
# *Documentation of Use Cases for NFC Mobile Devices in Public Transport*

Version 1.7.4

*WORKING DOCUMENT*

# Contents

# 1 Introduction

The increasing use of smart phones and the transformation from classical to mobile service offers is one of the major global trends.

Compared to other sectors that have to build up mobile infrastructures from scratch, the Public Transport industry is in a unique position because current contactless eTicketing infrastructures are in principle compatible with NFC-enabled mobile devices. It is possible to introduce mobile services based on these existing infrastructures.

NFC Mobile Devices (NMD) may be used

- as Public Transport PT object (substituting the customer's card or token).
- as personal mobile sales terminals (pPoS) by which the customer may obtain information about services and products, purchase products and make payments.
- for new service offers (e.g. multi-modal travel planning and travelling) that take advantage of a smart phone's capability to integrate and access online-applications.
- NFC tags may be used.
- to provide customers access to traffic, schedule and fare information.
- as an alternative approach to classical reader-based infrastructures.

The mobile enhancement of classical fare management systems requires that NFC Mobile Devices are technically interoperable with the contactless readers and the PT object that are used for ticketing and payment in Public Transport.

## 1.1 Applicable Documents or References

| Document | Short name | Version / date | Issuer |
|---|---|---|---|
| NFC Handset Requirements | [TS.26 ] | Version 9.0, 2016 | GSMA |

## 1.2 Administration

Documentation of Use Cases for NFC Mobile Devices in Public Transport

Smart Ticketing Alliance INPO
c/o UITP, rue Sainte Marie 6
B – 1080 Brussels

Tel.: +32 (0)2 673 61 00

**www.smart-ticketing.org**

Editors: **Cord Bartels** cord.bartels@cbcon.de
**Mike Eastham** mike.eastham@itso.org.uk

## 1.3 Special Word Usage

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

## 1.4 NFC Name and Logo Usage

The Near Field Communication Forum’s policy regarding the use of the trademarks *NFC Forum* and the NFC Forum logo is as follows:

- Any company MAY claim compatibility with NFC Forum specifications, whether a member of the NFC Forum or not.
- Permission to use the NFC Forum logos is automatically granted to designated members only as stipulated on the most recent Membership Privileges document, during the period of time for which their membership dues are paid.
- Member’s distributors and sales representatives MAY use the NFC Forum logo in promoting member’s products sold under the name of the member.
- The logo SHALL be printed in black or in colour as illustrated on the Logo Page that is available from the NFC Forum at the address above. The aspect ratio of the logo SHALL be maintained, but the size MAY be varied. Nothing MAY be added to or deleted from the logos.
- Since the NFC Forum name is a trademark of the Near Field Communication Forum, the following statement SHALL be included in all published literature and advertising material in which the name or logo appears:

  NFC Forum and the NFC Forum logo are trademarks of the Near Field Communication Forum.

## 1.5 Abbreviations, glossary

| | |
|---|---|
| CICO | Check-In / Check-Out |
| EMD | Electro-magnetic disturbance (specified in ISO/IEC14443) |
| eID | Electronic Identity |
| eSE | Embedded Secure Element |
| ID | Identity |
| IFMS | Interoperable Fare Management System |
| NFC ANA | NFC Forum analog specification |
| NFCF | NFC Forum |
| NFCF Type F | Stands for “NFC-F” as used in the NFC Forum analog specification |
| MNO | Mobile Network Operator |
| NMD | NFC Mobile Device |
| NMD process | Business process that involves NFC Mobile Devices |
| NMD Use Case | Use case that involves NFC Mobile Devices |
| nPA | German identity card |
| OTA | Over-the-Air – communication via the wireless network connection of the NMD |
| PCD | Proximity Coupling Device |

| | |
|---|---|
| PICC | Proximity Integrated Circuit Card |
| PT | Public Transport |
| PT object | Contactless smart card, token or other device used as (PT) fare media by the PT customer |
| SE | Secure Element |
| STA | Smart Ticketing Alliance |
| TSM | Trusted Service Manager |
| TSP | Transport Service Provider |
| UICC applications. | Universal Integrated Circuit Card. May host SIM, USIM and e.g. PT |
| USP | Unique Selling Proposition |
| µSD | microSD |

## 1.6 Revision History

| Version | Description of update or change | Date | Author |
|---|---|---|---|
| **STA Document V1.7.4** | **Updated document. General editorial amendments. Updated references to CEN TS/16794. Definition of PT object added.** | **October 2016** | **Mike Eastham** |
| **STA Document** | **Adapted from VDV ETS / ITSO document version 1.7.3 with new introduction.** | **February 2016** | **Jarl Eliassen** |
| **1.7.3** | **Adoption from VDV ETS / ITSO document version 1.7.2** | **June 19th, 2015** | **C. Bartels** |

*Note: A further update is planned in 2017 to introduce additional enhancements to this document following experience gained in the Optimos Project in Germany.*

# 2 Purpose of this document

This document shall support the implementation of certified technical interoperability between NFC enabled mobile devices and Public Transport systems. This shall be achieved by documenting the way that NFC Mobile Devices are used in Public Transport and by identifying the relevant requirements on this basis.

A special boundary condition is that smart phones are usually marketed globally; there will be no specific mobile devices for certain PT system implementations, countries or regions. Therefore NFC Mobile Devices have to be seen as generic platforms that should support Public Transport eTicketing worldwide. Consequently, all globally relevant Public Transport eTicketing schemes have to be considered when documenting the use of NFC Mobile Devices and identifying the resulting requirements. The following step-by-step approach was used to compile and document the necessary information:

1. Description of PT business processes that involve NFC-enabled mobile services and NFC Mobile Devices
2. Documentation of the technical implementation of these PT business process per Use Case:
    a. Description of specific Use Cases that involve NFC devices
    b. Identification of PT readers and PT objects that communicate with NFC devices
    c. Documentation of relevant parameters for interoperability
    d. Identification of specific requirements per parameter
    e. Aggregation across Use Cases and consolidation of requirements

The document is intended as an informative resource for standardisation activities.

# 3 Documentation of NFC-enabled business processes

## 3.1 Introduction to the “Mobile service life cycle”

The introduction of NFC Mobile Devices (NMD) into PT eTicketing offers various options for practical implementation. The NMD can be used as PT object, as reader in a NFC tag infrastructure or as the customer’s interface to his personal online account in the PT service provider’s online shop.

As described in the previous chapter, the target of technical interoperability requires that in this step all business processes that may be used by any of the globally relevant PT eTicketing schemes are documented. The explicit goal is to cover all relevant business processes worldwide even if many particular PT implementations may only support a selection of these processes.

Moreover, the definition of business processes should not only the cover the transportation service and related business processes and Use Cases but also the entire life cycle of PT services. The customer should be in the position to conduct all relevant steps from establishing a personal account to validation of the entitlement / payment by his NFC Mobile Device:

A. Customer creates a personal account at the transport service provider’s online-platform
B. Customer selects products, pays for and downloads products, configuration of PT object or NMD
C. Customer uses transportation service
D. Back to (B): Purchasing of entitlements or maintenance of media, NMD.

   Back to (A): Management of the personal account

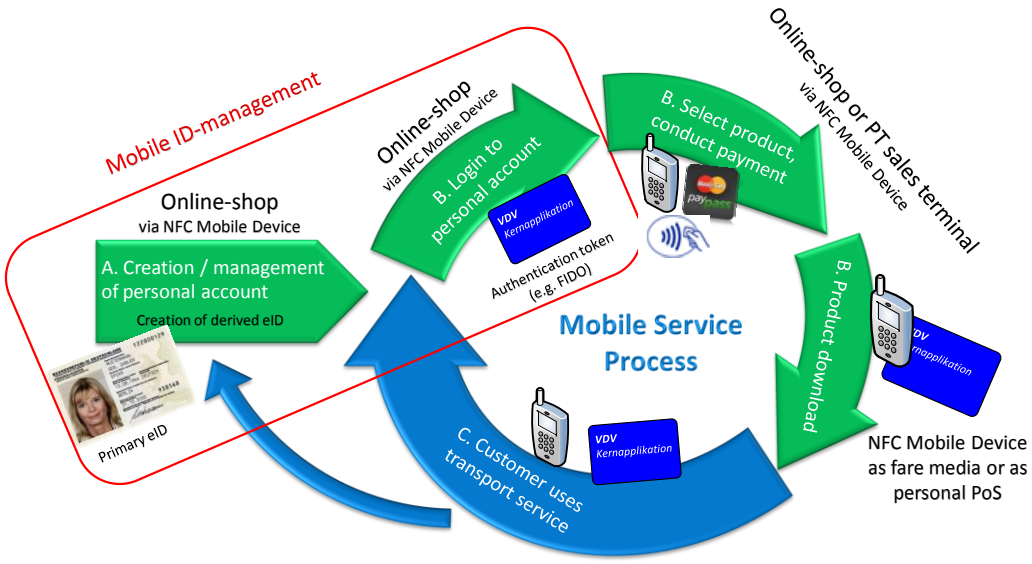


*Figure 1 Mobile service life cycle in Public Transportation*

Figure 1 shows the “Mobile service life cycle”. Every step may include one or more business processes. These business processes are described in chapter 3.3.

