White Paper

# Identity management in mobile services

## Accelerating the mobile service business with Liberty technologies

NOKIA

CONNECTING PEOPLE

# Contents

# Executive summary

New mobile devices commonly have features such as support for packet data transfer (GPRS or 1xRTT), colour screens and XHTML browsers. These raise the user experience to a new level, for instance when browsing for different mobile services. However, because of their size limitations, mobile devices are equipped with limited data entry capabilities using small keypads and have relatively small screens. It is essential to continue to improve the convenience of using mobile services to ensure that they become a success. A seamless service sign-on solution, which is based on open identity management architecture, provides users with a one-click access to personalised services in a way that supports the existing customer relationships and business systems. In more advanced service scenarios, open identity management architecture enables the use of standard user profile attributes, like age and gender, and authorisations for services, such as location, to bring a richer user experience.

An identity provider has a central role in the identity management business. The identity provider can be a company with existing customer relationships, which is positioned in the value chain of the specific service and which is able to orchestrate the business system. In the mobile domain, operators, major vertical and cross-industry portals and selected media houses are well placed to become identity providers. Financial institutions and governments are also well positioned to become the preferred identity providers for their specific markets and for services that need stronger user identities.

However, Nokia believes that mobile operators are in a good position to become the most favoured identity providers: They possess valuable static and dynamic user profile information which can be made available in a controlled manner to third parties through open standard Web Service interfaces. Mobile operators also have the unique ability to seamlessly authenticate users with the phone number on behalf of the service provider, should the customer want true seamless authentication to services.

To enable the creation of the mass market it is critical that authentication in the mobile domain is based on standard, open identity management architecture that can be flexibly adapted to existing business models. Therefore, Nokia is working in the Liberty Alliance Project together with over 160 other companies from various industries to standardise authentication and user attribute management technologies. In July 2002 Liberty Alliance released the specification for opt-in account linking and seamless sign-on. The specification for permission based attribute sharing was released in April 2003.

Since Liberty Alliance released its first set of specifications in July 2002, more than 20 organisations have announced Liberty-enabled products or future plans to build the specifications into their products or services. It is now time for operators and service providers to start deploying the open identity management architecture, make the benefits available to their users and take their position in the mobile service value chain.

# An introduction to identity management

The deployment of packet based mobile networks in most markets has provided mobile users with the capability to access mobile data services in a few seconds. Now is the time to optimise the services to provide a personalised user experience.

Difficulties in using and accessing services have been the most common reasons for slow service adoption. For mobile services to succeed, it is critical that the mobile users are able to get convenient and immediate access to the information and services they need in each situation, without going through long menus and having to enter various user names and passwords. This can be achieved by offering users convenient identity management services.

Identity and user profile are at the core of most digital services, thus efficient identity management will benefit services ranging from accessing bank accounts and corporate email to checking the latest news about sports team and participating in chat groups or peer-to-peer gaming.

Today, browsing is the most common way to access content via the fixed Internet and in certain mobile markets like Japan. With innovative services, fast networks, feature rich devices and convenient identity management services, mobile browsing is now ready to take off and generate revenue globally.

Operators are in the most lucrative position to benefit from increased browsing. They get the increased traffic revenue and can orchestrate the identity management business by taking the position as an identity provider. This will strengthen their customer relationships and result in reduced churn. Operators can also offer user authentication and user attribute broker services to other service providers. A practical example of an identity management service could be an operator offering phone number based user identities to an independent game portal or location data for a fast food chain upon the user's request.

Service providers that would benefit from efficient use of mobile identities include any service with established customer relationships, such as a loyalty programme. By deploying open identity management architecture as defined by the Liberty Alliance Project, service providers can maintain their existing customer and business relationships. At the same time, they can offer their customers effortless access to personalised services. Service providers will also benefit from the increased service usage and standardised interfaces with operators' identity management systems and other service providers.

This document provides an overview of Nokia's vision for identity management. Identity management based on open standards enables mobile users to easily:

- Identify themselves with an appropriate level of traceability and security
- Disclose some of their personal data to various services in a controlled and secure manner so that a personalised service can be provided
- Authorise services and other agents to perform certain actions such as accessing data, sending notifications and charging accounts

All of the above must be done while protecting the user's privacy, avoiding needless disclosure of the user's real identity and with a minimum amount of input and configuration by the users.

