NFC Functions and Security Certification overview

Approved Version 1.0

3rd April 2018

GSMA response to the request from European Central Bank, Euro Retail Payments Board (ERPB/2015/rec15)

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

This document provides an overview functional and security related certification processes relevant for NFC enabled Mobile Devices. The document focuses on a number of NFC services and identifies the key components within an NFC Mobile Device which are essential for providing the services and are in scope of certification.

The document is aiming to answer a GSMA assigned action by the European Central Bank, Euro Retail Payments Board (ERPB/2015/rec15):

> *"an overview paper on the functional and security evaluation/certification of NFC-enabled mobile devices (covering all aspects and configurations – SE, HCE, trusted execution environment (TEE), etc.) in cooperation with GlobalPlatform and EMVCo. In particular, issues related to contactless interference issues should be addressed."*

1.1 Scope

This document provides an overview certification process for an NFC enabled Mobile Device, it gives guidance for the functional and security evaluations required by NFC enabled Mobile Devices, and provides an overview of the handset architecture with each components certification requirement. This document only describes NFC technology communicating at 13.56 MHz carrier frequency.

The scope of services discussed in this document is limited to NFC payment services, NFC Ticketing services within the transport industry and NFC Digital ID services which today are the most common used NFC services. There are a broad range of propriety services for specific use cases, like access to building and hotel rooms, NFC Tag services and more which have not been included in this document.

1.2 Abbreviations

Term	Description
APDU	Application Protocol Data Unit
API	Application Programming Interface
CAST	Compliance Assessment & Security Testing
CAT	Card Application Toolkit
CEE	Card Emulation Environment
CMP	Contactless Mobile Payment
DSS	Data Security Standard
EMV	Europay, MasterCard, VISA
eID	Electronic ID
eSE	Embedded Secure Element
HCE	Host Card Emulation
HCI	Host Controller Interface
HW	Hardware
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization

Term	Description
LLCP	Logical Link Control Protocol
MMPPA	MasterCard Mobile Payment Partner Application
NFC	Near Field Communication
NFCEE	Near Field Communication Execution Environment
OS	Operating System
OTA	Over the Air
PCI	Payment Card Industry
PoS	Point of Sale
PPSE	Proximity Payment System Environment
REE	Rich Execution Environment
RF	Radio Frequency
RFID	Radio Frequency Identification
SE	Secure Element
SNEP	Simple (NFC Data Exchange Format) NDEF Exchange Protocol
SP	Service Provider
SSC	Security Standards Council
SWP	Single Wire Protocol
TA	Trusted Applications
TEE	Trusted Execution Environment
TSM	Trusted Service Manager
TSP	Trusted Service Provider
UI	User Interface
UICC	Universal Integrated Circuit Card
VCSP	Visa Chip Security Program
VMPA	Visa Mobile Payment Application

1.3 Definition of Terms

Term	Description
Reader	A terminal that reads information from either a card or device.
NFC enabled Mobile Device	In the context of this document, the term NFC enabled Mobile Device is used to represent any electronic equipment supporting the following NFC functionality: Reader/Writer, P2P and Card emulation and that provides a capability for a server to communicate with the device through an Over The Air (OTA) channel.

1.4 References

Term	Description
ISO/IEC Specifications	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards ISO/IEC 7816 Identification cards -- Integrated circuit cards ISO/IEC 18092 Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security
ETSI Specifications	ETSI TS 102 124 Smart Cards; Transport Protocol for UICC based Applications ETSI TS 102 127 Smart Cards; Transport protocol for CAT applications ETSI TS 102 225 Smart Cards; Secured packet structure for UICC based applications ETSI TS 102 226 Remote APDU structure for UICC based applications ETSI TS 102 613 UICC – Contactless Front End (Physical and data link layer characteristic) ETSI TS 102 622 UICC – Contactless Front End, HCI (Host Controller Interface)
3GPP	www.3gpp.org
CEN	www.cen.eu
Common Criteria	www.commoncriteriaportal.org
EU	www.ec.europa.eu
GSMA Specifications	TS.26 - NFC Handset Requirements TS.27 - NFC Handset Test Book
NFC Forum Specifications	Analog Technical Specification; NFC Forum Digital Technical Specification; NFC Forum NFC Controller Interface (NCI) Technical Specification; NFC Forum
EMVCo Specifications	**Specifications and White papers** EMV® Book D: Contactless Communication Protocol PPSE and Application Management for Secure Elements EMV® Mobile Payment: Software-based Mobile Payment Security Requirements Payment Card Management Whitepaper EMV® Level 1 Specifications for Payment Systems – EMV® Contactless Interface Specification **Certifications processes and webcasts** EMV® Mobile Product Level 1 Type Approval – Administrative Process EMV® Mobile Product Level 1 Type Approval – Validation and Interoperability Testing Requirements EMV® Mobile Product Level 1 Type Approval – Level 1 Test Application Requirements EMV® Contactless Mobile Payment Type Approval – Administrative Process EMV® Contactless Mobile Payment Type Approval CMP SE Test Applet Requirements

	EMV® Security Guidelines – EMVCo Product Certification Policy – Technical Requirements Webcast: Mobile Level 1 / Contactless Mobile Payment Approvals Webcast: Wearables Testing
GlobalPlatform Specifications	**SE technology** GlobalPlatform Card Specification Confidential Card Content Management - Amendment A Contactless Services Card Specification - Amendment C Card Contactless API and Export File for Card Specification UICC Configuration Common Implementation Configuration Contactless Extension Configuration **TEE technology** TEE System Architecture TEE Initial Configuration TEE Protection Profile **Mobile device technology** Generic API to access Secure Elements: Open Mobile API Specifications Secure Element Access Control
GCF	www.globalcertificationforum.org
PTCRB	www.ptcrb.com

2 NFC Technology Landscape

2.1 Introduction to NFC

Near Field Communication (NFC) was introduced to make the benefits of secure contactless smart cards available to Mobile Devices and mobile services. NFC supports reliability of service, user-friendliness, highest-level security protocols and high data throughput which makes it the ideal choice for mobile applications with medium or high security and privacy-protection demands.

