GlobalLogic®

Near Field Communication & Digital Transformation

Author: Ritesh Dubey
Co-Author: Vikas Khunteta

Contents

Introduction

Near Field Communication (NFC) is an RFID-based standardized, contactless, short-range wireless connectivity technology that makes life easier and more convenient for consumers around the world. It does this by making transactions simpler through exchanging digital content, and connecting electronic devices with just a touch. NFC is compatible with millions of contactless cards and readers already deployed worldwide.

This emerging technology, jointly developed by Sony and NXP Semiconductors, evolved from a combination of existing contactless identification and interconnection technologies. The goal was to establish an international valid transmission standard for the expeditious, uncomplicated exchange of data between two electronic devices.

NFC is used to exchange many types of data, such as:

- Mobile
- Images
- Media files
- Digital verification

Information is shared between the two NFC-enabled devices, such as mobile devices or an NFC-enabled mobile phone and compatible RFID chip card/reader. NFC only works when both the devices are in close proximity to one another. The NFC functionality can be used for the services such as cashless payment, ticketing, etc.

NFC Functionality

Working Mechanism

The NFC protocol works if the two devices are held near each other and the distance between the devices is short. On the communication layer side, NFC is based on RFID protocol (standard wireless connectivity technology) that uses magnetic field induction for exchanging information in close proximity. It provides a seamless medium for the identification protocols that validate secure data transfer. By using it, we can connect electronic devices simply by touching or bringing devices into close proximity.

NFC operates at a frequency range of 13.56 MHz and ISO/IEC 14443, ISO/IEC 15693 and offers a data transmission rate of up to 424 Kbit/sec within a distance of approximately 10 centimetres. This limited range means it is therefore ideally suited for purposeful and safety-related applications.

In NFC communication, one device must have an NFC reader/writer and the other an NFC tag. The tag is essentially an integrated circuit containing data, connected to an antenna that can be read and written by the reader.

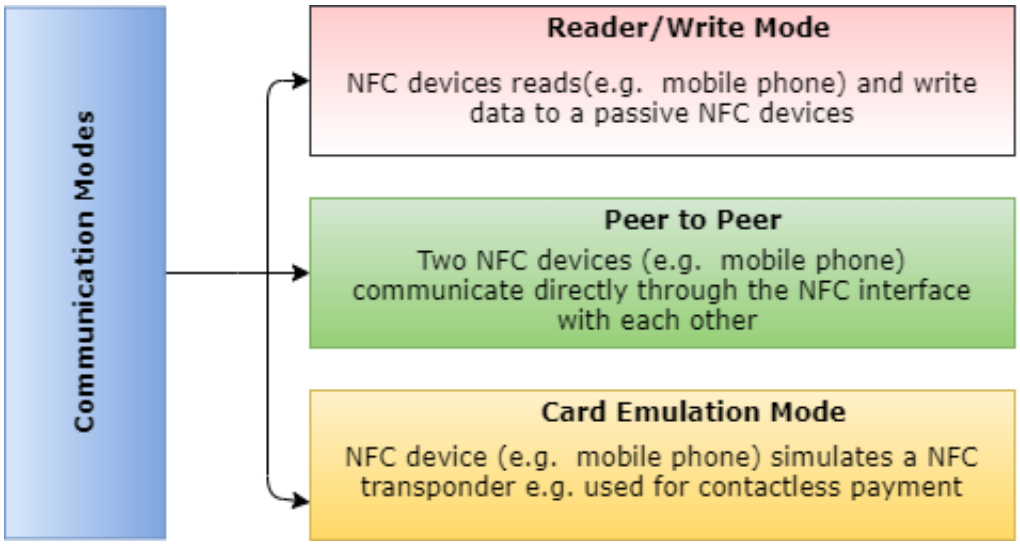
Use Cases

- ✓ NFC is suitable for many applications thanks to its intuitive handling, advanced security standard, and high distribution.
- ✓ Nowadays, many applications using NFC and the feature can easily be used between devices. There is a need to either touch or place the devices close to each other to access the services. Some real-time examples include:
- ✓ Wireless Charging: The latest specification in NFC enables the feature to charge wirelessly at a power transfer rate of up to one watt.

- ✓ User Authentication and Digital Keys for Access Control: NFC can be used to provide access to buildings, unlock offices or apartments, and unlock car doors.
- ✓ Exchange of Digital Data and Information: Between NFC-enabled devices such as smartphones and digital cameras or printers.
- ✓ Exchange Digital Card or Access Other Services: In ticketing, for example, the user can save tickets or event passes on an NFC-based smartphone.

