Digital Identity Management
A Critical Link to Service Success

A Public Network Perspective

A Telecompetition Group Market Study Report
January, 2007
# Table of Contents

1. **Executive Summary** .......................................................................................................................... 1
2. **Introduction** ...................................................................................................................................... 3
   2.1 An Industry in Transition .................................................................................................................. 3
   2.2 Trust .................................................................................................................................................. 5
   2.3 Identity Management Trends .......................................................................................................... 6
   2.4 Industry Standards and Liberty Alliance .......................................................................................... 9
3. **Telecommunications Services Market** ............................................................................................. 14
   3.1 Legacy Model .................................................................................................................................. 14
   3.2 The New "Networks" ballpark ........................................................................................................ 15
   3.3 The Natural, Being a Player ............................................................................................................ 17
   3.4 Mobile Operator Advantages ........................................................................................................ 18
   3.5 E-Government ............................................................................................................................... 18
   3.6 Market Size ..................................................................................................................................... 19
   3.7 Changing Structure ......................................................................................................................... 20
4. **The Identity Management Market** .................................................................................................... 22
5. **Future Scenarios** ............................................................................................................................... 27
6. **Scenario Analysis** ............................................................................................................................. 34
   6.1 Scenario Validation .......................................................................................................................... 35
   6.2 The Liberty Alliance Approach ...................................................................................................... 36
   6.3 Demand for Digital Identity ........................................................................................................... 37
   6.4 Factors Impacting Telco Revenue Growth ...................................................................................... 39
   6.5 Worldwide Network Operator Revenues ....................................................................................... 41
7. **Conclusions** ....................................................................................................................................... 44
8. **Additional Conclusions for Liberty Alliance Members** ...................................................................... 45
9. **Appendix A – Industry Evolution** .................................................................................................... 46
10. **Appendix B Scenario Planning Methodology** ................................................................................ 55
    10.1 Driving Forces including Critical Uncertainties .......................................................................... 57
    10.2 Mapping Critical Uncertainties .................................................................................................. 58
11. **Appendix C - Demand for Digital Identity Capabilities** ................................................................. 61
12. **Appendix D – Validating Scenarios: Laws of Identity** .................................................................... 63
13. **Appendix E – Regional Differences** .............................................................................................. 67
    13.1 Prepaid .......................................................................................................................................... 68
    13.2 Strong Authentication .................................................................................................................. 70
14. **List of Terms** .................................................................................................................................... 72
15. **References** ....................................................................................................................................... 73
16. **Study Participants** ........................................................................................................................... 74
17. **Index** ............................................................................................................................................... 75
Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Industry Structure Changes</td>
<td>4</td>
</tr>
<tr>
<td>2.2</td>
<td>Internet and Telecom Environments</td>
<td>5</td>
</tr>
<tr>
<td>2.3</td>
<td>Key Constituents in a Federated Approach</td>
<td>7</td>
</tr>
<tr>
<td>2.4</td>
<td>Layers of Digital Identity</td>
<td>8</td>
</tr>
<tr>
<td>2.5</td>
<td>Liberty Alliance Circles of Trust</td>
<td>10</td>
</tr>
<tr>
<td>2.6</td>
<td>Industry Bodies Involved with Identity Management Standards</td>
<td>11</td>
</tr>
<tr>
<td>2.7</td>
<td>Identity Architectures</td>
<td>12</td>
</tr>
<tr>
<td>3.1</td>
<td>Legacy Telco Business Model</td>
<td>14</td>
</tr>
<tr>
<td>3.2</td>
<td>Internet Applications Separate Transport from Services</td>
<td>15</td>
</tr>
<tr>
<td>3.3</td>
<td>Network Operator Bypass</td>
<td>16</td>
</tr>
<tr>
<td>3.4</td>
<td>Classical View of Telecommunications Service Revenues</td>
<td>20</td>
</tr>
<tr>
<td>3.5</td>
<td>Telco Revenue at Risk</td>
<td>21</td>
</tr>
<tr>
<td>4.1</td>
<td>Three Phases of Identity Management</td>
<td>22</td>
</tr>
<tr>
<td>5.1</td>
<td>The Identity Scenario Planning Matrix</td>
<td>27</td>
</tr>
<tr>
<td>6.1</td>
<td>Scenario Characteristics Relevant to Identity Management</td>
<td>35</td>
</tr>
<tr>
<td>6.2</td>
<td>Synopsis of the Liberty Alliance Approach</td>
<td>36</td>
</tr>
<tr>
<td>6.3</td>
<td>Scenario I, Value Chain Participants</td>
<td>37</td>
</tr>
<tr>
<td>6.4</td>
<td>Scenario II, Value Chain Participants</td>
<td>38</td>
</tr>
<tr>
<td>6.5</td>
<td>Scenario III, Value Chain Participants</td>
<td>38</td>
</tr>
<tr>
<td>6.6</td>
<td>Scenario IV, Value Chain Participants</td>
<td>38</td>
</tr>
<tr>
<td>6.7</td>
<td>Factors that Impact Revenue Growth</td>
<td>40</td>
</tr>
<tr>
<td>6.8</td>
<td>Worldwide Telco Revenue Comparison</td>
<td>41</td>
</tr>
<tr>
<td>6.9</td>
<td>Worldwide Telco Revenues by Scenario</td>
<td>42</td>
</tr>
<tr>
<td>6.10</td>
<td>Potential Variations in Cumulative Network Operator Revenue</td>
<td>43</td>
</tr>
<tr>
<td>9.1</td>
<td>Communication Industry Silos</td>
<td>46</td>
</tr>
<tr>
<td>9.2</td>
<td>Triple Play</td>
<td>47</td>
</tr>
<tr>
<td>9.3</td>
<td>Viral Networks</td>
<td>48</td>
</tr>
<tr>
<td>9.4</td>
<td>Voice as a Software Application</td>
<td>49</td>
</tr>
<tr>
<td>9.5</td>
<td>Enter the Webcos</td>
<td>50</td>
</tr>
<tr>
<td>9.6</td>
<td>Industry Structure</td>
<td>51</td>
</tr>
<tr>
<td>9.7</td>
<td>Traffic and Business Models</td>
<td>52</td>
</tr>
<tr>
<td>9.8</td>
<td>A Comparison of Internet and Telecom Environments</td>
<td>53</td>
</tr>
<tr>
<td>10.1</td>
<td>The Scenario Building Process</td>
<td>55</td>
</tr>
<tr>
<td>10.2</td>
<td>Mapping Critical Uncertainties for Identity</td>
<td>59</td>
</tr>
<tr>
<td>11.1</td>
<td>Factors that Impact Revenue Growth</td>
<td>61</td>
</tr>
<tr>
<td>11.2</td>
<td>Demand by Scenario for Liberty Alliance Solutions</td>
<td>62</td>
</tr>
<tr>
<td>12.1</td>
<td>Analysis of Scenario Drivers and the “Identity Principles”</td>
<td>65</td>
</tr>
<tr>
<td>13.2</td>
<td>Prepaid vs. Contract Connections, Differences by Region</td>
<td>69</td>
</tr>
</tbody>
</table>
This report has been prepared on behalf of the Liberty Alliance.

Many statements in this report represent the views of the original author, Telecompetition, Inc., and have not been subject to formal approval in the Liberty Alliance. However, the main conclusions and key findings in the report have been reviewed by the membership.

Copyright © Liberty Alliance 2006. All rights reserved, respecting the rights of earlier copyright holders. A reproduction of this publication in part for non-commercial use is allowed if the source is stated. For other use, please contact the Liberty Alliance.

All possible care has been taken to assure that the information in this report is accurate. However, no warranty of any kind can be given with regard to this material. The Liberty Alliance is not liable for any errors contained in this report or for incidental consequential damages in connection with the use of the material. Comments or questions may be addressed to info@telecompetition.com or bglade@projectliberty.org

Report Scope

A clear distinction needs to be made between private and public environments. This report is focused firmly on the public telecommunications environment. This, by definition, excludes communications services and traffic within an enterprise. Under the umbrella of telecommunications we include all voice and data traffic that is public. Public is defined as traversing a common carrier, public network operator including an ISP network. It includes the full range of access networks such as wireline, cellular mobile, broadband wireless, and cable networks.
1 Executive Summary

“Identity validation, security, and privacy are increasingly critical issues in the world. A large community of players has developed to address these critical issues and propose solutions that are relevant to their needs. Like many emerging trends that are enabled by technology and propelled by social and political change, the solutions to this emerging identity crisis will arrive much more rapidly and profoundly than many businesses may contemplate. Thus, the current participants will likely reap the rewards of risk, while those that hope to be flexible followers may find the market has moved past their responses.”

Eileen Healy, CEO Telecompetition Group

When technology advances coincide and join with changes in the social, political and regulatory environments the effects can be explosive. The result can transform industries.

This study looks at the opportunity and challenges facing all public network operators – companies, whether they have fixed, wireless or mixed infrastructure. Such large, capital-intensive companies have survived many societal transformations and in many ways, they have thrived. The roadmap is not quite as clear as we look forward at the next transformation-- to a world where many different players are able to delivery compelling content and services often without the burden of large investments in infrastructure. The operator becomes the pipe while others enjoy the openness and other benefits of IP-based technologies.

The study analyzed identity management and its crucial role in enabling personalized services. Identity management is viewed as a crucial element in a basket of technology enablers that will be instrumental in preventing network operators from experiencing a dreaded “bit pipe” fate. Wireless operators are also at risk, right along with their fixed line counterparts.

The analysis focused on a high level global view through 2015. While certain operators may be able to “beat the odds” on a local basis, the overall picture is not pretty. The ability to use appropriate identity data, deliver a personalized user experience and protect user identity is necessary to maintain the enviable market position that network operators have enjoyed in the past.

Indeed, a large percentage of network operator revenue is already at risk through the ubiquity of IP, convergence and the emergence of powerful “Webcos” such as Google. By 2015, fully one half of the projected $2.5 trillion in service revenues is at risk.

So what can a public network operator do to protect these revenues? Under a broad range of plausible futures described in this report, an early focus on identity management and the types of capabilities that the Liberty Alliance and other protocols enable can preserve anywhere from 8 to 25% of this at risk
revenue. While the deployment of an identity management solution or market positioning as an identity provider is not the only factor that will preserve this revenue, it is a fundamental platform, indeed requirement, for any company intending to be more than a bit pipe in the future.

We believe all public network operators have a current advantage over Webcos and other new entrants as identity providers. This is due to the historic trust relationship with their users, which includes the protection of billing and customer data and the relative absence of spam in voice telephone networks. While not part of the quantitative aspects of this study, hybrid network operators, those with both fixed and mobile networks, are potentially further advantaged. This is due to their ability to leverage investments in identity management across both types of networks and customer bases.

A brief window of opportunity exists where the higher quality, more stable and trusted environment of telecom – especially mobile – can be successfully leveraged to retain customers. This initial defensive posture will lead over time to an opportunity to increase revenue through enhanced identity dependent applications and services.
2 Introduction

When technology advances coincide and join with changes in the social, political and regulatory environments the effects can be explosive. The result can transform an industry.

The communications and IT sectors are currently experiencing such a transformation. Technology developments have already initiated a radical restructuring of the sectors with significant impacts on both the dynamics of the industry and its regulatory environment. Social and societal factors are driving significant changes in end user behavior and expectations.

Evolving regulatory regimes are resulting in pressures for deployment of new technologies while at the same time imposing restrictions on the manipulation and sharing of personal data or identity information. Identity management is in the process of becoming a defining element that will impact the future structure of the converging communications and IT sectors.

These domains of change are of considerable significance in themselves. But combined they spawn new industry players and give rise to radical new business strategies that promise to transform the communications and IT sectors. Industry transformations driven in such a way are inexorably irreversible and potentially disruptive. Industry players who fail to ride the wave of change may not survive.

This Report uses a scenario planning methodology to explore the options and opportunities for identity management arising from the transitions currently being experienced by the communications and IT sectors. It addresses the issues by identifying and analyzing those drivers of change that most impact the deployment of identity management solutions but whose outcome is uncertain.

