NFC Application: Access

Public

BU Security and Connectivity
April 2015

Index

- Introduction to NFC access control
  - Where we come from
  - NFC in access control
  - Access control applications
- Components in an NFC access control system
  - Credential
  - Transceiver
  - Controller
  - Central server
- NFC access control system architectures
  - Off-line architectures
  - On-line architectures
- NXP products
- NXP support material

Introduction

What do we want in an access control application?

- Access denied to unallowed users
- Access guaranteed to allowed users
- Intuitive and fast access
- Simple and flexible management
- Credential can be used in other applications
- Easy installation and optimized cost

Introduction

Where we come from

Keys

- Easily clonable
- Lock can be forced
- Not convenient

Pin pads

- PIN can be copied and replayed
- Not convenient

Magnetic stripe cards

- Easily clonable
- Fragile (scratches, magnetic fields...)
- Maintenance costs

LF cards

- Easily clonable
- Communication can be sniffed and replayed
- Relay attack

Introduction

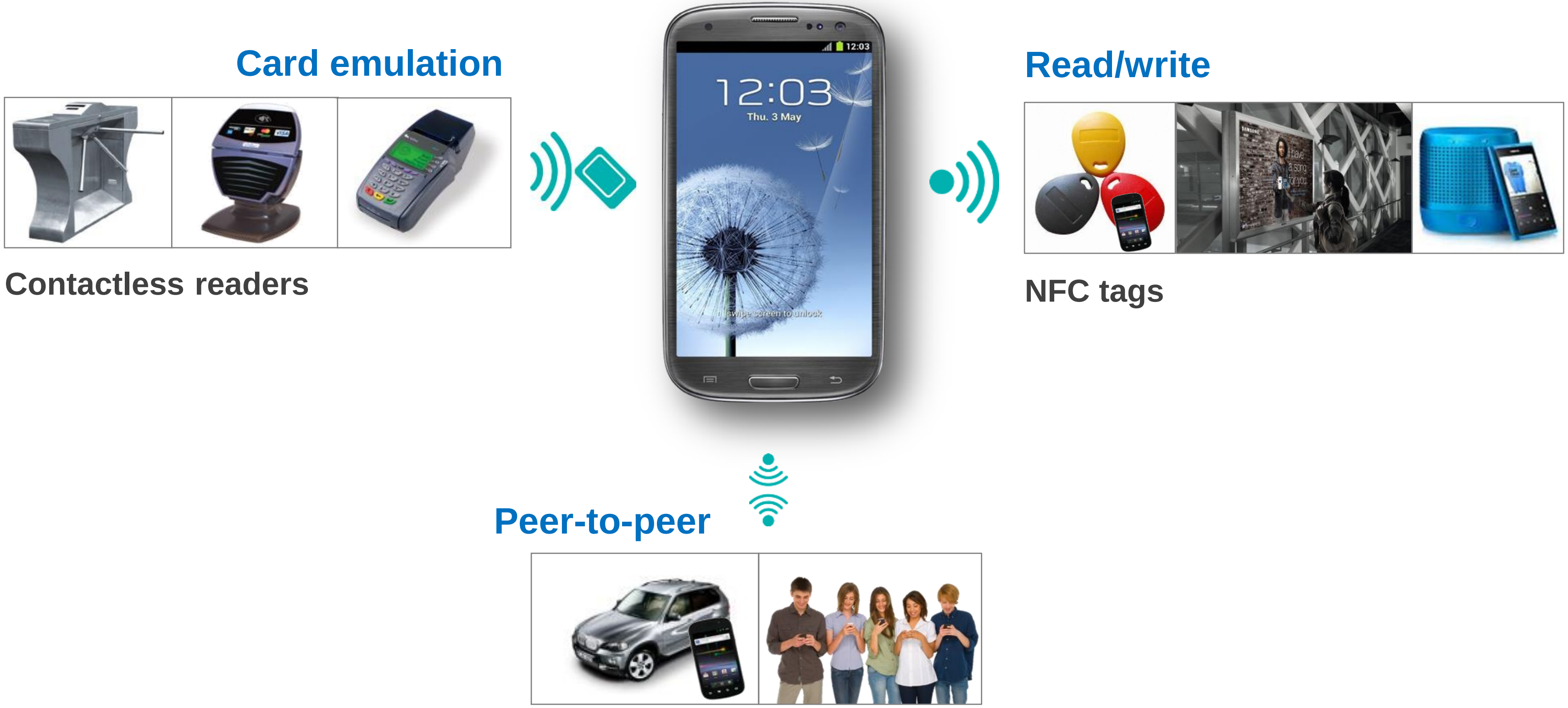
LF vs NFC

	LF (proximity card) 	NFC smart card 	NFC device
Frequency	125 kHz	13.56 MHz	
Bit rate	2 – 8 kbps	106 – 848 kbps	
Security	Low	Very high	
Memory	8 – 256 Bytes	64 – 64k Bytes	
Cost	Low	Low	-
Flexibility	Low	High	High
Multi-application	No	Yes	Yes
Connection to cloud	No	Yes*	Yes
User interface	No	Yes*	Yes
Compatibility	-	With NFC devices	With NFC smart cards