The model of the “Mobile service life cycle” can be seen as a set of business process, Use Cases and functions that may occur in mobile PT eTicketing. As described above, NFC

mobile devices shall be capable of supporting all known and relevant business processes and uses cases. Therefore the considerations in this document need to reflect the complete overview. However, from the perspective of the particular application system, not all business processes and Use Cases may be required. The following examples illustrate this:

- eTicketing schemes that are using electronic IDs or credentials for authentication don't need any download of products (tickets, entitlements) to the PT object. The PT object may be substituted by a carrier media for the ID.
- Some eTicketing systems are implementing payment for every single trip. In such case the customer may just need his credit card account and a contactless credit card. There is no direct connection between the customer and the Transport Service Provider (TSP) and no need for a personal account with the TSP.

## 3.2 Identification of NFC-enabled business processes

This sub-chapter provides an overview on the business processes that may involve NFC Mobile Devices (NMD processes).

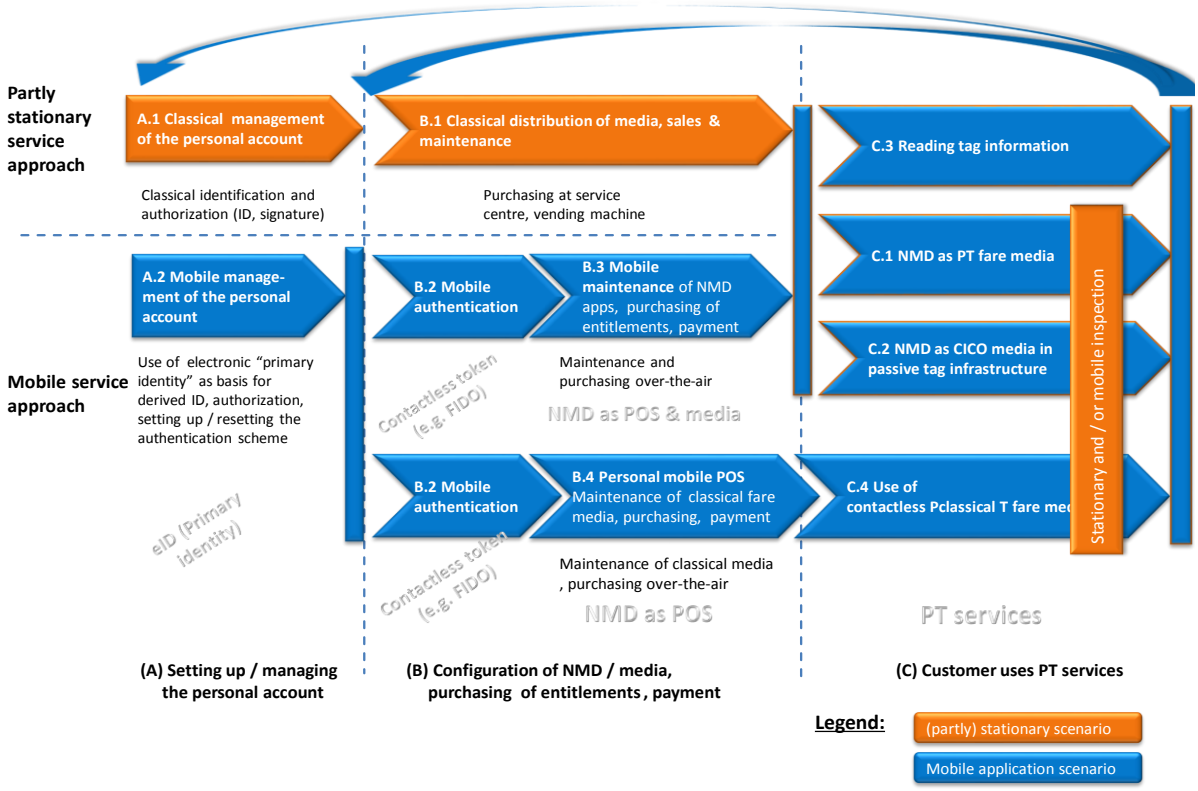


*Figure 2 NFC-enabled business processes and PT mobile service life cycle*

The business processes shown in Figure 2 are briefly described in the following table.

| NMD process | Description |
|---|---|
| **For information only:**<br>**A.1 Classical management of the personal account (no usage of NMD)** | The classical management of the personal account requires the customer to visit a service center.<br>In case of a classical online registration, there may be a significant waiting time until the account can be activated because the customer's personal data has to checked and confirmed by a back office process. This check would be redundant and waiting times can be avoided if a trustworthy primary eID is used. This is described in the following processes. |
| **A.2 Mobile management of the personal account** | Successful implementation of mobile eTicketing services requires that the PT customer can cover all steps of the service life cycle by using the NMD.<br>A convenient and fast way of creating and managing a personal account is provided if the customer owns a contactless electronic ID card that provides trustworthy identity data. In this case, the ID-data can be read by the TSP's online platform via the NMD's contactless interface. Since this data is considered trustworthy, there is no need for additional checks and the account can be activated immediately. In some cases, eID cards may also be used by the customer to authorize debit payment schemes.<br>Alternatively other approaches for online-identification of the consumer could be used. Stakeholders that own trustworthy electronic ID of the customer like mobile network operators (such as GSMA's mobile connect) or payment service providers could offer such services. Since these concepts are not generating requirements to the NFC interface they are not described in this document. |
| **B.1 Classical sales and maintenance process** | When using NFC Mobile Devices, management of applications, purchasing of entitlements and payment will normally be done over-the-air. As fallback, there should be the option to use the TSP's classical sales infrastructure in service centres and at sales terminals. In this case, the ticket would be loaded onto the NMD via the NFC-interface. |
| **B.2 Mobile authentication** | Classical login to online-platforms using "Username / Password" can no longer be considered secure. As a future proof alternative the TSP's online platform may require support of two-factor-authentication for access to the personal online-account.<br>In some cases, a customer may use contactless authentication media (authentication token or eID) with their NMD to access their personal account. |
| **B.3 Mobile sales and maintenance process** | Customer's NMD connects directly to the TSP's online platform supporting online maintenance of the NMD's configuration, selection and purchasing of products, payment and download of the products to the NMD. |
| **B.4 Personal Point of Sales (pPoS)** | Customer uses his NMD as a personal mobile sales terminal (pPoS) or information device:<br>Loading of applications or entitlements to the customer's PT object (contactless card, token)<br>Checking contents and status of the PT object |
| **C.1 PT object** | The NFC Mobile Device is used as the customer's PT object and replaces the contactless card or token. Depending on the TSP's service offer, the NMD shall not only support ticket validation but also automated fare |

| NMD process | Description |
|---|---|
| | calculation and related check-in and check-out processes. This business process implies high requirements to transaction times with the NMD. |
| **C.2 Check-in / check-out with passive infrastructure** | Stationary tags containing location data are used for check-in and check-out (CICO). Allows introduction of advanced fare management services without investment into an eTicketing reader infrastructure. Ideal for "green field" situations. |
| **C.3 Reading tag information** | Stationary NFC tags can be used for various services around public transport eTicketing. They may for example be deployed at stations and bus stops and could e.g. contain a URL. The PT customer will be linked to the TSP's ticket shop or the online schedule when tapping the NFC tag with his NMD in reader mode. |

*Table 1: Overview of NMD processes*

## 3.3 Description of NFC-enabled business processes

### 3.3.1 NMD process A.2 "Mobile management of the personal account"

#### 3.3.1.1 Description

Successful implementation of mobile eTicketing services requires that the PT customer can cover all steps of the service's life cycle seamlessly by using his mobile device. From the business perspective, one of the most relevant steps is setting up a user account, the authorization of debiting schemes and secure sign-on by using the personal NMD. It is essential that the customer can conduct this conveniently, quickly and without waiting times before activation of the account.

The TSP is dependent on trustworthy customer data and legally binding statements from his customer. Therefore, up to now, the customer has typically had to present his ID at the customer service centre in order to establish a customer account and to sign a contract to authorize debit payment. If the customer registers online, the TSP needs to check and confirm the personal data causing waiting times before activating the account (see "Classical management of the personal account"). Both procedures are inconvenient for the customer, costly for the TSP and don't fit into a mobile service portfolio.

For a seamless mobile approach to PT services, the customer's identity data should be provided by an electronic "primary identity" that interfaces with the customer's NMD. Such data can be regarded as trusted data. There is no need for an additional cross-check before activating the account and e.g. establishing a debit payment agreement. Contactless governmental eID cards that serve as electronic "primary identities" can serve this purpose. They have been deployed or are planned by several countries. The TSP benefits from reduced cost of sales, trusted customer data and convenient access of customers to his services.

#### 3.3.1.2 NFC value proposition

All known electronic "primary identities" are implemented as smart cards with contact and increasingly with contactless interface according to ISO/IEC14443. An NMD may interact with such contactless cards and allows the use of primary identities as enabler of a seamless mobile business process. This is a true USP for NFC compared to other interface technologies.

Alternatively other approaches for online-identification of the consumer could be used. Stakeholders that own trustworthy electronic ID of the customer like mobile network operators (like GSMA's mobile connect) or payment service providers could offer such services. Since these concepts are not generating requirements to the NFC interface they are not described in this document.

