

INTERNATIONAL TELECOMMUNICATION UNION

STUDY GROUP 17

**TELECOMMUNICATION
STANDARDIZATION SECTOR**

TD 2144

STUDY PERIOD 2009-2012

English only

Original: English

Question(s): 10/17

Geneva, 24 August-2 September 2011

TEMPORARY DOCUMENT

Source: Editor of X.mob-id

Title: Revised text on draft Recommendation ITU-T X.mob-id

Summary

This Recommendation proposes baseline capabilities and a framework for mobile identity management (IdM). The mobile IdM framework provides basic capabilities which can include user requirements to meet user's needs for the framework and functional capabilities for a system to be satisfied when a mobile IdM system is developed based on a specified framework. The framework specifies mobile IdM and security to provide baseline identity lifecycle management and security mechanisms in mobile device. It also provides identity operations that can provide functions that are required to build up secure and personalized mash-up applications that can provide privacy enhanced identity services that collect, analyse and use personal information.

Table of Contents

1	Scope.....	4
2	References.....	4
3	Terms and definitions	4
	3.1 Terms defined elsewhere:.....	4
	3.2 Terms defined in this Recommendation.....	4
4	Abbreviations and acronyms	5
5	Conventions	5
6	Introduction.....	5
7	Use case scenarios	6
	7.1 Smart shopping.....	6
	7.2 Authentication and access control.....	6
8	Usage of personalized services in mobile environment	7
9	Mobile IdM Requirements.....	9
	9.1 User requirement	9
	9.2 Functional requirements	10
	9.3 Security requirements.....	10
10	Mobile IdM framework	11
	10.1 Entities in the framework	12
	10.2 Management and security.....	13
	10.3 Identity operation.....	13
	10.4 Service	14
11	Mobile IdM structure.....	14
	11.1 Operation layer	14
	11.2 Software structure.....	16

ITU-T Recommendation X.mob-id

Baseline capabilities and mechanisms of IdM for mobile applications and environment

1 Scope

The scope of this Recommendation will be as follows:

- Define the use of identity and IdM in the context of mobile applications and environments, including use cases that highlight the unique requirements of mobile scenarios.
- Identify the types of identity information used in a mobile context and explore their characteristics. Then define the requirements of IdM for mobile applications and environments based on the use cases above. The requirements should reflect multiple aspects such as user, system and security.
- Specify the baseline capabilities and core functions necessary to satisfy the requirements defined above.
- Specify a framework to illustrate how IdM entities interact to provide personalized services in mobile environments. The framework will include mechanisms for the use of IdM in the development of applications in mobile environments.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[ITU-T X.1205] Recommendation ITU-T X.1205, *Overview of Cybersecurity*

[ITU-T Y.2760] Recommendation ITU-T Y.2760, *Mobility security framework in NGN*

[Editor's note] put all Q.16/13 Recommendation for mobile NGN in here

3 Terms and definitions

3.1 Terms defined elsewhere:

This Recommendation uses the following terms defined elsewhere:

[TBD]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

- 3.2.1 mobile application:** add-on software for handheld devices, such as smartphones and personal digital assistants (PDA).

3.2.2 mobile device (also known as a **handheld device**, **handheld computer** or simply **handheld**): a pocket-sized computing device, typically having a display screen with touch input and/or a miniature keyboard.

3.2.3 smartphone: a mobile phone that offers more advanced computing ability and connectivity than a contemporary feature phone. Smartphones and feature phones may be thought of as handheld computers integrated with a mobile telephone.

4 Abbreviations and acronyms

[TBD]

5 Conventions

None

6 Introduction

It is expected that the market for smart phone will be grow to 39.9% of all mobile phone by Gartner. This means that 40% of people who uses mobile phone will use smart phones for their mobile communication. In addition, it means that those people can use their smart phone as a computer and connect to the Internet for anytime and anywhere. In this situation, many services and contents can be provided to meet individual user's requirements. Personalized online advertisement is also possible example for this kind.

As smart phones are expected to be prevalent, mash-up services that utilize identity information such as relations, preferences and purchases, stored in the device, will easily be available and widespread rapidly. Here many personalized identity information will be needed to provide such services and more privacy sensitive information is required for targeted personalized services. Various credit card, membership card, discount card and coupon can be contained and used in the smart phone for smart payment and shopping.

