Training Mobile Knowledge

Security in NFC Readers

Public

Content

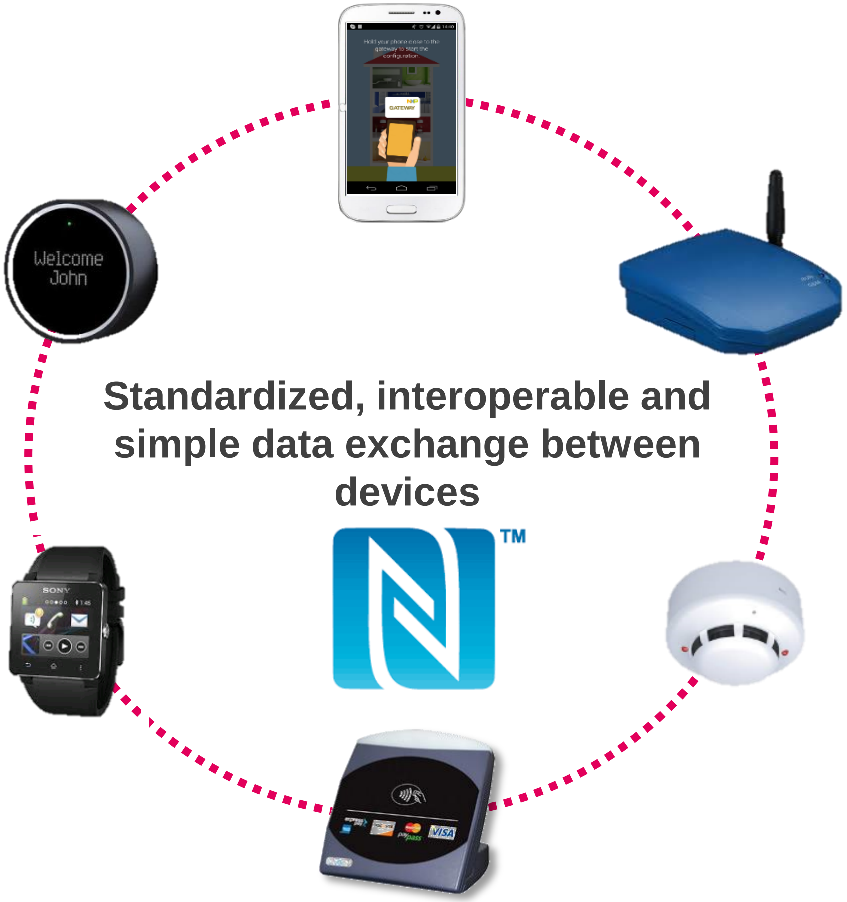
- NFC and security
  - NFC, a different kind of wireless
  - Under the hood of NFC based systems
  - Enhancing the security of an NFC architecture
- Secure data exchange
  - Information security goals
  - Cryptographic techniques
  - Secure Access Module
- Unauthorized access protection
  - Remote access
  - NFC interface access
- Use cases
  - Access control system
  - Internet gateway
- NFC security cookbook and conclusions

NFC AND SECURITY

NFC, a different kind of wireless

NFC at a glance:

- Contactless proximity technology
- Standardized under ISO/IEC18092 and ISO/IEC 21481
- Operating range: 10 cm (4 in)
- Easy, simple and convenient data exchange between devices
- Open and interoperable data following NFC Forum specifications
- Privacy and security inherent to short range



Standardized, interoperable and simple data exchange between devices

The three modes of NFC: A tap is all it takes

Read/Write Mode

- Interacts with an NFC-enabled device
- Reads data in from device or writes data out

Get information or initiate an action

Peer-to-Peer Mode

- Establishes two-way communication between NFC-enabled devices
- Each device serves as an endpoint

Passive and active communication

Card Emulation Mode

- System behaves as contactless smartcard*
- Makes NFC-enabled systems compatible with contactless cards

Ticketing, payments, access control, transit…

** ISO/IEC 14443-compliant smartcard*

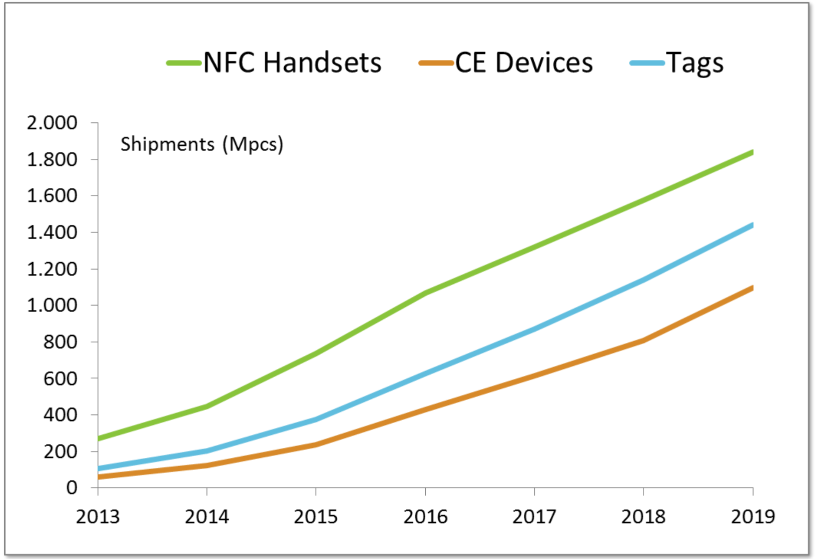
NFC connected devices

Market update - some key figures

- 1.2 billion smartphones shipped in 2014
- Smartphone's share expected to continue growing from 67% in 2014 to > 80% or even higher in coming years
- 850 million NFC handsets shipped between 2012 and 2014
- 3 in 4 mobile phones to come with NFC by 2018
- > 5 billion NFC handsets will be shipped between 2013 and 2018
- NFC-enabled CE devices and tags growing exponentially, **IoT wave coming.**

** Updated list of NFC phones and tablets available in the market: http://www.nfcworld.com/nfc-phones-list/*

11.0B+ NFC-enabled devices shipping 2013-2018



Sources: ABI Research, Sep'14

The Internet of Things Revolution

Ingredients for security challenges

- The Internet of Things (IoT) is the interconnection of **uniquely identifiable** embedded computing devices within the existing Internet infrastructure (wikipedia)
- **Distributed communications**
- **Large number of heterogeneous devices**
- It is about
  - sensing, **collecting** and sharing data;
  - control, actuation, **automation.**