#### 3.3.1.3 Use Cases

In this application scenario, the NMD will be used in "NFC reader mode" and communicates with contactless eID-media. The process includes the following Use Cases:

- UC -A.2-1 "Loading application software onto the NMD"
- UC-A.2-2 "Creating the personal account via NMD and contactless eID"
- UC-A.2-3 "Authorization of direct debiting schemes via NMD and contactless eID"
- UC-A.2-4 "Sign-on to the personal account via NMD"

#### 3.3.1.4 Security aspects

The communication between the eID application (whether on a separate card or in the secure element / UICC of the NMD) and the backend is secured cryptographically end-to-end. A security weakness in the communication between an eID card and an NMD does not directly influence the communication between eID and backend. Furthermore, the user must enter the correct PIN for the eID application and has only a very limited number of attempts. The loss of the NMD and eID application (whether on a separate card or in the NMD) alone does not lead to a serious threat. The types of successful attacks, similar to the case of using the eID with a reader and home computer online, are based on introducing malware onto the NMD that can capture the PIN during entry and send messages to the eID application using it as a slave.

### 3.3.2 NMD process B.1 "Classical sales and maintenance"

#### 3.3.2.1 Description

Today, the PT customer usually obtains his PT object, entitlements and tickets via the provider's service centre or vending machines. If maintenance of the PT object (e.g. installation of new software) is supported, this will normally be carried out in the secure environment of a service centre or by special maintenance devices. Also, online portals are common in PT. These usually support the management of the customer's data and the ordering of media and entitlements. Loading of entitlements to customer's PT object isn't a common function of online portals today and requires a reader infrastructure on the customer's side, the "customer home infrastructure", or the implementation of action lists at pick-up points in stations. These action lists contain information about tickets bought by customers online that are to be loaded to cards or other user media (e.g. an NMD). These classical variants do not leverage the ability of the NMD to communicate directly with ticker-servers in the backend and are less convenient for users.

When using the NMD as PT object, management of applications, and purchasing of entitlements should be done over-the-air. The classical sales and maintenance infrastructure described above shall only be used as a fallback solution. When using NMD, the relevance of this process is limited.

In this process, the NMD will be used in "NFC card emulation mode" and communicates via the NFC interface with the following PT infrastructures:

- Stationary sales infrastructure
- Customer home infrastructure

Coverage for non-personalized PT object and anonymous purchasing of products

NMD are usually linked to a specific person. Nevertheless, anonymous purchasing of products and use of entitlements is possible. For obtaining a non-personalized PT object or anonymous purchasing of tickets, the customer has to visit the TSP's service centre or a vending machine.

Payment should be in cash or by using a stored-value scheme (or credit card payment). The issuance of tickets that themselves do not contain any reference to a person is possible by the usual issuance processes. In the usage of such tickets it is then possible that the identity of the ticket-holder will not be conveyed to the TSP; however, to prevent copying these kinds of tickets, they must be stored in a SIM or secure element. Access to the secure storage has to be protected by cryptographic measures.

#### 3.3.2.2 Use Cases

The process includes the following Use Cases that are relevant to NMD:

- UC-B.1-1 "Management of the secure storage via the NFC interface"
- UC-B.1-2 "Loading and management of entitlements via the NFC interface"

### 3.3.3 NMD process B.2 "Mobile authentication"

#### 3.3.3.1 Description

Secure sign-in to the customer's online account is a fundamental function of the seamless mobile service approach. Ideally a two-factor-authentication should used.

This authentication function could be supported by an eID, the PT object (secure NMD or card based) or a specific authentication token. With an open concept like FIDO[1], the authentication function could probably also be used for other applications than PT.

#### 3.3.3.2 Use Cases

The process includes the following Use Cases:

- UC- B.2-1 "Setup of the authentication mechanism"
- UC- B.2-2 "Sign-on to the personal account via NMD"

[1] https://fidoalliance.org/

### 3.3.4 NMD process B.3 “Mobile sales and maintenance”

#### 3.3.4.1 Description

When using the NMD as PT object, management of applications and purchasing of entitlements will normally be done over-the-air.

The NMD connects to the customer’s account in the TSP’s online customer portal via the mobile network. This online portal and the customer’s NMD have to support the following Use Cases:

- setup and maintenance of the NMD (settings and installation of software)
- setup and maintenance of the secure storage (eSE, SIM, µSD etc.) loading and management of entitlements on the NMD
- purchasing of entitlements (incl. Payment, refund)

#### 3.3.4.2 Use Cases

The process includes the following Use Cases:

- UC- B.3-1 “Loading application software onto the NMD”
- UC- B.3-2 “Management of the secure storage over-the-air”
- UC- B.3-3 “Purchasing and management of entitlements over-the-air ”
- UC- B.3-4 “Payment”

### 3.3.5 NMD process B.4 “Personal Point of Sales”

#### 3.3.5.1 Description

A huge number of contactless PT objects (cards or tokens) have been issued by TSP and are in use by PT customers. The card holders may use their NFC Mobile Device as personal sales and information terminal that connect these PT objects to the TSP’s online service platform from any location and at any time.

The NMD serves as the PT customer’s personal mobile sales and information device:

- Loading of applications or entitlements to the customer’s PT object
- Checking contents and status of the customer’s PT object

The advantages are twofold: The TSP reduces cost of sales and the customer benefits from easy access to entitlements, tickets and information related to transportation services. In addition, there is no need for a secure storage in the NMD and a TSM that administers this secure storage.

#### 3.3.5.2 NFC value proposition

Today and in future, the vast majority of PT customers will be equipped with contactless cards or tokens. Several billion cards have been issued worldwide to date. This huge infrastructure can be integrated into a mobile service offer by using the NFC interface of the customer’s NMD.

#### 3.3.5.3 Use Cases

In this application scenario, the NMD will be used in “NFC reader mode” and communicates with the contactless PT object via the NFC-interface. The process includes the following Use Cases:

- UC-B.4-1 “Loading application software onto the NMD”
- UC- B.4-2 “Purchasing and management of entitlements ”

- UC- B.4-3 “Payment”

### 3.3.6 NMD process C.1 “PT object”

#### 3.3.6.1 Description

In this process, the NMD serves as the customer’s PT object. Tickets or entitlements are obtained via the NMD processes B.2 “Mobile sales and maintenance” or B.1 “Classical sales and maintenance” and stored in the secure storage of the NMD.

As alternative to an entitlement, also an ID or an ID-token may be used if the PT eTicketing infrastructure follows the principles of account-based ticketing or tokenization.

The PT customer presents the NMD for inspection or check-in respectively check-out to PT readers (stationary inspection infrastructure) or to mobile inspection devices.

In terms of transaction time and security, the NMD has to fulfill the same requirements as card-based PT objects. Depending on the protection demand of the products and data to be stored, the NMD may need a secure storage and related trusted service management and interfaces.

The NMD replaces the classical PT object. The TSP may save the cost related to issuing and managing cards. In addition, the NMD can support additional application scenarios and services which makes it a flexible and future proof media.

If the entitlement, the ID or the ID-token are stored in the NMD (SIM-card, eSE, uSD or other storage of the NMD) the concept works also if the NMD is not online.

The NMD operates in “NFC card emulation mode” and communicates with the following infrastructures:

- Stationary inspection infrastructure
- Mobile inspection infrastructure

#### 3.3.6.2 Use cases

Before starting this NMD process, the customer has to make sure that the NMD (incl. secure storage) is configured for this process and has to purchase and load the required entitlements, ID or tokens.

The NMD process includes the following Use Cases:

- UC-C.1-1 “Ticket validation, check-in / check-out”
- UC-C.1-2 “Mobile inspection”

### 3.3.7 NMD process C.2 “Check-in / check-out with passive infrastructure”

#### 3.3.7.1 Description

TSP may use stationary NFC-forum or ISO/IEC-conformant tags that are located at platforms, bus stations or in vehicles instead of a classical reader infrastructure. In combination with the customer’s NMD, such tag infrastructures can support the customer’s check-in or check-out process (CICO) and provides all means that are required not only for validation of classical tickets but also for more demanding PT services like automated fare calculation (AFC). System implementations that support check-in and check-out as well as others that use check-in only should be considered.

Compared to classical stationary reader infrastructures, the TSP benefits from a significant reduction of cost since NFC tags are much cheaper than readers and need no network connection or energy supply. The concept provides a very economical and service-oriented approach to “green field” situations where an eTicketing system can be built up without the necessity of integrating incumbent eTicketing infrastructures and if the requirements on transaction speed and throughput are moderate.

For check-in or check-out, the NMD will be used in NFC reader mode. During inspection by the conductor or revenue inspector, the NMD will emulate a PT card media. Thus, the NMD has potentially to communicate with the following infrastructures:

- NFC-forum or ISO/IEC14443-conformant tags.
- PT Mobile inspection readers.

#### 3.3.7.2 NFC value proposition

An NFC-enabled mobile device can read information from passive tags that contain e.g. information about the platform or the station. This Use Case didn’t exist in eTicketing until the advent of NFC tags. But it is also important that the NMD can seamlessly be integrated into an existing mobile inspection infrastructure that was designed for classical contactless PT object. The NFC-interface provides the flexibility to combine innovative new concepts and interoperability with legacy infrastructures.

#### 3.3.7.3 Use Cases

Before using this business process, the customer has to make sure that the NMD (incl. secure storage) is configured for this process and has to purchase and load the required entitlements, ID or tokens.

