White paper on Identity Management Requirements, Issues, and Directions for Mobile Industry

Version 2.0

20 August 2007

Security Classification Category (see next page)	
Unrestricted	Industry
	Others

Security Classification: Unrestricted

This document is subject to copyright protection. The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association.

Copyright Notice

Document History

Version	Date	Brief Description
0.6	12-Jun-2007	Document v0.6 received email approval by the SRG as a public document.
1.0	20-July-2007	Upgraded version number to 1.0; corrected document classification to Unrestricted.
1.1	3-Aug-2007	Revised version incorporating comments from the DAG and EMC.
1.2	10-Aug-2007	Revised version incorporating comments from PMO.
1.3	20-Aug-2007	Update following SRG comment on title.
1.4	4-Sep-2007	Text update
1.5	24-Sep-2007	Final update, incl. OpenID provision and final reference number
Changes Since Last Version		

Other Information

Type	Description
Document Owner	SRG SPT on Identity Management
Revision Control	As Required

Table of Content

Figures

1. Executive Summary

Identity Management (IDM) represents a broad field of issues with growing concerns for a multitude of stakeholders: government, public security entities, financial institutions, service and content providers, operators of mobile and fixed networks, individual persons and corporations.

Under auspices of the GSM Association[1], the IDM Project[2] has been chartered to develop common guidelines within an overall Identity Management Framework to address operators' requirements to manage mobile subscriber/user identities in support of emerging mobile applications (such as, Single Sign-on web browsing, mobile payments and other UICC[3] enabled applications).

The mobile network infrastructure in conjunction with the UICC intimately supports the subscriber/user authentication. Leveraging this information, together with knowledge of his/her preferences and/or device capabilities, can seamlessly support the user launching into successive applications and services with Single Sign-on experience. Pursuing such use cases as opportunities can enhance the user experience with potential benefits of improved subscriber satisfaction and reduced churns. The important role of the UICC in the mobile operator IDM framework is discussed in Sections 3.1 & 3.2.

The GSMA IDM Project aims to define an Identity Management Framework that can keep pace with innovative mobile services and applications, and one that adapts applicable open standards and best practices to meet emerging requirements and concerns of users and the mobile network community.

Purpose and Target Audience

The main purpose of this white paper is to communicate the operators' awareness of identity management in the contexts of use cases relevant to mobile and convergent operators, the derived IDM requirements both from the mobile network system perspective and to meet the challenges of enhanced SSO user experience in emerging applications.

Internal target audience is all GSMA groups, projects and members affected by IDM. The primary external target audience includes SDO and industry fora working on IDM global solutions. A secondary external target audience includes Service Providers and other IDM eco-system parties, as natural partners to the mobile operator community.

Summary

This whitepaper reports on the Gap Analysis comprising of operator use cases, requirements and a survey of relevant IDM standards and technologies.

Key features of this gap analysis include:

[1] See www.gsmworld.com/news/statistics/index.shtml and www.gsm.org.

[2] ***Note: This version of the white paper is based on activities within standards bodies such as 3GPP and the Liberty Alliance. The possible impacts of other initiatives, such as OpenID, are for further study.***

[3] UICC: Universal Integrated Circuit Card (also referred to as 'Smartcard'). The UICC is evolved from the SIM card commonly known to GSM phone users; however the 'SIM' functionality is now one of multiple applications that can reside in the UICC, e.g. 2G SIM (TS 51.011) and 3G USIM (TS 31.102). See also Glossary of Terms.

- Analysis of over 30 mobile service/application use cases motivated by parallel GSMA projects focused on SIM enhancements and M-Payment applications.
- Input from operators regarding issues and challenges arising from their existing IDM infrastructure and operations.
- IDM requirements derived from the above two inputs.
- A survey of relevant 3GSM network and UICC standards, industry fora specifications and notable vendor solutions with a high level comparison of their capabilities against the operator IDM requirements with any significant gaps or dependencies identified

Key IDM Framework requirements derived from the gap analysis are categorized in the following aspects (see Section 6):

- Trust Worthiness & Auditability
- SIM/UICC Focus
- Alignment With Open Standards
- Single Sign-On & Sign-Off
- Multiple Domains And Circles Of Trust
- Hierarchical Identities supported
- Identity Attributes supported
- Multi-Factor User Authentication
- Multi-Tier Authentication
- Network Access And Services Independent
- Authentication Method – Usability
- Subscriber And User Privacy

Key findings from the IDM technology survey are summarised below (see Section 7):

a) 3GPP GAA/GBA provides a solution to leverage existing 3GPP tokens (i.e. USIM/ISIM) as the basis for obtaining other tokens that can be used towards outside service providers.

b) 3GPP and Liberty Alliance specifications combined appear to offer the most likely complete IDM framework solutions in the 3GSM operator environment. Relevant building block capabilities (e.g. ETSI SCP USSM[4] specifications for the UICC) are sufficiently mature.

c) 3GPP GAA/GBA interworking with Liberty Alliance ID-FF and ID-WSF has been defined in a technical reference TR 33.980.

d) Smartcard technologies are sufficiently mature to support both authentication of identities and the federation of various identities. They can support several tokens, both in the context of 3GPP access (i.e. based on USIM/ISIM) as well as generic Internet based access.

e) UICC compliant to Rel-7 is a crucial technology required to support functionalities and requirements envisaged in the mobile operator centric IDM Framework.