2.1 An Industry in Transition

The Liberty Alliance was formed in 2001, just as the dotcom boom was ending and as the telecommunications industry was about to suffer a massive downturn. The industry that has now emerged from the downturn bears only a superficial resemblance to that which had been in place, little changed, for the last two decades of the last century.

Services developed outside the traditional telecoms domain are driving fundamental changes within the industry. Presence and instant messaging are shaping the way communications services will be delivered in the future. Web services are emerging as the paradigm for communication between applications.

The introduction of IP networks has transformed service provisioning, lowering the barriers to entry for new service providers and introducing new service paradigms. Voice services are now being delivered commercially over the
internet. VoIP is no longer dismissed as a second rate service. Cable broadcasters are offering telephony. Television programs are being accessed over fixed and mobile telecom networks.

There is no longer a one-to-one relationship between services and access technologies. The widespread and ever increasing availability of broadband access is a major trigger opening up the industry value chain to new players.

Companies such as Google® and eBay should be seen as potential competitors to the traditional telcos. Such portal companies, which we call Webcos, offer communications applications as part of a wider service portfolio and attract subscribers away from the traditional network operators. This structure, illustrated in Figure 2.1, is still evolving and the relationship between network operators, content providers and service providers remains an uneasy one.

![Figure 2.1 Industry Structure Changes](source: Telecompetition Group, December 2006)

These new service providers threaten much of the traditional network operators’ revenue. Changes in the industry including open systems and convergence form the basis for key parts of the revenue forecasts including revenue at risk.
presented in this report. Further detail about this evolution can be found in Appendix A.

2.2 Trust

The internet world is still far from a trusted environment, wrought with security and privacy challenges (Fig 2.2). It’s a world in which end user expectations are that services and information are generally free. In the telecom world, however, end users are accustomed to paying for service. In return they expect, and receive, high quality of service levels. In general the telecom world is also regarded as a more trusted environment. Mobile networks in particular are known for their strong encryption and authentication procedures.

Figure 2.2 Internet and Telecom Environments

Source: Telecompetition Group, June 2006

All telecom networks have grown from a base of spam-free, high quality voice. Customers are used to a billing relationship where their personal information in generally protected. This existing climate of trust creates a brief window of opportunity for telecommunications operators, particularly those with converged offerings that include cost effective broadband access for computing devices.
2.3 Identity Management Trends

“In today’s information economy, trust is the necessary foundation for secure interoperability, and central to the successful realization of what’s possible on the Web. From the user perspective as well as that of the deploying organization, it’s an issue of who is trusted with what….and that requires policy, business and technology understanding and infrastructure. Thus the Liberty Alliance emerged: a first-of-its-kind standards organization with a global membership that provides a holistic approach to identity. “

Identity management is an integrated system of business processes, policies and technologies that enable content providers to facilitate and control their users’ access to online applications and resources which protecting confidential personal and business information. It represent interrelated solutions that administer user authentication, access rights, access restrictions, account profiles, passwords, and other attributes that enable use of applications. Identity management plays a key role in enabling personal, business and government activities. The integration and management of security, privacy and trust is of prime importance.

Individuals now play different roles in multiple activities that span across diverse contexts. The role of individuals themselves has become both more prominent and more tightly integrated into the digital environment.

Identity management is evolving to embrace these developments. But it faces different and often competing demands from stakeholders such as identity subjects, enterprises, service providers and government agencies, who all have different objectives and priorities when dealing with the management of digital identities. Increasingly the management of security, privacy and trust are the defining issues.

A universal, one-size-fits-all identity management solution is not going to materialize. Solutions that target enterprise environments are unlikely to satisfy the requirements of end users on public networks.

Identity management systems have to accommodate the needs of three communities (Figure 2.3). These needs have been expressed as follows [Durand, 2005]:

- **Individuals** need to know where information resides and to control sharing of their personal information

- **Businesses** (typically the "other party" to an identity interaction) need to identify and authenticate, to track interaction history, and to share certain information with partners

---

1 Definition largely drawn from Wikipedia.
• Governments have a need to know certain information themselves in certain circumstances and also need to act on behalf of individuals to regulate the use of information amongst businesses.

An identity management system may require separate components to address the different needs of these constituencies. But the market demand for identity management solutions may appear at different times and evolve at different rates in the different constituencies. An imbalance between the levels of demand is likely to persist for some time, undermining the economic sustainability of across-the-board solutions. The Liberty Alliance is a key worldwide body focused on aligning the various solutions.

**Figure 2.3. Key Constituents in a Federated Approach**

Successful identity federation requires that the needs of three different constituents are met: Individuals, governments and business.

*Source: Ping Identity Corporation, 2002*

Identity management solutions must not only address the requirements of consumers’ of identity information but must also meet the needs of the identity subjects. It is important to make a distinction between identity owners and identity attributes. Identity attributes may be provided by third parties who may or may not be known by the identity subject.
A commonly accepted framework is based around the notion of layers of digital identity illustrated in Figure 2.4.

**Figure 2.4  Layers of Digital Identity**

![Layer 3: Inferred Identity](image)

- **Inferred Identity**
  - Attributes = assigned, abstracted, you have no control

- **Layer 2:**
  - **Work Identity**
    - Issued in connection with employment
  - **Citizen Identity**
    - Passport, National ID Card, Social Security
  - **Customer Identity**
    - Airline Mileage, ATM card, Credit Card, Grocery Card

- **Layer 1:**
  - **Personal (My) Identity**
    - Attributes = You alone control, assertions you make about yourself

- **Layer 0:**
  - **Physical Identity**
    - Attributes = physical, biometrics

Source: André Durand, Ping Identity Corporation

The framework allows different digital identities to be created and matched to different circumstances or environments. It recognizes that identity attributes can come from a range of sources, some of which may not be known or controlled by the identity subject. Indeed, Layer 1 may be irrelevant where the identity of the individual is deemed to be subsidiary to the identity of a broader constituency. In many circumstances the identity that takes precedence may be driven by family, tribal, political or religious affiliations.

Identity information is used in a variety of contexts ranging from social blogging (in which the identity owner may deliberately desire to hide their true identity) to e-commerce or e-government in which proof of genuine identity is required. Identity management approaches that are appropriate in the enterprise environment may not be optimal or even viable in the social arena. Approaches tailored for e-government interactions may not satisfy the particular needs of e-commerce.
Identity subjects expect to have control over their identity assets. They expect to be able to configure their own policies and preferences for the management of their personal information, delegate to service providers or trusted third parties to act on their behalf and have degrees of assurance of the accountability of the involved parties.

2.4 Industry Standards and Liberty Alliance

The Liberty Alliance Project is an alliance of more than 150 companies, non-profit and government organizations from around the globe. It is committed to developing an open standard for the management of federated network identities that supports all current and emerging network devices [Do, 2006].

In the public network environment, network identity refers to the global set of attributes that are contained in an individual's various accounts. A user's network identities are like isolated islands spread across different service providers. Federation builds bridges that interconnect these islands together and allows information flows between them, allowing users to move seamlessly from one service provider to another.

Such a federation built on bilateral alliances between all involved service providers would be unmanageable. The Liberty Alliance therefore introduces the concept of an Identity provider, an entity that assumes the management of the users Federated network Identity and the user authentication. Identity providers are central to the Liberty Alliance concept of Circles of Trust (Figure 2.5).

A Circle of Trust is a group of service providers and identity providers that have business relationships and operational agreements based on the Liberty Alliance architecture. Within circles of trust users can transact business in a secure and apparently seamless environment.

The principal is the user, employer, customer, game user, etc. whose federated network identity is managed by an identity provider.

Leveraging identity providers acting as trusted third parties was a feature of the Liberty Alliance initiative’s early work on the provision of single sign-on for a federated environment [Casassa Mont, 2003]. Such work provides basic identity management functionality as well as addressing the issues of security, privacy and trust through a federated approach.

---

2 The Liberty Alliance (http://www.projectliberty.org/) is an open organization working on the technical, business, and policy aspects of identity. Initial work around identity federation has now moved on to value-add specifications around web services.
A federated identity approach satisfies end users’ requirements for privacy and control over identity information to a greater extent than a centralized approach. End user information is distributed in a federated approach, providing no central point of failure, and end users are authenticated once only, using pseudonyms to identify them to service providers. This approach allows identity information to be dispersed and stored across separate domains with separate control, providing an inherent capability for satisfying regulatory data protection requirements.

Federation is a familiar concept for mobile network operators and service providers for whom roaming is a central element of their business model. Roaming is built on federation, relying on an underlying technology combined with a set of business agreements that clarify issues such as payment responsibilities. Mobile network operators have therefore already resolved many of the agreements and issues involved with federation. The mobile industry works mainly through peer-to-peer relationships using standardized agreements as a starting point. Such agreements, created and managed by industry organizations such as the GSM Association, would give mobile network operators a head start in the deployment of federated identity approaches.
A number of industry groups are working on standardizing aspects of identity management (Figure 2.6). Different groups tend to optimize their solutions for the specific market segments with which they are associated but there is increasing cooperation and commonality between many of the groups.

Figure 2.6 Industry Bodies Involved with Identity Management Standards

![Diagram of industry bodies involved with identity management standards]

Source: Intel, December 2005

The Liberty Alliance for example originally worked on identity federation/single sign-on. That work was inspired by and built on the SAML activities from the OASIS group.³ Liberty produced several iterations of specifications around this activity while the OASIS group did a couple of iterations of SAML. Ultimately, the Liberty Alliance contributed its work back to the SAML group, and SAML V2.0 was produced as a grand convergence.

Although the initial work of the Liberty Alliance centered on identity federation the focus now includes the full range of identity solutions, including both user centric and federated approaches. It has become the international focal point for standardization of identity management protocols in a public network.

³ http://www.oasis-open.org/committees/security
environment and has been instrumental in creating an open dialog with the social networking, enterprise and other identity stakeholders.

A number of user-centric identity systems are available ranging from simple URL-based systems such as OpenID and LID (Light-Weight Identity), commercial offerings such as Sxip and Microsoft CardSpace and collaborations on user-centric systems like the Higgins Project.

User centric and federation are not competing models, they are both ultimately about the user experience.\textsuperscript{4} Issues such as where user centric begins, where federation begins, and where user centric and federation converge are being hotly debated. One attempt to distinguish between the different architectures is illustrated in Figure 2.7.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{identity_architectures.png}
\caption{Identity Architectures}
\end{figure}

\textit{Source: Telecompetition Group, August 2006}

Proposed, but not agreed, definitions for the different architectures are:

- User-Centric: user decides every time what identity attributes to reveal to the content provider
- Domain-Centric: user approves identity attributes appropriate to specific domains
- Federated: user approves transferring of identity attributes already given to other federation members

\textsuperscript{4} User privacy has been a focus from the beginning in the Liberty Alliance activities.
Debates on fundamental definitions can sometimes disguise the fact that practical solutions already exist in the market place. Different approaches are optimized for different situations. A range of possible solutions are available – there is no single “correct” solution for any given problem. The Liberty Alliance protocols support these various approaches.
3 Telecommunications Services Market

Adoption of standardized identity management solutions in the $1.5 trillion public telecommunications market will not only create a trusted environment where new identity dependent services can flourish, but will insulate network operators from dramatic revenue loss. While identity provision will not guarantee revenue growth, it is a necessary element for continued growth. Trust is an important aspect of this market, and one of its current strengths when compared with the internet market (Section 2.2). The market is described in this section.

3.1 Legacy Model

Two categories of business predominated in the legacy telco world – retail and wholesale (Figure 3.1).

In the wholesale supply route the external service provider tends to take the majority of the profit. Reduced margins for the network operator mean that wholesale operations may be regarded as a useful source of supplementary revenue but not as a viable substitute for retail business.
3.2 The New “Networks” ballpark

The introduction of IP networks and emerging technologies such as IMS mean that service creation and provisioning is no longer confined to the telcos. It’s not IP as such that is fundamentally disruptive. It’s not the fact that packets are used for data transport. The fundamental difference is the twofold separation of transport from services – technically and commercially (Figure 3.2).