NFC devices will only communicate at proximity distances typically between 0-4 cm which means that a dedicated action by the user, the so-called tapping is required. The term “Near field communication” indicates this fundamental privacy feature and differentiates NFC from other contactless technologies, e.g. RFID which is designed for vicinity-distances up to several meters, these also provide only low-level security and are typically used for automated identification or tracking of goods.

There are a large number of existing applications and services using contactless proximity smart card technology, which include payment, ticketing, identification and access control. NFC Mobile Devices offer new options in content distribution, smart advertising, money transfer and value-added services such as loyalty and gift services.

It is a major goal of NFC to provide interoperability with relevant infrastructures in order to support a seamless enhancement of existing applications by mobile services. This requires in the first place, that the NFC-interface of the Mobile Device can communicate reliably with the existing contactless readers and cards.

Secondly, it requires that the Mobile Device can process and store sensitive data with the same security level as the secure smart cards which are used for these applications. This is typically achieved by chips with Secure Elements which are directly connected to the NFC interface of the Mobile Device. The Secure Element protects the sensitive data from threats and attacks which may be launched e.g. via the Mobile Device’s online connection.

Consequently, the considerations on certification have to include not only the NFC interface but the architecture of the Mobile Device including the Secure Elements.[1]

2.2 Challenges for interoperability and certification

The globally relevant application infrastructures for Payment, Fare Management, and eID are following different contactless standards:

1. ISO/IEC 14443 is globally used for transport fare management, electronic ID, passports, access control etc.
2. ISO/IEC 18092[1] has a strong position in the Asian transport fare management, payment and ID solutions.
3. EMVCo contactless is globally used for payment and has some deployments in transport fare management.

[1] The ISO/IEC 18092 passive communication mode with 212/424 Kbit/s transmission speed is defined as NFC-F technology in the NFC Forum specifications. The technology is also specified in the Japan Industry Standard JIS X 6319-4.

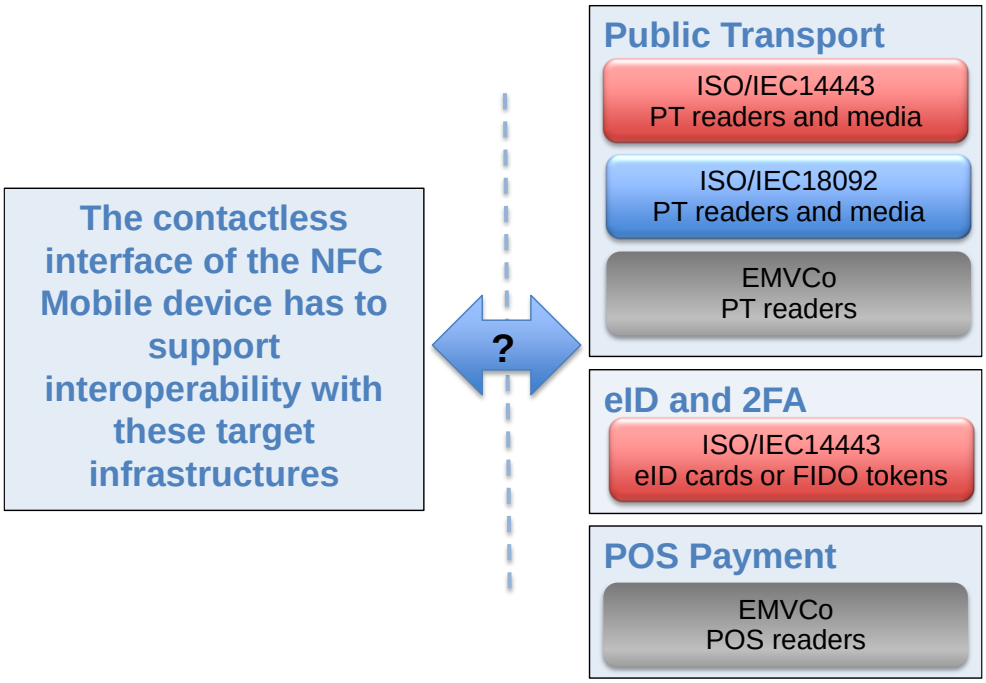


Figure 1 Interoperability scenarios required for a NFC Mobile Device

All these standards share the same technical foundation but in certain scenarios, interoperability between the standards is not provided e.g.

- ISO/IEC18092 is not interoperable with ISO/IEC14443 and EMVCo.
- ISO/IEC 14443 and EMVCo are close but there are some differences that could cause contactless interference issues.

Additionally, the conformance testing of ISO/IEC 14443 and EMVCo is implemented by fundamentally different concepts and therefore it cannot be ensured an EMVCo certified reader device for payment or transport will also pass ISO/IEC14443 certification or vice versa.

In practice, a contactless reader which shall interact with NFC Forum and EMVCo-conformant Mobile NFC devices has to pass both certifications. This is a major technical and commercial obstacle for e.g. Public Transport readers.

2.3 Interoperability solutions

The NFC Mobile Devices are typically designed to be compliant with NFC Forum specifications for a global market and expected to support the relevant global existing contactless applications. Therefore, NFC Mobile Devices have to provide interoperability with the contactless specifications listed in chapter 2.2. For this purpose the NFC Forum worked already together with EMVCo to align the Digital Technical Specification 1.1 with the EMVCo specifications.

In the past, the interoperability of the analogue interface layer was not guaranteed between NFC Mobile Device and the readers used e.g. in the transport sector. Pilot implementations in Public Transport and eID demonstrated the need for a dedicated effort to establish interoperability between NFC Mobile Devices and the three contactless standards from ISO/IEC 14443, ISO/IEC 18092 and EMVCo.

In order to accomplish the interoperability goal, a joint working group was founded between GSMA, NFC Forum, CEN and stakeholders from the public transport sector. The main target by the Public Transport stakeholders was to ensure the existing ISO conformant infrastructures can be re-used without changes. It was therefore expected the necessary adaptations were implemented on the interface of the NFC Mobile Devices within the NFC Forum specifications.

