Tier 2 Business Guidelines: Mobile Deployments

1 EXECUTIVE SUMMARY

1.1 Abstract

For the reader active in the mobile business market, this document provides generic guidance and information sources – legislation and articles – for examining the broad federated-identity business issues within the mobile-services industry, as generally identified by the Alliance. The Tier 2 Scenario document combines the significant business issues that span the various Liberty implementation scenarios (B2B, B2C mobile, etc.) from mutual confidence, risk, liability and compliance perspectives. (See Business Guidelines document- July 03)

For people wanting to deploy a Liberty-enabled infrastructure, this document will help them understand the business stakes involved in the federation process. It is written using the mobile-industry market input written in Liberty marketing-use cases and requirements that serve as the foundation of the Liberty specification.

1.2 Summary

- Mobile operators are well-positioned to provide Liberty-defined identity services to service providers and/or SIM services to other identity providers:
    - Liberty Alliance serves as the de facto standard for identity services in the mobile industry and can enable data services between GSM operators, similar to what the GSMA has done with voice service roaming.
    - Liberty Alliance can benefit access control and data services immediately (remote payment, geolocation…)
    - The improved identity solution at the right cost benefits the entire mobile ecosystem
    - Identity, and therefore the Liberty Alliance, furnishes the focal point for many mobile-industry efforts

- Key trends that reinforce the Liberty message:
    - European Commission funding of the t2r project for mobile-enabled identity and a sharable SIM
    - The Mobile Web Services announcement around SIM-based authentication
    - Various examples from Europe and Central America of downloaded credentials to a mobile device and cooperative business models around a shared SIM
    - The convergence of Web services that occurs among mobile, enterprise, media and Internet domains require a standard approach of managing identities, bridging the mobile and fixed network.

2 THE MOBILE INDUSTRY'S ANTICIPATION FOR FEDERATED IDENTITY

2.1 Liberty's Solution and the Mobile Industry

The Liberty Alliance, created in 2001, addresses business, technical and policy considerations that impact 'identity' in both the wired and wireless world. The consortium consists of more than 140 members from various industries and regions across the globe and develops open standards for federated identity and identity-based Web services.

The Liberty Alliance pioneered the federated approach of sharing and managing identity information. In its identity framework, various terms have been defined, which are:

- Identity Provider, or IdP, identifies and authenticates a user. The IdP may rely on various identity data stored with other entities called Attribute Providers

- Service Provider, or SP, provides a value-added service to the user. The SP likely will maintain service-specific data on the user but, with the user's permission, is free to rely upon the IdP or attribute providers for additional user data, such as location or payment options

- Circle of Trust, or CoT, is a user-controlled federation, or linking, between Service Providers and an Identity Provider. Once a CoT is established, a user may engage conveniently with any federated service without reestablishing identify (Single-Sign-On) and can control confidently any user data that personalizes the service offering

The Liberty Alliance framework is emerging as a 'de facto standard' for mobile data services. Within Liberty, member companies collectively represent:

- 200+ million mobile subscribers via DoCoMo, Orange, Sprint and Vodafone
- More than half of the mobile devices via Ericsson, HP, NEC and Nokia
- 80% of all SIM's via Axalto, Gemplus and Giesecke & Devrient,
- 55% of the mobile network infrastructure via Ericsson, NEC, Nokia and Sun

The existing mobile infrastructure of network, mobile equipment and subscriber identity module (SIM) is ideal for identity services like user authentication and consent:

- Global Interoperability – 850 million GSM users form a virtual 'GSM-land' and data services, such as short messaging, work across mobile technologies.

- User habit – The phone serves as a very personal device that users are rarely without

- Trust – Operators are trusted brands for consumers *and* service providers

- Security – The SIM is a smart card, a common element in advanced identity services

- Event-based Billing – Operators can aggregate small value transactions and share revenue on a global scale as is done with roaming agreements.

With the Liberty Alliance framework, mobile operators are well positioned to offer solutions that potentially could halve the annual cost of strong authentication and user consent and, thereby, reduce risk and online costs:

1) **Mobile Operators as Identity Providers** - Online service providers can rely on identity services (authentication and consent) performed by mobile operators on an event-based (per authentication) or subscription (per annum) model.

2) **Mobile Operators as Infrastructure Service Providers** - Identity providers can add their identity credentials to a SIM supplied by a Mobile Operator. A possible model compensates the Operator for the loading and use of additional IDs. To control liability, a trusted third party can load additional IDs confidentially so operators do not 'see' the data being loaded.

	New Authentication Methods	Device Cost(s)[2]	Setup & Support Cost	Messaging Cost[1] (€0.03/SMS)	Total Yearly Cost
Today's Standards	Password	0	14€	0	14€
	Leading Token	28€	8€	0	36€
Liberty's Proposals	Identity Service Provider	0	3€	11€	14€
	Shared SIM	0	15€	0€	15€

Notes   1) Logins / year = 245 work days / yr * 1.5 logins / day = 367.5
2) Operators pay for the SIM; services have no hardware costs

3) **Mobile Operators as Attribute Providers -** Any mobile customer needing an enhanced service experience can, for instance, allow the Service Provider to access his/ her information from the Mobile Operator. Liberty Alliance provides flexibility to support a wide range of business models. In this exchange, the operator may release the information based on the user recommendations.

4) **Mobile Operators as Service Providers -** Using the extended privacy support provided by the Liberty specifications, operators can provide personalized and individualized experiences to their customer. For example, messaging, payment, presence typically are services needing maximum privacy support.

Liberty models support mobile data services and allow for the mobile infrastructure to serve as a complementary 'trust' channel for existing content channels, as shown in the examples below. Note that the user is prompted for a PIN so that a lost or stolen mobile phone does not compromise security.

2.1.1   Access Control

Liberty aims to lower the risk and costs associated with password authentication by Web services, such as corporations, banking, brokerages, insurance providers and governments.

When users wish to log-on, for example, they could use their phone and a PIN to generate a one-time password that is entered into the Web site. Credentials from multiple services could be stored on the phone and represented in the phone's menu by Web-site name. A user simply needs to scroll and select the appropriate site.

This very basic, calculated one-time password model is ideal because no connection exists to the PC that might increase support costs, and no communication expenses, latency or lack of coverage exists as they sometimes do within office buildings or secured facilities.

2.1.2   Remote Payment

Remote transactions represent the fastest growing form of payment – and the most expensive. Liberty works to lower the risk and costs associated with remote payment by enabling banks to add the equivalent of their bankcard into the SIM to deliver stronger authentication and user consent.

