IoT and security
MobileKnowledge

MobileKnowledge is a team of HW, SW and system engineers, experts in smart, connected and secure technologies for the IoT world. We are your ideal engineering consultant for any specific support in connection with your IoT and NFC developments. We design and develop secure HW systems, embedded FW, mobile phone and secure cloud applications.

Our services include:

- Secure hardware design
- Embedded software development
- NFC antenna design and evaluation
- NFC Wearable
- EMV L1 pre-certification support
- Mobile and cloud application development
- Secure e2e system design

We help companies leverage the secure IoT revolution
We are your ideal **engineering consultant** for any specific support in connection with your **IoT** developments, applications and related secure ecosystem.

We design and develop secure HW systems, embedded FW, mobile phone and secure cloud applications.

**Everything you need to build a trusted, future-proof, and robust solution**
IoT is opening new business opportunities across nearly every sector, but when we multiply the connections between the physical world and the cyber world, we also multiply the risks.

We therefore need to:

- safeguard **integrity** of code running on devices.
- authenticate users and their devices.
- protect your system from cyber and physical attacks.
- protect the **privacy** of sensitive user data.

MobileKnowledge will help you choose the right **end-to-end security measures** tailored to your solution, at device, network and system levels, and in the most effective and efficient way.

Security needs to be built in from the start, with device and data security fully integrated to protect all IoT applications and solutions.
What security architecture do I need?

We provide a structured process for understanding your security needs and selecting your security strategy

A complete understanding of the application allows the user to identify possible threats and, therefore, decide on the security measures to incorporate.

Whether you want:

- to protect your brand and ensure the authenticity of each of the devices within the network.
- to ensure you have a secure and trusted connection to the backend.
- to protect the end consumer’s data privacy.
- or to protect your system software from attackers by ensuring a secure boot and secure update.

Maintain full control of your solution when deployed in the field and avoid attackers damaging your business.

We will help you build a holistic security approach to your solution

1. Understand the solution and identify threats
2. Select the required security measures
3. Define the security strategy and how to implement the adopted measures

Usual security measures

- **Device origin and integrity**: Ensure that the combination of HW/SW is kept under control of device manufacturer, avoid vulnerabilities in the field
- **Data security and integrity**: Ensure that data in and out of the device is protected and kept unaltered
- **Secure OTA upgrade**: Regular SW upgrades are reliable; upgrade device functionalities
- **Authentication**: Ensure that a “trusted” IoT network is established; only original devices work as expected, thus protecting revenues
- **Device life cycle management**: Full control on device status; prevent exploitation of decommissioned devices
- **User privacy protection**: Compliance with GDPR regulations; increased trust in IoT
IoT end-to-end security

MobileKnowledge services

Our services cover the complete IoT ecosystem, from hardware and embedded firmware-related services to mobile or cloud connection gateway solutions up to cloud services development or integration with existing platforms. Our holistic approach to security enables MobileKnowledge to address the complete end-to-end IoT ecosystem.

Connected Devices / IOT
Make the appropriate decisions when designing the HW and the appropriate security architecture for your solution
- Support in the design of HW with secure elements or authentication ICs
- Support in the development and integration of FW/SW stacks for secure element and cloud connectivity technologies
- Expertise in hardware security, biometrics and sensors

Cloud connection & user experience (mobile/gateway)
Select the appropriate interfaces to interact with your IoT solution while ensuring the overall e2e security.
- Keep control and interact with your solution through a neat and simple user experience
- Development of mobile and PC applications to interact with your IoT devices (Android, iOS) and cloud services
- Commissioning and secure onboarding of IoT devices

Cloud services & platforms
Connect to the appropriate cloud base services for full control of the whole life cycle of your IoT solution.
- Ad-hoc cloud services to support your required use cases
- Server applications development and maintenance
- Support the life cycle management of IoT devices:
  - Secure credential provisioning and management
  - Secure OTA management of IoT devices

---
e2e secure architecture design and consultancy
e2e user experience
We offer you an “à la carte” set of engineering competences where you can find and select the support you need.

**IoT end-to-end security**

**MobileKnowledge competences**

- **Connected Devices / IOT**
  - Make the appropriate decisions when designing the HW and the appropriate security architecture for your solution
  - **System, HW & SW Design**
    - RF performance
    - EMV L1
    - NFC Antenna Design
    - User Experience
    - Power Consumption
    - Innovative Antennas
    - Wireless Charging
    - Energy harvesting
  - **Applet**
  - JC
  - RTOS
  - SigFox
  - NFC
  - SE
  - HOST
  - CONN

- **Cloud connection & user experience** (mobile/gateway)
  - Select the appropriate interfaces to interact with your IoT solution while ensuring the overall e2e security.
  - **Android**
  - iOS
  - User Experience
  - UI Design
  - Backend integration
  - **Applet**
    - JC
    - RTOS
    - SigFox
    - NFC
    - SE
    - HOST
    - CONN

- **Cloud services & platforms**
  - Connect to the appropriate cloud base services for full control of the whole life cycle of your IoT solution.
  - **Cloud platform integration**
    - Certificate generation
    - Certificate provisioning
    - Key provisioning
  - **PKI management services**
  - **Cryptographic services**
  - **Device management services**
  - **Global Platform**
  - **Transport Layer Security (TLS/SSL)**
  - **Android**
  - **iOS**
  - **User Experience**
  - **UI Design**
  - **Certificate generation**
  - **Certificate provisioning**
  - **Key provisioning**
  - **Transport Layer Security (TLS/SSL)**

**Additional Services**

- **RF performance**
- **EMV L1**
- **NFC Antenna Design**
- **User Experience**
- **Power Consumption**
- **Innovative Antennas**
- **Wireless Charging**
- **Energy harvesting**
- **Android**
- **iOS**
- **User Experience**
- **UI Design**
- **Certificate generation**
- **Certificate provisioning**
- **Key provisioning**
- **Transport Layer Security (TLS/SSL)**

**Platforms and Services**

- **Android**
- **iOS**
- **User Experience**
- **UI Design**
- **Certificate generation**
- **Certificate provisioning**
- **Key provisioning**
- **Transport Layer Security (TLS/SSL)**
NFC end-to-end secure applications
MobileKnowledge competences

**NFC / Connected Devices**
- Make the appropriate decisions when designing the HW and the NFC secure architecture for your device
- RF performance
- EMV L1
- NFC Antenna Design
- User Experience
- Power Consumption
- Innovative Antennas
- Wireless Charging
- Energy harvesting

**Mobile connection & user experience**
- Select the appropriate interfaces to interact with your NFC device while ensuring the overall e2e security and a great consumer experience
- Android
- iOS
- User Experience
- UI Design

**Cloud services & platforms**
- Connect to the appropriate cloud based provisioning services (payment, access, transit …)
- Cloud platform integration
- Wallet Server
- NXP Service Platform
- Key provisioning

**System, HW & SW Design**
- RTOS
- SigFox
- JC
- FW
- Bluetooth
- Linux
- ZigBee
- LoRa
- MQTT

**Backend integration**
- PKI management services; Loader Service ecosystem (Applet, Client MW, Root Entity)
- Security (Crypto, SE, TLS, HSM …)
- Global Platform
- MIFARE ecosystem (Applet, Client MW, Backend Service)
- NFC Wearable stack

We offer you an “à la carte” set of engineering competences where you can find and select the support you need.

Make the appropriate decisions when designing the HW and the NFC secure architecture for your device.
Select the appropriate interfaces to interact with your NFC device while ensuring the overall e2e security and a great consumer experience.
Connect to the appropriate cloud based provisioning services (payment, access, transit …)