

# NFC Essentials and Beyond

## Use cases and products

Product Line Secure Transactions and Identification  
September 2019

Rodolfo Gomes EMEA FAE, NFC & IOT ecosystem



SECURE CONNECTIONS  
FOR A SMARTER WORLD



## Agenda

- NFC introduction
- NFC news
- NFC Usecases
- Access control architecture
- New Product Introduction:
  - NTAG 5 family
  - Live-demo
- Q/A session

# Why NFC?

NFC is a short-range wireless communication technology that allows phones, tablets, laptops, and other devices to easily share data with other NFC-equipped devices.



## Easy of use an intuitive

Tap to initiate an action



## User-initiated

User control with deliberate expression of intent



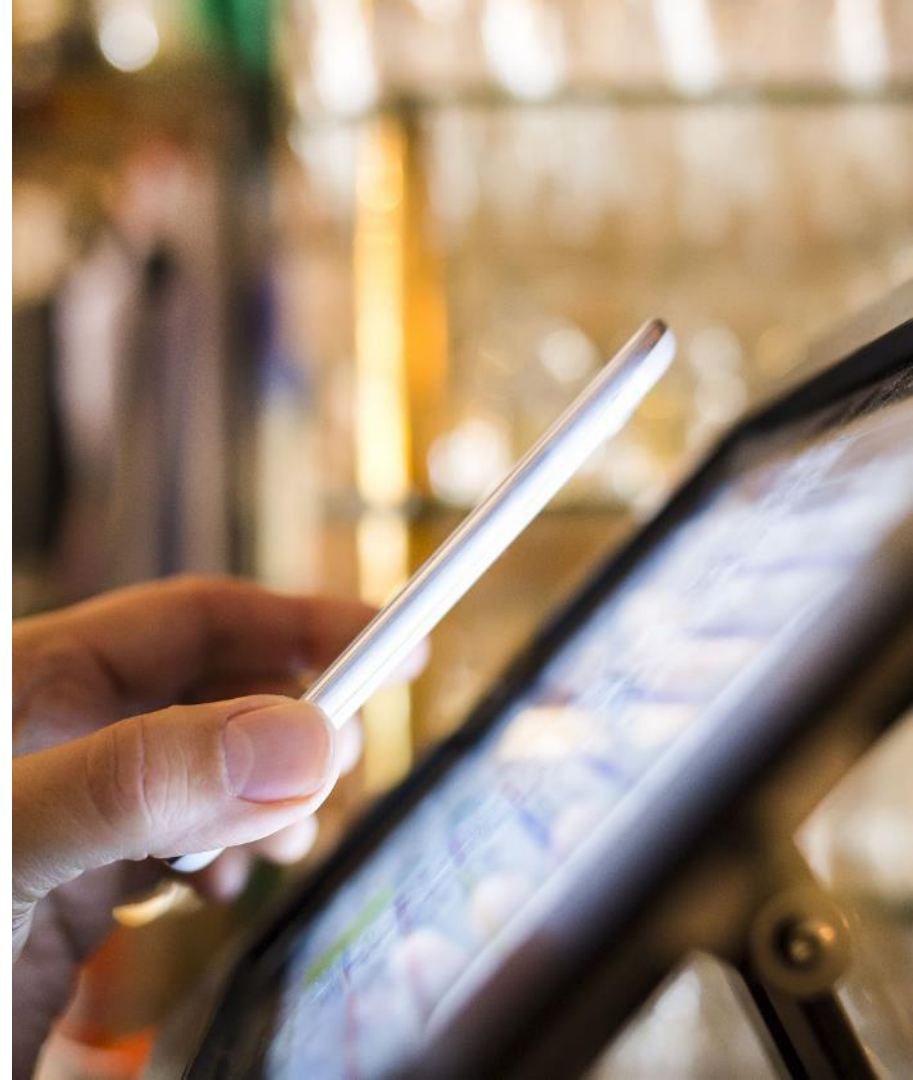
## Use Power very efficiently

Only one of the two devices needs to be powered



## Trusted addition to other technologies

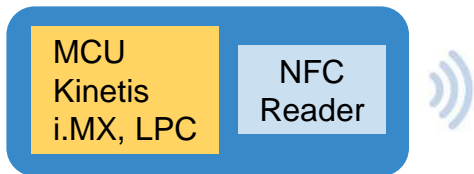
Especially for pairing devices



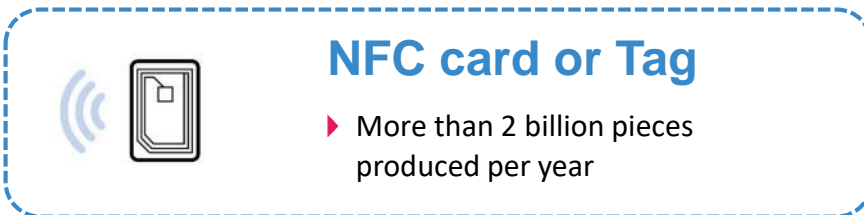
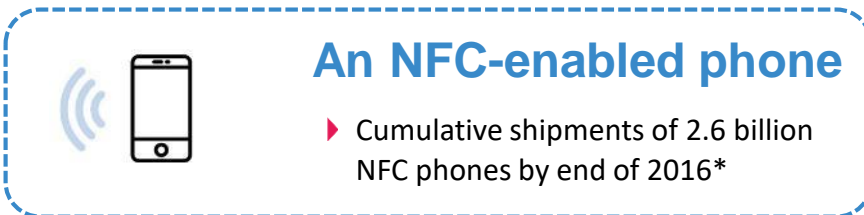
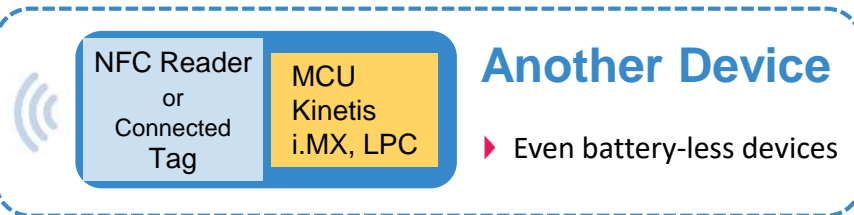
# With NFC, you can interface ...

## Any Device

- Powered by battery or mains
- Can initiate NFC connection
- Reads data in from device or writes data out
- Small: typically ~25 mm<sup>2</sup> IC, 40x30mm antenna
- Many form factors