The NFC Forum worked with ISO and CEN to harmonize the NFC Forum specification for the NFC interface with the ISO/IEC14443 standard for contactless readers and cards. This harmonization work took more than 2 years and was finalized in summer 2016 with the release of NFC Forum Analog Technical Specification version 2.0.

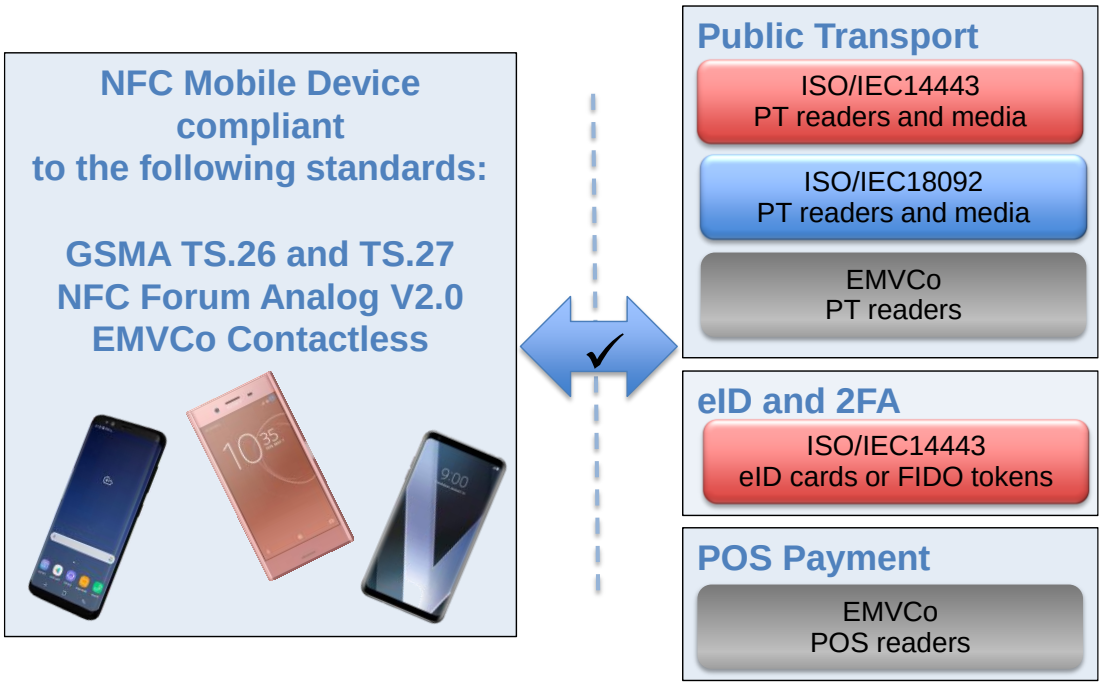


Figure 2: Interoperability provided by a NFC Mobile Device

The updated NFC Forum Analog Technical Specification was introduced in the GSMA specifications TS.26 NFC Handset Requirements and TS.27 NFC Handset Test Book and the testing was adopted by device certifications schemes GCF and PTCRB. GCF and PTCRB are membership driven telecom industry certification schemes, open for all industry players and with balanced influence on processes and certification criteria based on publically available Test Specifications. From June 2017 all certified devices supporting UICC based NFC are considered to support the interoperability with readers and cards compliant with ISO/IEC14443 and ISO/IEC18092. EMVCo provides their own specifications for the contactless interface of NFC Mobile Device which are developed in parallel with the NFC Forum specifications and both specify the NFC analog interface and related card emulation. Only NFC Forum supports reading of cards and Tags by the NFC Mobile Device.

EMVCo provide their own certification scheme based on own specifications which are not publicly available. NFC Forum and EMVCo worked together to ensure coexistence of their respective contactless specifications. This means a NFC Mobile Device currently requires

certifications within both GCF/NFC Forum and EMVCo. Mobile device manufacturers and their customers consider this a duplication of effort and are asking for harmonization of the test methods for NFC Forum and EMVCo test and certification.

3 NFC Enabled Mobile Devices

An NFC enabled Mobile Device is typically composed of various NFC components such as the NFC Controller, Secure Element Environment and various Software related components. This chapter describes an example architecture illustrating the essential components and its functionality within an NFC Mobile Device and the components are later referenced in relation to certification of a NFC Mobile device.

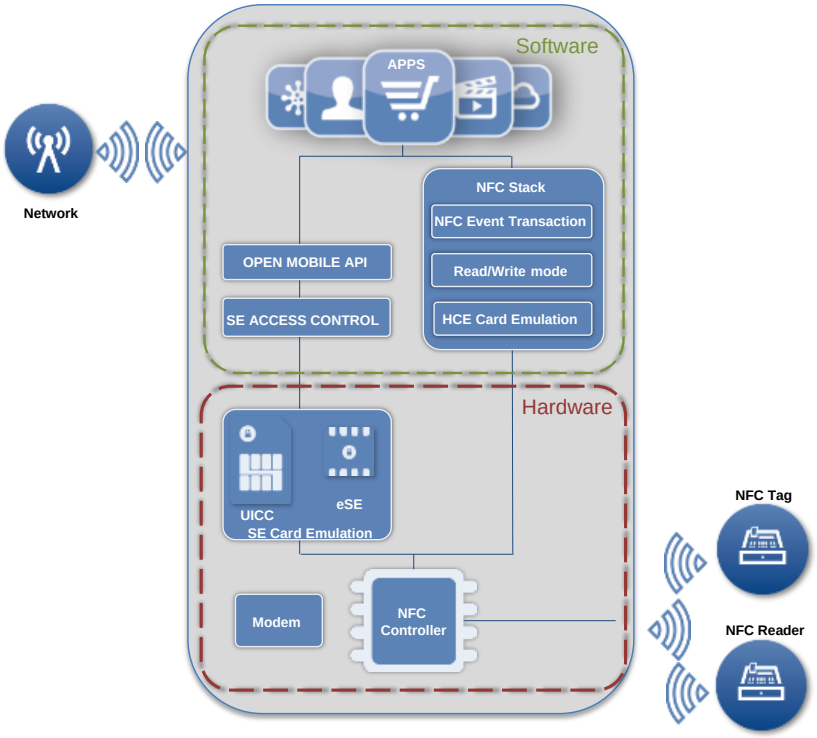


Figure 3: Example architecture for a NFC enabled Mobile Device with Secure Element NFC services

The Software NFC Stack provides the general functionalities towards the NFC Controller and the user interface and user applications installed on the device. The user application can only access the Secure Element Execution Environments via Open Mobile API and with strictly defined access rules.

