INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 1351

English only

Original: English

Question(s): 10/17 Geneva, 8-17 December 2010

TEMPORARY DOCUMENT

Source: Editor of X.mob-id

Title: Revised text of draft Recommendation ITU-T X.mob-id: Baseline capabilities and mechanisms of IdM for mobile applications and environment

Abstract

In December 2010 Q.10/17 meeting, the contribution C366 has been presented and discussed. The meeting has agreed to the contribution to be its 1st revised draft text, published as TD.

In this contribution, the following texts are proposed as the first draft text.

- Clause 6 Introduction
- Clause 7 Concept of mobile identity
- Clause 8 Requirements
- Clause 9 Conceptual Model for Mobile IdM
- Clause 10 Mobile IdM Framework

The scope of X.mob-id is changed to reflect the meeting's concern that this work should proceed in sequence: use case scenarios, requirements, capabilities, framework and mechanisms.

Editor's note has been placed in clause 7, 8, 9 and 10 to indicate how each clause can be prepared to resolve meeting's concerns of this contribution at the next meeting.

Contact: Sangrae Cho
ETRI
Korea (Republic of)

Tel: +82 42 860 6939
Fax: +82 42 860 1471
Email: sangrae@etri.re.kr

Summary

This Recommendation proposes a new work item on 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 identity management and security to provide baseline mobile identity lifecycle management and security mechanisms. It also provides mobile identity operations that can provide functions that are required to build up secure and personalized mash-up applications and mobile identity services that can provide privacy-aware identity services that collect, analyse and use personal information.

Table of Contents

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::

[Editor's note: do gap analysis between X.1250 and this work item to identify new requirement specific to identity used in mobile environment]

- 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*

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:

[TBD]

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 mobile identity information such as relations, preferences and purchases, stored in the device, will easily be available and widespread rapidly. Here many personalized mobile 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 mobile 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.

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

7 Concept of Mobile Identity

[Ed Note: the definition of "mobile identity" needs to be redefined to reflect meeting's concern that mobile identity is actually the same as identity in most contexts]

Mobile identity is a digital identity that is issued and used in a mobile device including credentials, personal information and preference information. In addition, this mobile identity contains extra important personal context information, which is location. The location information exists uniquely in mobile environment. The figure 1 illustrates various different types of mobile identity that can be used in a mobile device.

Figure 1 Types of Mobile Identity

The following is a list of mobile 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

The basic characteristics of mobile identity have a close relationship with the existing digital identity. Here it is more suitable to examine the definition of identity. Currently the term identity is defined as follow in ITU-T X.1250.

- The representation of an entity in the form of one or more information elements which allow the entity(s) to be sufficiently distinguished within context. For IdM purposes the term identity is understood as contextual identity (subset of attributes) i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

The definition of identity is specified in very broad spectrum to cover every aspect of identity. Mobile identity is a subset of identity. The all attribute in mobile identity is a member of digital identity. The distinct characteristic of it is mobility. Therefore, basically mobile identity can be considered as an identity with mobility.

The term mobile identity is defined in several research reports and academic papers. In FIDIS report for mobile identity, the mobile identity is defined as " a partial identity which is connected to the mobility of the subject itself, including location data".

Referring to FIDIS Report [1][2] about mobile identity, Mobile identity takes into account location data of mobile users in addition to their personal data. Therefore it is defined as an identity that is connected to the mobility of the subject itself, including location data. In [3], Mobile (digital) identity is an extension of the concept of digital identity that illuminates the importance of mobility. It suggests three modes of mobility, which is from device to device, location to location and context to context.

In this Recommendation, mobile means mobility of an entity moving from a location to another location. [Mobile identity] is defined as an identity used in mobile environment with related to the mobility of a subject including location data.

- Mobility of device: in mobile environment, a user can move from one device to another device to login to that device. Mobile identity can be used to authenticate a user to a device where the user tries to login.
- Mobility of domain: the domain that a user stays can be constantly changed when he moves between different domains that are physically separate. In this case, mobile identity is required for authentication and authorization when the new domain is entered.
- Mobility of context: context information – time, temperature, and ambient data - that can be obtained from sensors is collected when a user moves from one context to another one. This information can be used to provide personalized mobile services.