For example, when an eCommerce user pushes the 'BUY' button when shopping online, a message might be sent to the phone, the user prompted for a PIN and the receipt signed by the bank's payment application, such as EMV, on the SIM. This moves the transaction toward a lower-cost card-present transaction model and could guarantee payment for the merchant.

2.2   Identity's Near-term Markets

More than 90% of online services use passwords to authenticate a user. However, passwords are cumbersome to remember and easy to fake, causing increased costs from fraud losses, penalties and lost-revenue potential from reduced service offerings.

Passwords are considered insufficient for high-risk markets, including:

1) Remote payment – such as e-Commerce and Mail-order/Telephone order
2) Access control – such as corporate VPN's, home banking and commercial extranets

For example, merchants pay nearly 1B Euros in remote-payment fraud losses and fees:

- Remote payments account for about 25% of all credit-card payments (MasterCard, 2003)
- 2.1% of online transactions are fraudulent, compared with 0.1% in traditional card purchases (*The Wall Street Journal* using data from Celent Comm., 2002)
- In the United Kingdom, remote payment fraud was $690M (Apacs, 2003)
- In the U.S., total credit-card fraud was $1.6B in 2001, $1.8B in 2002 and estimated to be $2.4B in 2003 (*The Wall Street Journal* and Celent Communications)
- In the U.S., merchants paid $500M in charge-back fees (*The Wall Street Journal*, 2002)
- More than 50% of e-Commerce fraud attempts are in North America (U.S. 47.8%, Canada 4.66%); followed by the United Kingdom (5.25%), Nigeria (4.81%) and Israel (4.46%) (Verisign, 2003)

However, using comparative data drawn from Liberty-member experiences, the annual cost of independently issuing and supporting a security token for even simple tasks like access control can approach 30+ Euros.

Today's Authentication Methods	Device Cost(s)[2]	Setup & Support Cost	Messaging Cost[1] (€0.05/SMS)	Total Yearly Cost
Password	0	14€	0	14€
RSA SecurID	28€	8€	0	36€
SMS Password Push	0	12€	18€	30€
Smart Card	20€	15€	0	35€
Smart 'Key'	22€	15€	0	37€

Notes 1) Logins / year = 245 work days / yr * 1.5 logins / day = 367.5
2) Device cost reflects the 'street price' at 5000 unit pricing levels

High costs have limited the number of identity tokens in use; IDC estimates the market for even lower-cost identity tokens, such as RSA's' SecurID, is only 18M units worldwide. Reducing token cost and complexity allow services dissatisfied with passwords to transition more easily to advanced authentication options.

Strong authentication improves user confidence and convenience, but the real beneficiaries are:

A) Merchants who now pay nearly 90% of the 1B Euros in fraud-related costs
B) Corporate intranets and extranet providers (e.g. Banks, Governments, Trading Portals, etc.) that assume the risk of offering services online
C) Issuing banks that will be liable someday for remote-payment fraud when merchants use 3-D Secure. Issuing banks are concerned because they are unable to transfer fraudulent costs onto card users
D) Mobile operators who can offer strong identity services or offer their infrastructure to other identity providers

2.3 Liberty Benefits for the Mobile Industry

The definition of 'federated identity' allows an authenticated user to be recognized and take part in services across different and independent domains. Domains in a mobile context can be mobile operators, application/content providers and related entities.

Users expect mobile data services to be as easy as the "dial and hang up" action of voice services. However, data services typically require more user interaction with the mobile device. For some users, the sleeker, smaller, more sophisticated mobile phones of today make it difficult to type in multiple user names and passwords when accessing each new service. For mobile phone users, time literally is money.

But the challenges transcend mere convenience. Mobile operators need to ensure interoperability to attract service providers across the world. Emerging privacy and number-portability legislation are making interoperability even more complicated and more critical.

2.3.1 Mobile Operator Benefits

Liberty Alliance allows mobile operators to extract value from their infrastructure investment, increase data over their licensed airwaves and expand their brand's reach. In addition, the telecom industry's event-based billing processes, already interoperable on a global scale, represent the target billing model for nearly all computer-related products and services. To summarize:

- New revenue
    - Identity services including user authentication and consent
    - Infrastructure sharing, including SIM, with other ID providers, when operators choose not to be the identity provider because of risk or geographical coverage
    - New data services generate an increase in data traffic
    - Third-party billing enables event-based pricing models for non-operator related services and guaranteed payment for small transactions

- Interoperability
    - A de-facto-identity Liberty framework enables data and services to be exchanged between operators, i.e. "Identity Roaming"
    - Liberty compliance simplifies the service-provider interface, and without many operator proprietary interfaces, accelerates integration and availability

- Positions the mobile network as a preferred channel for trusted services
    - Operators can link disparate identity information (between fixed, Internet and wireless accounts) while using pseudonyms to protect user information
    - Mobile operators can confirm a user's request to exchange private data securely (e.g. presence, geolocation) with services that use the information
    - The mobile network is commercially ready; it is trusted, managed, convenient, reliable and regulated

- User convenience
    - Single Sign-on (SSO) allows users to move seamlessly between federated services without entering numerous user names and passwords
    - Permission-based Attribute sharing enables personalization of the service delivery; providing a better customer experience.

- Regulatory Compliance
    - Liberty's privacy framework and pseudonymous linking allow users to log-on anonymously and still have access to their designated services.
    - Interaction with governing agencies promotes an acceptable sharing of services with other services in a country or across national borders

2.3.2   Service Provider Benefits

Service provider benefits generally derive from a lower cost-of-business and a larger available market. The mobile network also enables a new level of customer care. To summarize:

- Larger Available Market
    - A Liberty circle-of-trust for operators lets service providers offer their services to all possible users (regardless of their choice of operator) through a single interface (see the diagram below)
    - Liberty compliance provides the security to improve user confidence and the personalization to maximize services

- Lower Cost-of-Business
    - A standard developer platform for using operator services (i.e., payment, messaging applications, etc.) lowers the integration effort and accelerates time-to-market
    - Two options exist for enhanced identity services:
        1. The service provider can rely on an identity provider and 'outsource' the overhead of user authentication; this allows the service to focus on the value it provides users
        2. A service provider can continue to authenticate users but leverage the savings from an operator-enabled shared SIM

- New Levels of Customer Care
    - The mobile network puts the user at the center of services; the user is no longer required to 'go to' the network as with points-of-sale or the fixed-line Internet; the network… and service… are more accessible

2.3.3 User Benefits

Users benefit directly from more services, which are easy to use at a lower cost. With mobile networks, privacy and consent are requirements for success. To summarize:

