Management and Use of Identities in Mobility and Transport

Market Requirements Document

NFC Forum™

Version 1.0.0 / 2020-04-28

Mobility, Identity and Transport SIG

This document is copyright © 2020 by the NFC Forum.

All rights reserved by the NFC Forum.

Contents

1 Introduction

Identities which represent and identify natural persons, organizations or technical components in the digital world are also of increasing relevance in mobility and transport.

In the past, seamless travel was often limited to local or regional transport ticketing schemes which supported mainly public transportation. Today, multi-modal travel and Mobility-as-a-Service (MaaS) is a major global trend. Customers demand transport service offers that include all legs from the start of the journey to the final destination including the first and last mile. In addition to public transport services, modes of transportation like taxi, car rental or car sharing, bikes, scooters or ride sharing have to be supported.

A system solution that supports MaaS, the mobility platform, has to integrate a variety of modes of transportation and the related service operators and it has to support not only fare management and payment but also end-to-end journey planning, traveler guidance throughout the journey and validation of entitlements. This leads to some important consequences:

1. Only the smartphone is capable to support all these applications and is by this the only practical customer medium for MaaS. Customer media like contactless chipcards are limited to classical eTicketing.
2. A consistent ID concept is required to link all modes of transportation and the related systems for a seamless travel experience.
3. MaaS requires support of new use cases by the NFC interface such as gathering trustworthy ID information from governmental documents and tag reading for traveler guidance.

This document describes business processes and use cases which support a consistent ID concept for use in system solutions for MaaS and names requirements to NFC mobile devices which may result from these use cases.

1.1 Applicable Documents or References

Document	Short name	Version / date	Issuer
Documentation of Use Cases for NFC Mobile Devices in Mobility and Transport	PT NFC use cases	Version 1.7.3 / 2015-06-19	NFC Forum
ISO/IEC 24760-1- A framework for identity management – Part1: Terminology and concepts	ISO 24760-1		ISO
ISO 24014-1, edition 3	ISO 24014-1		ISO
NFC Handset Requirements	[TS.26]	Version 14.0, XX Jul 2019	GSMA
REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN	[eIDAS]		European Union

Document	Short name	Version / date	Issuer
COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32015R1502	[IMP_eIDAS]		European Union

1.2 Administration

The NFC Forum Data Exchange Format Specification is an open specification supported by the Near Field Communication Forum, Inc., located at:

401 Edgewater Place, Suite 600
Wakefield, MA, 01880

Tel.: +1 781-876-8955
Fax: +1 781-224-1239

http://www.nfc-forum.org/

The transport working group maintains this document.

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 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 color 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 Intellectual Property

The document conforms to the Intellectual Property guidelines specified in the NFC Forum's Intellectual Property Right Policy, as approved on November 9, 2004 and outlined in the NFC Forum Rules of Procedures, as approved on December 17, 2004.

1.6 Abbreviations

eSE	Embedded Secure Element
ID	Identity
IDF	Identifier
IFMS	Interoperable Fare Management System
MaaS	Mobility as a Service
NFCF	NFC Forum
MPO	Mobility Platform Operator
NMD	NFC Mobile Device
PT	Public Transport
SE	Secure Element
TSO	Transport Service Operator
TSP	Transport Service Providers
USP	Unique Selling Proposition

1.7 Revision History

Version	Description of update or change	Date	Author
0.1	First draft of document structure	June 9th, 2019	C. Bartels
0.2	Update after kick-off call	June 14th, 2019	C. Bartels
0.3	Update after 1st comments	June 20th, 2019	C. Bartels
0.4.1	Revision after Stuttgart MIT SIG meeting	Oct 22nd, 2019	C. Bartels
0.5.1	Update after WI team call on Oct 23rd	Nov 5th, 2019	C. Bartels
0.5.2	Update after MIT SIG meeting Singapore	Nov 7th, 2019	C. Bartels
0.5.3	Update after MIT SIG call on Dec 12th		S. Shibata
1.0.0	Updated ONLY the VERSION/Date to Version 1.0.0 / 2020-04-28	Apr 28th, 2020	P. Khemani

2 Purpose of this document

This document describes business processes and use cases that demonstrate how Transport Service Providers and Mobility Platform Operators may act as providers of trustworthy identities.

This includes:

1. the generation of identities and identifiers for customers, customer media and applications which are specifically designed for PT and MaaS-purposes,
2. the consolidation of existing customer identities in order to achieve a defined level of trust,
3. the enhancement of existing sets of customer ID attributes according to the needs of certain modes of transportation (e.g. validity of the customer's driver license for car rental or car sharing),
4. the maintenance and management of identities and related attributes,
5. the provisioning of identities and ID attributes for use by partners of the mobility platform and other transport service providers.

3 Introduction to identity management in mobility and transport

Identity information is the link that connects the various modes of transportation and their service operators in order to support MaaS and enable a seamless multi-leg and multi-modal journey for the Customer. These identities must be available to the involved Partners who operate the various transportation and mobility services and they must be trustworthy to gain acceptance by the involved Partners.

Especially public transport service providers have huge customer data bases available which shall be made available as foundation for ID services which support MaaS.

3.1 Roles

As far as possible, the terms and roles as defined in [ISO 24014-1] and [ISO 24760-1] shall be used for the Mobility and Transport domain.

The term "Identity provider" as defined in [ISO 24014-1]) may be used instead the term "Identify information provider" as defined in [ISO 24760-1]. In this document, the term "Identity provider" is references the [ISO 24760-1] roles "Identify information provider" and also "Identify information authority" in the mobility and transport domains.

In addition, the following roles are defined for the purpose of this document:

Partner	Organization which cooperates with Identity Provider's organization in the area of MaaS or other services. The Partner provides own mobility or other services and uses the transport organizations customer media and the MaaS ID service.
Transport Service Provider	Organization that offers and operates transport services. For interoperable fare management systems, this role would be covered by the IFM-Manager and his delegated roles.

3.2 Definition of general identity terms and used identities

As far as possible, the terms as defined in [ISO 24760-1] shall be used for terms in identity management e.g.:

Entity	Item (person, organization, device etc.) that has recognizably distinct existence and may be identified.
Identity	Set of attributes related to an entity
Identity information	Set of values of attributes optionally with any associated metadata in an identity. Note: In an IT system an identity is present as identity information.
Identifier	Identity information that unambiguously distinguishes one entity from another
Attribute	Characteristic or property of an entity that can be used to describe its state, appearance, or other aspects (e.g. entity type, address information, telephone number)

The following terms are specifically defined for the purposes of this document:

Derived eID	ID attributes which are derived from governmental or other external eID by using an unidirectional algorithm. They represent these external eID for the purposes of the identity provider's service.
eID	Electronic identity card or application. Typically issued by governments or their representatives. Typically provides a defined level of trust.
IDc	Customer identity. Defined and issued by the Identity provider. May be derived from a governmental eID document or identity information obtained from an external trust service.
IDc attributes	Attributes which are related to the IDc
IDx	Identity of customer media issued by the Media or Application retailer. Any customer media or applications identity must be uniquely identified by an identifier and may have a set of additional attributes.

