When a baby first becomes aware, psychologists tell us, it knows only “me” and “not-me.” Then it learns to distinguish “me,” “mother” and “other.” From that point, it develops an ontology of the world and the people in it, starting with its immediate family and lots of familiar objects. All these people and things, initially defined by their relationships to the child at the center of the universe, gradually assume their own independent identities. Eventually, the child learns that other children have their own mothers and fathers, perhaps also called Mommy and Daddy, or Mom and Pop, or even Juan and Alice. The question of identity is strongly linked to the context, and to relationships: As George Bernard Shaw wrote in *Pygmalion*, “The difference between a flower girl and a lady is not how she behaves, but how she is treated.”

At the other end of the universe, there’s cyberspace, where objects traditionally haven’t been linked to human context. For example, the job of the Domain Name System is to transcend the boundaries of context and allow any resource to be reachable by any other, with no need to know who’s asking or from where. That is, one can find not my mother or your mother, but a particular, unique mother identified by top-level domain (TLD), second-level domain and beyond, as specific as necessary. Different TLDs imply different contexts, but you do not need to be inside a particular context to see or reach its resources.

In the middle, identity management technologies, such as they were, historically attached themselves to individual applications or resources.
Support for contextual identity is now taking hold in the digital world as a fundamental infrastructure element supporting stand-alone services. Though much of the underlying technology is the same, the specifics are different between people/users and other objects in the digital world (consider agents a hybrid); here we focus on people and personal identity.

In more and more online situations, there are requirements for knowing people’s identities – for security, for billing, for recognizing friends, for marketers to sell us what we want, for conducting our daily business of commerce and political and social interaction. As a general rule, everyone wants identity information to be accurate, but there are three counterforces: individuals’ desire for privacy (which should be respected); bad guys’ intentional misrepresentation or misuse of identity information either to gain advantage or escape accountability; and the sheer sloppiness of the real world, which leads to inconsistencies, omissions and redundancies of data (what the Germans call Freiheit durch Schlamperei, or freedom through messiness).

There are also legal/social policy questions surrounding access to all this information: Who controls it? Who quality-controls it? Who is responsible for errors? Who resolves disputes, and by what rules?

Self-disclosure about this issue: From stranger-to-stranger to friend or foe

Last fall, we took an initial look at digital identity management systems in connection with Web services and security (see Release 1.0, October 2001). Beginning this month, we examine the issues surrounding identity, and especially personal identity, more deeply. We will outline the transformation of our virtual, abstract world of content and systems – the one we have been building online for a generation now – into a concrete, tangible world full of recognized and recognizable people. Before, this world was unaware of specific people; now, we’re creating virtual passports and ID cards for people to use as they travel online; virtual suitcases for them to carry familiar objects and tools with them; virtual clothing with which to
make fashion, political, economic or social statements; and virtual real estate that they can call home and where they can be in or out. There are also virtual bouncers and tollbooths, virtual butlers and security guards and personal assistants. None of this seems that revolutionary; each of these things can be done already, but they will happen on such a broad scale that it will utterly transform the online world of virtual local villages into one where anyone can travel widely and yet remain as at-home – and as visible – as in his own neighborhood. Some people may like this; others may long for the anonymity of the electronic frontier, which will still exist but will become relatively smaller as the newly visible digital world expands.

Specifically, in this issue we start by introducing identity management in general, and exploring the technical infrastructure of identity management – directories and authentication – and the primary functions they support: authorization/access/security, and credentials. We look at a variety of sometimes overlapping examples (rather than the whole field) of the architecture of identity management as it changes from a feature of applications to an independent application/service. Then we outline the roles of the two major political players in the authentication space: Microsoft (with Passport, a service), and Liberty Alliance (a consortium, with a forthcoming spec), along with AOL’s Magic Carpet. And finally, we discuss the important issues of trust and verification.

In our July issue, part 2 of this set, we will focus on a variety of do-it-yourself ways of establishing and expressing your personal identity and presence in cyberspace. We will also explore a range of newer identity-based applications, from new kinds of presence management to automated call-handling and spam deterrence.

(Finally, in part 3, this fall, we will address the many technical issues around identity that apply not just to people but also to things: products, (Web) services and IT resources.)

**Digital Identity Management: What For?**

Virtually every application in the future will make use of identity information, but there are some specific areas that will lead in its development and use. Of course, what can be managed is not the ineffable “identity” of a person, but all the relationships with and data about that individual – the profile. Identity-based functions include authentication, authorization, security and access. Those functions support
applications such as billing and payment, direct marketing and CRM, provisioning, roaming (basically, remote provisioning), presence management, workflow, and knowledge management (especially as managers start to realize that most knowledge is in people's heads, not in databases). It's hard to think of a sector that can't use these functions, but the leaders are those that are personal-data-rich and change- and security-intensive, such as financial services, travel services and health care.

Meanwhile, scalability and portability are key features of all these identity-based systems. Indeed, scaling up is the meta-problem that they handle. Identity on a small scale doesn't need handling. Each person or thing can be handled as a specific case. The essence of identity management is defining people and things as classes or groups, to which you can apply policies or draw conclusions. Identity management crosses contexts and reduces complexity by finding the common elements across individuals so that they can be handled on the basis of policies rather than one by one… yet treated as individuals if they happen to call a help desk, check in at a hotel, ask for a particular set of data or make a phone call from a cell phone in a foreign country using a third-party wireless carrier. They want responses in their own language, tailored to their own history and preferences.

Finally, as users move from place to place, they usually want to take some information with them. One question is: Who holds that information? As identity management becomes more transparent and visible, it will also feel more concrete; people will know where their data is. Just as data practices become more standardized and explicit, so will data policies. Privacy issues are likely to be easier to resolve as users can easily understand, define and control what happens to their data.

Identity vs. credentials, identity vs. profile
It's worth making the distinction between identity – the unique person – and a variety of other kinds of information – unique or not – linked to that identity. Call it the profile. The profile includes parameters, such as age, weight, income; categories, such as nationality or status; and pure data, such as address or membership number. Parameters and credentials, such as income category or membership status, can be derived (accurately or not) from pure data. In the box, you can see the variety of information potentially linked to a single individual – items not necessarily linked among themselves. Much of the challenge of identity management is to make and manage those links. The canonical goal of actually collecting all the info in one (virtual) place is neither possible nor necessarily desirable. Even if we tried, we’d always be generating new information in new places.
In addition, while in some applications specific identity matters, it’s often simply a matter of “what kind of” are you and what (how much) are you good for? What services are you likely to want? What credentials (and privileges) do you have? What role do you play in this context? Who will vouch for you? That is, there’s a difference between identifying an individual, and defining a role that could be fit by many individuals, whether it’s “someone authorized to see this plan” or “someone worth more than $10 million who has purchased more than three yachts in the last five years.” However, paranoid bouncers – online and off – often require ID when a mere credential would do.

**Identity emerges...into a federation**

Identity management technology has been around for a long time, in mostly implicit ways (just as we managed data long before we had database management) – and of course the data was disconnected and redundant. Every listing of employees, every application’s list of registered users and passwords, every marketing database and contact list is a precursor of a kind of identity management, but generally on a local, nonstandard, ad hoc basis, to say nothing of identity papers, badges and the
like from the prehistoric era before pcs. What we’re talking about now is collecting all that information into a form that can be shared and used across functions and applications, linked by a unique identity. That doesn’t mean a single, unified global database, but a set of standards and protocols so that information can be shared (according to policies), or “federated” as the popular term has it.

The real federation happens at the center of the universe – where the individual interacts with and through all these identities. Although law enforcement, creditors, girlfriends or boyfriends and others all want to know everything about a person, most people maintain a variety of distinct identities or at least facets of a single identity. Likewise, a variety of organizations maintain different information about each individual in the context of their relationships with that individual – as employees, customers, partners and the like. Integration of a single identity is not a binary question. With some effort, it’s usually possible for an individual to maintain multiple distinct, never-linked identities. It is also usually possible – with some more effort – for law enforcement or others to pierce the veil and fit most pieces together.

This ability to pass profile information linked to a single identity from context to context is key for most of tomorrow’s distributed systems. No longer are most computers used by anonymous users, any more than mail will be sent to occupants or a plane will be boarded by anyone but a well-identified traveler.