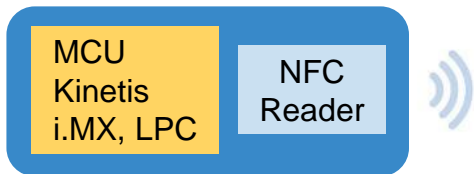
to



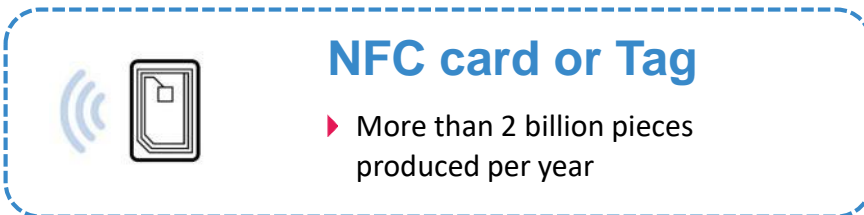
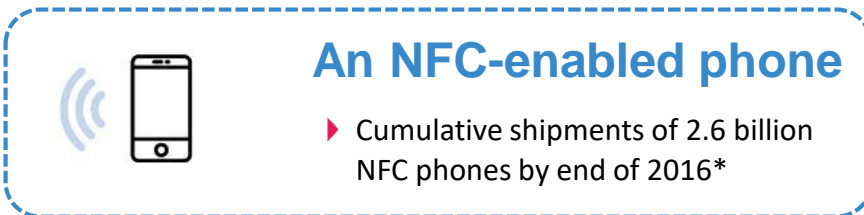
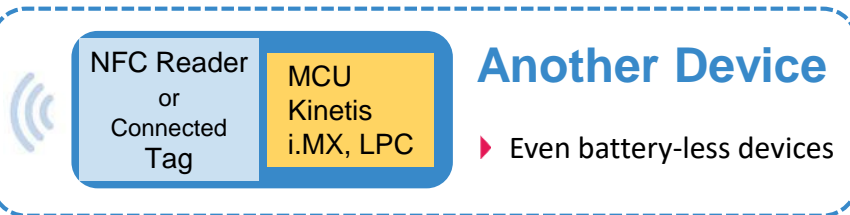
# With NFC, you can interface ...

## Any Device

- Powered by battery or mains
- Can initiate NFC connection
- Reads data in from device or writes data out
- Small: typically ~25 mm<sup>2</sup> IC, 40x30mm antenna
- Many form factors