# The business of identity management

## Demand for efficient identity management

Several service providers on the Internet are offering users personalised services to improve the user experience and increase customer loyalty. To access their personalised account, users typically authenticate themselves by entering a username and password combination that is unique to the service provider. If the same person always uses the same PC and the services do not require secure authentication, the user can be authenticated by placing a cookie on the PC.


*Figure 1. Mobile service authentication without efficient identity management*

The small keyboards on most mobile devices make it far too cumbersome to enter usernames and passwords. Additionally, cookies cannot be commonly used to store identity information. However, because of screen size, bandwidth and input limitations, companies offering mobile services have an even greater need to offer seamless access to personalised services.

The need for efficient identity management is becoming an issue now that XHTML and colour screens are boosting the creation of compelling services that are encouraging greater use of browsing. For example, during the second half of 2002 the time spent browsing in the Orange France network increased 130% resulting in an average usage of 1Mb per month per user.[1)] In the UK there were over one billion mobile portal page impressions in 2002, with growth during the fourth quarter of 2002 ebing 18% resulting in 13.5 million impressions per day in December.[2)]

Most service providers must maintain close customer relationships making it unacceptable for them to have a middleman controlling their customer relationships. By deploying the open identity management architecture as defined by the Liberty Alliance Project it is possible for service providers to maintain and control their own customer relationships. At the same time, service providers can offer users seamless access to personalised services without frequently having to enter their usernames and passwords. This is achieved by using a mobile operator's authentication services.

## Identity management business system

The identity management business system comprises users, identity providers and service providers. The user has user accounts at identity providers that provide seamless authentication services to one or more service providers. As long as the service provider and identity provider have an agreement on providing seamless access for their common customers, the user can choose to link his service provider user account with the one at the identity provider. The next time the user authenticates at the identity provider, he can seamlessly access his personal account at the service provider within the same authentication domain.

[1)] Ovum Research, December 2002
[2)] Mobile Data Association, 30th of January 2003

The linking and seamless use of accounts in the identity management system involves no exchange of customer data unless authorised by the user. Only the unique identifier known by the identity provider and the service provider is exchanged during each seamless authentication.

The identity provider has a central role in the identity management business. An identity provider can be a company with existing customer relationships, which has a position in the specific service's value chain and which is able to orchestrate the business system. In the mobile domain, operators, big portals and selected media houses occupy the most natural position to become identity providers. Also financial institutions and governments are well positioned to become preferred identity providers for their specific markets and for the services where users need stronger identities.

However, Nokia believes that mobile operators are in a good position to become the most favoured identity providers because they possess valuable static and dynamic user profile information, which can be made available in a controlled manner to third parties through open standard Web Services interfaces. Mobile operators also have the unique possibility to seamlessly authenticate users with their phone number.

### User Benefits

- Immediate and easy access to services through seamless sign-on
- Access to personalised services even without registration
- Ability to use pseudo identities or remain anonymous when using different services
- User is in control of his profile data and can decide on its use

### Operator Benefits

- Increased service usage and stronger customer relationships as a result of improved privacy and better usability
- New possibilities in providing authentication services to external service providers
- Ability to sell dynamic user data like location and presence to service providers
- Open standard provides choice of products from multiple vendors

### Service Provider Benefits

- Ability to offer personalised services even for first time users without registration
- Improved quality of customer data because users feel they are in control of their profile
- Ability to use dynamic user data like location and presence from the operator network

## Business scenarios

A user is likely to have multiple identities from various identity providers, for instance from his mobile operator, bank, government, favourite game portal and others. The identity provider will help the user to manage his identity and the related profile data. In addition, the identity provider will often take care of the user and service authentication and will know or suggest which identity the user should present to a particular service. The user must have complete control over deciding what profile data to disclose and which identity to present. Profile data potentially encompasses a wide range of information from the basic, such as name and address, to preferences for aspects such as languages and sports, to sensitive data such as credit card numbers and location.