Keeping some info in a database is simple; managing the link from an authenticated identity in realtime to authorize or deny access, treat a referred customer as a welcome guest rather than a stranger, offer a browser an appropriate selection of content, respond to a query or a phone call in the context of a relationship…or cut off all access immediately to a fired employee – those are the tasks enabled by identity management.

There’s not a lot of whizzy technology, but a need for punctiliousness, speed, data integrity, etc. Pattern recognition and the like come into play in security applications and of course marketing/data mining/data laundering/predictive modeling. And there’s a certain amount of black magic in recognizing that Juan Martinez and Joan Martinex are the same person….
Components of Identity Management

Identity management, broadly defined, includes a data store (the directory or metadirectory), and a variety of processes that populate it, update it, and rely on its information to derive roles and control (access to) other system resources—everything from plain old access through a firewall to discrete permission ("authorization") to use a specific application function on a specific set of data at a specific time of day. This diagram is misleadingly clear, since many of these components can be either bound together or, increasingly, teased apart. Role information and access rules can be kept in the directory, or they can be separated out into an authorization or control layer (as Oblix does). Tools that work together may also overlap.

Directories: From Text String to Living User-with-ID

Originally, to the extent that software was aware of identity, it was hard-coded into an application or time-sharing system. An application may have had its own notion of a user, and a password list and authorizations. Other applications may have been about individuals, such as a payroll application, or an accounting database. But these were just records. While a customer database is interesting, until recently it was just that—a database manipulated by applications.

But when computers are linked together, the notion of users with individual privileges and profiles becomes important. And as companies move online, suddenly all their customers—once dry, passive entries in an accounting system—turn into users too. Instead of being manipulated, they manipulate. They show up every day at Websites and on intranets, requesting access to corporate information and services. They want to check on their balances, change their profiles, track their orders, and even write to a human being from time to time. Meanwhile, corporate borders are getting more porous. Applications operate across multiple machines and multiple organizations, and will do so increasingly as Web services start to proliferate (see RELEASE 1.0, SEPTEMBER AND OCTOBER 2001). Consultants and partners come and go:
Access rights and provisioning (the process of opening and closing user accounts for corporate IT services such as mail, applications, purchasing authority and things as mundane as cafeteria privileges or gym use) need to work not just within corporate boundaries but also across them. You may revoke all privileges the day an employee gets fired, but will your corporate partner remember to tell you when one of its employees – the one working on your payroll system, say – gets fired?

It all started with directories... in a variety of contexts. Here we illustrate just a few of the contexts from which today’s directories and meta-directories have emerged, and the specialties they are supporting. Novell had one for network operating system (NOS) resources. Metamerge emerged from large systems integration projects, such as tracking and scheduling hospital employees. Critical Path began by managing mailboxes, while Madison integrates the identities of patients in hospitals. As directories are becoming a commodity – just one more piece of infrastructure – the value is in using them to support something in particular.

**Novell: From Netware to dir-ware**

In computer terms, a directory means a repository of users and resources independent of any particular application – or ideally of any particular operating system. The original idea was simply to keep track of users – i.e. employees – and resources in a reference list. About a decade ago, a standard emerged for an all-dancing, all-singing directory that would keep track of everything in the world – X.500 – that delighted everyone with its completeness and rigor. However, it proved almost impossible to use in any real environment; it couldn’t match the ambiguity and dynamism of the real world except in a few highly structured (or artificial) organizations, notably government, military and some financial institutions.

Instead, people started using a subset of X.500 called LDAP (for Lightweight Directory Access Protocol). LDAP began as a simple means of connecting a client to a directory server (simpler than X.500’s DAP, anyway!). It was touted as a way to make different directory services as interoperable as possible, essentially routing around a platonic X.500 directory and operating as subsets of a global directory that usually didn’t exist. LDAP is now widely used; Novell has even extended LDAP to include functionality (Universal Description, Discovery and Integration (UDDI) version 2) for Web services and proposed it to the Internet Engineering Task Force standards body.
In the PC/LAN world, Novell was the initial leader in popularizing the notion of a directory, though it focused mostly on user access to operating system resources — files, printers, LANs and the like — as an extension of its Netware operating system, called “the Bindery.” For years, Novell had the best PC-oriented directory on the market, but it limited its own success by offering it only on top of Netware. Under Eric Schmidt’s leadership, Novell made its directory offerings the centerpiece of the company (see RELEASE 1.0, APRIL 2000), though it continued to lose ground to Microsoft and others.

Now, as the directory market is maturing, Novell counts 420 million users in its eDirectory worldwide, which it claims is more than any other vendor — counting somewhat differently from Sun, which makes the same claim.

Novell also has a new vice chairman: Chris Stone, who was an executive at Novell under Schmidt before leaving to found Tilion, a supply-chain event-management startup; previously, he had run the Object Management Group, a standards organization. He says: “Not only do identities breed like rabbits, so do the repositories that hold them. Virtually every piece of software and every device you purchase includes a repository for your identity. How do you rationalize them? How do you manage them? How do you get to just one?” He is re-focusing the company, both in software and services, on standards-based infrastructure including a healthy dollop of identity management and Web services. Novell has just announced plans to acquire Silverstream, a Web services tool company.

As LDAP directories (and application servers/UDDI tools) become virtually a commodity, Novell has plans to make waves in the provisioning space…but it faces the same problem it had with Netware one quantum over, because its provisioning services rely on the use of Novell’s eDirectory and its DirXML meta-directory. Nonetheless, the company’s sales lead pipeline for provisioning alone was $50 million last year and it is now $250 million, says Stone.

Novell has always “got” the technology early, but it was limited by loyalty to its own installed base of Netware. Now, with provisioning services and a greater respect for standards, Novell has a chance to gain traction. As Microsoft did with Hailstorm, Novell needs to learn to do about-faces in response to market feedback.
Metamerge/IBM: Metamerger

What is a meta-directory? It’s not what you would imagine – a directory that comprises all other directories, but it does usually create a central directory of its own that’s tightly linked to existing directories with automatic two-way updates.

Although directories in theory can hold information for any use, in fact, directories are often targeted at specific functions: access to network resources for employees, for example, vs. one focused on e-commerce and credit transactions. In short, a meta-directory links existing directories: Its very existence is a recognition of the reality of installed bases and the persistence of the many different contexts in which each individual operates. Rather than merge all a person’s identities into one, it links them as needed, and tries to keep the same information consistent across contexts, while leaving information relevant to only one context in its place. (The first significant meta-directory came from Zoomit of Toronto; it was acquired by Microsoft in July 1999 and is now part of Microsoft’s Active Directory.)

Meta-directory software solutions, also called directory integration, usually consist of an LDAP/X.500 directory service, a “join” engine to link data via identifiers – i.e., Juan’s phone number according to HR and Juan’s phone number according to the company switchboard – and connectors for multiple types of data sources – i.e., a method for transforming an extension number into a full phone number. The quality of a meta-directory is reflected in how automatically and how accurately it can reconcile conflicting data... and how smoothly it supports human intervention when the conflicts are simply unreconcilable. Of course, it works on rules given it by humans: For example, HR and its directory determine (and “own” the data about) when an employee is hired or fired, whereas the mail administrator and the e-mail directory assign and own the mailbox ID.

Integrator, developed by Metamerge of Oslo, Norway, is an even more “hollow” meta-directory solution that consists of a join engine and connectors for multiple types of data sources, but it plays especially well with other systems because it has no central directory of its own. Instead, it operates peer-to-peer, assembling just-in-time identities as required. It provides standard two-way translators for common directory formats and applications, and provides tools so that (expert) users can create their own. For example, different subsets of data could be held and managed in an Oracle database, a comma-separated flat file and Microsoft’s Active Directory. That data needs to be merged and then used to populate an enterprise LDAP-based directory. Different parts of the merged dataset also need to go back into the source
system. Metamerge Integrator manages this by creating an assembly line consisting of connectors for each of the four systems, with rules pertaining both to how the data is to be merged and the directional data flows.

Metamerge was founded in 1998 by Michael Knagenhjelm and Bjorn Stadheim. They had worked with a number of large global companies and organizations grappling with complex directory synchronization and messaging integration challenges. They ended up designing their own tools, and established Metamerge to sell them.