In this environment, lifecycle of identity information needs to be managed securely and efficiently if mash-up services are properly provided. There must be a protection mechanism if a mobile device is lost or stolen. Communication security is important since there is security vulnerability in mobile communication. Smart payment and shopping with mobile payments need to have confidentiality, integrity and non-repudiation for its financial transactions.

The security for transport layer in NGN environment has been specified in [ITU-T Y.2760], which includes security mechanisms such as authentication and key management; security context establishment; IP mobility security; and security of mobility management, control and transport in the transport stratum of NGN. In this recommendation, security mechanisms are considered only for mobile application services.

[Editor 'note] include reference to mobile payment and mobile security work from Q16/13

Therefore, it is necessary to discuss what baseline capabilities are required to support mobile application services and how mobile IdMframework can be specified to provide secure and privacy protected identity services to mobile mash-up applications.

7 Use case scenarios

7.1 Smart shopping

Credit and royalty card, coupon can be issued to a mobile device by OTA(Over-The-Air). Then when user visits an offline store, the user can use the device to pay for the shopping using NFC using issued credit card. In the case when the user visits online store, the cards that issued earlier can be used for smart shopping as well. The mobile device can also recommend optimal payment solution for maximum discount. After the payment transaction is processed successfully, the device receives a transaction result that is stored in the storage and then processed to extract user preference or pattern for personalized service later.

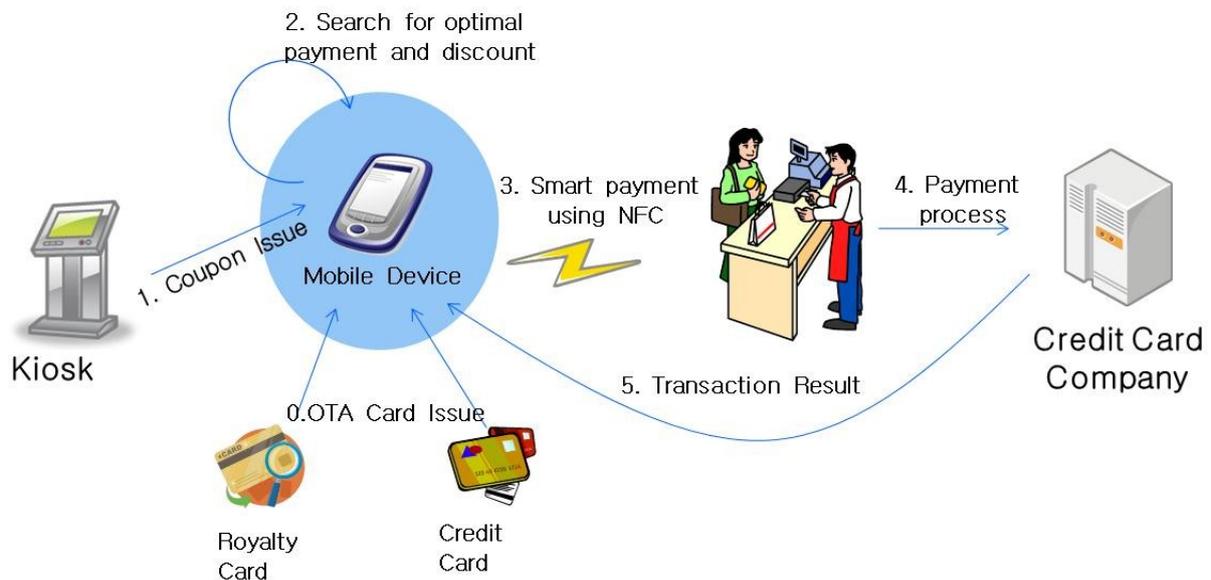


Figure 1 – Smart shopping scenario

In order to realize the scenario described above, the following requirements are needed.

- Authentication to the mobile device (e.g. authentication to the device to authorize the credit card transaction)
- Communication security for OTA (NFC security) and online
- Protection of information stored in the device for loss or theft of a mobile device
- Platform to accumulate and process transaction records to extract new identity information
- Backup and archive records in server optionally

7.2 Authentication and access control

User can use a mobile device to access a building to enter his workplace. When he comes to his desk, the login to PC (Personal Computer) can be carried out in the mobile device. The mobile device even can be used to login to a website. This can be secure and convenient if the user is in public domain.