*through an NFC device

Introduction

What is NFC



Card emulation

Contactless readers

Read/write

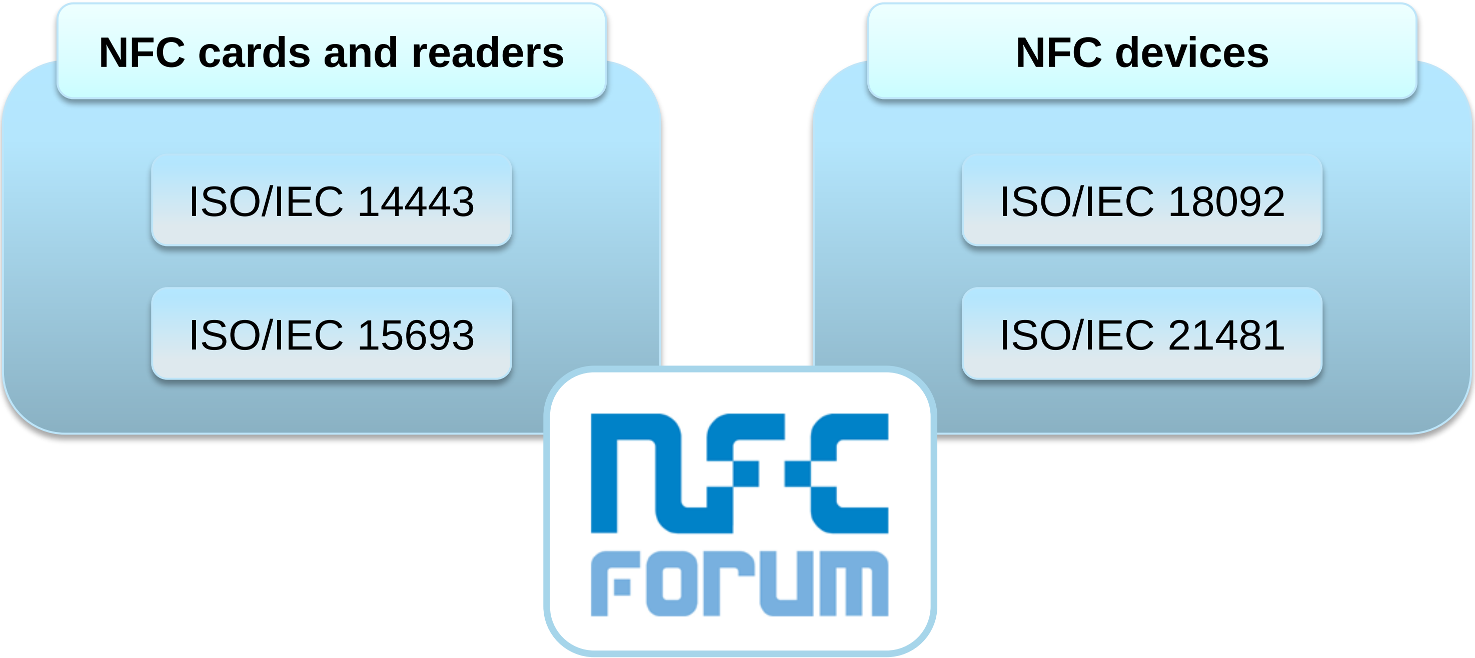
NFC tags

Peer-to-peer

Other NFC devices

Introduction

NFC Standards



NFC cards and readers

ISO/IEC 14443

ISO/IEC 15693

NFC devices

ISO/IEC 18092

ISO/IEC 21481

Introduction

NFC in access control

More secure

- Protection mechanisms to **avoid cloning**
- Use of **cryptography**
  - Authentication, encrypted communication…

More convenient

- **Fast**
- **No need** to put the card in a **specific position**
- Allows **multi-application** solutions
- Allows **multi-site** solutions

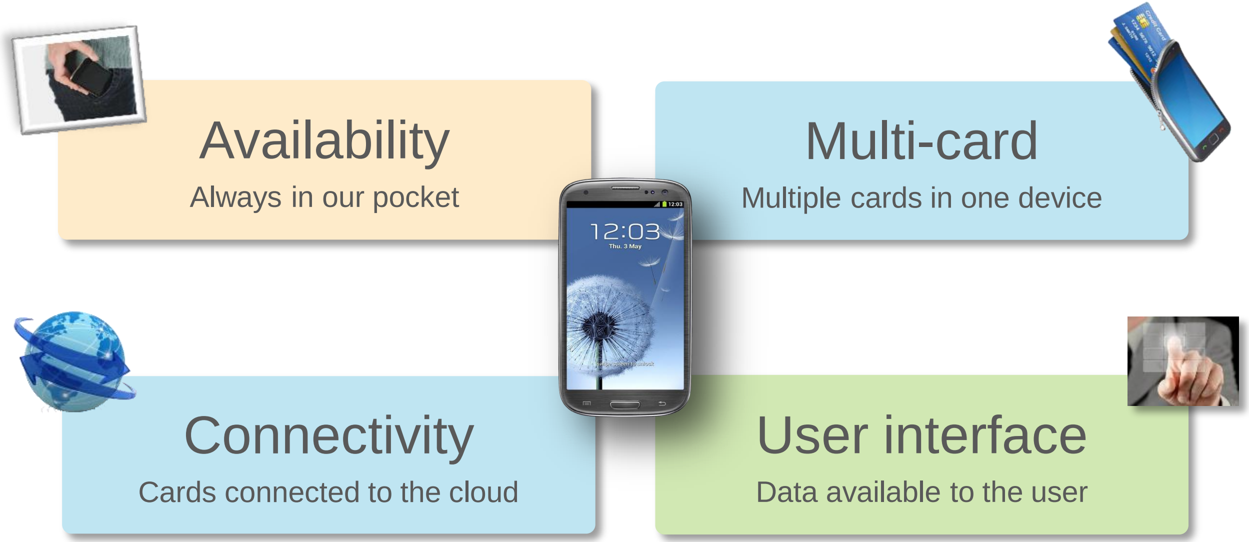
Low maintenance costs

- **No contact** needed between the reader and the card
- **Durable** card

Introduction

NFC in access control

- Using the smartphone instead of a card makes it even more convenient



Availability

Always in our pocket

Multi-card

Multiple cards in one device

Connectivity

Cards connected to the cloud

User interface

Data available to the user

Introduction

Access control applications

- Used in enterprise and government offices, hotel rooms and campus buildings worldwide

Corporate
Access to corporate facilities and services including
- Access mgmt.
- Logical Access
- Resource mgmt.
- Payment
- Parking
- IT Services

Hospitality
Access to facilities and services including
- Room Access
- Leisure facilities
- Parking
- Vending

Campus
Access to campus facilities and services including
- Access mgmt.
- Logical Access
- Attendance ctrl.
- Payment
- IT Services
- Library services

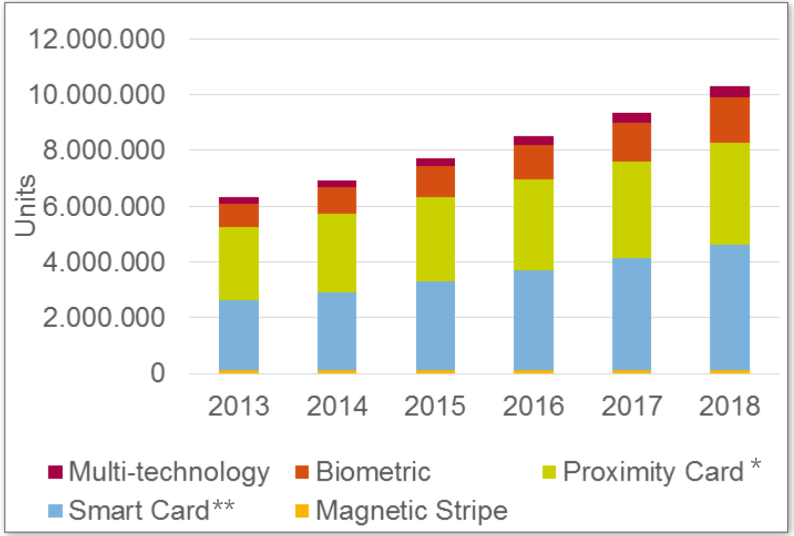
Leisure
Access to leisure activities such as
- Theme park
- Fitness studio
- Stadium
- Event ticketing
- Waterpark and Spa
- Ski resorts

Residential
Access to residential buildings
- House
- Apartment building
- Residential complex

Introduction

Access control applications

Reader end market, by technology



* "Proximity Card" stands for LF card.
** "Smart Card" stands for NFC card.

