

SE保驾护航物联网安全

October 2017 @ SCA

Yuyang Wang
Product & Marketing Manager



SECURE CONNECTIONS
FOR A SMARTER WORLD



IOT SECURITY

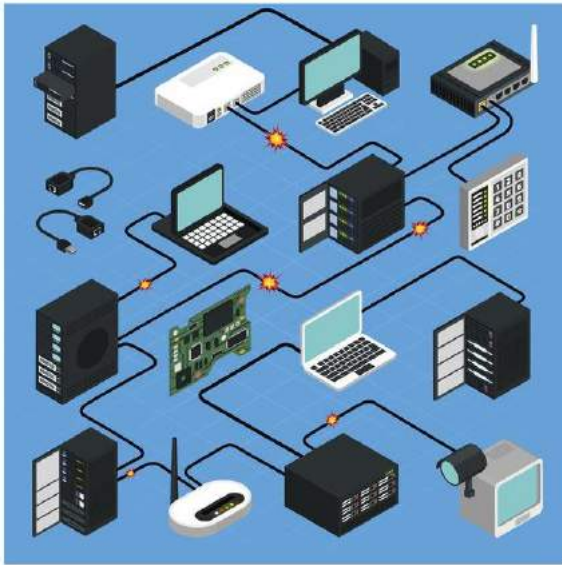
The lack of Security in IoT is now tangible

LILY HAY NEWMAN SECURITY 12.09.16 7:00 AM

THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY

Mirai botnet

Disruption of major Internet services



Software bug makes Nest Cams vulnerable to hacks



Jeep hack

Loss of control over vehicle



Nest Hack

Security camera shut down by a simple click on a phone

A Risk Exacerbated by Hacking Tools' Availability



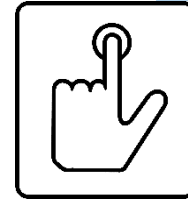
- Hackers do not necessarily need to be highly skilled to replicate attacks, leveraging hackers' work
- Internet search engines like Shodan or Censys provides powerful tools to spot/locate vulnerable devices
- End 2015, security researchers found with the help of Censys that lazy manufacturers of home routers and Internet of Things (IoT) devices have been re-using the same set of hard-coded cryptographic keys, leaving around 3 millions of IoT devices open to mass hijacking.



What is IoT Security?

Common today's attacks

1. SW bugs leveraged to inject malware, leak data, etc,
2. Insecure SW Update
3. Lack of (strong) authentication & encryption
4. Absence of access control to device features