Communication Methods

Different communication methods are used in NFC:



A Proposed Solution for Opening Digital Car Doors & Locks Securely Using NFC

1. Open the Car's Door

As in the above image at left, we can open car doors using NFC. Here, the car's door works as a Reader Emulator, and our phone the Card Emulator. When we move our phone to the car door handle, it makes a connection and sends credentials to the car's device. The car's device (Reader Emulator) will validate that credential and if it is good, will allow it to open the door. Our smartphone works like a key to unlock the car's door.

2. Open Digital Lock

In the same way, we can open digital locks. There are multiple examples where we could apply this solution like:

- Office Doors (Commercial Buildings)
- Apartments (Residential Buildings)
- Hotels
- E-Commerce

Here, the smartphone works as an access card so users do not need to bring their physical access card or keys to open the doors.

3. Smart Elevator

This is a business use case where users could call an elevator and select the destination floor with their smartphone.

Smart Locks: Based on NFC Protocol

Brief Introduction

Smart locks can be based on multiple protocols, as existing current solutions implemented on Bluetooth, Wi-Fi, or NFC-based technology. All three of these are wireless protocols and effectively provide a solution for a smart lock.

As this document mainly focuses on NFC protocol, we will elaborate more in detail about the smart lock based on NFC technology. Near-Field Communication (NFC) is based on RFID protocol, which can be used for exchanging data over short distances. The NFC-enabled devices are connected via a point-to-point contact over a very short distance (0 to 2 centimetres).

NFC-based smart locks have embedded NFC chips, which are a standardized set of rules applied to RFID chips. RFID stands for radio frequency identification, which uses radio waves to communicate identification information between devices.

Smart locks have active NFC chips inside of them and need a source of power. NFC uses such little energy that it is enough to place a couple of batteries there and it will work for months or years at a time.

Smart Lock Solutions (Core Components)

Here, there are two main components — the Card Emulator and Reader Emulator — that play a crucial role in credentials verification. In addition, there is one central server, which provides a way to store and share keys required in the solution, as well as a Gateway which is a communication interface between the Reader Emulator and Central Server.

1. Card Emulator

The Android OS has a Smart Card Emulator that allows the emulation of a smart card that can operate contactless. Here, the emulator uses Android's HCE to fetch APDUs processes from a NFC-based Reader device.

Host Card Emulation (HCE) is the software specification that provides similar virtual data of multiple electronic identities. A Card Emulator creates a secure key <public-private key pair>, which is stored inside the device secure area. This key has the crucial role in the authentication process of a smart lock.

2. Reader Emulator

This is a NFC Reader attached with the smart lock hardware. It is used to read credentials sent by contactless smart cards. It verifies credentials and requests to unlock the lock if the credentials are successfully verified.

3. Central Server

This is a Backend system that stores data (like public keys) required in Smart Lock verification.