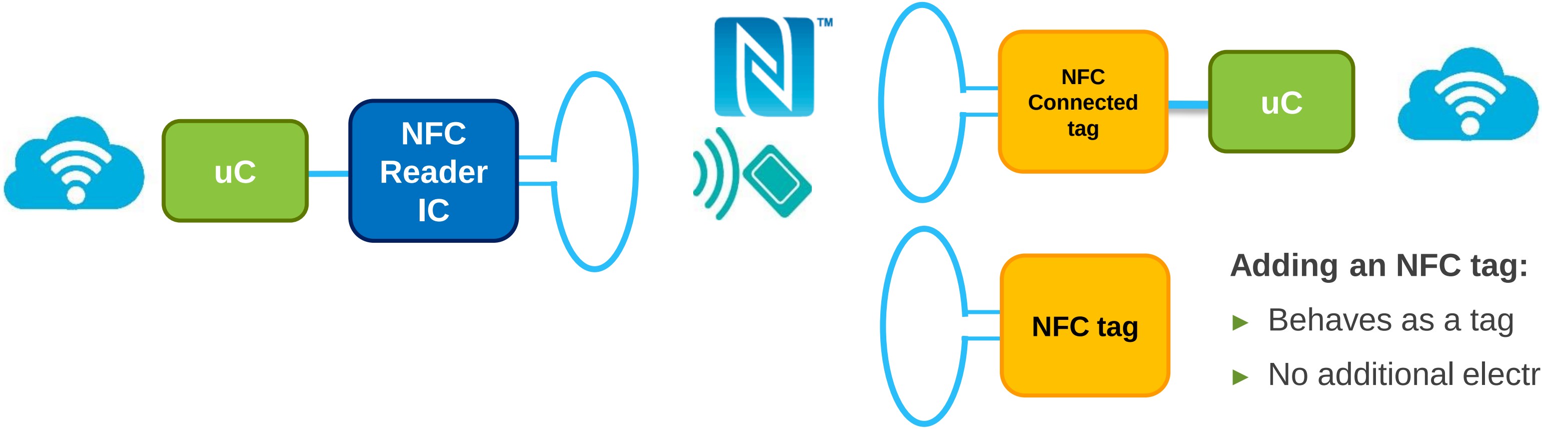
Under the hood of NFC based devices

Adding an NFC reader IC:

- Full/partial NFC capabilities
- Active NFC device

Adding an NFC Connected tag:

- Behaves as a tag
- Connected to an active device

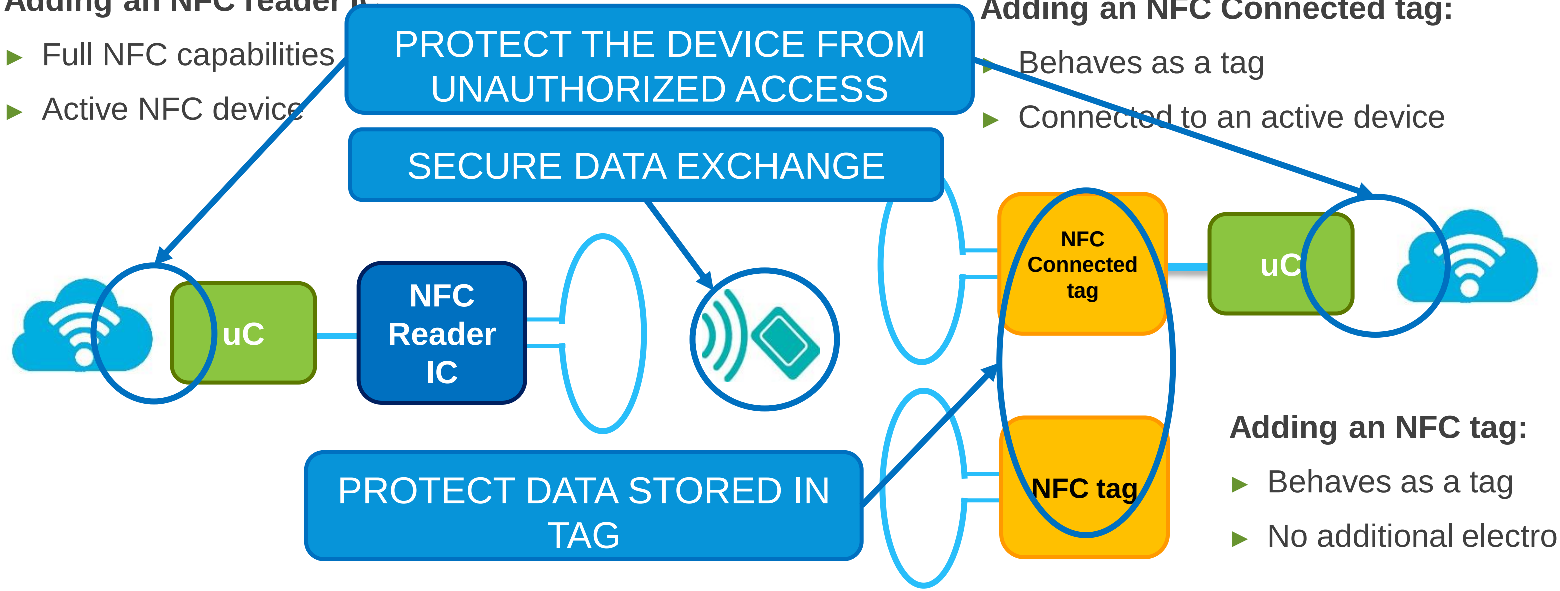


Adding an NFC tag:

- Behaves as a tag
- No additional electronics

NFC INHERENTLY SECURE DUE TO ITS PROXIMITY

Enhancing the security of an NFC-based architecture



Adding an NFC reader IC:

- Full NFC capabilities
- Active NFC device

Adding an NFC Connected tag:

- Behaves as a tag
- Connected to an active device

Adding an NFC tag:

- Behaves as a tag
- No additional electronics

PROTECT THE DEVICE FROM UNAUTHORIZED ACCESS

SECURE DATA EXCHANGE

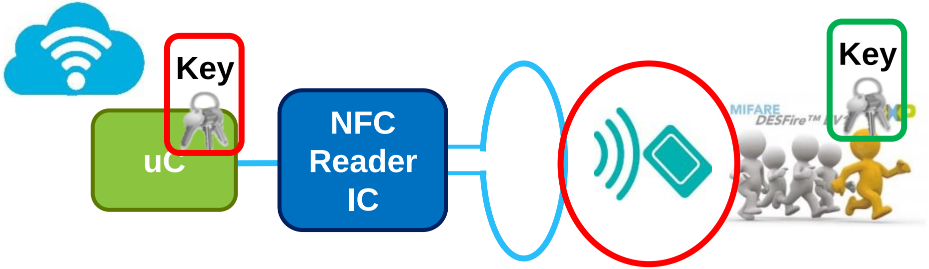
PROTECT DATA STORED IN TAG

DATA SECURITY

UNAUTHORIZED ACCESS PROTECTION

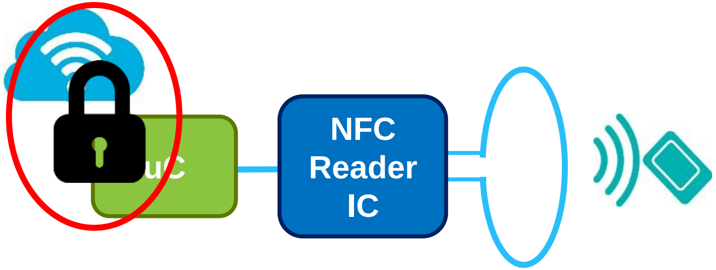
Security need: Secure data exchange

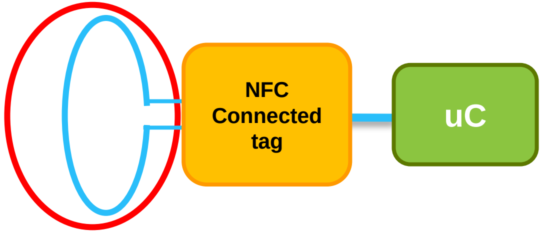
- NFC systems are interoperable and open by default.
- Securing data exchanged through RF channel through cryptographic methods.
- Using cryptography implies the usage of cryptographic keys on both sides of the communication.
- Data is now protected through cryptographic means, NFC system is not open/interoperable anymore.
- **Cryptographic methods can be:**
  - **Dynamic**
  - **Static**
- **Cryptographic algorithms and keys can be:**
  - **Symmetric**
  - **Assymetric**
- **Key management and cryptographic implementation needs to be considered.**



Security need: Protection from unauthorized access

- Any device connected to the “cloud” is subject to be compromised and attacked if not properly protected.
- This has a negative impact on consumers, infrastructure owners and equipment manufacturers alike.
- **Need to implement security mechanisms to:**
  - **Grant access to authorized servers**
  - **Prevent exposure of user related data (privacy)**
  - **Secure communications between device and backend**
  - **Ensure system integrity**
  - **Protection of credentials**
- Above objectives can be ensured through:
  - **Cryptographic methods**
  - **Hardware based security**
- EEPROM of NFC tag can be modified through NFC interface.





Security… a big word!

- Security is a state of mind
  - Lack of objective approach towards security
- Securing the information and process on NFC based devices requires the combination of techniques and protocols
- Cryptography as inter-disciplinary science to achieve information security goals
- Compromise between security and risk
  - What do I need to protect?
  - Trade-off between benefit vs cost for an attacker
- Your system is as secure as your weakest link
- Perfect security does not exist!

A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI . . .
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
... IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

SECURE DATA EXCHANGE

What do we want to protect?

- Remember: NFC by default is open and interoperable, data exchange is inherently secure due to its proximity.

- We want to secure the information exchanged through the NFC interface between A and B.

- **Information security goals**
  - **Confidentiality**
  - **Integrity**
  - **Authenticity**

- **Cryptography as a means to achieve information security goals.**

Threat

Information Security goal

Mechanism

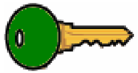
Algorithm

Information Security goals

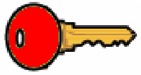
Security goal	Description	Mechanism	Algorithm
Confidentiality	Guarantee that data cannot be read by an unauthorized entity	Encryption/Decryption	**TDES, AES, RSA, ECC**
Integrity	Guarantee that data cannot be changed by an unauthorized entity	CMAC and Digital Signatures	
Authentication	Guarantee mutual identification of two parties entering into a communication	Static (password, PIN,…) Dynamic (challenge-response protocol)	

- Using cryptographic algorithms implies usage of **secret keys.**
- **Cryptographic algorithms:**
  - **Symmetric: Same key on both sides. TDES, AES.**
  - **Asymmetric: Public/private key pair. RSA, ECC.**

Secret key

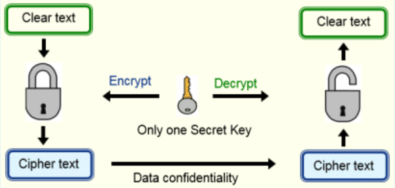
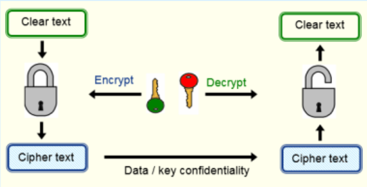
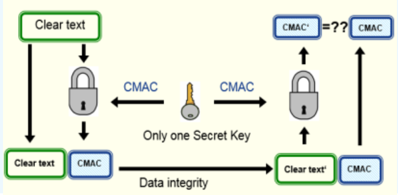
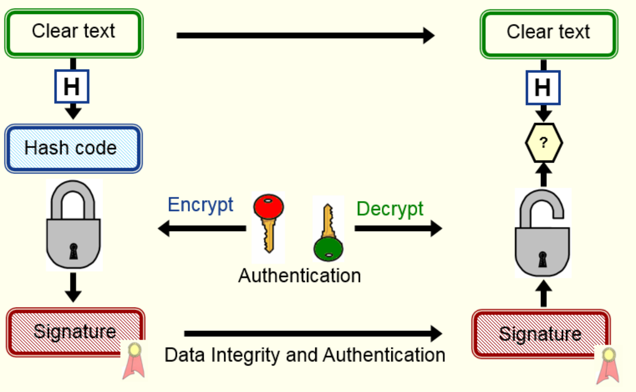
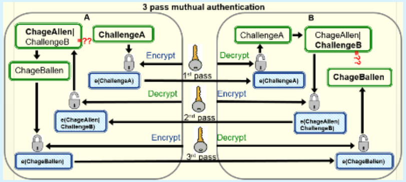


Public key



Private key

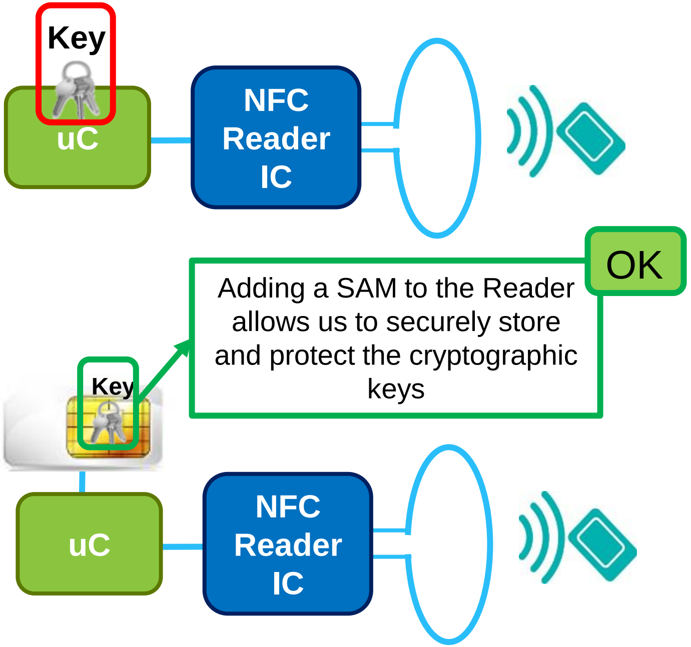
Cryptographic mechanisms summary

	Symmetric	Asymmetric
Confidentiality	 Clear text Encrypt Decrypt Clear text Only one Secret Key Cipher text Data confidentiality Cipher text	 Clear text Clear text Encrypt Decrypt Cipher text Data / key confidentiality Cipher text
Integrity	 Clear text CMAC' =?? CMAC CMAC CMAC Only one Secret Key Clear text CMAC Data integrity Clear text' CMAC	 Clear text Clear text H H Hash code ? Encrypt Decrypt Authentication Signature Data Integrity and Authentication Signature
Authentication	 3 pass muthual authentication A B ChageAllen| ChallengeB =?? ChallengeA ChallengeA ChageAllen| ChallengeB Encrypt Decrypt =?? ChageBallen e(ChallengeA) 1st pass e(ChallengeA) ChageBallen Decrypt Encrypt e(ChageAllen| ChallengeB) 2nd pass e(ChageAllen| ChallengeB) Encrypt Decrypt e(ChageBallen) 3rd pass e(ChageBallen)	