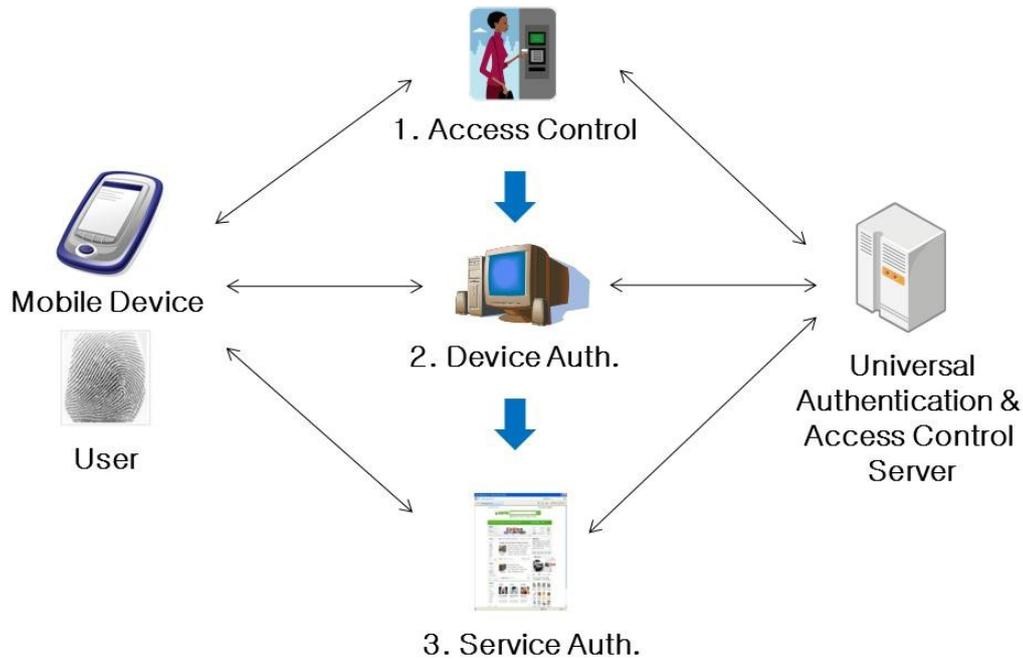


Figure 2 – Seamless authentication scenario

In order to provide seamless authentication and access control in mobile environment, the following requirements are mandatory.

- Authentication to the mobile device
- Credential management for authentication and access control
- Communication security for secure channel

8 Usage of personalized services in mobile environment

A digital identity including credentials, personal information and preference information can be issued and used in a mobile device. In addition, this identity contains extra important personal context information, which is location. In a mobile environment, location information belonging to a user can be used to provide personalized services. The figure 3 illustrates various different types of identity that can be used in a mobile device.



Figure 3 – Types of Identity in a mobile device

The following is a list of identity with its examples.

- Authentication information
 - ID/PW, Digital Certificate, Smart Key
- Payment information
 - Payment Information
 - Credit Card, Royalty Card, Discount Coupon
- Static personal information
 - Address, Telephone number, etc.
- Dynamic personal information
 - Shopping record, Travel record, Access record, etc.
- Personal context information
 - Location, Time and Ambient Access record, etc.
- Preference information
 - Personal preference and interest, etc.

Figure 4 shows the usage of personalized services in mobile environment. An application in a mobile device can contain identity such as credentials and authentication, payment information. The various data such as location, purchase record and preference information can be collected in a mobile device since transactions generating this information are carried out in the same place. The one characteristic of mobile device is to be used in online and offline. Online means that the device

directly connects to the Internet for web services and offline implies that the device contacts physical object for the communication. Therefore, many user data can be collected and accumulated in the mobile device.