![Figure 3.2 Internet Applications Separate Transport from Services](image)

Source: Telecompetition Group, August 2006

VoIP is the classic example of an Internet application resulting from the separation of transport from services.

Internet applications allow any service provider anywhere in the world to offer services to anyone, anywhere who is connected to the internet. There is no need for the service provider to enter into any contractual arrangements with the end users’ access network providers.

Service providers can deal directly with end users, bypassing the network operators (Figure 3.3).
Broadband access is now widely available from other service providers and provides users easy access to sources of content which are often free – supported by advertising revenues. Subscription revenues are declining at many ISPs as customers forego paying for their content and migrate to alternative broadband access providers.

Some major ISPs are responding to this dilemma with a radical change in their business model. The reliance on subscription fees is being abandoned in favour of advertising based strategies. These ISPs are planning to offer their full menu of services, including e-mail, free of charge to users with high-speed internet access or even a dial-up service from another provider. The gamble is that loss of subscription revenue will be more than compensated by increased advertising revenues.

This is a fundamental shift in strategy, from a transactional business model anchored in the telecom environment to a participatory or community based approach enabled by the internet. Essentially these ISPs are abandoning the traditional ISP market to become broadband web portals, speculating that content is better off being free, with a multiplicity of advertising offerings, than being a paid subscription service.
Many service providers are adopting a participatory rather than a transactional business model approach. Basic services are provided free of charge, building up a community of loyal subscribers. Once a sizeable community has been established, revenue can be generated from value added services supplied to sections of that community and, more importantly, from external advertisers interested in reaching members of the community. Such an approach is viable in the internet environment as there is no need for massive investment in network infrastructure.

There is still a need to provide access to the internet and the relationship between access network operators and service providers will remain an uneasy one.

### 3.3 The Natural, Being a Player

Significant business is only just beginning in the intersection of the telco and internet environments. Combined business models are at an emerging stage.

The ability of network operators to deliver authentication and identity management could play an important role in a transactional advertising environment. A new cooperative relationship could emerge in which network operators become “service enablers” for service providers, providing the QoS necessary for a trusted environment delivering security, privacy and reliability.

Webcos such as Google®, funded by advertising, rely strongly on the size of their user base. As there are over four times as many connections to mobile networks as connections to the internet, the mobile market would seem a natural target for companies like Google®.

No preferred business model for this has yet emerged although market research company Ovum notes that at least three options are being tested [Delaney, 2006].

- Google® going it alone.
  
  Google® has had a WAP search page for several years and has also added phone access to additional services such as Gmail.

- Limited, one-off deals with mobile operators

  T-Mobile in Europe uses a specially adapted version of Google® Search as the home page of its Web n Walk mobile internet service. But there is no ongoing development or revenue sharing. Other operators such as Japan’s KDDI intend to incorporate Google® search into their mobile internet service.

- Formal partnerships and joint developments with mobile operators
Google® will replace the white-label search engine in Vodafone’s Live! content portal. The service will return search hits on Live! first, followed by sponsored links, followed by other hits. Vodafone will take a share of the revenue generated by users clicking on sponsored links.

3.4 Mobile Operator Advantages

Mobile operators deliver not only a significant volume of subscribers but also the potential to create and define communities. Mobile phones are intimately associated with their owners, giving rise to personalization services such as ringtones (that deliver significant revenues) as well as location-based services and applications. The addition of identity management to these capabilities creates a powerful combination.

Mobile operators can provide value-added services and QoS functionality to service providers in many ways. Authentication of mobile users delivers security and fraud prevention services, particularly with SIM-based systems that can provide strong authentication. Sharing data can support targeted advertising services using identity management techniques to ensure privacy.

Mobile community services are an increasing focus of attention for many mobile network operators [Jupiter Research, 2006]. They promise near term revenue potential from increased usage of data services with longer term potential arising from advertising-based models. Marketing campaigns or services linked with social networking sites such as MySpace are attempting to shift familiar online experiences onto mobile phones, enhanced with location, messaging, personalization and presence capabilities.

3.5 E-Government

E-government initiatives in areas such as health, social welfare, transport and logistics, regional safety and community training are an important market segment and driver for identity management services in many countries.

In Europe, for example, the 25 European Commission (EC) member states and nine accession countries have all signed up to a new inclusion plan that could make accessibility in e-procurement mandatory. They have committed to an 'Internet for all' action plan, designed to ensure the most Web-disadvantaged groups can get online.

An online public consultation on the EC’s future e-government policy towards 2010 identified the main barriers to citizen involvement and participation [European Commission, 2006]. Top of the list were: lack of trust and security, insufficient access to information and communication technologies for citizens and businesses, and lack of leadership.
The consultation recommended that the European e-government policy should focus on electronic identification and authentication, good practices and solutions sharing and organizational change as key enablers. The main barriers in realizing electronic identification and authentication for public services across borders were seen to be the lack of interoperability, national legislation and lack of awareness of benefits. The top three required actions identified by the consultation exercise are: mutual recognition of electronic identities provided by Member States, a federated, multilevel e-identity model, and a framework for interoperable electronic documents.

Major government projects involving digital identities are currently in progress in many countries. These include the introduction or enhancement of identity card schemes and the coordination of medical records. Identity management solutions incorporating a federated approach that deliver security and privacy would seem to be an essential component of these projects. In these cases a key target market for identity management solution providers will be the large systems integrators who implement the projects under contract to national or regional governments.

3.6 Market Size

Many changes are underway which will have an impact on service revenues in the telecommunications market. Due to the scope and scale of the changes underway, it is impossible to predict future revenues with any certainty. Instead, we explore the likely scale of change as non-traditional competition accelerates due to convergence.

Figure 3.4 shows a trending of current telecommunications service revenues using simple growth models based upon growing usage and a growing subscriber base. This view of growth has been used for decades to predict future revenues in this market.

We recognize that the traditional names that categorize revenues have become less relevant as convergence has accelerated. Fixed line and Mobile transmission revenue can be driven by both voice and data. Internet revenue can be the result of transmission revenue or the use of advertising on ISP portals. Figure 3.4 depicts the future growth of this market based on historic trends (“classical” view).
The $1.5 trillion market for 2006 is not in question. The projection of this market to $2.5 trillion in the next eight years is. This growth is dependent on key technology enablers such as identity management.

### 3.7 Changing Structure

Many new, non-traditional telecommunications service providers are emerging. In many cases they not only do not view themselves in this service provider role, but they do not seek revenues from traditional services. Indeed, in many cases, transport of data is viewed as a service enabler not a billable service in its own right.

Figure 3.5 gives an indication of the scale of the potential revenue loss to network service providers in this changing environment. This revenue at risk was determined by identifying broadband subscribers most likely to have relationships with Webcos. The revenue at risk was calculated by assuming that these subscribers would abandon telcos for all services, including nomadic wireless access and voice. In addition, without robust solutions for identity management and other advanced platforms to deliver new data services, a significant portion of new data service revenue will also be lost.
As shown in this figure, this revenue loss will increase as Webcos add voice services to their portfolio of services supported by advertising revenues. Revenue at risk was calculated by assuming voice revenues are significantly reduced once any broadband services are widely available whether they are delivered with 4th generation mobile or a fixed broadband infrastructure. Worldwide ARPU per service type were then used to calculate total revenue at risk.

Source: Telecompetition Group, December 2006
4 The Identity Management Market

Three phases can be recognized for the identity management (IDM) market in the public network environment. The phases are distinguished by the degree of cooperation between network providers from the telecom world and content providers from the internet world. We label these phases Independent, Connected and Combined. They correspond roughly to the past, present and future (Figure 4.1).

*Figure 4.1 Three Phases of Identity Management*

4.1.1 The Independent Phase

In the past, network operators in the telecom world and content providers in the internet world acted independently in their dealings with end users. Telecom network providers were concerned primarily with connectivity services delivered securely and reliably with high quality of service. In contrast, content providers delivering information and entertainment data services over the best effort internet environment suffered from the inherent security, reliability and privacy issues.

*Source: Telecompetition Group, July 2006*
Identity management was not a priority for network operators in this independent phase. Telecom network providers already operated in a secure and trusted environment with well developed and sophisticated authentication procedures. End users expected to have control over their identities as part of their basic service. End users assumed additional identity management functionality such as single sign-on would be provided wherever appropriate – but they did not expect additional charges.

Content providers in the independent phase on the other hand certainly required identity management to handle security, privacy and fraud issues. But these requirements were generally met by enterprise solutions within the content providers’ own organizations; they did not demand solutions specific to the public network environment.

Although both network operators and content providers have the potential to act as identity providers for end users such approaches have experienced limited commercial success. End users take the benefits for granted; their willingness to pay is close to zero. Identity management specifications and protocols offer the capability to create service packages tailored to specific communities and interests defined by subscriber profiles or elected choices. Network operators have evidenced little appetite for such wholesale ventures. There are few “frequent flyer programs” available to telecom subscribers.

### 4.1.2 The Connected Phase

Two separate convergence processes are currently in progress. Consolidation is occurring between network operators in the telecom world to produce converged operators capable of delivering triple and quadruple play services. This consolidation creates a demand for interoperability between multiple back-end systems and processes – a demand that can be satisfied by federated identity management solutions [Pichelin, 2006]. A similar consolidation process can be seen among content providers in the internet world.

But the second convergence process is potentially more significant for identity management. As discussed in Appendix B, commercial connections between network operators in the telecom world and content providers in the internet world are being forged to mutual advantage. Identity management techniques can support enhancement of these links well beyond the previous wholesale level relationships, providing significant added value to the market place. New service offerings that are emerging as a result of these commercial connections include:

---

5 A more appropriate term would perhaps be “identity protector”.

January 2007
• Many end users have expressed willingness to receive targeted advertising in exchange for discounts on telecom services. Content providers value a targeted audience highly; targeted advertisement prospects are worth an order of magnitude more than untargeted prospects. Network operators can share selected data and user profiles with content providers to improve targeting of advertisements.

• Mobile terminal devices are intimately associated with their owners. Knowledge of the geographical position of the device together with the communication status of the device owner therefore allows the creation of truly personalized services. Mobile network operators can utilize their access to location and presence information to create identity enabled services for content providers.

• Content providers can offer targeted services to end user communities within the network operator’s customer base. Branded services tailored to specific communities of interest increase traffic and reduce churn for the network operator.

• Network operators have the ability to authenticate end users, increasing their advertising worth and reducing fraud for content providers. Mobile network operators with SIM based systems can provide strong authentication without log-in. A web service on a mobile terminal that authenticates transactions would reduce fraud and card-processing costs for content providers to the equivalent of in-person transactions – a very significant potential market opportunity.

Identity management solutions for these services need to provide a trusted environment in which information can be shared in a secure fashion, respecting privacy considerations and protecting against fraud.

This current connected phase is essentially about existing players working together on a revenue sharing basis to grow the market. Some new business models and approaches are being tried as the focus moves from voice to data services. Many network operators have adopted a walled garden approach\(^6\) but with limited success. In general, the business models of the existing players have not changed substantially – they remain remarkably similar to their legacy versions.

Increasingly though, traditional approaches are being overturned by the land grab for customer loyalty. The growing emphasis on the importance of customer relationships and “stickiness” as a key differentiator recognizes the pivotal role of trust. Social and cultural perspectives are changing as awareness of the dangers of the internet environment increases. These new perspectives are driving recognition of the crucial importance of identity.

---

\(^6\) Here “walled garden” refers to a closed portal where users cannot readily access information generally available on the www. This approach is often used in cellular networks where bandwidth constraints require significant packaging of content.
### 4.1.3 The Combined Phase

The advent of ubiquitous broadband availability is a primary driver behind the success of the "internet business models" of companies such as Amazon, AOL, eBay, Google® and Yahoo. These companies are now entering the “second derivative” stage of their existence in which they may partner either with each other or with companies such as telecom network operators [Randall, 2006]. Such partnerships will deliver the next generation of services, exemplified by Web 2.0 activities such as blogs, RSS, digital media, online advertising, vodcast, and consumer generated media.