IBM has just announced plans to acquire the company and integrate it into IBM’s Software Group, where it expects it to be “a key integration enabler among IBM’s four software brands – WebSphere, DB2, Lotus and Tivoli.”

One recent contract win is with the UK’s National Health Service, which has 1.2 million employees – though not all can easily be found in its records, notes Metamerge chief marketing officer David Goodman. Metamerge’s role, as a subcontractor to EDS, is to extract data from a wide range of distributed data sources, merge them and push them into a centralized directory. The resulting directory will support a range of identity-based services such as centralized messaging and scheduling for hospital staff as well as new white and yellow page services for NHS employees – from consultant surgeons to doctors and nurses and administrators.

**Critical Path: Off the critical list**

Critical Path, from a start as an outsourced mail provider, has gone through both a business and technical transformation. Emerging from a period of alleged fraud and accounting problems and with new management (brought in by returned and once-again departed founder David Hayden), the company reported revised revenues of $104 million last year. It started by managing mailboxes, which gave it experience with directories, and now it’s providing that same expertise in its “Communication Platform,” comprising both messaging and identity management. Its software handles set-up and administration for a broad range of communication services including telephone lines, messaging services such Short Message Service (SMS) text messages and other exotica, as well as plain old e-mail. Its tools include the intelligence to dynamically translate e-mails into SMSs and vice versa, depending on what devices a customer is using at any given time and for any given set of correspondents. That is, one’s “identity” includes one’s device. . . .
Critical Path doesn’t provide telco services, but it sets them up as an outsourcer or provides the software to do so, for over 190 service providers, 40 carriers, 750 enterprises, and 35 governments. Its software currently manages 150 million mailboxes—or identities—around the world, of which 13 million are hosted. They operate for customers including eight national post offices for which it manages public electronic communications facilities, and carriers and enterprises such as British Telecom, Deutsche Post and DuPont. Coming from the e-mail world, Critical Path will run into companies such as Mobileum (in our next issue), which came into directory services from the wireless services end.

Thus, while Novell’s notion of a directory is still more focused on operating system services and provisioning than, say, e-commerce, CP’s directories and meta-directories are tailored for communications services. Each sees its individuals primarily in one context that reflects its heritage.

**Madison Information Technologies: Data laundry**

In a perfect world, such as the one imagined by X.500, there’s one person, one ID. (And because it’s perfect, no one has anything to hide.) In reality, a person will have multiple IDs in many contexts. Problems arise when a person escapes accountability for actions in one identity by assuming another.

But more often multiple identities are inadvertent—as when a single person’s “identity” is captured several times and the profile information is spread across multiple records rather than linked to a single identity.

There’s a range of services to avoid that. At the low end, there are list-scrubbing services, which go through multiple-source mailing lists to identify obvious duplicates and remove known bounces or “return-to-senders.” But there’s still an enormous amount of duplication as well as missing records in single organizations where this is less expected and more costly—and annoying both to companies and to individuals. It results in a customer having to enter or state the same data over and over again, inconsistent records, lack of credit for one’s business (frequent flyer points), or even the wrong brand of mint on your pillow. (There are also false positives, where a pseudo-duplicate is removed, leading to the occasional two travelers with the same name claiming the same airline seat or
hotel room. However, as companies’ data practices improve, it becomes tougher and tougher to double-book, at least on a single airline!)

There are places where all this matters more. Two frequent flyer accounts is a small problem; two conflicting drug therapies could mean life or death. “Almost one in seven repeat patients at a typical hospital have multiple medical records, based on our experience in analyzing over 500 million records in hospital databases,” says Jim Bodenbender, president of Madison Information Technologies of Chicago. Madison’s only business is identity management, including customer data integration and duplicate record detection, primarily in health care, although it recently won a contract with Choice Hotels (Comfort Inns, Comfort Suites, Clarion Hotels and others). Many of its properties keep their own databases, as do each of the chains.

The company, still privately held, launched its software and services four years ago. Basically, it’s a meta-directory specialized for working with messy data. Given the market Madison sells into, and its increasing concerns for liability and overall scale, it can afford to deliver and charge for some premium services (it all comes out of your insurance, of course). Its signature offering is Aligndex™ and its Alta™ algorithms for duplicate detection. (Alta stands for Advanced Linkage Technologies of America, which Madison acquired in 1998.)

Bodenbender won’t go into detail, but suffice it to say that Alta™ weights data not by attribute type but by attribute value… For example, that two identities are of the same sex is not a good sign of a match, but that they are of different sexes is a fairly strong negative indicator. That two people are called [last name] Smith doesn’t mean much, but that they are both Bodenbender means a lot. Some attributes – such as hair color – change, whereas others – such as eye color – don’t (though they can always be recorded inaccurately). The algorithm can be adjusted for a local population – a prevalence of certain names or characteristics, for example – rather than national norms.

Moreover, Madison delivers its service in realtime – as an injured patient is queried at admissions, for example, or as an impatient overnight guest wonders why the hotel can’t retrieve his frequent sleeper number. Most of the competition, says Bodenbender, does batch merge-and-purge and discovers discrepancies and redundancies only after the fact.
Indeed, Madison has had discussions with a number of government agencies about its technology. “Since we don’t merge the data but simply link the records,” says Bodenbender, “we’re very interesting to them. Most of our competition eliminates data that doesn’t match, but we keep it.” Sometimes it comes in handy later. On privacy issues, Bodenbender demurs. That’s up to his customers. But he can do a better job than most of making sure that opt-in or opt-out permissions are consistent across identities – as long as the consumer herself was consistent.

Authorization for Access and Security: Disappearing Perimeter; Emerging Control Layer

Directories are containers, necessary but not sufficient for identity management, especially in its broader sense. They provide the basic information needed to interact with other identity-related information, including rules concerning roles and access rights. Those rules can be stored and executed anywhere, either within an application or an access or security system, or centralized into a separate “control layer” that manages a variety of complementary local services, some of them access systems, and some of them the actual resources. The rules and the resulting conclusions may be arbitrarily granular.

Meanwhile, the increasing complexity of networks, eloquently limned in a series of reports from the Burton Group about the “disappearing perimeter,” means that security is no longer simply a matter of keeping secrets and trusted people inside, and everyone else outside (see also Release 1.0, February 2001). Now insiders work closely with conditional insiders – business partners, suppliers, law firms, accounting firms (who has access to those documents and who should shred them?), and of course systems integrators. Internal resources need to be made available to a variety of outsiders, on the basis of a variety of policies – all of them dependent on the intersection of the individual requester’s identity and roles, and policies governing access (use, copy, modify) to each resource. The authorization policies can be arbitrarily complex, and they should be intelligible and explicit. (That very explicitness helps in corporate governance: “The chairman’s cousin has access to everything” is a policy that should not survive once it is exposed.)
Before identity management became a separate function, Juan (a MegaMat employee) and Alice (a consultant to MegaMat) had separate passwords and IDs for each of the applications and resources they used. Most of these applications maintained their own user lists—a management nightmare susceptible to human error or intentional circumvention. In addition, Alice was outside the firewall and could do very little useful work without files emailed to her by Juan. Adding more people and other resources would make the chart—and the tasks of the IT department—much more complex, with lines everywhere.

But now, Alice has a certificate that allows her to be authenticated in the same way as Juan, though she has access only to the specific application and data she’s working on. The identity information is concentrated by the meta-directory into the control layer.
Topological tangles: Oracle and SAP and Oblix

Of course, there’s room for endless argument about precisely how these functions should be layered or abstracted into discrete (usually Web) services. Should the authorization occur at the application level (through intermediaries allowing multiple applications to recognize the same identities) or should it happen lower down?

At one end, you have Oracle arguing that access should be authorized down to the level of records in a database, by the database. If you use application-level security, notes Mary Ann Davidson, Oracle’s chief security officer, you risk having some alternative application, such as a query tool, coming into the database by the back door and getting at all your corporate secrets. (That’s only if you don’t secure the entire database, of course, but those kinds of things do happen.) It’s a competitive advantage, she continues, for Oracle over SAP, which “treats the entire database like a file system.”