[4] USSM: UICC Security Service Module, TS 102 569 Rel-7, (Rel-7 TS 102 266 Stage 1 and 102 569 Rel-7.Stage 2 specifications).

f) Liberty Alliance provides the most commonly agreed model for IDM interoperability inside operator Circle of Trust (CoT) and between Circles of Trust; both Single Sign-On and hiding of real identity of the user by means of federation are supported. Microsoft/IBM WS Federation also provides this option. Hence, it needs to be further ascertained as to:
    - Which inter-domain federation solution is most suitable to meet the user and mobile industry requirements?
    - How to solve interworking (e.g. Liberty compliant IdP/SP to WS Federation-SP/IdP) or, if possible, convergence between federation technologies (e.g. ‘Concordia’ initiative in Liberty Alliance).

The main conclusion from the Gap Analysis is that, with specific dependencies duly noted as above (including solutions expected from the Concordia initiative), based on available information, it is technically feasible to formulate an IDM framework by combining the Liberty Alliance model and the 3GPP GAA/GBA and Rel-7 UICC capabilities, as well as other means, to fulfil the user authentication, whereby the operator could play the role of IdP.

Based on findings from the gap analysis and this conclusion, work is continuing in the GSMA towards defining an IDM Framework that enables user friendly access to new services and applications with increasing demand for robust security and user privacy. This IDM Framework will also meet operator imperatives of efficiency, scalability and open interoperability with diverse key players of IdPs and SPs.

Lastly, it is recognised that major industry efforts in Identity Management based on open standards and fora specifications (such as, 3GPP, the ITU-T Focus Group on IDM and Liberty Alliance) are continuing, the outcomes of which may well influence the current mobile industry’s understanding and directions of IDM as discussed in this paper.

2. Glossary of Terms

The following glossary of terms is adopted by the GSMA IDM Project.

Access Control	A discrimination process of determining whether an actor X (e.g. a person, program or device) is allowed to have access to data, functionality or service Y.
Assertion	A statement by an actor towards a concerned party concerning the Identity of another actor. Usually this statement is made by an Identity Provider (IdP) towards a Service Provider regarding the validity of an ID Claim made by a User.
Attribute	A description of a characteristic of an identity. Examples include: hair colour, age, presence status, location. Note that an attribute may be uniquely identifying the identity in which case it is an identifier. Also see: Identifier, Identity.
Authentication	Authentication is the overall process of establishing that the actor being authenticated is indeed the actor in whose name assertions are being made, with an implicit or explicit level of confidence and liability. The actor in question may be a human or any non-human system entity (client, server, application, etc). The authentication authority may perform authentication for the benefits of another that resides in another domain.
Authentication authority	An actor guaranteeing that an assertion is indeed correct, with an explicit or implicit level of confidence and liability.
Authentication Level	A hierarchical assignment of authentication methods reflecting increasing strengths to resist violations and attacks.
Authentication Mechanism	Functions that validate claimed identities and that output a status that is either true (verified) or false (rejected). Also see: Mutual and Single sided.
Authority	A data structure that can be validated and that contains one or more identifiers and various contexts.
Certificate	A data structure that can be validated and that contains one or more identifiers and various contexts. It is an apparition of a credential.
Circle of Trust	A federation of service providers and identity providers that have business relationships and operational agreements and within which actors can interact in an environment characterized by implicit or explicit level of security.
Credentials	Actor-specific information that is transferred stored and processed in order to authenticate an actor or authorize a transaction. Credentials may be of three different types: - “Something you know” (e.g. a password) - “Something you have” (e.g. a bank card,) - “Something you are” (e.g. an iris reading, a MAC address)
Data Retention	Retention of traffic data for forensic purposes. In Europe regulated by the EU-Directive on Data Retention (2005) that mandates operators to retain traffic data logs (time, addresses etc.) from 6 to 24 months.
Domain	A business or governmental area characterized by one supreme administration authority and a set of rules (policy) that applies within its context and confinement.
End-User	A physical person operating through a client.
Entity authentication	When the identity information representations belonging or relating to the same actor, belonging to different IdPs are linked or bind together (see also user authentication).

Federated Identity	When the identity information representations belonging or relating to the same actor, belonging to different IdPs are linked or bind together.
Identifier	An attribute that is unique within a defined scope. Examples are: MSISDN, email address, account number. Also see: Attribute, Identity.
Identity	The collective aspect of the set of characteristics by which an actor is uniquely recognizable or known. The set of behavioural or personal characteristics by which an actor (e.g. individual or group) is recognizable. An identity is described by its attributes, some of which may be identifiers. Also see: Attribute, Identifier.
Identity Claim (ID Claim)	A claim made by an actor stating its identity. Without validation, no assumptions can be made regarding the actor's identity. An Identity Claim is usually made by a User towards a Service Provider.
Identity Federation	The process of setting up a cross-domain relationship and the act of requesting, passing and using user-related information ***across*** different administrative domains. In this context, federated identity standards define what amounts to an "abstraction layer" ***over*** the legacy identity and security environments of these diverse domains. Each domain maps its own local identity and security interfaces and formats to the agreed upon identity federation standards which are to be used externally, without the need to divulge sensitive subscriber data.
Identity Management (IDM)	A set of processes, technologies and services in order to manage principals' identities (creation, maintenance and termination of principal accounts), secure access to the operator's resources (data and services) and protect principals' private data.
Identity Mapping	Mapping of identities between different IdPs or between local subsystems.
Identity Provider (IdP)	A provider that manages identity information including providing that information to other actors, on behalf of users and also provides statement of authentication to other actors.
Identity Token	A credential used in a specific context.
IMEI	International Mobile Equipment Identity: a globally unique identifier (hard-coded in the handset).
Implicit Authentication	A result when two or more communicators share the same crypto key-pairs and decryption works OK.
Implicit Authorization	The result of authentication alone if non-discrimination for different allowances is executed among defined users or processes.
IMSI	International Mobile Subscriber Identity: the basic structured identifier for the SIM/UICC in GSM mobile systems.
MSISDN	Mobile Subscriber ISDN Number: a structured Identifier for the subscriber indicating his A-Number.
Multi-tiered authentication	The actor is initially authenticated by an identity provider. The actor is then to be re-authenticated due to a requirement for another form of authentication, and as a result of a policy decision. Ultimately, the actor must present another assertion of identity, such as, a public-key certificate.
Mutual authentication	Mutual authentication implies that the authenticating actor authenticates itself with the actor being authenticated as well as vice versa.
Policy	A Set of rules that regulates authorizations as well as levels of authentication.
Qualified Certificate (QC)	An X.509 certificate issued to physical persons that fulfils the requirements given by ETSI and IETF standards.