- Convenience
    - Single Sign-on (SSO) allows users to move seamlessly between federated services without entering numerous user names and passwords
    - Permission-based Attribute sharing personalizes the user experience and convenience

- More services
    - A Liberty standardized-service interface accelerates time-to-market for services
    - Improved authentication reduces risk and allows additional service options

- Confidence
    - Users can set up their own privacy controls and intrusion levels. A Liberty implementation and pseudonymous linking allow users to log on anonymously and still access their designated services.
    - Users can control which services are linked, or federated, and what data are shared

- Lower cost
    - Less fraud means fewer charges passed on in a lower price
    - Economy of scale… integrated services reduce the average cost per transaction
    - Lower identity-related costs reduce the overhead service providers must charge

2.3.4 Vendor Benefits

Mobile vendors, including network infrastructure, devices and platform, benefit from an increased demand for standardized, higher-end devices that leads to volume savings in production cost. To summarize:

- High-end devices
  - 'Smart phones' that support voice and data services
  - User demand for identity-enabled services that accelerates device renewal
  - Advanced operating systems that support multi-credential requirements

- Lower cost
  - Economies of scale… standards for devices that span multiple industries and combine support for multiple identity providers
  - Standards-based implementations help reduce production costs and shorten time-to-market

- Larger market
  - Multi-credential management, an extension to existing issuer-personalization services, that securely updates a SIM remotely in a neutral manner
  - Easier use of terminals increases user experience and brand loyalty
  - Standardized service interfaces accelerate wide-scale adoption

2.4   Example Identity Trends in the Mobile Industry

For the past three years, efforts to extend the mobile operator's role in identity services, such as authentication and user consent, have intensified and converged in the Liberty Alliance.

Since 1999, the mobile-security industry organization Radicchio had been defining a platform for mobile-assisted identity services.   The Trusted Transaction Roaming, or t2r, effort was expanded in a 2003 European Commission project with Gemplus, Orange, Radicchio, SmartTrust, Ubizen and Vodafone.

The t2r work, recently transferred into the Liberty Alliance via Radicchio, enables:

1. Multiple credentials from existing identity providers (Banks, Operators, Corporations and Governments) to be loaded into a secure storage, such as the SIM card

2. Service providers a single entry point into an interoperable 'mesh' of numerous mobile operators

In addition to the Liberty Alliance, similar identity and SIM-sharing efforts are in the works:

- Mobey's 2003 pilot downloaded a Java-based credential to a Nokia-model phone

- RSA has announced a SecurID downloaded onto a Nokia-model phone

- Mobile Payment Forum discussed methods for mobile-assisted "3rd Party Authentication" to enhance 3D-Secure online-payment models

- Mobile Web Services announced a mobile-assisted identity effort

- Operators and banks in Central and South America already share the SIM to simplify pre-pay top-up

- 3GPP looks to standardize user profile in 2004.

- As part of the t2r European Commission project, input and recommendations were sought from several United Kingdom banks, BACS, Simpay and European card associations Visa, Mastercard and American Express

Many of these early efforts lack the cooperative business model being discussed within the Liberty Alliance's Mobile Business Guidelines.

To accelerate wide-scale deployment, operators must be compensated fairly as identity, SIM and attributes providers.

For entities to rely on operator-supplied services and infrastructure, they must be equitable for all.   For this reason, efforts such as Global Platform, the banking industry's standard for a multi-issuer card, are being considered.

3 BUSINESS GUIDELINES OVERVIEW

The following is a high-level overview of the Business Requirements that must be considered during a large-scale deployment. For more information, refer to the business guidelines document (URL).
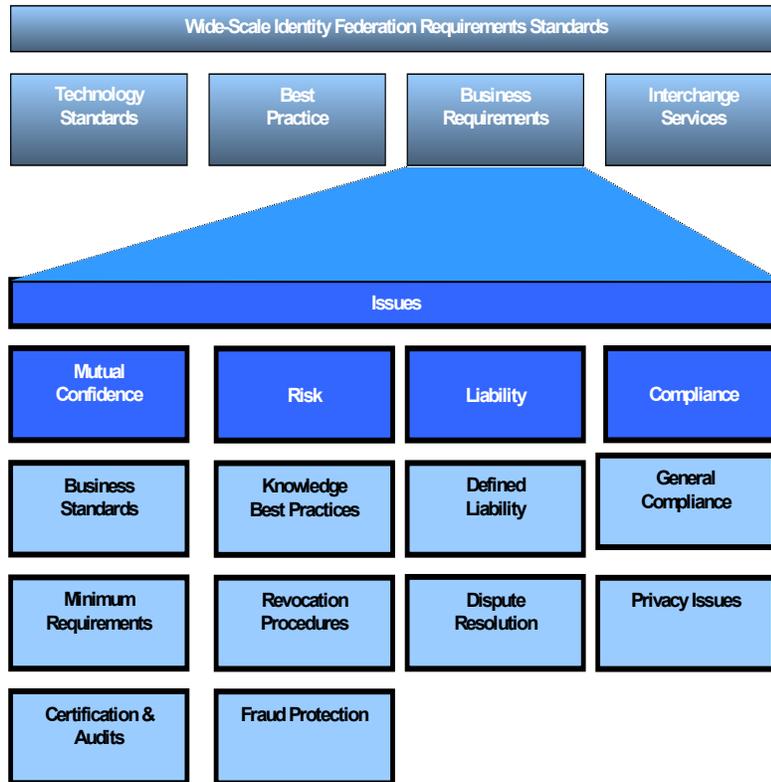

Figure 1: Positioning the Liberty Business Guidlines in the Federated Identity Business Requirement Framework

Each of the major modules identified above is discussed in greater detail in the sections that follow.

3.1 Mutual Confidence

Mutual confidence is one of the basics of employing federated identity, i.e., the ability to rely on identity assertions and the integrity of identity-related information exchanged among members of a federation.

The integration of Web-services technology brings unique benefits, as mobile terminals can:

- Refer to one person
- Enjoy greater global adoption than computers
- Serve as a trusted environments to their users
- Support high level of security
- Assist fraud prevention

By using mobile phones, customers could be alerted quickly in case of fraud, and they also could be more responsible for transactions being confirmed or certified with their mobiles.

Of course, introduction of mobile-phone mechanisms also mean new challenges, regarding:

- Handling and user interface, especially referring to complex transactions

- Deployment of architecture and capabilities of the Liberty specifications at mobile network operators

- Mobile terminal loss and theft

Insurance and new prevention systems are being introduced to protect mobile phone users from terminal loss and theft.