She adds, “It is meaningful to store centrally that John has the SALESREP role. Determining what SALESREP means on any granular level (access to database Z, but only certain privileges on certain tables) belongs in the database because databases are optimized for performing those kinds of access checks. The last thing you want to do is query a third party authorization server to determine if John is allowed to INSERT into this table or UPDATE on this column and worry about synchronizing all that. There are things we take from the directory in terms of access rights, but the access enforcement should be in the database, ultimately. Or in other words: Build strong security once, not bypassable security many times."

On the other hand, SAP has just agreed to support the use of Oblix’s NetPoint identity management suite to control user access and single sign-on (see Release 1.0, March 1999). What does that mean? It doesn’t mean one click and you have access to all of SAP (and all the Oracle-stored data underneath!). Precisely the opposite; it means you have single sign-on to get to exactly the data and functions you’re authorized to get, in all the resources that NetPoint talks to. (Note that SAP also works with BMC, IBM Tivoli and Netegrity, among others.)

When the user comes along to sign into SAP, for example, Oblix NetPoint intercepts the request and authenticates the user before the user can get in. NetPoint then checks on that user’s privileges, and passes the information on to SAP. Right now there’s a bit of technical negotiation going on, since both SAP and Oblix define roles and execute rules to define specific permissions. Future versions of SAP will look to
a directory by default for its user and role information, which will make it easier for control-layer tools such as NetPoint and its competitors.

To make that happen, NetPoint needs to be configured to work with SAP, and with each other application or resource. In the beginning, for vendors such as SAP, Siebel, Peoplesoft, BEA, Plumtree and Epicentric, Oblix has done the work itself to gain market acceptance. When and if application vendors start putting hooks for Oblix themselves, the company will have arrived. Right now, Oblix is working with Oracle on hooks for Oracle, and it will do the work itself to integrate with Microsoft .Net.

Oblix is creating something of a new space by separating out the control functions for identity – the management of identity by groups, rules, authorizations – as well as integration with an arbitrarily large set of specific resources to which access can be granted or denied. Rather than a directory, it’s an application for defining and executing rules – about identities held in a directory, plus roles and circumstances it knows about itself. Obviously, working with any single application is not very exciting; the key is allowing granular, decentralized access to a variety of applications and resources via a single policy and identity infrastructure, for a broad user base.

Oblix is purely a control-manager, with a broad suite of identity-management administration tools: It works with existing LDAP and other directories such as Novell’s eDirectory, Sun’s Sun ONE (née iPlanet, descended from Netscape), Microsoft Active Directory and IBM Directory Server. It offers tools to assign and manage roles, set up and implement rules and policies regarding those roles, and implement those rules through the controls each supported application offers. Of course, NetPoint is a user of itself, since it offers role-based workflow tools for delegating authority to set those policies or assign the groupings to specific managers according to their roles. The rules can concern the individuals, roles and resources, and of course they can also be set to depend on any factors you can represent through a NetPoint policy description such as time of day or the date (for embargoed financial information, for example), the use of a particular (strength of) authentication technique, and the particular (class of) device the user is using.

Although Oblix does hardly any of the dirty work itself, it is in charge of keeping the identities and the rules governing them consistent, setting those policies, and imple-
WHAT YOU CAN DO: UPDATES ON OUR PRIVACY RECOMMENDATIONS

The tools have changed and the visibility of the issues has risen, but we stand by our policy prescriptions of more than four years ago. Here they are, excepted from RELEASE 1.0, April 1998, with updates in italics.

If you’re Bill Gates, information industrialist: By appealing to consumers and the public interest, you can help keep Joel Klein off your back. Use Firefly’s expertise in the public-domain P3P “privacy” technology to work in collaboration with the W3C. Build user-friendly tools on top of it for competitive advantage: data-management controls for users, along with server-side data tools. Promote consumer empowerment as central to the new Digital Nervous System meme you’re promoting (interacting neurons, if you like). Remember what Ford did with the $5-dollar day: Other industrialists thought he was nuts, but he was creating a market for his products that went way beyond his own employees. He raised the bar and doubled wages nationwide. To their amazement, businesses benefited: One company’s employees were another’s customers. Likewise, your empowered users will lose their fear and be active customers for every vendor. Not bad: though you don’t promote privacy in the Passport sales pitch, control over user data is a clear part of the message.

If you’re Joel Klein: Use the leverage you have to get Bill to do the right thing. Encourage Microsoft to keep working with the W3C to keep the underlying technology standards improving and freely available. Quietly encourage Netscape to call Microsoft’s bluff. Build a bridge to Europe. Or decide the Microsoft case will never end and go join Bertelsmann!

If you’re Jim Barksdale: Take the initiative. Keep working with Firefly/Microsoft and the W3C on user-privacy technology. Then, get all those third-party source-code hackers to help you incorporate it into the next browser release with your own tools and interface, or do it yourself. Make good on your idea of building in a feature that looks for a privacy statement and notifies the user if it’s absent. Thanks, Jim! Though Netscape is no longer independent, it drove the development of LDAP when it did the first corporate version of Navigator. That led to Sun ONE directory, the de facto standard for LDAP directories, and some components of Magic Carpet.

If you’re Lou Gerstner (or Sam Palmisano): Take advantage of your own power. After all, it was you standing next to Bill Clinton at the Framework for Global Electronic Commerce festival (sorry, we mean “announcements”). You can set the agenda both with your own corporate clients and with the public. If you support the Council of Better Business Bureaus, make sure its program is industrial-strength. Come up with a killer ad campaign and take the high ground. Big business is your market, and you’re much more persuasive with them than all those Internet types. Well, individuals just aren’t IBM’s sweet spot, but it’s acting awfully friendly with Microsoft (and has so far declined to join Liberty Alliance). Could it bring the two together?

If you’re Steve Case: You’ve been talking the talk, and even trying to walk the walk. (Your recent internal failures have been embarrassing, but your heart and your policies are in the right place.) Like it or not, you’re a spokesman for the Net. Don’t be shy; use privacy as a marketing message. Or just keep saying: Our users trust us!

If you’re the Word Wide Web Consortium: Hire a good PR guy. Become open and friendly. You operate in the public interest; you control technology (P3P) that individuals could use to protect their privacy, but your organization is hard to reach and your Website is confusing. Remember that openness is not just technical or legal; it’s attitude! W3C did finally come out with P3P, but hardly anyone noticed.

If you’re TRUSTe: Round up some more support, and try to find a bad guy to go after to gain some credibility. Convince businesses that voluntary liability and choice of venue is preferable to mandatory liability and a patchwork of jurisdictions. Start delivering on your promises, and disclose your own practices better. Make up your minds whether you stand for disclosure, or for some particular standards of privacy. TRUSTe really missed a chance at the big time. It now has a large number of sites using its trustmark, but it doesn’t stand for much. Its licensees include the likes of Yahoo! and Doubleclick.
WHAT YOU CAN DO (CONT.)

If you’re the US Administration or Congress:
You’ve sent about as many messages as you can. Finally, the folks are beginning to listen. Sorry it took so long! Be patient for a couple more months without relaxing the public pressure. It will pay off, and then you can devote your scarce energies to more useful tasks, such as fixing the IRS, Y2K, Social Security – and pleading the case for the de-centralized approach (don’t call it “the US approach”) to other governments. If you must “do something,” focus on disclosure and rules concerning kids and medical information. You could also do something about tightening the rules for protection of personal data collected by the government – or reduce the amount collected overall. Yes, the market is starting to work. The big issue now is the data you guys are collecting....

If you’re an accounting, insurance or law firm:
This is a great opportunity for recurring revenues. Build a data-protection assurance practice, fast. Tell your clients they’re at risk, and help them figure out how to reduce the risk. Support the AICPA’s WebTrust program, and get the AICPA to put some teeth into it. Well, maybe not if you’re an accounting firm, but it is a great market for assessing the risks and liabilities of defective identity management – and for consultants and systems integrators. With luck, the SEC will promulgate security-liability disclosure rules, and then you’ll really be in clover.

If you’re an advertiser or merchant; Remember you need customers’ trust; you have to earn it. Your customers do want to tell you (almost) all, but remember your loyalty should be to them and not to other merchants. Don’t sell (out) your customers’ trust to make small change on the side through list rentals or dubious cross-promotions. And don’t be shy about promoting your data-protection practices. (If you rent lists for a living, find another business!) Still true!