Users can authorise service providers to access their profile data attributes located at other service providers known as attribute providers. These attributes can, for example, include location, notification and charging data provided by the network operator on behalf of the user, who might want to remain anonymous to the service. Hence, authorisations allow distribution of profile data.

Providing an appropriate level of privacy for the user will greatly enhance the use of services, due to the sensitivity of some data such as location, medical records or financial details. The fact that users' profile data is stored in multiple locations should be taken into account when designing privacy control functionality.

# Identity management technology

## Business requirements

Mobile and Internet service providers are increasingly facing the same identity management challenges as services in both domains continue to develop. There is clearly a need for an open standard technology for identity management that can be applied to both fixed and mobile services. There is also a strong requirement from many industries for the identity management architecture to be adaptable to existing business models and systems, allowing a flexible development of these.

Companies from several industries came together in December 2001 and founded the Liberty Alliance Project, an open industry forum, to standardise the open identity management architecture. The architecture defined by the Liberty Alliance Project allows users to:

- Identify themselves with an appropriate level of tractability
- Disclose some of their personal data to various services in a user controlled manner so that personalised service can be provided
- Have high levels of privacy
- Authorise services and other agents to perform certain actions such as accessing user data, sending notifications, charging accounts, etc.
- Choose the identity to be presented in a specific context of a certain service
- Control identity by allowing mobile device to issue authorisation decisions

Liberty architecture provides building blocks and a framework for many other enablers to use, including location, presence, payment, messaging, device management and content downloading. The generic identity management architecture as defined in Liberty is needed in all services requiring basic functions such as authentication, authorisation and identity aware Web Services.

## Open identity management architecture

A federated network identity that links the various user identities delivers the benefit of simplified sign-on to users. This is achieved by granting rapid access to resources to which users have permission, but it does not require the user's personal information to be stored centrally. This increases security and improves identity control. With the federated network identity approach, users authenticate once and can retain control over how their personal information and preferences are used by the service providers.

A group of service providers that enable linking of user accounts and which have business agreements in place is known as a circle of trust. The attribute sharing policies within a circle of trust are typically based on:

- A well-defined business agreement between the service providers
- Notification to the user of information being collected
- User granting consent for types of information collected
- Where appropriate, recording both notice and consent in an auditable fashion

It is critical for identity management architecture to be adaptable to the various existing and emerging business models. The open end-to-end architecture defined by the Liberty Alliance Project consists of architectural entities, which are not bound to any network element or location, and allow full federation of entities, functions and responsibilities.

This concept allows the user to bind together and expose separate Web Services about himself in a controlled manner so that he understands who can access what information or Web Service and for what purpose. Liberty architecture automates the discovery of these federated services and the collection of the necessary information to use these services.

Elements of the Liberty architecture

- Identity Provider, manages identities presented to services in the form of authentication assertions, provides also bootstrapping information for finding identity related Web Services
- Discovery service, a directory for identity related services for individual users, also provides authorisation assertions to Service Providers
- Service Provider, an entity providing services such as XHTML portal to users. It also makes Web Service invocations for identity related Web Services, such as location, personal attributes, presence, messaging or wallet.
- Web Services Provider, an entity exposing Web Services related to user identities and representing the user in the Web Services transactions, managing user privacy and access rules.