to

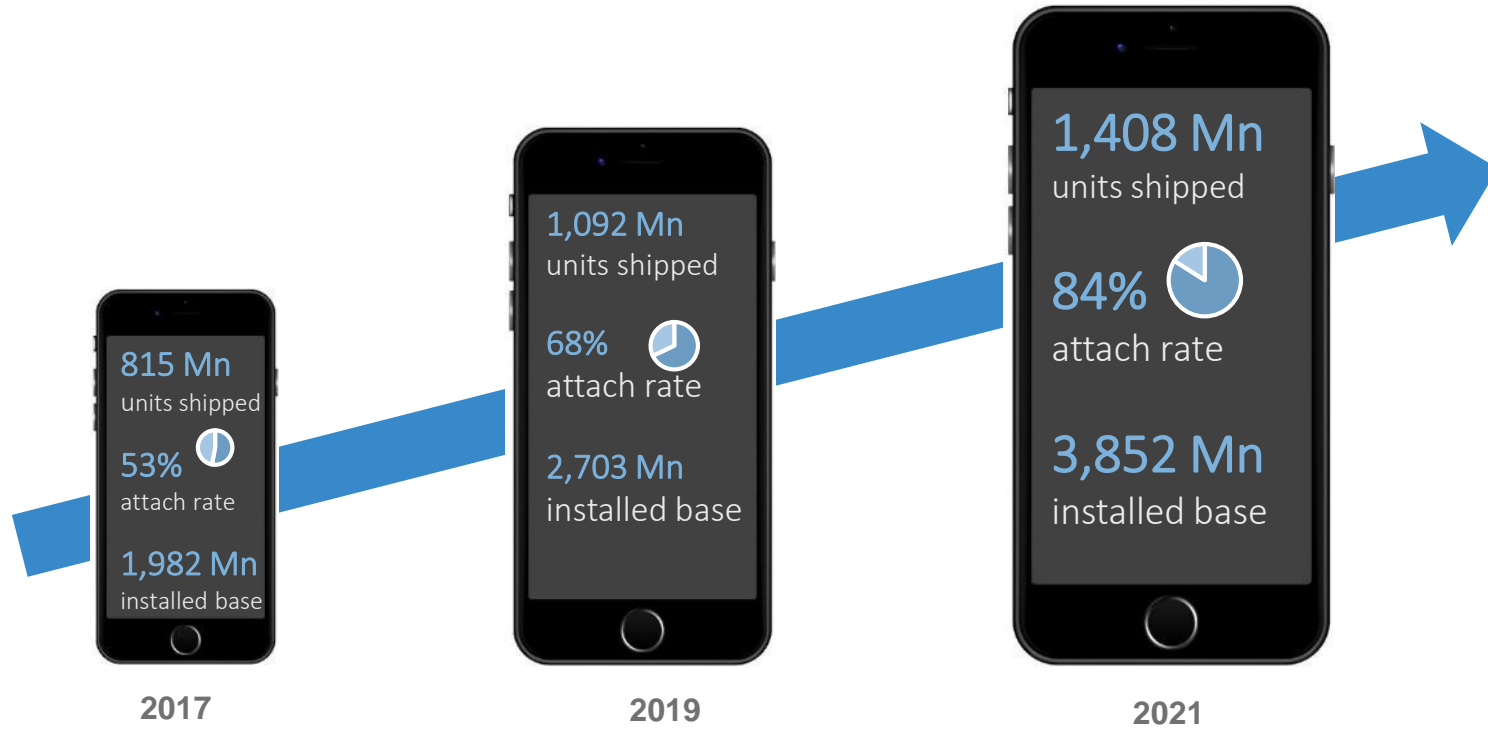


# NFC NEWS

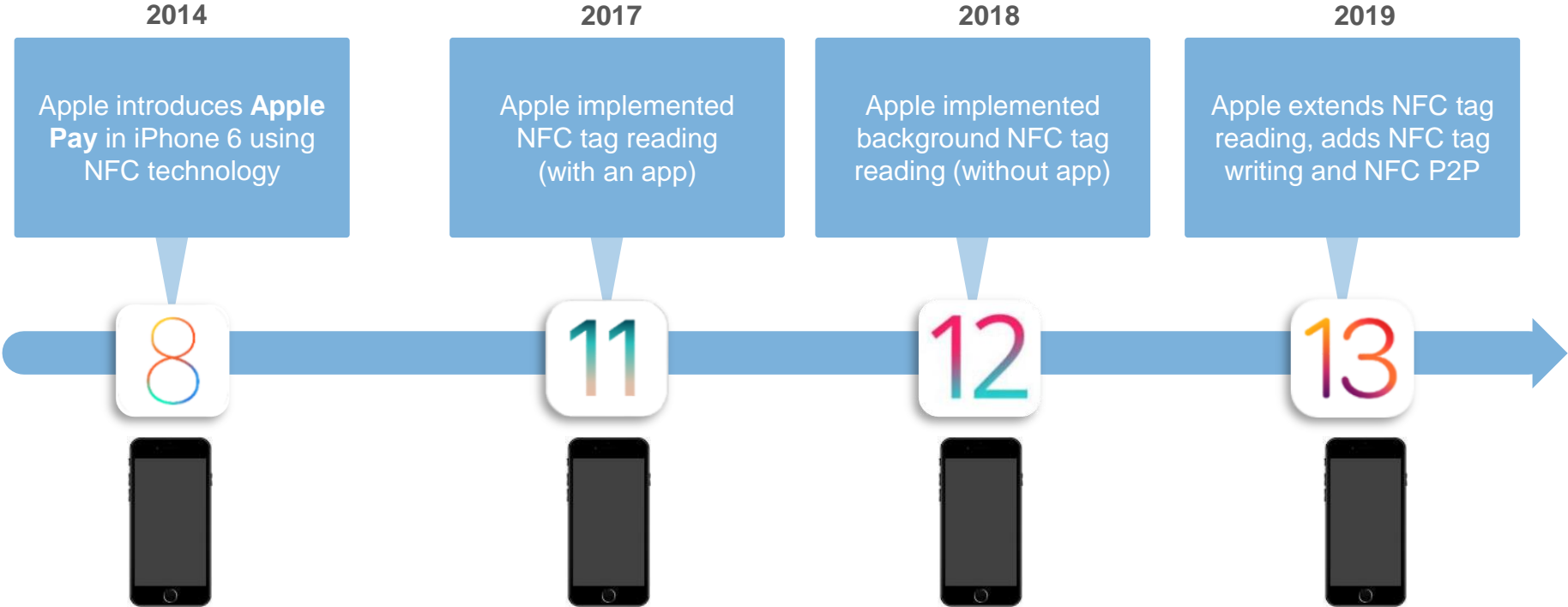


# Dynamic NFC Smartphone Growth

NFC Shipments, Attach Rates and Installed Bases



# Apple expands NFC in iOS 13





# iOS13 includes NFC tag writing in Core NFC framework



	8	11	12	13
<b>NFC payment</b>	Apple Pay	Apple Pay	Apple Pay	Apple Pay
<b>Read NDEF</b>	No	With an app	Yes	Yes
<b>Write NDEF</b>	No	No	No	Yes
<b>Native tag reading</b>	No	No	No	Yes
<b>MIFARE support</b>	No	No	No	Yes
<b>ISO15693 support</b>	No	No	No	Yes
<b>ISO7816 support</b>	No	No	No	Yes
<b>FeliCa support</b>	No	No	No	Yes

# PRESENT AND FUTURE NFC USECASES



# NFC enables a world of use cases



# NFC Use Cases for Home Appliances

- Last stage FW configuration in factory
- Simplify the pairing of connected devices
- Add wireless connectivity to phones & cloud
- Authentication and configuration
- Replace cable
- Authenticated redirection
- Improve safety
- Solve the installation of smart home system



Save  
cost



Bring  
ease-of-use  
to customers



Increase  
revenue

# Firmware update in last production stage

- **Write data wirelessly into the brush memory**

- Write configuration data
- Write URL for easy replenishment
- No need to power on the brush



- **Write data wirelessly into the handle**

- Write firmware, e.g. in User Interface micro-controller
- Write configuration data to generate multiple product variants from a single platform
- Write serial number to facilitate warrant registration, return logistics
- No need to disassemble the handle, only power



# NFC helps to pair connected Home Appliances to your network



***Applications: Smart refrigerator, washing machine, oven, laundry dryer, robot cleaner, air conditioner, air cleaner, IoT bridge, ...***

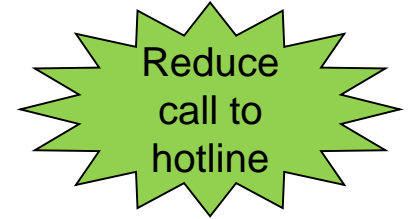
- NFC is used for establishing a connection link between 2 devices, e.g. a WiFi Gateway and a home appliance, this is called “connection handover”
- WiFi pairing becomes very easy
  1. Pair the phone to the WiFi network
  2. Send the WiFi credentials to the home appliance, with NFC, by just one tap with phone
- Saves cost by reducing customer care calls: no search for the network SSID, no long password, forget mixing “0” and “O”, upper/lower case
- Works only with Android NFC phone today

# Pair your device to your phone with a tap



*Bluetooth pairing  
in one tap*

- **So easy:** pairing in just one tap
  - No need to go into menus of the phone
  - No need to search for BT device
  - No conflict is possible
- **Inherently secure** by proximity
- **Save costs:** reduce customer care calls



# Add connectivity to phone and the cloud

- NFC is a straightforward technology for adding connectivity to any - not connected – home appliance
- Integrating NFC enables the following use cases
  - **Register the device** in one tap
  - **Program the device** with phone\*
  - **Run self diagnostics and fix problems** with cloud assistance
  - **Update the firmware** with phone\* if necessary
- Applications: any Home Appliance

reduces  
calls to  
hotline (5\$)

\* works only with Android NFC phone today





# Authentication and configuration

- For devices with a removable part which needs regular replacement, NFC allows to
  - **Authenticate the removable part**, making sure that the right genuine part is used, thus protecting revenue
  - **Configure the base unit** to the accessory E.g. rotating and spinning parameters
  - **Easy replenishment**: tap NFC phone to the accessory and connect directly to the right web page for ordering
- Applications: air filter & conditioner, electric toothbrushes, facial brushes, hair dryer, ...



NFC tag

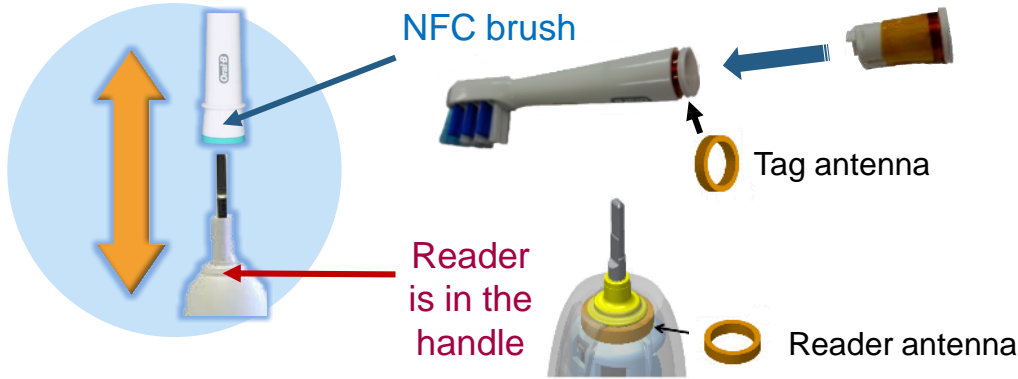


NFC Reader in the base



Increase accessories revenue

# NFC in electric toothbrushes: how it works



A simple tap  
for  
replenishment



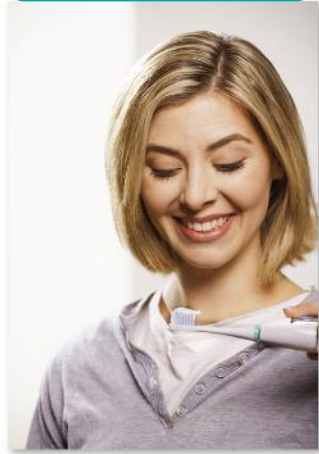
- Upon activation, brush profile is read & tag counter is incremented
- Tag counter increments at start of use, and ignores short cycles within intervals of less than 10 seconds
- Upon expiration, handle vibrates and/or illuminates to indicate it's time for replenishment
- Consumer simply taps brush for a convenient re-order experience

# Authenticated redirection

- Effortless consumable replenishment in one tap
- How this works?



- 1 Replacement notification
- 2 Phone read NFC Tag in consumable
- 3 Consumable authenticated via the cloud
- 4 Easy re-order from authorized suppliers



Consumer scans the consumable with an NFC-enabled phone. Data stored on the tag directs user phone to initiate appropriate action.