Examples for using the mobile infrastructure with Liberty-enabled infrastructure include:
- Taking advantage of the SIM to validate transaction, personalize service portals and capture user consent.
- The ability of users to control the sharing of their personal attributes and identity.

3.1.1 Business Standards

Business Standards comprise the set of rules, conventions and guidelines that participating members of a circle of trust need to follow. The business standards most critical in creating a circle of trust related to identity transactions include:

- ✓ Legal structure of circle of trust, relationships among participants. In many cases, this likely will build up on current Web-services' business standards and service-contractor contracts

- ✓ Technical standards and associated levels of performance

- ✓ Security and Privacy standards, which usually will refer to the required security and privacy standard

- ✓ Accreditation standards and guidelines that refer to regional banking laws. In most European countries, mobile operators are not allowed to cash more than

10€ at a time for a third party. Guidelines could define the payment provider according to different amounts of money

✓ Trade standards for vertical and cross-vertical transactions, such as automatic delivery in case of undermining certain stock levels and billing

✓ Adoption and alignment with legal standards (such as HIPAA and privacy law)

Federation governance provides the frameworks for the definition, development, execution and enforcement of these standards. The governance framework numbers among the measures used by the circle of trust members to demonstrate how to manage the risk of federating identity, and how to achieve regulatory compliance.   It drives the legal structure of the circle of trust and the relationships among its participants. Regulatory considerations encompass how membership in the trust circle is determined and managed, member service pricing, and avoidance of anti-trust exposure. For example, liability and charges could depend on the security level a service provider requests from the identity provider and the Principal.

Business standards related to information privacy and customer information management also are material for both practical business and regulatory reasons.

Monitoring and enforcement of minimum acceptable standards for all members of a federation (or a circle of trust) ensures that no weak link creates exposures for the participants. Additionally, liabilities may be incurred by lapses in adherence to the standards.

The fundamental structure of the circle of trust as outlined in the Liberty specifications must be decided. Mobile network operators are expected to act as identity providers for their subscribers. Liberty supports both a single, industry-wide circle of trust with a neutral party providing common functions and multiple circles of trust where users are able to use their identity-dependent services when roaming between circles of trust. The choice between one or many circles of trust depends on regional regulations such as privacy and commercial factors such as service localization.
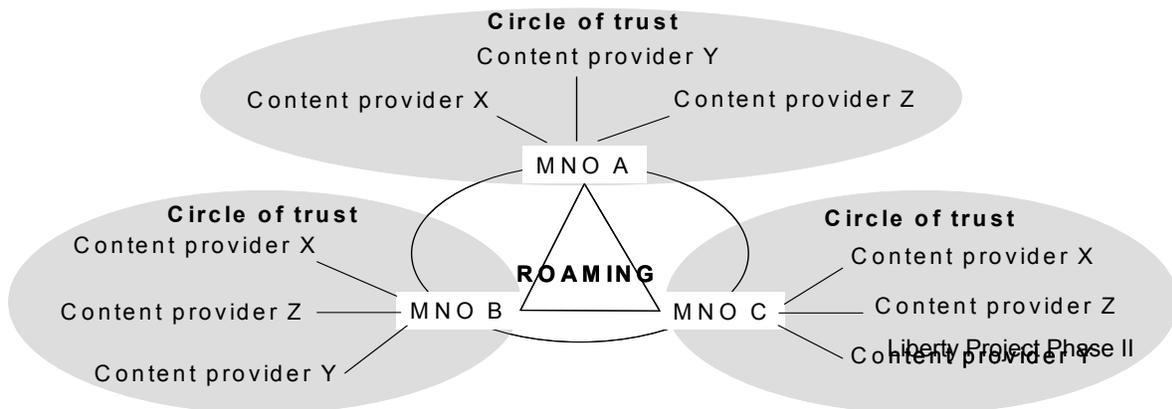
The broadest level of interoperability is made easy with a single circle of trust among all participants. However, some operators are likely to favor coexisting with other more limited Liberty deployments. The current specifications do allow for sharing of

authenticated identity; but don't yet provide a robust solution to share the identity attributes when roaming across circles of trust. However, that functionality is planned for Phase III, enabling full interoperability across circles of trust.


Liberty Project Phase III
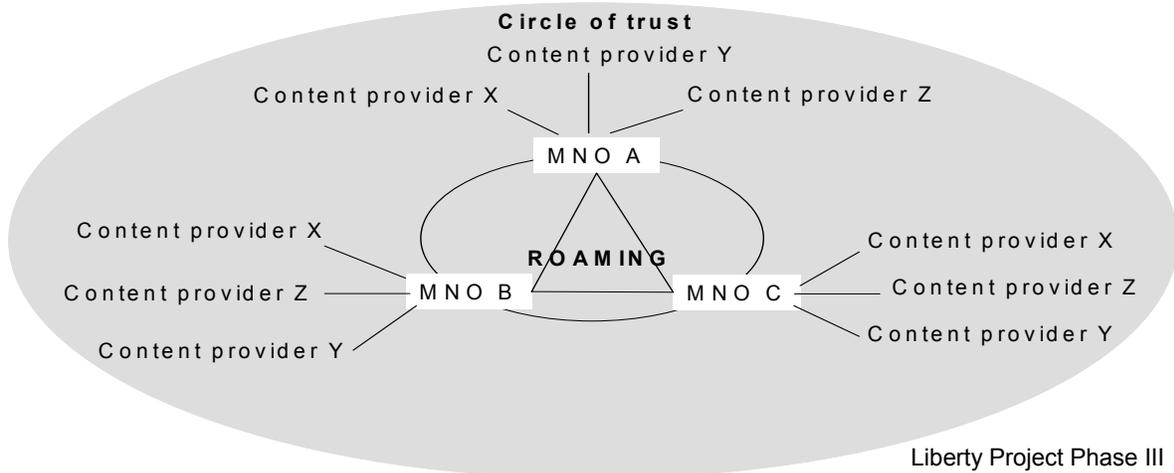
For the purposes of simplification, we assume a single CoT exists within the Mobile environment.

The following Liberty entities in a circle of trust must be mapped and mutual dependencies and obligations incorporated in the contracts forming the legal structure of the federation:

- Identity Provider (IDP)
- Attribute Provider (AP)
- Service Provider (SP)
- Discovery Service (DS)
- Principal (End-user, consumer)

The Discovery service will be deeply linked naturally with the Identity Provider, as the principals enable the IP to disclose certain attributes. With the Discovery Service, an identity provider can present service providers with the information they can obtain about the principal. The principals can store the required attributes for the services they use at different Web/WAP Service Providers and with their mobile operators, as well as link them. The attribute provider can be any service provider (including mobile network operators) that might provide an attribute within a principal's identity, but not the identity as a whole. Therefore, different attribute providers could provide attributes contained in the Discovery Service.