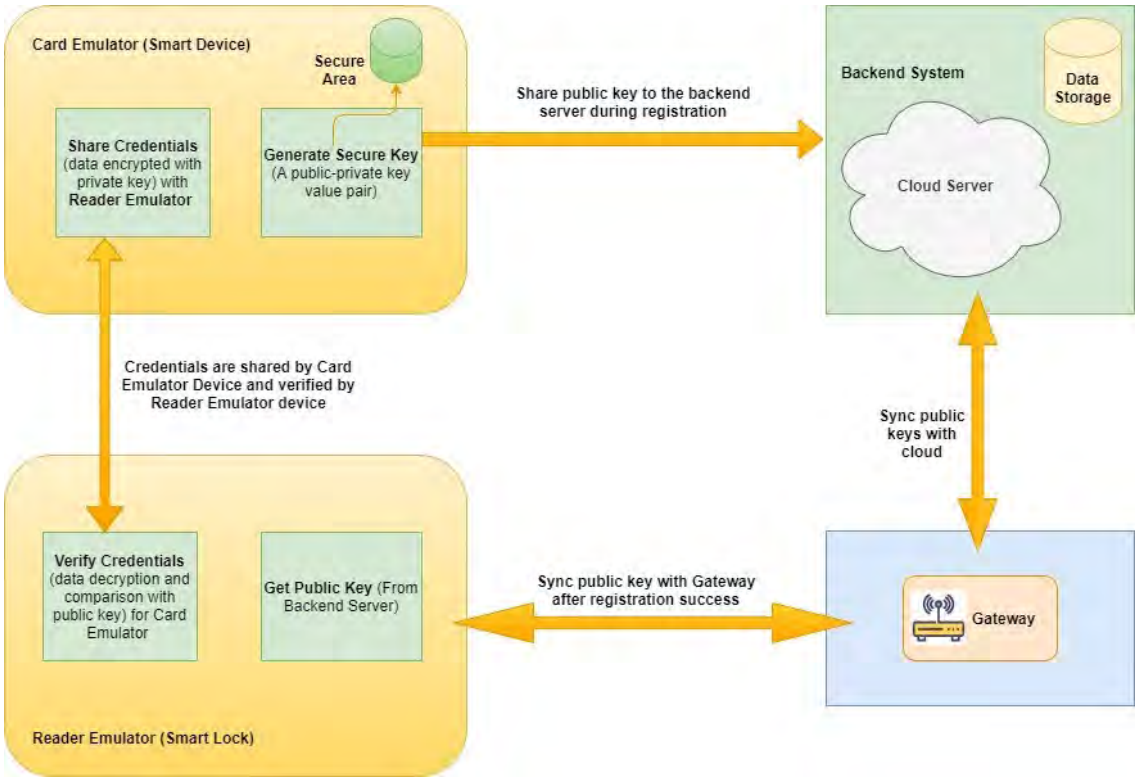
4. Gateway

A Gateway system is a communication interface between the Reader Emulator and the Cloud Server that pulls and keeps updated and registered user's keys public.

Smart Lock (High Level Solution Diagram)

The diagram below depicts the NFC-based smart lock solution at a high level:

At a glance, the Card Emulator (Smart Phone) generates a **secure public-private key-pair** and sends the public onto the cloud server during the registration process. The Card Emulator stores this key inside the secure area of the device.



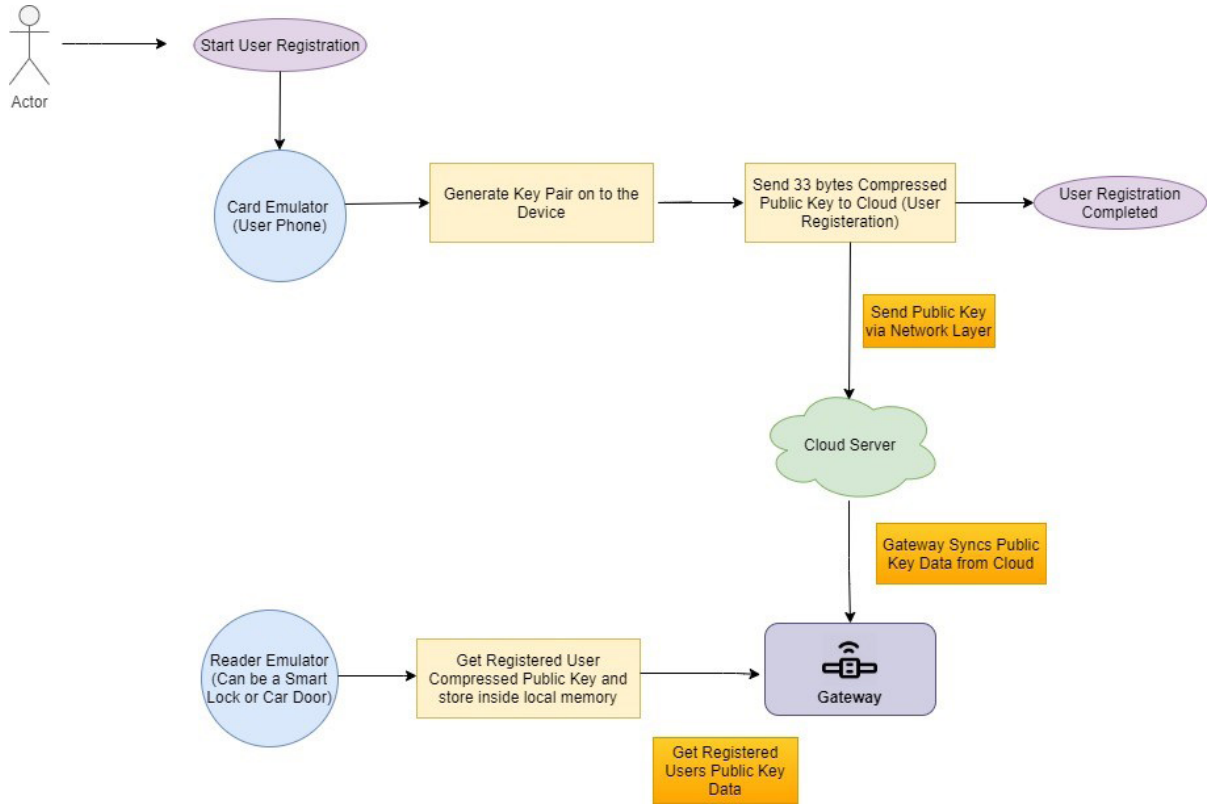
The cloud system stores public keys inside the database and registers the user. The Reader Emulator (Smart Lock) device uses this public key in the credential verification process further.