## Benefits to the OEM

- Increased revenues
- Reduced ads cost
- Real-time analytics
- Offer more services

## Benefits to the Consumer

- Much faster
- Verify correct model
- Ensure genuine replacement
- Pre-approved retailers

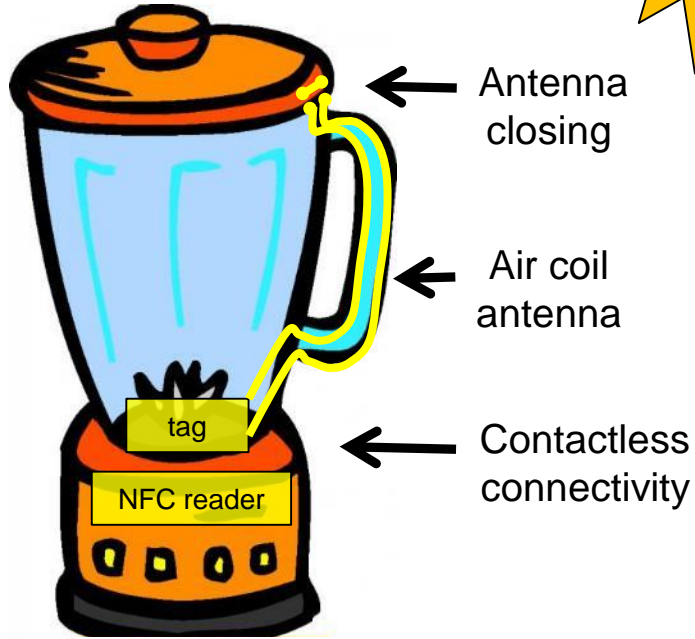


# NFC improves safety

9600 injuries  
in USA  
in a year

+20%  
YoY

Safe  
latch



- NFC is an effective solution for adding a safety interlock to a container
- 100% protection: no power until the container is properly placed and closed on its base
- Add more use cases on top: container configuration, authentication → increase revenue
- Applications: blender, food processor, ...

# NFC replaces cables

- Bi-directional contactless connectivity between 2 parts



*Communication speed up to 106kbits/s*

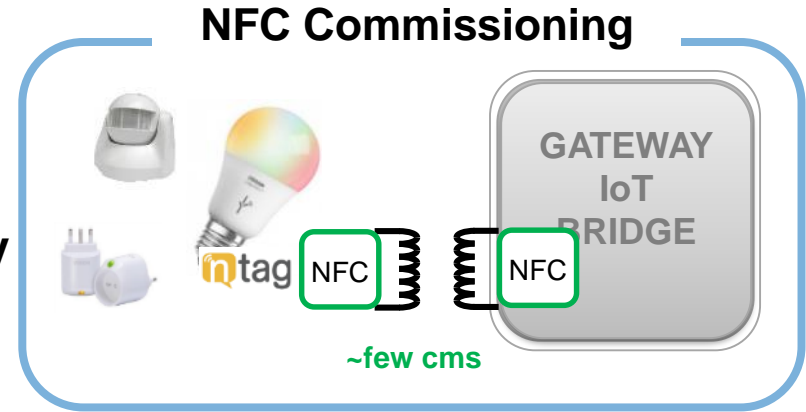
- Save cable and connectors cost, and remove mechanical constraints
- Give battery-free parts the ability to communicate, powered by the NFC field
- Applications:
  - Any home appliance



# NFC solves the installation of smart Home system

- 1) Tap the NFC node to the Gateway to load the network credentials  
No need to power on the node
- 2) Power on the **node**, and it's **automatically added to the smart home network**

- ✓ **Easy:** no manual entry
- ✓ **Flexible:** all kind of protocol supported
- ✓ **Secure:** network key exchange guaranteed by proximity
- Applications: smart lighting, home automation



# WHITE GOODS USE CASES



# Smart Washing Machine

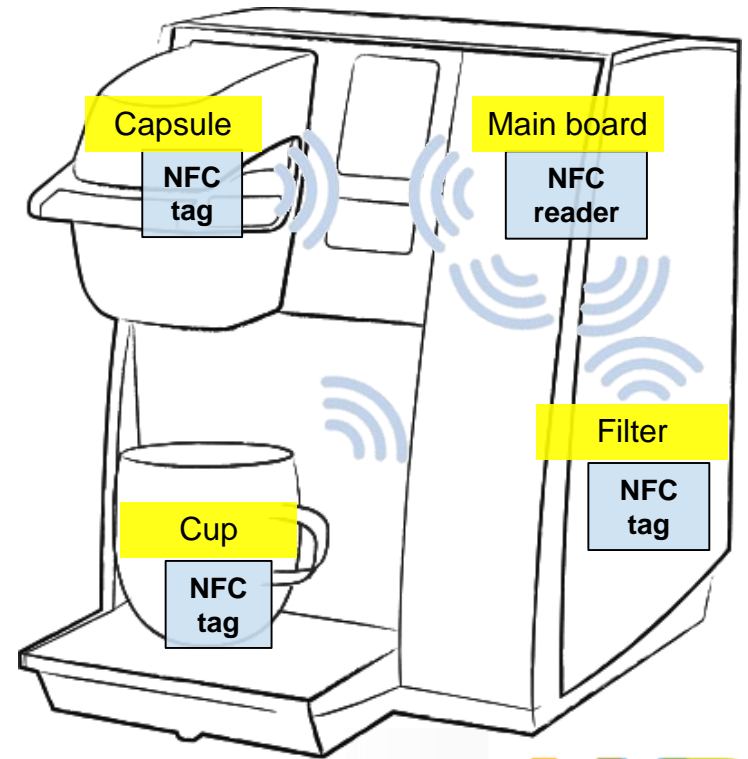
Use case	Detection Location
User authentication	A
Washing agent tabs identification	B
Washing Agent fluid identification	C
Diagnostic – service with NFC	A



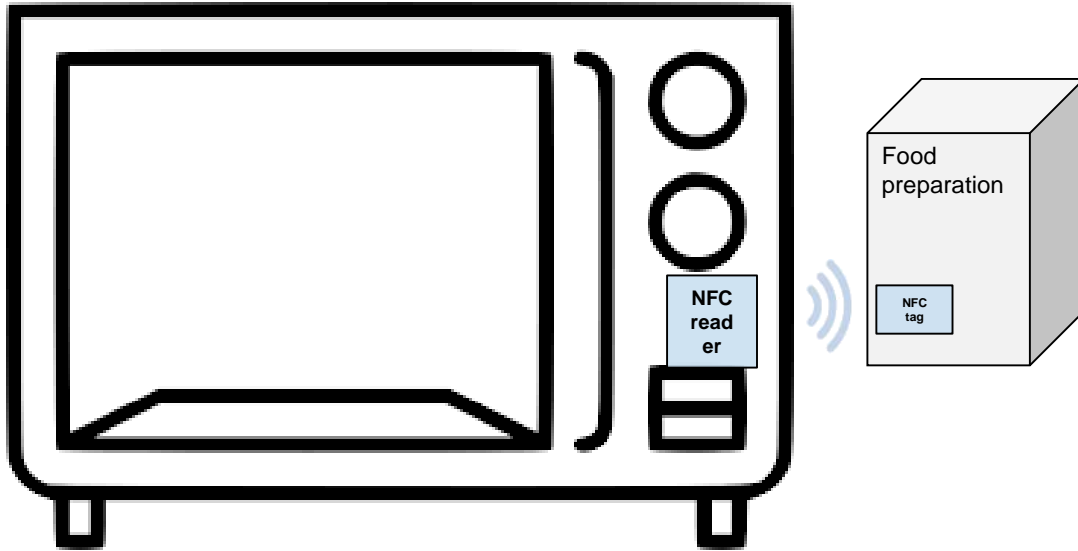


# SMART COFFEE MACHINE

- Cup detection
- Coffee capsule authentication
- Coffee refill bag authentication
- Water filter detection
- Machine data collection with NFC phone
  - Product data
  - Production data
  - Production tracking
  - Link product to cloud
- Product maintenance