ISO/IEC 24760-1supports the definition of identities not only per entity but also per market domain. This means that a specific person may have different ID with a different selection of attributes e.g. for payment, for governmental purposes and for mobility and transport services. In this example, the role "Identity Provider" includes the [ISO 24760-1] roles "Identify information provider" and also "Identify information authority" for the mobility and transport domain.

The customer identity IDc is specifically designed for the mobility and transport domain. It is generated and maintained by the Identity Provider and includes attributes which are required for the mobility services of the transport organization and its external Partners. These attributes include the name, address and payment data as in most other application areas. In addition, there may be attributes that are specific to transport: It may be useful to include an attribute that informs if the customer is eligible for special fare discounts or needs assistance when travelling. For mobility services it would be instrumental to include an attribute that provides a trustworthy information if the Customer has a valid driver license. In both examples, the attributes may not be managed by the customer for security reasons. Instead, there needs to be a trustworthy external source of information and a frequent synchronization with these sources.

Error! Reference source not found. provides an example for a customer identity IDc which is specifically designed for the mobility market.

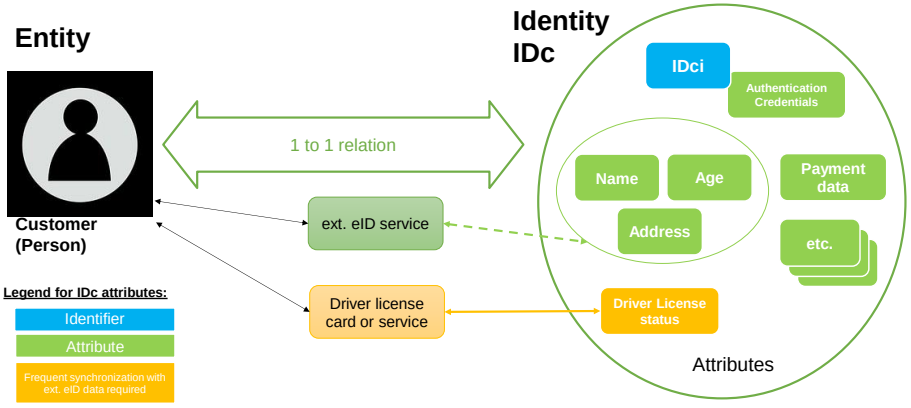

Figure 1: Example for a mobility-specific customer identity IDc

Not only the Customer but also the customer media can be characterized by an identity and its particular attributes. The identity IDx are typically generated and maintained by the transport organization. The attributes include at least on identifier and typically also credentials that support authentication and identification of the customer media.

The Customer shall be able to manage his IDc and connect or disconnect his customer media to or from his IDc via his online account. If disconnected, an anonymous use of the customer media is supported.

Figure 2 provides an example how MaaS-specific customer identities IDc and media identities IDx can be implemented and connected.

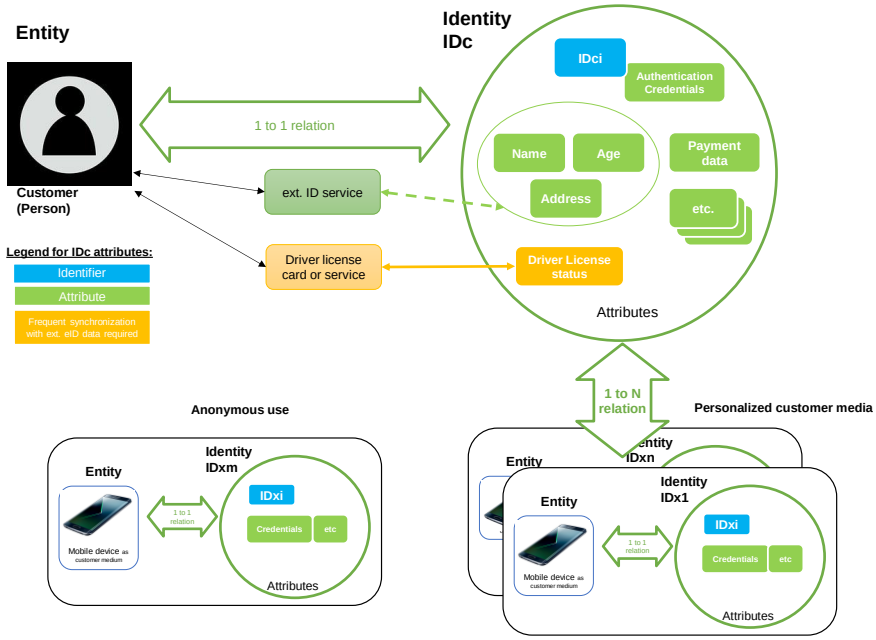

Figure 2: Identities for mobility and transport (MaaS-identities)

4 Documentation of identity management business processes

4.1 Identification of the business processes

The following business processes cover the core life cycles of the ID service solution. They are essential for the implementation and operation of the trustworthy MaaS ID service:

1. Definition, implementation and maintenance of the ID service

   This business process includes all activities that are necessary to define, establish and maintain an ID service which is based on internal customer data and that supports internal and external Partners to operate MaaS.

2. Partner life cycle management

   For the implementation of the ID service, 2 types of partners must be considered:

   a. Partners who are using the ID service's trustworthy identity information for MaaS or other purposes.

   b. External Identity Providers who are sources of trustworthy values for ID attributes.

   In both cases, the entire life-cycle of the relationship from "establishing the partnership" via "daily operations" to "terminating the partnership" must be covered by defined business processes.

3. Identity management and identity provisioning life cycle

   Business processes for identity management shall ensure that identity information is trustworthy, up to date and according to the needs of the MaaS ID service's clients, the internal and external Partners. In addition, customer rights, privacy and other obligations must be obeyed.

   Identity provisioning addresses the handover of identity information to the internal and external clients of the MaaS ID service. Security aspects and the potential agreements with the specific Partner have to be implemented.

Each of these life cycle processes may consist of several business processes which represent the relevant stages of the particular life cycle. This next level of detail and the relationship between these business processes is shown in Figure 3.