The following Use Cases are relevant when using the NMD with a passive tag infrastructure:

- UC-C.2-1 “Check-in or check-out”
- UC-C.2-2 “Mobile inspection”

The NMD will be used in reader mode to perform the check-in and check-out but serves in general as the customer’s PT object.

### 3.3.8 NMD process C.3 “Reading tag information”

#### 3.3.8.1 Description

The TSP may use simple, stationary NFC forum-conformant tags that are located at platforms, bus stations or in vehicles to provide additional services to their customer. Common examples for such additional services are tags that link PT customers directly to the specific online time table and ticket product in the TSP’s online ticket shop.

#### 3.3.8.2 NFC value proposition

NFC supports the concept of passive tags with defined data structure or even predefined applications like URL linking. In contrast to alternative approaches that are e.g. based on bluetooth connections, these tags don’t need a battery, are inexpensive and very durable.

#### 3.3.8.3 Use Cases

The NMD communicates in ”NFC reader mode” with NFC-forum or ISO/IEC14443 tags. The process includes the following Use Case:

- UC-C.3-1“Reading tag information”

# 4 Identification of requirements per Use Case

In most cases NFC Mobile Devices (NMD) will be introduced into existing Public Transport eTicketing infrastructures where PT readers and PT objects are already deployed. An NMD may be used in "NFC reader mode" as PT sales terminal, for reading tags or in "NFC card emulation mode" as a PT object. These two modes of operation shall be distinguished. The "NFC peer-to-peer mode" is not expected to be used in PT infrastructures and is therefore not considered here.

The business processes involving NFC-enabled mobile devices are described in chapter 3. Now, the analysis goes into more detail. In order to identify the relevant requirements to interoperability between PT infrastructures and NFC mobile devices it needs to be identified which particular components of a PT eTicketing infrastructure have to communicate with NFC mobile devices under which particular boundary conditions. This information can be derived from the typical parameters of these components and an analysis of the Use Cases that implement a particular business process.

## 4.1 Specifics of the contactless interface

### 4.1.1 Relevant standards for the contactless interface

1. PT eTicketing

   Currently, several different standards for the contactless interface are in use with relevant Public Transport eTicketing implementations worldwide:

   - EMVCo L1 is used by infrastructures that use a payment-centric approach to ticketing e. g. TfL in London, EZ-Link in Singapore
   - ISO/IEC14443 provides the basis for many fare management systems (brands are e.g. Calypso, CEPASS, EasyCard, ITSO, OV-chipkaart, RabbitPass, T-Money, Touch'n'go, VDV KA, YiKatong as well as system solution brands like MIFARE and CIPURSE). This is a non-exhaustive list and doesn't tell the particular relevance of these brands.
   - CEN/TS16794 has been recently developed to define a PT-specific profile for ISO/IEC14443-based PT infrastructures. STA adopted CEN/TS16794 specifications as the contactless communication specification for PT devices and has set up a Europe-wide certification scheme for creating the basis of European contactless interoperability between PT devices. It is most likely therefore that CEN/TS16794 will be used in Europe for ensuring interoperability between PT devices (readers or objects) and shall be taken into account for interoperability with NMD.
   - ISO/IEC18092 is compatible with NFC Forum's analog specification. This covers also JIS X 6319-4 and supports the FeliCa-brand system implementations like Octopus and SuiCa.

   Payment

   Contactless payment is part of the mobile business processes for Public Transport as described in chapter 3. The following RF-standards have to be considered for this application:

   - EMVCo L1 is the worldwide leading standard in contactless payment. The major credit card schemes are testing their interfaces and customer media according to this standard.
   - ISO/IEC18092 is compatible with NFC Forum's analog specification. This covers JIS X 6319-4 and supports payment in the context of FeliCa system implementations

2. eID, authentication

   Contactless electronic ID cards and programmable security controllers that could be configured as authentication media (e.g. according to FIDO specifications) are using ISO/IEC14443 as standard for the contactless interface. There are also authentication tokens that are using ISO/IEC18092 in the market globally.

### 4.1.2 Operating distance

The term "operating distance" specifies the distance between the reader and contactless object in which the contactless object has to work according to its specifications.

For time critical use cases an operating distance of several cm is expected (depending on the particular infrastructure) so that there is as much time as possible for the card to be powered and operating when inside the field in a "touch and go" situation. (Note that for compliance purposes a minimal operating distance of 2cm is specified in CEN/TS16794 for PT IFM readers in Europe.)

In practice it can be useful or even necessary to specify not only the distance between contactless reader and object for a single point but an area that covers several points in the specified distance in which the card or NMD will operate. The NFC Forum specifies dedicated radii for the defined distances and consequently names this parameter not "operating distance" but "operating volume".

## 4.2 Categorization of Public Transport infrastructures and media

### 4.2.1 Public transport infrastructures

The following types of Public Transport eTicketing components could interact with NFC Mobile devices:

1. Stationary sales infrastructure

   The category "Stationary sales infrastructure" includes contactless readers that are used for the maintenance of applications and personal data on the PT object, payment and loading of products. These readers are deployed in customer service centers, vending machines and information terminals.

   The requirements on these readers are usually moderate. The implementation reflects a compromise between performance and cost. The relevant parameters can be assumed as follows:

| | |
|---|---|
| Transaction performance: | Moderate |
| Reader Antenna size: | Commonly in the order of PICC class 1, not smaller than PICC class 3. Also, sizes larger than PICC class 1 are used. |
| Operating distance: | 0 to min. 5mm (card or NMD touches reader surface) |
| Supported RF-standards: | Depending on system implementation (EMVCo L1 or ISO/IEC14443 (or CEN/TS16794)- or ISO/IEC18092 / NFCF Type F) |
| Special requirements: | Support for EMD and "extended APDU" acc. to ISO7816 in case asymmetric cryptography is used.<br>Extended reliability and temperature range. |

2. Online service and ticket portal

   This category includes online platforms owned by the Transport Service Provider or resellers which support customer accounts, online maintenance of the PT object and online sales of PT products.

3. Customer home infrastructure

   The PT customer may use a contactless reader that is connected to his local home IT infrastructure (e.g. PC) to connect to the Transport Service Provider's (TSP) online platform and to manage his account, load tickets, view the contents of his PT object etc. This type of reader is categorized as "Customer home infrastructure".

   The requirements on these readers are usually very moderate. The implementation focuses on minimization of cost. The relevant parameters can be assumed as follows:

| | |
|---|---|
| Transaction performance: | Moderate |
| Antenna size: | In the order of PICC class 1 - 3, may go down to class 6 |
| Operating distance: | Card or NMD touches reader surface → 0 to min. 5mm |
| Supported RF-standards: | Depending on system implementation (EMVCo L1 or ISO/IEC14443 or ISO/IEC18092 / NFCF Type F) |
| Special requirements: | Support for EMD and "extended APDU" acc. to ISO7816 in case asymmetric cryptography is used |

4. Stationary inspection infrastructure

   This category includes readers that are integrated into gated infrastructures, check-in/check-out-readers in stations or vehicles and are used for validation of entitlements or check-in or check-out.

   Requirements to transaction performance, operating volume and reliability are very high for this category of readers. The relevant parameters can be assumed as follows:

| | |
|---|---|
| Transaction performance: | Very high. Less than 500ms system transaction, in cases even a maximum of 200ms. |
| Antenna size: | In the order of PICC class 1 or even larger |
| Operating distance: | Card has to operate already at a distance → 0 to min. 20mm, typically up to 100mm. |
| Supported RF-standards: | Depending on system implementation (EMVCo L1 - or ISO/IEC14443 (or CEN/TS16794) - or ISO/IEC18092 / NFCF Type F) |
| Special requirements: | Support for EMD<br>Extended reliability and temperature range |

5. Mobile inspection readers

   Mobile control devices that are used by conductors and mobile revenue inspectors for ticket validation and ticket sales in vehicles and trains are categorized as “Mobile inspection readers”.

   Requirements to transaction performance and operating volume are moderate for this category of readers. The relevant parameters can be assumed as follows:

| | |
|---|---|
| Transaction performance: | High. Less than 500ms for a system transaction. |
| Antenna size: | In the order of PICC class 1, not smaller than class 3 |
| Operating distance: | Card or NMD touches reader surface → min 5mm |
| Supported RF-standards: | Depending on system implementation (EMVCo L1 - or ISO/IEC14443 (or CEN/TS 16794) - or ISO/IEC18092 / NFCF Type F) |
| Special requirements: | Support for EMD and “extended APDU” acc. to ISO7816 in case asymmetric cryptography is used.<br>Extended reliability and temperature range |

   It is assumed here that NMD will not be used as mobile inspection readers.

6. Tag infrastructure

   Tags may be positioned at platforms, bus stops, in vehicles, etc. These tags may store data that e.g. provides information about the location, links to PT schedules and seat reservation as basis for services provided by the TSP.

   Standard tags have been specified by the NFC Forum (Tag type 1-4). The relevant parameters can be assumed as follows:

| | |
|---|---|
| Antenna size: | Classes from 1 down to 3. Smaller sizes (down to class 6) are expected to become relevant as well. |
| Mounting: | Often mounted behind e.g. plexiglas |
| Supported RF-standards: | Depending on system implementation (NFCF ANA or ISO/IEC14443) |
| Special requirements: | Extended reliability and temperature range |

   If mounted behind e.g. screens or panes, testing and certification of the tags has to be performed for the entire system including NFC-tag, screen and glue.