If you provide programming services or software:
There are lots of opportunities to build tools and applications around data-protection. Consumers need a way to manage the data about themselves, including passwords, personal information, transaction records and the like. Data gatherers need a way to tag data so they know what they can re-use, under what conditions, and what they must delete after a certain time or after, say, a bill is paid. There are huge opportunities in serving both sides of the market. Also still true! You can find many good ideas to copy... or, extend in this issue.

If you’re Esther Dyson: Publish a newsletter; write a book. Hold a conference. Publish on the Web. Use your bully pulpit to promote the idea of self-organizing governance systems. Because your organization is so small, you have a chance to promote the market without looking like a shill for “money-grubbing marketers.”

If you’re a customer: Educate yourself. Stick up for your rights, and use merchants whose practices you like. Let them know that that’s what you’re doing. Freedom of choice implies obligation to choose, and choose wisely. And now you have a lot more tools and services to choose from. Make your preferences known.

If you’re anyone else: Guess our data-mining tools haven’t found you yet. If you run a Website, get cracking and develop data-management procedures, get your accounting firm to audit them, and post a disclosure statement on your site. Once you’ve gone to all that trouble, you might as well sign up with TRUSTe, because the license is the easy part. If you offer a business-to-business service, encourage your partners, clients, resellers or whatever to sign up with TRUSTe. Market the dickens out of your enlightened privacy policies. Let your Congressperson and the press know what you’re doing.
menting them by controlling access to the applications. Like any manager, it does the key and value-added job of ensuring that the workers do the right work.

The initial benefit of a discrete and comprehensive control-layer tool such as Oblix is its flexibility in defining people’s rights and privileges centrally, for decentralized use just in time. But perhaps the most important benefit is the corollary: When someone leaves, you can cut off access everywhere, to everything, in one fell swoop. (Or you can define a new role – alumnus – which leaves employees who left on good terms with precisely the right kind of lightweight privileges good business sense suggests.) But in reality, of course, Oblix generally coexists with other identity managers . . .

The company has brand-name funding from Kleiner Perkins et al. and a brand-name ceo, Gordon Eubanks, who ran Symantec for 15 years. Co-founder Nand Mulchandani worked in the developer products group at Sun, where he got a patent on his work on the JIT compiler for Java. “And I have been convinced by Gordon three times not to attend Harvard Business School,” he adds.

Authentication: The Big Two (And the Drummer)

Once you’ve put everyone into your directory (or as you do so) and organized all the policies and privileges, the first operating task is to manage authentication – ensuring that a user in fact is the person claimed. Then this individual should get the privileges and access linked to that identity. This assumes, of course, that the record was originally created and verified properly (see page 32).

Authentication is becoming a plug-in task – a separate layer or service. (The trick is to make sure it’s firmly plugged in!) In the past, every repository used its own authentication mechanism. Federated systems, such as Microsoft’s Passport and the Liberty Alliance, tie these mechanisms together, a necessary step for more pervasive identity management (see release 1.0, march 2002 and october 2001).

The simplest, most universal (and amazingly insecure) form of authentication is the simple logon/password routine. That’s what most applications use, what most Websites use, and what Passport uses. The flaws are well known, and we won’t cover them here. But it is worth noting that neither Passport nor Liberty Alliance, as currently conceived, would be suitable for any kind of high-value, high-risk applica-
tions. Without strong verification and authentication mechanisms, many other issues – like liability and non-repudiation – are much tougher to handle.

Better methods of authentication, worth an issue of RELEASE 1.0 in themselves, include the canonical “What you are” (biometrics), “What you know” (passwords, challenge and response), and “What you have” (tokens or certificates). Using any combination of these rather than a single one increases security. Apart from digital certificates, a market dominated by VeriSign, there are lots of interesting new approaches in each of these categories, including 3D face recognition (A4vision, which recently received 4 million Euros in funding from Logitech and Italian VC myQube), user recognition of faces (RealUser passfaces, easy to remember but impossible to write down or pass on), and all kinds of devices that a user can carry, from a SIM chip in a cell phone to an encrypted-sound-emitting card that can be used over phone lines without the need for a local reader (ComSense). [DISCLOSURE: ESTHER DYSON IS AN INVESTOR IN REALUSER AND COMSENSE.] Of course, most people no longer “know” all their passwords; instead, they have them stored on their machines – securely or otherwise.

But for now assume that the original verification/certification has been done properly, and you have a user and an identity firmly linked (though with a measurable, less than 100 percent level of confidence). . . .

Apples and apple trees
Federated authentication basically means single sign-on: If the authentication is shared (or federated), you can sign on once and the information is passed to a different authorization services for each particular resource you try to use. That is: Authenticate once, authorize many times. Other than the user’s identity, no personal information is passed (in the pure form, anyway). Call it meta-authentication, as compared to meta-directory.

There are two big initiatives in federated authentication, though one is an apple and the other is an apple tree (or something like that). Microsoft’s Passport is an operating authentication service, while Liberty Alliance is a consortium of companies developing a spec for how authentication services can interoperate and rely on one another for assertions of identity. Both address corporations who in turn address consumers, though Microsoft also offers Passport directly to users through Windows and its Websites.
The idea of Liberty Alliance is a kind of balance-of-powers notion where all the companies compete to be the customer’s first point of contact, whereas the Microsoft approach simply takes it for granted that Microsoft/Passport is the primary point of contact (for authentication, at least). But in deference to business partners, Microsoft now offers them the ability to run their own identity/authentication server as well (or instead), and for the Passport identities to continue to work. Nonetheless, when a user uses Passport authentication at any site, he clicks on the Passport button, whereas, in deference to its members, Liberty assumes its spec will operate invisibly behind each partner’s distinct user interface. (With its recently announced TrustBridge (see below), Microsoft is back to corporate mode in a big way.)

The big issue is still control of the consumer. The optimistic point of view says that the services below will empower consumers to control their own data and to go where they want. However, Microsoft will make it easier for them to go to Passport partners...which is hardly a sin in a competitive market. Will it be a competitive market? Or will Passport be to the Net (not just.Net) what Windows is to the PC?

In fact, there’s reason to be optimistic. Even Passport pales beside today’s large-scale production authentication/authorization systems such as Visa and Mastercard— which handle not just lightweight authentication for log-ins, but financial transactions, airline reservations and the like. Liberty’s members—as Liberty itself notes—aren’t likely to give up their internal systems in favor of the Liberty spec for anything other than authentication, and they include heavyweights such as American Express, General Motors, AOL Time Warner, Nokia, Citicorp, Sony and VeriSign. What we’re optimistic about is that heterogeneity will win, not despite, but because of all the politicking going on around identity management.

**Passport: Who do you want to be today?**

Passport is the service that made identity management famous. It is based on technology Microsoft acquired in 1998 when it bought Firefly, a rigorously privacy-conscious collaborative-filtering company born at MIT (see RELEASE 1.0, NOVEMBER 1996, FEBRUARY 1998, MARCH 1998 AND APRIL 1998). When Microsoft announced Hailstorm (now .NET MY SERVICES; see RELEASE 1.0, OCTOBER 2001), Passport was the authentication mechanism supporting what would become an overall infrastructure, says Fitzgerald—but for the moment it was a proprietary Microsoft service that everyone was supposed to use, with users’ data behind it. With Hailstorm, the company was thinking about the technology and the customers, it says...but it forgot the politics. “We’re the big piñata,” says Charles Fitzgerald, general manager, platform strategy group.
“Everyone had to have a go at us.” Indeed, a service that would have been inoffensive if launched by some lesser company with little chance of success created a firestorm of opposition precisely because it might actually have gained dominance.

The initial model for Hailstorm was for MSN to be the first operator of the services, with support for other operators to come later. Fitzgerald says, “We went back and said we need to do a generalized platform version that anyone could use to operate an instance of the services. We retrenched a couple of months ago, and got back to a pure platform play of providing software to enable these services.” Nonetheless, Fitzgerald asserts that Microsoft can do authentication 100 times cheaper than almost anyone else – a plausible claim given the 3.5 billion authentications it performs on 200 million Passport accounts per month. (Since the sign-up is so simple and unverified and hard to undo, it’s anyone’s guess how many individuals those 200 million accounts actually represent.)

