NXP SEMICONDUCTORS

Emerging IoT Threats and Ethical Hacking Practical Countermeasure & Solutions

Marc Gebert – Sr. Director BD IoT Security

IoT Week – June 6th, 2018

Secure Connections for the Smarter World

Processing

40B+ devices with intelligence shipped in 2020

Connectivity

1B+ additional consumers online, 30B+ connected devices

Security

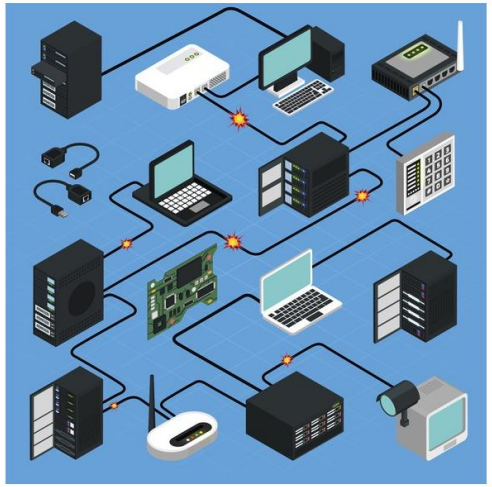
Potential economy savings up to half a trillion dollars

Automotive | Industrial | Connected Devices | Internet of Things

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

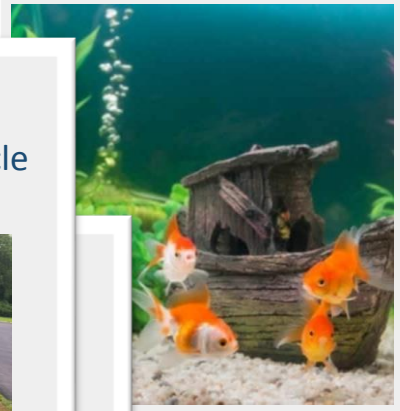
Software bug makes Nest Cams vulnerable to hacks

Nest Hack

Security camera shut down by a simple click on a phone

Jeep hack

Loss of control over vehicle via WiFi connection



Casino hack

Overview of high-rollers extracted via thermostat of a fish-aquarium in the lobby

Target Hack

Target declared that the total cost of the data breach had been $202M *NBC news, May 24, 2017*

TARGET

SEPTEMBER 20, 2017 by Mamta Badkar in New York

Parcel delivery company **FedEx** said on Tuesday that a June **cyber attack** on its **TNT Express** unit **cost** the company **$300m in the first quarter**, … the **NotPetya cyber attack**, which originated from tax preparation software in Ukraine and resulted in the disruption of communications systems at TNT Express.