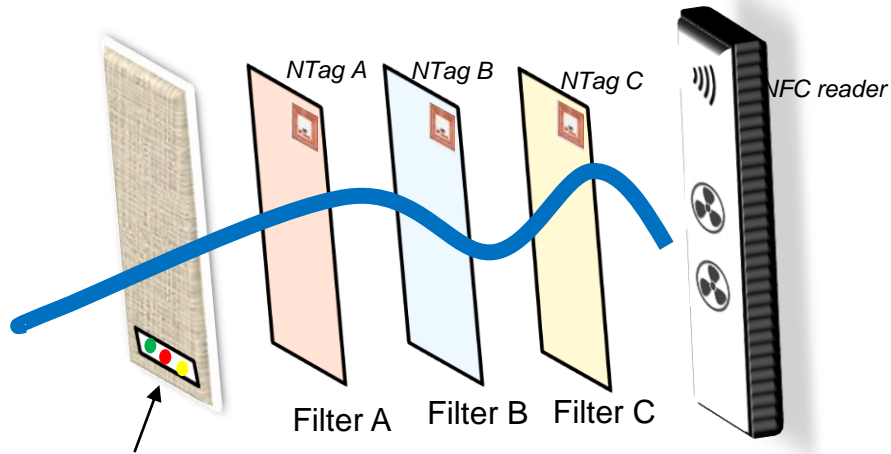


# Smart Oven



- Food identification
  - Transfer of cooking parameters
- NFC enables the oven to capture instructions from product and to prepare food automatically based on product's recipe.
- Machine data collection with NFC phone
    - Product data
    - Production data
    - Production tracking
    - Link product to cloud

# Smart Air purifier



Front panel with LED indicators

- Filter presence check
- Filter authentication
- Genuine filter verification
- Filter status check
- Filter orientation check
- Filter re-ordering



# Big release of NFC devices in the last 12 months

**mi** Xiaomi



Air Purifier 2S



Air purifier Pro

**PHILIPS**



Visapure

**nest**



Secure alarm

**Vitamix**



A2500 &  
A3500



Link

**LG**



LWD3063BD

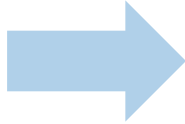
# ACCESS CONTROL ARCHITECTURE



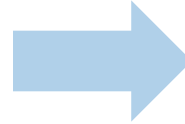
# NFC access management becoming more personal



Corporate Access



Hospitality



Residential Access



# NFC in access control



## More secure

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



## More convenient

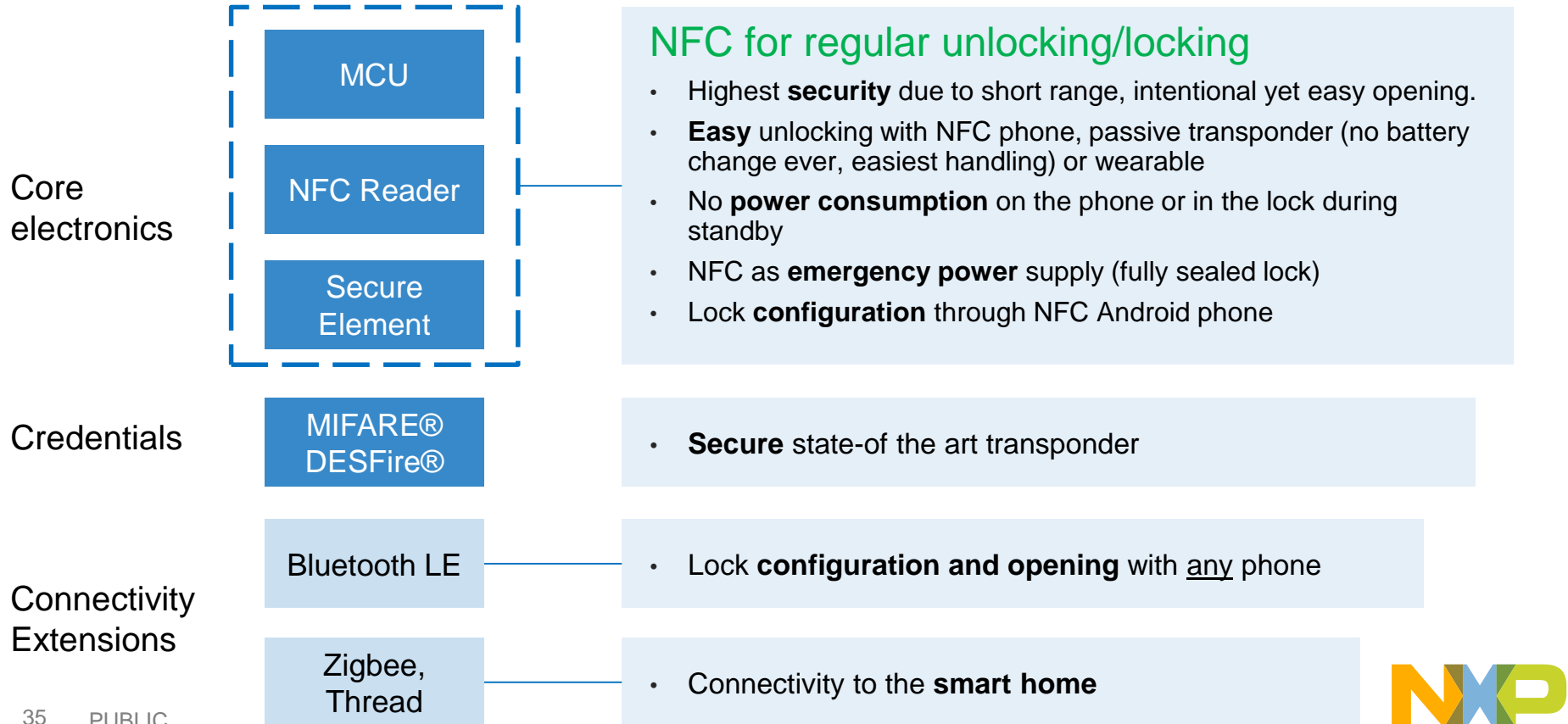
- ▶ **Fast**
- ▶ **No need** to put the card in a **specific position**
- ▶ Allows **multi-application** solutions
- ▶ Allows **multi-site** solutions