Source: IHS 2014, CMI

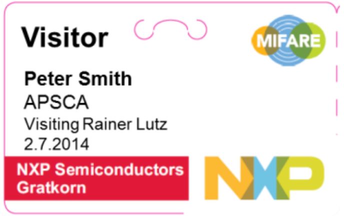
- NFC readers are growing fast, and they are expected to keep on growing
- Something similar happens to biometric readers
- Multi-technology readers are growing fast, but this growth will decrease in a few years
- LF readers are growing at a slower pace
- Magnetic stripe readers are in decline

Introduction

NFC access control in Corporate

- Access to corporate facilities and services
- Same card can be used for multiple applications:
  - Access management
  - Logical access
  - Resource management
  - Payment
  - Parking
  - IT Services
- Require confidentiality, efficiency, reliability and system availability
- Highly fragmented market
  - Many different technologies (magnetic stripe, LF, NFC...)
  - Many unknown or small players

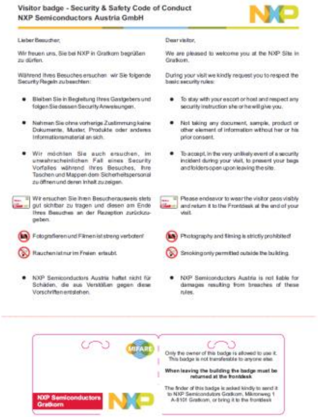
- Example: NXP Hamburg, NXP Gratkorn
  - Personalized disposable visitor badges
  - Based on MIFARE DESFire EV1
  - Personalization and printing in one step
    - Badge can be printed in a regular printer
  - Eco-friendly, paper based
  - Ideal solution for visitors, contractors or temporary staff



Visitor

Peter Smith
APSCA
Visiting Rainer Lutz
2.7.2014

NXP Semiconductors
Gratkorn



Visitor badge - Security & Safety Code of Conduct
NXP Semiconductors Austria GmbH

Lieber Besucher,

Wir freuen uns, Sie bei NXP in Gratkorn begrüßen zu dürfen.

Während Ihres Besuches ersuchen wir Sie folgende Security Regeln zu beachten:

- Bleiben Sie in Begleitung Ihres Gastgebers und folgen Sie dessen Security Anweisungen.
- Nehmen Sie ohne vorherige Zustimmung keine Dokumente, Muster, Produkte oder anderes Informationsmaterial an sich.
- Wir möchten Sie auch ersuchen, im unwahrscheinlichen Fall eines Security Vorfalles während Ihres Besuches, Ihre Taschen und Mappen dem Sicherheitspersonal zu öffnen und deren Inhalt zu zeigen.

Wir ersuchen Sie Ihren Besucherausweis stets gut sichtbar zu tragen und diesen am Ende Ihres Besuches an der Rezeption zurückzugeben.

Fotografieren und Filmen ist streng verboten!

Rauchen ist nur im Freien erlaubt.

- NXP Semiconductors Austria haftet nicht für Schäden, die aus Verstößen gegen diese Vorschriften entstehen.

Dear visitor,

We are pleased to welcome you at the NXP Site in Gratkorn.

During your visit we kindly request you to respect the basic security rules:

- To stay with your escort or host and respect any security instruction she or he will give you.
- Not taking any document, sample, product or other element of information without her or his prior consent.
- To accept, in the very unlikely event of a security incident during your visit, to present your bags and folders open upon leaving the site.

Please endeavor to wear the visitor pass visibly and return it to the Frontdesk at the end of your visit.

Photography and filming is strictly prohibited!

Smoking only permitted outside the building.

- NXP Semiconductors Austria is not liable for damages resulting from breaches of these rules.

NXP Semiconductors
Gratkorn

Only the owner of this badge is allowed to use it. This badge is not transferable to anyone else.

When leaving the building the badge must be returned at the frontdesk

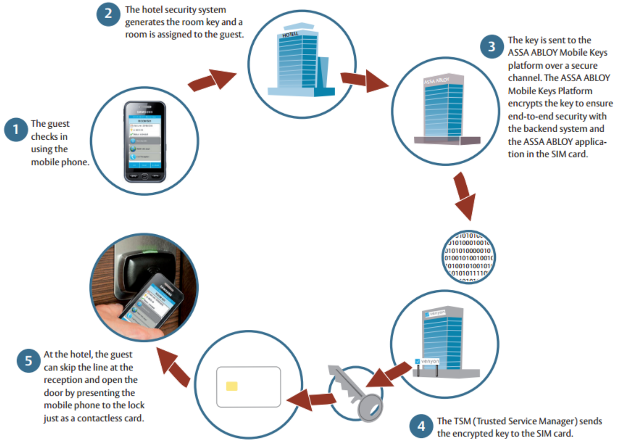
The finder of this badge is asked kindly to send it to NXP Semiconductors Gratkorn, Mikronweg 1 A-8101 Gratkorn, or bring it to the frontdesk

Introduction

NFC access control in Hospitality

- Access to facilities and services
- Same card can be used for multiple applications:
  - Room Access
  - Leisure facilities
  - Parking
  - Vending
- Require convenience and availability
- Big players with high influence on small and medium players
  - Market (excl. China) led by Assa Abloy (Vingcard), Kaba, Salto, Cisa (Allegion) and UTC. Top 5 players own 79% of the market

- Example: Clarion Hotel Stockholm
  - The first complete solution for hotels using mobile keys in the World
  - The credential is the user´s smartphone
  - Check-in and check-out is done on-line
  - Keys are delivered on-line
    - No need to wait in line



1 The guest checks in using the mobile phone.

2 The hotel security system generates the room key and a room is assigned to the guest.

3 The key is sent to the ASSA ABLOY Mobile Keys platform over a secure channel. The ASSA ABLOY Mobile Keys Platform encrypts the key to ensure end-to-end security with the backend system and the ASSA ABLOY application in the SIM card.

4 The TSM (Trusted Service Manager) sends the encrypted key to the SIM card.

5 At the hotel, the guest can skip the line at the reception and open the door by presenting the mobile phone to the lock just as a contactless card.