**Faster than the DMV**

In case anyone doesn’t know (we just signed up ourselves to try the experience), Passport lets you sign up with a minimum of (unverified) personal data. In the end, all you need is a working e-mail address and a password. (You can sign up using someone else’s e-mail address, but then you won’t get the confirmation e-mail with a link needed to finish the process.) In essence, it provides persistent pseudonyms – as many as you want. . .The secure part is the setting of the cookie and the communication from the Passport server to each site as it validates the user’s ID; it is well plugged in. “

In its pure form, Passport is just authentication; it does not assert attributes other than the correspondence between identity and e-mail address,” says Brian Arbogast, the Microsoft vp responsible for Passport. It requests only e-mail/user name, password, zip code, state, and country – and verifies only the e-mail address. “In time, we may strip it down to the barest nub,” says Fitzgerald, “but try to have them better validated.” Think of it as a cheap version of persona management: You can create as many different accounts as you want. Once you’re registered with Passport, you get a cookie each time you sign in that lets you move seamlessly from site to site (the famous single sign-on) based on that single authentication.

Although all Passport handles is authentication, authentication does come in different strengths/confidence levels. Some of the Passport partner sites, especially in financial services, require more stringent authentication – with an additional pass-
“We’re changing the way we think about the application. It used to be bits that run in one machine. Now we have this broader view that the application spans multiple machines, people, services… You used to have one device in your life; now you have many. To make these things work together today, you get to play personal systems integrator. Our goal is to get the technology in your life to work together, on your behalf, under your control. Identity is fundamental to this goal.”

– Charles Fitzgerald, General Manager, Platform Strategy Group, Microsoft

word challenge, for example – or put limits on the duration of a single authentication cookie’s validity. “We have multi-factor authentication today, and we’ll add support for certs and biometrics and smartcards,” says Arbogast.

**Where does Microsoft want you to go today?**

The notion of Microsoft empowering consumers makes sense, up to a point… It is, after all, the company most identified with freedom from the mainframe. While some would argue that we have simply found a new master, in truth all Microsoft wants is our money, while employers and the like want our souls.

“We were more worried about the direct marketing cabal [than about privacy advocates],” says Fitzgerald. “We said, ‘Let the user make an explicit decision about who to give their data to.’ We intentionally turned the dial to save you from the evil marketing people of the world. For example, every vendor in the world would love to be on your calendar. But with this approach, you can decide to let them in, and then if they abuse it, you can explicitly revoke it. It’s amazing how willing companies were to work with this” – perhaps because the vendors Microsoft talked to were reputable ones in the first place. On the other hand, he notes, “the pure direct-marketing guys are very focused on maintaining control.”

At a technology level, he continues, “Passport and services that support it use an opt-in model. This is the user-in-control model. We thought this would be unpopular with marketing companies, but we have been surprised at how many of them actually want to play by a user-in-control model and try to build a long-term relationship with customers who will get enough value to invite those companies into their digital world.”

In fact, the Microsoft approach – where the user controls the account and signs himself up at each partner site, makes sense. Is Passport or one of its ancillary services such as Alerts where we would put our most private information? Probably not. But we would trust such a service to help us manage and control interactions with vendors we selected. Indeed, Microsoft still has to sell its
Passport-based services, because Passport will support other choices as well. It’s not that Microsoft doesn’t want to win, but it actually does look at what users want. It’s what many of us were hoping for years ago: that Microsoft and others would actually market this kind of service!

Ultimately, what’s exciting about Passport is the same thing that draws many people to work for Microsoft: It’s fun to roll out new ideas on a large scale and actually see them used.

**The business case**

The Passport service is free to users. It costs service partners $10,000 plus $1500 per year. “There’s no variable cost today,” says Fitzgerald. “If we get hammered by costs from a particular user we would reevaluate that.”

“No one asks for an identity,” says Arbogast (and everyone else we talked to). “They want a particular service. We go out and we say, we’ve got a service to do alerting, and underneath it is the authentication service. We’re also offering voice-over-IP, and that uses Passport for authentication. There are others coming along, but identity is not a business in itself.” Of course, that has a familiar ring to those who thought identity was a business in itself, and were hoping to make money off it. For Microsoft, it’s just one more part of the infrastructure.

Where Microsoft does hope to make money off Passport is with services that use it, such as My Calendar, and of course Hotmail. It also offers .Net Alerts – a realtime alerting service that can be used, for volume-based fees, by any Passport partner that wants a third party to handle the plumbing of sending out ad-hoc messages to users on vital topics such as delayed flights, plunging stock prices, eBay bidding deadlines and the like. (Meanwhile, the user needs to define his whereabouts (routing preferences and delivery points) only to Alerts, not to a multiplicity of services.) That sounds great if you’re in the business of selling something that requires alerts, but not if you’re in the alerts business itself.

“Passport will encourage federation by becoming a Web service rather than making the federation become like Passport.”

Meanwhile, as part of .Net rather than Passport per se, Microsoft is developing a range of further options around Passport, especially in the area of security. First to come was a set of Web services security standards announced jointly with IBM and VeriSign. Next is TrustBridge – a software suite using these standards that will allow three models of federation: Active Directory to Active Directory, Active Directory to Passport and Active Directory to other systems that support the WS-Security-based federation model. (IBM and VeriSign amongst others are logical candidates to provide such infrastructure.) TrustBridge is very much focused on the corporate market – while Passport is there as a placeholder for a consumer authentication-only service.

Although TrustBridge supports standards such as Kerberos (for security), it puts Microsoft’s own Active Directory at the center of things (although unlike Novell, Microsoft may be able to get away with that approach). And it does not so far support SAML [Security Assertion Markup Language, the XML-like language for making authentication assertions] – which the market seems to be saying it wants. Yet Microsoft is clearly trying hard to play well with the other children. Says Fitzgerald, “We are working surprisingly closely with IBM on all the Web services, and in particular on the security model. We’re pretty aligned there on the standards side, though you’ll see us compete with typical aggressiveness on the product side.”

TrustBridge will include management of profile information and authorizations, and also a variety of Web services interactions that have no authentication/identity component. The real issue it and its competitors will face is not technical, but rather the assumption that companies will trust each other enough to want to create secure shared spaces on a grand scale. (See page 32.)

**Liberty Alliance: Freedom from what?**

Liberty Alliance has 105 members, recently enlarged to include more small companies and nonprofits as well as its original corporate giants (for $1000 or nothing a year, versus $120,000 for “sponsor” members). Its stated purpose is to create a specification for “Federated Network Identity [which is] account federation and federated single sign-on. Account federation enables associating, connecting, or binding a user’s multiple Internet accounts within an affiliated group established between or among commercial and/or non-commercial organizations and governed by some legal agreement.” That is, it lets a user sign on to one account with one vendor, and then move seamlessly to another vendor’s site without signing in again – once the initial links between the two vendors and between the user and each of the two vendors have been set up.
The idea is not to create a platform for sharing personal data, but rather for passing and linking unique IDs and confirming that they have been authenticated. The spec itself, to be released this summer, is basically a set of XML/SAML definitions – hardware, OS, and even programming-environment-independent. It allows a service provider (e.g., United Air Lines) to offer its customers the option of linking their accounts to some other provider, e.g., Vodafone, the European wireless operator. They exchange no profile information, just a link, says Dean. Technically, that link is an entry in a federation table that asserts the correspondence between two user IDs. In a sense, it’s an identity-oriented version of UDDI, the identity standard for Web services. (See Release 1.0, September 2001)

To describe Liberty’s (changing) personality, start with Brian Arbogast’s comment: “When it was announced [in September 2001], Liberty Alliance seemed very Sun-driven, but now there’s new rhetoric. We keep asking ourselves, ‘Is there a way that we can bridge the gap so we could join?’ But joining or not joining, there are lots of ways for us to work together.” Increasingly, both Passport and Liberty Alliance are driven by enterprises rather than vendors…and those enterprises at least occasionally listen to their customers – the users.

Indeed, if neither side insists on declaring victory or what Fitzgerald calls “getting religious,” they can work together without declaring anything at all. In the end, if Passport followed the Liberty spec and supported SAML, almost all it would take is for consumers to decide to link, say, their AmEx accounts to their Passport IDs, and the essential part of “working together” would happen.

Indeed, one has to wonder why a consortium was necessary for such a lightweight spec. But in fact, the spec is probably the easy part. Any two implementations of it may not necessarily interoperate, without two authentication partners defining a joint “federation table” and agreeing on business arrangements. The granular task of deciding what data to share, and under what constraints, still needs to be negotiated case by case – or under general, explicit policies.