### 4.2.2 Public transport PT object

The following types of cards or media shall be considered:

1. Contactless PT object

   Smart tickets, cards or tokens with contactless interface that are used as PT object by the PT customer are categorized as “Contactless customer PT objects” or simply “PT objects”. The relevant parameters can be assumed as follows:

| | |
|---|---|
| Antenna size: | PICC classes from 1 down to class 3 are common. Smaller sizes (down to class 6) are expected to become relevant as well. |
| RF-standards: | Depending on system implementation (EMVCo L1 - or ISO/IEC14443 (or CEN/TS16794) - or ISO/IEC18092 / NFCF Type F) |

2. Contactless eID-card or authentication media

   Personal eID- or authentication cards with contactless interface that may be used as "primary identity" and/or for login and management of online services are included in this category. The relevant parameters can be assumed as follows:

| | |
|---|---|
| Antenna size: | PICC classes from 1 down to 3. Smaller sizes (down to class 6) are in use as authentication tokens and are expected to become relevant as well. |
| RF-standards: | ISO/IEC14443, for authentication media also ISO/IEC18092 |
| Special requirements: | Asymmetric cryptography |

3. Contactless payment card

   This category includes contactless cards that are used for payment. The relevant parameters can be assumed as follows:

| | |
|---|---|
| Antenna size: | PICC classes from 1 down to 3. Smaller sizes (down to class 6) are expected to become relevant as well. |
| RF-standards: | Depending on system implementation (EMVCo L1 or ISO/IEC18092 / NFCF Type F) |

## 4.3 Description of Use Cases, identification of related requirements

### 4.3.1 NMD process A.2 “Mobile management of the personal account”

The process is described in chapter 3.3.1. It includes the following Use Cases.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-A.2-1** | Use case “**Loading application software onto the NMD**” | | | |
| | Description: | Communication between TSP’s online portal and the eID media via the customer’s NMD requires installation of specific software on the NMD.<br>This Use Case covers the download and installation of the eID issuer’s app and the TSP’s app onto the customer’s NMD. Typically the Apps will be made available in one of the known App-Stores like Google Play. Alternatively Apps could be obtained anonymously or under pseudonym e.g. from the TSP or the eID issuer. | | |
| | PT object: | 1. NMD | NMD mode: | 1. Over-the-air |
| | Infrastructure: | 1. OS supplier’s app store | | |
| | Requirements: | 1. eID issuer’s app and TSP’s app must be available and released for the NMD’s OS version.<br>2. Maintenance for these apps has to be provided by the eID issuer and the TSP | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Mandatory | | |
| **UC-A.2-2** | Use case “**Creating the personal account via NMD and contactless eID**” | | | |
| | Description: | Customer registers for a personal account at the TSP’s online platform.<br>The TSP’s online platform reads personal data from the customer’s contactless eID card which serves as “primary ID”. Since the ID attributes obtained from the eID card can be considered reliable and trustworthy, verification isn’t necessary. The customer’s new account can be activated immediately.<br>If supported by the eID-system and the TSP’s online platform, the customer could chose to use a pseudonym instead of his real name.<br>The TSP usually generates a “derived ID” for this customer based on the data obtained from the primary ID. This derived ID is used as reference to the particular customer for all related data and further relations.<br>This concept will coexist with other ways to establish personal accounts like username/password or by using ID provided by MNO or other ID providers. | | |
| | PT object: | 1. Contactless eID card | NMD mode: | 1. NFC reader mode, over-the-air |
| | Involved Infrastructure: | 1. Online service and ticket portal | | |

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| | Requirements: | 1. NMD in NFC reader mode has to be interoperable with contactless eID-card (primary eID).<br>2. NMD needs access to the TSP's online platform via internet. | | |
| | Relevance: | Relevance for NMD: Mandatory for interoperability considerations<br>Relevance for PT system implementations: Only relevant if contactless primary eID generally available to PT customers. | | |
| **UC-A.2-3** | Use case "**Authorization of direct debiting schemes via NMD and contactless eID**" | | | |
| | Description: | The customer authorizes direct debiting schemes for his bank account at the TSP's web platform by using his contactless eID card. Avoids additional verification effort and waiting times. | | |
| | PT object: | 1. Contactless eID card | NMD mode: | 1. NFC reader mode, over-the-air |
| | Infrastructure: | 1. Online service and ticket portal | | |
| | Requirements: | 1. NMD in NFC reader mode has to be interoperable with contactless eID-card ((primary eID).<br>2. NMD needs access to the TSP's online platform via internet. | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Optional | | |
| **UC-A.2-4** | Use case "**Sign-on to the personal account via NMD**" | | | |
| | Description: | Sign-on to the personal account via NMD.<br>The customer's personal account at the TSP's online service and ticket platform is the major interface between customer and TSP in a seamless mobile service process. The customer will typically purchase and manage products and services via this channel. Secure and convenient access to this account is a crucial part of the mobile service offer. Classical "User name / password" concepts can't be considered secure and should not be used.<br>Two concepts could in principle support a convenient 2-factor-approach:<br>1. The NFC-interface of the NMD supports communication with external contactless authentication cards and tokens. The NMD serves as transparent interface between the TSP's online service and ticket portal and such an external authentication function and supports secure and convenient sign-on in this way. This authentication function can e.g. be supported by the eID card that was used as primary identity, an authentication token or a classical PT object that supports secure authentication.<br>2. Alternatively the NMD could be equipped with a secure authentication function by e.g. loading an authentication application into the secure storage of the NMD. This scenario requires sufficient and approved protection in the NMD's system architecture for PIN or passwords that have to be entered by the user via the NMD's keyboard or biometric data that comes from e.g. the fingerprint sensor of the NMD. This is currently not generally provided. Therefore an external authentication media | | |

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| | | acc. to 1. should be used until security of the internal solution can be guaranteed. | | |
| | PT object: | 1. Contactless PT object or eID card with authentication function, authentication card<br>2. NMD, that supports a secure authentication function | NMD modes: | 1. NFC reader mode, over-the-air<br>2. Over-the-air |
| | Infrastructure: | 1. Online service and ticket portal<br>2. Online service and ticket portal | | |
| | Requirements: | 1. NMD in NFC reader mode has to be interoperable with ISO/IEC14443 - or ISO/IEC18092 - conformant eID- or authentication media (Antenna class 1-3, processor card, asymmetric and / or symmetric cryptography).<br>2. NMD needs access to the TSP's web platform via internet. | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Mandatory | | |

*Table 2: Relevant Use Cases of the NMD process A.2 "Mobile management of the personal account"*

### 4.3.2 NMD process B.1 “Classical sales and maintenance”

The process is described in chapter 3.3.2. It includes the following Use Cases that are relevant to NMD.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC – B.1-1** | Use case “**Management of the secure storage via the NFC interface**” | | | |
| | Description: | Normally the initialization and configuration of the NMD’s secure storage and the loading and installation of the TSP’s application software (typically a Java applet) into the secure storage will be performed over-the-air. This Use Case serves as a fallback solution or additional scenario. In this case this task is carried out via the NMD’s NFC interface in a secure environment like the TSP’s service centre.<br>This Use Case has to be carried out before loading and management of any entitlements, ID or tokens. | | |
| | PT object: | 1. NMD | NMD mode: | 1. NFC card emulation mode |
| | Infrastructure: | 1. Stationary sales infrastructure | | |
| | Requirements: | 1. Availability of external or built-in secure storage (eSE, UICC, µSD) for PT service provider’s applet, credentials and customer’s entitlements, check-in-data etc.<br>2. Drivers etc. officially supported by the OS, NMD vendor.<br>3. Availability of an open, interoperable trusted service for initialization and management of the secure storage<br>4. Contractual relationship and operational / technical interfaces between Trusted Service Manager (TSM) and TSP established<br>5. NMD in NFC card emulation mode has to be interoperable with PT readers of the stationary sales infrastructure (incl. asymmetric and / or symmetric cryptography). | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Mandatory | | |
| **UC-B.1-2** | Use case “**Loading and management of entitlements via the NFC interface** ” | | | |
| | Description: | Normally entitlements (alternatively ID or tokens) purchased in the TSP’s online store are loaded over-the-air into the secure storage of the NMD. This Use Case serves as a fallback solution or additional scenario. In this case this task is carried out via the NMD’s NFC interface in a secure environment like the TSP’s service centre. | | |
| | PT object: | 1. NMD | NMD mode: | 1. NFC card emulation mode |
| | Infrastructure: | 1. Stationary sales infrastructure (sales readers, vending machines)<br>2. Customer home infrastructure | | |
| | Preconditions: | 1. Secure storage of the NMD configured<br>2. Purchase process (incl. payment, refund) completed | | |
| | Requirements: | 1. Availability of external or built-in secure storage (eSE, UICC, µSD) | | |

| No. | Use case / *Description* | |
|---|---|---|
| | | 2. Availability of an open, interoperable trusted service for loading entitlements into the secure storage.<br>3. NMD in NFC card emulation mode has to be interoperable with PT readers of the stationary sales and the customer home infrastructure (incl. asymmetric and / or symmetric cryptography). |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations:<br>– Support of loading and management via the "stationary sales infrastructure" is mandatory as first fallback option if over-the-air should not work.<br>– Support of loading and management via the "customer home infrastructure" would be a second fallback option and is considered optional. |