To clarify these connections, this graphic visualizes them and describes the non-Liberty functions of the Players in fat letters on top of the icons, while different Liberty-defined roles that a player can hold are represented by different shades. The main role of a player is indicated on top of the functions, arranged according to expected priority in Liberty functions.
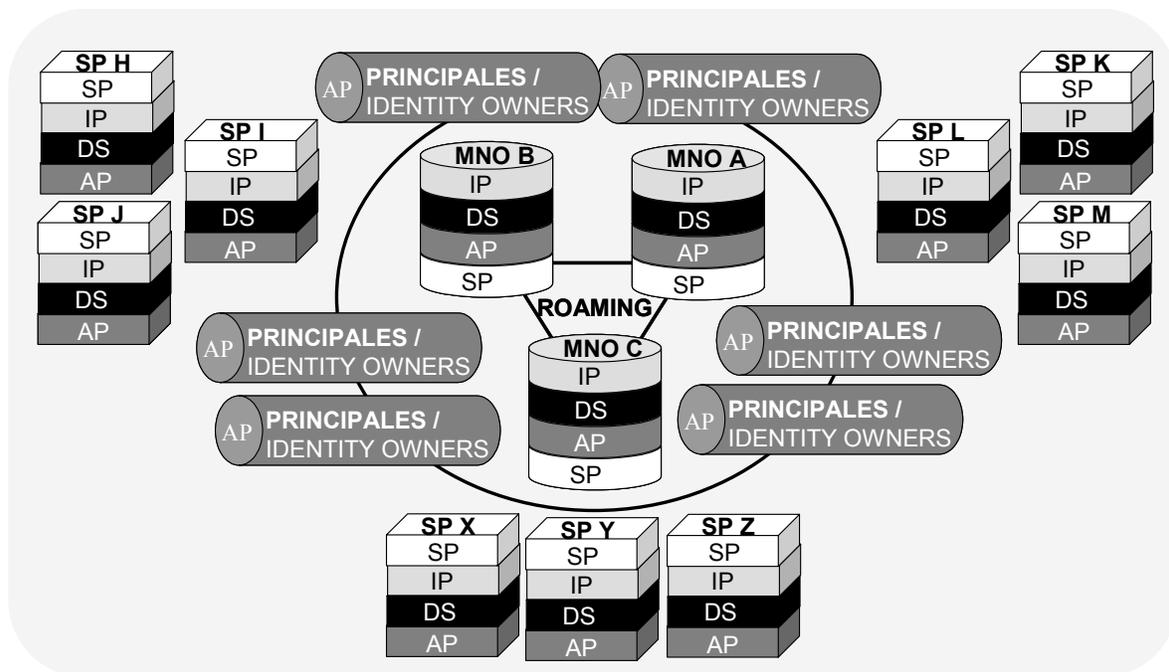
Given the multiplicity of mobile devices with varying functional components, air interfaces, and terrestrial network capabilities, business standards are needed to ensure consistent identity provider services (e.g., authentication) through abstractions of devices, access methods, and authentication means. Ideally, this abstraction model would be extensible for future technologies and broad enough to encompass the range of existing technologies in use (e.g., WiFi, peer-to-peer, as well as GSM/GPRS/3G, and CDMA 1x/2000).

Privacy, of increased concern in the mobile environment, should allow for affirmative end-user action (consent) before using a service offering. It also should provide for disclosure of privacy policy, enable consumers to elect which types of information can be disclosed to which kinds of entities with which kind of consent.

One key element to be defined embraces the list of allowed authentication contexts and their meanings; i.e., how the subscriber was authenticated (pin/password, SIM card, cert, etc.). Service providers will apply their acceptance policy to the authentication context in an identity assertion to determine its adequacy for the service being requested. To avoid Liberty services requiring additional sign-on whenever services from different providers are requested, a limited number of authentication levels should be agreed to within a circle of trust. (See 4.3)

Existing roaming agreements must be assessed for potential impact, or utility, in establishing the legal framework for an identity federation as well as existing contracts between service provider and customers (e.g., legal frameworks and common contracts for online banking).

These business standards are essential to defining the authentication standards associated with vertical and cross-vertical transactions.

3.1.2 Minimum Requirements for Service Delivery Control

These are the quality-control measures for service delivery that must be articulated clearly and enforced to lessen operational performance risks:

- ✓ Internal controls
- ✓ Service level achievement against controls and technical standards
- ✓ Employees' integrity/certification requirements
- ✓ Audit

Each member of a circle of trust must assert they can and will adhere to a minimum level of standards and requirements. In addition, each member must have the ability to confirm and validate that these standards are being followed (see Certification & Audits).

Further, recourse must be defined for instances when minimal requirements are missed or when a participant is disqualified. Disqualification criteria should be defined to reflect the effects on the circle of trust when a service provider's reputation is damaged (e.g., public scandal, referring to abuse of customer data) or when complaints of poor/non-delivery of service accumulate.
The federation likely will need to provide for continual improvement in the level of minimum requirements to ensure the quality of services delivered over time.

The mobile environment poses a number of unique challenges that must be addressed in the form of minimum requirements. These factors include:

- Poor, erratic, or dropped RF signal coverage. Impacts to user sessions and interactions, restoration of logically consistent states upon signal recovery

- Recovery from a device's loss of power or power-down by user

- Simplified human interface that includes checks against accidental input errors

- Requirements that apply to federation members (e.g. content/application providers) that are not mobile operators

- Micro payments for Web services might raise principals' expectations of quality of service and require contact persons to deal with occurring problems

3.1.3 Certification & Audits

Certification represents the act of confirming that certain facts are true, and that the levels of performance and conformance are maintained. Factors include:
- Authentication Contexts – how the different authentication contexts are certified for consistency across the federation. Service providers rely upon the veracity of the authentication context when applying their own local acceptance policy to an authentication assertion. Three levels of authentication could be used:

  - Low authentication level: single sign on at Web sites and e-mail providers

  - Medium authentication level: sign on at Web site, receive SMS with WAP link that requests SIM confirmation through the user's mobile phone

  - High authentication level: Recheck SIM authentication when entering highly confidential data and/or usage of TANs

Service Providers joining a circle of trust can choose which authentication level they wish to require from a principal entering their service. Principals should be able to choose a certain minimum level for all their transactions as well.