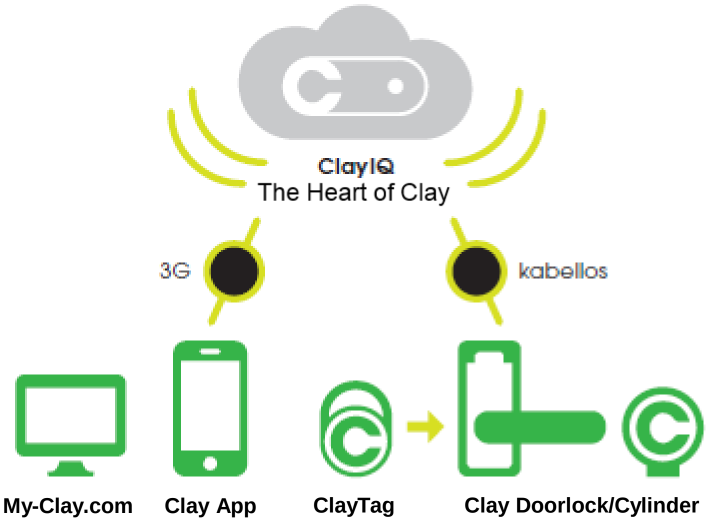
Source: Assa Abloy

Introduction

NFC access control in other applications

- There are many other applications where NFC technology can be used for access control
  - Campus
  - Leisure
  - Residential
  - …
- Large systems, such as Campuses, may use a dedicated solution
  - e.g., University of Oxford uses a system based on MIFARE DESFire EV1
- Others may prefer using a more general-purpose solution
  - e.g. Clay by Salto

- Example: Clay by Salto
  - Designed for small businesses and homes
  - Based on MIFARE DESFire EV1
  - Door lock uses the NXP PN512 reader IC
  - Can be managed by the user though an intuitive app

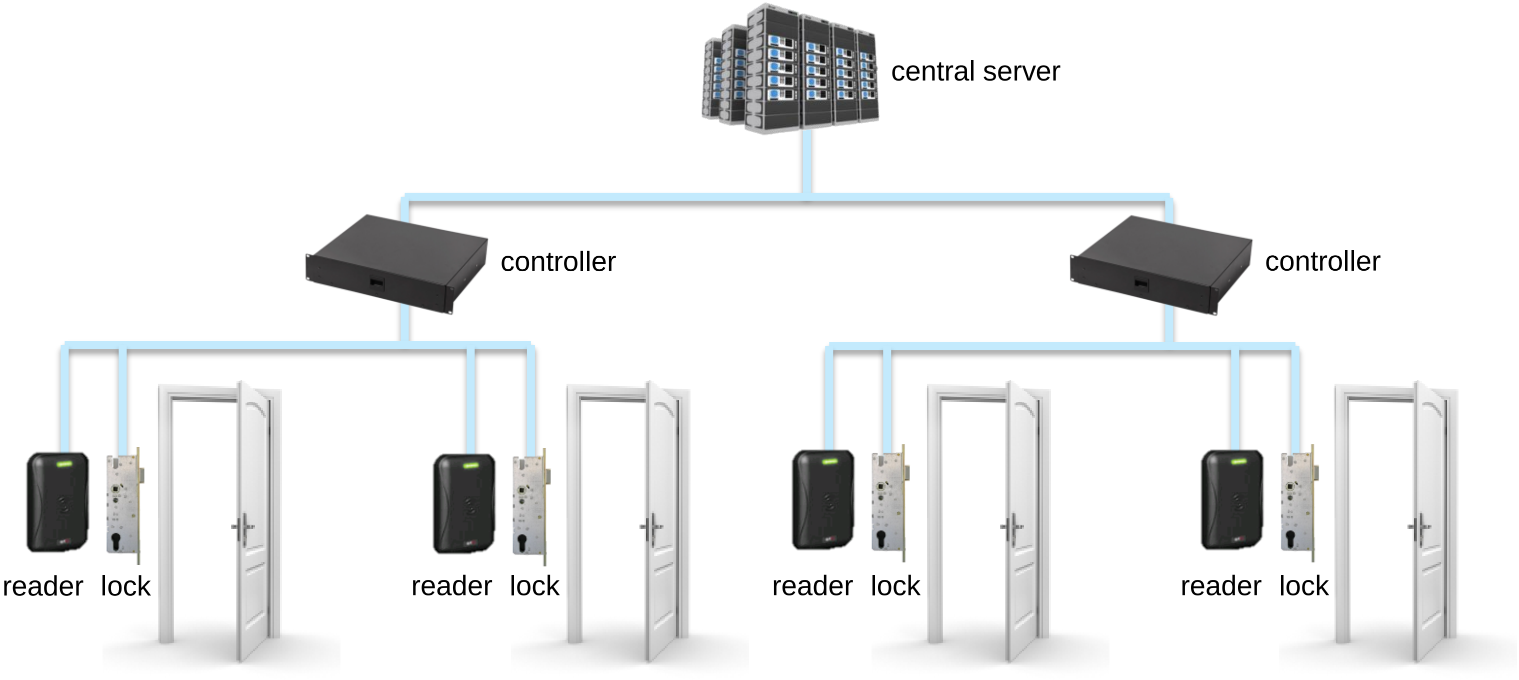


Source: Salto

Components in an NFC access control system

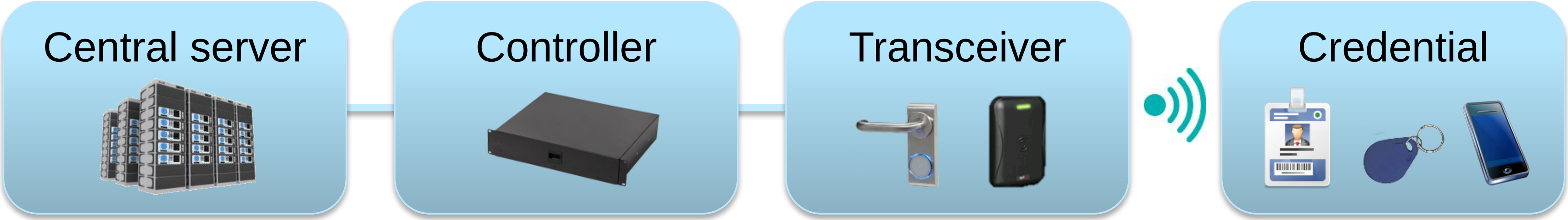
Components in an NFC access control system

A typical NFC access control system



Components in an NFC access control system

Main components



Central server

Controller

Transceiver

Credential

Central server

- Centralized place that collects data from every on-line controller
- It may be consulted by on-line controllers for access decisions
- Optional element

Controller

- Collects user’s electronic credentials and makes the access decisions (potentially in cooperation with the central server)
- Hosts the security functionality
- May contain a **SAM** to store the keys in a safe way
- May control several transceivers or readers

Transceiver

- The RF frontend that allows the controller to communicate with the credential
- It has no security functionality
- Possibly in the same device as the controller. The whole device is known as **reader**
- If separated from the controller, it is also known as “active antenna”

Credential

- It stores the user electronic credentials
- Different form factors: card, keyfob, NFC phone...