Attacks occur in many forms: different types and locations

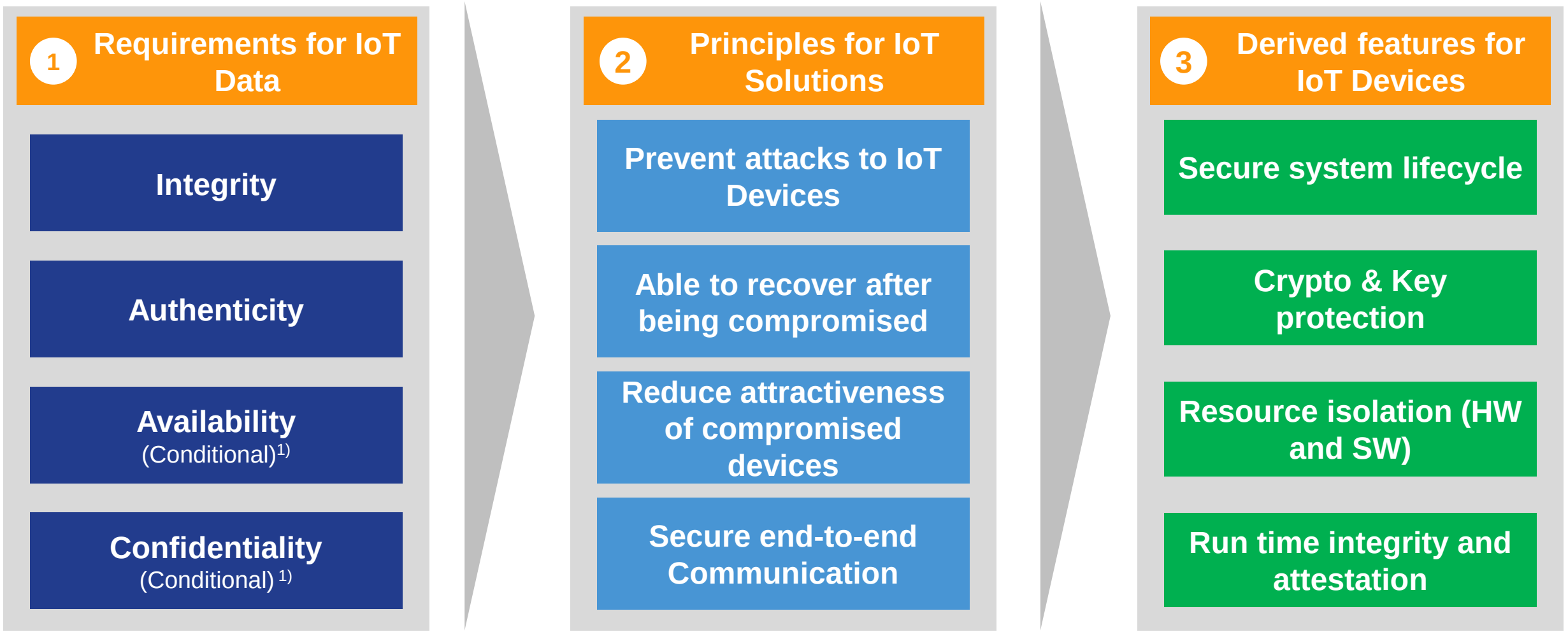
Attack type

- ***Physical*** – making use of physical properties or deficiencies in the device
- ***Logical*** – by sending malicious messages, the software will misbehave

Adversary's location

- ***Local*** – adversary must be in the proximity of the device
- ***Remote*** – adversary can be anywhere

IoT device security features derived for IoT data requirements



1) Conditional requirements depend on the device – they are not always required

Overview of chip based security architectures

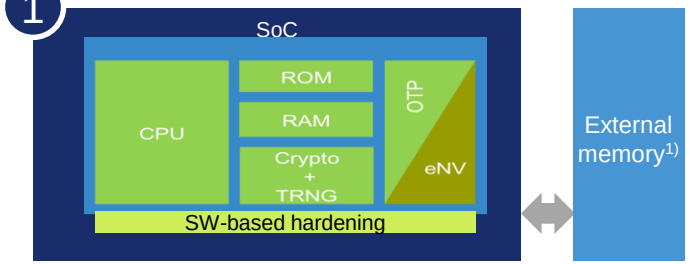
Security Architectures supported by current shipping NXP products

Add Trusted Execution based on ARM TrustZone® and/or isolation features[2] on the SoC

Add SE to architecture

Standard SoC with basic security hardening

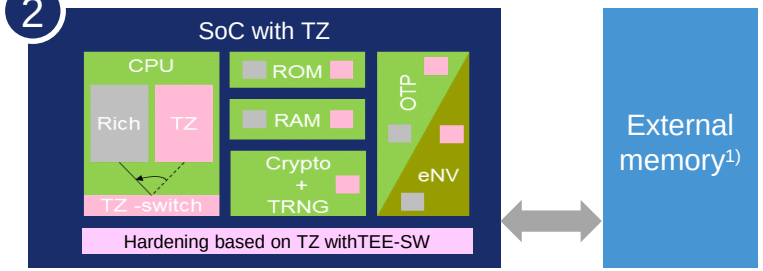
1



Allows for
- *Secure Boot*
- *Secure Debug*
- *Cryptographic Operations*
- *Tamper Detection*

SoC with basic security hardening & TrustZone

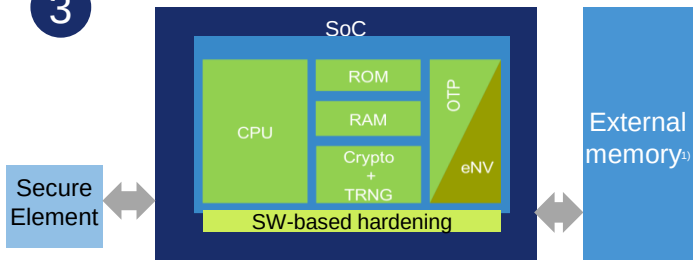
2



Additional features:
- *Secure execution environment (“Trusted”)*
- *Rich execution environment (“Non-trusted”)*