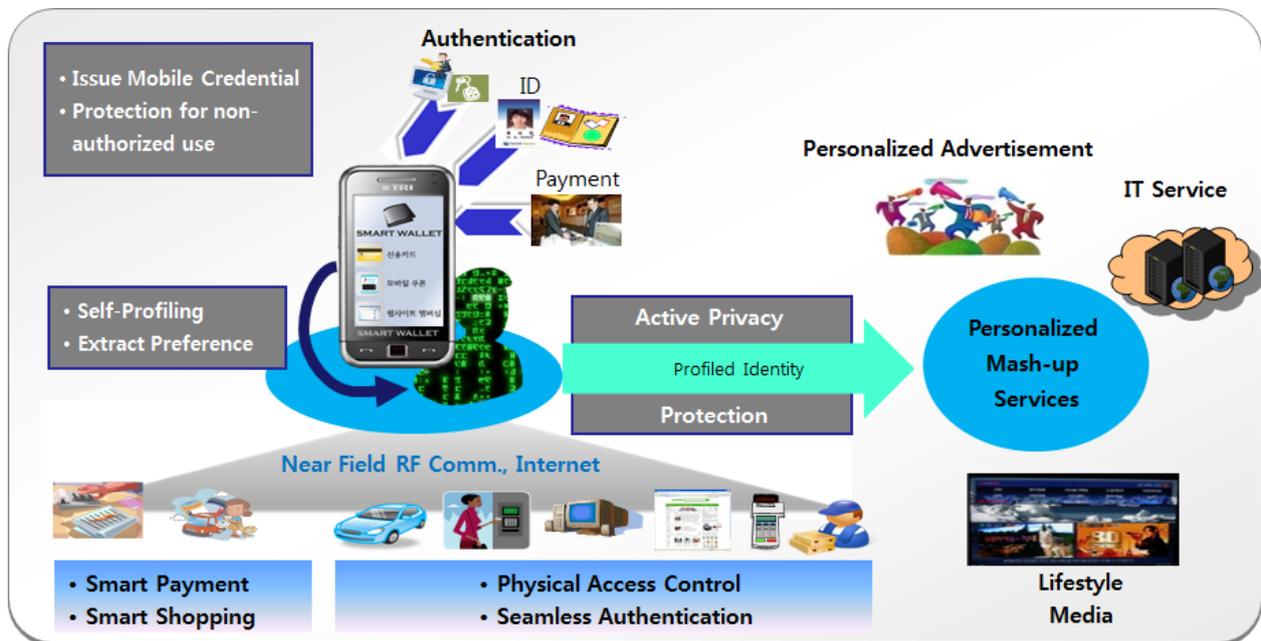


Figure 4 – Usage of personalized services in mobile environment

This primitive user data can be processed to extract user's behavior, preferences and patterns, which can be called a user profile. The user profile is a set of attributes that does not contain any information identifying a user.

When the user profile is provided to a service provider, services are filtered and recommended based on the user profile to provide tailored services for the user. The various mobile IdM capabilities are required to provide such a service. Even if personal information is used for personalized services, privacy problems are mitigated since the user profile does not contain any information connecting to the user.

9 Mobile IdM requirements

The mobile device where an identity is managed is different in many aspects. At first, the display size is quite limited compared to general PCs and the probability of losing the device is high since the size is small and portable. In addition, since the mobile device has characteristics such as portability, mobility, anywhere connectivity and offline interaction, the functionality that cannot be provided in existing PC is possible and it requires different user experiences.

In this clause, the requirement is divided into three categories: user requirements, functional requirements and security requirements. User requirements represent the aspect of user's convenience that can improve the user experience. The requirements specified in the user and functional parts below are mandatory unless indicated as optional.

9.1 User requirement

In this clause, the requirements for mobile IdM are elaborated from the user aspect.

- 1) Provide user interface that is suitable for mobile device, which uses finger touch for input

in addition to keyboard

- 2) Provide simple and intuitive user interface for mobile IdM since user is used to simplified and clear interface design in mobile applications
- 3) Provide for a mobile device to be used as an authentication token to login to other device. This is useful requirement for the user to login a device such as PCs since the mobile device is always carried by user (Optional)
- 4) Provide import and export of user's identity from one mobile device to another. This is convenient if supported because a user is tended to change mobile device quite often (Optional)

9.2 Functional requirements

In this clause, the requirements for mobile IdM are elaborated from functional aspect.

