White Paper

Identity Federation and Web services – technical use cases for mobile operators

NOKIA
CONNECTING PEOPLE

Sun microsystems

Table of Contents

Abstract

This white paper shows how mobile operators can implement Liberty-enabled solutions to meet the needs of both the Identity Federation and Identity Web Services. Pure mobile operators can achieve more business opportunities by implementing open interfaces with third party service providers, while the same solution can be used to de-fragment an Identity Management infrastructure.

For operators offering both fixed and mobile products, the solution can help to unify the domains, as well as reinforce customer loyalty by creating additional benefits for customers with several access methods, including fixed/mobile telephony and fixed/wireless broadband access. The white paper outlines a number of technical use cases to illustrate the implementation, which can largely be done on top of an existing infrastructure, and discusses the network entities included in the solution as well as its functionality.

Introduction

Operators are increasingly implementing Identity Management solutions to give users an enhanced experience, increased privacy and improved security. This white paper shows how to an Identity Web Services architecture can be deployed that is federated in nature and based exclusively on open specifications, and how this implementation allows both browser- and application-based services.

The Liberty Alliance Identity Web Services and Identity Federation specifications are being implemented in the mobile industry to bring a number of benefits to mobile users, including:

- Automated access to services through Single Sign-On (Identity Federation), Authentication, Service Discovery and invocation to create a simplified, yet secure, user interface – seamless access for both browsing and using applications
- Service Providers can easily be added to the framework thanks to the standardized approach, and authentication can be handled at the Identity Provider, offering new, cost-effective business opportunities for Identity Providers
- Developers enjoy the service-focused approach, as the underlying complexity is shielded from through the use of standard API calls. In other words, the standardized approach to exchange authentication, discovery and service invocation information promotes cost-effective development, including of niche applications, whose development costs would otherwise have been insurmountable.
- Interoperability across operators, and domains, helps to build differentiated service offerings, regardless of the size and structure of operations.

The Liberty Alliance organizes conformance events, successful participation in which means that the vendor's product implementation gains the right to use the Liberty Alliance Interoperable™ logo, a guarantee that the products are implemented according to the specifications. The Liberty Alliance also provides guidance for implementers of Liberty-enabled solutions in privacy and business matters through its Privacy and Business Guidelines.

Generic Use Cases

By implementing the full Liberty Identity Federation and Identity Web Services architecture, operators will be able to support numerous use cases. This white paper divides typical use cases into three main groups, briefly outlined in the following sections.

Third Party Ecosystem – Mobile Circle of Trust

In this ecosystem, which is likely to be operational in many networks during the next year, the customer can get seamless access to many services with the help of the mobile browser. It is also possible to provide access to the Single Sign-On environment through PCs, laptops, and other devices.

Mobile connection (WiFi, GPRS, EDGE, CDMA, WCDMA, etc.) is made through the operator's access network. In the operator environment, a rough subdivision can be made into Resource and Services Zones.

The resource zone is where the necessary IT resources and Network resources are located. In the Services Zone, the operator sets up an IdP, Identity Provider (by integrating an Identity Server) – typically by themselves, but the IdP function can also be outsourced. The operator's own Web applications and Web services are also located in this logical domain. The Identity Server can not only manage the Identity Federation, but also take care of Identity Web Services Authentication and Discovery.

External third party Service Providers can be added to the Circle of Trust, so that their services, upon successful federation, can be accessed by means of Single Sign-On. Participants in a Circle of Trust will benefit from the ease of use, making these the preferred services for users.

Operator-centric Ecosystem – local, regional, multinational

The second group of use cases is the Operator-centric Ecosystem. To some extent, it builds on the Third Party Ecosystem, since external services can be provided in a similar way. The additional benefit is that by deploying Liberty-enabled Identity Federation and Identity Web Services solutions, operators can offer their customers a very large number of services, originating in their own (national) network, other operators' services, and own and other operators' Third Party Service Providers. Typically, such a scenario is popular among operators with operations in several countries, but the model could also be applied for cases where individual national or regional operators set up collaboration programs to achieve both economies of scale and a larger supply of services.

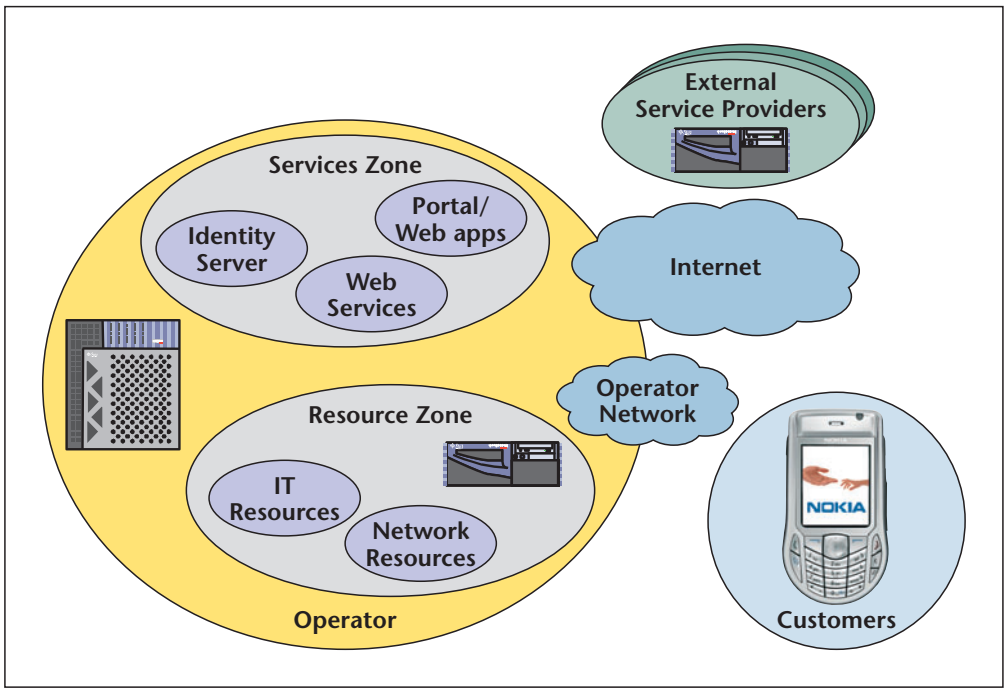
Identity Web Services Ecosystem – Mobile Enterprise Solutions

With Web services being widely deployed as the Service-Oriented Architecture of choice for internal processes in organizations, there is also an emerging demand for using Web Services enabling mobile working, business-to-business use cases, and business-to-consumer use cases. By adding Identity to Web services, it is also possible to handle transactions of value over un-trusted networks. The number of possible use cases for professional is unlimited – with a developer-friendly environment, where the underlying framework complexity is shielded by standard APIs, it will become quicker, and more cost-effective, to develop various (often niche) applications for mobile and remote working. Liberty Identity Web Services Framework specifications are developed to address security, integrity, and identity issues, regardless of the user device and access method.