Required Security Technologies

Device hardening

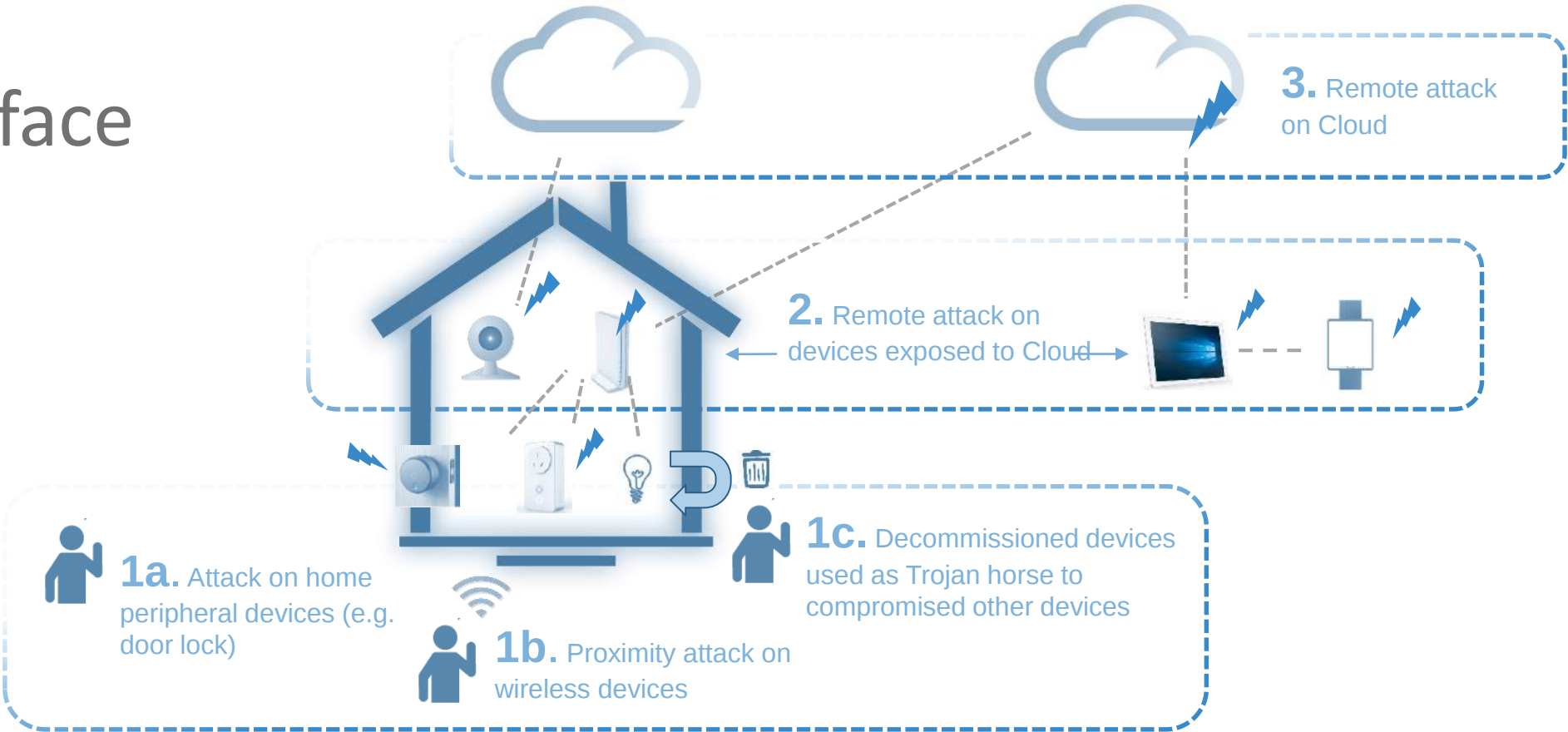
Authentication

Public Key Infrastructure

API security

Identity & Access Management

A Large Attack Surface



1

Local Attacks on
Nodes

Reach of attack: ● ○ ○

2