*Table 3: Relevant Use Cases of the NMD process B.1 "Classical sales and maintenance"*

### 4.3.3 NMD process B.2 “Mobile authentication”

The process is described in chapter 3.3.3. It includes the following Use Cases.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-B.2-1** | Use case “**Setup of the authentication mechanism**” | | | |
| | Description: | The setup of a secure login based on 2-factor-authentication between the TSP’s Online service and ticket portal and the customer’s NMD requires some preparations:<br>1. Customer has to obtain a suitable contactless authentication media as described in chapter 4.2.2. Customers will obtain such media normally from external sources (e.g. eID-providers, providers of FIDO-tokens). Alternatively, an authentication function could also be implemented on the PT object.<br>2. Customer may have to download an application-specific software (App) that supports the authentication media and has to install this on the NMD<br>3. The setup procedure between the customer’s account on the TSP’s online service and ticket portal and the authentication media has to be carried out. In the case of FIDO, this includes the generation and exchange of keys. | | |
| | PT object: | 1. NMD<br>2. Authentication media | NMD mode: | 1. Over-the-air<br>2. Over-the-air and NFC reader mode |
| | Infrastructure: | 1. OS-supplier’s app store<br>2. TSP’s Online service and ticket portal | | |
| | Requirements: | 1. TSP’s app must be available and released for the NMD’s OS version.<br>2. NMD must be interoperable with authentication media | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Mandatory | | |
| **UC-B.2-2** | Use case “**Sign-on to the personal account via NMD**” | | | |
| | Description: | See UC A.2-4 | | |
| | PT object: | See UC A.2-4 | NMD modes: | See UC A.2-4 |
| | Infrastructure: | See UC A.2-4 | | |
| | Requirements: | See UC A.2-4 | | |
| | Relevance: | See UC A.2-4 | | |

*Table 4: Relevant Use Cases of the NMD process B.2 “Mobile authentication”*

### 4.3.4 NMD process B.3 “Mobile sales and maintenance”

The process is described in chapter 0. It includes the following Use Cases.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-B.3-1** | Use case “**Loading application software onto the NMD**” | | | |
| | Description: | See UC-A.2-1 | | |
| | PT object: | See UC-A.2-1 | NMD mode: | See UC -A.2-1 |
| | Infrastructure: | See UC-A.2-1 | | |
| | Requirements: | See UC-A.2-1 | | |
| | Relevance: | See UC-A.2-1 | | |
| | Relevance: | See UC-A.2-1 | | |
| **UC-B.3-2** | Use case “**Management of the secure storage over-the-air**” | | | |
| | Description: | This Use Case covers over-the-air initialization and configuration of the secure storage, loading and installation of the TSP’s application software (typically a Java applet) and related software (drivers, API). Concerning security, this is a quite critical operation that is usually not carried out in a trusted environment like a personalization centre or sales office as known from PT object. The mobile service concept requires that it shall be possible to conduct this operation at any location where the user can connect to the mobile network. Therefore a non-secure environment has to be assumed where attacks on the transaction can’t be excluded.<br>Typically, a trusted service manager (TSM) provides these services on behalf of the TSP. The TSP’s online portal will e.g. link the customer to the TSM’s system.<br>This Use Case has to be performed before loading and management of entitlements, ID or tokens can be carried out. | | |
| | PT object: | NMD | NMD mode: | Over-the-air |
| | Infrastructure: | 1. Online service and ticket portal (linking to the TSM’s system) | | |
| | Requirements: | 1. Availability of external or built-in secure storage (eSE, UICC, µSD) for TSP’s applet, credentials and customer’s entitlements, check-in-data etc.<br>2. Drivers etc. officially supported by the OS, NMD vendor.<br>3. Availability of an open, interoperable trusted service for initialization and management of the secure storage<br>4. Contractual relationship and operational / technical interfaces between Trusted service manager (TSM) and TSP established<br>5. Open protocol that supports secure authentication, communication and installation over-the-air (GlobalPlatform, ISO7816) | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Mandatory | | |

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-B.3-3** | Use case "**Purchasing and management of entitlements over-the-air** " | | | |
| | Description: | The PT customer uses his personal account at the TSP's online service and ticket portal to purchase or change entitlements. Entitlements are loaded or managed over-the-air and kept in the secure storage of the NMD.<br>This Use Case prepares the NMD for use as PT object. | | |
| | PT object: | 1. NMD | NMD mode: | 1. Over-the-air |
| | Infrastructure: | 1. Online service and ticket portal | | |
| | Preconditions: | 1. Secure storage of the NMD prepared according to B.2-3<br>2. Purchase or management process (incl. payment, refund) completed | | |
| | Requirements: | 1. Availability of external or built-in secure storage (eSE, UICC, µSD)<br>2. Secure communication between secure storage of the NMD and the TSP's online service and ticket portal respectively the TSM's system. | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations:<br>– Mandatory for system approaches working with entitlements or tokens<br>– Not necessary if ID-based ticketing or payment-centric schemes are used. | | |
| **UC-B.3-4** | Use case "**Payment** " | | | |
| | Description: | Payment is an integral part of the purchasing process. Payment may be conducted by bank account-related debiting schemes that are established by the customer when opening the customer account (see chapter 3.3). Alternatives that can be supported by NMD are:<br>1. As first alternative, the NMD could be used to connect a contactless payment card to the TSP's online service and ticket portal and conduct payment for entitlements. The entitlement would be handled as described in UC-B.3-3. For EMVCo-conformant payment cards this has to be seen as a future option that depends on the progress of the related specification work in EMVCo.<br>2. As second alternative, a payment function that is stored in the NMD could be used (e.g. provided by a wallet) to pay for purchases on the TSP's online service and ticket portal. This option requires sufficient and approved protection in the NMD's system architecture for PIN or passwords that have to be entered by the user via the NMD's keyboard or biometric data that comes from e.g. the fingerprint sensor of the NMD. This is currently not generally provided. Therefore this option should not be used for online-payments. It may be used at the PoS (e.g. the service center or a ticket machine) if the PIN or password are entered at the PoS-reader. | | |
| | PT object: | 1. Contactless payment card<br>2. NMD with | NMD mode: | 1. "Over-the-air" for online connection to TSP's online portal and "NFC reader mode" for communication of NMD with |

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| | | payment application | | contactless payment card<br>2. Use of a payment application of the NMD "Over-the-air" |
| | Infrastructure: | 1. Online service and ticket portal | | |
| | Requirements: | 1. The use of an NMD-internal payment application requires special protection for PIN or passwords that potentially have to be entered by the user via the NMD's keyboard.<br>2. NMD in NFC reader mode has to be interoperable with contactless payment cards | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Optional, depending on system-specific concept for payment | | |

*Table 5: Relevant Use Cases of the NMD process B.3 "Mobile sales and maintenance"*

### 4.3.5 NMD process B.4 “Personal Point of Sales”

The process is described in chapter 3.3.5. It includes the following Use Cases.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-B.4-1** | Use case “**Loading application software onto the NMD**” | | | |
| | Description: | See UC-A.2-1 | | |
| | PT object: | See UC-A.2-1 | NMD mode: | See UC-A.2-1 |
| | Infrastructure: | See UC-A.2-1 | | |
| | Requirements: | See UC-A.2-1 | | |
| | Relevance: | See UC-A.2-1 | | |
| **UC-B.4-2** | Use case “**Purchasing and management of entitlements on the PT object**” | | | |
| | Description: | The PT customer uses his personal account on the TSP’s online service and ticket portal to purchase or change entitlements or tickets.<br>Entitlements are kept in the customer’s PT object and loaded or managed via the NFC-interface of the NMD. The NMD establishes a transparent connection between the PT object and the TSP’s online service and ticket portal for this purpose. | | |
| | PT object: | 1. PT object | NMD mode: | 1. “Over-the-air” for online connection to portal, “NFC reader mode” for communication of NMD with PT object |
| | Infrastructure: | 1. Online service and ticket portal<br>2. PT object | | |
| | Requirements: | 1. NMD in NFC reader mode has to be interoperable with PT object | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations:<br>Mandatory for system approaches that are using PT objects for mobile services and are working with entitlements or tokens<br>Not necessary if ID-based ticketing or payment-centric schemes are used or if PT objects are not used. | | |
| **UC-B.4-3** | Use case “**Payment** ” | | | |
| | Description: | See UC-B.3-4<br>The entitlement would be handled as described in UC-B.4-2. | | |
| | PT object: | See UC-B.3-4 | NMD mode: | See UC-B.3-4 |
| | Infrastructure: | See UC-B.3-4 | | |
| | Requirements: | See UC-B.3-4 | | |
| | Relevance: | See UC-B.3-4 | | |