- 1) Provide identity lifecycle management that enable a mobile device to create, modify, search and delete identity directly
- 2) Provide import and export function for identity information such as credit card and public certificate, which is managed by mobile IdM system
- 3) Provide authentication capability for a mobile device to login to other device such as PCs using wireless communication (Optional)
- 4) Provide seamless authentication service in both online and offline environments using a mobile device (Optional)
- 5) Provide mobile payment for goods and services purchased using a mobile device. Credit, royalty and membership card can be issued and managed in the mobile device.
- 6) Provide smart payment for mobile shopping to give a user various discount information (Optional)
- 7) Collect identity information that is generated when purchasing goods and subscribing website. This information later can be used to provide personalized mobile services. (Optional)
- 8) Provide identity for personalized services with privacy enhanced capability to preserve user's privacy. (Optional)
- 9) Enable a service provider to query user' identity to provide personalized services.
- 10) Enable a service provider to search and discover a user with user's attribute that can be found in a mobile device. (Optional)
- 11) Enable a user to limit the scope of identity that can be provided for a service provider for privacy protection.
- 12) Enable a user to authenticate him to prove his identity using a mobile device in online and offline services. (Optional)
- 13) Provide a user with credential that can access to a physical space using short-ranged RF communication such as Bluetooth and NFC. (Optional)

9.3 Security requirements

In this clause, the requirements for mobile IdM are elaborated from security aspect.

- 1) Store and manage user's identity securely in a mobile device.

- 2) Manage user's identity in encrypted form for confidentiality.
- 3) Use secure storage that is provided by mobile device OS or temper-proof device such as USIM (Universal Subscriber Identification Module). (Optional)
- 4) Provide automatic locking capability to lock mobile IdM client when the valid time is over.
- 5) Provide a mechanism to protect a mobile device when it is lost or stolen.
- 6) Provide a mechanism to protect a mobile device using context-aware risk analysis. This mechanism enables a user to deal with a lost or stolen mobile device according to various situations the device can confront. (Optional)
- 7) Provide automatic locking when a mobile device is away from a user. The automatic locking can lock the device or sound the alarm. (Optional)
- 8) Provide remote data removal for lost or stolen mobile device to remove identity stored in the device.
- 9) Provide communication security when a mobile device communicates with other computing devices.

10 Mobile IdM framework

The following figure shows the mobile IdM framework for the reference. The framework contains mechanisms that are categorized into three groups:

- Management and security
- Operation
- Service

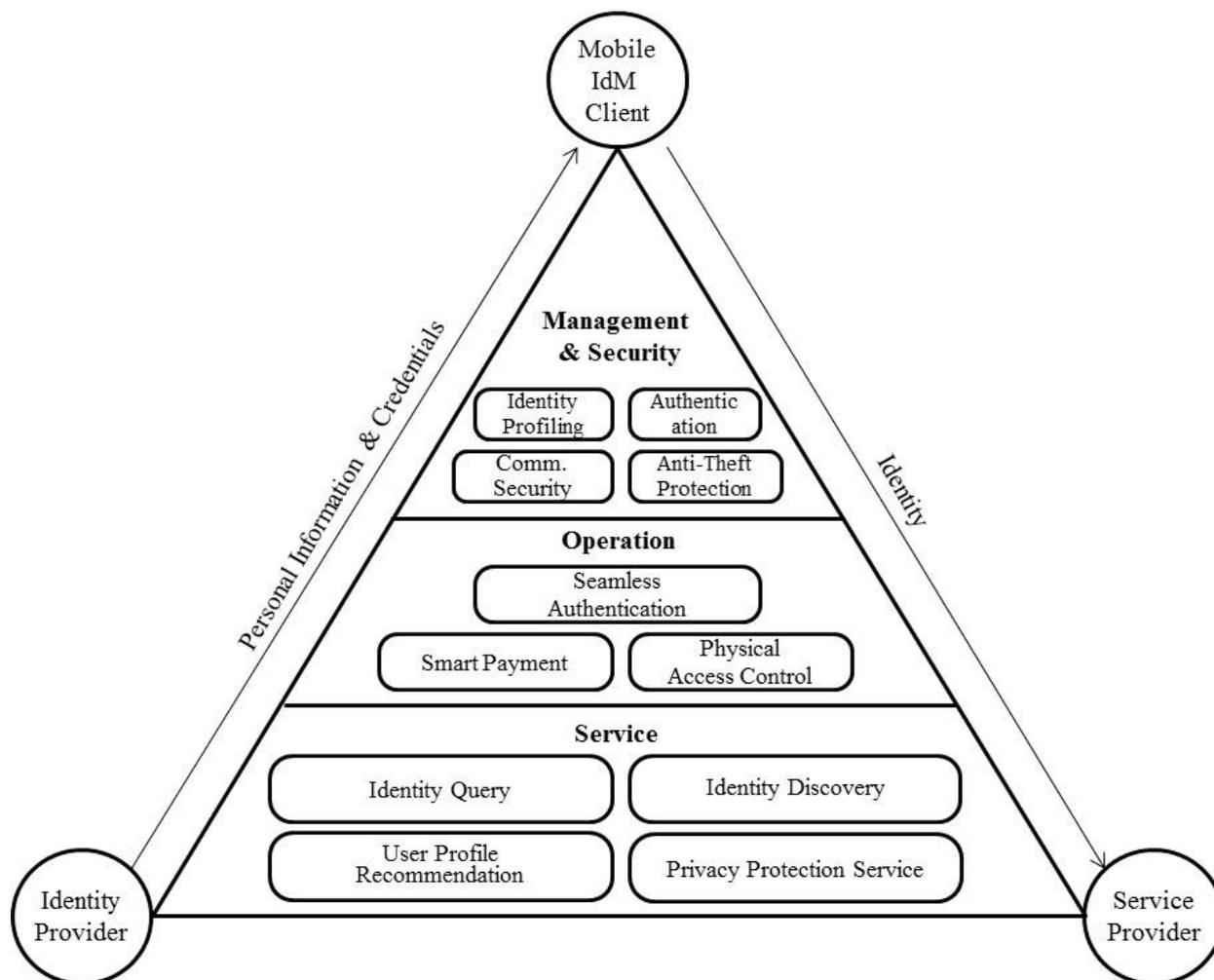


Figure 5 – A framework for mobile IdM

IDP (identity provider) provides personal information and credential for a mobile device when requested. Such provided information and credential is managed with information that is collected from various services and context information such as location in a mobile device. The user provides a SP (Service Provider) with identity for various personalized services. All mechanisms in the framework is installed and operated in a mobile device. However SP and IDP only uses necessary mechanisms to provide services. The main objective of the framework is to transform personal information that is provided by IDP to identity that is profiled and later can be used for personalized mobile services while security and privacy concerns are preserved.

10.1 Entities in the framework

10.1.1 Identity provider

IDP is the entity that issues and manages identity or credential to a user or an entity. With related to identity, IDP provides credential, payment or location information. In Figure 3, IDP is the entity that provides personal information and credential for a mobile device.

10.1.2 Mobile IdM client

Mobile IdM Client is an application program that is installed in a portable mobile device. Mobile IdM Client is equipped with all the mechanisms that the framework provides. It also enables the device to accumulate various identity information through identity profiling process to extract

personal preferences that can be used in other mobile applications or disseminates to SP for personalized services.

Mobile client is the personal identity platform to provide security and privacy of identity services to develop high value-added identity based application services. This is the program that utilizes user's authentication and personal information for convenient services and mobile payment and it also provide security and privacy enhanced mechanism to protect its identity from any illegal activities.

10.1.3 Service provider

SP is the entity that receives identity from a mobile IdM client and provides personalized or customized services for the user.

10.2 Management and security

This is the core building block of the framework that is responsible for management and security mechanisms of mobile IdM.

10.2.1 Identity profiling

Any activity that includes purchases, accesses, payments and movements performed by a mobile IdM client is monitored and recorded to extract personal preference or interest. This data should be carefully structured through systematic modeling process to be used in mobile IdM operation and service later on.

10.2.2 Authentication

Since mobile IdM client can retain confidential or sensitive user information such as credentials and identity with related to financial transactions, a user has to authenticate to the client program. This authentication is carried out to login to a mobile device. This can be done by typical password-based authentication or it can be executed by biometric technology or patter-matching authentication mechanism.

