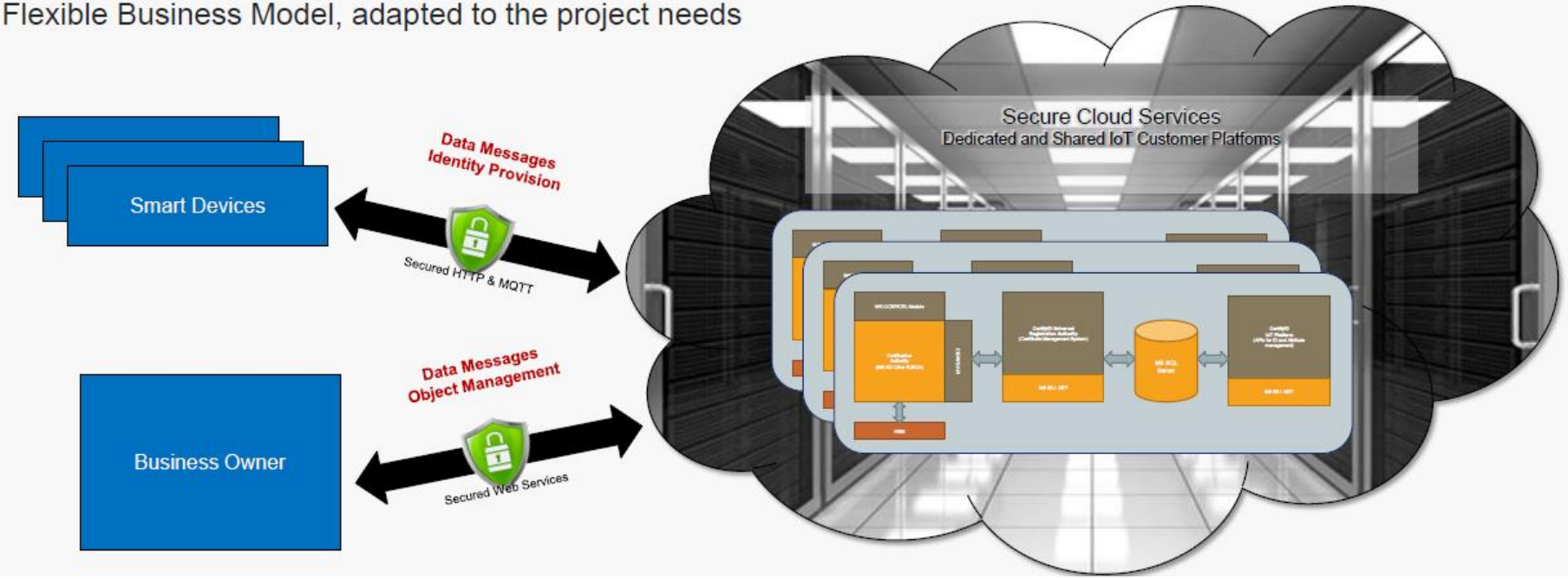


Components:

- CertifyID CA Web Services API (connects MS CA or EJBCA to our CMS)
- CertifyID URA (our CMS. Product built on .NET
- CertifyID IoT components (can run in the same server than the CMS)
- WISeKey OCSP module (provides real-time OCSP capabilities to a MS CA)
- Third party components: HSM (if required) and SQL Database (MS SQL Server)

A FLEXIBLE OFFER 1/2

- For customers not willing to deploy their own infrastructure, WISeKey can provide managed services from our secure datacenters in Switzerland, USA and China
- Customers can choose among a securely shared or dedicated platform
- The managed platform can be accessed through browser and web-services API
- Flexible Business Model, adapted to the project needs



A FLEXIBLE OFFER 2/2

- Customers can choose among three options for the CA and trust model:
  - Dedicated Private CA not under WISeKey's Root
  - Dedicated Publicly Trusted CA, signed by the WISeKey's Root
  - Shared Publicly Trusted CA, owned by WISeKey
- Additionally, customers can choose among four deployment options:
  - On-Premises Dedicated CA (Private or Public), accessible through a dedicated CMS infrastructure hosted by the customer in its premises
  - Managed Dedicated CA (Private or Public), accessible through a dedicated CMS infrastructure hosted by WISeKey
  - Managed Dedicated CA (Private or Public), accessible through a shared(*) CMS hosted by WISeKey
  - Managed Shared Public CA, accessible through a shared(*) CMS hosted by WISeKey

(*) A single instance of WISeKey's CMS (namely CertifyID Universal Registration Authority) is designed to support any number of CAs and it allows to create groups to manage sets of users and certificates, and delegate safely the administration of each group to a different entity

Thank you for your attention!

WISeKey