“My security architect back at Andersen used to argue with me that in the Internet world you had to design for security first. I resisted, because security is generally articulated as a negative: Keep the unwanted out. But then it occurred to me that if you think positively: Who is this communicating with me and what are they authorized to do? You can think of security – or identity – as the foundational piece of the control logic.”

– Eric Dean, Chairman, Liberty Alliance
The consortium may simply be a good place for all this to happen, and for the IT vendors to get a sense of urgency about supporting the enterprises.

Meanwhile, there’s a third party involved in each case: the user. Indeed, once the technical and business arrangements are reached, each specific link between two vendors should come from a joint customer who went to one supplier or the other and said (by filling out some form or other): “Hi, I’m Juan Tigar, number X and Super-Duper Premium Member. I’d like to give you my Vodafone Hungary cell phone number so you can notify me when your flights are late.”

However, Liberty Alliance does not in fact require this; it leaves these details up to its own customers, who could indeed share and try to match customer lists. In practice, companies who do so will get poor reputations.

**Who sets the rules?**

It might be appropriate for Liberty to set some standard policy regarding the necessity for customer opt-in – where it’s the individual who specifies what records can be linked. Although Liberty has a policy committee, chaired by Chuck Cosson of Vodafone, it fairly explicitly does not want to meddle in its members’ policies among themselves or with consumers. That may be a mistake: We’d venture that consumers are more concerned about whom to trust than about how many times they have to type their password.

Perhaps the ultimate benefit of Liberty and Passport will be to make authentication and data-sharing practices open and visible.

In the case above, for example, it’s not really necessary for Vodafone to know anything about Juan’s flight details, but he might make a similar arrangement with a car service in which he does want Lufthansa to pass on the details. And that could be the real benefit of Liberty Alliance: Pretty soon non-members will be able to use the standard, too, and any two-bit car service that buys standard software tools and has a service agreement with Lufthansa will be able to hook up to specific users’ information within LH’s database…with permission.

The precise authentication techniques are also up to each provider, as is the user interface, says Eric Dean, chairman of Liberty Alliance: “Most service providers have a big investment in developing a dialogue with customers, and you can’t intrude on that. There’s no specific user interface required, and no user software required” –
though, like Passport, these vendors will also set cookies.

**Rock, paper, scissors: Code beats specs**

Liberty’s biggest challenge right now is to come out with its spec as promised, this July. Chairman Dean, who is also CIO of United Air Lines and a Microsoft customer in good standing, professes great admiration for Passport – a working transaction system on a scale that earns respect even from a $16-billion airline. As a CIO, he knows the nitty-gritty problems well. United has a hodge-podge of legacy systems, including everything from a Novell directory for employees, to an internal custom-built customer information database assembled from several internal sources. Indeed, for most of Liberty’s members and their colleagues, federation begins at home, among their own internal databases and often inconsistent records.

“Microsoft has a hell of a huge production system running,” says Dean. “I’m one of their Hotmail users [and thereby a Passport accountholder]. They’ve got my kind of problem! Passport is an operating production system, not just an OS or a piece of technology that they can obsolete next year. One of the great values to me of Liberty Alliance is going to be interoperability with the installed base; it’s just as important as interoperability with new products. The notion that we’re actually competing will disappear.”

Of course, not all of Liberty’s members are user companies, but enough of them are to give the organization a distinctly practical nature. They are focused on implementing something that will work in the real world, with legacy systems. It will bring out its first spec this summer, assuming it encounters no unexpected problems with either technology or intellectual property rights, says Dean. “What we’re doing is not a competitive thing. We’re saying, ‘Let’s design the field where we’re going to play soccer.’”

**…..and Magic Carpet**

AOL does not like to discuss Magic Carpet in public, since it has no announced identity yet. Nonetheless, the code name exists… It covers a collection of products/services that may or may not ever turn into an actual product suite, but if and when they do, most of them will have been in operation for a while, i.e., user-tested! If announced, Magic Carpet will comprise at least some of the identity services AOL already offers: alerts, a wallet (linked to the user’s credit card
Writing about identity for **RELEASE 1.0** is like writing about sex for a medical journal. So it's worth wondering: Does sex education really take the mystery and wonder out of sex? And will “data education” take some of the paranoia out of identity management without necessarily eliminating our instincts for privacy or the wonder of progressive disclosure?

We believe that the coming proliferation of identity management tools and the accompanying marketing efforts will take some of the mystery out of data control (let’s use the clinical term here now). Free content will increasingly acquire registration, whereas paid-for content needs to be paid for somehow – and users will become aware of the trade-offs of freedom vs. free-beer freedom. As users get a better understanding of how all this works – not necessarily the underlying SAML calls but how to allow or restrict the passage of data from one vendor to another by selecting items off a list – they will feel more comfortable and more in control. Users will likely vary broadly in their actual preferences, and they will be able to specify data practices to suit themselves. Some will be happy with conventional notions of privacy; others will have more personal preferences. Some will trust a variety of vendors; others will trust no one at all.

If the US government plays a role at all, it should consider borrowing just two things from our friends in Europe (all the while recognizing that not every vendor operates out of the US): disclosure (in plain English, which is more likely to result from competition rather than regulation), and access/recourse – that is, the ability to see the data a vendor has about you, and correct it if it is inaccurate (yes, that’s a can of worms too). This is not a small subject, but we will leave it at that for now.

### Where the Wild Things Are

But that doesn’t mean that privacy problems will go away. While the use of “commercial” data profiles – with account numbers, valuable data subject to theft, transaction records and the like – may be the subject of the most attention, it is not generally the toughest issue.

Two other areas are more intractable. The first is coerced data. People are generally free to decide whether to engage in commercial transactions, and if they don’t like the data practices involved, they can walk away. But they have little choice when the government asks for information... and now the government and its agencies are starting to ask for access to commercial information (such as travel information, scuba-training records and credit histories) as well as data it collects from individuals in their roles as drivers, taxpayers, schoolchildren and the like. Health care is another situation where individuals have little control over the information they reveal.

And finally, there’s the information generated outside one’s direct control. Lots of companies and people, online and off, won’t necessarily post or abide by rules for data-handling; the world will never be entirely regulated, even though in theory outfits that don’t deliver on the policies they promise can be prosecuted for fraud in some countries. Like it or not, services such as Passport and groups such as Liberty Alliance will have to perform some kind of quality control/governance, and make sure that their licensees operate as promised. Otherwise they will fail to keep their users.

Beyond that, users who post, users who send mail or appear in other people’s cc: fields, users who sign up for special offers, users who blog or set up their own Websites, users who talk in chat rooms, answer online surveys or do almost anything in semi-public, end up leaving a slime trail that attracts dust over time. Some people are also written about, by friends (??) or the press. Google almost anyone, and you can see that slime trail. Ask US Search or other investigation agencies to check someone out (for employment, for credit, or just for personal reasons), and you can find out a lot more – purchase records (and patterns), credit data, mortgages, phone call records and the like.

Although there will never be a single database of everyone, the ability to match identities across databases makes it harder and harder for anyone to keep multiple identities completely discrete. From an artificial, antiseptic neon world of commerce and advertising, hiding a murky, inscrutable secret world of cookies and tracking, we are moving towards a more integrated, more transparent world where the tracking and the trackees are equally visible.

Nonetheless, it’s a central tenet of American mythology that anyone can reinvent himself, escaping a troubled past. Perhaps, as more is known, we will all learn to become more forgiving...
information), instant messaging, and most importantly, AOL’s Screen Name Service which lets users register and maintain persistent pseudonymous identities.

There’s no requirement to be an AOL member to use SNS. Any web user can sign up at http://my.screenname.aol.com. However, all of AOL’s Web properties (as opposed to Web services), including AOL Instant Messenger, Netscape Mail, Netscape Calendar, use SNS as their registration/authentication engine, and most of those are not AOL members. To give an idea of numbers, there are more than 50 million registered Netscape users and 140 million registered AIM users (probably including some duplicates) – all of whom use the SNS for registration. Like Passport, SNS may not be a huge revenue generator in itself (given that no information from it is used for advertising or marketing purposes) but it could enable a wide range of other online and e-commerce activities. For example, SNS users could, in future, sign up for subscription services from AOL partners using an SNS wallet, or register for partner Web sites using their SNS profile information (as specified by the user), or just be more likely to register and complete transactions at partner sites thanks to the easy registration/sign-on process.