Such a future could result in services such as telephony and television riding “free” over IP and so threaten the existence of conventional telecom network operators. Eventually the Webcos would have to take over the responsibility for the network infrastructure.

An alternative future is one where network providers become a recognized and valued part of the new value chain rather than just utility operators. This requires new business models involving a true payment methodology for QoS that reflects value.

Such business models will require content and context aware networks combined with intelligent content distribution. The environment will be one where content value adds to connection value, rather than replacing it.

From a telco perspective, business models in this combined phase unite the complementary approaches represented by the network-centric “core-heads” and the device-centric “edge-heads”. Both admit that intelligence is required both within and at the edges of the network. Neither of the extreme scenarios of all intelligence located in the core network or all intelligence located in edge devices will provide the functionality required for services that deliver both real time connectivity and non-real time content.

The complementary identity management approaches of federation and user centricity are in many ways analogous to the complementary network centric and device centric approaches in the telco and internet worlds. A combined approach to identity management will also be required in the combined phase.

In this scenario the issue is not who owns and moves the bits, but the command and control of moving the bits. How will end users know they received the right data from the right person, or that the data or the sender or the receiver can be trusted? An organization – often referred to as a trusted third party – is required to provide security, to protect the data while respecting privacy. In some regions of the world the involvement of a trusted third party may well be the only
acceptable way to protect privacy and prevent fraud.\footnote{This raises the question of who watches the third party. A neutral organization can be envisaged that provides a digital identity bank operating under restricted and clearly specified access policies.} Trusted third parties will have to operate both within national regulatory regimes and across international boundaries – conditions familiar to telecom network operators today who are certainly candidates to fill the trusted third party role. The role of the combined network operator in the future may not be as a seller of bandwidth but as a service enabler, a provider of quality of service and a trusted third party.

An important element within the combined phase will be next generation networks, envisaged to be in place by 2015. The architectures adopted and the functional characteristics demanded from these networks will be an important element in determining the nature and size of the future identity management market.

A group of the world’s largest mobile network operators is now articulating their requirements for the decade beyond 2010 [Akhavan et al, 2006]. Their vision involves a next generation mobile network based around a packet-switched core together with a new radio access technology. One of the key drivers for such a next generation mobile network is specified by the group as “Trust Based Services” which are specified as services delivering security, safety and dependability. Trust based services require the network to support high levels of authentication and systems that enable effective and cost-efficient fraud protection in devices and network infrastructure.
5 Future Scenarios

In this section, four distinct views of the future as it relates to identity management are explored. Detailed information about the methodology used to develop the four scenarios, key drivers and uncertainties can be found in Appendix B.

Critical uncertainties have been mapped onto the end user and industry domains as indicated in Figure 5.1. They could equally be mapped against other domains – there is no “correct” choice. But the domains selected do encompass all the critical uncertainties and suggest two orthogonal axes of uncertainty:

- Dominant end user activity
- Changes in institutional structures and industry ecosystem

These two orthogonal axes define four quadrants of uncertainty each containing a distinct and plausible future scenario. The resulting matrix (Figure 7.3) maps end user values and concerns against the characteristics of the institutions and organizations with which end users interact and is a logical framework in which to explore identity management issues.

![Figure 5.1 The Identity Scenario Planning Matrix](source)

The horizontal axis in the scenario planning matrix covers the range of end user activities. At the left hand end the dominant end user activities are social and end
user attitudes are driven by their needs and concerns as individuals or members of social groupings and will encompass a multitude of different identities, some of which may be deliberately anonymous. At the right hand end of this axis the dominant end user activities are driven by business contexts where commercial transactions are conducted, requiring varying degrees of authentication and disclosure of end user identities. End users will occupy different positions on this axis at different times, depending on the nature of their activity at that time. This axis of uncertainty reflects the fact that end user attitudes and activities vary with time and situation but the environment is largely shaped by the dominant end user activity.

The vertical axis in the scenario planning matrix represents the organizational structure of the ecosystem with which end users interact to obtain a wide variety of communications related services. At the top of this axis the institutions forming that ecosystem are well defined in terms of both their specific roles and their inter-relationships. This represents a structured and somewhat inflexible environment in which relatively few organizations coexist within a precisely specified hierarchy. In contrast, the bottom of the axis describes a flexible and constantly changing environment in which a multitude of players both compete and cooperate at a variety of levels.

The matrix in Figure 5.1 delineates four distinct scenarios that are plausible in the year 2015. In each quadrant, different drivers determine the dominant end user activity and the structure of the industry ecosystem. The resulting scenarios describe four very different outcomes.

The scenarios focus on factors germane to identity management services but they do not describe specific identity management futures. They describe the environments which identity management solutions will likely have to face. The value of the scenarios is as a test bed for the validation of identity management systems and solutions.

The scenarios are not predictions. They do not prescribe the most likely outcomes. Rather they outline the boundaries of what could become possible in 2015. They are intended to be plausible scenarios, encompassing the extremes of possible situations. The reality will be some combination of these scenarios.

### 5.1.1 Scenario I – Day in the Park

In Scenario I in the top left quadrant of the identity scenario planning matrix end users are pursuing social and community activities in a well ordered but economically constrained environment. The internet has evolved into a relatively safe medium free of spam and viruses and enables service providers to offer a rich portfolio of voice, text, image and video communication functionality based on peer-to-peer software and primarily carrying user-generated content. The web has evolved from a primarily one-to-many to a many-to-many medium. Services
are funded by advertising or supported by government agencies and are generally free to the end user.

Instant messaging type services encompassing multimedia functionality have become a favored communications mechanism within many communities, particularly among young people. Interoperability between the various IM systems has become widespread and IM is well on the way to join voice and email as the third truly universal communications medium.

Most network operators run converged mobile and fixed broadband access networks in a licensed but lightly regulated environment. Most services are best effort and quality of service is sometimes low, depending on network loading. Investment for network upgrades is scarce and most operators are dependent on government support through municipal service contracts or national e-government projects in areas such as health.

Many governments have embraced the social benefits of e-government and offer compelling information and services to their citizens. This general acceptance of the positive aspects of identity management helps to foster a strong social networking community and an advertising-based e-commerce environment where goods and services tend to be free or low cost. Citizens feel relatively comfortable that their identities and privacy are protected and exchange of identities is often limited to those entities where the individual determines they feel a level of trust or control over release of their identity. Peer-to-peer transactions thrive. People choose trusted relationships and the need for the selection of a single identity provider is limited. An entrepreneurial spirit pervades the entire society and many people are self-employed.

5.1.2 Scenario II – Safety at a Price

In Scenario II in the top right quadrant of the identity scenario planning matrix a small number of major players lead the industry in a highly regulated, stable but rather staid sector in which e-commerce thrives. Consolidation through mergers and acquisitions in the operator and manufacturing communities has resulted in a few large organizations that dominate the sector. Alternative carriers have not achieved significant market share and most have perished. Surviving smaller players have formed partner alliances to achieve competitive economies of scale. Most service providers offer converged services across multiple access technologies and aggregate material from a wide range of content providers.

Massive investment in e-government has supported the development of secure and trusted communication systems and applications built from web services. Such developments have been accompanied by ubiquitous broadband availability, often state subsidized, and government led initiatives on education leading to high levels of computer literacy. Citizens are encouraged to use e-services which increases end user awareness and acceptance of e-commerce. Regional bodies such as the EU and global organizations such as the WTO have
been successful in encouraging harmonized standards and data protection legislation for e-government and e-commerce applications. Regional cooperation amongst governments is driven by economic as well as political factors such as concerns about terrorism. These factors have stimulated markets with significant size and potential but have also, to some degree, tended to stifle innovation.

The dominance of the major players results in a highly regulated sector. The widespread deployment of e-government obligates the introduction of consumer protection measures through regulatory mechanisms. Regulatory burdens are further increased by an emphasis on corporate governance legislation, but the consequent compliance and audit requirements generate identity management awareness and encourage the adoption of high level security solutions.

Many governments adopt a standardized approach to identity management and mandate that specific interactions with the government are conducted electronically. The government acts as an identity provider and also certifies a small number of identity providers that everyone uses. E-commerce thrives as consumers are willing to pay fair prices for a variety of goods and services. Citizens are generally comfortable that their identities are protected and therefore willing to cede certain aspects of their privacy for the common good.

At a regional level there is increasing adoption of international norms for identity disclosure and common licensing regimes for identity providers. Severe penalties are imposed for non-compliance with licensing and certification criteria and conditions.

### 5.1.3 Scenario III – Anything Goes

In Scenario III in the bottom left quadrant of the identity scenario planning matrix individuals and communities take advantage of a wide variety of web-based communication services in a dynamic but insecure environment. Traditional telcos have lost their legacy revenue from voice services as a high proportion of end users have switched to ‘free’ IP-based services delivered over cheap, ubiquitous broadband access. Neither multimedia services nor advertising based business models have produced alternative revenue sources capable of generating the return on investment necessary to justify further telco network expansion. Triple and quadruple play convergence strategies have failed to stem revenue loss but have instead accelerated the commoditization of all media services.

The gulf between the Internet and telco philosophies is as deep as ever and net neutrality quarrels remain unresolved. Lack of cooperation between the two communities means that quality of service cannot be guaranteed for Web-based services. Bandwidth constraints in access and core transport networks regularly cause service failures. Networks are constantly clogged with spam and end users continue to be plagued by viruses, spyware and identity theft attacks. Unreliability of networks and services and the industry’s failure to address
security, privacy and trust issues have caused the abandonment of most e-government initiatives.

The sector is fragmented and unsettled but it does engender a constant stream of entrepreneurial new entrants, most with limited service capabilities and many with a short lifespan. The large number of players at any given time allows the authorities to regulate with a light touch, relying on market forces to ensure competition.

There is a general lack of cooperation and some governments impose more rigid law enforcement, wiretapping and other mechanisms to control citizens. Other governments use existing civil and criminal laws to manage the environment, with difficulty in prosecution for violations that occur from outside their jurisdictions.

Although the environment is not suitable for either e-government or e-commerce, individuals have an endless array of opportunities for commerce and interaction which are all “buyer beware”. Consumer information on supplier integrity is difficult to obtain so buying is limited to brand names. Entrepreneurs find it difficult to gain customers and even large companies confine their value chain interactions to a small, static number of partners. Legitimate suppliers are constantly seeking massive amounts of information about their customers in order to “secure” their relationship and create side businesses out of selling the information to other suppliers.

Certain elements of social networking, on the other hand, particularly those based on anonymity or personas, thrive in this environment. End users may suffer from unpredictable service quality levels but they have multiple ways in which to communicate. Interacting with people is driven by groupings of known friends (buddy lists) or by self declared personas. Self declared personas allow individuals to participate anonymously in a wide variety of activities without concern for repercussions.

Consumers give little thought to identity management and tend to casually give out their identities to just about anyone who asks. At the same time, a certain level of fear permeates society because of widespread media coverage of identity theft or other misuse of identity. Fraudulent actions are facilitated by the lack of verified knowledge about either the individual or the buyer. Identity theft is relatively simple, and techniques such as phishing and pharming make easy prey of unwary individuals.

5.1.4 Scenario IV – Vibrant Diversity

In Scenario IV in the bottom right quadrant of the identity scenario planning matrix a multitude of players exist within a standards based, lightly regulated but highly fragmented and competitive environment. Most players are specialist in nature and regional in coverage, deploying technologies optimized to deliver the
highest performance for the specific services on offer and tailoring their solutions to best meet local requirements. End users pick and mix applications from specialist service providers to create a personal portfolio well matched to their requirements.

Network operators and service providers come from a wide variety of backgrounds in both the internet and telecom worlds. Convergence has occurred across access networks as well as across services, spurred by the genuine – as opposed to long-promised – intelligent network separation of services from access. The high number of players competing in each market segment allows a light regulatory regime to be imposed, relying on market forces to control prices and competition.