10.2.3 Anti-theft protection

When a mobile device is lost or stolen, this function prevents from illegal use and unwanted information disclosure. It also provides proximity-based locking and remote device destruction to prevent from unauthorized misuse of the device.

10.2.4 Communication security

Identity is basically transmitted using wireless Internet or near field RF communication channels. Security for wireless Internet is the same as security for the Internet. But if mobile payment, identity service, authentication and access control is carried out using near field RF communication channels such as NFC and Bluetooth, then security mechanism is crucial to protect these communication channels.

10.3 Identity operation

10.3.1 Smart payment

A mobile device can contain various credit card, membership card, royalty card and coupons. This operation provides intelligent payment matching service that can search for best combination of cards for optimized payments.

10.3.2 Seamless authentication

A mobile device can be used to login a website on the Web and the device itself can be used as a key to access physical buildings or doors. This operation provides integrated authentication mechanisms to interconnect between online and offline services

10.3.3 Physical access control

Mobile device can be used to access a building or a door in physical world using short range RF technology such as NFC. In this case, mobile IdM client manages issued credentials and uses it for access control.

10.4 Service

10.4.1 Identity query

This is the service that enables an application to request identity to a mobile device and the device processes the request and returns identity for application services.

10.4.2 Identity discovery

An application service may search for users with certain attributes that meets specific search criteria. It simply looks for an individual without authentication. The search process should not disclose person's identity or infringe his privacy.

10.4.3 User profile recommendation

After processing identity profile function, mobile IdM client has accumulated user information that can be manipulated to extract a personal preference. When a SP needs certain user's identity information e.g., location and shopping list, mobile IdM client can recommend user profile to the SP for personalized service.

10.4.4 Privacy protection

There should be no privacy violation when identity is provided for a customized service. There are two technologies for this service. The first one is de-identification. There should be no relationship between past and current identity that is provided for the service. This technology anonymizes any identity to prevent from identity disclosure. The second one is autonomous privacy policy management. This technology helps a user establish privacy policy that contains constraints, purpose and service provider for identity and make a decision automatically whether identity is provided for whom and what scope through negotiating any privacy policy issues with the service provider.

11 Mobile IdM structure

11.1 Operation layer

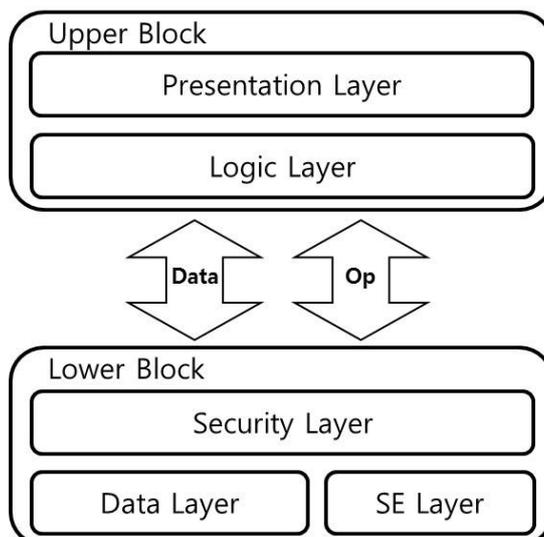


Figure 6 – Logical structure of the framework

Figure 6 shows the logical structure of processing flow in the framework. As it is described, the operation layer is divided into two blocks to process operations: upper and lower block. The upper block is responsible for usage and management of mobile IdM operation and the lower block is for security and storage operations. Data and operations are processed separately between the upper and lower blocks. The reason for having separate two blocks is to provide maximum flexibility to the upper block in application environment whereas there will be minor customizing requirement for the lower block. Between the upper and lower block, most transactions are carried out using data interface. However, in order to use functions provided from secure element such as USIM, operation interface is needed.

11.1.1 Presentation layer

The presentation layer takes inputs from user and displays the result of an operation as a form of user interface. This layer is used when the software needs to interact with a user to process services. Since presentation layer is different depending on application services, it can be designed to meet application's requirement.

11.1.2 Logic layer

The logic layer processes interaction and collaboration between operations and services and its role is to receive and process data from the lower layer to return its result to the presentation layer. There are two ways to access the lower block. Most of functions can use data interface to access the lower block. However, to call functions in the SE layer, operation interface is called directly to access functions provided from SE.