8 Requirements

[Ed Note: use case scenarios is needed to extract requirements and the requirements should not contain any technological or platform specific materials]

[Ed Note: consider the device like iPad, which has no limitation in display and input method when requirements are defined]

The mobile device where mobile identity is managed is different in many aspects. At first, the display size is quite limited comparing 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.

8.1 User requirement

In this clause, the requirements for mobile IdM are elaborated from 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) Support for PIN (Personal Identification Number) authentication mechanism. This is weaker than password in security aspect. But for convenience it is necessary for general mobile applications
4) 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)
5) Provide import and export of user's mobile identity from one mobile device to another. This is convenient if supported because a user is tended to change mobile device quite often (Optional)

8.2 Functional Requirements

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

1) Provide mobile identity lifecycle management that enable a mobile device to create, modify, search and delete mobile identity directly
2) Provide import and export function for identity information such as credit card and public certificate, which is created and 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
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 mobile identity for personalized services with privacy enhanced capability to preserve user's privacy. (Optional)
9) Enable a service provider to query user' mobile identity to provide personalized services. (Mandatory)

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 mobile identity that can be provided for a service provider for privacy protection. (Mandatory)

12) Enable a user to authenticate himself to prove his identity using a mobile device in online and offline services. (Optional)

13) Provide a user with pseudonymous identity not to disclose his identity if not necessary. (Optional)

8.3 Security Requirements

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

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

2) Manage user's mobile identity in encrypted form for confidentiality.

3) Use secure storage that is provided by mobile device OS or temper-proof device such as USIM. (Mandatory)

4) Provide automatic locking capability to lock mobile device when the valid time is over. (Mandatory)

5) Provide a mechanism to protect a mobile device when it is lost or stolen. (Mandatory)

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 mobile identity stored in the device. (Mandatory)

9) Provide communication security when a mobile device communicates with other computing devices. (Mandatory)

9 Conceptual Model for Mobile IdM

[Ed Note: this clause should be use case scenarios to explain how identity in mobile environment is used to provide personalized services and the figure 2 should be changed to reflect that]

Mobile client is the personal mobile identity platform to provide security and privacy of mobile 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 mobile identity from any illegal activities.

The figure 2 shows the conceptual environment that mobile IdMI operates. The client in a mobile device contains mobile identity such as credentials and authentication, payment information. Any mobile identity is interchanged between a mobile device and application servers using the Internet or near field RF (Radio Frequency) communications. Mobile identity is totally managed by the

mobile client in the mobile device. Security countermeasure against theft or lost is provided through the mobile client to prevent for non-authorized use of the device.