Many countries have encouraged e-government services by supporting local and regional specialized service providers. Protectionist measures have also been deployed to boost e-commerce by favoring solutions tailored tightly to local conditions. Global organizations such as the WTO have long been dismantled, falling victim to the isolationist policies of some major developed nations. National solutions have been funded in many countries driven by fears of US hegemony. Local language implementations receive preferential consideration. Parallel versions of the Internet are being developed in some countries to cater to local conditions and to break away from western dominance.

Specialized service providers within a territory specifically address the security, privacy and trust problems by building tailored solutions, mostly proprietary but some based on open standards. Interoperability between solutions is rarely standardized but frequently offered through preferred partnership alliances.

This hybrid future is dominated by trusted network operators and service providers who do not hold or provide identity, but who act as a trusted protector and aggregator of a minimum number of identity attributes applicable to the task at hand. Network service providers transparently outsource this function to a neutral trusted 3rd party. End users have flexible control and management of their identities and often opt to pay their network service provider a small monthly fee to provide value added identity management services such as a monthly download of all recent transactions. This gives the user a level of comfort and control and drives premium pricing for a range of data services. Here government has been an early adopter of e-government services that require some level of standardized identity management.

Significant volumes of personal profiling and identify information are available in society and consumers generally have control over the information released in an individual transaction. End users do have the ability to be their own identity provider for non-financial transactions. A small number of companies tend to dominate specific aspects of society because a federated approach to web services doesn’t exist. While e-commerce thrives and customers have some
willingness to pay for goods and services, they only do this with a small number of players who in turn build value chains that they tightly control.
6 Scenario Analysis

The scenarios presented in Section 5 describe plausible environments in which Identity Management and Web Services may operate over public networks in the future. These scenarios are entitled:

- A Day in the Park
- Safety at a Price
- Anything Goes
- Vibrant Diversity

The scenarios are based on the Identity Scenario Planning Matrix (Figure 5.1). In this matrix the horizontal axis is concerned with end user activity whilst the vertical axis, institutional structure, represents the organizational characteristics of the ecosystem with which end users interact to obtain a wide variety of communications related services. The scenarios focus on factors germane to identity management services but they do not describe specific identity management futures. They describe the environments which identity management solutions will likely have to face.

In this study a number of steps were taken to validate the scenarios. These included discussions with a range of industry leaders representing various camps and geographies to test plausibility. In addition the key drivers within each scenario were endorsed through comparisons with other published works in this area.

Beyond this validation, this section explores the implications of those scenarios for specific aspects of identity management. Specifically, the following can be found starting in Section 6:

- The key participants in the value chain for each scenario
- Factors impacting telco revenue growth
- Network operator (telco) worldwide revenue forecast by scenario
- Differences that may impact regional revenues

By way of review, Figure 6.1 summarizes some specific characteristics of these scenarios from an identity management perspective.
6.1 Scenario Validation

In addition to using an independently validated approach to creating the scenarios, an interviewing process was following where recognized industry leaders\(^8\) from a range of backgrounds reviewed the scenarios and provided input as to the value and credibility of the scenario assumptions, drivers and uncertainties.

The four extreme scenarios presented in this report would produce very different levels of demand for different types of identity management services in the public environment. A specific identity management service may not be viable in one scenario if there is little perceived need for the solutions it can offer. In another scenario, however, the same service may successfully address key concerns and needs particular to that environment.

\(^8\) Interviewees are listed in Section 16.
6.2 The Liberty Alliance Approach

The Liberty Alliance combines specifications and protocols with policy guidelines to produce solutions. Liberty Alliance conformance and certification programs guarantee interoperability to create a global ecosystem of identity solutions that (Figure 6.2):

- Solution Deliverables – attributes of Liberty Alliance specifications and protocols that solve specific problems or deliver value
- Solution Characteristics – attributes that make Liberty Alliance specifications and protocols reliable, robust and flexible
- Liberty Alliance Characteristics – attributes that make the Liberty Alliance a credible source of solutions

**Figure 6.2 Synopsis of the Liberty Alliance Approach**

<table>
<thead>
<tr>
<th>Solution Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundancy of Information Sources</td>
</tr>
<tr>
<td>No Single Point of Control</td>
</tr>
<tr>
<td>Minimal Disclosure</td>
</tr>
<tr>
<td>Federated Social Networking, Circle of Trust &amp; SSO</td>
</tr>
<tr>
<td>Mutual Authentication</td>
</tr>
<tr>
<td>Security and Privacy Protection</td>
</tr>
<tr>
<td>Robust Services Framework, Strong Authentication Potential</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Capability, Device Independence, End-to-End solution</td>
</tr>
<tr>
<td>Trusted, Flexible, Business Relationships including Roaming</td>
</tr>
<tr>
<td>Flexible, Adjustable Format Allows Many Business Models</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Liberty Alliance Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strength and Breadth of Product Portfolio</td>
</tr>
<tr>
<td>Interoperability Checks including Conformance Testing</td>
</tr>
<tr>
<td>Open, Diverse, Large Global Industry Forum ecosystem</td>
</tr>
<tr>
<td>Open Standards, Market Driven Use Cases and Consensus</td>
</tr>
<tr>
<td>Regulation Conscious, Holistic International Perspective</td>
</tr>
</tbody>
</table>

*Source: Liberty Alliance and Telecompetition Group, August 2006*

This approach is used in the following section to consider deliverables and characteristics in terms of the demand under each scenario.
6.3 Demand for Digital Identity

Value chains vary by scenario. The participant that has the direct relationship with the end users including as an identity provider has greater control over the revenue sharing among the value chain. In Scenario I, revenues are shared among a small number of value chain players (Figure 6.3).

**Figure 6.3 Scenario I, Value Chain Participants.**

Government initiatives prompt a growth in broadband. Webcos and content providers share the bulk of the enhanced service revenue using an advertising-based business model. The implications for the telcos in this environment are of concern.

In Scenario II, revenues are shared among a small number of value chain players. In this case the telcos are in a stronger position with the end users (Figure 6.4).

**Figure 6.4 Scenario II, Value Chain Participants.**

Broadband penetration increases rapidly due to e-government initiatives and enhanced service revenues grow. Both trends result in a higher telco ARPU.
In Scenario III, traffic increases dramatically without a commensurate increase in revenues. ARPU drops due to predominance of free VoIP services. Advertising based business models dominate (Figure 6.5).

**Figure 6.5 Scénario III, Value Chain Participants.**

![Scenario III Anything Goes
Dominant Participants in the Value Chain](image)

*Source: Telecompetition Group, July 2006*

In Scenario IV, there are many participants in the value chain. Competition is high and the content provider community is diverse and healthy. No large Webcos dominate the environment (Figure 6.6).

**Figure 6.6 Scenario IV, Value Chain Participants.**

![Scenario IV Vibrant Diversity
Dominant Participants in the Value Chain](image)

*Source: Telecompetition Group, July 2006*

This is a vibrant environment with a multiplicity of service providers. This is a favorable environment for a network operator that embraces identity management and has built a trusted market position.
6.4 Factors Impacting Telco Revenue Growth

The business and financial aspects of identity management were analyzed from a public network operator perspective. A number of challenges are immediately apparent in this type of analysis. Firstly, identity management is a technology enabler and for the most part expected by consumer and business end users. Secondly, even though telcos have a more secure base than the public Internet, they have done little to build confidence in their ability to manage and protect identity; and finally, because there is little end user awareness of the protective role an IDP can play.

Given these constraints, this analysis considered four basic attributes of the network service provider revenue: ARPU, penetration rate, subscriptions and subscriber growth rates and the basic value chain in each scenario.

For each scenario the environment is assessed in light of the impact it would have on factors that affect a telco revenue stream such as pricing and competition. Figure 6.7 shows a summary of these factors. This environment was used to trend the forecasted revenues over the forecast horizon of 2006 to 2015.
**Figure 6.7 Factors that Impact Revenue Growth**

<table>
<thead>
<tr>
<th>Telco Environment</th>
<th>I Day in the Park</th>
<th>II Safety at A Price</th>
<th>III Anything Goes</th>
<th>IV Vibrant Diversity</th>
</tr>
</thead>
<tbody>
<tr>
<td>End user service pricing expectations</td>
<td>Free</td>
<td>High</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>Regulatory regime for communications sector</td>
<td>Light</td>
<td>Strong</td>
<td>Moderate</td>
<td>Light</td>
</tr>
<tr>
<td>Competition from other network operators</td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Competition from Webcos (other SPs)</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Number of Active Content Providers</td>
<td>Huge</td>
<td>Small</td>
<td>Large</td>
<td>Medium</td>
</tr>
</tbody>
</table>

*Source: Telecompetition Group, July 2006*

A use of surrogates to assist in the analysis of future uncertainties represents a defensible approach to study markets. In the case of digital identity management and its impact on network service provider revenues, two different surrogates were considered. Public network messaging including both short message services (SMS) used in mobile networks and instant messaging (IM) used in fixed networks were studied. I-mode, the NTT DoCoMo mobile content service was also studied. Messaging was chosen because interoperability has been a necessary condition for widespread adoption. Adoption rates for both SMS and IM in different regions are reasonable surrogates for adoption of federated identity dependent services. I-mode as a proprietary “federated” information service with network service provider and content provider revenue sharing was also studied to better understand deployment and adoption issues associated with identity.

The value chain participants’ role in relationship to the end user was analyzed to determine worldwide average ARPU for the telcos in each scenario. The strength of the telco in the value chain was used to modify ARPU for each scenario. This ARPU was then combined with an assumed penetration rate to estimate overall
revenues. These sections are then followed by a comparison of revenues for all the scenarios.

6.5 Worldwide Network Operator Revenues

Given the demand assessment and environmental factors in Figure 6.8 a high level analysis bounding worldwide network operator revenues was created.

The top bounding is based on the classical telecommunications & service revenues, the baseline (or bottom bounding) assumes the traditional telecommunications providers, en mass, elect to provide no form of Identity Management.

Furthermore, the baseline reflects that the at-risk revenue shown in Figure 3.5 is indeed significantly lost in 2015 without identity management capability. This is based upon the user impact of a high take rate of identity management capable broadband based services, opening the door for large revenue losses from traditional voice services – both fixed and mobile, when contrasted with similar offerings without identity management.

---

9 See Appendix D – Regional Difference for a discussion of variations
10 See Appendix B – Demand for Digital Identity Capabilities for an additional approach
Figure 6.9 compares the forecasted baseline with the four scenarios. The impact of not offering any form of identity management capability, though quite unlikely, has a significant impact as customers choose to move to providers who “have it all”. The gap between the baseline (no form of identity management for any traditional telecom) and the scenario revenue can be as high as a trillion US dollars in the year 2015.

Source: Telecompetition Group, July 2006

In Scenario I, an advertising based pricing model where users perceive services as free and demand is relatively low is the least favorable environment for the telcos. Here the telcos are most advantaged with business customers, but even that opportunity is offset by the light regulatory environment and relative strength of the Webcos.

In Scenarios II, III and IV telco revenues do a bit better but for different reasons. In Scenario II the strong regulatory environment and greater user willingness to pay directly for services favor the telco. In Scenario III the Webcos and content provider strengths challenge the telcos. These players dominate the marketplace. Finally, Scenario IV is somewhat positive for telcos just because it is a positive environment for all players and the telcos still have the opportunity to maintain a direct billing relationship with the end user.
Scenario II is an environment where a telco that deploys identity capabilities late may still achieve some revenue growth due to the strong regulatory environment combined with the lack of large aggressive Webcos.

A key message implicit in the results is that for telcos to thrive, with revenues shown here, they will need to implement some strategy to manage identity. Another way to review these results is to consider the cumulative revenue impacts in all four scenarios when compared against a future where a network operator chooses not to invest in key technology enablers such as identity management. Figure 6.10 shows these relationships.