Secret Keys need to be protected and securely distributed

Secret Key management

- How are the secret keys loaded into the NFC Reader?
- Where are the keys located in the NFC Reader?
  - Microcontroller not designed to protect secret keys
- Using NXP’s Secure Access Modules:
  - Highest level of protection for cryptographic keys
  - Secure remote management of key storage tables
  - Additional support for MIFARE products’ cryptography



Adding a SAM to the Reader allows us to securely store and protect the cryptographic keys

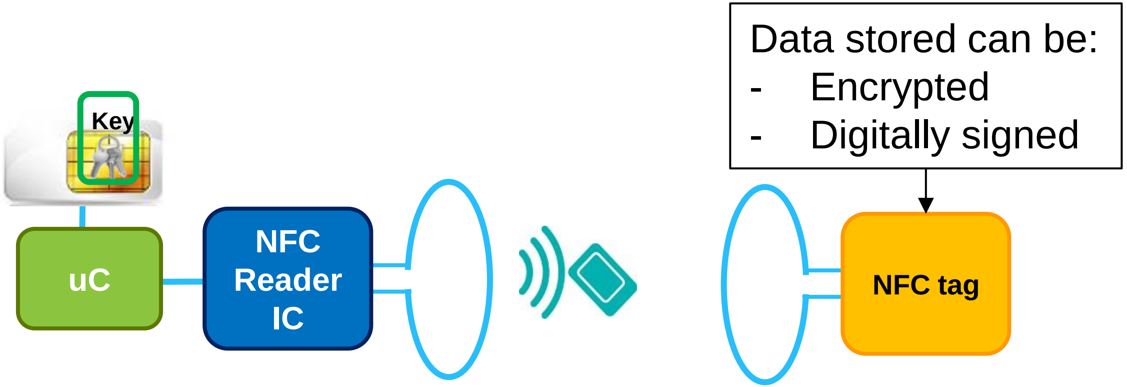
Secure Access Modules (SAMs)

MIFARE SAM AV2

- ▶Supports MIFARE DESFIRE EV1, MIFARE Plus, MIFARE Classic and MIFARE Ultralight C
- ▶Can be used for generic cryptography (symmetric and asymmetric)
- ▶Supports TDES, AES, RSA and Crypto1 cryptographic algorithms
- ▶128 key entries
- ▶ISO/IEC 7816 contact interface, with a communication speed up to 1.5 Mbps
- ▶Can work in X-mode
- ▶Hardware Common Criteria EAL 5+ certified

Data protection for NFC tags

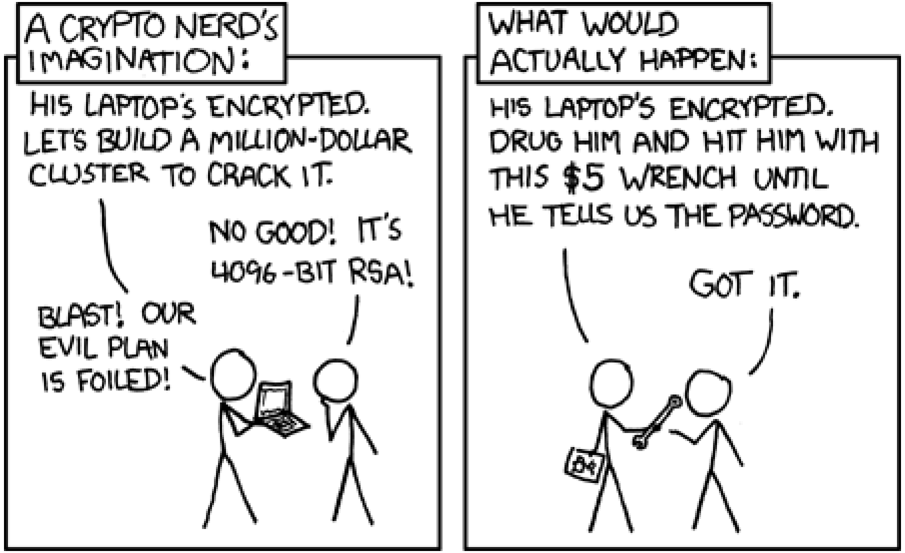
- To ensure confidentiality of the written data in the tag:
  - Data stored are encrypted.
  - Secret key to decrypt it stored in SAM in the NFC device.
- To ensure data integrity and authenticity of the written data in the tag:
  - Digital signature added to data stored.
  - Secret key to verify digital signature stored in SAM in the NFC device.



Data stored can be:
- Encrypted
- Digitally signed

Secure data exchange summary

- Objective: secure data being exchanged through RF interface or available in EEPROM of NFC tag.
- Use cryptographic mechanisms to achieve information security goals:
  - Confidentiality
  - Integrity
  - Authenticity
- Cryptography implies the usage of keys: how are keys securely distributed and stored?
- **NXP Secure Access Modules (SAM) to ensure highest level of protection in your NFC device.**

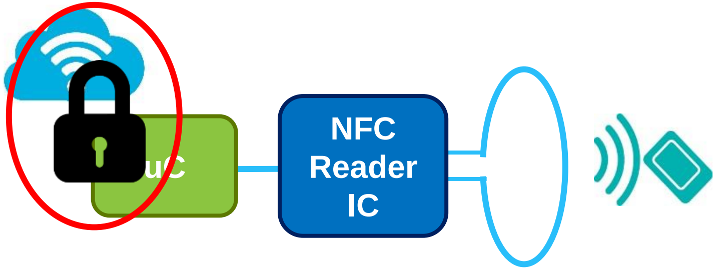

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

PROTECTION FROM UNAUTHORIZED ACCESS

NFC device access considerations

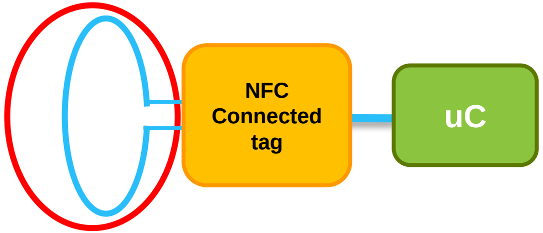
Remote Access protection:

- A device that is connected to the cloud is subject to be compromised and attacked if not properly protected



NFC Interface Access protection:

- An NFC Connected tag is inherently secure due to proximity, however to avoid unauthorized modifications of data through NFC interface it needs to be properly configured.