RADIUS	Remote Authentication Dial In User Service: the most common AAA (authentication, authorisation and accounting) protocol for Internet accesses today.
Registration	The process of binding a person (entity, object or similar) to an identity. Registration normally comprises of: 1. Enrolment. 2. Binding between a verifiable user ID and a system-assigned ID (policy dependent). 3. Provisioning (client and systems).
Registration Provider	A function that is responsible for the enrolment of physical users into the identity registry of the IdP, where the user is represented by one or more identifiers. The RP executes necessary controls to corroborate that the identifiers really represents the correct user, and for which the RP also may be liable. Depending on policy and available technology, a registration may include physical appearance and authentication of the user by provisioning of legally approved and valid proof of identity means like passports, driver's license with picture, biometrics, etc. RP function may also include the storage of copies of such proof for an applicable time. Finally, it may include external verification controls against legally approved databases like social security registries. The policy may depend on national and international law, system, and service (registration of a bank account owner differs from a Telco subscriber). Comparable concepts are the formal LRA and RA in PKI systems, e.g., IETF RFC 2527, and also ETSI TS 101 456 for Qualified Certificates.
Service Provider (SP)	Service Provider is a provider of services and/or goods, which may require an actor authentication and/or transfer of actor information for purposes of a particular transaction.
SIM	Subscriber Identity Module: an application on the UICC that stores and handles the Subscriber identities (IMSI) and also the authentication and session key derive functions for GSM (A3/A8)
SIM Toolkit (SAT or STK)	SIM Toolkit provides a set of commands which allow applications, existing in the UICC, to interact and operate with a mobile client which supports the specific command(s) required by the application. Using the SIM Toolkit, applications can be downloaded to the SIM in a secure manner.
Single Logout	Same as Single Sign-Off.
Single Sign-Off (aka Single Sign-Out)	When a user logs out, all sessions initiated by the single sign-on that might be open are terminated for that user, and closed.
Single Sign-On (SSO)	The process and the notion of an actor being authenticated once for later access to multiple resources and services across security domains
Single-Sided Authentication	Only one side in a communication session independently to authenticate each other. Also see: Mutual Authentication.
Subscriber (also known as Customer or Bill Payer)	Role carried out by a company (usually represented by an administrator) or a person (or a group), which pays for the services offered by the operator. These services are used by the End Users linked to the Subscriber (i.e. 'Subscriber: End User' relationship is 1:N, where N=1, 2, …). A person (or a group) may play both roles, Subscriber and End User, but also only one of them.
UICC	A physically secure device, an IC card (or 'smart card'), that can be inserted and removed from the terminal equipment. It may contain one or more applications. Examples of such applications

	may be a USIM and the SIM. Popular: erroneously denoted as the 'SIM' or 'SIM-card' (SIM is an application on the UICC).
User Agent	Software that a "user" interacts with directly. A user agent typically implements a user interface.
User authentication	The process of authenticating a personal (physical) user. User Authentication may consist of one, or combinations of the following (independent) three elements: something the user know, has or is. If only one factor is used, UA is denoted as "weak" (like PIN or password only); 2-factor UA is denoted "strong".
User authentication methods	Commonly classified as being one-factor, two-factor, or three-factor, whereas the said factors are normally: "something you have", i.e. a physical device (e.g. a smart card), "something you know" (e.g. a password), or "something you are" (e.g. a biometric factor, such as a fingerprint). Also see: Credentials.
USIM	An application on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security.
Validation	The process of determining whether an Identity claimed by an actor (see Identity Claim) is valid, possibly on behalf of a third party. The result of this process is an assertion towards the concerned party on whether or not the ID claimed by the actor is valid. Validation is usually requested by an SP towards an IdP when a User has made an ID claim.

3. Introduction

The GSMA Identity Management project aims to define a common Identity Management framework comprising of a functional architecture with specific references to best suited technology solutions based upon which the Operator can play the role of the Identity Provider (IdP)[5]) and one that adapts applicable open standards and best practices to meet emerging requirements and concerns of users and the mobile network community.