## Low maintenance costs

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

# NXP solutions for smart door locks

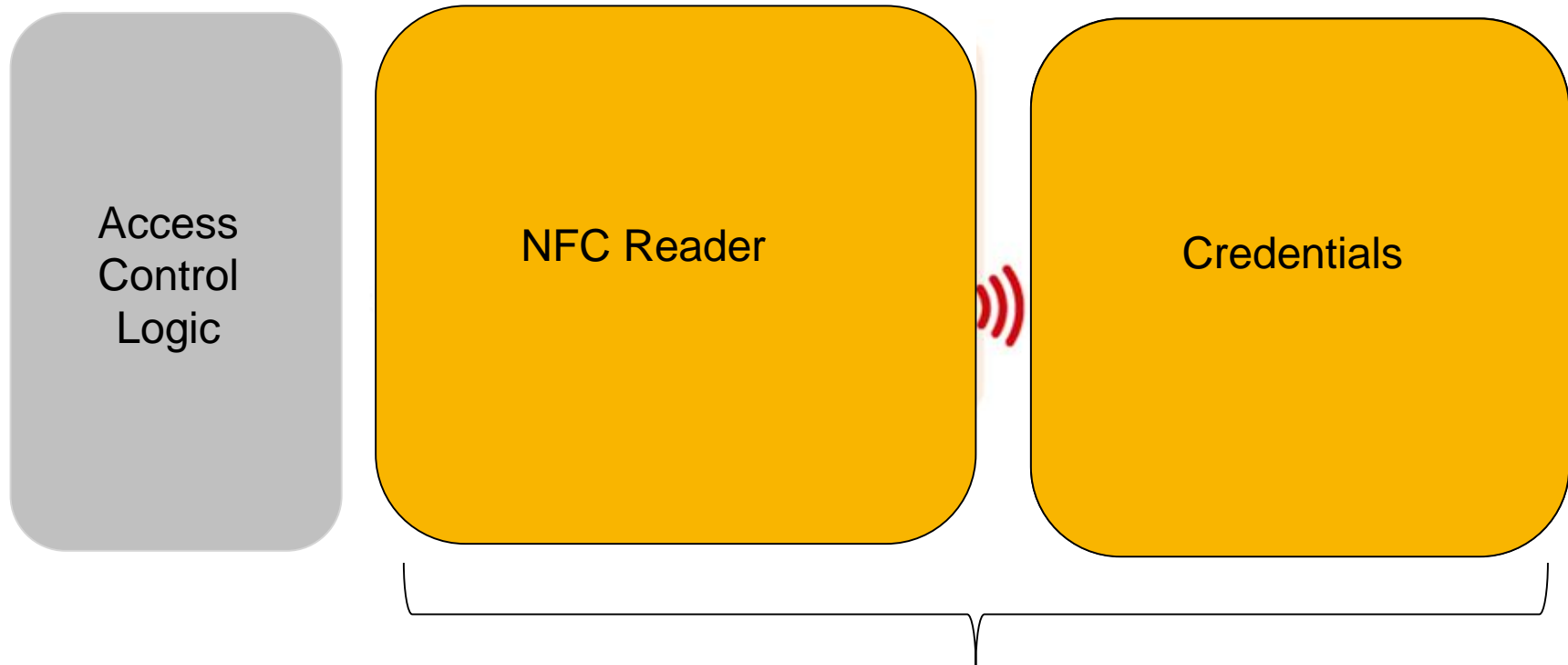




# NXP PRODUCTS FOR ACCESS CONTROL



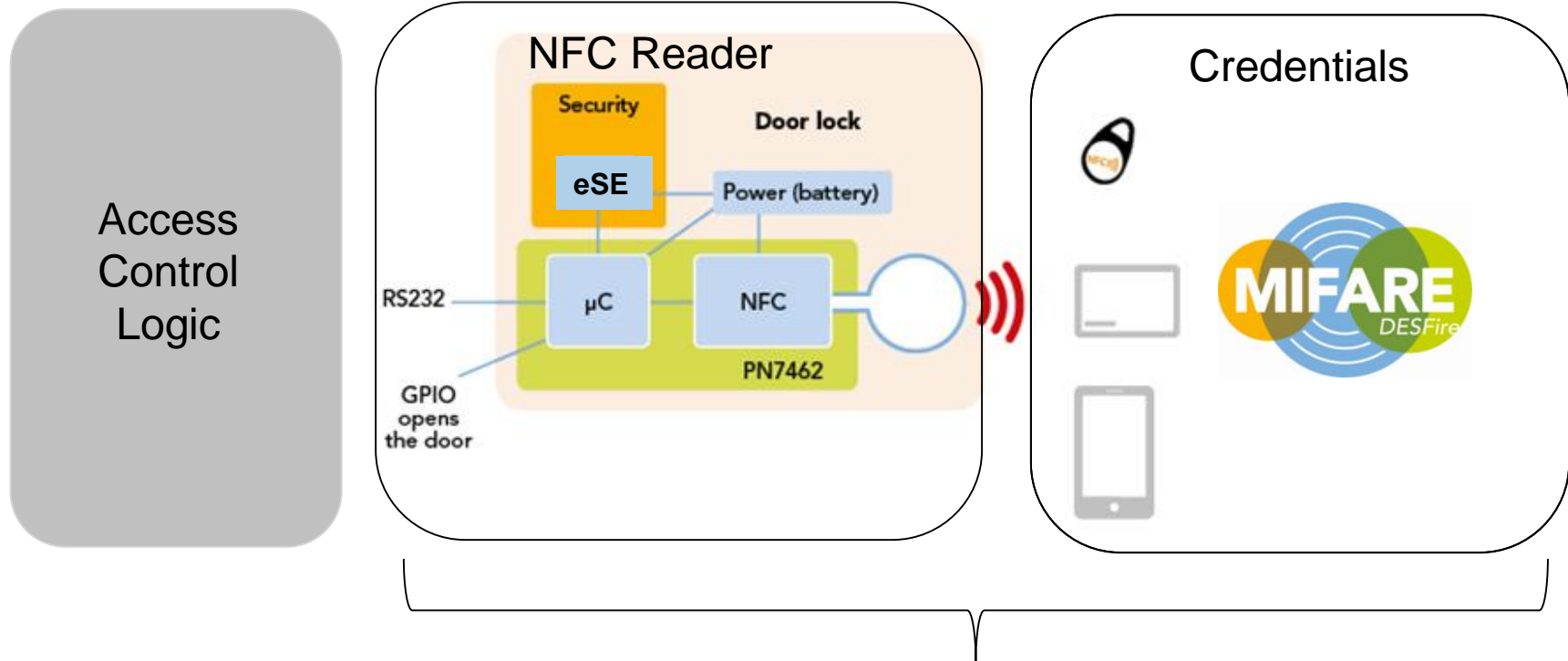
# NFC building blocks for Access Management



**NXP reader and card IC offering perfectly matching for highest security, functionality and performance**



# NFC building blocks for Access Management



**NXP reader and card IC offering perfectly matching for highest security, functionality and performance**



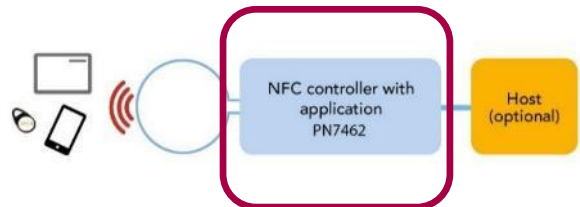
# NFC for Access Management – featured products

NFC controller solutions

Combination of NFC frontend with an advanced 32-bit microcontroller.

Options include integrated firmware or freely programmable microcontroller.

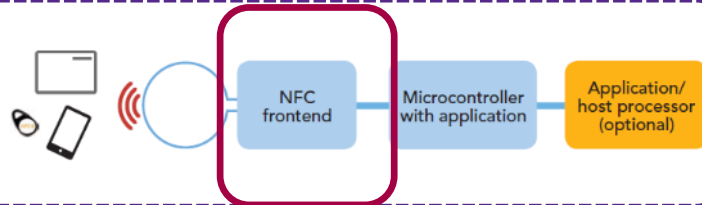
**Product: PN7462**



NFC frontend solutions

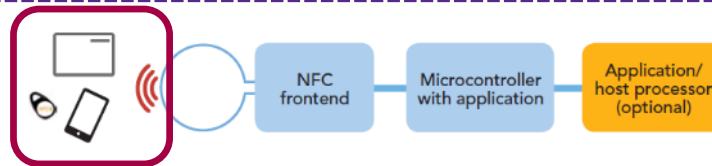
The most flexible way to add NFC to a system.