SoC with basic security hardening and a SE

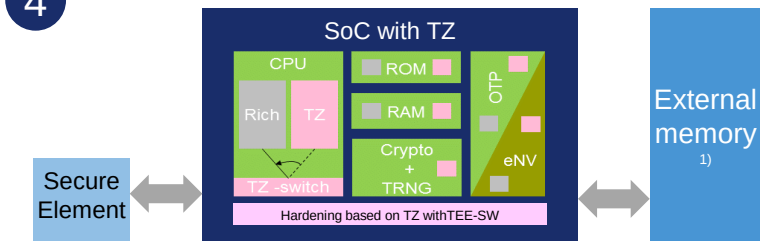
3



Additional features:
- *Tamper Resistant Protection of root keys*
- *Credentials can be securely injected in SE*
- *Provisioned keys are delivered directly to the customer through a secure channel*

SoC with basic security hardening, TZ & SE

4



Additional features:
- *Combined features of architecture 2 and 3*

1) Not mandatory for MCUs/MPUs when they have embedded memory;
2) Features like RDC (Resource Domain Controller) on i.MX

A connected/smart device is vulnerable throughout its lifecycle

Develop, manufacture and distribute

Local Attacks (physical and logical)

- Extract keys/certificates
- Overproduction of original device
- False certificate/private key injection
- Malicious image loading
- Counterfeits of devices
- IP Theft

Remote attacks not possible as device not connected

Onboard, operate and update

Local Attacks (physical or logical) – Device level scale

- Tamper the IC to obtain access to data and SW and re-use for remote attacks (Trojan horse, DoS on Cloud, …)
- Especially dangerous for non-diversified Symmetric key protection: “Break one, Break all”

Remote attacks – All products are the attack surface

- Create unauthorized connection to extract data, abuse functionality or inject malware to turn device into a bot
- Perform malicious software update to do the same

Decommission

Local Attacks (physical and logical)

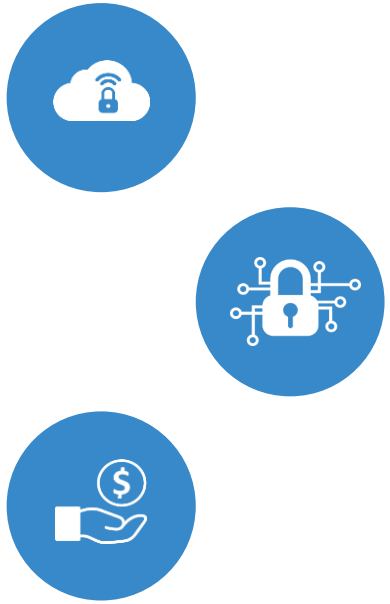
- Extract credentials (user data, keys, certificates)
- Inject malware to network

Remote attacks are possible by re-commission the device to attack the network or cloud