*Figure 6.10 Potential Variations in Cumulative Network Operator Revenue*

![Graph showing potential variations in cumulative network operator revenue.](image)

*Source: Telecompetition Group, December 2006*
7 Conclusions

The world of telecommunications has indeed changed. A closed and comfortable competitive marketplace is rapidly being replaced with an amorphous and fluid market introducing many non-traditional players. With respect to identity management as a key technology enabler for the future, a wait and see posture as a technology follower is the riskiest approach a traditional telecom carrier – whether fixed, mobile or combined, can take. A brief window of opportunity exists where the higher quality, more stable and trusted environment of telecom – especially mobile – can be successfully leveraged to retain customers. This initial defensive posture will over time lead to the opportunity to increase revenue through enhanced identity dependent applications and services.

It will take time to develop all the aspects of identity management needed succeed in the marketplace. This includes building an identity infrastructure, strengthening customer positive perceptions of network operators’ trustworthiness, building compelling federations and user-centric approaches for service delivery, and gaining proficiency in seamless delivery of complex services. This will take time – years in fact – and there is no time to waste.
8 Additional Conclusions for Liberty Alliance Members

Moving from today’s connected phase of converged networks and services towards the future combined phase embracing next generation networks will require a further evolution of identity management solutions. The next generation will erode the distinction between public and private networks.

Just as the complementary network centric and device centric approaches of the telco and internet worlds are combining in the definition of next generation networks, there will be a need to combine the complementary federated and user centric approaches to identity to create next generation identity management solutions. The Liberty Alliance should reach internal consensus on definitions and approaches to address the “long tail” that the user-centric community believes is missing from the Liberty Alliance protocols.

The Liberty Alliance has established itself as a supporter of open dialog and made significant progress hosting open discussion with the various camps within identity space. As with most human endeavors, much of the tension between different camps is due to lack of a common language. Continued face to face meetings in a non-confrontational format will help. This work should be enhanced and accelerated.
9 Appendix A – Industry Evolution

The industry that has now emerged bears only a superficial resemblance to that which had been in place, little changed, for the last two decades of the last century.

The communications and IT sectors continue to experience a period of significant transition. Whether that transition will be complete by 2015 – nine years from now, the time period covered in this report – is difficult if not impossible to predict.

For almost the entire history of the communication access technologies, IT and broadcast services and have been separate and siloed (Figure 9.1). Voice was provided over fixed or mobile networks, each subject to distinct regulatory requirements. Data was carried over separate data networks and internet access provided by internet service providers (ISPs), again with their own discrete regulatory regimes. Video services were delivered by broadcasters, with different sets of regulations applying to cable, satellite and terrestrial TV networks.

![Figure 9.1 Communication Industry Silos](image)

Source: Telecompetition Group, June 2006
Some regulators are seizing the opportunity to lighten regulatory regimes, relying on market forces to engender competition. They are deliberately breaking down the silos by introducing technology and service neutrality into regulatory regimes and by combining previously distinct regulatory bodies for communications and broadcasting into a single organization. The potential for disruption is massive. Fundamental changes to industry structures are already becoming apparent as everyone focuses on triple and quadruple play offerings as a mechanism to consolidate their existing subscriber base and to poach subscribers from their competitors (Figure 9.2).

**Figure 9.2** **Triple Play**

![Triple Play Diagram](image)

*Source: Telecompetition Group, June 2006*

Advances in technology have changed all this. The introduction of IP networks has transformed service provision, lowering the barriers to entry for new service providers and introducing new service paradigms. VoIP is no longer dismissed as a second rate service for geeks. Voice services are now being delivered commercially over the internet. Cable broadcasters are offering telephony. Television programs are being accessed over fixed and mobile telecom networks. There is no longer a one-to-one relationship between services and access technologies.
Services developed outside the traditional telecoms domain are driving fundamental changes within the industry. Presence and instant messaging are shaping the way communications services will be delivered in the future.

These developments are not simply perturbations on a theme. They are representatives of an alternative approach to communications that treats the network as a shared common resource – an approach that has been termed viral networking (Figure 9.3). An important fundamental difference in approach is that traditional telcos place intelligence at the core of the network whereas viral networking places intelligence at the edge. The previous battle between bellheads and netheads has morphed into one between coreheads and edgeheads!

Source: Telecompetition Group, June 2006

Communities play a central role within the viral networks approach. Social networking and communities are at the heart of many of the web-based companies that have achieved significant and rapid success during the past few years. These companies are based around social software applications and regard voice and video services simply as software add-ons (Figure 9.4).
But not all is sweetness and light. The current internet is a seriously unsafe environment swarming with spam, viruses and spyware, and supporting fraudulent activities through developments such as phishing and pharming. Despite these dangers, the Internet has spawned new communications phenomena such as instant messaging, blogging, social networking websites, Wikis and peer-to-peer and swarming software that is driving entirely new traffic patterns. Peer-to-peer traffic from a small number of subscribers currently dominates the internet backbone.

Figure 9.4 Voice as a Software Application

Source: Telecompetition Group, June 2006

Companies such as Google and eBay have been characterized as forms of content distribution networks and some observers claim they should be seen as potential competitors to the traditional telcos. Such portal companies, let’s call them the Webcos, could offer communications applications as part of a wider service portfolio and attract subscribers away from the traditional network operators (Figure 9.5). The widespread availability of broadband access is a major trigger opening up the industry value chain to new players.
Such an approach could represent a major challenge to the conventional industry structure in which network providers play a central role enabling communications between end users and content/service providers. This structure, illustrated in Figure 9.6, is still evolving and the relationship between network operators, content providers and service providers remains an uneasy one. Continuing debates and uncertainties surround the positioning of Mobile Virtual Network Operators (MVNOs) and the applicability of walled garden\(^\text{11}\) approaches. Revenue sharing and exclusivity are major areas of contention; the i-mode\(^\text{12}\) model is a rare example of success within the conventional industry structure.

\(^{11}\) Here “walled garden” refers to a closed portal where users cannot readily access information generally available on the www. This approach is often used in cellular networks where bandwidth constraints require significant packaging of content.

\(^{12}\) I-mode is a highly successful service offering of NTT DoCoMo where many content providers partner with DoCoMo in a revenue sharing arrangement.
Numerous flavors of convergence are now adding new dimensions to the industry structure and are creating new value chains. Convergence across access networks, enabled by developments such as the IP Multimedia Subsystem (IMS), opens up new service possibilities spanning the traditional telecom and internet worlds.13

But attitudes towards converged services still reflect an organization’s or observer’s origins – a phenomenon nicely illustrated by the current net neutrality controversy. Whether the two camps will converge or diverge is a major uncertainty affecting the future of the communications industry.

What is not uncertain is that traffic patterns have already changed substantially and irreversibly, highlighting both the impact of new business models and the necessity to evolve those business models in the future (Figure 9.7).

---

13 IMS uses VoIP and other standard technologies to enable telecommunications operators to provide all the services, including multimedia, that the internet does while allowing for control of, and charging for each service.
Traditional transaction-based business models in the telecom world are under threat from participatory (or collaborative) business models emerging from web-based communities in the internet world. The two worlds have very different characteristics. The telecom world delivers quality of service (QoS, a mandatory requirement for real time services) and customer support and is funded mainly by a transaction charging business model. The Internet world is best effort (a workable solution for non-real time services), self service and free to the customer, funded through participatory business models increasingly supported by advertising revenues.

Both worlds can deliver a rich variety of network services. The telecom world can use IMS application servers to create service delivery platforms. The internet world can use service chaining to combine individual web services. Both approaches work across multiple access networks.

From the perspective of the internet world connectivity for free can be viewed as a mechanism for value generation through viral networks. That value can then be realized, in principle, through other revenue generating instruments, such as advertising.
From the perspective of the telecom industry connectivity for free is viewed as economic nonsense. But Webcos and other Internet portals argue that the capacity is already paid for by the telecom industry’s subscribers. The use of advertising-based models by the telecom industry could possibly replace a proportion of declining telecom transaction revenues. That proportion may not be high enough to deliver the return on investment necessary to maintain an adequate global network infrastructure.

Today, the contrasts between the internet world and the telecom world are stark (Figure 9.8).

Figure 9.8 A Comparison of Internet and Telecom Environments

The existing climate of trust creates a brief window of opportunity for mobile operators, particularly those with converged offerings that include cost effective broadband access for computing devices. But it requires a “real time communications” business model in which end users are willing to pay for the delivery of bundled communications and content with QoS. Such a model will have to compete with “non-real time communications” models offering “free” service without QoS based on open core IP networks where voice is treated as just another application.
The current internet world is a dangerous place to play, wrought with security and privacy challenges. It’s far from a trusted environment. It’s a world in which end user expectations are that services and information are generally free. In the telecom world, however, end users are accustomed to paying for service. In return they expect, and receive, high quality of service levels. In general the telecom world is also regarded as a more trusted environment. Mobile networks in particular are renowned for their strong encryption and authentication procedures. While the situation will change as Internet access through mobile handsets becomes more common, there has so far been little spam, few viruses, and remarkably little phishing and pharming in the mobile environment.
10 Appendix B Scenario Planning Methodology

Making decisions in the midst of uncertainty is not easy. Making the right decisions is even harder. Key decisions that need to be made today can have significant impacts in the future – even resulting in life or death situations for organizations – but the future is impossible to predict. Scenario planning is a tool designed to address this dilemma (Figure 10.1).

![Figure 10.1 The Scenario Building Process](image)

Scenario planning acknowledges the impossibility of resolving the uncertainties that will eventually determine the success or failure of a key decision. Instead, scenario planning creates a set of distinct, divergent yet plausible views of the future. The purpose is not to select a most likely scenario but to draw attention to the major forces that could drive the future in different directions. Scenarios are a way of understanding the dynamics shaping the future. Understanding the dynamics allows the robustness of different strategies to be compared by evaluating how well they play across a range of different scenarios.

Source: Lawrence Wilkinson in McClelland, Ultimate Telecom Futures, 2002
The scenario planning process is outlined in Figure 5.1. The initial step is to articulate the focal issue to be addressed. Then the long term forces that are relevant in the context of this focal issue are enumerated. These primary driving forces fall roughly into four categories: social dynamics, economic issues, geopolitical issues and technology.

The list of driving forces is then analyzed and sorted into predetermined elements and uncertainties. Predetermined elements are those such as demographic factors that are completely outside our control and will affect all possible scenarios. They can be discarded; it is the uncertainties that determine different futures.

Many certainties will be identified of course. But some will be more important than others. A small number of uncertainties will not only be pivotal to the focal issue but will also be particularly impossible to predict. These are classed as the critical uncertainties. They are key factors that contribute to the range of possible outcomes that characterize the future in the context of our focal issue.

At first sight all the critical uncertainties might appear to be unique. But behind the critical uncertainties lurk some underlying commonalities. Recognizing these commonalities allows some of the critical uncertainties to be bundled together, creating an axis of uncertainty. One group of critical uncertainties, although coming from different categories, will have the same underlying commonality, defining a single axis of uncertainty. Another group will be characterized by a different underlying commonality and will define a different axis of uncertainty.

Simplifying the situation to a small number of axes of uncertainty not only draws attention to the most fundamental issues influencing the future but also creates a powerful analysis tool. Matrices defined by the crossing of these axes specify separate sectors with distinct characteristics. Each sector represents one possible scenario. Taken together, the set of possible scenarios provide an effective framework for exploring the future.

Experience with scenario planning shows that the fewer the scenarios the better. Although hundreds of scenarios could be created from different combinations of the driving forces, the most effective framework has proved to be one that contains only one, two or three axes of uncertainty.

The goal is to simplify the entire list of related uncertainties into two orthogonal axes, defining four very different, but plausible, quadrants of uncertainty. Each of these quadrants is a separate scenario, defining a limited but comprehensive set of logical futures that can be explored.

Describing how the primary driving forces characterize the dynamics of each scenario creates scenario descriptions, inevitably and necessarily of an exaggerated nature. The scenarios are not intended to be an accurate
representation of the future. Rather they delineate the outer limits of what is plausible. The future will likely contain elements of all scenarios.