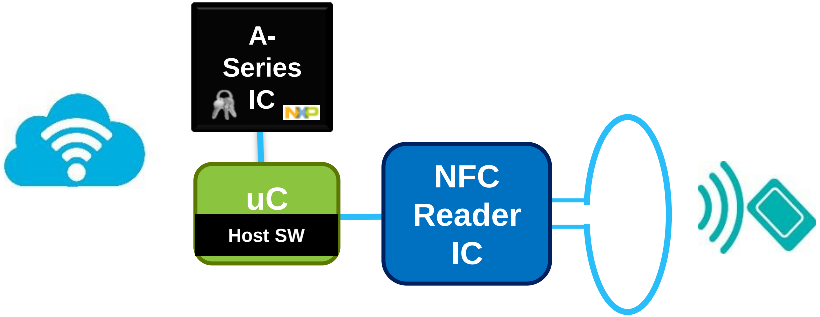


Remote access protection

- Need to implement security mechanisms to:
  - Grant access to authorized servers
  - Prevent exposure of user related data (privacy)
  - Secure communications between device and backend
  - Ensure system integrity
  - Protection of credentials
- Above objectives can be ensured through:
  - Cryptographic methods
  - Hardware based security
- **A-Series ICs from NXP** are **HW Security Module** for IoT Devices
  - Supporting wide variety of use cases and targeting multiple applications
  - Off-the-shelf solutions offering key injection service, on chip application SW and host library with a high level API.

A-Series Security ICs

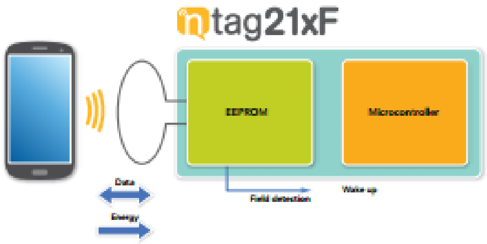
ADAPT TO ANY TYPE OF µC

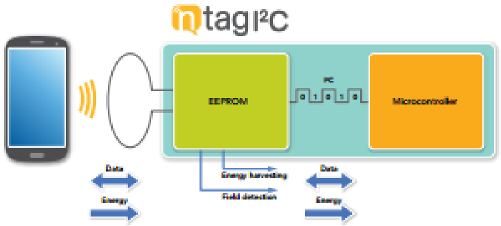


NFC Access protection

- Ensure that data written in EEPROM from NFC tag cannot be modified.

- NFC tags from NXP offer several features to protect EEPROM:
  - **All NTAG Lock bits for read-only EEPROM**
  - **NTAG21xF Password protection mechanism**
  - **NTAG I2C no WRITE Access from the NFC side through configuration registers**





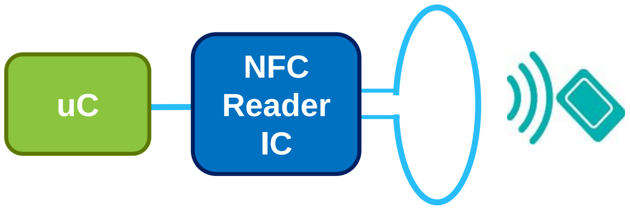
USE CASES

Access control systems

- What do we want to achieve in Access Control systems?
  - **Secure** system with optimized cost
  - Intuitive and fast access
  - Simple and flexible management
- NFC Technology fully covers the above requirements.
- Credentials designed to securely store and protect cryptographic keys.
- NFC Readers shall be designed to offer the same level of protection.

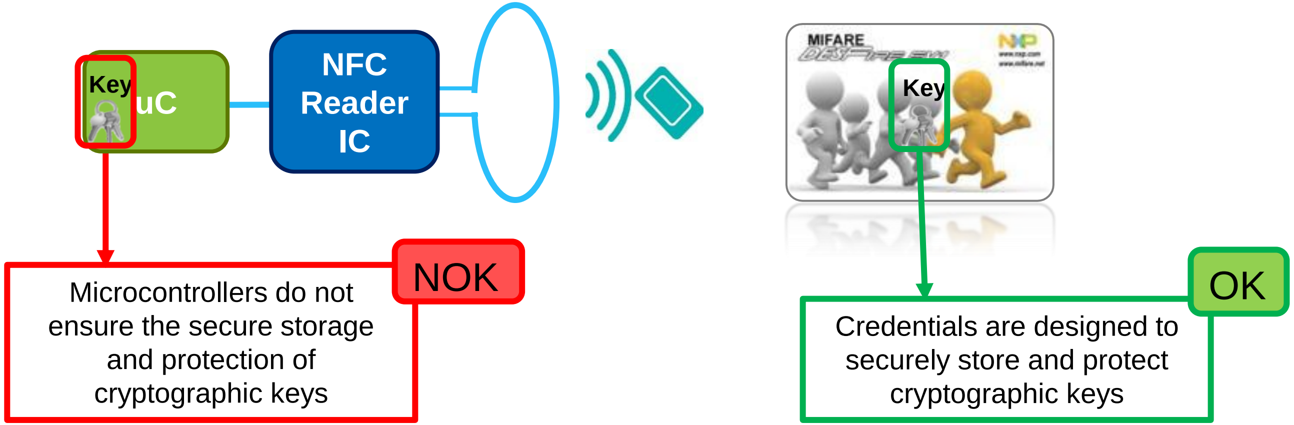
NFC Readers

Credentials



Security design in NFC access control systems

Cryptographic keys



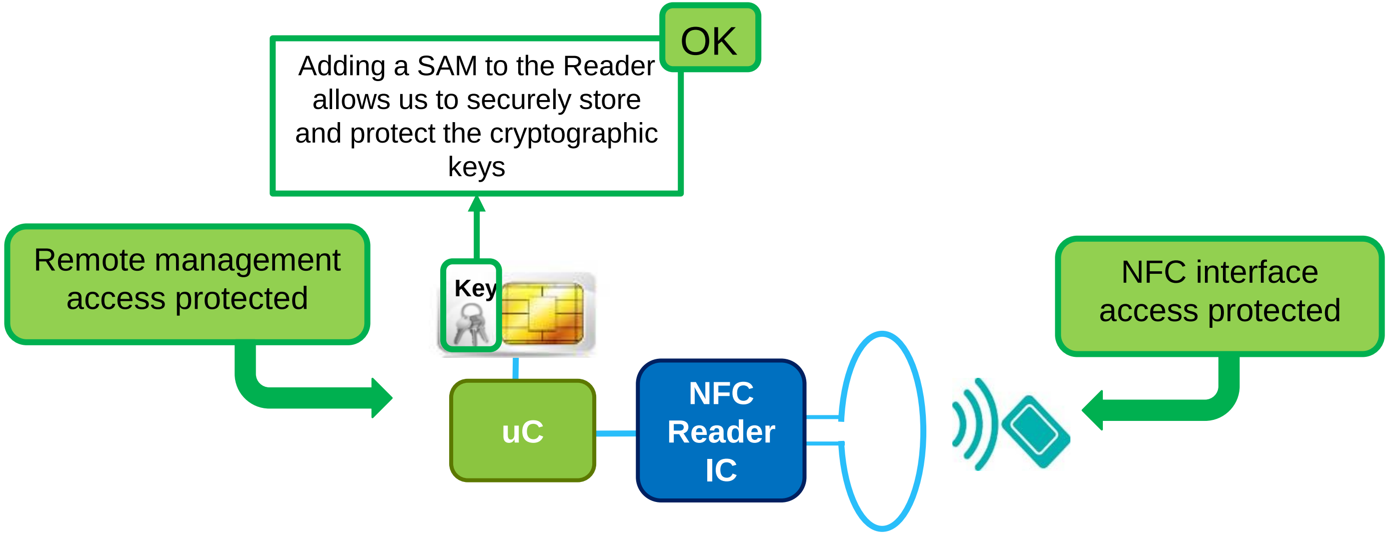
Microcontrollers do not ensure the secure storage and protection of cryptographic keys