Components in an NFC access control system

Credential

- Stores the user electronic credentials
  - It securely contains the user-specific data such as employee ID
  - It may contain the user entitlements (e.g. what rooms the user has access to)
- Different form factors: card, keyfob, NFC phone...
  - Cards
    - Different types (MIFARE Classic, MIFARE DESFire, MIFARE Plus...)
    - Recommended cards:
      - MIFARE DESFire EV1: ideal for multi-application
      - MIFARE Plus: recommended for migration from MIFARE Classic
      - SmartMX with MIFARE implementation: to implement also logical access solutions
  - Keyfobs and other objects
    - Same technology as cards
  - NFC devices (smartphones...)
    - Emulate a card
- Can be multi-technology
  - E.g., LF+NFC card

Components in an NFC access control system

Credential: NFC device

- Card Emulation mode
  - The NFC device behaves the same way a card does
    - It always answers to reader commands
  - Regular card readers can be used
  - Requires a SE or the use of HCE
    - SE: requires a TSM
    - HCE: requires connection to the cloud in order to be secure
  - In case the device emulates a MIFARE card
    - MIFARE4Mobile 2.1 simplifies the management of the card

- Peer-to-Peer mode
  - The NFC device behaves according to the ISO/IEC 18092 standard
    - Protocols defined by the NFC Forum
  - Requires that the readers are NFC-ready
  - Can be used for maintenance/update of readers

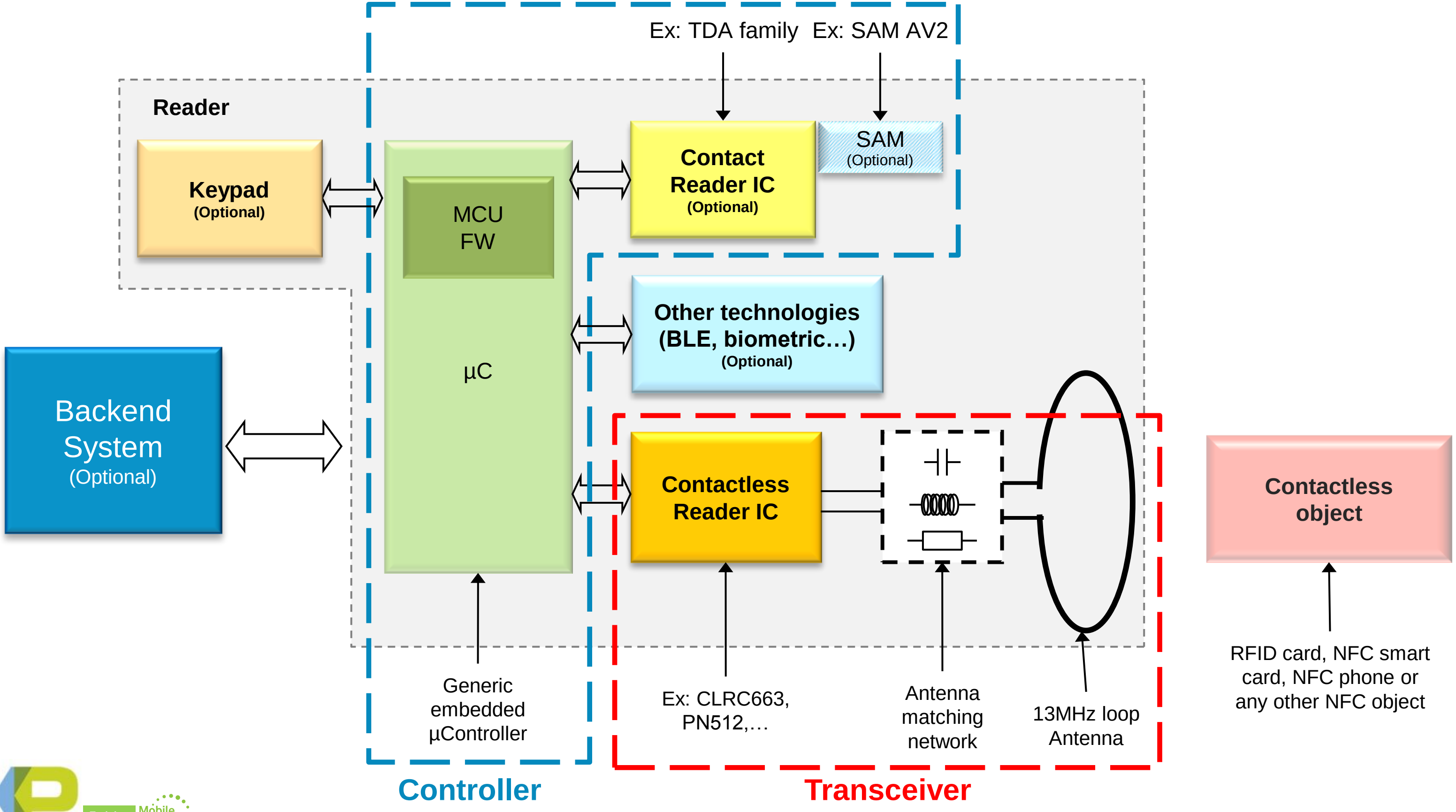
Components in an NFC access control system

Reader

- Can be from a simple transceiver with no intelligence to a complex reader that communicates with a backend and/or makes access decisions on its own
- Conceptually, two parts:
  - Transceiver (the RF frontend)
  - Controller (interacts with the credential through the transceiver, and possibly communicates with other controllers or with the backend)
- May be multi-technology
  - Several technologies in the same device, e.g., NFC, BLE, LF, magnetic stripe, pin pad, biometric...
- Different types: door locks, wall readers, stand-alone readers…
- Everything related to security (keys...) must be in a secure area or stored in a SAM card