In the next section, the three groups of use cases will be elaborated on. Nokia's and Sun's offerings are then briefly explained, followed by a short summary.

Note: At the time of writing, Liberty Alliance has not commenced work on specifying a payment interface. Therefore, this white paper does not elaborate on this aspect in any great detail. However, charging and payment features can certainly be supported by other means, for example, by the Nokia Intelligent Edge.

Figure 1. High-level global architecture



Detailed use cases

Third Party Ecosystem – Mobile Circle of Trust

A typical wireless operator is a self-contained ecosystem, where services and authentication share a consistent domain for network, identity authority, protocol, etc. This makes the extension of the ecosystem to a 3rd party quite complex and making it more difficult to follow the rapid growth of data services.

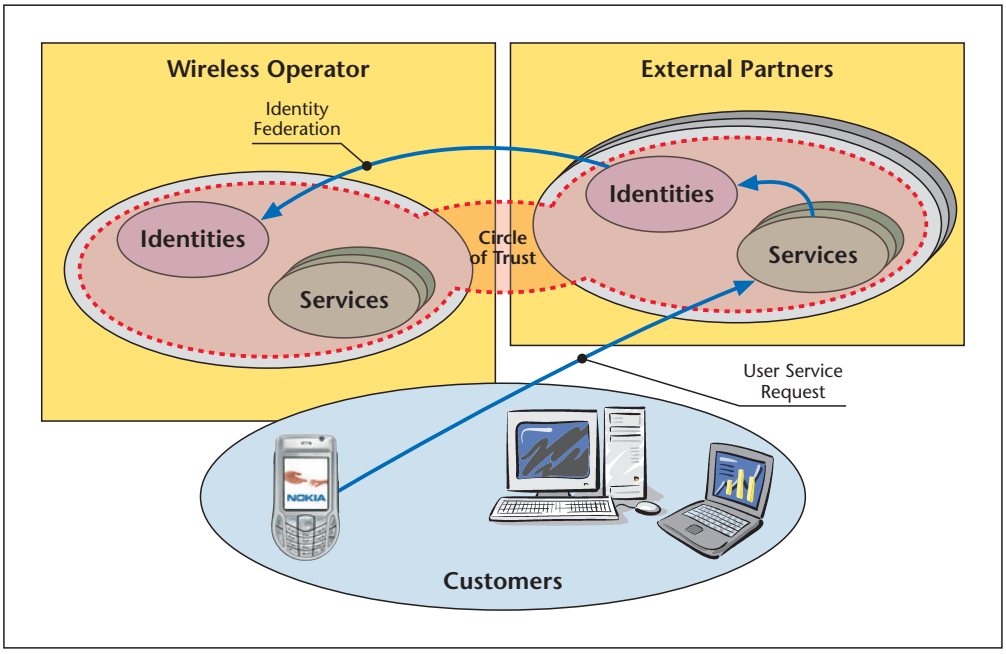
Although the operator already has external partners providing data services, these are usually treated as more or less a part of the operator's internal circle of confidence, sharing the same legacy and/or proprietary protocols. The main drawbacks in the current setup are that:

- Adding new external service providers takes too much time and causes high costs, due to the complexity of the network.
- Major service providers are reluctant to adapt their services to the required custom protocols and/or security constrains.

The operator is interested in gaining more benefits from their infrastructure and their knowledge of their customers. While wireless devices still have some GUI and performance limitations compared to, for example, desktop computers, operators have a payment mechanism, a financial relationship, presence and location systems. They also know many of their customers' key attributes, such as postal address, phone number, and often typical customer preferences and usage patterns in data, voice, and messaging.

Liberty proposes an identity federation mechanism in order to map the different custom circles of confidence into one CoT *[Circle of Trust]*. A Liberty CoT contains an IDP *[Identity Provider]* who acts as "the authentication authority" and as many SPs *[Service Providers]* as needed. The Liberty mechanism allows local and external SPs to be treated as equal, providing a nice user experience with a transparent SSO *[Sign Sign-On]* between external and internal SP, while leaving to each SP the ability to handle its private identity attributes. Liberty CoT also defines an identity link *[federation]* between a SP and the IDP. This offers a pseudonymous/anonymous relation between SPs and the IDP, allowing the enforcement of customer privacy and preventing identities being leaked from the IDP to the SP.

Figure 2. Ecosystem extension to external partners



Under the Liberty model, the user connects directly to the requested service and it is up to the service to check with the IDP if the user already has a valid SSO session or not. If the user is already logged on, either from a previous service, or automatically authenticated based on the network access authentication, the SP will receive a pseudonymous token corresponding to the user for that specific service or group of services. If there is no valid SSO session, the user will be redirected to the IDP for authentication.