Remote Attacks on
Gateway/Router/Edge Nodes

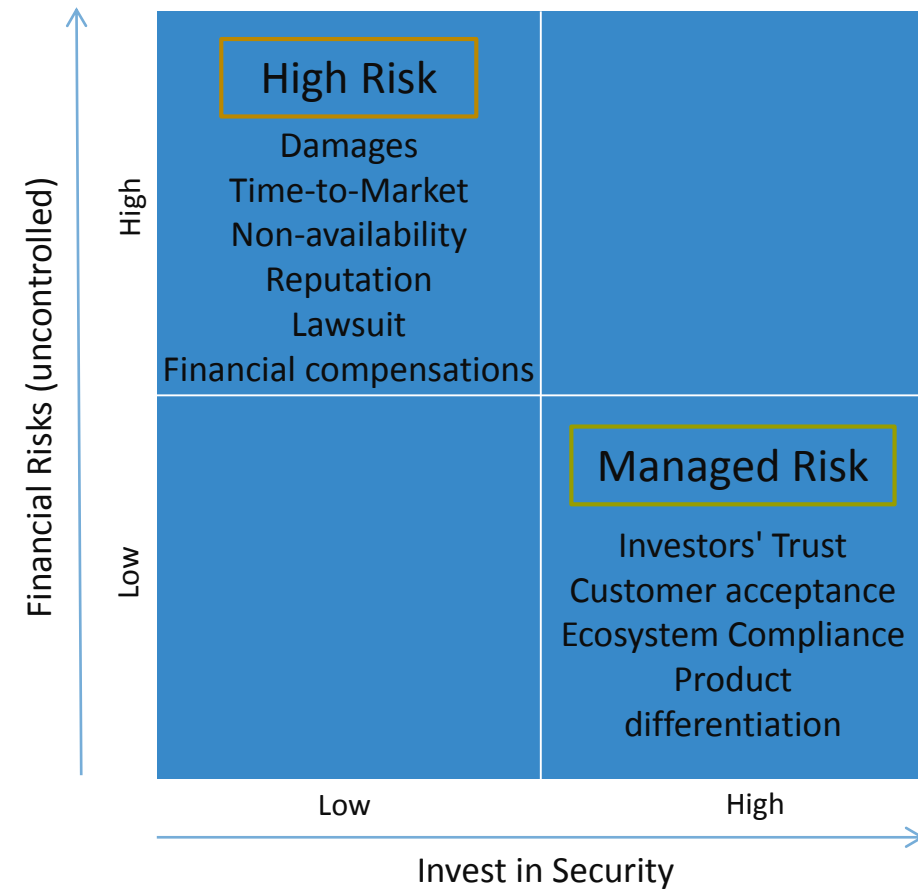
Reach of attack: ● ● ◐

3

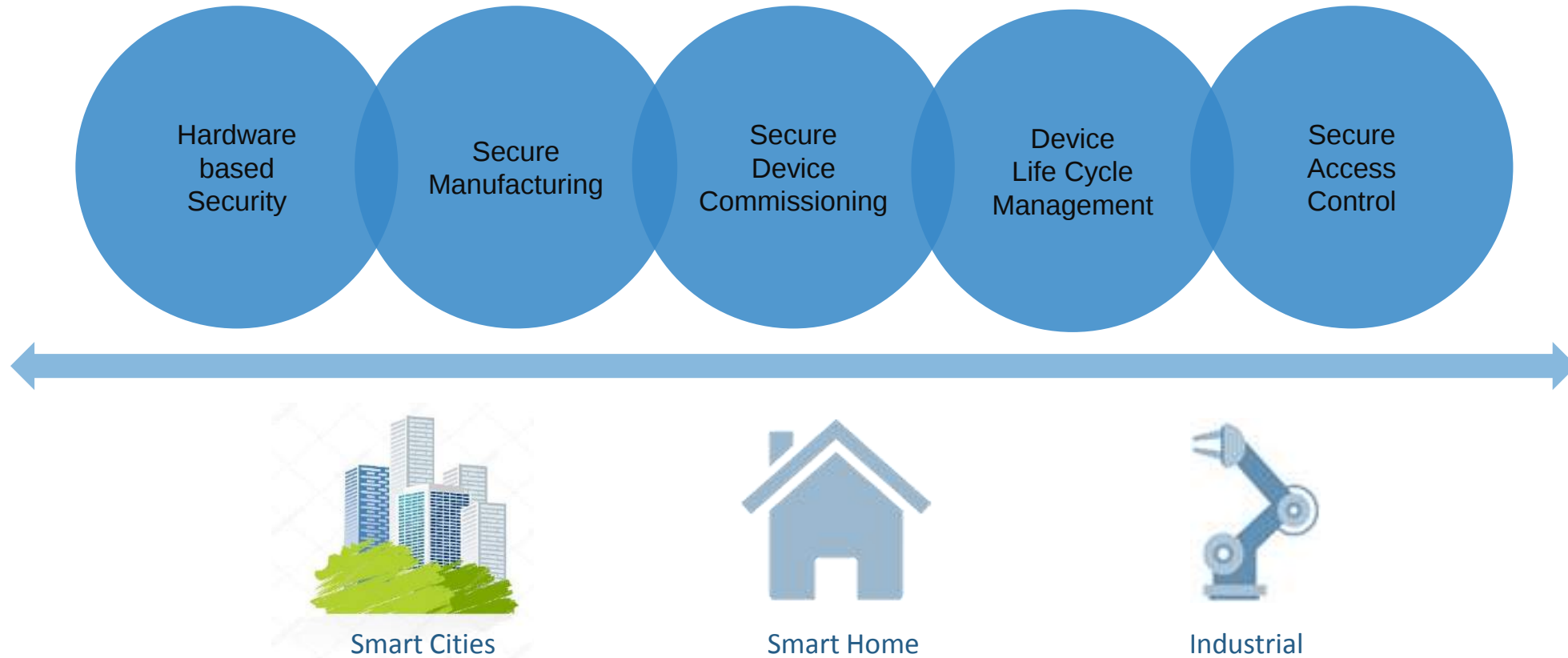
Remote Attacks on
Cloud Service Providers

Reach of attack: ● ● ●

Non-Security has a cost for OEMs!