- Liberty IOP Conformance - conformance with Liberty standards for mobile devices and the terrestrial network-service elements to ensure interoperability with Liberty protocol standards.

- Identity Proofing – certification of identity providers' processes to ensure compliance with minimal identity-proofing, and revocation, requirements

- Legal Conformance – right of independent third parties to audit members' conformance to legal and business-process obligations

- Audit logs – requirements to maintain transaction audit trails for troubleshooting and non-repudiation

Certifications and accreditations are measures used by circle-of-trust members to validate the effectiveness of their standards, and to ensure ongoing mutual confidence vis-à-vis managing risks and complying with regulatory requirements.

Certification could be achieved by self-assertion of facts by a party, notification of compliance by accepted third parties such as external auditors, statement of compliance from an accredited testing organization, or through examination by representatives of the federation. It is possible that various methods might apply, depending on the category of the standard, the maturity of the standard, and the critical nature of the requirement.

3.2 Risk Management

The challenges inherent in the mobile environment require a comprehensive risk-management strategy to minimize potential costs and legal exposures.

Risk-management mechanisms should include considerations such as:

- The local/regional/national law and applicable international trade (EU/US/Country-Specific, etc.) law. A mobile identity infrastructure (e.g., data protection, usage of mobile signatures) is expected to interoperate even with different legal requirements between individual jurisdictions.

- Competition regulations (in terms of circles of trust issues of limiting the inclusion of additional parties by boycott, etc.) *Note: Circles of Trust neither enhance nor take care of legal/competition problems!*

- The code of conduct/practice within the mobile industry, possibly using existing roaming agreements and business contracts.

- A process to deal with actual or attempted fraud or identity theft, including responsibilities of each party

- Process for identity revocation, revocation of issued assertions, and notifications of affected parties

- Obligation of consumers to notify about device theft in a timely manner, and disclosure rules for consumer liabilities, if any.

- Process and standards for financial liabilities or chargebacks associated with revoked credentials

All entities face risk for potential exposure to financial injury or loss. Within the context of a federated identity, risk can manifest itself as actual losses due to fraudulent use of an identity, loss or exposure of identities or attribute information, and loss of business integrity from insecure processes and data. Both the identity user and the service provider are subject to financial loss and the loss of personal or business reputation (such as in the case of identity theft and fraud), but all parties in the identity network are exposed to the risks from insecure processes and data. Federations can manage risk through disseminating knowledge of best practices, revocation procedures, and fraud-protection measures.

3.2.1 Mobile Authentication Context Classes

Liberty does not prescribe a single technology, protocol, or policy for authentication between the principal and identity service. Consequently, if a service provider is to place sufficient confidence in the authentication assertions it receives from an identity provider, it is necessary for the service provider to know which technologies, protocols, and processes were used in the authentication.

This additional information is provided in the Authentication Context. The benefit of this "container" approach is that additional authentication mechanisms can easily be added.

The Mobile Authentication Context Classes need to align with historical 'authentication context classes,' so as those used in bankcard payment. For example, authentication of bankcard payments places a large distinction on the number of authentication factors used. In particular 'card present' payments with a principal's signature or PIN typically have a lower associated risk.

- **MobileTwoFactorContract** – Reflects mobile contract customer registration procedures and a two-factor based authentication. For example, a digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that requires explicit proof of user identity and intent, such as a PIN or biometric

- **MobileOneFactorContract** – Reflects mobile contract customer registration procedures and a single factor authentication. For example, a digital signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but *no* required PIN or biometric. Note that MobileOneFactorContract refers to 'something-you-have'… leaving the definition of 'something-you-know' to the password authentication context classes that already exist elsewhere

- **MobileTwoFactorUnregistered** – Reflects no mobile customer registration procedures and a two-factor based authentication, such as secure device and PIN. This context class is useful when a service other than the mobile operator wants to 'link' their customer ID to a mobile supplied two-factor authentication service by capturing mobile phone data at enrollment.

- **MobileOneFactorUnregistered** – Reflects no mobile customer registration procedures and an authentication of the mobile device. Again, this context authenticates the device, not a password, and is useful when services other than the mobile operator want to add a secure device authentication to their authentication process.

3.2.2 Disseminating Knowledge of Best Practices

Insight and experience when creating technical standards, entry criteria, and processes and rules, are inherent in the design and deployment of federation. However, risks will continue to emerge as technologies and experience in the marketplace evolve. The most effective way to stay up-to-date on these risks, design deterrents, and upgrade requirements and specifications involves deploying the best practices of the industry as the technology evolves. Best practices will be critical in the area of: sources of attacks, methods of attacks, sources of detection and safeguards.

3.2.3 Revocation Procedures

Revocation is the process of suspending the access rights of a principal, and also serves as a powerful potential tool to lessen risk. This could reflect a mutual agreement between the principal and one or more members of the circle of trust; or it could be the result of a breach or a dispute between the parties.

The following set of federated procedures can be defined and integrated into the operational delivery environment:

- Credential revocation
- Identity suspension
- Confidence lowering of a type of interaction (e.g. risk scoring)
- Affected party notifications
- Transaction revocation, cancellation, or reversal
- Fees and costs for these procedures, if any.

3.2.4   Fraud Protection Measures

The mobile device can be exposed to fraud once initial SIM authentication has been made, and the mobile is still switched on (through the PIN code). Since it cannot be guaranteed that the user is the correct one, a Liberty-enabled service must fulfill some basic security requirements, such as forcing user re-authentication (e.g., entering a password) after a certain amount of time has expired (e.g., 30 minutes), or each time after power has been cycled off and on. For certain classes of users, single sign on may be disabled, requiring per-transaction authentication. Or, re-authentication timers may be set based on user experience (longer times for those with a good usage record, shorter for those with less experience).

In the identity space, one area to consider in particular is the fraudulent use of an identity following its theft. This can entail creating and using invalid identities, repudiating a legitimate transaction by a user, or using a network's capabilities by a service provider without legitimate users behind its transactions. Each of these forms of fraud requires specific protections and constant vigilance, actions and alerts. This implies the need for active management and oversight of operations, procedures, data, and pooled information.

To address identity theft, companies issuing identities should consider delivering a clear statement to their end users. Attribute providers and service providers should do the same for the attributes they manage or use. The goal is to inform the end user of the scope and responsibilities of the different entities:

- Security Policy for Identity Management Providers (IdP)
- Security Policy for Attribute Management Providers
- Security Policy for Service Providers (attribute confidentiality).