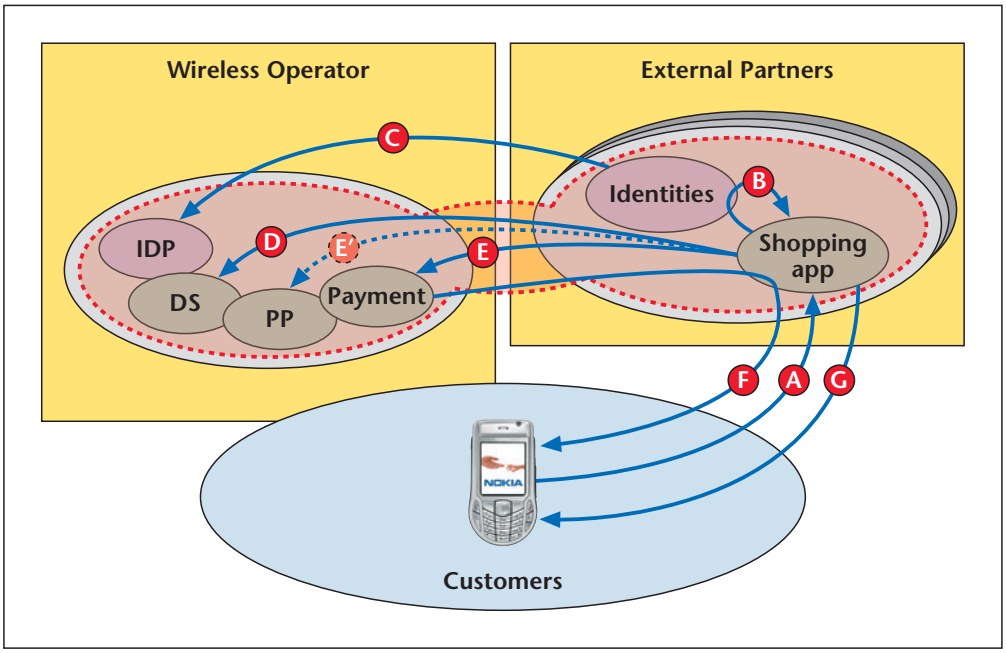
Liberty, with its ID-FF *[Federation Framework]*, allows the implementation of seamless Single Sign-On for users interacting with applications. Support for ID-WSF *[Web Services Framework]* allows the discovery and invocation of web-services applications.

A typical use case for this scenario would be the implementation of a mobile shopping service. The customer can purchase goods, have the postal address automatically provided through the back-end interaction between the External Partner and the Wireless Operator (Identity Provider), and have a choice of payment options (post-payment with the phone bill, credit card, etc), while maintaining an acceptable level of privacy. From the user's point of view, the main steps in finding a shop, accessing it and making a purchase would be as follows:

- Selection of a shop from the wireless portal home page or from anywhere else
- Browse the Web pages of the shop.
- At some point click on "Buy now".
- Get a request for "Payment Consent" from the operator.
- Depending on the type of goods
  - Delivery is done electronically [example: cinema ticket, ring tone, song, etc.]
  - Shipped at the customer portal address, provided by the operator (Identity Provider)

Sequence flow explanation

Figure 3. Shopping use case



A. The user browses an application anonymously, and at some point chooses to buy something, either goods or services.
B. User surfs in anonymous mode.
C. The shop SP *[Service Provider]* needs to authenticate the user – it sends an authentication request to the IDP *[Identity Provider]*, in our example, the operator.
   - The User connects to a Service Provider (via the WAP Gateway).
   - At some point the SP sends back an authentication request. Since the WAP Gateway added the LECP (Liberty-Enhanced Client/Proxy) profile, the authentication request is sent back to the Liberty-enabled WAP Gateway. The Gateway then retrieves the MSISDN (phone) number and sends it to the IDP. The IDP could then trust the WAP Gateway and not check anything, but in most cases, it will check with the database (e.g. LDAP) if this MSISDN is authorized to access that SP in order to login the user.
   - The IDP returns a valid SSO token as the authentication response. This token is usually a pseudonymous token, but can when requested be fully anonymous, depending on whether or not the SP needs to keep track of the user.

D. At some point the shop SP needs to request payment. It then contacts the Liberty DS *[Discovery Service]* of the IDP requesting the payment service. If authorized *[this depends on the business agreement]*, the IDP returns the payment endpoint *[URI for payment Web service]* and a RID *[resource identification]* token for the shop to be able to request payment on behalf of the user.
E. The shop requests payment on behalf of the customer, and receives a "Must Interact" from the payment WSP *[Web Service Provider]* and redirects the user browsing session to the Payment Service.
E'. The shop may also use other Liberty Web services, such as the PP *[Personal Profile]* to retrieve the customer postal address for shipping the goods.
F. The Payment Service interacts with the user in order to get his consent for the shop's charging request.
G. Confirmation message sent, the goods are delivered to the customer.

Note: A delivery may request a couple of extra exchanges between the shop and the operator. If, for instance, the product is a cinema ticket, the shop SP would have to request the SMS/MMS Web services gateway to deliver it as, for example, a bar code image or ticket number.

OMA Web Services
The Open Mobile Alliance (OMA) has recognized the business opportunities offered by standardized Identity Management solutions. A mobile subscriber may use several services, not all of which belong to the trust domain of its network operator. To ensure the end user has a valuable experience, the concept of Identity Federation is required. Network identity is the term used to describe basic functionality that is used with a variety of network services to provide a coherent use of state or data related to an end user.

OMA's Mobile Web Services specifications include Network Identity Specifications, the first version of which was approved in July 2004. It provides normative descriptions of the components needed to provide aspects of the Network Identity related capabilities, such as Identity Provider Introduction, Identity Federation and Single Sign-On.

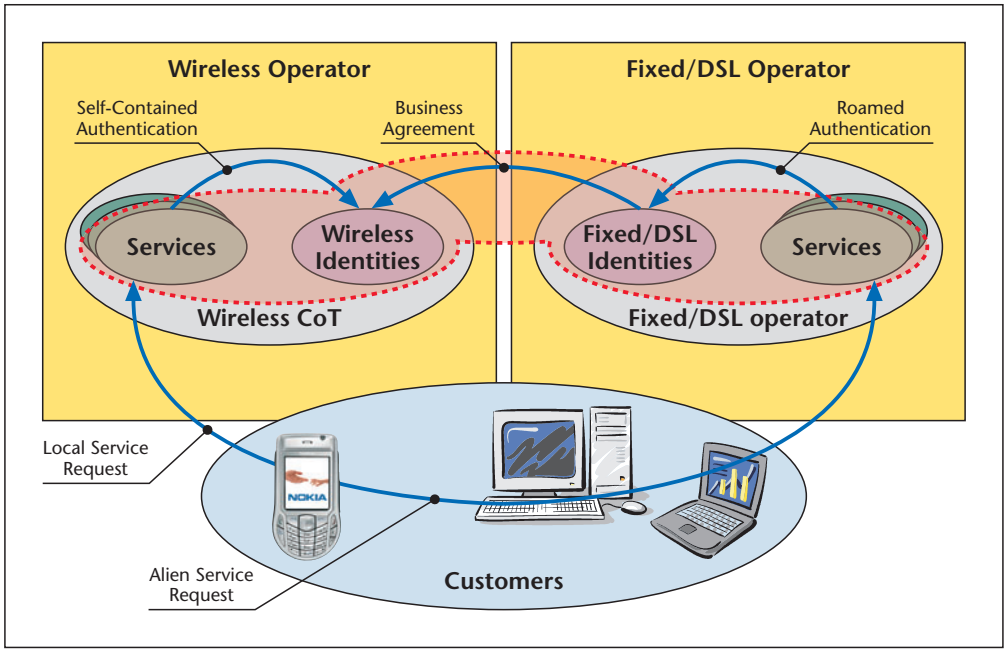
For further information, please refer to:
http://www.openmobilealliance.org/release_program/owser_v10.html
Specification: OMA-OWSER-Network_Identity-Specification-V1_0-20040715-A.pdf

Operator-Centric Ecosystem

Many telecom operators are in a position to offer a full-service solution, including for instance fixed, mobile and DSL services. There are several advantages of such an offering:
- Operators can share infrastructures to reduce cost
- Operators can exchange customer knowledge to implement a joint commercial offering.