**Product: CLRC663 plus**



NFC Cards

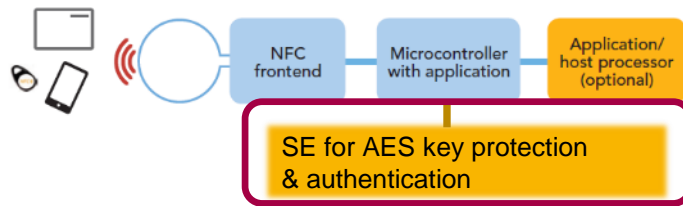
**Product: MIFARE DESFire EV2**



Secure Elements (SAM, eSE)

Secure key Storage in reader (optional)

**Products: MIFARE SAM AV3, SE050C**



# MIFARE DESFire EV2 – features & performance

## Contactless Performance

Convenient touch'n'go experience through excellent read range

Fast and reliable transactions

Design freedom for smaller form factors on the credential and reader side (key fobs).



## Security & Privacy

Next level security certification CC EAL5+

Security self healing mechanism with rolling keys

Random ID for privacy protection



## Multi-application

Enabling new business models through seamless integration of additional services like loyalty or micropayment



# MIFARE DESFire EV2 – features & performance

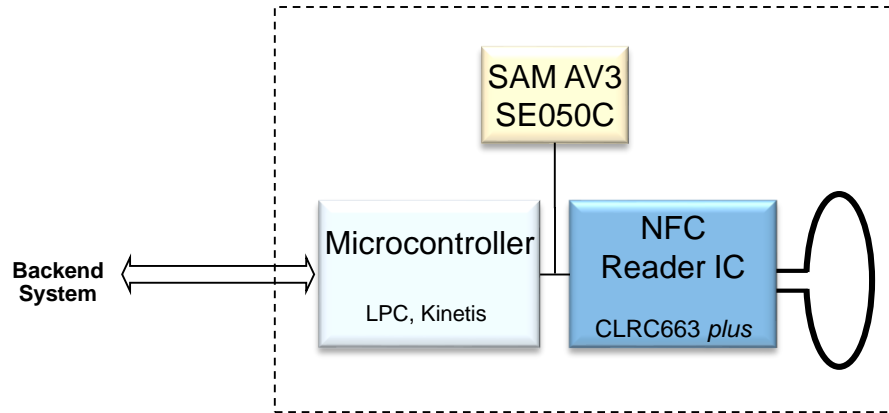


- 3<sup>rd</sup> generation of MIFARE DESFire family
- Bringing multi-application supports to the next level
- Improved end user experience with superior operating distance and performance
- Benchmark security design with Common Criteria EAL 5+ certified HW & SW

ISO/IEC 14443 A 1-4	✓
ISO/IEC 7816-4 support	extended
EEPROM data memory	2/4/8KB
Flexible file structure	✓
NFC Forum Tag Type 4	✓
Secure, high-speed cmd	✓
Unique ID	7BUID or 4B RID
Number of applications	unlimited
Number of files per app	32
High data rates support	up to 848 Kbit/s
Crypto algorithms support	DES/2K3DES/ 3K3DES/AES
CC certification (HW + SW)	EAL 5+
MIsmartApp feature	✓
Transaction MAC per app	✓
Multiple keysets per app	Up to 16 keysets
Multiple file access rights	Up to 8 keys
Inter-app files sharing	✓
Virtual Card Architecture	✓
Proximity Check	✓
Delivery types	Wafer, MOA4 & MOB6

# Secure element to protect keys and execute 3-step authentication

- ▶ Secure storage of application keys in an embedded secure element based on common criteria certified HW
- ▶ Dedicated SAMs (Secure Application Module) offering for NXP card ICs (e.g.: MIFARE DESFire EV2)
- ▶ Compatibility with all established NXP smart card IC's, smart tags and label technology



# MIFARE Secure Access Modules (SAMs)

- ▶ NXP's MIFARE SAMs offer **secure storage** and **communication** in a variety of infrastructures



**MIFARE SAM AV2**  
**NEW!! MIFARE SAM AV3**

- ▶ Supports MIFARE DESFIRE, 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, ideal for public transport operators
- ▶ 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

More information: [Data sheet](#)

[SAM AV3 overview page](#)



# Embedded Secure Element for MIFARE DESFire authentication

- ▶ NXP's EdgeLock SE050C secure element offers **secure storage for symmetric keys** and **MIFARE DESFire communication scheme** for simple access control systems



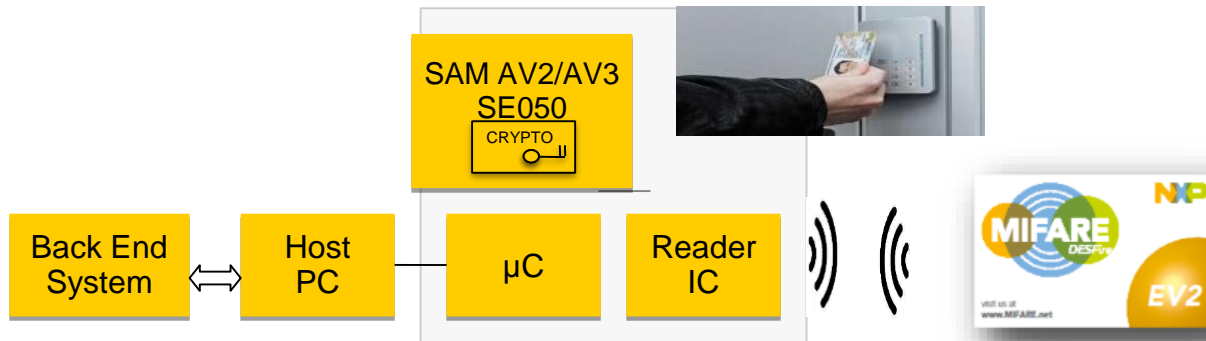
**SE050C**

- ▶ Supports MIFARE DESFire key derivation and authentication
- ▶ Can be used for generating session key based on symmetric cryptography (then export it to MCU for communication with card)
- ▶ Supports TDES, AES, RSA and ECC cryptographic algorithms
- ▶ 50kbyte eSE space to store and protect symmetric keys
- ▶ I2C slave interface up to 3.4Mbps
- ▶ Hardware Common Criteria EAL 6+ certified

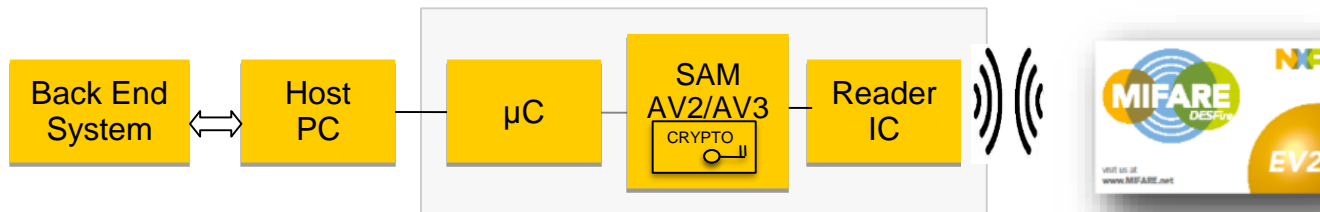
More information: [Data sheet](#)

or simply go to <https://www.nxp.com/SE050>

## Reader Design with SAM AV2/AV3 or SE050C (for PN7462)



## Reader X-Mode design supported by SAM AV2.6 and AV3 (for CLRC663 *plus*)



The SAM is directly communicating with the ReaderIC → it is directly writing into the registers for the IC  
SE050C does not support X-Mode