Components in an NFC access control system

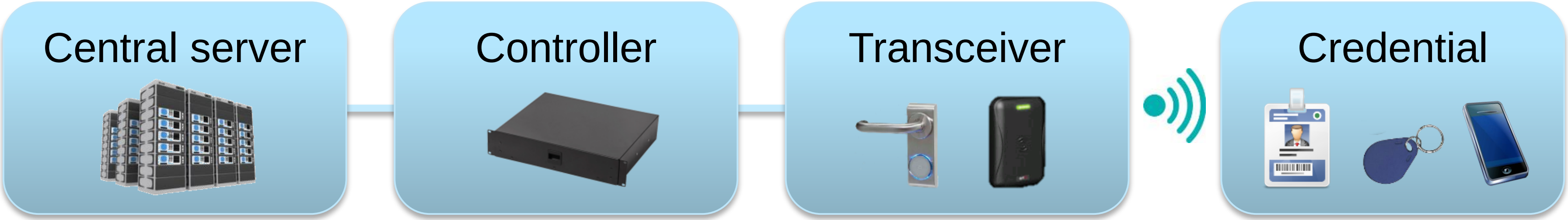
Generic reader architecture



NFC access control system architectures

NFC access control system architectures

Components in an NFC access control system



Optional

May be in the reader and/or separated

In the reader

Independent of the architecture

NFC access control system architectures

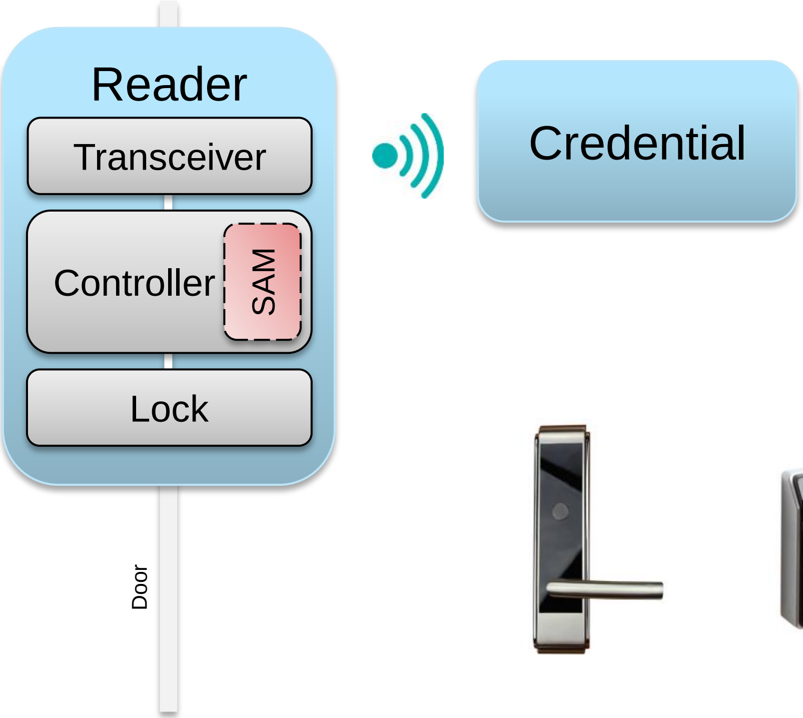
Offline architecture with the controller in the door (door lock)

Advantages

- Cost
  - Easy installation
  - Optimized cost

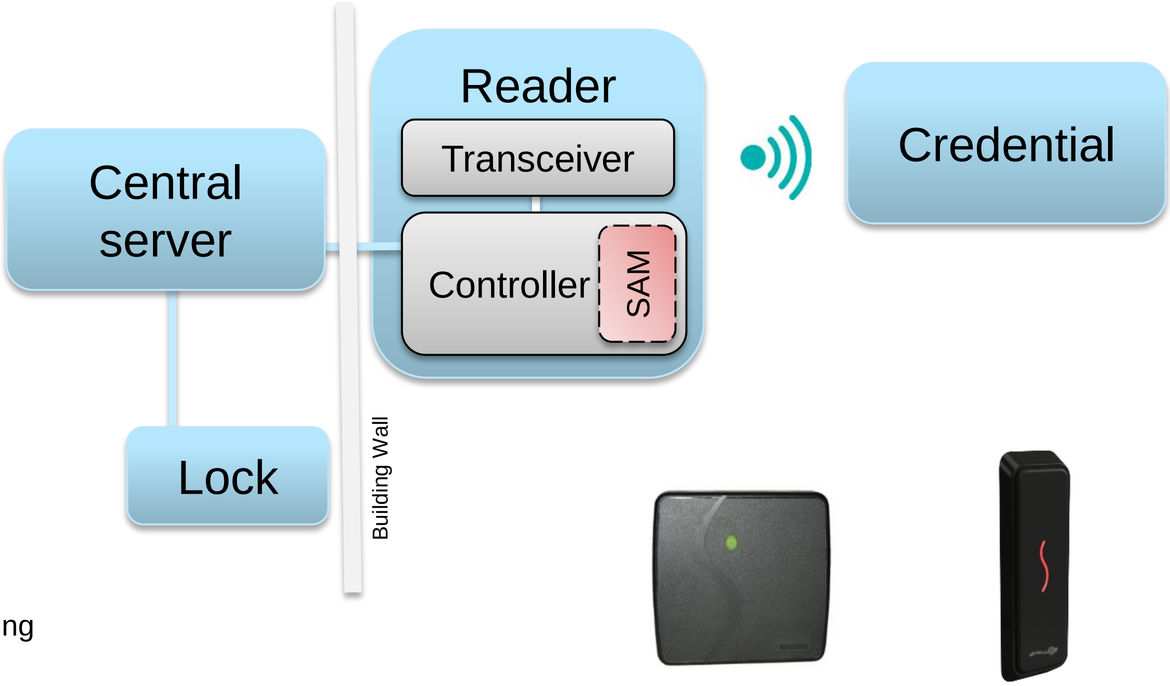
Disadvantages

- Security
  - Can be improved by using a SAM
- Management
  - Complex for a large installation



NFC access control system architectures

Online architecture with the controller outside



Advantages

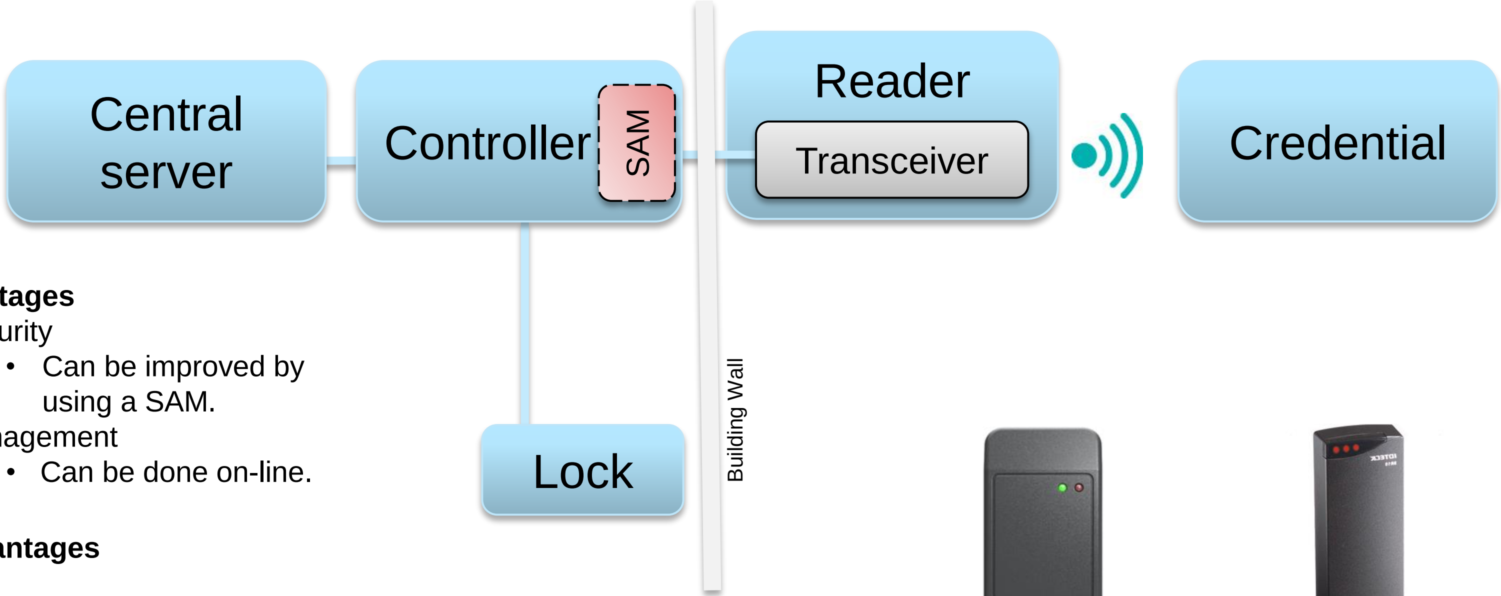
- Management
  - Can be done on-line.