Security is a Risk – NXP is the Partner to manage this Risk





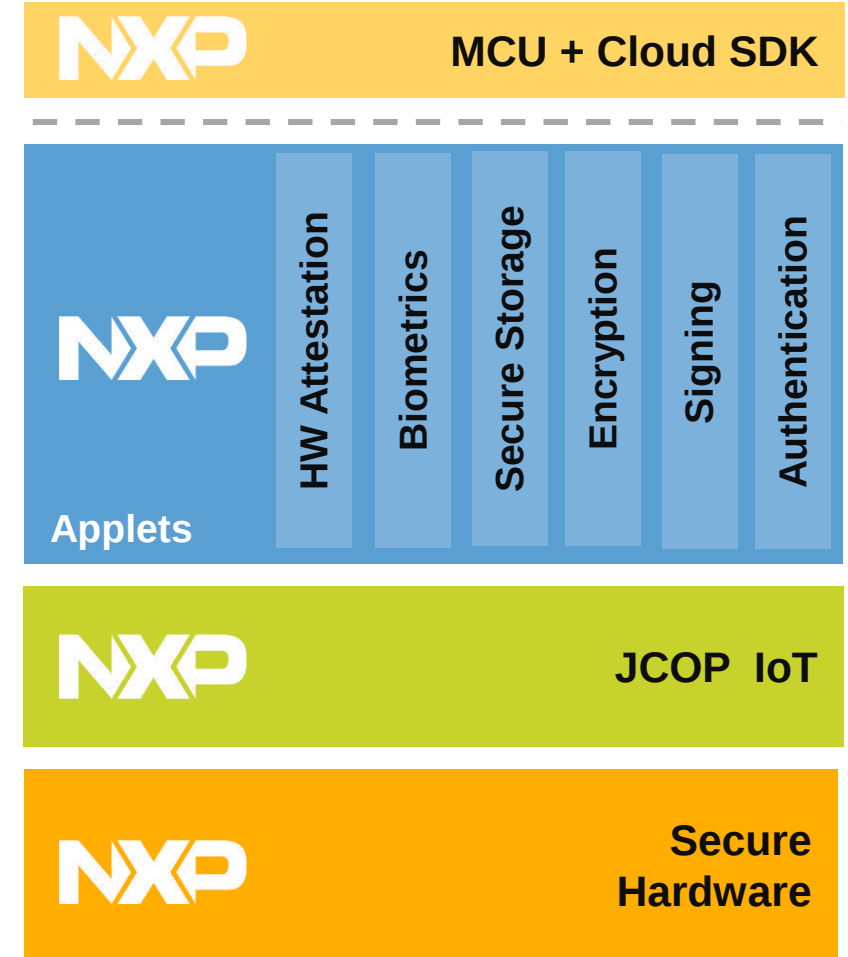
NXP SECURE IDENTITY TECHNOLOGY



NXP IoT PLATFORM – ONE STOP SHOP WITH JCOP PLATFORM



- ✓ Absolute Flexibility
- ✓ Shortest TTM
- ✓ Strong security
- ✓ Easy integration with IoT Clouds
- ✓ Global Standards
- ✓ HW Attestation



Key Applications

A-Series Security ICs



COMPANY CONFIDENTIAL

- **Energy Management / Smart Grid**
 - Smart Home Appliances, smart Plugs
 - Residential & Industrial Meters
 - Metering Gateways
 - Home & Building Automation systems
 - Grid Automation
 - Data concentrators, routers
 - Electrical & Hybrid Vehicles
 - (H)EV Charging Stations, batteries
 - Street Lighting, Solar panels
- **Industrial**
 - PLC, RTUs, IED, Industrial equipment & parts, remote monitoring systems
- **Medical & Healthcare**
 - Home care/monitoring Gateways
 - Medical Devices
 - Traceability solutions
- **Transport**
 - ITS (car2car), Telematics
 - Infrastructure networks, Tolling
- **Vending**
 - PoS terminals, ATMs
- **Smart Applications/Services**
 - IP cameras, sensors, Smart Cities, Smart Homes, Automation systems, etc
- **Security Systems**
 - Authentication tokens, access control systems, biometric controls, etc



Example 1: NXP securely connects UK Smart Energy Infrastructure



UK is about to deploy more than 100 millions smart energy equipment including residential communication hubs, gas & electricity meters, In-home displays, in order to optimize energy management in the country



NXP will connect a significant part of the UK infrastructure with a secure connectivity chipset enabling zero-touch secure commissioning of hubs and smart meters



NXP receives Cyber Security Award at Smart Metering Europe Summit in London

"NXP is a provider which takes the security responsibility of the shoulders of the smart meter manufacturers, and provides a building block that can be integrated into the smart meters to provide a large part of the security functionality"

Example 2: NXP secures German Smart Metering Gateways



A80SM Cyber-Security Solution

**Best-in-class security
for connected devices**

NXP introduces the A80SM turnkey solution; a high performance security module designed to meet the most demanding embedded applications, including Common Criteria certification (EAL4+) against Protection Profile BSI-CC-PP-0077 for Smart Metering Gateways.