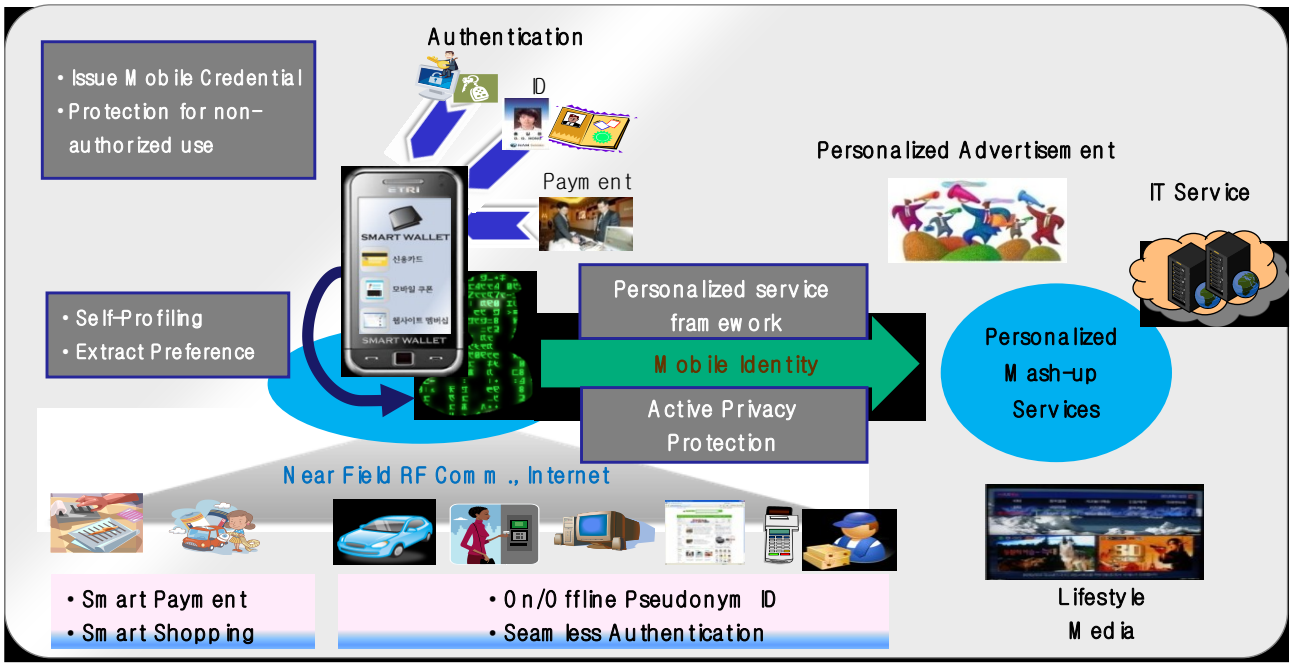

Figure 2 Conceptual Model of Mobile Identity Management

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. The mobile client provides online and offline seamless authentication, identification and smart purchase and payment services.

In addition, the mobile client collects and profiles dynamic user behaviour information, which is produced when the mobile device is in use. Dynamic personal information including personal context such as location is injected into personalized convergence services through active control of user's mobile identity. Personalized convergence service means a customized service that includes customized media, advertisement and IT services. Active control of mobile identity means that a user selects what personal information he wishes to provide for a service and it provides privacy protection mechanism by anonyms or pseudonyms. This will enable mobile service providers to leverage their services for more tailored and personalized mash-up services.

10 Mobile IdM Framework

[Ed Note: make the framework independent of any technology and operating platforms. Identify any existing work with related to mobile communication and privacy and put that in the document as a reference]

[Ed Note: re-organize the framework figure to illustrate some of mechanisms are common to all entities and some of them are just used for specific entity]

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

- Mobile Identity management and security
- Mobile identity operation
- Mobile identity service