Credentials are designed to securely store and protect cryptographic keys

Security design in NFC access control systems

SAM ensures protection in overall system

- Secure Access Module (SAM) in the NFC Reader:
  - Ensure data exchange protection over NFC interface
  - Protect remote access to the NFC reader



Adding a SAM to the Reader allows us to securely store and protect the cryptographic keys

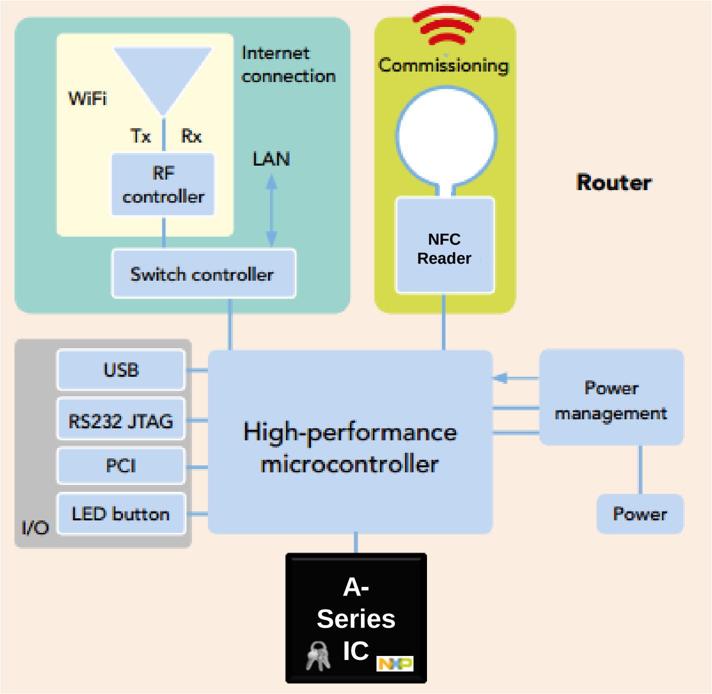
OK

Remote management access protected

NFC interface access protected

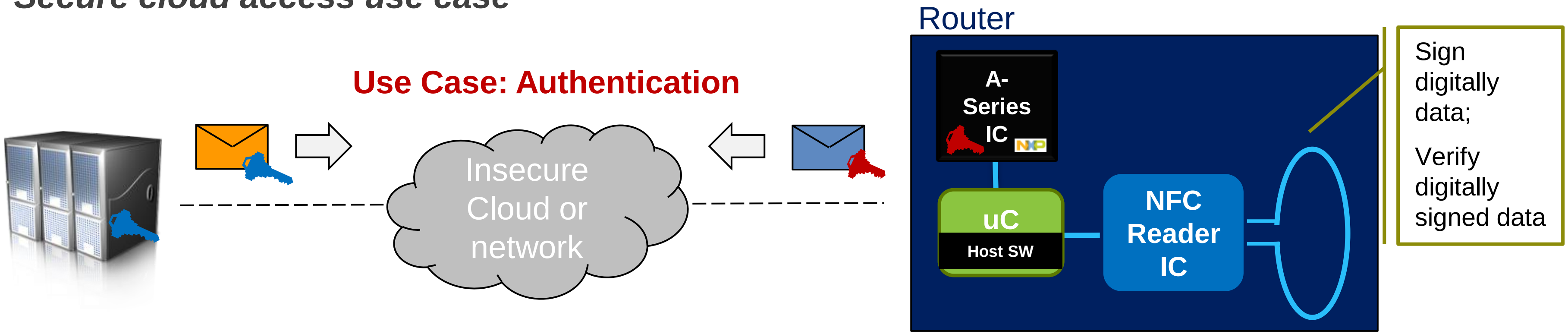
Internet gateway

- As homes become “smarter”, the number of IoT devices continues to expand. The router is truly the heart of the “Smart Home”.
- Router acts as a home Gateway, providing internet access to all devices.
- A-Series to ensure security towards the internet.
- NFC Reader for confidential commissioning.



Internet Gateway

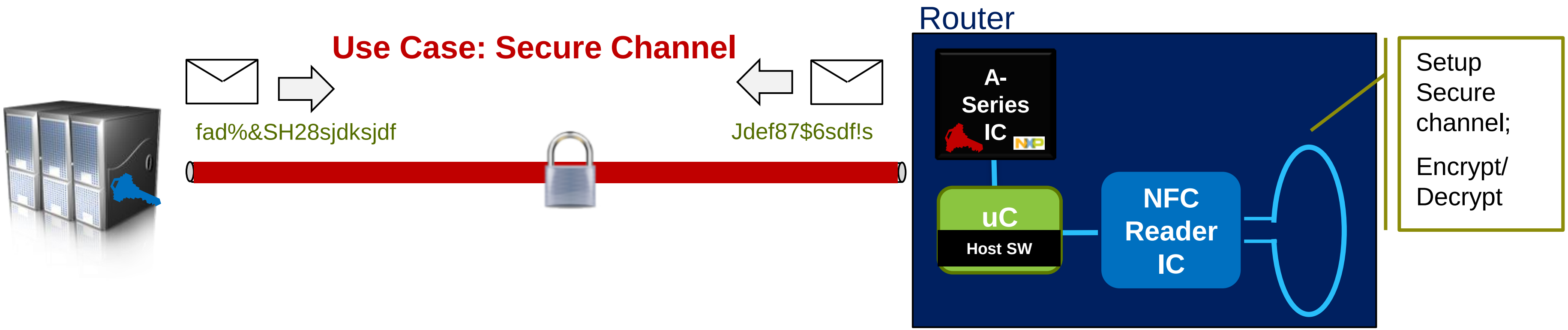
Secure cloud access use case



Use Case: Authentication

Sign digitally data;