The SE Card Emulation environments contains traditionally two Secure Elements either integrated in the UICC or as a standalone Secure Element. The SE provides a dynamic and secure execution environment for programs and data and more than one Secure Execution environment can communicate with the NFC controller.

The analog NFC interface is provided by the NFC controller and the NFC antenna.

3.1 NFC Device components

3.1.1 NFC controller

The NFC Controller handles the physical transmission of data over the RF interface and antenna, and it manages the protocol and data communication. The NFC controller enables the NFC link in the Mobile Device – it includes the modulator and demodulator for the RF

signal seen by the antenna. The NFC Controller is connected directly to the NFC software Stack of the device. The logical communication interface between the NFC Controller and the NFC software Stack is implemented in accordance to the NFC Forum NFC Controller Interface NCI) Technical Specification.

In addition the NFC Controller contains interfaces to Secure Elements (SE) and in case of a Secure Element integrated of an UICC, the communications protocol is the Single Wire Protocol (SWP) standardized by ETSI. Communication protocols between NFC Controller and other Secure Element may be device manufacturer proprietary protocols.

3.1.2 NFC Software Stack

The NFC software stack is the main application process of the handset and is part of the main software and the device operating system (OS).

The NCI interface allows the NFC Controller to communicate directly with the NFC Software Stack. NCI is standardised in NFC Controller Interface (NCI) Technical Specification from the NFC Forum.

3.1.3 Secure element

There are two different form factors of SE: Universal Integrated Circuit Card (UICC) and, the embedded SE. The UICC is traditionally removable whereas the eSE is embedded in the NFC Mobile Device. In addition to the UICC, the eUICC which provide remote SIM provisioning can be either removable or embedded in a NFC Mobile Device. Each form factor links to a different business implementation and satisfies a different market need.

A Secure Element is a tamper proof platform providing a secure storage and execution environment for sensitive data and programs (e.g. payment application). It offers both physical and logical protection against attacks, ensuring integrity and confidentiality of its content.

Secure elements are typically certified to meet dedicated evaluation assurance levels as defined by Common Criteria and/or EMVCo.

A Secure Element is typically certified with CC EAL4+ or higher.

3.1.4 Trusted Execution Environment

A Trusted Execution Environment (TEE) provides a way to enhance security of a Mobile Device by providing an isolated execution environment for sensitive operations separated from the main operating system. Its uses a multi layered approach and relies on root of trust for boot; storage, provides cryptographic functionalities, allows for the secure storage of data and keys, and executes Trusted Applications (TA) in a controlled environment separate from the mobile OS.

A TEE is designed to resist software-based attacks, but does not offer the tamper resistance of a Secure Element.

TEE is typically certified up to CC EAL2+.

3.1.5 HCE

Host Card Emulation (HCE) is a technology introduced to the market in order to enable the possibility to emulate a card directly from the device operating system without using any secure element.

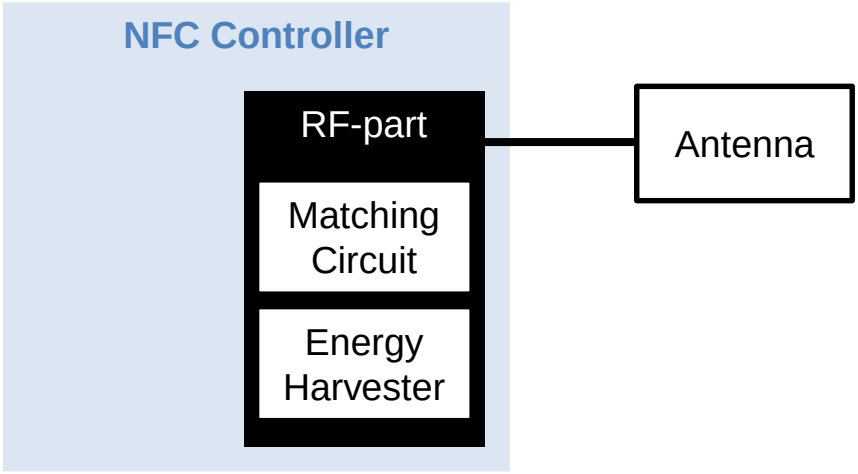
The security of the HCE implementation on the device is bound to the security of the operating system running on the device.

3.2 NFC Device interfaces

3.2.1 NFC Front end

In contrast with most wireless communication mechanisms, NFC is based on electromagnetic induction – coupling between a pair of NFC-enabled devices is electrically akin to an air-coupled transformer. It is this use of magnetic coupling that gives NFC systems their predictable short range and ability to transfer electrical power from one device to another – allowing for devices such as tags that operate without a power source of their own

As a consequence, the NFC front-end differs somewhat from a typical RF communication system. The diagram below shows some of the distinctive aspects.



The NFC Antenna is usually a simple loop design printed on a flexible PCB. To enhance the efficiency of the magnetic circuit, it is often mounted on material that concentrates the magnetic field such as the device battery or a piece of ferrite.

For optimum performance, the antenna would be as large as the dimensions of the device would allow thus improving the strength of magnetic coupling with other devices. Device packaging decisions (e.g. use of metal cases) and cost considerations often lead to selection of smaller antenna designs than would be ideal, which can lead to interoperability challenges with legacy infrastructure. The Matching Circuit is designed to tune the performance of the system to an optimum centre frequency. The Antenna and Matching Circuit form a very high-Q filter, so effective signal transmission occurs with high efficiency, but only when the communicating devices are tuned to operate at very close to the same frequency. This tuning can be another cause of interoperability challenges.

The Energy Harvester is an optional component within the NFC Controller. It allows the NFC Controller to recover sufficient energy from the field induced in the antenna when it is acting

as a receiving device to power both the NFC Controller and an attached Secure Element. Operation in this manner is described as "Battery Power-off mode" operation.