Users can operate services in several ways, for example checking the latest calls and charging from his DSL connection.

Figure 4. Bridging Circles of Trust



The main issue when bridging a Circle of Trust is to find out how to link the different identities that a customer has. Usually, there is no automatic method to federate them. And, even if this could be achieved, there may also be legal constraints, preventing, for example, the mobile operator from sharing its users database with the DSL organization.

Mobile/DSL joint commercial offering use case

"XyZ" is a communication company with two branches: DSL and Mobile. "XyZ" wants its customers to have a contract with both the DSL and Mobile operators, so starts a campaign to charge mobile subscriptions at a discounted price. When the GSM/DSL users then connect to the DSL portal/web mail, they can click on a link, after which they are redirected from the DSL portal to the corresponding "XyZ" mobile portal. This transfer, as well as the commutation from the DSL identity to the Mobile identity, should be seamless for the user, with a fully transparent SSO.

In order to make this possible, the first step is to bridge the user DSL and Mobile identities. As explained previously, this cannot usually be done automatically – also, before allowing the user to perform Single Sign-On between the DSL and Mobile, we have to federate the identity. The following sections provide scenarios from the point of view of the user:

Opt-In federation of DSL and Mobile identities

- When the user checks his personal web mail with the DSL account, he sees a commercial that proposes, "50 free Short Messages" for any "XyZ" Mobile user who accepts the offer.
- This commercial is an http link that redirects the user to the "XyZ" mobile portal pages.
- The user is now on a mobile portal Web page, where he is asked to enter his phone number.
- The mobile portal sends a SMS to the user with an activation code.
- The user enters this activation code on the mobile portal.
- The mobile fixed Identity Providers from "XyZ" can federate the user's identities.

Use federation to make product offers

- The user checks his personal web mail and receives an "Exclusive Offer" to change his prepaid subscription to post-paid. *[This is possible because DSL now knows that this user has a mobile/fixed federated account].*
- The link redirects the user to the "XyZ" mobile portal pages.
- As the user is already federated, "XyZ" mobile can propose the offer without asking for any identity information. The login can be Single Sign-On (because the federation has already taken place), and "XyZ mobile" can propose to ship the new SIM card to the address where the DSL contract is established *[as DSL is connected to fixed phone network and knows the postal address].*

Use federation to offer new services

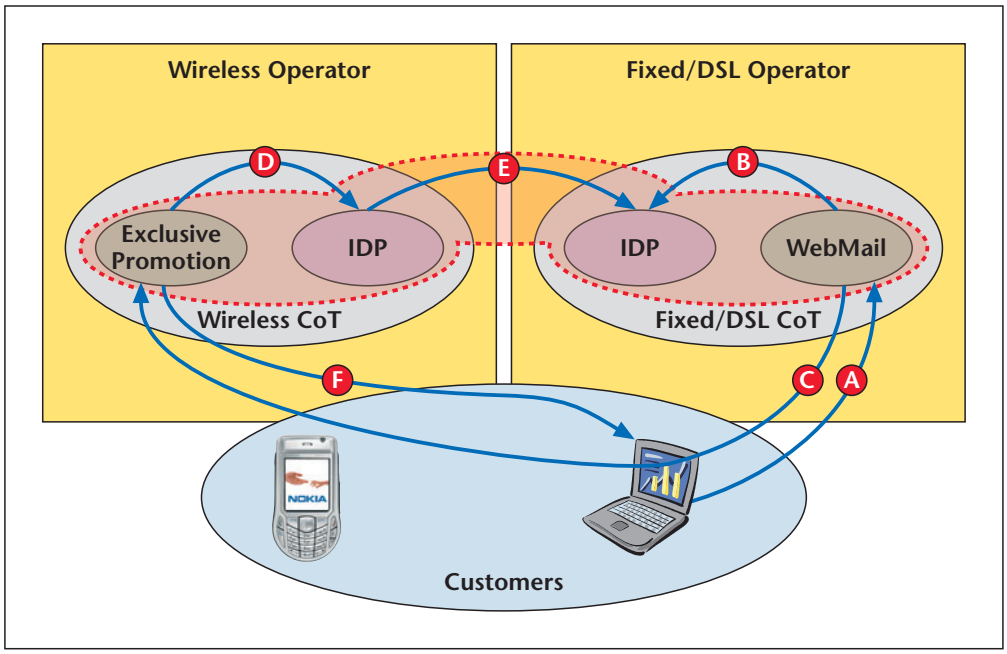
- The user is notified by web mail that he has a message regarding his mobile subscription.
- By clicking on the "Mobile Subscription" link, the user is redirected to his Mobile portal.
- The user enters the mobile portal (with Single Sign-On) and checks out the message from his computer.

Note: While the example describes bridging between two subsidiaries' Circles of Trusts, the same model could be used for any Circles of Trust that are willing to establish a strong business relationship, where trust is not established at the SP/IDP level as within a self-contained ecosystem, but at the CoT/CoT level.

Technical data flow

Making the assumption that the step to federate in order to bridge the Circles of Trust was done *[e.g. through an Opt-In approach as described earlier]*, the flow to implement the "joint commercial" scenario would be as depicted as follows:

Figure 5. Alien service request



A. The user connects to his DSL web mail.
B. The DSL web mail authenticates the user, either through SSO if previously logged on, or through a traditional user password mechanism.
C. The DSL web mail commercial hyperlink redirects the user to the "Mobile Exclusive Promotion" service.