11.1.3 Security layer

The security layer is responsible for security functions such as user and risk-based authentication. It also provides function that use digital certificate. Every function call from the upper block has to be checked for further user authentication. This layer is also invoked to provide digital signature.

11.1.4 Data layer

The data layer handles processes that store data into a database and manage it.

11.1.5 Secure Element layer

The Secure element layer manages credit card information for online and offline payment services. This layer includes USIM, which provides services with its own data storage. This layer is only needed if a mobile device has a secure element.

11.2 Software structure

Figure 7 illustrates the software structure that uses and manages an identity in mobile devices. This structure enables mobile IdM framework to provide mobile IdM services by developing components that are listed in the figure.

Mobile IdM service consists of management, security, storage and functional components.

Management component provides installation, startup, and termination of MIDM. It also manages the user's configuration data. Security component carries out user and risk-based authentication and it provides authentication and digital signature services using digital certificates. Storage component stores various data used in MIDM and manages it securely in a database. Functional component is used to work with SE API to provide necessary services that supports for online and offline payment and credit card issuance.

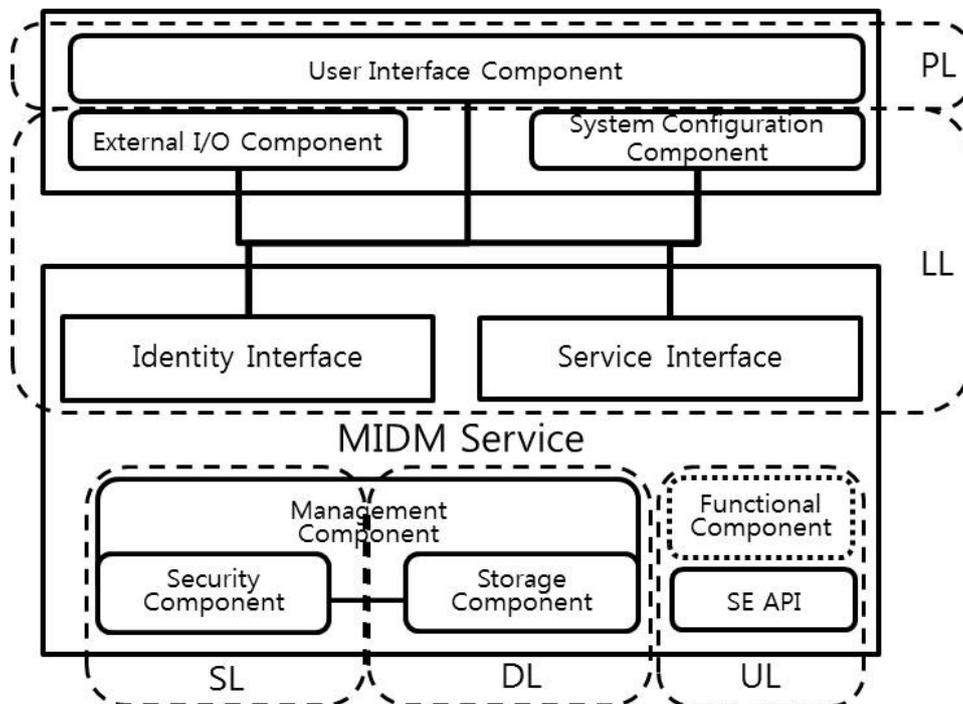


Figure 7 – Software structure of Mobile IdM

The MIDM services are connected to user interface and external I/O component by utilizing two interfaces: Identity and service interfaces. Identity interface is a data layer providing a way to access a database from the upper layer. This interface is used to retrieve credit card, digital certificate and transaction information from a database to be displayed in the user's interface. The interface is also used for external application to access MIDM's information. Service interface is used to call functions that are provided by MDIM's service. This interface is used for instance when online and offline payment is made or a credit card is issued.

There are three components in the top of the figure. External I/O component is the service endpoint that can be accessed external applications, which are provided by telecommunication operator or

web service provider. User interface means GUI part that is displayed for user interactions. System configuration component is the block that manages configuration data needed to operate MIDM services.