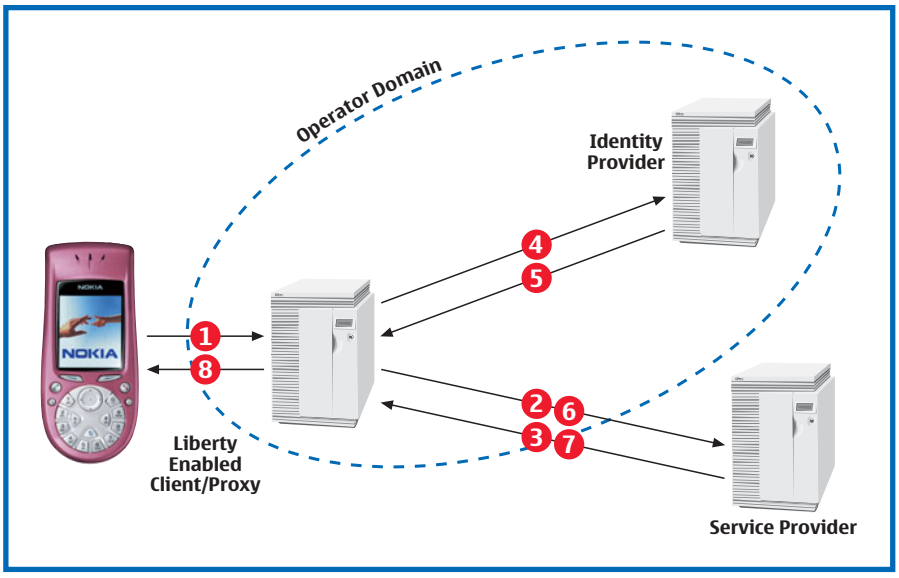


*Figure 2. Operator assisted authentication using Liberty Enabled Client or Proxy*

1 User makes a request for service by clicking a link
2 Proxy forwards request to Service Provider
3 Service Provider asks user to authenticate
4 Proxy redirects authentication request to Identity Provider
5 Identity Provider provides authentication info based on e.g. phone number
6 Proxy redirects authentication info to Service Provider
7 Service Provider provides personalised service
8 Proxy forwards service to the user

## Mobile device in identity management

The most effective way to implement the open identity management architecture is to extend it to the client device. The architecture allows all services to be accessed by two types of client: plain browser clients and Liberty Enabled Clients (LEC).

The first implementations in the fixed Internet have been made using the plain PC browser clients. This method has the benefit that it requires no modification to the existing client software. On the other hand the service provider has no way to seamlessly detect the identity provider of the particular user. So in practice, the service provider has to ask the user to either select his identity provider from a list or manually enter it. This type of user experience can be acceptable for example when using the company intranet and the company is the only possible identity provider but it does not provide adequate usability for consumer services where the number of possible identity providers can be hundreds.

Much better for users accessing consumer services, particularly those services accessed with mobile devices, is to use a Liberty Enabled Client. All services that support the open identity management architecture defined by the Liberty Alliance can recognise from the service request that a LEC is accessing the service. Now the service provider does not have to burden the user with a separate dialogue but can directly ask the user identity from the LEC that redirects the request to the right identity provider.

The LEC can be implemented in the actual client such as aPC, set-top-box or mobile device, or in a network element such as a WAP gateway or HTTP proxy. The service deployment using a LEC in a network element is naturally faster to roll out and it is suitable for users without LEC in their own device. However, the LEC must be in the device to be able to use secure TLS connections or have the same user profile data and identity information available for proximity services, for example over Bluetooth. There is also a risk that without the LEC in the device the length of the URL can become too long for some browsers due to several redirects.

Although it is necessary to have the user profile data in the device, it is not enough. Some parts of the profile, like location, are actually generated in the network and many of them, like presence, have value only if they are available as real time Web Services in the network. It is clear that the user profile has to be stored both in the device and in the network and these two have to be synchronised.

## Implementing Liberty based identity management for mobile services

Although open identity management architecture can be flexibly adapted to various business models there are certain scenarios in the mobile domain that are especially attractive. The Liberty based architecture provides seamless sign-on to both

