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?

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access denied to unallowed users</td>
</tr>
<tr>
<td>Access guaranteed to allowed users</td>
</tr>
<tr>
<td>Intuitive and fast access</td>
</tr>
<tr>
<td>Simple and flexible management</td>
</tr>
<tr>
<td>Credential can be used in other applications</td>
</tr>
<tr>
<td>Easy installation and optimized cost</td>
</tr>
</tbody>
</table>
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**

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

*through an NFC device*
Introduction
What is NFC

Card emulation
Contactless readers

Read/write
NFC tags

Peer-to-peer
Other NFC devices

Contactless readers

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

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

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

- More secure

- More convenient

- Low maintenance costs
- No contact needed between the reader and the card
- Durable card

More secure
More convenient
Low maintenance costs
Introduction
NFC in access control

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

- 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

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

Source: IHS 2014, CMI
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
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

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 through 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
- Centralized place that collects data from every online controller
- It may be consulted by online 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

**Reader**
- Keypad (Optional)
- MCU FW
- Contact Reader IC (Optional)
- Contact Reader IC
- Backen System (Optional)
- SAM (Optional)

**Controller**
- Generic embedded µController
- Ex: CLRC663, PN512, ...
- Antenna matching network
- Ex: TDA family
- Ex: SAM AV2
- 13MHz loop Antenna

**Transceiver**
- Contactless object
- RFID card, NFC smart card, NFC phone or any other NFC object
NFC access control system architectures
NFC access control system architectures
Components in an NFC access control system

Central server
Optional

Controller
May be in the reader and/or separated

Transceiver
In the reader

Credential
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...

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)

- 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

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

<table>
<thead>
<tr>
<th>Product</th>
<th>Board</th>
<th>Photo</th>
<th>Description</th>
<th>More info</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFRC523</td>
<td>MFEV710</td>
<td><img src="image1" alt="MFEV710" /></td>
<td>Reference design for development and testing, supported by the NFC Reader Library.</td>
<td><a href="http://www.nxp.com/demoboard/MFEV710.html">www.nxp.com/demoboard/MFEV710.html</a></td>
</tr>
<tr>
<td>CLRC663</td>
<td>CLEV663</td>
<td><img src="image2" alt="CLEV663" /></td>
<td>Evaluation board for multi-protocol CLRC663. Testing reader IC functionalities.</td>
<td><a href="http://www.nxp.com/demoboard/CLEV663.html">www.nxp.com/demoboard/CLEV663.html</a></td>
</tr>
<tr>
<td>CLRC663</td>
<td>CLEV663B</td>
<td><img src="image3" alt="CLEV663B" /></td>
<td>A two-board combination, with a CLRC663 board stacked on an LPC-Link prototyping board, for use with NXP’s LPC microcontrollers.</td>
<td><a href="http://www.nxp.com/demoboard/CLEV663B.html">www.nxp.com/demoboard/CLEV663B.html</a></td>
</tr>
<tr>
<td>PN512</td>
<td>PNEV512B</td>
<td><img src="image4" alt="PNEV512B" /></td>
<td>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.</td>
<td><a href="http://www.nxp.com/demoboard/PNEV512B.html">www.nxp.com/demoboard/PNEV512B.html</a></td>
</tr>
<tr>
<td>PRH601</td>
<td>PREV601</td>
<td><img src="image5" alt="PREV601" /></td>
<td>Development board for PR601 frontend, supported by the NFC Reader Library.</td>
<td><a href="http://www.nxp.com/demoboard/PREV601.html">www.nxp.com/demoboard/PREV601.html</a></td>
</tr>
<tr>
<td>PR601</td>
<td>PREV601M</td>
<td><img src="image6" alt="PREV601M" /></td>
<td>Microboard with PR601 and 13,56MHz antenna. Powered by a single battery, and supported by the NFC Reader Library.</td>
<td><a href="http://www.nxp.com/demoboard/PREV601M.html">www.nxp.com/demoboard/PREV601M.html</a></td>
</tr>
</tbody>
</table>
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

![](image)

<table>
<thead>
<tr>
<th>Card Identifier</th>
<th>PACS Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Information to use in the discovery phase</td>
<td></td>
</tr>
<tr>
<td>- Plain data</td>
<td></td>
</tr>
<tr>
<td>- Mutual authentication mode, communication encryption...</td>
<td></td>
</tr>
<tr>
<td>- Standard implementation for access control</td>
<td></td>
</tr>
<tr>
<td>- Encrypted data</td>
<td></td>
</tr>
<tr>
<td>- Version, credential ID, digital signature...</td>
<td></td>
</tr>
</tbody>
</table>

Application master key (personalization)

Application validation key (validation)
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
Further documentation and tools

**Documentation**

- **AN11359 - Access Management Quick Start Guide**

- **AN10922 - Symmetric key diversification**

- **Establishing Security Best Practices in Access Control by SRLabs/RWE**

- **Access Control Reader and Credential A&E Specification: Annotated Version by Smart Card Alliance**

- **NXP applications – Physical access management**
  - [http://www.nxp.com/applications/access-management/physical-access-management.html](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

- **LPCXpresso IDE**
  - Development environment for NXP’s LPC microcontrollers
  - [http://www.lpcware.com/lpcxpresso](http://www.lpcware.com/lpcxpresso)

- **MIFAREdiscover**
  - Windows application to get started with MIFARE cards

- **MIFARE SDK**
  - Android software library providing an API to simplify the interaction with MIFARE cards
Conclusion
NFC as the solution for access control

- 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

- Use of state-of-the-art cryptography.
- Contactless technology more resistant to vandalism.
- Simply put the credential next to the reader.
- Smartphone credentials can be managed online.
- MIFARE DESFire EV1 supports multi-application.
- Low maintenance costs due to contactless.
NFC Application: Access
Franz Van-Horenbeke (Speaker) / Eric Leroux (Host)

Time for Q & A
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.
Thank you