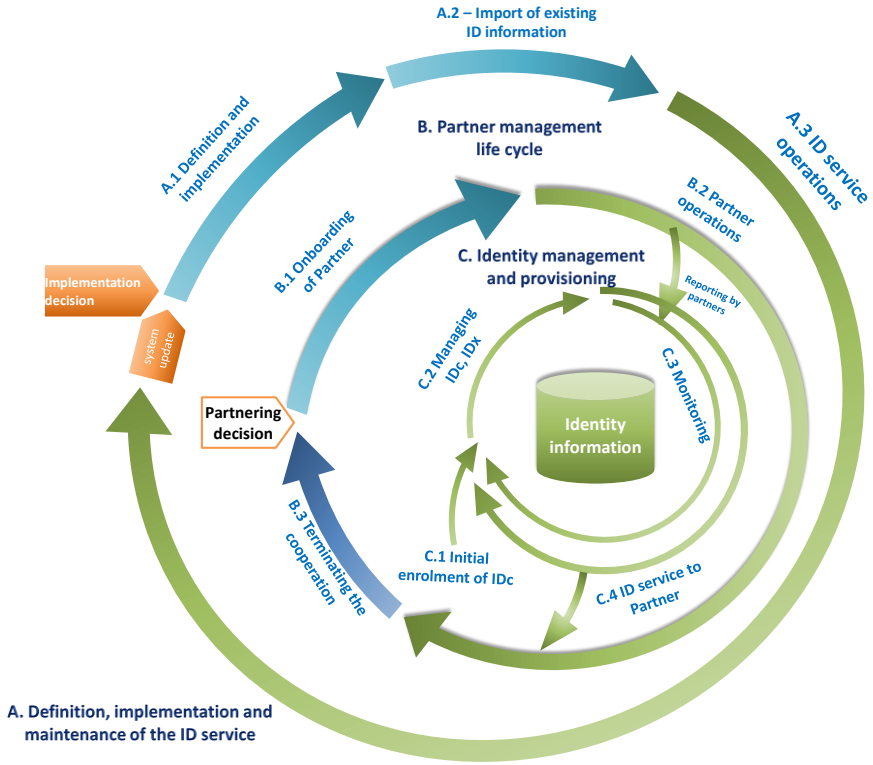

Figure 3 Implementation of life cycle support by business processes

These business processes cover specific functions as Figure 4 shows. These functions may be documented as use cases. The same use case may support more than one business processes.

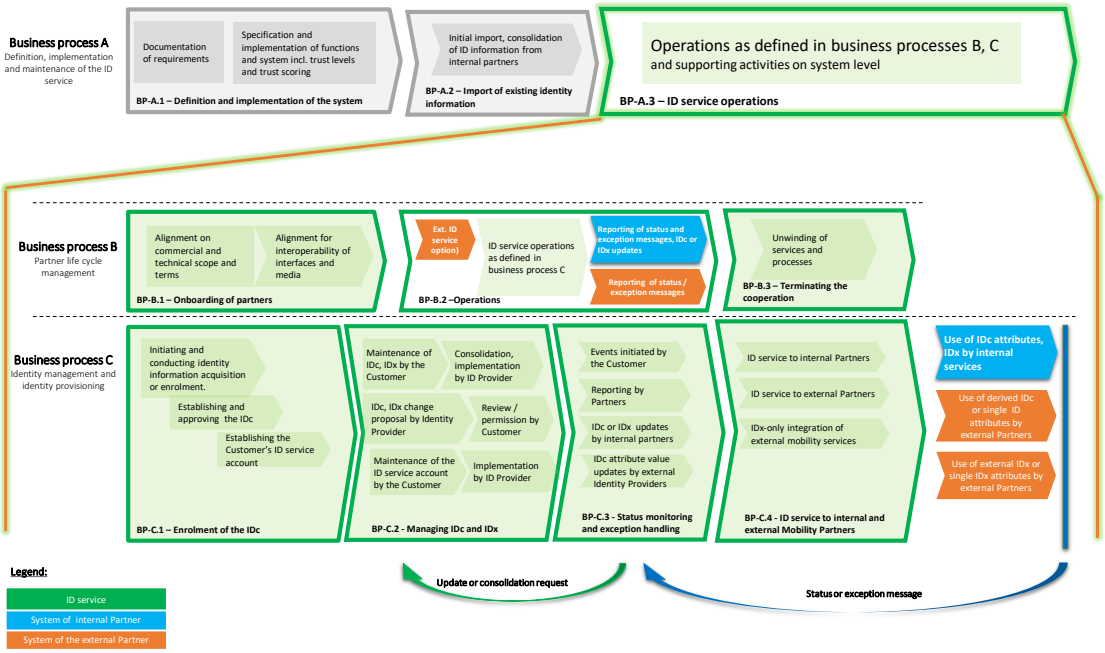

Figure 4: Business processes and supported functions

The business processes shown in Figure 4 are briefly described in the following table.

Business process	Description
BP-A	**Definition, implementation and maintenance of the MaaS ID service**
BP-A.1 – Definition and implementation of the system	This business process includes all activities that are necessary to define and implement an MaaS ID service system which re-uses customer data which is available within the organization as basis for establishing a mobility-specific ID management and that supports internal and external Partners.
BP-A.2 – Import of existing ID and ID attributes	This business processes collects the available customer and media data from the various internal Partners, performs a first consolidation across these sources and generates preliminary identities IDc for Customers and IDx for customer media. On this basis, the Identity Provider can approach the Customers for permission to use the preliminary IDc for purposes of the MaaS ID service. If the Customer agrees, activities according to business process C.1 will follow.
BP-A.3 – ID service operations	The particular activities of the Identity Provider for ID and partner management and operating the MaaS ID service are described in detail by the processes B and C. In addition, this business process includes all supporting activities of the Identity Provider which are not mentioned in B and C but which are necessary to operate the MaaS ID service.

Business process	Description
BP-B	**Partner life cycle management**
BP-B.1 – Onboarding of partners	Establishing cooperation with internal and external partners requires preparations and agreements that cover commercial, operational and technical aspects. This applies for Partners who plan to use the Identity Provider's MaaS ID service and also for Partners like Identity Information Providers or Identity Information Authorities who provide trustworthy values for IDc attributes to the Identity Provider. In particular, the purpose and scope, organizational processes, the supported functions, the required trust level and the technical implementation have to be specified.
BP-B.2 – Operations	This business process includes the daily operations of the cooperation with internal and external clients of the MaaS ID service and external Identity Providers as defined in business process B.1.
BP-B.3 – Terminating the cooperation	This process defines all activities of which have to be conducted if the cooperation between the Identity Provider and a specific Partner comes to an end.
BP-C	**Identity management and identity provisioning**
BP-C.1 – Initial enrolment of the IDc	This process describes the activities which are conducted to generate the Customer's IDc and his ID service account. This process is triggered in the following cases: 1. A preliminary IDc and the Customer's permission to use his identity information are available as result of BP-A.2 2. A new Customer wants to establish a service account with an internal Partner. The identity information which is provided by the Customer for this purpose will be used to establish the IDc. For both cases, the identity information will undergo a consolidation with other data sources and a trust scoring according to the rules which have been defined in BP-A.1. The consolidated information will be included as IDc attribute values and a trust level for the IDc attribute values will be defined. IDx of customer media which belong to this Customer will be connected to this IDc. In a further step, the Identity Provider establishes an online account for the Customer and submits the login credentials to the Customer. As a result of this process, the IDc and the customer online account are established and the Customer may manage his IDc and his IDx via the online account as described in BP-C.2. The internal Partner will rely on the MaaS ID service's IDc for the purposes of his services to this Customer instead of maintaining customer identity information by himself.