The role of the scenarios is to act as a test bed for decisions. Some decisions will make sense across all of the futures; others will make sense in only one or two. Those that work across all the scenarios can be regarded as robust. Those that make sense in only one or a few of the scenarios are more problematic. Confidence in these depends on recognizing the early warning signs indicating that particular scenarios are beginning to unfold. As the leading indicators for a given scenario are not always obvious, scenario planning helps by identifying the critical signs that need to be monitored.

10.1 Driving Forces including Critical Uncertainties

The focal issue addressed by the analysis in this report is the future demand worldwide for Identity Management and Web Services in public networks. The time frame is specified as the year 2015.

Following the scenario planning methodology outlined in Section 5, an extensive list of driving forces that could lead to disruption and uncertainty was compiled within each of the four basic scenario planning categories of Social Dynamics, Economic Issues, Geopolitical Issues, and Technology. Removing the predetermined elements from this list and ranking the remaining elements by order of importance to the focal issue resulted in a set of driving forces. These driving forces included:

- Level of industry cooperation
- Privacy concerns
- Values consumers place on identity management

Further analysis of these driving forces resulted in a subset of driving forces that represent the most critical uncertainties. The impact of any of these critical uncertainties could significantly influence the demand for public services enabled by identity management and web services.

The five most important critical uncertainties identified within each of the four basic scenario planning categories are listed below.

10.1.1 Social Dynamics

- Differing end user (consumer and business) values and behavior across a range of evolving social and commercial environments
- End user expectations of service quality and perceptions of value
- End user concerns about security, privacy and fraud
• Social networking, the influence of communities and the emergence of new peer-to-peer communication mechanisms
• Varying loyalty patterns and attitudes towards service providers

10.1.2 Economic Issues
• Industry structure changes resulting from new regulatory regimes
• The impact of alternative technologies, emerging developer communities and new service providers
• The impact of convergence both within and between sectors and the emergence of new competitive players
• Net neutrality controversy
• New value chains within the industry ecosystem

10.1.3 Geopolitical Issues
• Corporate governance crises driving compliance regulation
• Regional perspectives on Intellectual Property Rights (IPR) and Digital Rights Management (DRM)
• Future of world trade and economic organizations
• E-government initiatives and data protection legislation
• Emerging markets and the shifting balance between regions

10.1.4 Technology
• Implications of all-IP networks
• Separation of services from access
• Interoperability and industry dynamics
• Next generation network architectures
• Proprietary systems, open source and standardization

10.2 Mapping Critical Uncertainties
The driving forces and critical uncertainties listed in Section 7.2 have been further analyzed and debated in depth within group discussions. Some key conclusions emerged from that analysis:
• Some critical uncertainties are related to end user activities or attitudes
• Some critical uncertainties are related to communications industry structure or dynamics
All critical uncertainties are related to either end user attitudes or communications industry dynamics

Many critical uncertainties are related to end user attitudes as well as communications industry dynamics

The impact of the critical uncertainties is most frequently related to the interaction between end user activities and the communications industry dynamics

These relationships can be in either direction. Major uncertainties can be driven either by the impact of end user activities on industry dynamics or the impact of industry dynamics on end user activities

Given these conclusions it seems natural to map the critical uncertainties onto the end user and industry domains. A high level view of this mapping is presented in Figure 10.2.

**Figure 10.2 Mapping Critical Uncertainties for Identity**

<table>
<thead>
<tr>
<th>Social Dynamics</th>
<th>Economic Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impacts end user attitudes</td>
<td>Impacts industry structure</td>
</tr>
<tr>
<td>• End user expectations of service quality and perceptions of value</td>
<td>• New value chains within the industry ecosystem</td>
</tr>
<tr>
<td>• End user concerns about security, privacy and fraud</td>
<td>• Industry structure changes resulting from new regulatory regimes</td>
</tr>
<tr>
<td>Impacts end user attitude and industry structure</td>
<td>Impacts end user attitude and industry structure</td>
</tr>
<tr>
<td>• Differing end user (consumer and business) values and behavior across a range of evolving social and commercial environments</td>
<td>• The impact of alternative technologies, emerging developer communities and new service providers</td>
</tr>
<tr>
<td>• Social networking, the influence of communities and the emergence of new peer-to-peer communication mechanisms</td>
<td>• The impact of convergence both within and between sectors and the emergence of new competitive players</td>
</tr>
<tr>
<td>• Varying loyalty patterns and attitudes towards service providers</td>
<td>• Net neutrality controversy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Geopolitical Issues</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impacts end user attitudes</td>
<td>Impacts industry structure</td>
</tr>
<tr>
<td>• Future of world trade and economic organizations</td>
<td>• Interoperability and industry dynamics</td>
</tr>
<tr>
<td>Impacts end user attitude and industry structure</td>
<td>• Next generation network architectures</td>
</tr>
<tr>
<td>• Corporate governance crises driving compliance regulation</td>
<td>• Implications of all-IP networks</td>
</tr>
<tr>
<td>• Regional perspectives on IPR and DRM</td>
<td>Impacts end user attitude and industry structure</td>
</tr>
<tr>
<td>• E-government initiatives and data protection legislation</td>
<td>• Separation of services from access</td>
</tr>
<tr>
<td>• Emerging markets and the shifting balance between regions</td>
<td>• Proprietary systems, open source and standardization</td>
</tr>
</tbody>
</table>

Source: Telecompetition Group, July 2006

To see how the mapping of critical uncertainties onto the end user and industry domains works at a more detailed level we take the example of the critical uncertainty “separation of services from access” within the technology category.

Separation of services from access has been a long-awaited goal within telecommunications. Separation of services from the transport layer was a design feature of intelligent networks that paved the way but somehow never fully realised its promise. Separation of services from access is promised by IMS but
there are few expectations of full interoperability and vendor independence in the early stages of deployment.

Separation of services from access has however unexpectedly been delivered in the form of Skype, a proprietary VoIP solution using peer-to-peer technology that has been proven to scale\textsuperscript{14}. Skype is an example of an emerging communications paradigm that has been termed a “social software application” [Gabrielsson, Mitra and Skog, 2006]. The Skype model offers voice, video and IM capabilities but has no relationship whatsoever with access providers. It is a disruptive development that truly separates services from access – a somewhat ironic development given that the technology emerged from outside the conventional telecommunications industry.

Unlike conventional telecoms business models, applications such as Skype do not require any formal or continuing contractual relationship between the service provider and the end user. The value of social software applications lies in the community they are able to attract, they follow Metcalfe’s Law on networking: the more who have it, the more valuable it becomes.

Technologies such as Skype enable VoIP, offer free telephony over the internet and have attracted a significant community of users. There is already a clear impact on both residential and business end user expectations and behaviour – end users like “free” – and considerable uncertainty as to how that impact will evolve in the future, particularly now that Skype has been acquired by eBay. Skype threatens the substantial voice revenues enjoyed by traditional telcos and therefore could have a major, but again highly uncertain, impact on the industry structure and dynamics.

Other technology developments are breaking down the previous one-to-one relationships between service types and access technologies, driving significant changes in end user behaviour, where triple play options from a variety of sectors are significantly increasing choice, as well as accelerating demands for technology and service neutrality in the regulatory environment that are forcing fundamental changes in industry structure. Separation of services from access is clearly a critical uncertainty affecting both end user attitudes and communications industry dynamics.

It could be argued that separation of services from access is a consequence of the move towards all-IP networks, one of the other critical uncertainties in the technology category. This illustrates that overlap often occurs between critical uncertainties – they are rarely unique. The implementation of all-IP networks, however, has other very direct impacts on industry structure and dynamics, implying the phasing out of circuit switched networks and encouraging the development of third party developer and service provider communities.

\textsuperscript{14} Some purists say Skype is not strictly peer-to-peer as it relies on some central servers for authentication and software distribution.
11 Appendix C - Demand for Digital Identity Capabilities

The level of market demand for identity management capabilities conforming to the Liberty Alliance synopsis was investigated from the perspective of a telco network operator. Four separate market segments were considered in each scenario: consumer, business and government end users, and service provider partners.

Individual demand estimates were made for each market segment in each scenario for every one of the Liberty deliverables and characteristics listed in Figure B.1 (Figure 8.8. in the body of this paper).

*Figure 11.1 Factors that Impact Revenue Growth*

<table>
<thead>
<tr>
<th>Telco Environment</th>
<th>I Day in the Park</th>
<th>II Safety at A Price</th>
<th>III Anything Goes</th>
<th>IV Vibrant Diversity</th>
</tr>
</thead>
<tbody>
<tr>
<td>End user service pricing expectations</td>
<td>Free</td>
<td>High</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>Regulatory regime for communications sector</td>
<td>Light</td>
<td>Strong</td>
<td>Moderate</td>
<td>Light</td>
</tr>
<tr>
<td>Competition from other network operators</td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Competition from Webcos (other SPs)</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Number of Active Content Providers</td>
<td>Huge</td>
<td>Small</td>
<td>Large</td>
<td>Medium</td>
</tr>
</tbody>
</table>

*Source: Telecompetition Group, June 2006*

The question explored was: “How well does the environment inherent in the scenario satisfy the market segment need met by a Liberty attribute?” If the requirements or expectations of the market segment are completely satisfied by the scenario environment then there is little or no demand. If the scenario environment fails to meet the requirements or expectations of the market segment then there is strong demand.
The combined results are presented below where relative rank means that the needs of the segment are not met by the environment depicted in each scenario. These unmet needs result in market demand for identity solution provided by the Liberty Alliance.

*Figure 11.2 Demand by Scenario for Liberty Alliance Solutions*

High demand for at least one market segment was estimated to be present in all four scenarios. In each scenario shown, at least two market segments had strong demand (> 50%) for standardized identity management solutions. Liberty Alliance is the key worldwide body establishing industry standard solutions.
12 Appendix D – Validating Scenarios: Laws of Identity

The “Laws of Identity” are widely misunderstood. They focus on a single environment – the enterprise. If the scenario framework is valid for a wider range of environments that include public networks, then an analysis of the laws should show that they are not robust across the scenarios. Indeed, as shown in Figure 12.1, these laws are only strongly aligned with Scenario I.

The Laws of Identity originated in the desire to address the problem of eroding public trust in the internet. The internet was designed for anonymity. There is no inherent mechanism for determining who or what you are connected to over the internet. There was originally no perceived need for such a mechanism as the internet was created by a small group of like-minded people who all knew and trusted each other. The need to authenticate identity was an alien concept in the pre-web era of the internet.

As the internet became a public and pervasive tool the lack of any identity or security layers resulted in an extremely unsafe environment in which theft and deception proliferated. Bringing security, privacy and trust to the internet is clearly an important task.

The “Laws of Identity” [Cameron, 2005] were proposed as a prescription for providing an identity layer for the internet. They have been well received and accepted across the identity community. But they are not laws in the conventional sense. They do not result from empirical observations that allow the formulation of a set of rules that describe and determine the behavior of a system. Instead they are a set of guiding principles that provide a rational and meaningful framework for the construction of an identity metasystem.15

We adopt here the term “Identity Principles” in an attempt to avoid misinterpretation. The seven “principles” can be summarized as follows:

1. User Control and Consent – Technical identity systems must only reveal information identifying a user with the user’s consent

2. Minimal Disclosure for a Constrained Use – The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution

3. Justifiable Parties – Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship

15 Some observers have noted that strict observance of one of the “laws” can lead to violation of another “law”. This is not unexpected. Laws tend to be mutually exclusive whereas principles do not.
4. Directed Identity – A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5. Pluralism of Operators and Technologies – A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6. Human Integration – The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7. Consistent Experience across Contexts – The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

While one may argue the specifics of these statements they provide a well understood set of guidelines to evaluate various ways of approaching the complex problems of identity where multiple forces are interacting from a uniformly stated set of principles composed from the viewpoint of the participants.

The set of seven “Identity Principles” can be used to delineate a generic identity management approach. A qualitative analysis of how well the Identity Principles are satisfied in each of the scenarios presented in this report can give insight into the viability of this approach in the public network context. A summary of this analysis is shown in Figure 5.2.