3.2.2 Secure Element access

3.2.2.1 SWP

The SWP interface is a physical transport and data link layer supporting full-duplex serial data transfer between a Master, the NFC Controller in an NFC system; and a Slave, the Secure Element.

A distinctive feature of the SWP interface is that is can supply power from the NFC Controller to the Secure Element. This enables use-cases in which an NFC-capable device can continue to offer services when the battery power of the device is depleted.

The SWP interface is defined in ETSI TS 102 613.

3.2.2.2 HCI

HCI specifies the logical communication interface between the NFC Controller and a Secure Element.

An HCI network consists of a number of Hosts which are physically connected in a star topology to a Host Controller which is responsible for message routing.

HCI defines mechanisms to allow Hosts including the Host Controller to discover the services, or "Gates" in HCI terminology, offered on the network. A Host wishing to make use of a service provided by a Gate on a remote Host creates a Pipe - a logical channel between one of its Gates and a Gate on the remote Host.

The HCI specification defines procedures for establishment of Pipes between Gates, service discovery and a set of standard services including services especially relevant to NFC use-cases.

In an NFC-capable device, the NFC Controller has the role of Host Controller in the HCI network and Secure Elements are Hosts. The transport layer used to support the HCI network is SWP.

HCI is defined in ETSI TS 102 622.

3.2.2.3 Secure Element Access Control

Secure Element Access Control provides a mechanism which allows the Issuer of a Secure Element to control which applications running in the REE or TEE have access to the services provided by applets resident on the Secure Element.

There are two main components to Secure Element Access Control: an Access Control Enforcer and a set of access rule definitions.

The Access Control Enforcer is a piece of software running in the REE and/or TEE which is able to determine information about the identity of an application wishing to access the Secure Element, and then to check with the access rule definitions in the Secure Element before allowing or denying access based on that identity.

There are two forms of access rule definitions that may be used, and the Access Control Enforcer should support both. The ARF, which is a legacy format only deployed on UICCs, represents access rules in a file structure. The ARA is an application to perform the access determination, and can be deployed on all type of Secure Elements.

The security provided by the Secure Element Access Control mechanisms is limited by the security of the platform on which the Access Control Enforcer executes. As such, it is of limited benefit in protecting the Secure Element applets if the device has been rooted.

Secure Element Access Control is defined in GlobalPlatform Secure Element Access Control Version 1.1 (GPD_SPE_013).

3.2.2.4 Open Mobile API

The Open Mobile API provides a standard set of APIs which enable applications running in an REE or TEE to access applets running a Secure Element. It provides mechanisms allowing applications to discover the available Secure Elements on the device, and to establish communication with applets hosted by them.

Communication between applications and applets is supported by Channels, a concept defined in ISO7816-4. Most Secure Elements support only a limited number of Channels, and the Open Mobile API ensures that management of this limited resource by applications is not necessary.

The Open Mobile API uses the Secure Element Access Control mechanism to ensure that applications wishing to communicate with applets are authorised to do so.

The Open Mobile API is defined in GlobalPlatform Open Mobile API Specification (GPD_SPE_075).

3.2.3 NFC Controller/NFC stack

Management of the NFC Services provided by an NFC-enabled device is split between firmware running in the NFC Controller and software running on the device REE which is known collectively as the "NFC Stack".

The NFC Stack manages the NFC operating modes, which represent the roles that an NFC-enabled device can play in a contactless transaction. These are:

- Reader/Writer: in this mode the device can read from, or write data to, a Tag. A typical use case might be to tap on a "Smart Poster" that automatically takes the user to a website. This is similar to QR code usage, but with a much enhanced user experience.
- Card Emulation: in this mode the device emulates the operation of a Smartcard – usually one conforming to the ISO7816-4 specification. The Card Emulation is performed either by an applet in the Secure Element or by an application running on the REE (this is often called Host Card Emulation). A typical use case would be mobile payment or transit ticketing.
- Peer to Peer: in this mode the device and its peer are able to discover services running on both sides of the link, and to interact with those services. A typical use of peer to peer operation is to share photos or videos with another device by setting up a fast link (e.g. Bluetooth) and transferring the data.

The NFC Stack provides services and APIs that allow NFC-enabled applications to configure the operation of the NFC Controller and to register to receive notification of NFC events.

The NFC Stack manages a routing table that determines which application is notified when interaction with other contactless systems takes place – this application may execute on the REE or may be an applet in a Secure Element. Where applications are running on the REE, the NFC Stack generates notifications which will cause the correct application to run and react appropriately. Different events are indicated during reader/writer, Card Emulation or peer to peer operations.

The NFC Stack communicates with the NFC Controller using NCI. The NCI specification describes a protocol and management principles allowing the NFC Stack to manage the NFC Controller: configuring, reading and writing data and receiving notifications.

NCI is specified by the NFC Forum as the NFC Controller Interface.

3.2.4 Service Management on Secure Element

Service management platform or TSM may use any of the following channels:

- BIP/CAT_TP (or SMS as backup): referenced by SCP 80 (as defined in GlobalPlatform Card Specification) based on ETSI TS 102 225
- Remote Application Management over HTTP(S) (as defined in GlobalPlatform Card Specification Amendment B) when the SE provides OTA

Remote Application Management over HTTP(S) (as defined in Secure Element Remote Application Management Specification) where an Admin Agent in the device implements the OTA connectivity

4 Specification and Standardisation Organisations for NFC Systems

An interoperable set of standards is essential for a successful NFC ecosystem. This section provides information about the relevant standardisation and industry organizations.

4.1 Non-Profit Organisation

4.1.1 3GPP

3GPP (the 3rd Generation Partnership Project) unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners” and produce technical Reports and Specifications that define 3GPP technologies.

The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security and quality of service - and thus provides complete system specifications. Implementation of Mobile Devices used for mobile payment follows 3GPP specifications.

4.1.2 CEN TC278 WG3 SG5 “Interoperable Fare Management Systems”

This sub group of the European Standards Body CEN generates standards for Transport Fare Management Systems.