Disadvantages

- Cost
  - On-line architecture
- Security
  - Can be improved by using a SAM

NFC access control system architectures

Online architecture with the controller inside



Advantages

- Security
  - Can be improved by using a SAM.
- Management
  - Can be done on-line.

Disadvantages

- Cost
  - High speed cabling needed.
  - On-line architecture.

NXP products for access control applications

NFC frontends

- High-performance multi-protocol NFC frontend
- Compatible with ISO/IEC 14443-A&B, FeliCa and ISO/IEC 15693 cards
- Low power card detection
- NFC-Ready device (Read/Write, P2P Passive Initiator)

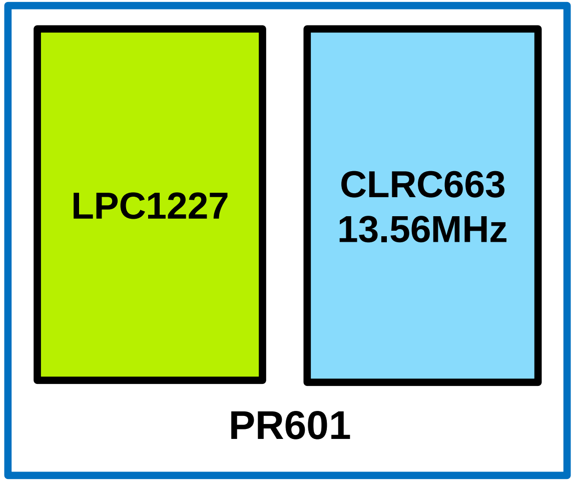
- High-performance MIFARE frontend
- Compatible with ISO/IEC 14443-A cards
- Low power card detection
- Cost-optimized

- Full NFC Forum-compliant frontend
- Compatible with ISO/IEC 14443-A&B, FeliCa and ISO/IEC 18092 devices
- Full NFC device (Read/Write, Card Emulation, full P2P)

NFC controllers

LPC1227

- ARM Cortex-M0 based microcontroller
- Up to 30 MHz
- 128 kB Flash memory
- 8 kB data memory
- Includes an RTC, two comparators, a DMA controller, a 10-bit ADC, a CRC engine...



LPC1227

CLRC663
13.56MHz

PR601

CLRC663

- High-performance multi-protocol NFC frontend
- Compatible with ISO/IEC 14443-A&B, FeliCa and ISO/IEC 15693 cards
- Low power card detection
- NFC-Ready device (Read/Write, P2P Passive Initiator)

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

MIFARE

MIFARE DESFire EV1

- ▶ Flexible file structure for multiple applications
- ▶ 2kB, 4kB and 8kB EEPROM memory
- ▶ Supports DES, 2KTDES, 3KTDES and AES cryptographic algorithms
- ▶ Hardware and software common Criteria EAL 4+ certified

MIFARE Plus

- ▶ 100% backwards compatible with MIFARE Classic
- ▶ 2kB and 4kB EEPROM memory
- ▶ Crypto1 and AES cryptographic algorithms
- ▶ Hardware and software common Criteria EAL 4+ certified

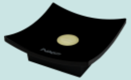
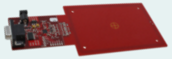
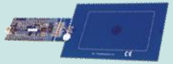
MIFARE 4Mobile

MIFARE4Mobile v2.1

- Specification for the remote management of MIFARE virtual cards and applications in the secure element
- MIFARE DESFire EV1 and MIFARE Classic cards

NXP support material for access control applications

Demoboards

Product	Board	Photo	Description	More info
MFRC523	MFEV710		Reference design for development and testing, supported by the NFC Reader Library.	www.nxp.com/demoboard/MFEV710.html
CLRC663	CLEV663		Evaluation board for multi-protocol CLRC663. Testing reader IC functionalities.	www.nxp.com/demoboard/CLEV663.html
CLRC663	CLEV663B		A two-board combination, with a CLRC663 board stacked on an LPC-Link prototyping board, for use with NXP’s LPC microcontrollers.	www.nxp.com/demoboard/CLEV663B.html
PN512	PNEV512B		A two-board combination that stacks a PN512 board on an LPC-Link prototyping board, for use with NXP’s LPC microcontrollers. NFC Forum-compliant reader IC.	www.nxp.com/demoboard/PNEV512B.html
PRH601	PREV601		Development board for PR601 frontend, supported by the NFC Reader Library.	www.nxp.com/demoboard/PREV601.html
PR601	PREV601M		Microboard with PR601 and 13,56MHz antenna. Powered by a single battery, and supported by the NFC Reader Library.	www.nxp.com/demoboard/PREV601M.html

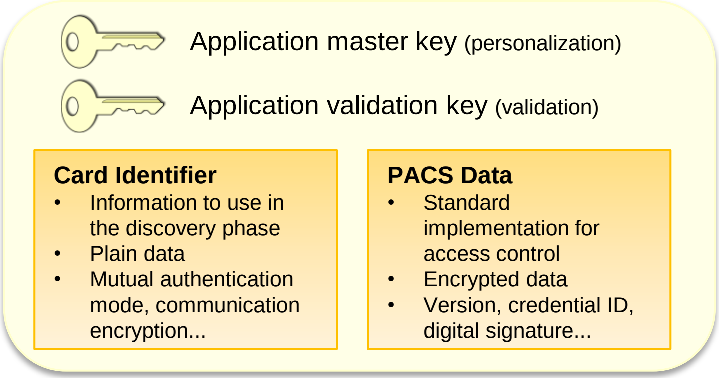
Training Mobile Knowledge

Generic Access Control Data Model

- Common data model that can be supported across card and reader manufacturers to provide interoperability between the card and reader on a physical access system
- Described in NXP application note: AN10957 - Generic Access Control Data Model
- Defines the card application and its content, and the originality check