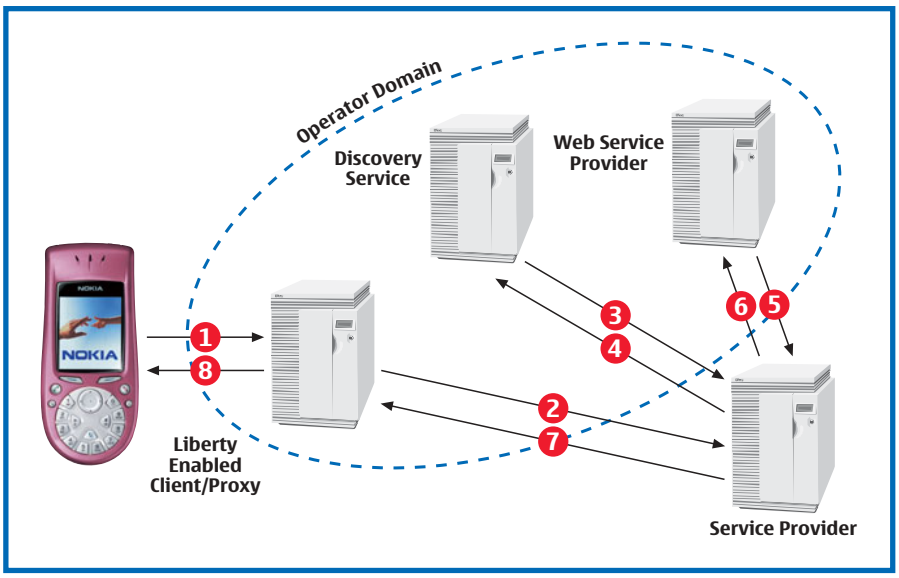


*Figure 3. Liberty Web Service architecture*

1 User makes a request for service by clicking a link
2 Proxy forwards request to Service Provider
3 Service requires access to user attribute and Service Provider asks the address of that attribute from Discovery Service
4 Discovery Service responds with Web Service Provider address
5 Service Provider requests attribute from Web Service Provider
6 Web Service Provider returns the attribute according to user preferences
7 Service Provider provides personalised service
8 Proxy forwards service to the user

operator services and third party services, which is the key value proposition that operators are well placed to take advantage of.

## Federated authentication in mobile services

Figure 2 shows one option to implement Liberty based authentication architecture in the mobile domain. In this scenario, the operator is running identity provider software. It has a Liberty enabled WAP gateway or HTTP proxy and the service provider has added Liberty support for its service. When the user selects a bookmark pointing to the service provider's URL the phone first opens a session with the operator gateway that then contacts the actual service. The service provider recognises from the HTTP traffic that the gateway is Liberty enabled and asks for a Liberty authentication. The operator's identity provider responds with Liberty authentication assertion. The operator can authenticate the user using for example PKI, user name and password or the phone number. The use of phone number is probably the most convenient because the operator can authenticate the user at the gateway automatically. The whole process is hidden from the user and takes only a few seconds.

## Attribute exchange in mobile services

Liberty based identity management architecture provides a generic identity aware Web Services framework, which allows for any identity related information to be exposed as a Web Service. Examples of such services include personal attributes, location and calendar.

Figure 3 shows one possible implementation scenario of Liberty based Web Service architecture in the mobile domain. In this scenario the user is browsing a service at the Service Provider's mobile portal. He selects a link that points to a service requiring his location information. From the HTTP headers the Service Provider finds the address of the operator's Discovery Service that directs the request to the correct Web Service Provider. The Web Service Provider checks that it has the user's authorisation to share the particular attribute, in this case location data, with this Service Provider and it provides the location information for the Service Provider.

Liberty based architecture can empower the user to always control and manage his preferences if he so desires. In the mobile domain a device with Liberty Enabled Client can be used to achieve this goal while retaining the convenience of having the device learning the user's preferences and act accordingly. This is possible both when the user is properly authenticated and when the user is totally anonymous to the service.

## Standardisation

User authentication and service authorisations reside in the core of current and future mobile services. Therefore it is vital to have them based on open and standard technologies. Open standards enable the whole value chain to benefit from healthy competition while service providers and users are not limited to predefined business models. Service providers will also benefit from a choice of solutions resulting in reduced costs for all constituents and allowing the business environment to freely develop.

Open identity management standards provide basic building blocks, which do not focus on the actual service offering or user experience. There can be a variety of different implementations of standards based services, providing much scope for differentiation. Liberty Alliance has a comprehensive interoperability programme that aims to ensure that true interoperability and an open market exists for all Liberty enabled products.

Nokia is active in various industrial alliances and standard bodies where architecture enabling Identity management is being specified. Within these groups, Nokia consistently emphasises ease of use, privacy, the use of non-proprietary technologies and mobile specific considerations.

Through the Liberty Alliance Project, the industry can enable the use of mobile identities for services of all kinds, contributing to a new generation of secure and seamlessly compatible mobile Internet services. Nokia's participation in the Liberty Alliance underlines the need for an open industry specification for seamless communications and transactions on the mobile Internet. The objectives of the alliance are in line with the goals of the Open Mobile Alliance initiative, which focuses on open standards and provides seamless interoperability of mobile services across terminals, operators and markets.