The great resource tapped by the Identity management is the relationship with the subscriber/user[6] as well as a growing amount of knowledge about the subscriber/user, i.e. identity data, comprising of identifiers (e.g. IMSI, MSISDN, IMPI, IMPU, digital certificates) and possibly other attributes (e.g. age over 21, location data, presence status). The said relationship and data, although established for other purposes, can be utilized in a whole new set of services within solely within the operator's domain, or in conjunction with third parties, hence improving the user experience and offering potential for commercially viable end user services.

[5] - Note that Mobile Operators in many cases may also be Service Providers (SPs).

[6] Within IDM, the distinction must be made between the (end) user and the subscriber. Whereas the (end) user is directly related to the device, the subscriber is directly related to the subscription. Multiple users may be authorised/allowed to consume services linked to a subscriber account (e.g. in a family or the enterprise or family setting). Unless specifically authorized to act as a proxy of the subscriber, users generally are not permitted to access to or modify the subscription profile data. In IDM discussion in this paper, the distinction between subscriber and user will be called out, as applicable (e.g. whenever user privacy versus subscriber privacy or access to subscriber profile is involved); otherwise, the terms 'subscriber' and 'user' are used interchangeably. See also Glossary of Terms for more information, and Note in Section 4 – Eco System.

For instance, use of smartcard technology[7] is a differentiating characteristic and part of the foundation of the GSM mobile network platform. To date, GSM smartcard technology, together with the mobile network infrastructure, fulfils authentication of mobile subscriber access to basic mobile services; this is evolving rapidly to enable user access to enhanced services and applications over the 3G network and beyond.

Within the context of the GSMA IDM project, the smartcard continues, through its existing and emerging standardised features, to present unique new opportunities for supporting user access to enhanced services in ways consistent with current managed user experience while promoting subscriber satisfaction and reducing churns.

The business drivers underlying this project are that ease of use and convenience are requirements for any mobile service. While secure and reliable identification of the user not only is a pre-requisite for access to basic mobile bearer services, it is becoming an increasingly important factor in the provision of online and point of sale services.

Therefore, to successfully provide new mobile and online services, network operators have to ensure secure user identity authentication and secure, user-friendly propagation of identity information to a variety of service providers. Moreover, this propagation of information needs to be in-line with accepted business practices and other applicable legal and regulatory considerations,

3.1 Business Drivers for IDM Framework

An ideal IDM framework should enable user friendly access to new services and applications with increasing demand for robust security and user privacy; it must also meet operator imperatives of efficiency, scalability and open interoperability with diverse key players of IdPs and SPs. Operators are motivated by the promises of a well defined IDM framework that can maximise the potential for tangible benefits.

For instance, the potential for mobile operators could be classified and described as follows:

1. Re-use of authentication status combined with knowledge of user/subscriber profile information or relationships and knowledge towards a new set of services within the operator’s own domain or in third party applications. For example, the operators could expose payment interfaces to the Internet merchants of both digital and physical goods, strong authentication capabilities to corporate users (e.g. VPN), banks, and the like. Such “micro-services” could also be integrated to a higher degree that can offer great convenience and utility to the benefits of users/subscribers..

2. User friendliness in service access through Single Sign-On across service domains (operator-operator, operator-service providers, both intra- and inter-Circles of Trust); in addition, exposure of user information (such as, personal preferences or device capabilities) to enhance the user experience of new services. Here, benefits of effective IDM would be increased usage of other services (browsing, messaging, mobile payment, etc.).

In both cases above, the business drivers are quite clear and will become even more important as the service portfolio and data service usage expands.

[7] - See footnote 2.

The UICC is the key part of GSM and 3GSM mobile networks that is symbiotic with the subscriber's mobile service subscription and should arguably be central to Identity Management plans in authentication contexts. Therefore, operators could act as a primary identity provider to the subscriber for mobile products and services. This operator role may also co-exist with operator support to third party secure applications enabled by emerging UICC secure domains capabilities being standardised, whereby the third party SP can be the IdP (see Section 4 - Eco System)

In the case of the operator acting as the IdP, the Identity Management Framework should facilitate the mobile network as an effective and efficient access point to mobile products and services, managing its user's identity and acting as a trusted party and proxy on behalf of the user towards third parties/service providers.

The target IDM Framework will:

- Promote and facilitate usage of data services, both those in the operators' domain as well as third party applications.
- Maximise benefits of the existing user/subscriber relationships and data.
- Position the UICC as a key Identity Management component for authentication.
- Support IMS-enabled services.
- Support for Convergent (Fixed-Mobile) Services, i.e.
    - IDM should be network access technology agnostic (same user via different access channel should bring out the same identity).
    - IDM should support several authentication mechanisms (UICC and non-UICC based) to cover scenarios where UICC-based authentication is not suitable for the service or UICC is not present (e.g. authorised user access to an operator portal via Internet for purchasing of ring tones from the operator or for managing his/her account, etc.).
    - IDM should support awareness and reuse of mobile subscriber identities if his mobile and fixed network subscriptions can be linked. In this case, it should be possible to leverage synergy between his two service accounts (e.g. a mobile user on an active mobile connection, upon arriving home, his mobile connection should be able to automatically switch over to his fixed network service without dropping the connection).
- Support IDM interoperability:
    - Inside the operator Circle of Trust (CoT): between the operator as ID Provider and (3rd party or internal) Service/Content Providers having business relationships with the operator.
    - Between Circles of Trust (CoTs): both “operator CoT-to-operator CoT” and “operator CoT-to-non operator CoT”.