Verify digitally signed data



Use Case: Secure Channel

Setup Secure channel;

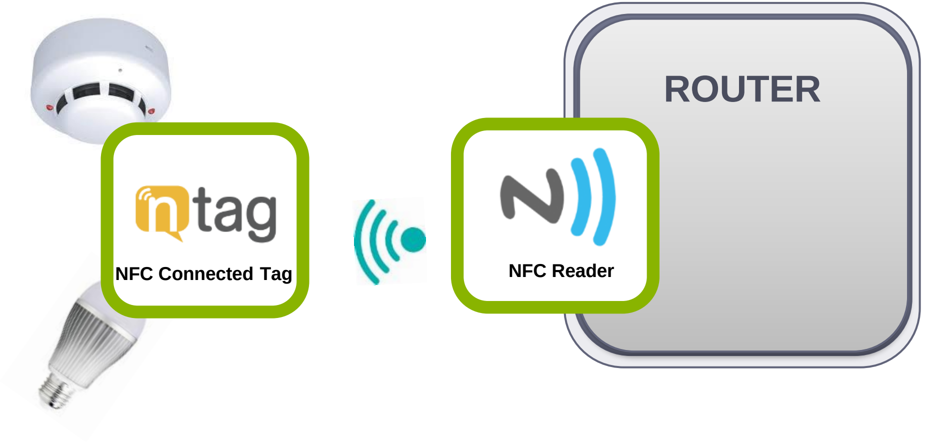
Encrypt/ Decrypt

Internet Gateway

Confidential commissioning use case

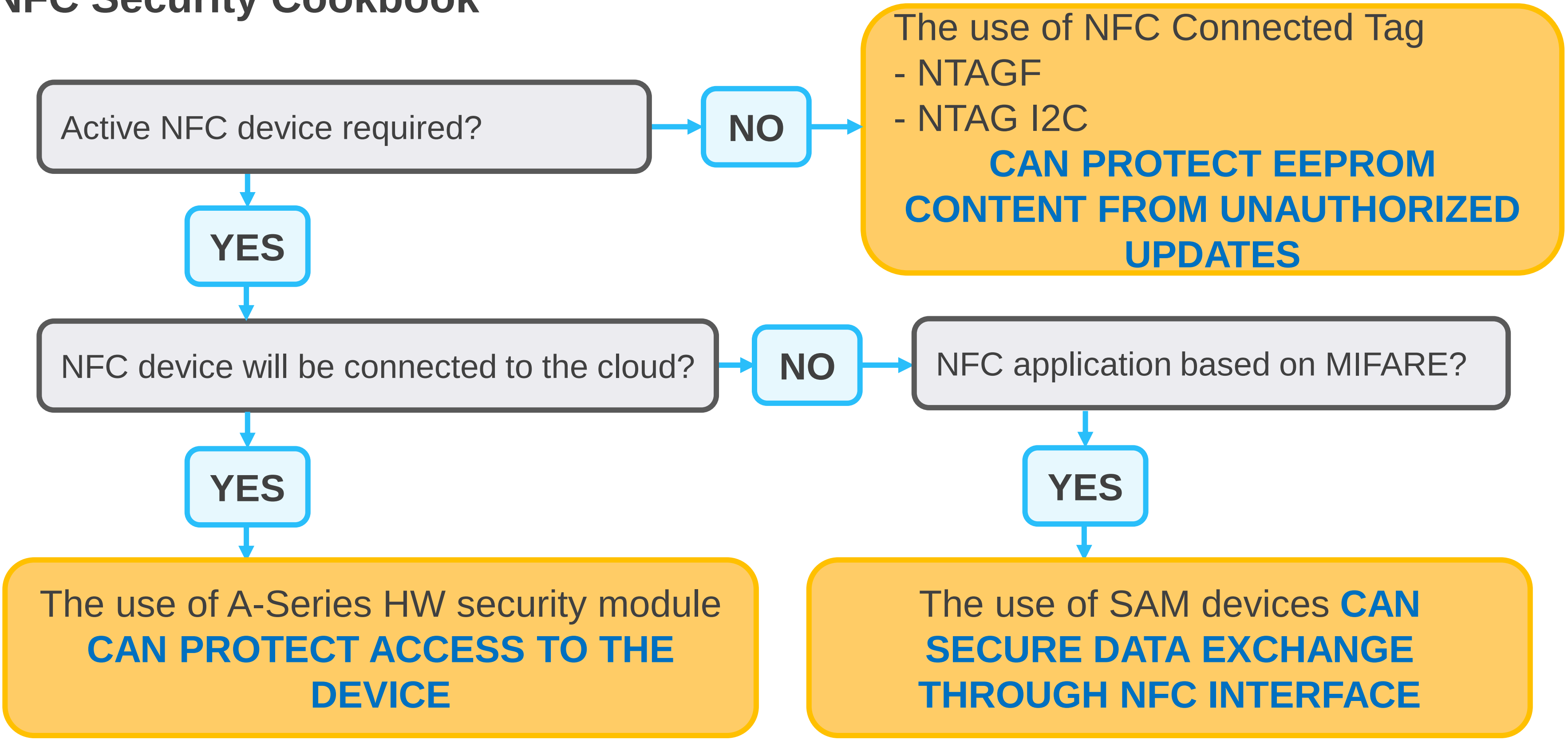
- IoT devices obtain access to home network through an NFC tap.

- Confidential mode:
  1. Router writes Network key in NTAG,
  2. IoT Device reads key through I2C bus,
  3. IoT Device deletes key in NTAG I2C.



CONCLUSION

NFC Security Cookbook



Active NFC device required?

NO

The use of NFC Connected Tag
- NTAGF
- NTAG I2C

CAN PROTECT EEPROM CONTENT FROM UNAUTHORIZED UPDATES

YES

NFC device will be connected to the cloud?

NO

NFC application based on MIFARE?