Business process	Description
BP-C.2 - Managing IDc and IDx	This business process summarizes all activities of managing the IDc, the IDc attributes and the media-related identities IDx. This may include: – Managing IDc attributes (incl. adding new attributes) – Managing attribute values – Managing and upgrading the trust level of IDc and related attribute values e.g. to qualify the IDc for services with a higher security demand In addition, there shall be processes that enable the Customer to manage his online account and his customer media.
BP-C.3 - IDc, IDx status monitoring, exception handling	This business process addresses the monitoring of the status of all valid identity information and the relations between the identities IDc and IDx. Updates by the Customer as described in BP-C.2 or reports about changes of identity information e.g. from internal Partners will be directed to functions in this process. The same applies if Partners or any other sources reported exceptions like stolen or lost media (IDx) or security incidents which affect the IDc or the IDx. Based on this information, BP-C.3 supports rules and functions that initiate identity management actions which are appropriate for the detected status changes or exceptions. These rules and functions define the core of the identity management process. They have to be defined and maintained by the Identity Provider in the documentation of this process.
BP-C.4 - ID service to internal and external partners	The MaaS ID service may provide all IDc and IDx to internal Partners. The scope agreement with these Partners which is prepared in BP-B.1 defines which data will be provided and what reporting is required from the internal Partner. The MaaS ID service shall be in enabled to provide all types of customer data also to external Partners. However, providing trustworthy customer data to external partners requires specific precautions in order to avoid that security breaches at the Partner's side may infringe the Identity Providers business or his Customers.

Table 1: Overview of business processes

4.2 Description of the business processes

4.2.1 BP-A.1 – Definition and implementation of the system

4.2.1.1 Description

This business process addresses all preparations that are necessary for the implementation of an MaaS ID service system which is based on internal customer data and that supports internal and external Partners.

This includes typically the following activities:

1. Identification of Partners as clients of the MaaS ID service
2. Documentation of requirements to the MaaS ID service and the supporting system
3. Definition of the targeted service portfolio
4. Identification of needed external ID services (e.g. for authorization of internal ID attributes or information on driver license or health insurance status)
5. Definition of the system architecture, the specification of components and interfaces
6. Implementation and test of the system and its interfaces
7. Definition of legal and commercial conditions for the cooperation with Partners and external Identity Providers

The definition of trust levels and the definition of related security measures for the system and components (e.g. for authentication and sign-in to the online account) are essential for an ID service. The goal that existing customer data shall be used requires the development and implementation of a methodology that evaluates and categorizes the level of trust. The respective definitions should be implemented in this business process.

4.2.2 BP-A.2 – Import of existing ID and ID attributes

4.2.2.1 Description

Typically, transport organizations have a strong customer base in their area of operations and a substantial amount of customer data available. Often, this customer data is distributed over several internal departments of the transport organization and managed by each department as required for its specific needs. The consistency across all data bases and trustworthiness of this data is often not exactly defined.

This business processes includes all preparations which are required to make the existing customer data available for the planned MaaS ID service. This includes typically the following steps:

1. Collecting the available customer and media data from the various internal sources i.e. the service providers in transport organization’s internal service providers and media retailers.
2. A first consolidation and consistency check of the data which has been obtained from these sources.
3. Compiling the consolidated customer data into preliminary identity information IDc per Customer.

4. Information about the Customer's IDx will be connected to the preliminary IDc.
5. An estimation of the trust level of the preliminary IDc data set according to the rules which have been defined in BP-A.1.

Since the generation of an IDc by the Identity Provider and its use for an ID service requires the permission of the Customer, the Identity Provider must approach the Customer before introducing the Customer's IDc into the MaaS ID service.

If the Customer agrees, the process continues with BP-C.1. If not, the preliminary IDc has to be deleted.

4.2.3 BP-A.3 – ID service operations

4.2.3.1 Description

This business process covers the regular operation of the MaaS ID service. It can be seen as superior level of the business processes B and C:

1. The particular activities for partner management are described in detail by the business process B,
2. the tasks of the Identity Provider for ID management and operating the MaaS ID service are documented in business process C.

In addition, this business process includes all supporting activities of the Identity Provider which are not mentioned in B and C but which are necessary to operate the MaaS ID service for all Partners and Customers. This may include e.g. quality assurance, security management etc.

4.2.4 BP-B.1 – Onboarding of partners

4.2.4.1 Description

This business process constitutes the first step of the partner management, the establishing cooperation with internal and external partners. This requires preparations and agreements that cover commercial, operational and technical aspects. This applies for both categories of potential partners:

1. Partners who plan to use the Identity Provider's MaaS ID service
2. Other Identity Information Providers or Identity Information Authorities who provide trustworthy values for IDc attributes to the Identity Provider

Typically, the following the following subjects have to be defined as preparation for a cooperation:

1. Scope of the cooperation
2. Legal and commercial conditions
3. Supported functions and services
4. Targeted trust level
5. Technical implementation and related testing
6. Updates and migration planning

7. Operational processes
8. Agreements for seizing the cooperation

External Partners and external Identity Providers may use own back-office technologies or media which deviate from those established by the MaaS ID service. Special measures for implementation of interoperability and a defined security level may be required.

[ISO 24014-1] provides guidance on how to establish partnerships with external Identity Providers and Partners.

4.2.5 BP-B.2 – Operations

4.2.5.1 Description

The particular scope of the cooperation between the Identity Provider and a specific internal or external Partner or an external Identity Provider should be agreed as described in BP-B.1. This business process addresses the daily operation between the particular partner and the Identity Provider.

Business process C contains descriptions of important parts of the cooperation between the Identity Provider and the internal and external partners:

1. The detailed activities for providing the MaaS ID service to internal and external Partners are documented in BP-C.4.
2. Internal Partners can be sources of trustworthy ID information and may be eligible to receive updates of IDc or IDc attributes. This relationship is covered in business processes C.1, C.3 and C.4
3. External Partners should report incidents which are related to the use of identities or media. This is described in C.3.