16 “Operator” in this context refers to an identity provider rather than a telecommunications network operator.
The method used for the comparison was to subjectively judge the degree to which the environment of each scenario was in harmony with the Identity Principles using a simple “stoplight” code to denote the level of agreement.

Scenario I (Day in the Park) had the most elements that were in harmony with the Identity Principles. As this scenario allows for social networks thriving and the natural emergence of an equivalent metasystem of federated systems it is as close a fit to the Identity Principles as is, most likely, possible. There is therefore little perceived need for an overarching identity metasystem solution in this scenario.17

Scenario II (Safety at a Price) provides partial agreement but is limited overall, being driven basically by a limited number of certified choices driven by governmental policy. While there will be a consistent experience and a clear human integration, these are driven by the government mandated structures for declaring identity which is considered the price for safety. With the large amount of government control directed parties are

---

17 The term “identity metasystem” can be interpreted in different ways by different members of the identity community. In this section the term is used specifically and solely to refer to a generic identity management approach delineated by the “identity principles.”
not present and the correlation of the end user’s identity data is accepted as a given. Proprietary implementations of identity management approaches based on the Identity Principles may not play too well in this scenario where governments would be naturally reluctant to relinquish control to the private sector, particularly if the predominant companies involved were based in other countries.

Scenario III (Anything goes) is the least in agreement and is the scenario that is closest to the cyberspace of the web that is the current reality. This would be the logical outcome given that the chaos, fraud and uncertainty associated with the web as we know it today is the fundamental cause of the burgeoning development of identity management products and philosophies currently occurring. The identity management approach delineated by the Identity Principles is particularly relevant to this scenario as it directly addresses the most important market demands.

Scenario IV (Vibrant Diversity) is in harmony with the “privacy” elements of the Identity Principles, but not with Principle 5, as the pluralism of operators and technologies and their interworking are not assured. Here an identity metasystem approach that bridges all of the standards based on proprietary systems offered on the market place is unlikely to be viable. This has a natural follow through on Principles 6 and 7, human integration and consistent experience across contexts.

This analysis indicates that an identity management solution based on the Laws of Identity considered here would only experience significant market demand in Scenario III. This is a consistent result that supports the scenario definitions. Scenario III is driven primarily by the lack of security, privacy and trust in the internet. The identity management approach delineated by the Identity Principles is designed specifically to address these very issues.

The analysis presented here is for public network services and indicates that the specific approach considered in this section is unlikely to satisfy market demand or provide a robust solution for all scenarios. This does not imply of course that the approach would not work across an equivalent set of scenarios in the private network enterprise space – the environment for which it is primarily designed.
13 Appendix E – Regional Differences

While Asia and Europe lead the world in next generation mobile services, of the issues covered in this report have emerged from developments within the internet community.

The telecommunications and IT sectors in the USA differ in many respects from those in the rest of the world. As mobile and fixed convergence accelerates, regional strengths will result in distinctly different identity environments. The environments are encompassed in the four scenarios.

In some areas the USA is the exception rather than the rule. Examples of this include:

- Inter-country roaming is a secondary consideration in the US telecom sector. In most other countries it is a primary factor.
- The cable industry is a significant media and communications player in the USA. Very few other countries have cable operators that can be viewed as competitive to the telecoms or internet sectors.
- Technology diversity is seen as positive in the USA and comparative marketing between technologies is common.
- The text messaging phenomenon – essentially a social networking phenomenon – started with SMS in the mobile telecoms sector in most of the world but lagged in the USA. In the USA it emerged as instant messaging (IM) from the internet sector.
- Most of the world operates on a calling party pays basis for telecom services. Mobile services in the USA are often based on a called party pays model.
- Less than 10% of mobile subscribers in the USA are prepaid. In most other countries the majority of mobile subscribers are prepaid (see discussion below). However, the proportion of prepaid subscribers is now beginning to increase in the USA. Prepaid users grew by 22% during 2005 compared with a 10% growth in contract customers [Hearn, 2006].

So, while the USA seems at the moment to be playing a key role in the future of identity management, to assume so over time may be dangerous and deceptive.

Mobile and fixed operators in other regions have proven repeatedly that innovation often comes from an unexpected sector. Asia continues to lead the world in next generation mobile services and is the growth leader in fixed broadband as well. Asian consumers, especially in Japan and South Korea have demanded leading edge services from their providers. In these societies identity management and even identity threat are less on the mind of end users.
13.1 Prepaid

Identity management in the mobile sector needs to recognize the existence of both prepaid and post-paid (contract) subscribers.

Figure 13.1 Worldwide Prepaid and Contract Connections

![Graph showing worldwide prepaid and contract connections over time](image)

*Source: Wireless Intelligence, April 2006*

Mobile service providers hold a significant amount of identity information about contract customers. Prepaid subscribers, on the other hand, are essentially anonymous. \(^{18}\) In principle, mobile service providers may have no knowledge of the identity of a prepaid customer.

On a global basis, prepaid currently accounts for 63% of mobile connections [Hearn, 2006]. This proportion is steadily increasing (Figure 13.1); in Q4 2005 over 80% of net additions were prepaid.

---

\(^{18}\) Many countries are now requiring identity information for prepaid subscriptions to be captured at the point of purchase on security considerations. However, this may not reliably identify the eventual user and usage of the identity information can be restricted for legal reasons.
There are significant regional variations in the proportion of prepaid subscribers

*Figure 13.2 Prepaid vs. Contract Connections, Differences by Region*

[Graph showing regional variations in prepaid vs. contract connections]

Source: Wireless Intelligence, April 2006

In some countries the mobile subscriber base is dominated by prepaid. In Italy, for example, 95% of total connections are on prepaid plans. In some other countries the situation is reversed. Prepaid accounts for just 2% of connections in Japan and Korea.\(^{19}\)

According to Wireless Intelligence, Western Europe is the only region where the annual growth rate of contract connections has been greater than that of prepaid over the past four years. The Asia-Pacific region appears from Figure 5.13 to be similar to Western Europe but China and India account for half the contract subscribers in the region and both these countries have larger prepaid subscriber bases than contract. If China, India, Japan and Korea are removed then the proportion of prepaid subscribers in the region is similar to that of Eastern Europe.

---

\(^{19}\) Prepaid has become associated with criminal activities in Japan and is now actively discouraged by legislation.
13.2 Strong Authentication

The central role of the SIM card in GSM based mobile networks can be a crucial factor in the provision of strong authentication. Through the SIM, mobile network operators can provide strong authentication and identity management to service providers.

Use of the SIM for strong authentication is a key aspect of the Fidelity Project\textsuperscript{20} which is implementing a proof of concept pan-European identity management system using the Liberty Alliance federated model based on open architectures and standards. The Fidelity Project is deploying circles of trust on four sites in different European countries to test interoperability. The project demonstrates how local identity federations can interact at a pan-European level, enabling exchange of identity and authentication of citizens between service and identity providers, whilst the usage and validity duration of identity data remains totally under the user's control and acceptance.

The Fidelity Project illustrates that mobile network operators are well positioned to act as identity providers, delivering value to end users in terms of protection and privacy. But end users are not willing to pay the costs. Service providers however should be willing to pay as strong authentication of end users is a vital mechanism for protecting their assets.

European countries are far ahead of the USA and the rest of the world in the adoption of strong authentication. In early 2006, the EMV (EuropayMasterCardVisa) strong authentication standard was launched to allow retailers to authenticate consumers through the use of smartcard-based cash and credit cards. The change in digital medium was accompanied by a shift away from a cardholders' signature to the input of a PIN, providing 2-factor identification and delivering an estimated 70% reduction in counterfeiting. [Fishbein, 2005]

The protection provided by the smartcard chip is significant enough that a liability shift is underway in Europe, the Middle East, Africa and Asia/Pacific. The party that does not support EMV smartcard technology, credit card issuer or corporate customer, will now bear all the risk for fraudulent transactions.

Identity solutions for these regions are incorporated into the Liberty Alliance protocols.

\textsuperscript{20} http://www.celtic-fidelity.org/fidelity/index.jsp
14 List of Terms

ARPU – Average Revenue per User
DRM – Digital Rights Management
IDM – Identity Management
IDP – Identity Provider or Protector
IM – Instant Messaging
IMS – IP Multimedia Subsystem
IPR – Intellectual Property Rights
IT – Information Technology
MVNO – Mobile Virtual Network Operator
QoS – Quality of Service
SMS – Short Message Service
SSO – Single Sign-On
WTO – World Trade Organization
15 References


European Commission. Your Voice on eGovernment 2010, online public consultation; report Jan 2006 V 1.0


Gabrielsson, Jan, Nilo Mitra and Robert Skog. Social Software Applications as a New Communications Paradigm – Skype versus the Traditional Telecoms Operator Model. in ICIN 2006.


ICIN 2006. Convergence in Services, Media and Networks. 10th International Conference on the Intelligent Service Layer of Communications Networks, Bordeaux, June 2006. edin@adera.fr


Randall, Roderick. The Future of Network Intelligence: IN 2.0. in ICIN 2006.

16 Study Participants

The following people participated in this study:

Liberty Alliance Study Project Team

  Miguel Cobo  
  Peter Davis  
  Britta Glade  
  Atsuhiro Goto  
  Philippe Lucas  
  Kenji Takahashi  
  Paola Tonelli  
  Kenneth Salzberg  
  Andrew Shikiar

Telecompetition Group

  Thomas Edrington  
  Eileen Healy  
  Stuart Sharrock  
  Terry Young

Contact: info@telecompetition.com

The following industry leaders were interviewed as part of this study:

  Kaliya Hamlin, Identity Woman, Network Director of Planetwork, USA  
  Dick Hardt, CEO, Sxip Networks, Canada  
  Alice Marwick, Independent Consultant and author of Tiara.org, USA  
  Mike Short, Vice President, R&D, O₂ Group Technology & Chairman, Mobile  
  Data Association, UK  
  Thanh van Do, Senior Research Scientist, Telenor R&D, Norway
17 Index

Authentication, 5, 9, 26, 28, 54, 60

Blogging, 49

Competition, 4, 6, 19, 31, 32, 38, 47, 49

Consumers, 3, 7, 29, 30, 31, 32, 34, 39, 50, 57, 58, 67

Content, 24, 28, 29, 37, 40, 49, 50, 53

Convergence, 5, 19, 29, 30, 32, 51, 53, 58, 73

Deployment, 3, 30, 40, 60

Disruptive, 3, 47, 57, 60

Drivers, 3, 26, 27, 28, 35, 65

DRM, 58, 72

e-Government, 37

Federated, 7, 9, 32, 40, 65, 73

Google, 4, 17, 18, 25, 49, 73

IMS, 51, 52, 59, 72

Industry structure, 47, 50, 51, 58, 60

IP, 3, 15, 25, 30, 47, 51, 53, 58, 60, 72, 73

Liberty Alliance, iv, 3, 9, 10, 74

Microsoft, 65, 73

Privacy, 5, 6, 9, 29, 30, 31, 32, 54, 57, 63, 66

Provisioning, 3, 47

QoS, 5, 52, 53, 72

Regulation, 1, 3, 30, 32, 46, 47, 58, 60

Revenue, 2, 14, 16, 17, 18, 19, 20, 21, 24, 30, 34, 37, 39, 40, 41, 43, 50, 52

Security, 5, 6, 9, 26, 30, 31, 32, 54, 57, 63, 66

Separation of services, 59, 60

Services, 2, 3, 4, 5, 9, 14, 19, 20, 26, 28, 29, 30, 31, 32, 34, 35, 37, 38, 39, 40, 44, 46, 47, 48, 49, 50, 51, 52, 53, 54, 57, 58, 59, 60, 66, 67, 73

SSO, 72

Traffic, iv, 38, 49, 51, 52

Trust, 5, 6, 9, 18, 24, 29, 31, 32, 53, 70

Viral Networks, 48, 52

Viruses, 28, 30, 49, 54