YES

The use of A-Series HW security module **CAN PROTECT ACCESS TO THE DEVICE**

YES

The use of SAM devices **CAN SECURE DATA EXCHANGE THROUGH NFC INTERFACE**

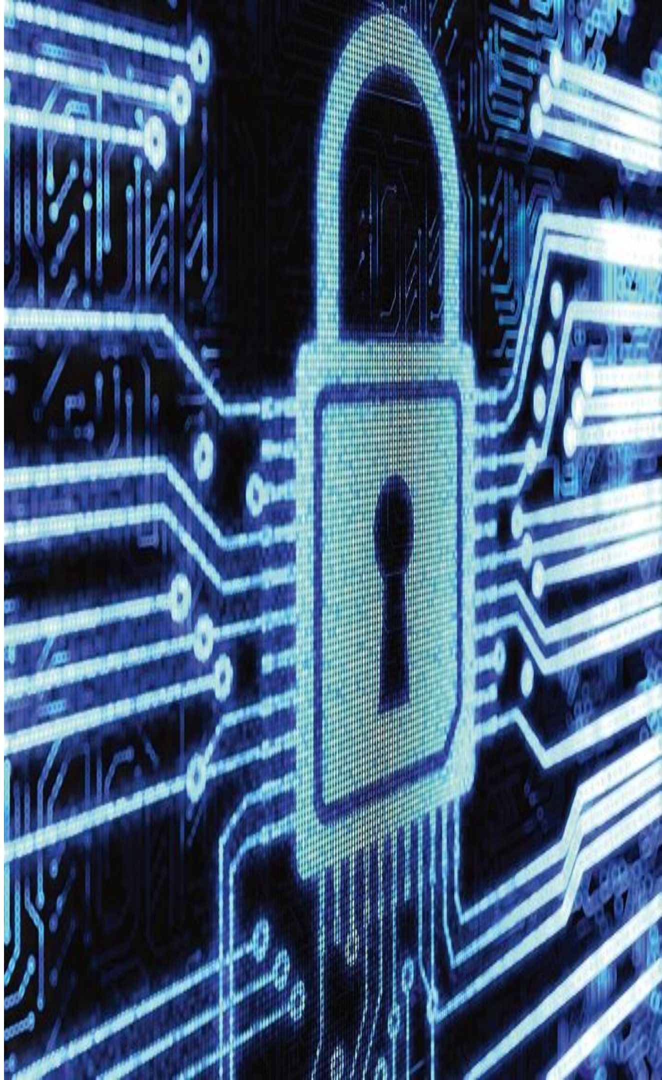
Summary and Conclusion

- NFC enabled devices are growing exponentially.

- Security enhancements for NFC enabled devices:
  - Secure data exchange
  - Unauthorized access protection

- Secure data exchange
  - Information security goals: confidentiality, integrity and authentication
  - Cryptographic mechanisms: encryption, MAC/Digital Signature, 3 pass mutual authentication
  - Symmetric and assymetric cryptography
  - SAM for secure key storage

- Unauthorized access protection
  - Remote access protection through A-Series HW security module
  - NFC access protection features in Connected tags



Need More? NXP - NFC Reader Solutions

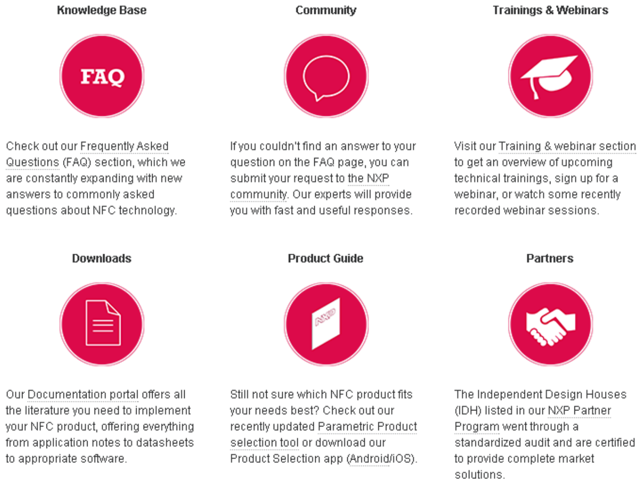
Reference material & documentation:

- **NFC Everywhere**
  http://www.nxp.com/nfc

- **NFC Everywhere support page:**
  http://www.nxp.com/techzones/nfc-zone/community.html

- **Reader forum:**
  http://www.mifare.net/en/micommunity/forum/mifare-and-nfc-reader-ics

For other questions or further support, please contact: nfc.readers@nxp.com



Knowledge Base

Check out our Frequently Asked Questions (FAQ) section, which we are constantly expanding with new answers to commonly asked questions about NFC technology.

Community

If you couldn't find an answer to your question on the FAQ page, you can submit your request to the NXP community. Our experts will provide you with fast and useful responses.

Trainings & Webinars

Visit our Training & webinar section to get an overview of upcoming technical trainings, sign up for a webinar, or watch some recently recorded webinar sessions.

Downloads

Our Documentation portal offers all the literature you need to implement your NFC product, offering everything from application notes to datasheets to appropriate software.

Product Guide

Still not sure which NFC product fits your needs best? Check out our recently updated Parametric Product selection tool or download our Product Selection app (Android/iOS).

Partners

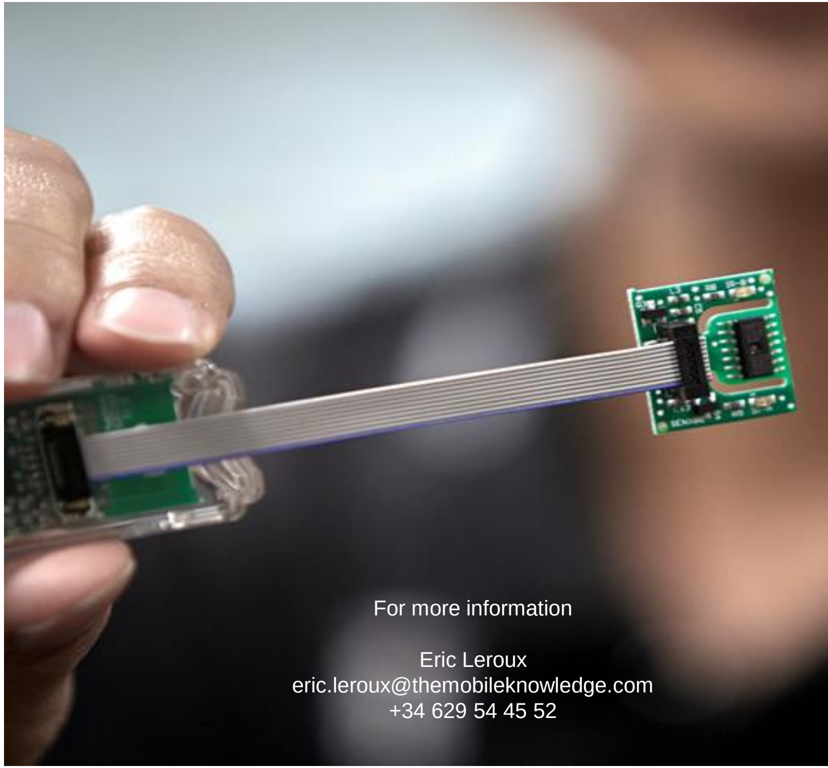
The Independent Design Houses (IDH) listed in our NXP Partner Program went through a standardized audit and are certified to provide complete market solutions.

MobileKnowledge

Thank you for your attention

www.themobileknowledge.com

- We are a global competence team of hardware and software technical experts in all areas related to contactless technologies and applications.
- Our services include:
  - Application and system Design Engineering support
  - Project Management
  - Technological Consulting
  - Advanced Technical Training services
- We address all the exploding identification technologies that include NFC, secure micro-controllers for smart cards and mobile applications, reader ICs, smart tags and labels, MIFARE family and authentication devices.



For more information

Eric Leroux
eric.leroux@themobileknowledge.com
+34 629 54 45 52