Once the user registration completes the Cloud System, the Gateway syncs the public key from the Cloud. Finally, the public keys then get pushed by the Gateway onto the Reader Emulator device. After this, the Smart Lock is able to verify the credentials.

Overall, this solution can be divided into two sub-processes.

1. User Registration

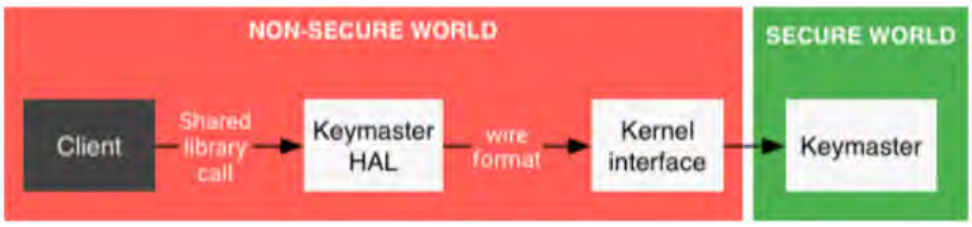
The diagram below depicts the registration process of the Card Emulator.



User Registration is the **setup process** for the creation of contactless cards. In this process, on the Card Emulator device, the application creates a secure key inside the smart device like a mobile, tablet, etc. This secure key is stored inside the chip embedded in the smart device.

The secure key has a public-private key pair where the private key is used for data encryption (Credential Generation) and the public key is used for data decryption (Credentials Verification).

The Card Emulator device stores keys inside the secure area of the device.



2. Communication Protocol (Between Card Emulator and Reader Emulator)

In smart lock solutions, a smart lock is a device which acts as a Reader Emulator whereas a smartphone acts as a Smart Card Emulator (Tag). The communication between the Card and Reader Emulator uses a standard communications protocol defined by ISO7816 for smart cards (contact and contactless).

The ISO7816 defines the standard mechanism based on the exchange of Application Protocol Data Unit (APDU) messages. In general, communication between the Card and Reader Emulator occurs with the exchange of APDU packets.

In order to communicate with the card, the reader first initiates a SEND "APDU Command" to communicate with the Card Emulator, and the Card Emulator sends an "APDU Response" in the result.

Below is a basic structure and example of an APDU command:

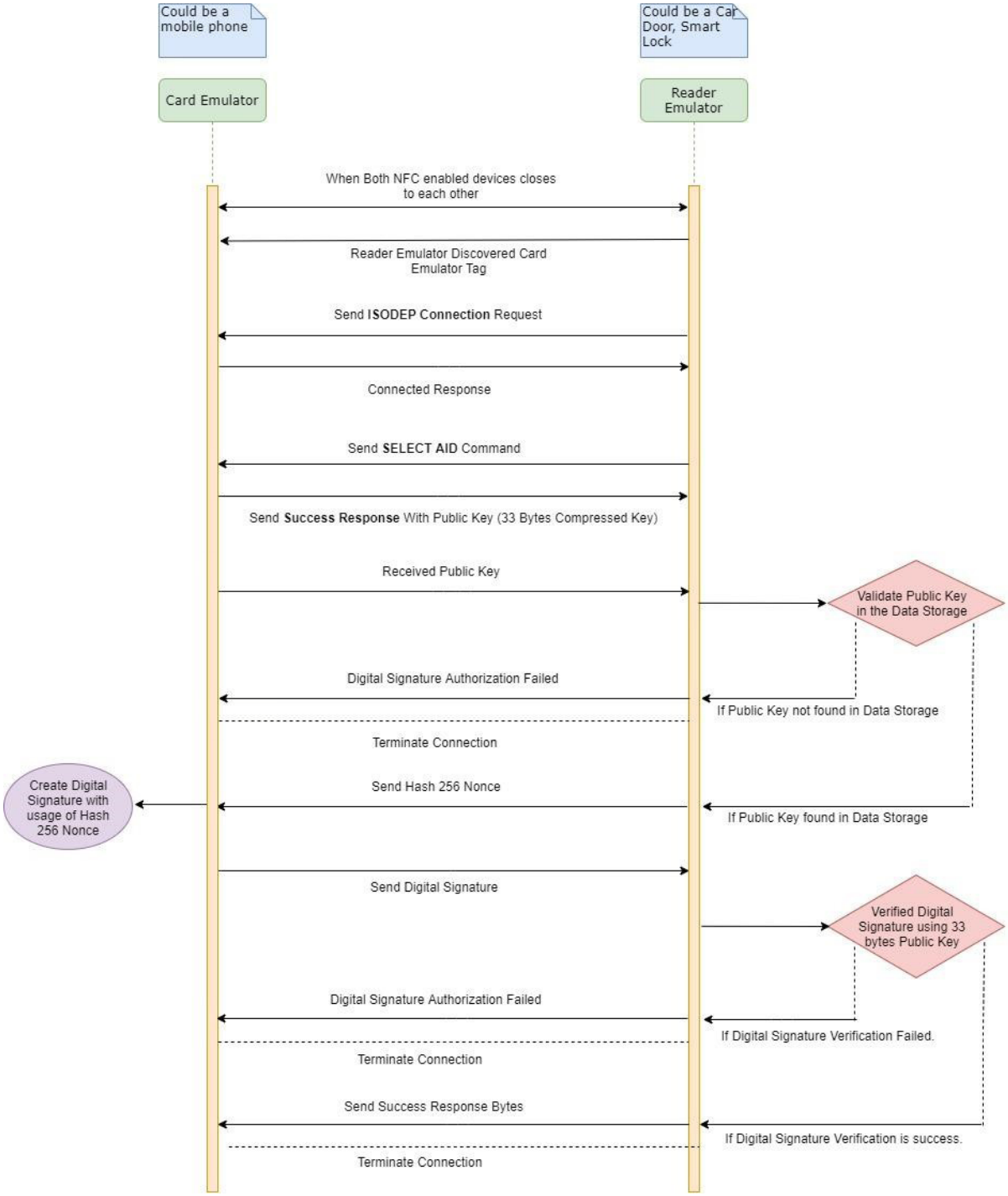
APDU						
Header				Body		
CLA	INS	P1	P2	Lc	Data	Le

Once the card receives the command, it will respond with an APDU response as follow:

APDU Response		
Body	Trailer	
Data Field	SW1	SW2

Sequence Diagram

The diagram below shows the sequence between the communication of a Card Emulator and a Reader Emulator.



NFC Limitations

For all its innovation and inherent benefits, NFC locks do have drawbacks. The main limitation is that NFC chips are not as widespread as Bluetooth chips are. It can only work in shorter distances (about 10-20 centimetres), and supports low data transfer (106 or 212 or 424 Kbps). In addition, power consumption is comparatively higher in NFC-enabled devices

Summary

To summarize, we could say that NFC is an immersive technology that is triggered by a simple tap and that it is easy to implement. NFC transactions are very secure and operate within a fraction of a second. Also, there are no additional steps required for starting NFC communication.

In NFC communication, generally only one device requires power (it does not apply for peer-to-peer mode). NFC works on the proximity of very short-range distances.

The NFC software stack is fully integrated into Android and iOS mobile operating systems. NFC provides a number of services that can be used to fulfill a lot of real-time business requirements. NFC technology will change the world in the coming days and will be used widely in firmware upgrades, wireless charging, Smart Driving (Car Access, Engine start, Tethering, etc.), contactless payment, and access controls solutions.

About the Authors

Ritesh Dubey has 10+ years of extensive experience in Xamarin, .NET, C#, ADO.NET, XML, MVC, WCF (API),WPF, WF, LINQ, Typescript, ES6, Angular, React/Redux, NCache, Nhibernate etc. He has working experience on AZURE and Microservices, and presenting the conceptualized system to higher management and business users. Ritesh is skills in database optimization in decentralized databases, Oracle and SQL Server, and in spearheading knowledge transfer to the team responsible for designing, developing, and testing the system.

Vikas Khunteta is a Software Consultant with vast experience on the mobility platform and delivering solutions on multiple technologies. He is enthusiastic about working on innovations and research that put his strong technical skills and ideas to work.

GlobalLogic®

GlobalLogic, a Hitachi Group Company, is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating our strategic design, complex engineering, and vertical industry expertise with Hitachi's Operating Technology and Information Technology capabilities, we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the automotive, communications, financial services, healthcare & life sciences, media and entertainment, manufacturing, semiconductor, and technology industries.



www.globallogic.com