D. As the user is not authenticated to the mobile CoT, the "Mobile service" redirects the user to its own Identity Provider
E. The mobile Identity Provider discovers that the request comes from a Bridged IDP *[e.g. from the IP address]* – it then functions as a Service Provider within the DSL Circle of Trust and proxies the authentication to the DSL IDP. Finally, it retrieves the federation token and logs the user on to the mobile CoT.
F. The mobile service can then fulfill the request.

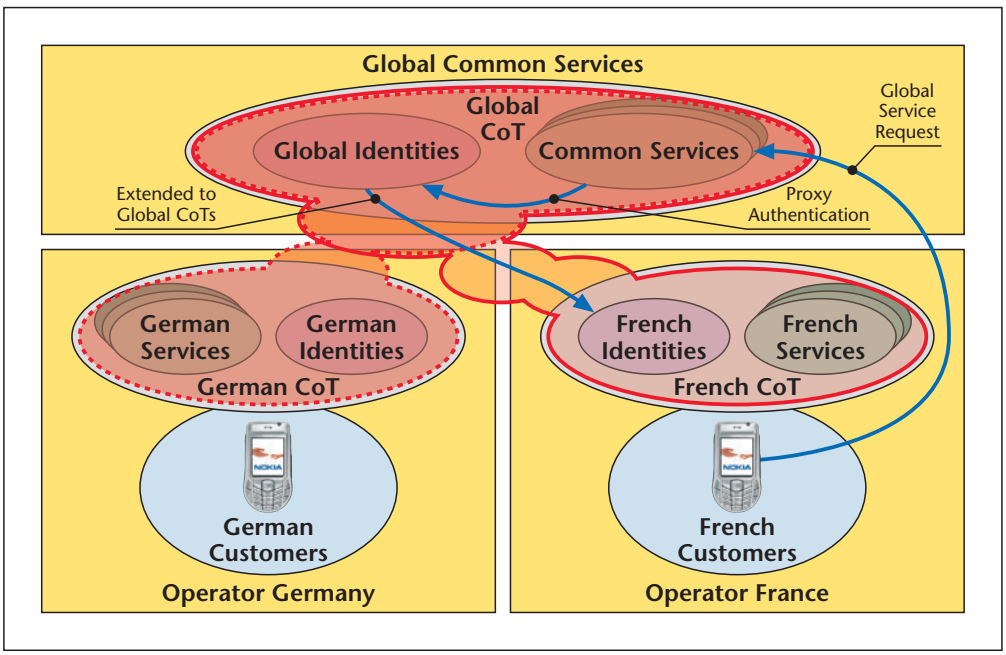
Note: Some extra message exchanges may be required. User consent should probably be requested to confirm the payment. It can be done directly from the Mobile Payment Service, on the DSL side or be added to the user's fixed phone bill. Some attributes, such as postal address from the personal profile, may also be provided in order to ship the device, so that the user himself does not have to type in the shipping address.

Global, shared Circle of Trust and services

Global and regional operators are active in more than one country. This typically creates one silo of identities per country, which makes the implementation of identity-aware shared services more complex. Liberty Alliance's specifications allow the implementation of global shared services *[for example, at the European level]* while the main identity remains at the country level. To exemplify, a Pan-European wireless operator may have independent business organizations in different countries and still implement a European (CR) Portal with shared services. In the following illustration, "XyZ" operator has relatively independent operations in France & Germany, but they share some common services. The user identity is split between local and global Identity Providers and authentication for wireless operations remains at the local level, while Internet user/password may be served directly at the global level. Both the global and local identities are federated, making this fully transparent for the user.

In order to make the example simpler, only two countries are represented, although this model is not limited to a specific number of local operators. The model could also be used by independent companies who would like to share some common global services.

Figure 6. Global Circle of Trust and services



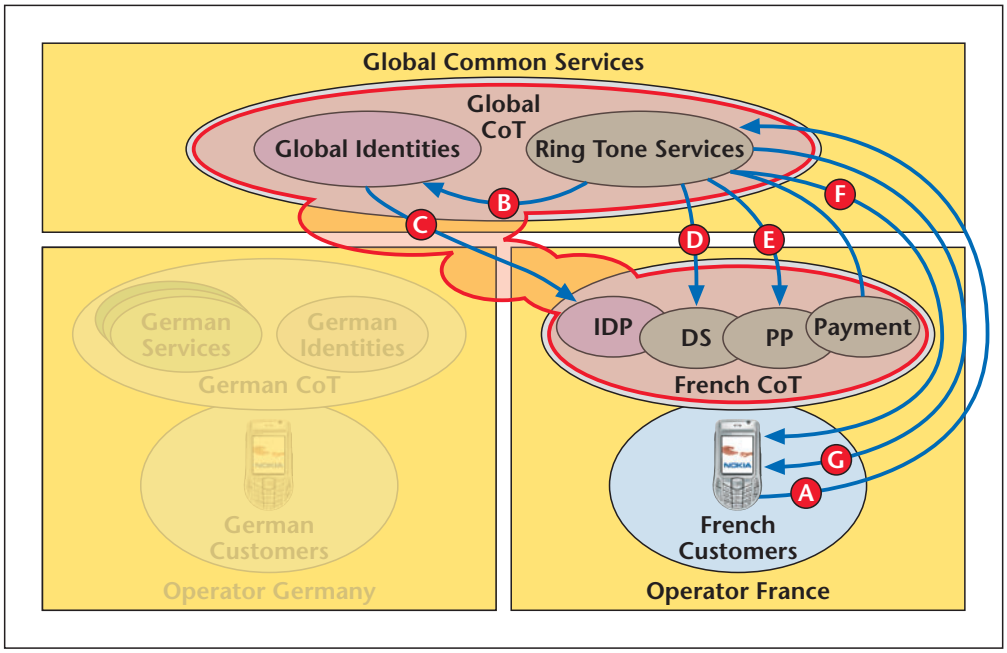
If we make the assumption that all "XyZ" users share a Pan-European portal infrastructure, from a user's point of view, when browsing and buying a digitally downloadable product *[for example a ring tone, cinema tickets, etc.]*, the following scenario could be implemented:

- The user clicks on a pre-provisioned link and goes to the global portal.
- The user is automatically signed on, and sees his personalized home page.
- The user browses on the "Ring tone of the Day" service link and selects a new ring tone.
- The user is asked for payment consent *[probably from his local operator]*.
- The user receives a new ring tone.