KEY FEATURES

- ▶ Integral solution built on best-in-class, high-performance NXP secure MCU family A800x
- ▶ ECC cryptography with support of NIST P-(256, 384) and BrainPool P-(256, 384, 512) curves
- ▶ ECDSA digital-signature generation and verification
- ▶ Key agreement based on Diffie-Hellman (ECCA-ECDH) and El-Gamal (ECCA-EG)
- ▶ On-chip ECC key generation
- ▶ True random-number generation
- ▶ ISO 7816 and high-speed (400 Kbits/sec) slave I²C interfaces
- ▶ Secure messaging using Password Authenticated Connection Establishment (PACE: ECDH-GM-AES-CBC-CMAC-128)
- ▶ Commands compliant with ISO 7816-4 and ISO 7816-8
- ▶ Large EEPROM memory (144 Kbytes) for flexible, future-proof storage of keys, certificate, PIN codes, passwords, application data, and (module) firmware upgrades
- ▶ Dynamic file system compliant to ISO 7816-9
- ▶ Secure administration, secure device life-cycle management
- ▶ Operational ambient temp range: -25 to +85 °C (A8003SMHN1)
- ▶ HVQFN32 package (pin-compatible with NXP A70CM turnkey solution)

KEY BENEFITS

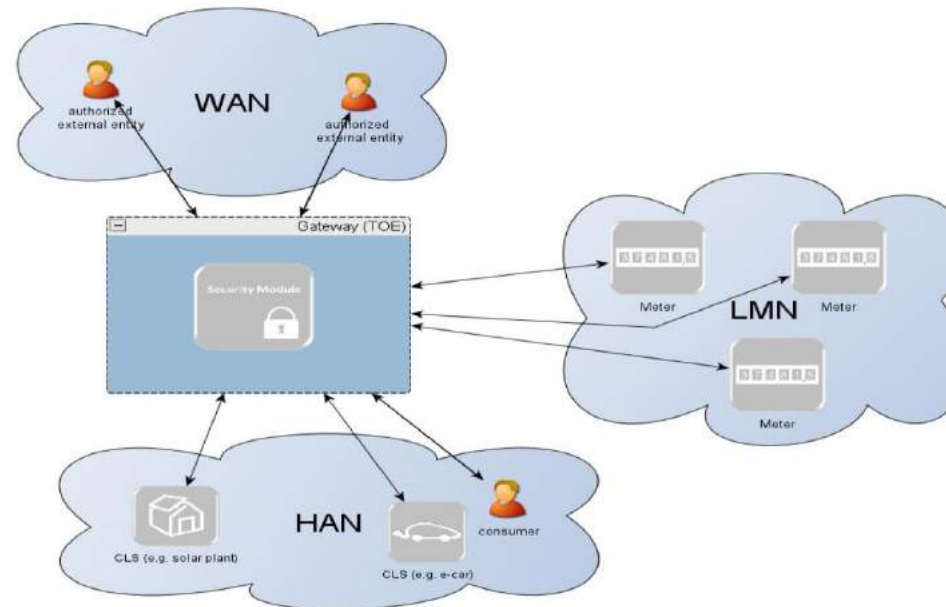
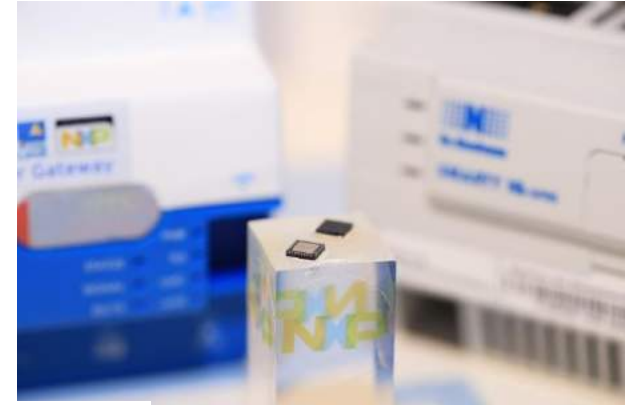
- ▶ Trusted device authentication, encryption, and secure access to infrastructure and services
- ▶ Secure verification of device software integrity
- ▶ Secure key management across untrusted networks or supply chains

KEY APPLICATIONS

- ▶ Smart Grid, Smart Metering,
- ▶ Home/building automation
- ▶ Industrial Automation
- ▶ Energy Management Systems
- ▶ Medical/healthcare devices and gateways
- ▶ Transport (infrastructures, telematics, tolling)
- ▶ Security, monitoring, and access-control systems
- ▶ Vending (POS terminals, cash machines, security tokens)



NXP is leader security provider for Smart Metering Gateways in Germany, delivering state-of-the art, BSI- certified security modules (A80SM)



System integrity, user privacy, brand protection



Thank you, Any Questions ?