In addition, this business process includes all supporting activities which are necessary to provide the partner-specific MaaS ID service and to obtain external ID information as defined. This may e.g. include joint maintenance activities, quality and security management etc. [ISO 24014-1] provides guidance on how this can be implemented.

4.2.6 BP-B.3 – Terminating a cooperation

This process defines all activities of the Identity Provider which have to be conducted if the cooperation with an external Identity Provider or an internal or external Partner shall be seized.

The specific rules for seizing the cooperation should be agreed and documented during onboarding (see BP-B.1). The following topics should be considered:

1. There should be a transition period that allows an alternative proposal and timely information to affected customers
2. Confidential data has to be returned to the owner and deleted
3. Equipment which has been used by Partners for e.g. accessing customer media has to be deactivated or returned

4.2.7 BP-C.1 –Enrolment of the IDc

4.2.7.1 Description

The business process C covers all activities of identity management and ID service provisioning according to the rules that have been set up in the business processes A and B. The execution of business process C requires that the ID management system is operational and that the initial import of existing identity information (BP-A.2) was successfully performed.

The business process C.1 describes how the Identity Provider establishes the foundation for Customer-related identity management by generating an identity for a Customer and by collecting all information which is known about this Customer.

The Identity Provider should consider the following scenarios for generating Customer identities IDc and related IDx for use by the MaaS ID service:

1. Business process A.2 describes the initial import of customer information. The Identity Provider collects customer data which is available from internal services as basis for the definition of the IDc and a first set of attributes. If an initial consolidation and trust scoring provides a sufficient result, a preliminary IDc can generated. Based on this information, the Identity Provider approaches the Customer and ask if he would like to benefit from the MaaS ID service.

   The next steps are included in BP C.1: In case of a positive response, the preliminary IDc and IDx would undergo full consolidation from all available sources and a trust scoring. Finally, the IDc and the related IDx would be stored in the MaaS ID system.

2. A Customer has opened an account with an internal Partner. In this process, the Customer will request an identity for MaaS via the ID function which is assumed to be integrated into the Partner's App. The Identity Provider uses the identity information provided by the Customer to generate a preliminary IDc.

Scenario 1 is mainly used for the initial setup of the ID service. The scenario 2 covers daily business after the initial setup has been put in place.

The management of identities of persons and organizations requires that these entities have the option to view, to select and to update their identity information.

In order to support this, the Identity Provider will offer an online account to the Customer, the ID service account. The Customer may use this account to view and maintain his personal IDc attributes. Depending on the applicable legal rules, it may also be necessary to provide the Customer with a function for closing the account and deletion of the IDc or for establishing or blocking certain attributes. The account shall provide following functions to the Customer:

a. View IDc attributes, the related trust level and the services that may be supported by this trust level
b. Add or maintain attributes and maintain attribute values
c. Delete IDc or single attributes
d. Select and de-select targeted services (which may need additional IDc attributes or an update to IDc attributes values in case a higher trust level is required)
e. Connecting customer media to the account and the IDc. The related IDx would be maintained by the Identity Provider.

f. Disconnecting customer media from the account and the IDc by removing the respective identifier IDi / ID1

g. Block customer media (e.g. if stolen or lost)

h. Termination of the IDc and the related account

i. Life cycle management of the login credentials

This availability of this personal ID service account is a prerequisite for the activities in BP-C.2.

4.2.8 BP-C.2 Managing IDc and IDx

4.2.8.1 Description

After the Customer's ID service account is established and the Customer has obtained access, he may add attributes to his IDc, update IDc attribute values like his address or payment data, upgrade the trust level of his IDc, manage his customer media identities IDx or manage his ID service account.

A variety of cases for managing the IDc and the IDx have to be distinguished:

- The Customer initiates the enrolment of a new IDc attribute which may be required for using certain services that he would like to use. An example for such a case is the attribute "Driver license status" which may be required for services like car rental or car sharing.
- The Customer changes the value of an attribute (e.g. because of moving to a new address).
- The Identity Provider may ask the Customer to update a value of an IDc attribute or to upgrade the trust level of his IDc attributes by connecting his governmental ID card or passport as source of attribute values.
- The Identity Provider proposes a new value for an IDc attribute or proposes to connect / disconnect or block an IDx and asks the Customer for permission.

Depending on the required trust level, the Customer may directly enter new values or he has to support reading of trustworthy value from external sources like the governmental ID card.

The Customer should be in the position to manage his customer media via his online account. This includes connecting or disconnecting and also blocking a customer medium.

The activities for managing and maintenance of the Customer's IDc and IDx may be initiated by the Customer or the Identity Provider. The activities are typically carried out by the Customer. If the Identity Provider would like to change attributes or attribute values of the Customer's IDc, he needs permission of the Customer. However, there may be special cases where the Identity Provider should not rely on the Customer if modifications are necessary. This applies in particular if the Customer would have a disadvantage from the change, e.g. if the Customer's student pass expired or his driver license was revoked. For such exceptions, the terms and conditions between Identity Provider and Customer should allow the Identity Provider to perform changes after notification but without the consent of the Customer.

4.2.9 BP-C.3 - IDc, IDx status monitoring, exception handling

4.2.9.1 Purpose of the business process

This business process shall ensure that IDc and IDx and related attributes which are stored by the ID service are trustworthy and up to date.

The maintenance and update of Customer data may be triggered by the Customer, an update or inconsistency message from an internal or an external Partner or an external eID service. Not only updates of IDc attributes and IDx but also the status of identities shall be managed (e.g. in case of blacklisting or restoration of a customer medium).

4.2.9.2 Description

The business process C.3 includes the following categories of activities:

1. Collecting and recording status information about IDc and IDx identities and their attributes.
2. Detect the need for updates of the identity data which is managed by the Identity Provider,
3. Initiating those updates by sending notifications to BP-C.2.
4. Informing MaaS ID service clients about relevant status changes and providing updates according to the agreements with the particular client.

The maintenance and update of customer data in the MaaS ID service may be triggered by various sources:

1. The Customer may use his ID service online account to maintain the values of certain IDc attributes as described in business process C.2. It is important to make sure that the sources of the data update conform to the level of assurance which is targeted for the particular piece of data. This excludes e.g. that the Customer updates his name and address manually if a level “substantial” or “high” is required.
2. The Customer may connect/disconnect a customer medium to his IDc and to block/unblock his customer media via his ID service account.
3. Internal Partners may report changes of their customer data or status changes of the Customer’s card-based IDx which may occur if new media are issued or if old ones are withdrawn or blacklisted.
4. External Partners may report incidents which may have occurred with IDc information or single IDx attributes which were provided by the eID service.