3.2 Motivations for using the UICC/(U)SIM

To sustain viable commercial service offerings, ID Management is normally a fundamental responsibility for a majority of Service Providers. Within a specific Service Provider service domain, the ability to identify users and personalise services requires an efficient, scalable, and reliable means to determine users' identity and to store personalization attributes.

Operators carry out the task to authenticate subscribers prior to authorising access to services in their networks. In the GSM/3GSM environment, the UICC hosts the relevant authentication applications (i.e. SIM, USIM, and ISIM). The UICC is the key element in Operator networks to perform authentication and grant authorisation to subscribers when they access a GSM/3G Network. Specifically, Operators could utilise the Generic Authentication Architecture 'GAA' (Ref: 3GPP TR 33.220 Rel-6) in conjunction with the UICC to act as Identity Providers for the GSM/3G services they manage.

In the foreseeable future, Operators could extend their current Identity Provider role such that they can act as Identity Providers for services they do not manage directly. For example, an Operator can be an IdP for services that are hosted/managed by third party Service Providers. In this way Operators can have visibility at some level, thus be able to participate in the ID management of the Services not necessarily provisioned through the Operators networks. Such extensions of operator infrastructures will involve both the network and UICC capabilities so that Operators can manage (establish, update, revoke, etc.) multiple user identities.

Going forward, the UICC can serve as the token that allows users:

1. To be identified when they access GSM/3G enhanced services and applications from the Home Operator beyond basic mobile bearer services;
2. To be identified when they access services offered by other Operators or third party Service Providers in which the Home Operator acts as the IdP.
3. The UICC is a familiar technology to the GSM/3GSM user experience for basic mobile access services; preserving this user acceptance and perception of the smartcard as a trusted environment for access to enhanced services is both intuitive and a natural extension from the user perspective.
4. The UICC being a tamper-proof, physically removable device comprises of CPU and secure memory resources for crypto algorithms and keys; it is designed to be mobile device independent and can be transferred to and used in other qualified devices than mobile handsets. The transportability of the UICC (something you have) in conjunction with password (something you know) lends itself to supporting multi-factor authentication for certain high-security applications (e.g. enterprise and government) accessed via mobile devices. With the arrival of non-conventional mobile devices (e.g. UICC in HSPA enabled laptops), the scale and depth of more challenging data applications and their need for IDM support is expected to rise.
5. International standards and/or de facto standard specifications on Identity Management schemes that rely on smartcards already exist (e.g. Liberty Alliance); interworking of such IDM standards (Liberty) with Operator infrastructures has been studied in 3GPP specifications (see 3GPP TR 33.980 Rel-7). Such a study has been kept in due consideration in the Identity Management project.

4. IDM Eco System

An IDM Eco System is assumed within the Identity Management Framework. Certain basic roles are played by three primary actors:

- The User (or Principal).
- The Service Provider (SP).

- The Identity Provider (IdP)

Note: The Subscriber (one who has established an account with the mobile operator) typically is also the User. However, multiple users may be authorised to consume services contracted in a mobile service subscription (e.g. an enterprise account with numerous employees, or persons within the same family). For purposes IDM discussion herein, whenever user identity data formally registered as part of the mobile service subscription is relevant, 'Subscriber' may be mentioned specifically; otherwise, 'User' is mentioned in a generic sense without qualification. The Subscriber role can be viewed as an instantiation of the User role; similarly 'Anonymous User' is another instantiation of the User role, where anonymity is enforced.

The term 'Identity Provider' appears to be too broad and insufficient to pinpoint varying roles necessary to be fulfilled in an IDM framework. In the GSMA IDM framework, the IdP is defined as an actor that plays, at the minimum, the role of Authentication Provider, Attribute Provider, or both. In addition, since the UICC is effectively acting as an extended element of the mobile network infrastructure, the operator could play one or more of the following roles:

a. Authentication Provider (AuthP)
Validates the credentials and makes authentication assertions (i.e. normally owning the associated risks).

b. Identity Attribute Provider (AttrP)

Facilitates sharing the user's defined attributes (typically a fairly diverse set of information may be supported) to trusted parties.

c. UICC "Real Estate" Provider (REP)
The UICC is a physical storage container and placeholder for various types of identifiers, security functions, keys and authorizations. Some functions and contents are normally hard coded before distribution, and some can be dynamically both uploaded and managed. It can be seen as "Real Estate" (analogous to a secure property administered under 'rental agreement') provided by the MNO. UICC capabilities supporting multiple Security Domains are being standardised in Global Platform and ETSI SCP, which will enable significant opportunities for the operator as UICC Real Estate provider to various third party SPs (Ref: Global Platform Card Specification v2.2, ETSI SCP 102 225 Rel-7 and 102 226 Rel-7).

d. UICC "Real Estate" Management Provider (Mgmt REP)
Provides managed services required in conjunction with the "Real estate", which may include third party application installation and provisioning, support services, etc.

Note that in the case of UICC Real Estate rental whereby a third party SP can own and operate a highly secure application within one of the security domains; thus, the third party SP may play the role of IdP (specifically, as Authentication Provider and/or Attribute Provider), while the operator may retain its roles of the REP and Mgmt REP.

To complete online services or transactions, in addition to the IdP, there is a Service Provider, who provides online services and/or content. The SP may require Subscriber/ User (Principal) authentication and/or transfer of Subscriber/ User (Principal) information for purposes of a particular transaction, as depicted below.