CEN TS16794:2017 provides guidance for the implementation of ISO/IEC14443-conformant Public Transport readers and fare media and a test specification that can be used for testing and conformance certification. CEN TS16794:2017 is synchronized with NFC Forum’s Analog 2.0 Technical Specification for NFC Mobile Devices in order to ensure interoperability between NFC Mobile Devices and Public Transport readers and fare media.

4.1.3 Common Criteria

Common Criteria is working on international standards (ISO/IEC 15408) for IT security certification specifying Security Functional and Assurance Requirements for vendors. It provides a framework for system users so they can specify their security, functional and assurance requirements through the use of Protection Profiles (PPs). System providers can then implement and / or make claims about the security attributes and test laboratories can evaluate the products to determine if the products meet the claim.

Common criteria provides a scalable approach to product security by defining so-called “evaluation assurance levels” (EAL) as described in http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf.

These cover a range from very basic requirements to the development process to a highly structured and supervised approach that includes the application environment and entire life cycle of the “Target of evaluation” (ToE).

4.1.4 ETSI SCP

The European Telecommunications Standards Institute (ETSI) is an independent, standardization organization in the telecommunications industry, whose members are equipment makers and network operators. ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. Within the context of NFC, ETSI SCP provides standards for the communication between secure element and NFC controller, and an applet to access the HCI events.

ETSI publish specification for Single Wire Protocol (SWP) and Host Controller Interface (HCI) which are used by GCF and PTCRB in their device certification criteria.

4.1.5 European Union

The European Union issued two directives which are relevant for the implementation of mobile services in the European payment and eGovernment market. Most important, requirements to security levels of identification and authentication are given which have an influence on the Mobile Device architecture and the SE, security mechanisms and certification levels:

1. The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

   More info can be found on: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid).

2. The Payment Service Directive (EU) 2015/2366 (PSD 2) governs the implementation of payment services in the European market. It includes e.g. high-level requirements to identification and authentication which also have to be fulfilled by NFC Mobile Devices.

4.1.6 GlobalPlatform

GlobalPlatform provides technical specifications which define both Secure Element and TEE as secure components and the way in which data and applications are provisioned, addressed, accessed, delivered and securely stored including contactless card services. GlobalPlatform also publishes several documents relating to the management and provisioning of secure elements on handsets, including the Secure Element Access Control and Open Mobile API specification.

GlobalPlatform publishes test specifications for the Open Mobile API and Secure Element Access Control which are used by GCF and PTCRB in their device certification criteria.

4.1.7 GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.

The TSGNFC group within GSMA publishes the requirements for an NFC handset in the technical specification TS.26, and an NFC Handset Test Book TS.27. These documents reference specifications from many other organisations, including EMVCo, NFC Forum, ETSI SCP, and GlobalPlatform in order to ensure an end to end service deployment. The TS.27 NFC Handset Test Book is used by GCF and PTCRB in their device certification criteria.

4.1.8 ISO/IEC

The IEC and ISO are both independent, non-government, organisations that develop and publish fully consensus based International standards. The IEC prepares and publishes international standards for many electrical, electronic and related technologies. ISO and IEC work together to provide worldwide standards.

The various parts of the ISO/IEC 14443 standard define two physical layers, commonly referred to as Type A and Type B. The ISO/IEC 18092 standard defines also two physical layers by its 106kbps passive mode (which is compatible with Type A) and its 212kbps/424kbps passive mode..

These specifications were used as the starting point for EMVCo and NFC Forum physical layer specifications.

4.1.9 NFC Forum

NFC Forum is an industry association formed to improve the use of NFC short range wireless interaction in consumer electronics, Mobile Devices and PCs. NFC Forum defines technologies including NFC-A, NFC-B, and NFC-F[2], which are derived from the corresponding physical layers. A process of harmonisation has ensured that NFC Forum and EMVCo specifications are aligned.

The set of protocol specifications defines the complete stack for an NFC Forum Device, from the RF interface up to reference applications. This encompasses Reader/Writer, Card Emulation, and Peer to Peer Modes.

4.2 For Profit Organisations

4.2.1 EMVCo

EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions. It accomplishes this by managing and evolving the EMV® Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Today there are EMV® Specifications based on contact chip, contactless chip, EMV® 2nd Generation, Common Payment Application (CPA), card personalisation, Payment Tokenisation, and 3-D Secure."

4.2.2 Payment Systems

Each payment system provides technical requirements and specifications to describe how the technology should work and interact with their network in line with the defined risk / liability for the payment industry (including issuers, acquirers, and processors). In the mobile payment

[2] NFC Forum defines additionally the NFC-V technology compliant to ISO/IEC 15693 which is out of scope for this document.

industry, the payment systems have a prominent role, requiring implementation and certifying solutions.

4.2.3 PCI Security Standards Council

PCI Security Standards Council is a global body which maintains the Payment Card Industry Security Standards for organisations and was set up to help businesses process card payments securely and reduce card fraud. It's intended to protect sensitive cardholder data and provides controls surrounding the storage, transmission and processing of cardholder data and how it is handled.

5 Certification Organisations

This chapter provide an overview of certification organizations which are providing certification services for NFC enabled Mobile Devices with specific testing and certification of the NFC portion of the Mobile Device. Most of the organizations have a broader scope of certification than the NFC technology which then is considered as a feature of the Mobile Device making the corresponding NFC testing applicable.

5.1 GCF and PCTRB

GCF (Global Certification Forum) and PTCRB manages a certification scheme for Mobile Devices which implements the cellular connectivity as defined by 3GPP and 3GPP2. The scope of GCF and PTCRB certifications is primarily to achieve interoperability between Mobile Device and Mobile Network and the schemes have also adopted specific testing of NFC related device components according to GSMA TS.27. Testing is undertaken by authorized laboratories.

Each certification scheme is independent and manages their own certification criteria based on test specifications developed by industry and standardization organizations. GCF and PTCRB currently both reference UICC and eSE based NFC as defined in GSMA TS.26 and TS.27.

5.2 EMVCo

EMVCo manages a contactless certification process for the card and reader functionality from an electrical interface; protocol and interoperability of cards and readers. EMVCo security evaluation of Secure Elements and Software based implementation (including TEE) are requirements for many payment applications. See also section 4.2.