Reasons to consider a secure element in IoT devices

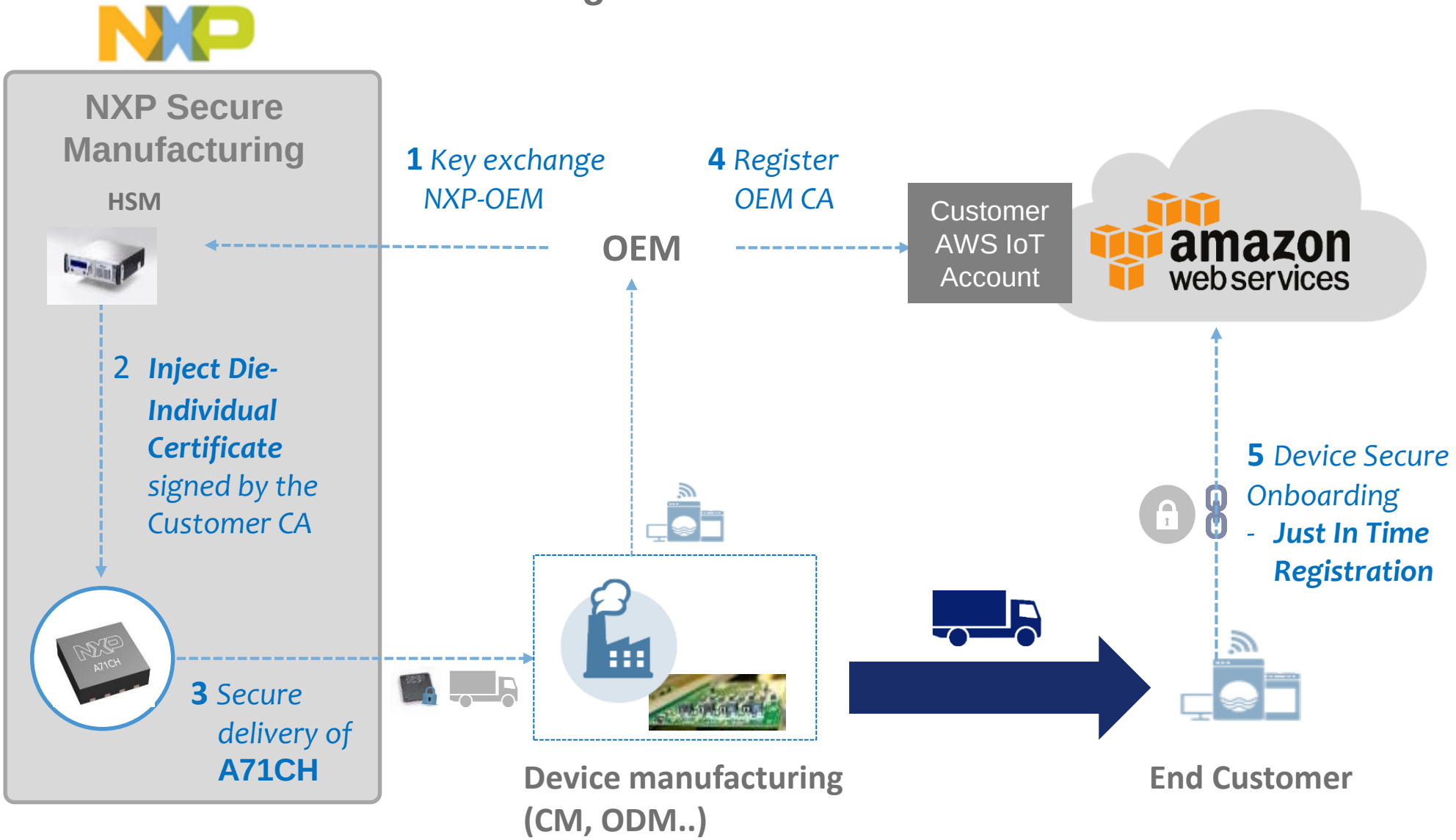
Why a discrete security IC in IoT devices?	
Root of trust	→ Security and key management throughout the whole value chain right from the start
Closed system	→ On Chip NV Memory with access policy → Closed system architecture to isolate memory access from host system. → NV memory only accessible via Chip OS / Applet
Out-of-the-box security	→ Scalable and ready to deploy → No need to develop secure SW

Keeping secrets secret



The Industry starts deploying E2E Security Solutions

NXP and AWS Just-In-Time Registration flow



BENEFITS

- No cost of ownership for key management
- End-to-end Security
- No reliance on EMS (easy switch)
- Less or no CAs to manage

Demand on Security creates need for Political & Industrial Initiatives

1 GDPR

The GDPR is ***strengthening the rights of individuals*** whose personal data is being processed through:

- the need for the individual's **clear consent** to the processing of personal data
- **easier access** by the subject to his personal data
- the **right to rectification**, to erasure and 'to be forgotten‘
- the **right to object**, including to the use of personal data for the purposes of 'profiling‘
- the **right to data portability** from one service provider to another

No privacy without security by design:

- Secure storage of keys
- Individual device ID
- Secure User Identities
- Secure communication channels

2 Charter of Trust

- Charter of Trust first signed at **Munich Security Conference, February 2018**
- Set the pace for **binding rules and standards** that ***build trust*** in cybersecurity and ***drive forward digitalization*** globally
- **12 partners** from different sectors signed the charter of trust, including NXP

Key principles:

- Ownership for cyber and IT security
- Responsibility throughout the digital supply chain
- Security by default
- User-centricity
- Innovation and co-creation
- Education
- Certification for critical infrastructure and solutions
- Transparency and response
- Regulatory framework
- Joint initiatives

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP and the NXP logo are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2018 NXP B.V.