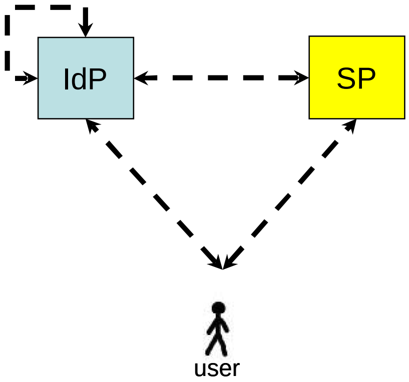

Figure 1 - Basic IDM Roles

To get access to a service (as an example), the following steps may be taken:

1. The user registers with an IdP (e.g. the Authentication Provider).
2. The user requests to access to a service.
3. The SP asks the IdP if it has validated the user's credentials (the exchange may be performed by redirecting the messages through the user).
4. The IdP verifies the user identity and checks if the credentials have been recently validated and then announces its decision to the SP. If the user credentials have not yet been validated, it may be done at this step.
5. If the user is not registered with the IdP that is used by the SP, the IdP will federate with another IdP with which the user was previously registered. Note that federation might include a chain of IdPs to link the involved SPs together in order to validate the user's credentials.

Based on the above course of action, the following twelve high-level functions required have been isolated.

User-to-Identity Provider

1. Provides means for user to register with IdP.
2. Provides means for IdP to assign a proof of identity to be used by the user.
3. Provides means for user to manage policies for the gathering and distribution of identity information by IdP (i.e. protect its privacy).

User-to-Service Provider

4. Provides means for user to be able to state its identity (client authentication).
5. Provides means for server authentication.
6. Provides means for facilitating choice of authentication/attribute class (by strength, type, validity, level of confidence, etc.

Identity Provider-to-Service Provider

7. Provides means for SP to ask IdP to validate a user's identity.
8. Provides means for discovery/establishment of relevant IdP.
9. Provides means for attribute distribution (status, location, credit worthiness, etc.).
10. Enables transfer of information required for determining risk (level, financial value, ownership, etc) and hence established level of trust.
11. Provides the use of pseudonyms to maintain the user's privacy.

Identity Provider-to-Identity Provider

12. Provides means for IdP to federate with another IdP maintaining all of the functionality that is offered to the SP

The above twelve functions identified were used as criteria in the technology survey as discussed in Section 7.

5. Generic Use Cases

To obtain a common view on the requirements for Identity Management, over 30 mobile service/application use cases were analysed in the GSMA IDM project. Many of the use cases refer to complex services, but from an Identity Management point of view they can be represented in a limited set of generic use cases in the following.

Four generic use cases (A, B, C, D) are identified for the use cases from the topology point of view, i.e.:

Use case A

Two parties provide identity data or authentication to a third party service provider. One of these two parties is an Operator; the other may be another Operator or a non-Operator party.

Possible applications: multi-party gaming.

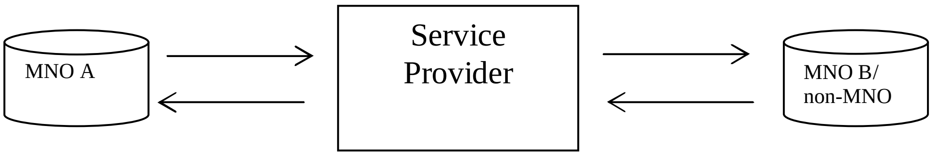

Figure 2 - Generic use case A

Use case B

Operator A provides identity data or authentication to third party service provider.

Possible applications: Mobile purchasing, age verification, loyalty schemes.

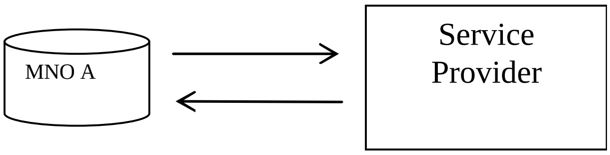

Figure 3 - Generic use case B

Use case C

Operator A provides identity data or authentication to Operator B.

Possible applications: Mobile purchasing of content where Operator B acts as service provider, service-aware roaming.

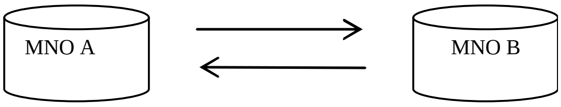

Figure 4 - Generic use case C

Use case D

Operator A utilises identity data or authentication when providing a service to its subscriber.

Possible Applications include single sign on for IMS applications.

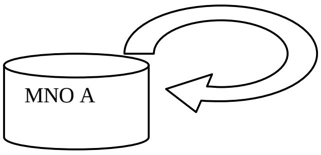

Figure 5 - Generic use case D

6. Mobile Network IDM Requirements.

The IDM requirements contained in this section were derived from over 30 mobile service/application use cases, including other IDM requirements derived from existing and mobile industry inputs. Such inputs were identified as either issues or concerns based on the operators' current IDM infrastructures or as desired enhancements in IDM operations going forward. The mobile network IDM requirements have been summarised in the following categories:

1) Trust Worthiness & Auditability

IDM Framework must be trusted and must be capable of conveying information relevant to risk assessment or possible auditing (e.g., time stamp, or other specifics of the authorization related to, the degree to which risk is being taken for a specific transaction).

2) SIM/UICC Focus

IDM Framework should optimize current levels of control and management of trust and shall apply hardware based UICC advanced standards. It will also be able to support UICC "Real Estate Rental" to third party Service Providers.