Technical data flow

Making the assumption that both global and local identities have earlier been federated, and that the user was previously authenticated at a local level, the technical data flow would be as follows:

Figure 7. Global Service technical data flow



A. The user browses the "Ring Tone Of The Day" web site *[he is probably re-directed from a link through a wireless portal]*.
B. "Ring tone of the Day" needs to authenticate the user, so it sends an authentication request to its own Identity Provider *[global IDP]*.
C. The Global IDP detects that the user originates from a "trusted" Circle of Trust and turns as an SP from the French IDP to proxy user authentication. The result of this authentication is a federation key provided by the French IDP to the Global CoT.
D. "Ring tone of the Day" sends a Discovery request to the Local Discovery Service to discover the user's Payment Service(s).
E. "Ring tone of the Day" sends a payment request to the user's local payment service.
F. The Payment Service asks the user to approve the charge and, after getting the user's consent, confirms the payment request to "Ring tone of the Day".
G. "Ring tone of the Day" delivers the ring tone to the user device.

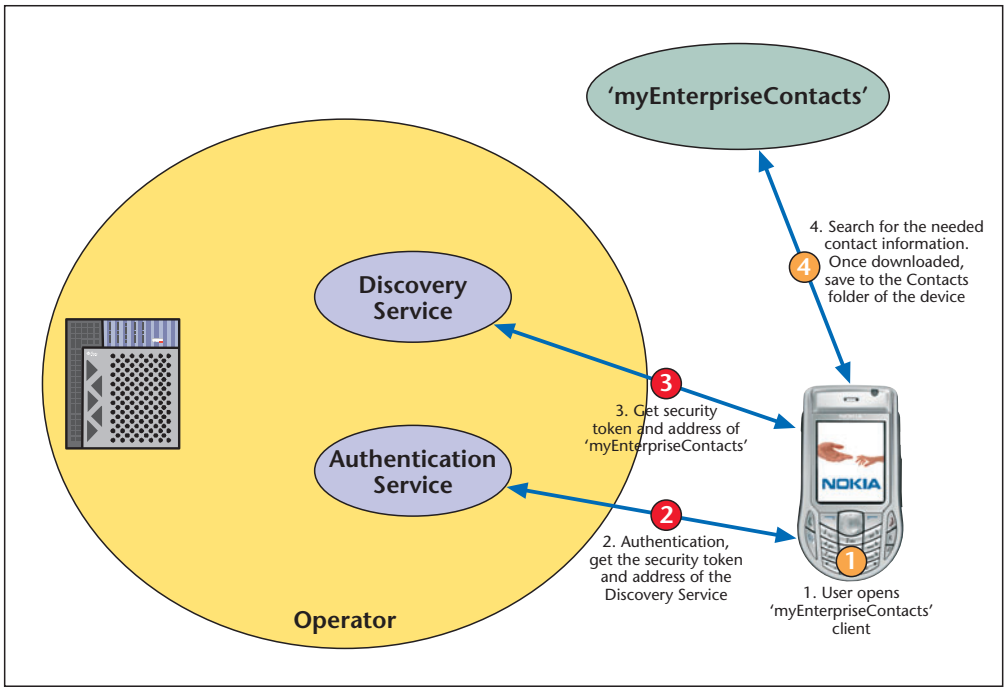
Note: Some extra exchange may occur, especially in order to deliver the ring tone; the service provider may have to discover and then invoke a SMS/MMS service, or another content download mechanism.

Identity Web Services Ecosystem – operator-driven enterprise solutions

In the following, two simple use cases illustrate how enterprises and the mobile operator can interact to enable convenient and secure access to services with the help of Identity Web Services applications. The approach is also certainly valid for consumer use cases, as will be discussed in the second, more extensive example.

In the first example, the user has been provided with a contact book client by his enterprise's IT department or the operator, in which the access credentials are embedded. With the help of this application, the user can access an intranet database to conveniently search and download contact information to his device. The use case is shown in the following figure.

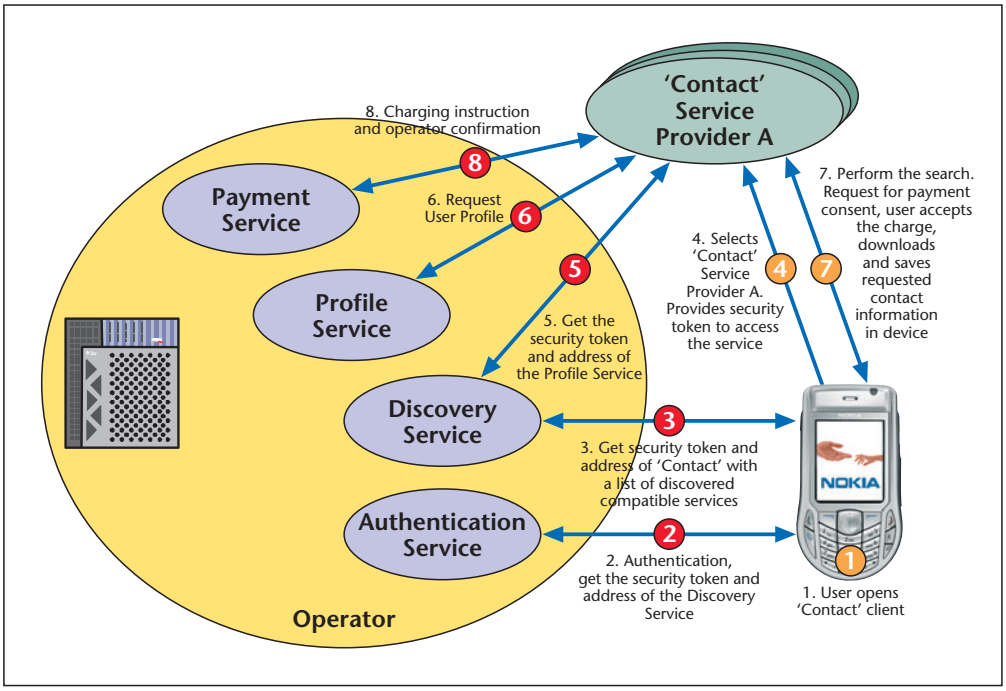
Figure 8. Simple enterprise contacts use case



In this simple use case, the user only needs to open the client (1), enter the search information, and save the downloaded information in the device's contact book (4). All other information is handled in an automated way, including exchange of security tokens, discovery, and setup messages (2–3).

This application could be a suitable starting point for the enterprise. It is, however, possible to expand the functionality by introducing further features. A small- to mid-sized enterprise is also more likely to need the operator's support to enable these services. The following use case is an example of how the user can access various contact books on the back-end with the dedicated client.