5.3 GlobalPlatform

GlobalPlatform operates a compliance program for Secure Elements and TEE implementations. In addition, GlobalPlatform operates a security certification program for TEE, based on a Protection Profile that it maintains. See also section 4.1.5.

5.4 Payment Systems

All payment related products (like new cards, PoS, mobile payment solutions) require certification before the schemes will accept the liabilities.

5.5 NFC Forum

The NFC Forum certification program consists of compliance, performance, and interoperability testing for three different classes of device: universal, reader, and tag. Compliance testing confirms that a device conforms to NFC Forum Technical Specifications, and is performed at an authorised test laboratory. Performance testing allows the measurement of the volume beyond the minimum operating volume in which a tag can be accessed by a reader. Interoperability testing events called Plugfests are held several times a year in different regions, and provide a safe, real-world environment where device, tag, and test tool interoperability can be verified across manufacturers' products. See also section 4.1.9.

5.6 Common Criteria

Common Criteria for Information Technology Security Evaluation provides a framework for international agreement, mutual interpretation and recognition of methodology and criteria for security evaluation.

Evaluation is performed by independent licensed laboratories to determine the fulfilment of particular security properties or protection profile. See also section 4.1.2

5.7 German federal Office for Information Security (BSI)

The German federal Office for Information Security (BSI) is one of the globally leading bodies for Common Criteria certification and deeply involved in current and planned activities in Common Criteria for chip and mobile security.

Globally, the majority of security chips are certified according to BSI's protection profile BSI-CC-PP-0084-2014. This protection profile is also proposed for GSMA's current draft of the Protection Profile for eUICC.

5.8 Japanese Transport

The Mobile FeliCa Certification program certifies devices for interoperability against deployed FeliCa infrastructure and assures a certain minimum performance of certified Mobile Devices. The test specifications used by the program, like the Mobile FeliCa RF Performance Certification Specification, are publicly available at http://www.felicatech.org/en/.

East Japan Railway (also known as JR East), the public transport operator responsible for the contactless fare application 'Suica', requires Mobile FeliCa Certification for devices used in their infrastructure. In addition, JR East requires an application level certification program to ensure that their Mobile Suica application runs properly on a Mobile Device. Only Mobile Devices that have passed both certifications are allowed to offer the Mobile Suica service.

6 Overview of Certification Requirements for NFC Enabled Mobile Devices

This section provides the overview of functional and security certification processes existing for NFC Mobile Devices with reference to the essential NFC components as described in section 3.1

6.1 Certification summary

Certification of NFC Mobile Devices with secure NFC services is essential on a global marked to ensure interoperability with global standards and with minimal fragmentation. NFC enabled Mobile devices are certified in different certification organizations and cover most of the NFC components from a NFC Mobile Device.

GCF and PTCRB certification provide the broadest scope of functional certification, this is mandated by mobile operators to support their business and technology need. The main services are currently payment, ticketing and access and the testing scope within GCF and PTCRB covers testing managed by the schemes as well they do also reference specific NFC components tested and certified within EMVCo and NFC Forum. GCF is a self-regulated certification scheme that pursues an open policy of publishing test plans and making test results available for review by operator members.

EMVCo certification provides payment related certification and is mandated by the payment industry to allow a NFC Mobile device to support payment services using the international payment systems. EMVCo testing is run on behalf of the Payment industry by the Payment industry and uses a closed ‘black box’ test certification environment, where test plans and test results are not made public.

In the current situation the functional certification of NFC Mobile Devices is considered to be well covered in the functional area and certification is mainly mandated by the mobile operators and the payment industry. In the current situation, the security related certifications have a smaller scope and usage than the functional.

Within the wider usage of secure NFC mobile services it is anticipated that the vertical industries like transport, automotive, security, health care, government, etc. in future will have an increased need for certification of secure NFC services.

6.2 Certification overview

NFC Mobile Devices contain several NFC related components and interfaces as described in chapter 0 which are tested by different certification organizations. Some of the components are certified within more than one certification organizations and in most of the cases where the same specification is basis for the testing, the testing and certification are mutually recognized between the different organizations.

The functional and security related certifications referenced below are considered as voluntary certifications for product manufacturer to complete based on business and commercial need - traditionally certifications are part of bi-lateral agreement on business-to-business need. None of the certifications are generally required by regulation or promoted or visible as an end-user requested certification. However some organizations have a prerequisite that

certifications from other organizations are completed. The business-to-business need or demand of certification can on general level be summarized as follows:

- *Common Criteria* - in the context of this document, certification relates to the HW and SW of the eSE (Secure Element) or the UICC embedded in the device or provided by mobile operators. Certification is currently mainly required by mobile operators and payment systems.
- *GCF and PTCRB* certifications - required by mobile operators for devices sold through operator channels. For devices sold on the open market, usually it is manufacturers' business choice to certify the device. The demand to certify depends on the mobile operator's or service provider's technology need to deploy secure NFC services.
- *GlobalPlatform* certifications – manufacturer's business choice to certify their products and demonstrate compliance to its specifications.
- *EMVCo* certification - required by international payment systems and most of the regional ones.

Each of the NFC components is certified in the certification organization as illustrated in table below:

	NFC Components/ interfaces	Common Criteria	GCF	PTCRB	GlobalPlatform	EMVCo	NFC Forum	Payment Systems	Transport Systems
Device	NFC Controller		X			X	X		
	NFC Analog layers (frontend)		X	X		X	X		
	NFC Protocol layers		X			X	X		
	UI interaction		X	X		X			
	Access control for TEE				X				
	Access control for UICC and SE		X	X	X				
	Service Management on Secure Element		X	X					
CEE	Coexistence of Multiple Card Emulation Environments (CEE)		X	X		X			
	TEE				X	X			
	SE/UICC	X				X			
	HCE					X			
	Payment applets							X	
	Transport applets								X

Figure 4 Overview of functional and security related certification of NFC components and interfaces.