3) Alignment With Open Standards

IDM Framework shall align with relevant open standards whenever available and must provide/support standardized, industry-agreed authentication categorization.

4) Single Sign-On & Sign-Off

IDM Framework shall be able to support Single Sign-on experience for mobile users when consuming services/applications hosted by the operator and in external domains (i.e., other MNOs, Service Providers and the Internet). Existing operator 3G security infrastructure, including: GAA/GBA, IMS and Smartcard technologies are used, where applicable and appropriate.

5) Multiple Domains And Circles Of Trust

IDM Framework shall support multi-operator and multi-service provider scenarios, and shall support federation of service providers and identity providers that have business relationships and operational agreements, within which actors can interact in an environment characterized by implicit or explicit level of security.

6) Hierarchical Identities

IDM Framework shall be able to, within the same session, identify a principal as a member of a group based on certain profile (i.e., sufficient for some services) and/ or as an individual (i.e., necessary for some services).

IDM Framework should support in the same session a principal being identified as a SUBSCRIBER and/or USER.

7) Identity Attributes

IDM Framework should be able to convey “attributes” associated with a user identity. Some attributes may be identifiers: pseudonyms or not, referencing a person (e.g., MSISDN, email) or a group (e.g., ISDN, “Board of Directors”); other attributes may be: roles, user profile data (e.g., age, sex and name) or service data (e.g., location, presence, contact book).

It will need to concatenate/combine the authenticated User ID with additional attributes (e.g., proof of minimum age, membership based on certain profile) as part of specific transaction authorization criteria and will need to provide linkage to other Operator service enablers or databases may be required.

8) Multi-Factor User Authentication

IDM Framework user authentication solutions shall be able to support multiple factors of security (i.e., “something you know”, “something you have” and “something you are”) in accordance with applicable standards.

9) Multi-Tier Authentication

Multi-tiered authentication should be supported, including:

- Authentication involving multiple operator networks.
- Authentication involving multiple service providers.
- Authentication involving both mobile and fixed network domains.

10) Network Access And Services Independent

IDM Framework should be possible to reuse Network Authentication validated via different operator network access, if available and also should be applicable to different access/ browsing technologies, e.g.,: Operator Network: WAP Browsing, SMS/MMS, Web Browsing (via GPRS or ADSL) and Other Networks: Inter-connected Operator Network or the Internet.

It should be able to support different types of services and their characteristics, e.g.

- Operator Services, such as Subscriber oriented services and User oriented services.
- Convergence services.
- Third Party Services.

11) Authentication Method – Usability

IDM Framework should take into account “usability” of authentication mechanisms; depending on access technology, and must be able to handle failed authentication and other types of transactions in a least disruptive manner.

12) Subscriber And User Privacy

Both Subscriber Privacy and User Privacy Protection should be ensured.

7. Survey of IDM Technologies

Recognising that IDM is a broad field with many players and numerous embedded technologies and solutions, the IDM Project conducted a general non-exhaustive survey of available IDM technologies (i.e. applicable standards, fora specifications, and in some cases, vendor solutions). The purpose of this effort was to: (a) build team understanding of the state of the art, and (b) gain insights as to potential solutions available which may be directly applicable to the IDM framework to be defined later.

The following IDM technologies have been assessed against the derived requirements:

Technology	**References** (latest version, unless otherwise specified)
3GPP GAA/GBA	TS 33.220 TS 33.221 TS 33.222 TR 33.980
3GPP USIM	TS 31.102
3GPP ISIM	TS 31.103
3GPP IMS	TS 23.228
3GPP GUP (Generic User Profiles)	TS 23.240 TS 23.241
Liberty Alliance	http://www.projectliberty.org/
SAML2.0	OASIS
Smart cards; Identity Files and Procedures on a UICC	ETSI TS 102 350
UICC Security Services Module	ETSI TS 102 266 and 102 569
Secure Channel between a UICC and an End Point Terminal	ETSI TS 102 484
WS-* (Microsoft/IBM)	http://www-128.ibm.com/developerworks/library/specification/ws-fedworld/
Microsoft CardSpace	http://msdn2.microsoft.com/en-us/library/aa480189.aspx
SIP Authenticated Identity	RFC 4474
SIP P-Asserted-Identity	RFC 3325
OMA Identity Management Framework	OMA-RD_Identity_Management_Framework-V1_0-20050106-D
OMA WAP Wireless Identity Module	OMA-WAP-WIM-V1_2-20050322-C
OMA Web Services Network Identity	OMA-ERELD-OWSER_NI-V1_0-20051220-C OMA-AD-OWSER_NI-V1_0-20051220-C

Table 1 IDM Technologies

Key findings from the IDM survey are as follows:

1. 3GPP GAA/GBA provides a solution to leverage operations of existing 3GPP tokens (i.e. USIM/ISIM) as the basis for obtaining other tokens that can be used towards outside service providers.