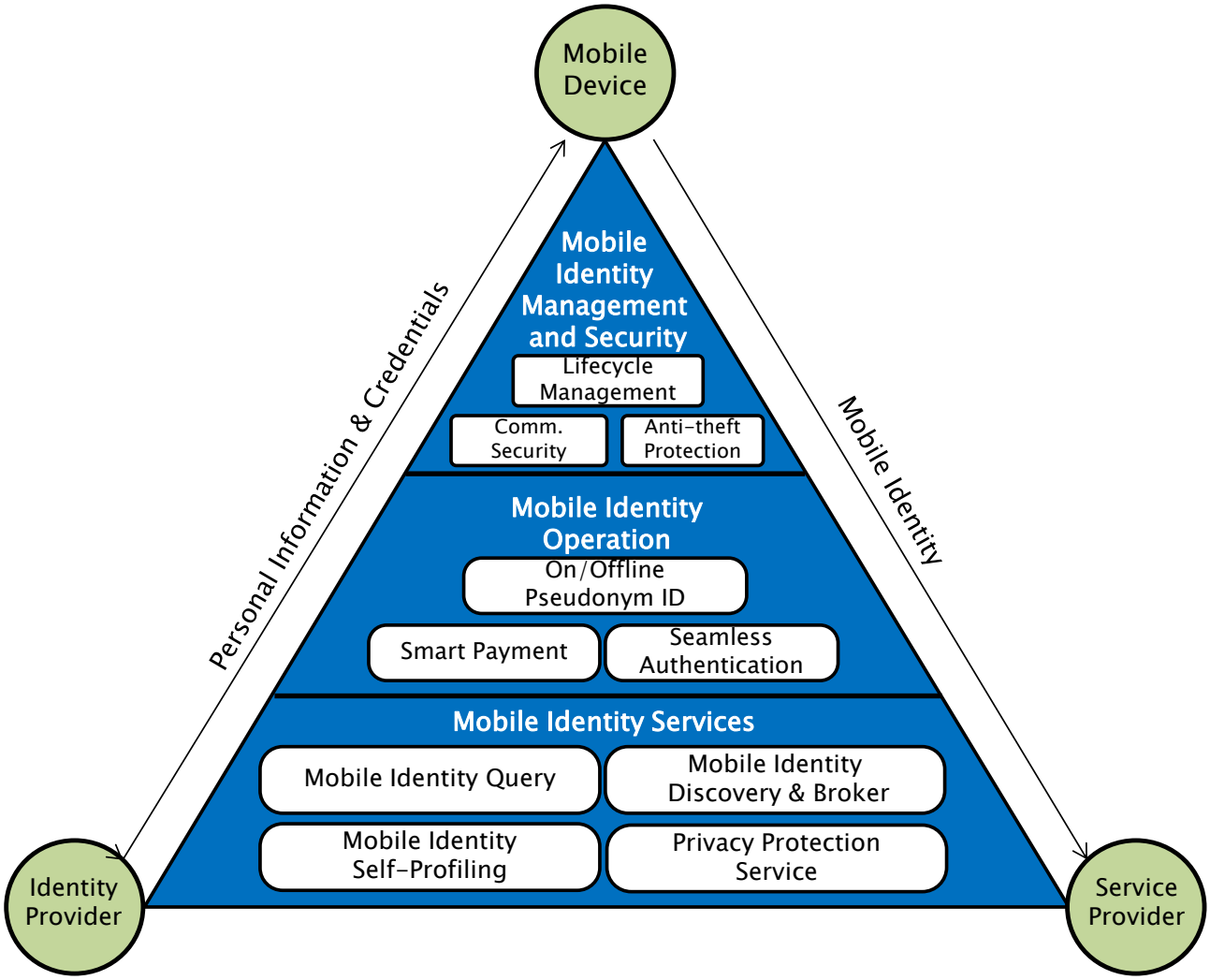

Figure 3 A framework for Mobile Identity Management

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 as mobile identity in a mobile device. The user provides a SP (Service Provider) with mobile 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 mobile identity that 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 mobile 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 Device

Mobile device is the portable device that can install an application program. Mobile device is equipped with all the mechanisms that the framework provides. It also enables the device to accumulate various identity information through self-profiling process and this information is processed to be used as mobile identity. The device later disseminates these mobile identities to SP for personalized services.

10.1.3 Service Provider

SP is the entity that receives entity's mobile identity from a mobile device and provides mobile personalized or customized services.

10.2 Mobile Identity Management and Security

This is the core function that a mobile identity management framework that provides as follows.

10.2.1 Lifecycle management

All mobile identity information including authentication, personal context, static and dynamic personal profile, preferences and location is managed using mobile identity lifecycle model by using systematic and consistent user interface.

10.2.2 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.

10.2.3 Communication security

Mobile 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, mobile 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 Mobile 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 On/Offline pseudonym ID

When a user doesn't want to reveal his real identity for authentication or a service subscription, pseudonym ID can provide a set of untraceable identity for anonymity in online and offline services.

10.4 Mobile Identity Service

10.4.1 Mobile identity query

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

10.4.2 Mobile identity discovery & brokerage

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 Mobile identity self-profiling

Any activity that includes purchases, accesses, payments and movements 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 identity management, search and query.

10.4.4 Privacy protection

There should be no privacy violation when mobile 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 mobile identity that is provided for the service. This technology anonymizes any mobile 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 mobile identity and make a decision automatically whether mobile identity is provided for whom and what scope through negotiating any privacy policy issues with the service provider.

Bibliography

[b-FIDIS05] "Study on Mobile Identity Management," FIDIS, 2005.

[b-FIDIS06] "D11.1: Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity," FIDIS, 2006.

[b-Roussos] Roussos G., Peterson D., and Patel U. Mobile Identity Management: An Enacted View International Journal of Electronic Commerce, (Fall 2003), 81-100

_____