Any identity federation will find that it must battle abuse of the system constantly through its use of pooled data, and that it will need to respond continually to nascent approaches of fraud and threats through new methods of detection and intervention.

3.3   Liability

Liability results from failures to satisfy obligations and requirements established in the legal structure (contracts) of the federation. The risk-management measures (described above) attempt to reduce the practical liability exposure in various scenarios. Liability is a function of the legal structure, business standards, and risk-management measures. Liability can be limited by mutual agreement in the contracts, as well as originating from the failure to meet contractual obligations.

3.3.1   Defined Liability

It is important to identify and define areas of potential liability, addressing each within an appropriate context (contracts, business standards, risk management, etc.). Liability areas to consider include

- Service Level Problems (i.e., the identity federation not working successfully)
    - o One result: A user can not be authenticated

- Identity misrepresentation by another individual
    - o By theft of device, username/password, etc.
    - o By failure to identity the principal adequately before issuing credentials
    - o By failure to revoke fraudulent or compromised credentials on a timely basis
    - o By failure to detect fraudulent use through appropriate fraud management practices

- Illegal or illicit activities over the network (e.g., terrorist activities)

- Ramifications of breakdown in specific services
    - o Failure of person-to-person money transfer can trigger domino effect of failed payments

Predetermined dispute resolution needs to be in place to address these and other issues:

- Assessing which federation member will bear costs associated with an identity network failure
- Source and amount of liability in case of fraudulent commercial activities
- Physical damages
- Failure to meet service-level assurances to relying parties

Failure to mitigate risk or to execute obligations defined in an agreed-to process or specification can generate liability. This can take the form of money damages or requirements to repair damages to another party in the event a) of an accident where the right of a principal (individual consumer or a company) was compromised; b) where laws or standards have been violated. In networked environments, potential liabilities exist for all parties, including providers, agents, and the network, based on agreements and expectations related to rules and performance.

Contractually identifying who bears what losses, and in what circumstances (minimum standards not being met, processes being omitted or shortcut, etc.), can help limit unnecessary frustration and expenses. Over time, the Web services and identity

federation industry likely will evolve customary practices for assessing and determining the allocation of liability between parties in a business relationship. In the absence of allocation of risk by private contract, recourse will be made to other less-preferable methods of dispute resolution.

3.3.2   Dispute Resolution

Identifying agreed-upon processes for resolving disputes can help minimize or eliminate the need for parties to resort to traditional and, often time-consuming and costly, means of resolving conflicts.

For example, if a customer of an online brokerage firm can't perform a critical trade because of a problem related to shared authentication, who is at fault? Who is financially liable? What is the individual recourse? What are the efficient and timely procedures for resolving the incident?

Traditional means of dispute resolution include mediation, arbitration, or recourse to appropriate legal or regulatory authorities. The means of resolving disputes should be specified in contracts.

Dispute Resolution methods tend to be human-resource intensive and may not be appropriate for the high-volume and automated environment of Web services. Parties should consider the extent to which mediation or arbitration options can be adapted for the online environment.

3.4 Compliance

Compliance with legal, business, technical, and operational requirements and standards are essential to achieving a practical level of mutual confidence to enable an identity federation to serve the needs of a major industry. Beyond the specific identity-related (e.g., Liberty standards) compliance issues, a host of other mutually interdependent compliance requirements exist that must be identified and ensured.

3.4.1 General Compliance

Compliance aligns agreed standards, policies and procedures. These standards, policies and procedures may be governed by contract – be they unilateral, bi-lateral or multi-lateral.

The principal drivers to follow to comply with the current market include:

- Existing mobile infrastructure requirements (GSM/CDMA/WiFi)
  - o GSM was first introduced in 1991 and, by 1998, GSM service was available in more than 100 countries and has become the de facto standard in Europe and Asia.
  - o Short for Code-Division Multiple Access, a digital cellular technology that uses spread-spectrum techniques. Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum.
  - o Short for wireless fidelity and is meant for use generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc.
  - o The t2r group already has prepared additional definition of Mobile Authentication Context Classes to be used as part of the Liberty framework. Other t2r material is being used to define the Intelligent Client portion of Liberty and the Business Guidelines for the Mobile market**.**

- Infrastructure deployment in progress, especially in the financial vertical: visa 3D secure is a clear driver for the market Liberty Alliance is tackling. It supports the financial industry's online-payment improvement program
  - o Continuing its leadership role in Internet payments, Visa has begun the global rollout of the Authenticated Payment Program. The Program, based on commercial incentives, will improve vastly the payment service for e-merchants, consumers and Visa Members by enhancing convenience, acceptance and security. Consumers will know they can shop safely and conveniently while preventing fraud on their card, and merchants will know they are dealing with a legitimate cardholder anywhere in the world. The newest authentication technology, 3-D Secure™, forms the basis for global interoperability of Authenticated Payments.

- Other applicable standard organizations: ETSI, OMA, ECBS, MPSA, among others
    - ETSI plays a major role in developing a wide range of standards and other technical documentation as Europe's contribution to worldwide standardization in telecommunications, broadcasting and information technology. ETSI's prime objective embraces the support of global harmonization by providing a forum in which the key players can contribute actively. The European Commission and the EFTA secretariat officially recognize ETSI. The discussion of regulations and laws includes a description of signature methods. Some Liberty Alliance members also lead the effort for standardizing mobile signatures, formally ETSI STF-221
    - The Open Mobile Alliance aims to grow the market for the entire mobile industry by enabling subscribers to use interoperable mobile services across markets, operators and mobile terminals. This is achieved by defining an open standards-based framework to permit applications and services to be built, deployed and managed efficiently and reliably in a multi-vendor environment.
    - The Mobile Payment Forum is a global, cross-industry organization launched in November 2001 to create a framework for the deployment of simple, secure and interoperable m-payments. The Forum provides an open, flexible and trusted environment in which member organizations can clarify the opportunities and address the complex challenges facing the industry.
    - In addition to this ETSI standards organization, Liberty Alliance interacted with Paycircle (a wallet initiative) and Mobile Payment Services Association (MPSA).

3.4.2   Privacy Issues

Most consumers are extremely reluctant to give out such information as a credit card number and expiration date for fear that it will be intercepted by a third party and fraudulently used or, will be otherwise susceptible to misuse while in the possession of a retailer. Others prefer not to use credit cards, wishing to preserve their privacy and anonymity online.

The European Union has the most advanced regulatory framework for data protection. Two European Directives relate directly to the t²r infrastructure:

- Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the Protection of Personal Data 95/46/EG adopted 24th October 1995

- Directive 2002/58/EC of the European Parliament and of the Council was adopted on July 12th, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (named EU data protection Directive for electronic communications). This Directive was to be transposed in member state legislations by 31 October 2003 and since this date it has replaced Directive 97/66/EC.