2. Currently, IMS can be used as a single sign-on solution for SIP-based services between mobile operators but not easily towards other non-mobile players. It is anticipated that this limitation may be overcome with SAML and IMS assertions combined.
3. 3GPP and Liberty Alliance specifications combined appear to offer the most likely complete IDM framework solutions in the 3GSM operator environment. Relevant building block capabilities (e.g. ETSI SCP USSM[8] specifications for the UICC), or generic capabilities inspired by best in class vendor solutions will be investigated further for possible adoption or integration into the target IDM framework in a cohesive way.
4. 3GPP GAA/GBA interworking with Liberty Alliance ID-FF and ID-WSF has been defined in a technical reference TR 33.980. A technical specification TS is not expected as no new technology needs to be provided.
5. The smartcard technologies provide the required support for both authentication of identities and the federation of various identities. They can support several tokens, both in the context of 3GPP access (i.e. based on USIM/ISIM) as well as generic Internet based access.
6. Further details relevant to smartcard standards and technologies are also highlighted. UICC's compliant to Rel-7 will support functionalities envisaged in this project to allow an effective Identity Management in a mobile network. In particular:
   a) 'GBA_U' functionality applicable to GBA aware UICC has been fully standardized since Rel-6.
   b) USSM Stage 1 standardization has been finalized in Rel-7, whereby a draft already exists (see [7]ETSI SCP TS 102 266 v7.1.0), and also a draft already exists for Stage 2 specification (see TS 102 569 v1.1.0). Although improvements could be done, the set of features that is included into Rel-7 and the features existing and already implemented in Java Card[9] 2.2.x will allow UICC's to effectively manage keys and algorithms to authenticate users in Identity Management schemes.
   c) "Secure Channel between the UICC and a terminal end point" standardization will be finalized in Rel-7 as well. An advanced draft already exists (see TS 102 484 v0.2.0), at the time of writing the part on the secure channel between applications is considered complete.
   d) Java Card 3.0 is being standardized; the standardization process should be finalized in 2008. The authorization mechanisms for Java Card API present in Java Card 3.0 could offer an alternative to USSM for the management of Sensitive Objects.
   e) Delegated Management is specified in Global Platform since release 2.1. Operators will be able to give Application Providers the capability to perform loading, installation, extradition and deletion of applications in their Security Domain.
7. Inter-domain federation supports the option of hiding the real identity of the user; Liberty provides the most commonly agreed model.
8. Liberty provides the most commonly agreed model for IDM interoperability inside operator Circle of Trust (CoT) and between Circles of Trust; both Single Sign-On and hiding of real identity of users by means of federation are supported. Microsoft/IBM WS Federation also provides this option. Hence, it needs to be further ascertained:

[8] USSM: UICC Secure Service Module, TS 102 569 Rel-7.
[9] See http://java.sun.com/products/javacard

a. Which inter-domain federation solution is most suitable to meet the user and mobile industry requirements, taking into account the widest market acceptance of the selected solution with respect to third party SPs?

b. How to solve interworking (e.g. Liberty compliant IdP/SP to WS Federation-SP/IdP) or, if possible, convergence between federation technologies (e.g. 'Concordia' initiative in Liberty Alliance).

8. Summary and Conclusions.

The GSMA IDM Project aims to define an Identity Management Framework that can keep pace with innovative mobile services and applications, and one that adapts applicable open standards and best practices to meet emerging requirements and concerns of users and the mobile network community.

This white paper reports on the Gap Analysis comprising of operator use cases, requirements and a survey of relevant IDM standards and technologies.

The gap analysis takes into account the derived requirements of the mobile service/application use cases, ranging from mobility and roaming to new opportunities in the mobile payment scenarios. In addition, other operator inputs were also identified based on issues and challenges arising from diverse IDM solutions in their current infrastructures as well as emerging requirements (such as), the need to support mobile access to convergent services. The sum of these considerations led to derivation of a set of key IDM requirements as presented in Section 6.

A list of significant IDM technologies and relevant standards and industry fora specifications was surveyed (in Section 7) to gain insights on potential solutions to different IDM requirements and aspects of the target IDM Framework. In particular, the emerging smartcard technology and standards were reviewed in detail.

It was concluded that based on available information, it is technically feasible to formulate an IDM framework by leveraging the 3GPP GAA/GBA and Rel-7 UICC capabilities to fulfil the subscriber/user authentication, whereby the operator could play the role of IdP. In addition, inter-domain (IdP-to-IdP and IdP-to-SP) identity federation could be based on at least the Liberty Alliance ID-FF and ID-WSF specifications to enable Single Sign-On experience for mobile subscribers and users in services and applications provided by the diverse service providers and content providers both inside the operator Circle of Trust, and inter-Circles of Trust. Specifically, interworking between GAA/GBA and Liberty implementations can be achieved as defined in 3GPP TR 33.980. Other key dependencies on the ongoing related standards work were also identified.

Based on results discussed in this paper, the GSMA IDM Project is continuing efforts towards defining the IDM framework, which will comprise of a functional architecture with specific references to possible technology solutions to fulfil the stated requirements..

Last but not least, as several major industry efforts in Identity Management based on open standards and fora specifications (such as, 3GPP, the ITU-T Focus Group on IDM and Liberty Alliance) are ongoing, it is recognised that outcomes from these efforts may well influence the current mobile industry's understanding and directions of IDM as discussed in this paper.

9. References

References applicable to the discussion have been provided in context within the various sections in this paper therefore are not repeated here. Due to recent developments in their respective specifications, the following additional references have been noted by the IDM Project team in the deliberation of its work.

[1] Liberty Alliance ID-WSF Advanced Client 1.0 DRAFT Specifications

http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_advanced_client_1_0_draft_specifications

[2] ITU-T SG 17 Focus Group on Identity Management (FG IDM)

http://www.ituwiki.com/index.php?title=Focus_Group_on_Identity_Management