Figure 9. Contact search with multiple Service Provider options



In this scenario, the operator can set up a federated ecosystem with various Service Providers, including the enterprise's own contact book database.

The operator, on behalf of the enterprise and the various service providers, can provision the service. Standard protocols and field definitions are applied to enable interoperability.

The user involvement increases somewhat in this use case, but it is kept at a minimum. Again, he opens the client (1), after which the Authentication and Discovery Service message exchange is performed automatically (2) and (3). This time, however, the user is presented with the optional alternative Contact Service Providers, and thus needs to select the preferred provider (4).

The selected Service Provider A now contacts the Discovery Service to find out where the user's Profile is stored (5). It is possible to add a request for user consent to share the required information, but it is not included in this example. Service Provider A then contacts the Profile Service to obtain user information – depending on the specific use case, it can be payment preferences, address information, phone number, etc.

The user performs the search, Service Provider A requests approval to charge the user's phone bill, the user accepts the charge, and the information is downloaded and stored in the device by the user (7). Finally, Service Provider A instructs the Operator to charge for the service by sending a request to the Payment Service (8).

It is possible to further extend the functionality in this use case, by, for instance, engaging a location service or resolving the user's location by other means. If the user is abroad, it may also be possible to offer local contact services for that country, along with the home country's Service Providers and the enterprise contact database.

After the session, the user can access the operator portal (optionally with the browser), to verify the amount charged by Service Provider A.

Company offerings

Nokia's Liberty-enabled implementations

Nokia Intelligent Edge and Nokia WAP Gateway

The Nokia Intelligent Edge solution allows operators to use identity federation for providing authentication services to its enterprise and third party content partners:

- Nokia Intelligent Edge provides user authentication, which can then be used for Liberty-enabled single sign-on. Besides authentication, Nokia Intelligent Edge also provides other access management functionalities such as service aware charging or service access authorization.
- The Nokia WAP Gateway functions as a proxy for mobile terminals. When, for instance, accessing a Web site that is Liberty-enabled, the Nokia WAP Gateway can handle the requests for and responses to single sign-on. The Nokia WAP Gateway is a part of the Nokia Intelligent Edge solution, and is the first WAP Gateway in the world to earn the rights to use the Liberty Alliance Interoperable logo.

For further information about Nokia Intelligent Edge, please refer to: http://www.nokia.com/cda1/0,1080,43029,00.html.

Nokia Web Services framework for mobile devices

The Nokia Web Services framework for mobile devices is Nokia's device platform feature, which allows the operator to provide its enterprise and content partners with the abilities to use Identity Web Services for several reasons:

- To replace existing or homegrown middleware with a cheaper, off-the-shelf and standards-based solution
- Provide easier integration of applications to achieve a particular business goal
- Ability to build a link with a business partner over the Internet
- Expanding the usability and reach of a developed application
- Opportunity to add rich features to existing applications
- Re-use of the framework lowers the cost for developing new applications, thanks to the sharing of common services such as authentication, discovery and service invocation mechanisms.

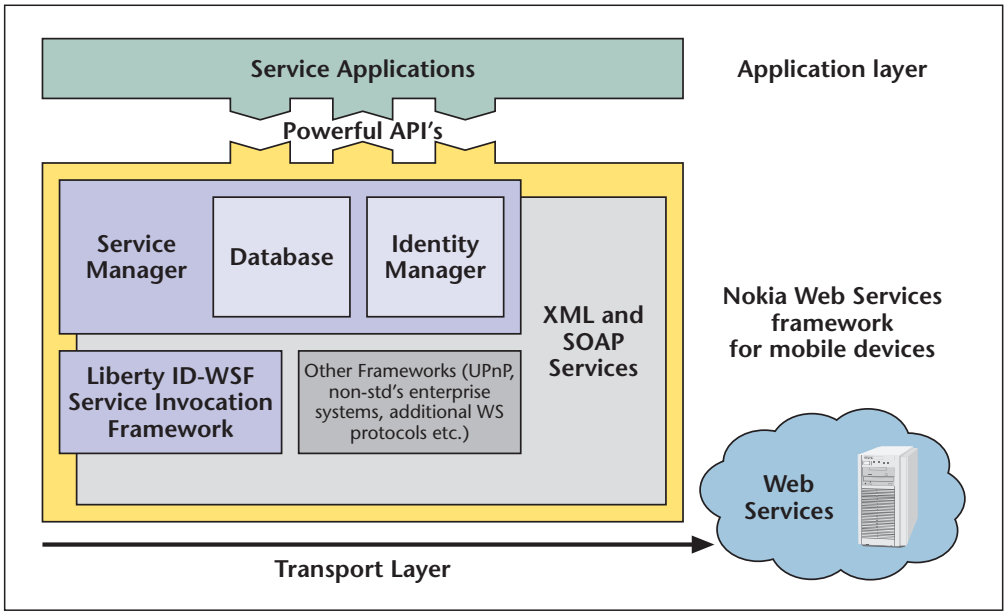


Figure 10. Nokia Web Services framework for mobile devices

As we can see from the figure, the framework consists of components for Identity Management and Discovery, and also has a placeholder for the addition of plug-ins, for instance new protocols or service invocation frameworks.

The Nokia Web Services framework for mobile devices are available for the new generation of Nokia Communicators, and a downloadable version will also be available for the Series 60 smart phone platform early in 2005.

Sun's Liberty-enabled implementations

Sun Java System Access Manager

Sun Java System Access Manager delivers secure, standards-based access management for:

- Improved security
- Enhanced user experience
- Increased revenue opportunities
- Reduced administrative costs

To compete effectively in today's economy, enterprises and service providers are using the Internet to deliver services to and share information with customers, employees, partners, and suppliers. To control costs and minimize the security risks of conducting business more openly, carriers need an access management solution that ensures secure access, no matter how large and complex access demands become, or how far within the service layer they extend.

Sun Java System Access Manager (formerly Sun Java System Identity Server) is a security foundation that helps operators manage secure access to Web applications across business-to-business (B2B) value chains. It provides open, standards-based authentication and policy-based authorization with a single, unified framework for:

- Securing the delivery of essential identity and application information to meet today's needs and to match growing business needs
- Improving the user experience through single sign-on (SSO) to all of an operator's Web-based applications
- Creating revenue opportunities through deeper relationships with partners, suppliers, and customers by enabling trusted networks with these key constituents

Java System Access Manager takes on the challenge of managing ever-increasing silos of identity – each of which would otherwise require independent administration of access and authentication credentials across several off-the-shelf or homegrown applications. It defines and enforces access privileges for diverse groups of users, reducing administration problems and cutting security risks.