The business process C.3 requires a set of rules that determines which status changes require an action and which specific activities have to be carried out as a response to a particular trigger.

4.2.10 BP-C.4 - ID service to internal and external Partners

4.2.10.1 Description

This business process includes functions that provide the Identity Provider’s IDc and IDx identity information to the internal and external Partners.

The identity information which is provided by the Identity Provider's MaaS ID service may differ from Partner to Partner. The scope and the implementation of the MaaS ID service for a particular client follow the agreements and specifications which have been documented according to BP-B.1.

This process shall enable the Identity Provider to serve the clients of the MaaS ID service in a flexible manner according to their needs and capabilities: Some external Partners may be supported by just sharing uncritical IDx attributes. Other external Partners may also sign-up for a certain set of IDc attributes. Internal Partners will typically obtain original IDc and IDx attributes.

The Identity Provider can rely on the security standards of Partners which are member of the own transport organization but he has only limited influence and insights about the security level of external Partners. Therefore, a special function shall protect the Identity Provider's MaaS ID service from being discredited by security incidents that might happen with external mobility providers. Critical attributes of the IDc or the IDx should typically not be shared with external Partners. Instead, attributes which are not considered sensitive or attributes which are specifically protected should be prepared for the use by external partners.

Another aspect which is to be addressed by this business process is the reporting which is required from internal and external Partners. Typically, Partners should at minimum report all kinds of incidents like stolen or malfunctioning customer media or if IDc attribute values like address or email turned out to be incorrect. There may be individual agreements concerning the scope and the implementation of the reporting per particular client. The details follow the agreements and specifications which have been documented during the on-boarding process BP-B.1.

In addition, there should be functions that track the status of the ID service per client. This is required to generate evidence for the delivered quality of service and may be relevant for billing.

5 Description of use cases, identification of related requirements

5.1 Definitions and scope

This document distinguishes between business processes and use cases.

The term business process is used for the documentation of processes that establish the overall business objectives and reflect the role model as well as organizational, commercial and legal aspects. The business process documentation is independent from the system architecture.

The documentation of use cases describes certain functions or parts of a business process in more detail. In contrast to business processes, use cases establish the technical context for these functions. They include the data flows and the roles of the individual components of the functional architecture of the supporting system. This concept may be used to determine functional requirements to certain architecture components.

A business process may include several use cases. Also, the functions which are described in a use cases may be used in more than one business process.

For the purposes of this document, this chapter will focus on use cases which involve the mobile device's NFC-interface or NFC-enabled tags.

The following selection of basic use cases will be documented:

1. **UC-C.1.1: Initial Identification**

   All communication between the Identity provider and the Customer should be possible online and via the Customer's mobile device. This includes the initial identification of the Customer where the Identity Provider has to make sure that he is in contact with the right person or organization. Such initial online identification solution must support adequate security measures if the Customer's ID service account shall manage MaaS ID with elevated trust levels.

2. **UC-C.2.1: Sign-in to the ID service account**

   The sign-in to the ID service account must support a level of security that matches the targeted elevated trust level of the MaaS ID information which is managed via this account. In practice, "2 factor authentication" with a defined level of assurance as e.g. defined by [eIDAS] and [IMP_eIDAS] is required.

3. **UC-C.2.2: Enrol / update attribute values from trusted sources**

   For elevated trust levels of the identity information it may be required that any influence of the Customer on the IDC attribute value is excluded and the attribute values are directly transferred from a trustworthy source. This applies in particular for attributes where the Customer may have disadvantages in certain scenarios. Examples are the attributes which are representing the status of the Customer's driver license or student card.

   Trusted sources of attribute values are e.g. the Customer's eID card, the Customer's passport or services from external Identity providers which support secure online-updates of the IDc attribute values.

4. **UC-C.2.3: Manage customer media via the ID service account**

   The customer media is the carrier of the identity information which is checked in the verification process across all legs of a MaaS route. The Customer shall be enabled to manage

his customer media i.e. enabled a medium for certain services, block media, enable media of family members etc.

This requires that the customer media can be recognized by the MaaS ID system and the Customer's ID service account and that the required identification and authentication of the customer medium may not be compromised by attackers.

5. **UC-C.2.4: NFC tag as authentication token**

   Online authentication is a key function of the MaaS ID system concept:

   1. A user-friendly, secure 2-factor authentication for sign-in to the ID service account is essential for reaching a defined trust level of the MaaS ID service.
   2. The MaaS customer media must support an online authentication function which is interoperable across all particular mobility modes and their infrastructures across the MaaS ecosystem.
   3. A stationary NFC tag with an online authentication function could be used for check-in/check-out implementations as described in [PT NFC use cases], chapter "NMD process C.2"

   A standardized NFC tag with a standardized online authentication function could be used for all 3 purposes.

   The implementation of this use case would require additional technical standardization work in the NFC Forum. It is currently discussed to which extend this will be implemented. A detailed description of this use case should be generated as part of this discussion.

In some cases, there are synergies with use cases which have been documented in [PT NFC use cases].

5.2 Use case C.1.1 - Initial identification

UC_C.1.1	Initial identification
Purpose, description	The ID service is depending on the Customer's support and feedback for the maintenance and management of the Customer's identity information IDc and IDx. The ID service account supports all required tasks online. Typically, the Customer's App which is provided by the Identity Provider's Partners will be extended by MaaS ID functions which support the maintenance of the Customer's identity information via the ID service account. The Customer shall have the option to conduct all activities online from his mobile device. This includes the initial identification of the Customer by the Identity Provider which is of fundamental relevance for the trust level of the ID service. The Customer's Maas ID information would be discredited if an unauthorized person or organization would get access to the ID service account.
Preconditions	1. The MaaS ID system must be in operations (BP-A.3) 2. The internal Partners must have implemented the MaaS ID function into their service Apps. 3. The Customer wants to benefit from the MaaS ID service and agrees to use the ID service account for managing his identity data.