*Table 6: Relevant Use Cases of the NMD process B.4 “Personal point of sales”*

### 4.3.6 NMD process C.1 “PT object”

The process is described in chapter 3.3.6. It includes the following Use Cases.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-C.1-1** | Use case “**Ticket validation, check-in / check-out**” | | | |
| | Description: | The PT customer uses his NMD as the PT object for ticket validation.<br>The PT customer uses his NMD as PT object when entering the gated area of the station or the vehicle. The following cases have to be distinguished:<br>1. When using a classical ticket product or a token:<br>– The inspection infrastructure reads the ticket from the NMD, validates the ticket, writes the result back to the NMD and allows entry.<br>2. When using an AFC-product:<br>– The inspection infrastructure reads the entitlement from the NMD, performs validation and check-in. The check-in information is stored in the NMD.<br>– At the destination, the inspection infrastructure reads the check-in information from the NMD and allows exit. The check-in and check-out information will be sent by the inspection infrastructure to the TSP’s AFC-back office system. This completes the customer’s check-out. The AFC-system (or the stationary inspection infrastructure) closes the journey, calculates the fare and initiates billing.<br>3. When using ID-based ticketing:<br>– The inspection infrastructure reads the ID from the NMD, validates the ID, writes the result back to the back-office and allows entry. If the system architecture supports distribution of valid IDs to the readers, the validation can be carried out by the local inspection infrastructure. The back-office will be informed about the outcome of the validation.<br>4. When using payment-centric ticketing:<br>– The inspection infrastructure performs a payment transaction, writes the result back to the back-office and allows entry. | | |
| | PT object: | 1. NMD | NMD modes: | 1. NFC card emulation mode |
| | Infrastructure: | 1. Stationary inspection infrastructure | | |
| | Requirements: | 1. Availability of external or built-in secure storage (eSE, UICC, µSD)<br>2. NMD in NFC card emulation mode has to be interoperable with stationary inspection infrastructure<br>3. Very high requirements to NMD’s transaction time. Complete process from presenting the NMD to the reader until granting of access may not take longer than with a PT object.<br>4. NMD shall function as specified also in “Battery low mode” which is defined in [TS.26] | | |
| | Relevance: | Relevance for NMD: Mandatory | | |

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| | | Relevance for PT system implementations: Only the system-specific ticketing approach and the offered products have to be supported. | | |
| **UC-C.1-2** | Use Case "**Mobile inspection**" | | | |
| | Description: | Inspection of the customer's entitlement and check-in data may be carried out in the vehicle by a conductor or revenue inspector.<br>The conductor or revenue inspector uses a mobile inspection device to read the data from the NMD via the NFC-interface. | | |
| | PT object: | 1. NMD | NMD mode: | 1. NFC card emulation mode |
| | Infrastructure: | 1. Mobile inspection infrastructure | | |
| | Requirements: | 1. Availability of external or built-in secure storage (eSE, UICC, µSD)<br>2. NMD in NFC card emulation mode has to be interoperable with mobile inspection readers as described in chapter 4.2.1.<br>3. NMD shall function as specified also in "Battery low mode" which is defined in [TS.26] | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Only if mobile inspection is in place. | | |

*Table 7: Relevant Use Cases of the NMD process C.1 "PT object"*

### 4.3.7 NMD process C.2 “Check-in / check-out with passive infrastructure”

The process is described in chapter 3.3.7. It includes the following Use Cases.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-C.2-1** | Use case “**Check-in or check-out**” | | | |
| | Description: | The NMD is used as the PT customer’s PT object.<br>When starting the journey, the customer reads the location information from a passive local tag by using his NMD in reader mode. This information will be sent by the NMD over-the-air to the TSP’s AFC-back office system. After processing the location data and validating the customer’s entitlement, the AFC-system generates a check-in confirmation which is stored in the secure storage of the customers NMD. With this the customer’s check-in is completed.<br>At the destination, the customer again reads the location information from a passive local tag. This information will also be sent from the NMD over-the-air to the TSP’s AFC-back office system. This completes the customer’s check-out. The AFC-system closes the journey, calculates the fare and initiates billing. | | |
| | PT object: | 1. NMD | NMD modes: | 1. “NFC reader mode” for reading tags and “Over-the-air” for connecting to the TSP’s AFC-system |
| | Infrastructure: | 1. Tag infrastructure | | |
| | Requirements: | 1. Availability of external or built-in secure storage (eSE, UICC, µSD)<br>2. NMD in NFC reader mode has to be interoperable with NFC tag infrastructure as described in chapter 4.2.1. | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Only system-specific ticketing approach and products have to be supported. | | |
| **UC-C.2-2** | Use case “**Mobile inspection**” | | | |
| | Description: | See UC-C.1-2 | | |
| | PT object: | See UC-C.1-2 | NMD mode: | See UC-C.1-2 |
| | Infrastructure: | See UC-C.1-2 | | |
| | Requirements: | See UC-C.1-2 | | |
| | Relevance: | See UC-C.1-2 | | |

*Table 8: Relevant Use Cases of the NMD process C.2 “Check-in / check-out with passive infrastructure”*

### 4.3.8 NMD process C.3 “Reading tag information”

The process is described in chapter 3.3.8. It includes the following Use Cases.

| No. | Use case / *Description* | | | |
|---|---|---|---|---|
| **UC-C.3-1** | Use case “**Reading tag information**” | | | |
| | Description: | This Use Case covers the use of NFC tags that link to information about PT services, to the TSP’s ticket portal etc.<br>The customer taps his NMD to the NFC tag that may be mounted at the platform, the bus stop etc. The NMD reads the information from the tag by using the NFC Data Exchange Format (NDEF) and the TSP’s application software. | | |
| | PT object: | 1. NMD | NMD modes: | 1. NFC reader mode |
| | Infrastructure: | 1. Tag infrastructure as described in chapter 4.2.1. | | |
| | Requirements: | 1. NMD in NFC reader mode has to be interoperable with the Tag infrastructure | | |
| | Relevance: | Relevance for NMD: Mandatory<br>Relevance for PT system implementations: Only if a tag infrastructure is in place. | | |

*Table 9: Relevant Use Cases for the NMD process C.3 “Reading tag information”*

# 5 Identification of relevant interoperability parameters

## 5.1 Interoperability of the contactless interface

The NMD communicates via its NFC-interface in reader mode, in card emulation mode or in peer-to-peer mode. Depending on the Use Case (see chapter 3), the boundary conditions for the information exchange between NMD and the PT-reader, the PT object or an NFC-tag can vary considerably.

The communication between NMD and NFC-tags will not be investigated because current NFC Forum implementation and test specifications cover this mode already. Peer-to-peer mode is not used in PT Use Cases and is therefore not considered in this document.

Globally, the majority of existing PT infrastructures and PT objects are following ISO/IEC14443, ISO/IEC18092 or EMVCo L1 standards for the contactless interface. An NMD should support interoperability with all these standards in order to provide the flexibility to be used in any PT infrastructure worldwide.

The requirements of the NMD's contactless interface in a PT infrastructure depend to a large degree on the parameters of the PT readers and PT object that communicate with the NMD. Chapter 4.2 provides an overview of the PT infrastructures. For each of these infrastructures we can assume specific implementations for the contactless interface.

### 5.1.1 NMD in card emulation mode

#### 5.1.1.1 Relevant combinations of NMD and contactless infrastructures

The following table shows the Use Cases that involve NMD in card emulation mode. The last column "Assessment of relevance" provides an assessment as to whether a Use Case or a particular scenario of a Use Case is needed for conducting the PT business process. If not, the particular combination of NMD and PT infrastructure (e.g. NMD and customer home infrastructure) doesn't have to be considered for interoperability between the NMD's contactless interface and the contactless interface of this infrastructure category.

| Use case | Infrastructure category | Assessment on relevance |
|---|---|---|
| **UC – B.1-1 "Management of the secure storage via the NFC interface"** | Stationary sales infrastructure | **Mandatory** for initialization and as fallback option if OTA-management isn't available |
| **UC- B.1-2 "Loading and management of entitlements via the NFC interface "** | 1. Stationary sales infrastructure<br>2. Mobile inspection infrastructure | Entitlements will usually be loaded and managed over-the-air. The use of the stationary sales or mobile inspection infrastructure is **mandatory** as fallback option if OTA-management isn't available. |
| | 3. Customer home infrastructure | **Optional,** probably redundant. Entitlements will usually be loaded and managed over-the-air. Fallback via stationary sales infrastructure should be sufficient. |
| **UC-C.1-1 "Ticket validation, check-in / check-out"** | Stationary inspection infrastructure | **Mandatory** (if used) |
| **UC-C.1-2 "Mobile inspection"** | Mobile inspection infrastructure | **Mandatory** (if used) |

*Table 10: Relevance of Use Cases involving NMD in card emulation mode*

As a result of these considerations, the following infrastructure categories have to be considered for interoperability between the contactless interfaces of NFC Mobile devices and the contactless PT infrastructures:

1. Stationary sales infrastructure
2. Stationary inspection infrastructure
3. Mobile inspection infrastructure

Support for "Customer home infrastructure" is optional.