Card application

- Contains 2 objects (files or sectors, read only) and 2 keys
- Application identifier: 0xF532FN



Application master key (personalization)

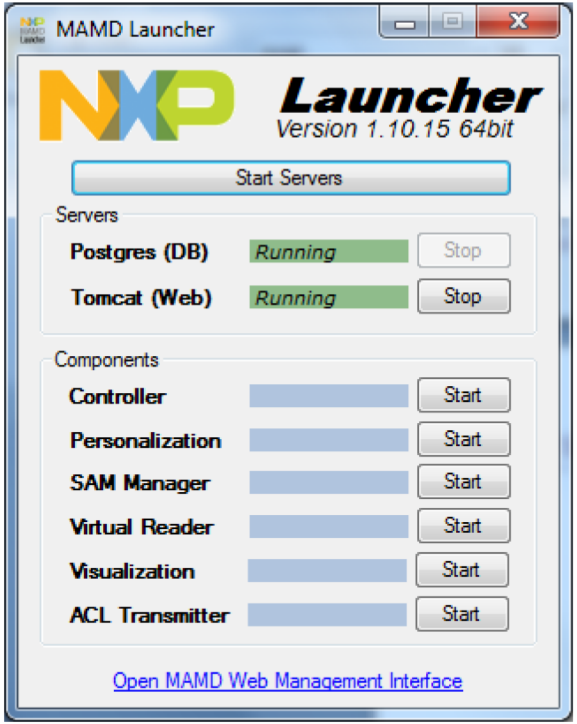
Application validation key (validation)

Card Identifier
- Information to use in the discovery phase
- Plain data
- Mutual authentication mode, communication encryption...

PACS Data
- Standard implementation for access control
- Encrypted data
- Version, credential ID, digital signature...

The MIFARE Access Management Demo (MAMD)

- Access management demo software to deploy an easy conditional access pilot
- Windows based
- Pegodas as readers (with or without SAM)
- Supports MIFARE Classic, Plus and DESFire cards
- Central server simulated in a webserver
- Main software components:
  - Controller (manages the readers)
  - Personalization (personalizes the cards)
  - SAM Manager
  - Virtual Reader (emulates a reader)
  - Visualization (simulates the doors opening)
  - ACL Transmitter
- Software and documentation available on Docstore



MAMD Launcher

Launcher
Version 1.10.15 64bit

Servers

Postgres (DB) Running

Tomcat (Web) Running

Components

Controller

Personalization

SAM Manager

Virtual Reader

Visualization

ACL Transmitter

Further documentation and tools

Documentation

- AN11359 - Access Management Quick Start Guide
  - http://www.nxp.com/documents/application_note/AN11359.pdf
- AN10922 - Symmetric key diversification
  - http://www.nxp.com/documents/application_note/AN10922.pdf
- Establishing Security Best Practices in Access Control by SRLabs/RWE
  - https://srlabs.de/blog/wp-content/uploads/2010/09/Access_Control_Best_Pratices_Study_v1.01.pdf
- Access Control Reader and Credential A&E Specification: Annotated Version by Smart Card Alliance
  - http://www.smartcardalliance.org/wp-content/uploads/AE-Generic-PACS-Smartcard-Reader-and-Credential-Annotated-Version-FINAL-v29-033115.pdf
- NXP applications – Physical access management
  - http://www.nxp.com/applications/access-management/physical-access-management.html

Software tools

- NXP Reader Library
  - Software library providing an API to simplify the development with NXP reader ICs
  - http://www.nxp.com/documents/software/SW297833.zip
- LPCXpresso IDE
  - Development environment for NXP's LPC microcontrollers
  - http://www.lpcware.com/lpcxpresso
- MIFAREdiscover
  - Windows application to get started with MIFARE cards
  - http://www.mifare.net/en/products/mifare-sdk/
- MIFARE SDK
  - Android software library providing an API to simplify the interaction with MIFARE cards
  - http://www.mifare.net/en/products/mifare-sdk/

Conclusion

NFC as the solution for access control

Access denied to unallowed users	✓	Use of state-of-the-art cryptography.
Access guaranteed to allowed users	✓	Contactless technology more resistant to vandalism.
Intuitive and fast access	✓	Simply put the credential next to the reader.
Simple and flexible management	✓	Smartphone credentials can be managed online.
Credential can be used in other applications	✓	MIFARE DESFire EV1 supports multi-application.
Easy installation and optimized cost	✓	Low maintenance costs due to contactless.

NFC Application: Access

Franz Van-Horenbeke (Speaker) / Eric Leroux (Host)

Time for

Q & A

MobileKnowledge

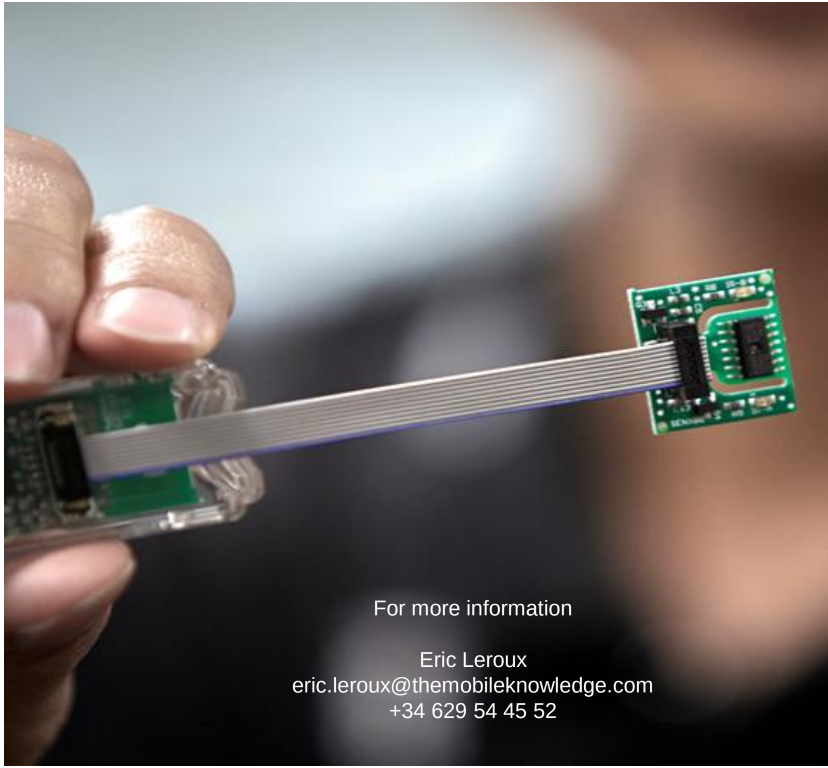
Thank you for your attention

MobileKnowledge
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

Thank you