UC_C.1.1	Initial identification		
Involved components	1. MaaS ID system as host of the ID service account 2. ID functions of the Partner's mobile Apps 3. Customer media as host of Partner's mobile Apps 4. If available, Customer's eID card or external mobile eID service	Business Processes	BP-C.1
Trigger for activities	1. Identity Provider has established a new IDc for a Customer. He wants to enable the Customer to use the MaaS ID service and to manage his IDc and IDx via the ID service account.	Initiated by	Identity Provider
Flow of activities (Standard)	Establishing the Customer's ID service account includes the activities from generating the ID service account in the MaaS ID system until the Customer is equipped with the credentials for accessing the account online. The Customer has to prove his identity before the credentials for accessing the ID service account are provided. A typical flow of activities is documented below: 1. The Identity Provider generates the Customer's personal ID service account and links the available IDc and IDx information to this account. 2. Viewing or managing data in the account requires that the Customer proves is identity first. 3. An online prove of identity requires a service that provides the Customer's fundamental identity information (name, address, age) with a defined, sufficient level of trust. This could be done by reading the Customer's passport, the governmental card online or by using a trustworthy mobile eID app (e.g. eIDAS conformant). 4. If an elevated trust level is targeted for the IDc identity information (which should be the standard case), login via weak authentication like username / password is feasible. A 2-factor authentication with a sufficient level of assurance would be required. This could be implemented by using an additional medium which could be read via the customer's mobile devices NFC-interface. 5. If confirmation of the identity was successful and a secure authentication to the ID service account was established, the Customer will be granted full online access to all functions of his ID service account.		
Flow of activities (Exception)	Several exceptions have to be considered: 1. If the Customer is not equipped with a trustworthy eID media or does not have a feasible NFC mobile device, he does not have the means to confirm his identity online via his mobile device → As alternative approach, the Customer should perform the initial identification at a service terminal or the transport organization's service center. 2. It may not possible to establish a secure authentication method for the Customer's use. As a consequence, updates of attribute values, managing IDx and providing legal statements (e.g. permissions) can potentially not be supported with the required trust level. → If the Customer owns a NFC mobile device, he could be equipped with a customer media which supports the required authentication function via the NFC-interface. This function could be integrated with classical transport card media or in NFC tags.		

UC_C.1.1	Initial identification	
Success end condition	The Customer accepts the Identity Provider's offer to use the MaaS ID service, may use his ID service account online with all provided features and trust levels.	
Failure End Condition	The ID service account was not established or can only be used for identity information and services with low level of trust.	
Deduced Functional Requirements		**Affected Components**
	There must be a method that supports a trustworthy online identification of the Customer before granting full access rights to his ID service account.	1. MaaS ID system 2. MaaS ID function for mobile Apps 3. External eID service
	There must be a 2-factor-online-authentication in place which the customer may use for accessing his ID service account.	1. MaaS ID system 2. MaaS ID function for mobile Apps 3. Customer medium

5.3 Use case C.2.1 – Sign-in to the ID service account

UC_C.2.1	Sign-in to the ID service account		
Purpose, description	The IDc and IDx information may only be viewed and managed by the eligible Customer. The sign-in procedure must ensure that only the eligible Customer may access the ID service account and that the security level which is provided by the authentication function matches the requirements as defined for specific trust categories for identity information which is maintained via this ID service account.		
Preconditions	1. The MaaS ID system must be in operations (BP-A.3) 2. The internal Partners must have implemented the MaaS ID function into their service Apps. 3. The Customer's ID service account is established and the Customer obtained online access to this account.		
Involved components	1. MaaS ID system as host of the ID service account 2. MaaS ID functions of the Partner's mobile Apps 3. Customer media as host of the Partner's mobile Apps 4. Potentially a carrier medium for 2nd authentication factor	Business Processes	BP-C.2
Trigger for activities	1. The Customer wants to access his ID service account online	Initiated by	Customer

UC_C.2.1	Sign-in to the ID service account		
Flow of activities (Standard)	1. The Customer uses the MaaS ID function of a Service Partner's mobile App to request sign-in to his ID service account. 2. The ID service account offers the authentication method that was agreed with the Customer and which matches the targeted trust level. 3. The Customer supports the sign-in by entering his credentials (if required by presenting a specific media or biometric property as second factor) 4. The Customer obtains access to his ID service account.		
Flow of activities (Exception)	Several exceptions have to be considered: 1. The customer fails to present the access credentials → Access to the ID service account is denied. 2. The Customer reports that he lost his access credentials or that his credentials may be compromised → In this case, the Identity Provider must support a backup-process in order to restore the Customer's access without compromising the trust level. Potential solutions are: a. The Customer uses an eID service to prove his identity and to gain access. The same media which was used for initial identification of the Customer in UC-C.1.1 could be used. b. The Customer possesses a second media with access credentials which he can use to access the ID service account and to manage the access rights. This concept is e.g. supported by FIDO authenticators. c. The Customer visits the Identity Provider's service center. There he may be identified and may receive new access credentials.		
Success end condition	The Customer obtains access to his ID service account and may use all agreed functions.		
Failure End Condition	The Customer sign-in fails and the account will be blocked. The Customer has to prove his identity to get new credentials and access to his account.		
Deduced Functional Requirements		**Affected Components**	
	The authentication method shall fulfill the security requirements for the targeted trust level of the identity information.	1. MaaS ID system 2. MaaS ID functions of Service Partner's mobile Apps 3. Customer medium 4. 2FA medium	
	The sign-in procedure shall support a backup mechanism that does also fulfill the security requirements for the targeted trust level of the identity information.	1. MaaS ID system 2. MaaS ID functions of Service Partner's mobile Apps 3. Customer medium 4. Potentially 2FA medium	

5.4 Use case C.2.2 – Enrol / update attribute values from trusted sources

UC-C.2.2	Enrol / update attribute values from trusted sources		
Purpose, description	For elevated trust levels of the identity information it may be required that any influence of the Customer on the IDC attribute value is excluded and the attribute values are directly transferred from a trustworthy source. This applies in particular for attributes where the Customer may have disadvantages in certain scenarios. Examples are the attributes which are representing the status of the Customer's driver license or student card. Trusted sources of attribute values are e.g. the Customer's eID card, the Customer's passport or services from external Identity providers which support secure online-updates of the IDc attribute values. The goal of this use case is to connect a trustworthy source of attribute values to the Customer's IDc so that the values can be transferred directly to the IDc attribute. The Customer may manage the process and see the result but he may not manipulate the value. Certain external eID cards or services could be used to perform the initial identification of the Customer as required in UC C.1.1.		
Preconditions	1. The MaaS ID system must be in operations (BP-A.3) 2. A partnership between the Identity Provider and the external Identity Provider and his identity service or eID media is established according to BP-B.1 and is operational as documented in BP-B.2. 3. The Customer is equipped with an ID service account and has online access. 4. The Customer is equipped with an eID medium or supported by a trustworthy eID service 5. The Customer is equipped with the necessary tools e.g. a NFC enabled mobile device which may be used to read the eID card or passport.		
Involved components	1. MaaS ID system as host of the ID service account 2. MaaS ID functions of the Partner's mobile Apps 3. System of the external Identity Provider incl. interface to the MaaS ID system 4. Potentially eID medium (eID card, student card, passport) 5. NFC mobile device or service terminal as reader of the eID medium	Business Processes	BP-C.2
Trigger for activities	1. The Customer wants to update a particular attribute value targeting an elevated trust level 2. The Customer wants to prove his identity to the Identity Provider (requires trustworthy eID media like eID card) 3. The Customer is asked by the identity Provider to conduct value updates.	Initiated by	1. Customer 2. Identity Provider (via BP-C.3)