The key points to notice are the coverage of NFC component which is most comprehensive is within GCF and PTCRB certifications and secondly some of the NFC components are certified in multiple certification organizations. In most of the multiple cases there is a mutual recognition of the testing between the involved organizations however there are cases where testing is required to be performed in multiple organizations due to variations in the specification as explained further below.

NFC Controller - tested and certified in NFC Forum and referenced in GCF certification. GCF recognizes the testing in NFC Forum and no extra testing effort required in GCF.

NFC Analog layers - tested and certified within GCF, PTCRB and NFC Forum based on the same specification. The testing is e.g. mutually recognized between GCF and NFC Forum meaning the device manufacturer only has to perform the testing once and use the results within each of the certification schemes. The NFC Analog layers are also certified within EMVCo but based on a different specification than NFC Forum Technical Specification. There are some overlaps between the specifications but the testing methods are different and therefore two-sided effort is required by the device manufacturers.

NFC Protocol layers – the specifications and testing within NFC Forum and EMVCo is different with two-sided effort required by device manufacturers – however technical alignment between the specifications are ensured by EMVCo and NFC Forum.

Access control for UICC and SE – certifications in GCF and PTCRB are based on GlobalPlatform specifications and the testing in GCF and PTCRB is a subset of the certification within GlobalPlatform.

The main demand for certification of NFC Mobile Devices currently originates from the mobile operators, mobile service providers and the payment industry and the certifications are provided by GCF and PTCRB towards the mobile industry and by EMVCo towards the payment industry. To some extent there are aligned global specifications available, however for the a NFC Mobile Device which shall support both the NFC Forum and the EMVCo analog interface, the device has to implement and pass certification for both EMVCo and GCF/PTCRB. This is considered as duplicated effort by device manufactures however with the current harmonization there are no fundamental conflicts impacting the implementations.

There are other use cases like secure eID, virtual Car Key or access control which could benefit of global specifications and certifications of the secure NFC technology. Secure eID services to access governmental services according to EU eIDAS Directive can be implemented using the secure element based NFC which already is available on NFC Mobile Devices. For the eIDAS conformant identification, it has to be mentioned that security certification is required for the higher assurance levels. However for lower assurance levels which are sufficient for access control and employee ID provided for private companies, it is a natural choice to provide a user convenient service on an NFC enabled device which is already in the hands of the user. Some car manufacturers through groups such as the Car Connectivity Consortium are looking to store digital car key in a mobile phone and use the NFC interface to open and start an end user's vehicle.

In order to ensure interoperability across the industry between NFC Mobile Devices and other infrastructures supporting existing and new use cases in a global market, it is anticipated a vertical industry to the mobile, like automotive, transport, security, and governments would have interest in certifications of secure NFC services.

7 Summary and Recommendations

The successful implementation of an open ecosystem for NFC mobile services requires some fundamental prerequisites for its technical infrastructure:

1. To ensure non-discriminatory access to the ecosystem for service and technology providers, all relevant functions and interfaces must be specified by open standards and specifications.

2. Technical interoperability between all devices has to be guaranteed. This requires harmonization of the relevant specifications for all involved devices as well as in the implementation of respective testing and certification schemes.

3. To support services that require a specific security level, a consistent and scalable approach to security (e.g. by defining assurance levels) must be defined for hardware and software of the devices and communications protocols.

NFC Mobile devices are marketed globally and intended to serve all relevant NFC applications and mobile services globally - either as a media or as a reader – it is not enough they are designed for a particular NFC application like payment or transport. Therefore, the implementation of the open NFC ecosystem requires that Mobile Devices support technical interoperability with all globally relevant applications and infrastructures.

The fragmentation of contactless specifications, as described in this document, proved to be a blocking point for global interoperability for many years. This obstacle has been addressed by the joint activities between GSMA, NFC Forum and ISO and their cooperation with EMVCo, GlobalPlatform and stakeholders from the Public Transport sector which resulted into the publication of the harmonized Analog and Digital Technical Specifications by NFC Forum, the cross reference by GSMA specifications and implementation by GCF as chapter **Error! Reference source not found.** explains. This cooperation established a framework for aligned global specifications, standards and certification supporting the relevant applications and market sectors.

The joint activities ensure that the existing standards developed by GSMA, NFC Forum on one side, and by EMVCo on the other side, are able to co-exist for NFC Mobile Devices. The joint activities also ensure that certifications schemes can co-exist and cover certification of the essential NFC components from a NFC Mobile Device.

GCF and PTCRB certification schemes provide the broadest scope of functional certification and are mandated by mobile operators to support their business and technology need - currently payment, ticketing and access as the main services. GCF and PTCRB do also refer specific NFC components tested and certified within EMVCo and NFC Forum.

EMVCo certification provides payment related certification and is mandated by the payment industry to allow a NFC Mobile Device to support payment services.

These certifications co-exist and provide a broad coverage in the functional area. However, there is still some duplicated effort in the certification process for mobile manufacturers. There is also a risk that new conflicts may be introduced with changes to the specifications on either side.

Therefore, the work is not fully completed and the maintenance of the specifications, the continuation to harmonize the testing and cross-recognitions of certifications should be the ultimate goal.

This requires GSMA, NFC Forum, EMVCo and other stakeholders to maintain or even extend their partnership and cooperation. Such extended partnership should improve the remaining work in the functional certification and start a process to create common and aligned security certification concepts which can serve relevant target markets and be applied to NFC Mobile Devices.

GSMA feel that the EU can play an important role in ensuring that continued alignment and drive to an open and transparent approach to specifications and certification is maintained and potentially accelerated.

GSMA would welcome discussions with the EU and its relevant bodies to ensure that the interests of the key players, regulators and the public are properly represented and taken into account as part of any certification framework so this delivers benefit that are in the consumer interest.

GSMA believes a harmonized approach across standardisation and certification will help to reduce some of the fragmentation seen in the services implemented within different eco-systems and by different device vendors. GSMA believes it would be a benefit for the consumers ensuring they are able to migrate and port services related to payment, ticketing, identity and access services with ease between devices.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	April 2018	First Approved version	GSMA TG	TSGNFC Group

A.2 Other Information

Type	Description
Document Owner	TSG NFC
Editor / Company	Kay Fritz / Vodafone

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.