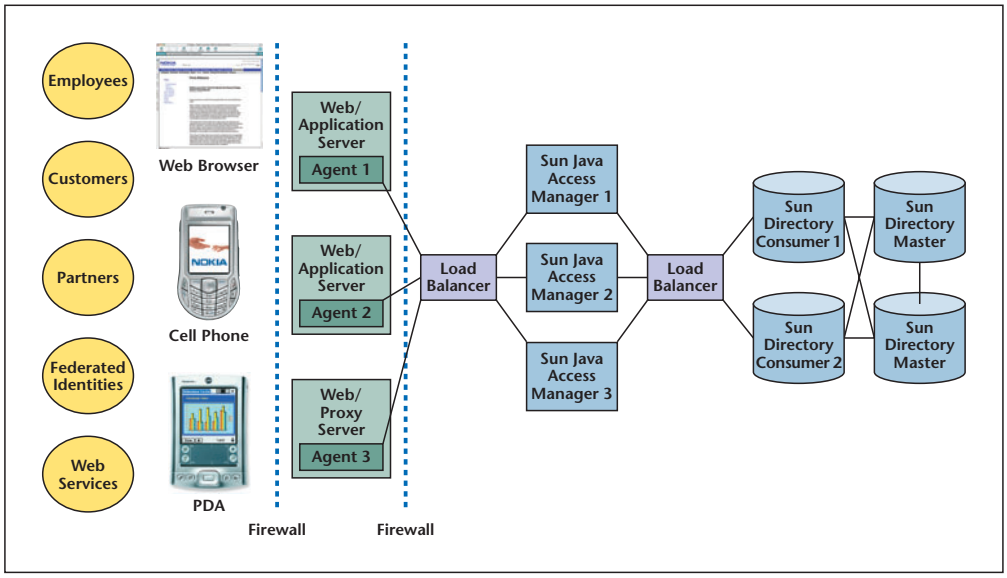
In addition, Access Manager allows operators to comply with industry regulations and legislative requirements as they manage this complex web of users, identities, and private information.

As the industry's first commercially-available access management solution to comply with the Liberty Alliance Phase 2 (ID-WSF) and Security Assertion Markup Language (SAML) 1.1 specifications, Access Manager provides operators with solutions for the widest variety of federation use cases, including:

- SAML Producer
- SAML Consumer
- Liberty Phase 1 Identity Provider

- Liberty Phase 1 Service Provider
- Liberty Phase 2 Web Service Provider services and service APIs
- Liberty Phase 2 Web Service Consumer components and client APIs

Figure 11. Sun Java Access Manager solution



The Access Manager architecture is based on open, scalable, and robust Java 2 Platform, Enterprise Edition (J2EE) technology, and:

- Delivers decentralized authentication and authorization services across internal and external computing domains
- Ensures that all appropriate authentication credentials are required of users, depending on the value of the protected resources
- Makes certain that authorized users have access to specific resources while protecting those resources from all but authorized users
- Presents streamlined navigation across enterprise Web applications through single sign-on
- Enables operators to audit all access activities, including authentication attempts, authorizations, and changes made, to assist in complying with regulatory audit requirements.

Access Manager has proved capable of being scaled up to meet operators' needs – in a recent federation benchmark, Access Manager provided federated single-sign on to a simulated user population of 80 million, handling over two million federation transactions (SSO/link accounts/unlink accounts) per hour with response times below one second.

Finally, the Java System Access Manager extends and leverages the carrier grade Sun Java System Directory Server, the most widely deployed general purpose LDAP Server in the operator market. The Sun Java System Directory Server has 1.5 billion entries deployed, it has been benchmarked with 160 million entries and is rated #1 in the Directory Server Magic Quadrant by Gartner Research, #1 market share leader by Radicati Research and #1 in market penetration by The Burton Group.

Conclusions and summary

This technical white paper has aimed to outline how operators can enable a wide variety of use cases by implementing open Web services and Identity Federation standards. To date, Liberty Alliance is the only organization to define a complete open Web services architecture. The architecture addresses privacy, identity and other security aspects, helping to increase the usability in a number of scenarios beyond what has been possible so far. Another aspect is that the specifications have been defined with the mobile industry in mind, making it useful with all kinds of user devices.

Not only is the Liberty approach appealing technically – it can also be seen as a strong business case:

- Increased user-friendliness (fewer clicks, easier password management, easier discovery of applications, automated service-oriented messaging, etc.) can boost data transfer and content revenues.
- By functioning as an Identity Provider, the operator can create business models around password and identity management. Service Providers can outsource large parts to the operator, and both parties can benefit from more efficient administration.
- The technical implementation, with a blend of own and third party offerings, enables a business ecosystem, where, for instance, revenue-sharing models and co-marketing campaigns are methods that can help to increase revenues.
- The Web services technology helps to bridge the operator and enterprise environments, enabling new business opportunities and ways to offer a stronger mobile enterprise solution.

For further information about the Liberty Alliance, please refer to http://www.projectliberty.org/.

About Nokia

Nokia is the world leader in mobile communications, driving the growth and sustainability of the broader mobility industry. Nokia is dedicated to enhancing people's lives and productivity by providing easy-to-use and secure products like mobile phones, and solutions for imaging, games, media, mobile network operators and businesses. Nokia is a broadly held company with listings on five major exchanges.

About Sun Microsystems

Since its inception in 1982, a singular vision – "The Network Is The Computer" – has propelled Sun Microsystems, Inc. (Nasdaq: SUNW) to its position as a leading provider of industrial-strength hardware, software and services that make the Net work. Sun can be found in more than 100 countries and on the World Wide Web at http://sun.com.

NOKIA CORPORATION
Technology Platforms
P.O. Box 300
FIN-00045 NOKIA GROUP, Finland
Phone: +358 (0) 7180 08000
www.nokia.com

SUN MICROSYSTEMS, INC.
4150 Network Circle
Santa Clara, CA 95054 USA
Phone: 1-650-960-1300
or 1-800-555-9SUN
Web: http://sun.com

NOKIA
CONNECTING PEOPLE

Sun microsystems

12/2004 Indivisual