UC-C.2.2	Enrol / update attribute values from trusted sources		
Flow of activities (Standard)	The flow of activities is depending on the type of eID media or eID service and the particular agreements with the responsible external Identity Provider. Typically, the following steps could apply: 1. The Customer selects the attribute that shall be updated. 2. The Customer connects his eID medium or allows the connection of a back-office external eID service. The particular implementation is depending on the specifics of the medium or the external eID service.		
Flow of activities (Exception)	The following exception has to be considered: 1. The Customer may not be supported for a feasible trustworthy online eID service or may not have means to read an eID medium online. In such case, a backup process involving a service terminal or a service center should be available.		
Success end condition	The Customer successfully implemented attribute value updates from a trustworthy data source.		
Failure End Condition	If the Customer fails to perform the wanted update online, he must use the backup in the service center or the service terminal.		
Deduced Functional Requirements		**Affected Components**	
	The customer medium should support reading ID cards, passports etc. via the NFC interface.	1. Customer medium	
	The Identity Provider must ensure interoperability with the external Identity Provider's medium or service	1. MaaS ID system 2. MaaS ID function of Partner's mobile Apps	

5.5 Use case C.2.3 - Manage customer media via the ID service account

UC-C.2.3	Manage customer media via the ID service account		
Purpose, description	The Customer shall have the option to manage his customer media via his ID service account. This includes the following functions: 1. Registration / de-registration of the customer media to the ID service account 2. Connecting or disconnecting the IDx to the IDc for personalized or anonymous use of the medium. 3. Releasing or blocking customer media (IDx) for specific services which are offered by internal or external Partners 4. Blocking IDx in case of loss or damage 5. Conformation of the Identity Providers proposals concerning IDx (e.g. in case misuse of a customer medium was reported by service partners)		
Preconditions	1. The MaaS ID system must be in operations (BP-A.3) 2. The Customer has access to his ID service account 3. The Customer is equipped with the necessary tools i.e. a NFC enabled mobile device which may be used to read the customer medium.		
Involved components	1. MaaS ID system as host of the ID service account 2. MaaS ID functions of Partner's mobile Apps 3. NFC mobile device as reader for the customer medium 4. Contactless customer medium	Business Processes	BP-C.2
Trigger for activities	1. The Customer wants to register/de-register a customer medium 2. The Customer wants to view the status of his IDx 3. The Customer wants to manage his IDx 4. The Customer is asked by the Identity Provider to modify status or accept changes to his IDx	Initiated by	1. Customer 2. Identity Provider (via BP-C.3)
Flow of activities (Standard)	Registration or de-registration of a customer medium: 1. The Customer signs-in to his ID service account (registration requires 2FA) 2. The Customer selects registration or de-registration of a customer medium 3. Registration of a customer medium: a. The customer uses his NFC mobile device to perform an authentication between the customer medium and the ID service account / MaaS ID system. b. The Customer enters a code which is related to the customer medium in order to prove that he has the medium in his hands. c. The Identity Provider will check if the same medium/application is registered for another ID service account.		

UC-C.2.3	Manage customer media via the ID service account	
	d. If not, the customer media will be registered and shown on the list of managed media 4. De-registration: a. The Customer selects the customer medium that he would like to de-register from the list b. The Identity Provider will de-register the customer medium Other functions: The customer may conduct all other functions listed under “Purpose” by selecting the targeted customer medium ´from the list of registered devices. Optionally, a new authentication of the device may be required before the function is executed.	
Flow of activities (Exception)	The following exception has to be considered: 1. If the customer medium is already registered with another ID service account, a registration is not possible.	
Success end condition	The Customer’s changes to the IDx are implemented by the ID service.	
Failure End Condition	The Customer fails to manage his IDx online.	
Deduced Functional Requirements		**Affected Components**
	The NFC mobile device shall support reading customer media via the NFC interface.	1. Customer mobile device
	The customer medium should support a secure online authentication function	1. MaaS ID system 2. MaaS ID function of service Apps

5.6 Use case C.2.4 - NFC tag as authentication token

UC-C.2.4	NFC tag as authentication token		
Purpose, description	NFC tag should be used as one of factors for 2-factor authentication of the MaaS ID system concept: 1. A user-friendly, secure 2-factor authentication for sign-in to the ID service account is essential for reaching a defined trust level of the MaaS ID service. 2. The MaaS customer media must support an online authentication function which is interoperable across all particular mobility modes and their infrastructures across the MaaS ecosystem. 3. A stationary NFC tag with an online authentication function could be used for check-in/check-out implementations as described in [PT NFC use cases], chapter "NMD process C.2"		
Preconditions	1. The MaaS ID system must be in operations (BP-A.3) 2. The Customer has access to his ID service account 3. NFC tags must be managed by Identity Provider or MPO. 4. The Customer is equipped with the necessary tools i.e. a NFC enabled mobile device which may be used to read NFC tags.		
Involved components	1. MaaS ID system as host of the ID service account 2. MaaS ID functions of Partner's mobile Apps 3. NFC mobile device as reader for the customer medium 4. NFC tag	Business Processes	BP-C.2
Trigger for activities	1. The Customer wants to authenticate the MaaS ID. 2. The Customer wants to check-in/check-out to the mobility services. 3. The Customer is asked by the Identity Provider to apply NFC tag for authenticator.	Initiated by	1. Customer 2. Identity Provider (via BP-C.3) 3. MPO
Flow of activities (Standard)	Authentication of the MaaS ID: 1. The Customer applies NMD to a NFC tag as one factor for 2FA, which is required for MaaS ID. 2. If the Customer lost a customer medium, the Customer will securely recover access to the MaaS ID by using the NFC tag. Check-in/Check-out function: 1. The Customer applies NMD to a NFC tag to check-in/check-out a certain mobility service. 2. Check-in/check-out tap will inform the MPO as the Customer wants to have a certain mobility service.		

UC-C.2.4	NFC tag as authentication token	
Success end condition	The Customer's authentication is done by the NFC tag The Customer's check-in/check-out is informed to MPO.	
Failure End Condition	The Customer fails to make an authentication to his MaaS ID.	
Deduced Functional Requirements		**Affected Components**
	The NFC mobile device shall support reading NFC tags via the NFC interface.	1. Customer mobile device
	NFC tags should support a user-friendly, secured 2-factor authentication.	1. MaaS ID system 2. MaaS ID function of service Apps