#### 5.1.1.2 Relevant parameters for interoperability of NMD in card emulation mode

In NFC card emulation mode, the NFC Mobile device communicates with the different categories of contactless PT infrastructures according to chapter 4.2. The following table gives an overview on the parameters that are relevant for interoperability of the contactless interface between these PT reader infrastructures and the NMD in card emulation mode:

| PT infrastructure | Description | Relevant reader parameters |
|---|---|---|
| **Stationary sales infrastructure** | **Contactless readers** deployed in customer service centres, vending machines and information terminals. | – Operating distance: 0 to min. 5mm<br>– Antenna size: Class 1 down to Class 3. In some cases larger than class 1<br>– EMD protection required<br>– RF- standards: EMVCo L1, ISO/IEC14443 (or CEN/TS 16794) or ISO/IEC18092 / NFCF Type F |
| **Mobile inspection readers** | **Contactless readers** in mobile control devices that are used by conductors and mobile revenue inspectors | – Operating distance: 0 to min. 5mm<br>– Antenna size: Class 3 or Class 1<br>– EMD protection required<br>– RF- standards: EMVCo L1, ISO/IEC14443 (or CEN/TS 16794) or ISO/IEC18092 / NFCF Type F |
| **Stationary inspection infrastructure** | **Contactless readers** integrated into gate systems, check-in/check-out-readers in stations or vehicles. | – Operating distance: 0 to min. 20mm<br>– Antenna size: Class 1 or larger<br>– EMD protection required<br>– Performance: very high transaction rate<br>– RF- standards: EMVCo L1, ISO/IEC14443 (or CEN/TS 16794) or ISO/IEC18092 / NFCF Type F |
| **Customer home infrastructure** | **Contactless readers** connected to the customer's home IT (PC) | – Operating distance: 0 to min. 5mm<br>– Antenna size: Class 6 to Class 1<br>– EMD protection required<br>– RF- standards: EMVCo L1, ISO/IEC14443 (or CEN/TS 16794) or ISO/IEC18092 / NFCF Type F |

*Table 11: Interoperability parameters for contactless PT infrastructures*

Table 11 shows that contactless PT readers used for stationary sales and mobile inspection have similar characteristics. Customer home infrastructures deviate only in terms of antenna size but don't have to be considered according to the results of chapter 5.1.1.1. Parameters of readers used in stationary inspection infrastructures differ significantly.

### 5.1.1.3 Conclusions for interoperability between NMD and PT readers

The PT infrastructures that may interact with the NMD via the contactless interface have been identified in chapter 5.1.1.1. Assumptions concerning the relevant parameters of the contactless interfaces of these PT infrastructures have been documented in chapter 0.

Chapter 5.1.1.1 shows that only the "customer home infrastructure" can be considered as not relevant. All other PT infrastructure categories and related parameters of the contactless interface need to be considered for interoperability with the NMD. This leads to the conclusion that PT reader antennas which are smaller than "Class 3"-size don't have to be taken into account for interoperability between NMD and PT readers.

Therefore the NMD's contactless interface has to support the following parameter settings at the PT reader. Implementation and test specifications for NMD have to cover these parameter settings on the PT reader.

| PT reader parameter | Value | Relevance |
|---|---|---|
| **Antenna size of PT reader**[2] | 1. Class 3, Class 1 or larger<br>2. Smaller than Class 3-size | 1. Mandatory<br>2. Optional |
| **Operating distance** | 1. 0 to min. 20 mm for Class 1 or larger reader antennas<br>2. 0 to min. 5 mm for Class 3 or Class 1 reader antennas<br>3. 0 to min. 5 mm for reader antennas smaller than Class 3-size | 1. Mandatory<br>2. Mandatory<br>3. Optional |
| **Performance** | Very high (fast transaction speed) | Mandatory |
| **RF- standards** | EMVCo L1 and ISO/IEC14443 (or CEN/TS 16794) and ISO/IEC18092 / NFCF Type F (as required by the specific PT reader). | Mandatory |
| **Operations in "Battery Low Mode"of the NMD** | All functions necessary for support of UC-C.1-1 and UC-C.1-2 have to work also in "Battery Low Mode"[3] of the NMD. | Mandatory |

*Table 12: Relevant parameter values for the contactless interface of NMD in card emulation mode*

[2] There is no requirement in ISO/IEC 14443 and CEN/TS 16794 relating to PT reader antenna size. PT reader manufacturers remain free to opt for the antenna design of their choice as long as the readers are able to accept PICC Class 1, 2 or 3.

[3] "Battery Low Mode" is defined in [TS.26]

### 5.1.2 NMD in reader mode

#### 5.1.2.1 Relevant combinations of NMD and contactless cards, tags and media

The following table shows the Use Cases that involve NMD in reader mode. The last column "Assessment of relevance" provides an assessment if a Use Case or a particular scenario of a Use Case is needed for conducting the PT business process. If not, the particular combination of NMD and PT card, media or tag doesn't have to be considered for interoperability of the NMD's contactless interface.

| Use case | Card, media or tag | Assessment on relevance |
|---|---|---|
| **UC – A.2-2 "Creating the personal account via NMD and contactless eID"** | eID card | **Mandatory** (if used) for support of the "mobile service life cycle" |
| **UC- A.2-3 "Authorization of direct debiting schemes via NMD and contactless eID"** | eID card | **Mandatory** (if used) Brings substantial benefits for TSP and customer. |
| **UC- A.2-4, UC-B2.2 "Sign-on to the personal account via NMD"** | 1. eID card<br>2. Authentication media | **Mandatory** (if used) |
| **UC- B.2-1 "Setup of the authentication mechanism"** | 1. PT object<br>2. eID card with authentication function<br>3. authentication media | **Mandatory** (if used) |
| **UC- B.3-4, UC-B4.3 "Payment"** | Contactless payment card | **Mandatory** (if used) |
| **UC- B.4-2 "Purchasing and management of entitlements "** | PT object | **Mandatory** |
| **UC-C.2-1 "Check-in or check-out"** | Tag infrastructure | **Mandatory** |
| **UC-C.3-1 "Reading tag information"** | Tag infrastructure | **Mandatory** |

*Table 13: Relevance of Use Cases involving NMD in reader mode*

As a result from these considerations, the following cards, media and tag infrastructures have to be considered for interoperability between the contactless interfaces of NFC Mobile devices and the contactless PT infrastructures:

1. PT object
2. Contactless payment cards
3. eID-cards and authentication media
4. Tag infrastructure

#### 5.1.2.2 Relevant parameters for interoperability of the contactless interfaces

In NFC reader mode NMD could potentially interact with the categories of contactless cards, tags and media that are described in chapter 4.2. The following table gives an overview of the parameters that are relevant for interoperability of the contactless interface between these cards, tags and media and the NMD in reader mode:

| PT infrastructure | Description | Relevant object parameters |
|---|---|---|
| **PT objects** | **Contactless cards or tokens** used as PT object by the PT customer | – All type of antenna size: PICC Classes[4] from 1 down to 6 have to be considered<br>– EMD limitation potentially required<br>– RF- standards: EMVCo L1, ISO/IEC14443 (or CEN/TS 17964) or ISO/IEC18092 / NFCF Type F |
| **Contactless payment cards** | Contactless cards for payment purposes (e.g. contactless credit cards) | – Antenna size: PICC Classes from 1 down to 6 have to be considered<br>– RF- standards: EMVCo L1 or ISO/IEC18092 / NFCF Type F |
| **eID- cards and authentication media** | Personal eID- or authentication media | – Antenna size: PICC classes 1 down to 6<br>– EMD limitation required<br>– RF- standards: ISO/IEC14443, ISO/IEC18092 |
| **Tag infrastructure** | NFC Forum – conformant or ISO/IEC14443 tags | – NFC-Forum tags: According to NFC Forum tag specifications type 1-4<br>– ISO/IEC14443-conformant tag infrastructures:<br>o Antenna size: PICC classes 1 - 6<br>– Tags often mounted behind e.g. plexiglas panes. This cover material needs to be included in testing and certification of the tag. |

*Table 14: Interoperability parameters for the contactless card or token interface per infrastructure*

Interoperability between NFC mobile devices and NFC Forum-conformant Tag infrastructures should be given by NFC Forum standards and testing.

[4] „PICC classes“ are defined in ISO/IEC14443. In this case, the term shall also cover antennas with similar size and electrical behavior of contactless objects that are following other RF standards.

#### 5.1.2.3 Conclusions for interoperability between NMD and PT cards, tags and media

In reader mode, the NMD's contactless interface has to support contactless objects (cards, tags and media) with the following parameters. Implementation and test specifications for interoperability between NMD and PT objects have to cover these parameter settings.

| PT object parameter | Relevant values for PT objects | Relevance |
|---|---|---|
| **Antenna size** | PICC Classes 1,2 & 3<br>PICC not claiming compliance to a class<br>PICC Classes 4,5 & 6 | Mandatory<br>Mandatory<br>Not currently used[5] |
| **Operating distance** | In all Use Cases where the NMD is operated in reader mode, the contactless PT object will be put on the NMD or the customer taps with his NMD on the NFC tag. For these cases the NMD is in direct contact with the contactless card or media. Therefore the typical required operating distance is close to 0 mm.<br>The distance between the NMD in reader mode and the contactless object increases if NFC tags are mounted behind Plexiglas. For such cases the material and thickness of the pane has to be included in testing and certification of the tag.<br>For functional safety reasons a margin should be provided. Therefore the NMD in reader mode should cover operating distance between 0 and 5 mm. | Mandatory |
| **EMD** | Limitation required → requires support of EMD feature by NMD in reader mode | Mandatory |
| **RF-standards** | EMVCo L1 and ISO/IEC14443 (or CEN/TS16794) and ISO/IEC18092 / NFCF Type F | Mandatory |

*Table 15: Relevant parameters values for the contactless interface of NMD in reader mode*

[5] PICC not claiming compliance to a class are tested as for Class 1 for load modulation and as for Class 1 or 2 or 3 depending on their antenna size for field strength and loading effect. Acceptance of PICC Classes 4, 5 & 6 can be achieved by not claiming compliance to a class for such PICCs.

END of DOCUMENT