The Liberty Alliance Project has now released the core specifications for the open identity management architecture. The current specifications already include account federation, Web Services framework and the core profile attributes. In the future the amount of standardised attributes will increase making Liberty based architecture even more adaptable to various industries and use scenarios. Several companies have already released Liberty enabled products and the number of commercial service implementations is rapidly increasing.

In addition to the Liberty Alliance Project, open identity management technologies are being standardised in W3C (SOAP, WSDL, XML, XML encryp, XML dsig), OASIS (SAML, WSS), WS-I (basic attributes) and Open Mobile Alliance (location, presence, messaging).

# Nokia's approach to identity management

Nokia has recognised the importance of a user friendly and open standard based identity management solution for the mobile service industry. Nokia is working actively in various industry forums like Liberty Alliance Project, Open Mobile Alliance, 3GPP and OASIS where technology for identity management is being specified.

The core elements of the identity management technology have been specified in the Liberty Alliance Project. Nokia is committed and has been actively contributing to the work in the Alliance since its foundation in 2001. Nokia will launch products supporting Liberty specifications during 2003.

# Conclusions and recommendations

Already today, everybody uses multiple identities. Such use is often associated with identity cards, loyalty card schemes and customer reward coupons issued by various service providers.

Nokia foresees that the mobile device will manage user profile information, being the most convenient tool for authentication, disclosing of profile data and authorising service providers to share information with third parties. However, having the user profile data in the device is not enough. Some parts of the profile, such as location and presence have value only if they are available as Web Services. It is clear that the user profile has to be stored both in the device and in the network and these two have to be synchronised.

Achieving maximum convenience and usability by minimising effort such as typing and configuration, is essential for rapid service adoption. All this should be done in a way that protects the user's privacy.

Identity management based on open technologies as defined in the Liberty Alliance Project benefits users by enabling immediate and easy access to personalised services. Improved user experience will boost service usage and strengthen existing customer relationships, resulting in increased revenue for operators and service providers. Additionally, by implementing open identity management architecture, operators will have new ways to provide authentication services to external service providers. Open standards also ensure freedom of choice and create the basis for interoperability between different products and services.

Standardisation for identity management technology is already mature and an increasing number of standard based products and services are being introduced. Operators and service providers can take advantage of the market situation by an early deployment of open standard based identity management architecture to provide a seamless user experience and secure their market position.

# Glossary of terms and abbreviations

| | |
|---|---|
| **GPRS** | General Packet Radio Service |
| **HTTP** | Hyper Text Transfer Protocol |
| **LEC** | Liberty Enabled Client |
| **MSISDN** | Mobile Subscriber Integrated Services Digital Network |
| **OASIS** | Organisation for the Advancement of Structured Information Standards |
| **SAML** | Security Assertions Mark-up Language |
| **SOAP** | Simple Object Access Protocol |
| **URL** | Uniform Resource Locator |
| **W3C** | World Wide Web Consortium |
| **WAP** | Wireless Access Protocol |
| **WSDL** | Web Service Descriptor Language |
| **WS-I** | Web Service Interface |
| **WSS** | Web Service Security |
| **XHTML** | Extended Hyper Text Mark-up Language |
| **XML dsig** | Extended Mark-up Language digital signature |
| **XML** | Extended Mark-up Language |
| **XML encryp** | Extended Mark-up Language encryption |

# References and links to standardisation

Nokia, http://www.nokia.com, Service Personalisation

Liberty Alliance Project, http://www.projectliberty.org

- Business Benefits of Federated Identity White Paper, April 2003
- Federated Network Identity Architecture Whitepaper, March 2003
- Liberty Alliance Specifications

OASIS, http://www.oasis-open.org

W3C, http://www.w3c.org

3GPP, 3rd Generation Partnership Project, http://www.3gpp.org

NOKIA CORPORATION
Nokia Mobile Phones
P.O. Box 100
FIN-00045 NOKIA GROUP, Finland
Phone: +358 (0) 7180 08000
www.nokia.com

NOKIA
CONNECTING PEOPLE