# Secure Access for Industrial IoT: Live Demo

Based on NXP's latest technologies:

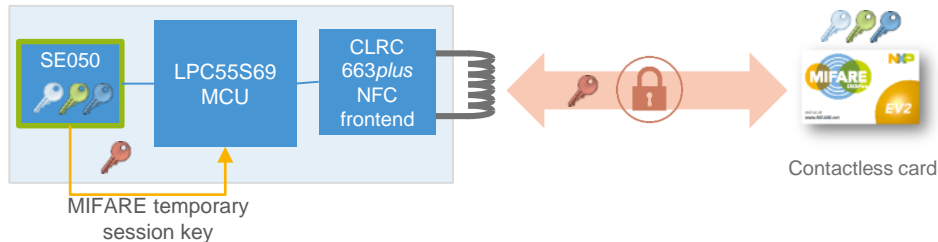
EdgeLock™ SE050 - LPC55S69 - CLRC663 plus - MIFARE® DESFire® EV2

## Role of SE050

- SE050 supports secure operation for MIFARE DESFire
- SE050 stores the secret key
- SE050 supports MIFARE key derivation function and generates the session key

## How it works

- The DESFire card and the EdgeLock SE050 store the secure keys
- The DESFire card is presented to the contactless CLRC663plus reader
- The CLRC663plus detects the card, notifies this to the LPC55S69, powers up and communicates with the card
- The LPC55S69 uses the SE050 to authenticate the MIFARE credentials
- SE050 derives and exports the MIFARE session key to the LPC55S69
- The LPC55S69 runs the standard Smart Card / MIFARE command set
- The DESFire is securely authenticated in the 3 step authentication.



# Application Notes and Links Access Management

## MIFARE DESFire EV2

[Short datasheet](#)

[Additional product infos](#)

Full datasheet: NDA required – send email to

[MIFARE\\_DESFIRE\\_NDA@nxp.com](mailto:MIFARE_DESFIRE_NDA@nxp.com)

## MIFARE DESFire Light

[Datasheet and application notes](#) (no NDA needed)

## MIFARE SAM's for reader design

[Website](#)

## eSE SE050

[Website](#)

## Reader ICs

[Overview](#)

[PN7462](#)

Access Management Quick Start Guide – [AN11359](#)

Symmetric key diversification – [AN10922](#)

Establishing Security Best Practices in Access Control by SRLabs/RWE – [Link](#)

NXP applications – [Physical access management](#)

# NEW PRODUCT INTRODUCTION: NTAG5



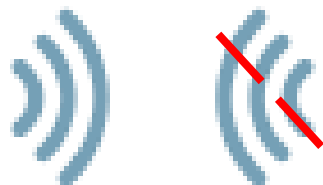
# NTAG 5 family overview – main features

Feature	NTAG I <sup>2</sup> C plus	NTAG 5 switch	NTAG 5 link	NTAG 5 boost
NFC interface	ISO/IEC14443	ISO/IEC15693	ISO/IEC15693	ISO/IEC15693
Energy harvesting	yes up to 15 mW	regulated up to 30 mW	regulated up to 30 mW	regulated up to 30 mW (in passive mode)
GPIO + PWM	-	✓	✓	✓
Memory areas	2	3	3	3
Memory protection	Password	Password	Password and AES authentication	Password and AES authentication
I <sup>2</sup> C interface	slave	-	slave / master	slave / master
Pass-through via SRAM	proprietary	-	proprietary and standardized	proprietary and standardized
Active load modulation (when V <sub>CC</sub> supplied)	-	-	-	✓

Launch: Q4/2019

# NTAG 5 boost brings NFC to tiny devices

NFC read range vs. Antenna sizes

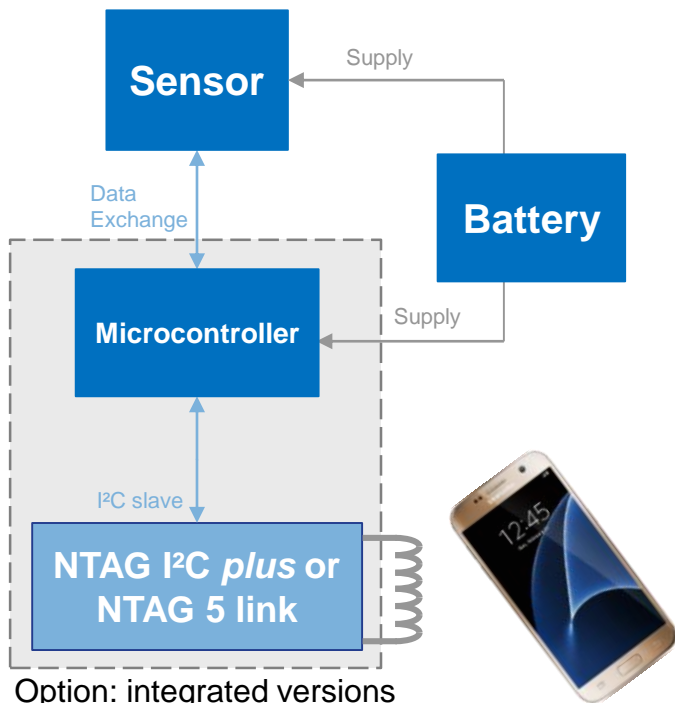


The small antenna cannot drive enough energy to sufficiently back-modulate to the reader.



# NTAG 5 link brings NFC to MCU-less devices

I<sup>2</sup>C master mode enables controlling any I<sup>2</sup>C peripheral via NFC



Option: integrated versions  
LPC8N04 or NHS31xx

Constant monitoring of sensors  
requires an MCU

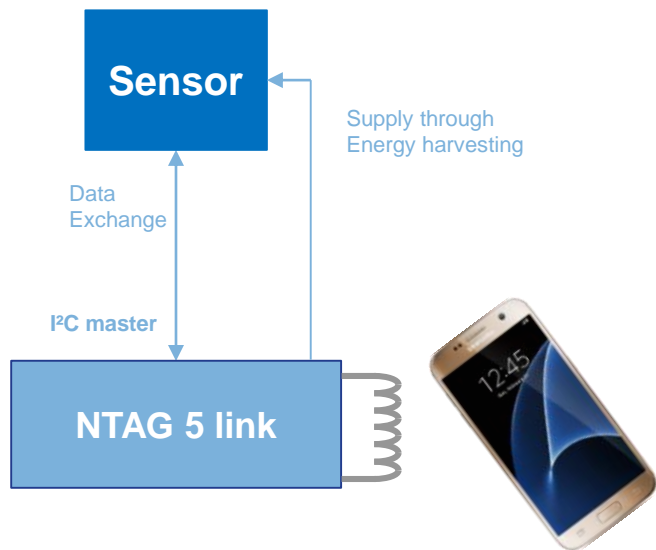
## NFC Benefits

- Device can be fully sealed  
NFC communication possible through  
plastic, glass, wood, ...
- Passive reading – no battery  
consumption
- Together with consumer mobile  
phone: cost efficient IoT solution



# NTAG 5 link brings NFC to MCU-less devices

IoT on demand: direct NFC → I<sup>2</sup>C bridge



## Benefits

- Overall BOM reduction:
  - **No Battery** needed
  - **No MCU** needed
  - data preparation in app or cloud
- Especially for devices where power is an issue
- Reading/writing to any I<sup>2</sup>C peripheral even when MCU is broken or non responsive

# BACKUP SLIDES



SECURE CONNECTIONS  
FOR A SMARTER WORLD