It would take too long to detail the directives' implementation, however here are summarized analyses of these texts.

Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the Protection of Personal Data 95/46/EG adopted 24th October 1995
The relevant general legislation across the European Union is the European Directive on the Protection of Personal Data 95/46/EG adopted Oct. 24, 1995 entered into effect on Oct. 25,1998. The Directive sets out, inter alia, basic principles and rules for collating and keeping computerized personal data about individuals, placing clear obligations upon those who wish to do so in respect of how that data may be gathered, for what purposes it may be used (i.e. those for which it was collected) and confidential and secure processing.

To remove the obstacles to the free movement of data while guaranteeing the protection of the right to privacy, the European Directive 95/46/EC aims to harmonize the national provisions in this field. The right to privacy of citizens, therefore, has equivalent protection across the Union. The Member States of the EU are required to put their national legislation in line with the provisions of the directive by Oct. 24, 1998. Most member countries have fulfilled these requirements.

'Personal data' are data relating to any identified or identifiable individual (the 'data subject'). Individuals are identifiable not only by their name but also by their pictures, their telephone number and by some special identification number, etc.
Data subjects are granted a number of important rights and may appeal to independent national authorities if they consider their rights are being disrespected. These rights include: information from subsequent data users about where the data originated (where such information is available), the identity of the organization processing data about them and the purposes of such processing; a right of access to personal data relating to him/her; a right to rectification of personal data shown to be inaccurate and the right to opt out of allowing their data to be used in certain circumstances (for example, for direct marketing purposes, without providing any specific reason).

In the case of sensitive data, such as an individual's ethnic or racial origin, political or religious beliefs, trade-union membership or data concerning health or sexual life, the Directive establishes that such data can only be processed with the explicit consent of the individual, subject to a number of exemptions for specific cases, such as consent of the data subject or where an important public interest exists (e.g., for medical or scientific research) where alternative safeguards have to be established. In the specific case of personal data used exclusively for journalistic, artistic or literary purposes, the Directive requires Member States to ensure appropriate exemptions and derogations exist which strike a balance between guaranteeing freedom of expression while protecting the individual's right to privacy.

Data controllers are required to observe several principles. These principles not only aim at protecting the data subjects but also are a statement of good business practices that contribute to reliable and efficient data processing.

- Data should be processed fairly and lawfully.

- They should be collected for specified purposes and used accordingly. The purpose of the processing should be explicit and should be legitimate.

- Data should be adequately relevant and not excessive in relation to the purpose for which they are processed.

- Data should be accurate and, where necessary, kept up to date. Data controllers are required to take any reasonable step to ensure the rectification or erasure of inaccurate data.

- Data should be kept in a form that permits identification of individuals for no longer than it is necessary.

- Personal data can be processed (i.e., collected and further used) if:

- The data subject has given his or her consent clearly (i.e., if he or she has agreed freely and specifically after being adequately informed), or

- Data processing is necessary for the performance of a contract or to enter into a contract requested by the data subject (e.g., processing data for billing purposes or processing data relating to a job applicant or for a loan), or

- Processing is required by law, or

- Processing of data is necessary to protect a vital interest of the data subject, or

- Processing is necessary to perform tasks in the public interest or by official authorities (such as the government, the tax authorities, the police, etc.) to show that they have accomplished their tasks.

Finally, data can be processed whenever the controller or a third party has a legitimate interest and this interest is not overridden by the interest of protecting the fundamental rights of the data subject, particularly the right to privacy. This provision basically establishes the need to strike a reasonable balance in practice between the business interest of the data controllers and the need for privacy of data subjects. This balance has to be struck in the first place by the data controllers under the control of the data protection authorities although, ultimately, the courts must decide.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directive 2002/58/EC complements Directive 95/46/EC for the electronic communications sector. It includes inter alia specific provisions regarding the confidentiality of communications, the handling of traffic and location data and the requirements and restrictions applying to the use of cookies as well as to unsolicited electronic communications, among which those transmitted by automated calling machines, fax and electronic mail. The Directive defines "electronic mail" as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient," so it relevant for any unsolicited transmission by SMS and MMS.

Member States had to bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive not later than Oct. 31, 2003. Most European member countries have employed the Directive.

The provisions of the Directive are aimed to protect, by supplementing the general data protection Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal person in the area of electronic communications and mobile networks by introducing specific legal, regulatory, and technical provisions, in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users.

The Directive considers the new advanced digital technologies introduced in public electronic communications networks, which gave rise to specific requirements concerning the protection of personal data and privacy of the user. More specifically, the Directive considers the development of the information society, characterized by the introduction of new electronic communications services and the cross-border development of these services, such as video-on-demand and interactive television. The success of these services, from the Directive's point of view, depends partly on the confidence of the users that their privacy will not be at risk.

4   EDITORS, REVISION HISTORY AND REFERENCES

Editors	Company
Frank Kaupa	American Express
Xavier Passard	Axalto, a Schlumberger Co.
Alain Nochimowski Philippe Deniau	France Telecom
Paul Miller	Gemplus
Mark Foster	NeuStar
Ian Nordman, Bjorn Wigforss	Nokia
Andrew Sikiar	SUN
Stephanie Manning Christina Hirsch James Vanderbeek	Vodafone

Revision History

Date	Version	Description	Editor
	01-03		
1 Nov 03	04	Introduced additional text from ITU Geneva Telecom & EC t2r study	Paul Miller
13 Nov 03	05	Extensive edits	Mark Foster
18 Nov 03	051	Edit Mutual Confidence section & Localized comments	Christina Hirsch Stephanie Manning
9 Dec 03	06	Edit compliance section	Xavier Passard
2 Jan 04	1.1	Combined all existing edits, fixed grammar & spelling flags, accepted all previous changes	Paul Miller
21 Jan 04	2.0	Replaced the intro with the mobile messaging brief	Paul Miller
6 Feb 04	2.4	Final meeting changes, professional edit and release to vote	Paul Miller

References

Document	Author(s)
LAP Telecom Case Study 09.25	Ketchum
Mobile Implementation Guideline	Liberty Alliance
Phase 2 Liberty ID-WSF Implementation Guide	Liberty Alliance
Tier 1 Business Guideline document	Liberty Alliance
Trusted Transaction Roaming, a Radicchio and European Commission Project	Radicchio, Gemplus, Orange, SmartTrust, Ubizen & Vodafone