There are currently about 45 existing partners (including internal AOL/TW brands) that range from WebMD to TeenPeople, Netscape Mail, CNN, PriceGrabber, CBS SportsLine, Petplace.com and PC World. The Screen Name site lists about another 50 coming soon.

Privacy issues are addressed in the contractual process with each partner, says AOL; it requires partners to have “robust and easily accessible privacy policies that respect the fundamental principles of notice and choice."

In addition, AOL is a member of Liberty Alliance, and SNS will support Liberty: That is, you will be able to sign on via the AOL Screen Name and use that authentication for whatever partners AOL has among the Liberty members (and where you have an account). The SNS is akin to Passport; it is primarily an authentication service that provides single sign-on to multiple services. However, both Microsoft and AOL also store profile information that the user can voluntarily release to partners. In that way, both are more centralized than Liberty Alliance, where any member vendor can hope to be the user’s primary point of contact. And indeed, in the case of Magic Carpet, that is what AOL is trying to do within Liberty Alliance.
Trust and Verification: A Lien in Cyberspace

All the foregoing begs one very simple question: It’s relatively easy to know who someone is by name (authentication). What’s much harder is to know what they are: to assess their track record and the predictability of their behavior – that is, their trustworthiness.

As with authentication – simplicity/scalability vs. robustness – there’s a trade-off for trust. You can trust on the basis of limited information, with higher risk. Or you can spend more time and effort, and lower the risk of a breach (but not the damage if a breach does occur).

In other ways, trust is like privacy. It depends in part on technology – encryption, digital certificates, access management and other tools. For business purposes, privacy results from keeping information inaccessible without permission, and trust results from systems that can confirm the accuracy and integrity of data. Just as control over data leads to privacy, so does sharing of data – and responsibility – lead to trust. Nonetheless, while you can set up and manage the technology, trust is a human condition.

With concepts such as TrustBridge and also Microsoft’s recently announced Palladium, among others, IT companies are trying to construct secure systems that can pass information securely from company to company or context to context. The theory is that this creates a trusted community. But in fact, it simply creates an “inside” – with no particular validation of the trustworthiness (as opposed to identity) of who is inside. The problem is more than just technical support for accepting or rejecting known parties: It’s getting to know those parties in the first place.

In fact, trust does not scale well. Unlike technology and networking in general, trust suffers from a sort of reverse Metcalfe’s Law: Its strength diminishes dramatically for each additional member of the trust network. Likewise, an indirect reference is worth less than a direct one, and so on. (If Juan trusts Alice and Alice trusts Fred, Juan may trust Fred – but not as much as he trusts Alice.)

Thus, ambitious IT systems designed to foster trust may not do so – just as the US government’s post-September 11 proposal to create a large, trusted alternative to the Internet is unlikely to succeed.
**Verification and recourse**

Meanwhile, two factors can support a conclusion of trustworthiness. One is verification – confirming people’s credentials or references, and checking enough of a track record to predict how they will behave. This is an expensive process, and can reach varying degrees of thoroughness.

The other is recourse – having the ability to collect damages or impose a penalty on someone who breaches trust.

Thus, the real challenge and expense of identity management come not from authentication and authorization, which can be fairly routine, but from the verification process beforehand – knowing something of the profile behind the identity when you grant the credentials supporting authorization in the first place. Yes, she’s now an employee, but can you really trust her? How can you verify the person’s claims? When you hire an employee, you have probably done some investigation into her trustworthiness. (Perhaps less than when you add someone you met at a bar to an address book.) When you add a customer, you may check a bank reference. And so forth. Over time, most individuals build up a record – i.e. a profile – and with it a certain amount of trust from institutions with whom that record was created.

The issuers of digital certificates, a market led by VeriSign, generally rely on representations from third parties (or they are the third parties, using technology from VeriSign and its competitors) and they issue credentials in some context – whether it’s an employer taking responsibility for the actions of an employee, a bank taking responsibility for the credit of a customer or a university vouching for the skills of its graduates. The issuers have generally conducted some investigation and performed some confirmation procedures to lower their risks, or they (institutionally) know the parties involved. (By contrast, Passport will vouch for an identity, but precisely because it knows nothing about the person behind the identity, it will vouch for little more. In essence, it vouches for a pseudonym: This John Doe is the same John Doe who came here before, and reachable via the same e-mail address.)
Alternatively, issuers have some contractual way of collecting payment due or damages if the credentialed party proves untrustworthy. An employer can fire an employee, for example, or sue for damages.

**Tucows: A lien in cyberspace**

It’s worth noting that the most widely used “digital certificate” around is a credit card number, representing an individual’s contractual promise to pay his bank, which in turn promises to pay the merchant that accepts that credential. This system has proved remarkably scalable, and works on the basis of finely tuned statistical credit-scoring algorithms. Credit card fees include each bank’s assumption of costs of verification traded off against the risks of untrustworthiness, and those institutions who are best this, such as Capital One, reap financial rewards.

But is there a way to create such a scalable system of recourse independent of financial assets and pledges? That’s the idea behind the credentialing program planned by Tucows, a Toronto-based domain-name registrar, and GeoTrust, a Boston-based vendor of digital certificates. (see release 1.0, October 2000.)

The idea is basically to tie a digital certificate to your cyber real estate rather than to your bank account. This sidesteps the reality that not everyone who is trustworthy has sufficient financial assets to pledge. And it enables an individual not only to build a record of responsible behavior, but also to build a nonfinancial asset that is valuable enough to that individual to be worth pledging as a guarantee of trustworthiness in an arbitrary, defined context.

That is, an individual can pledge virtual “fixed” assets – a domain name. To the extent that individuals are buying domain names and accompanying addresses, they are becoming landowners in cyberspace. Over time, they build up value and the possibility of a lien – more personal and less fungible than a mere charge to a bank account. (The new .pro registry from Register.com is similar in some respects: Lose your accreditation and you lose your right to a .pro domain name. But in this case the real damage is to your accreditation, with the loss of the domain name merely a consequence.) Another example is Square Trade’s seals, on eBay and other sites (see release 1.0, March 2001.)
As real estate goes, a domain name is pretty cheap: $35 US a year is typical. Add to that the cost of paying for a hosted Website and some software, and you’re still in the hundreds, not thousands, per year. (Of course, a person or a business can spend a good deal more than that.) With a little investment over time – and of time – a domain name and associated presence – a Website, a blog, a reputation – can become quite valuable to its owner, just like the home one lives in.

Says Elliot Noss, Tucows founder and CEO: “To start out, we are talking about using these credentials in a limited capacity – mostly around domain-name transfers and the Whois database – where there is currently a big problem with domain-name slamming.” That is, one domain-name vendor steals customers from another, usually by means ranging from outright fraud to sleazy marketing offers that confuse users into transferring their names when they thought they were just paying a bill. By requiring the routine use of a digital certificate plus specific language that makes the transaction clear, participating Tucows resellers could protect both themselves and their customers.

Meanwhile, in a decentralization of the verification process, a reliable customer could build up a record with their domain-name suppliers, who would vouch for the customer to Tucows; Tucows in turn would vouch to GeoTrust, building what Noss calls a “web of trust.” (Note that Tucows is based in Canada, where trust in general is easier to achieve than in many parts of the world.) Somewhere in there we assume the possible presence of an insurance company, which will have checked out the odds and indemnify everyone for a reasonable premium. That would help even out the risks, reassure Tucows’ and GeoTrust’s investors, and help make the system scalable.

Meanwhile, the customer who wants someone to trust him can sign a contract agreeing to behave honorably (in whatever context) and pledging the domain name and related assets for breaching it. The other party can take a look at the Website and the accompanying record of prompt payment or whatever, and decide whether that is sufficient collateral. (In the same way, we tend to trust businesses who say “serving customers since 1945” or “5 million hamburgers served.”)

Although the full service won’t launch until early next year, Tucows and its resellers already have the first stage in place – an installed base of about 3.5 million domain names, whose holders are building up records of reliability with the resellers who serve them – and intangible assets on their Websites. Says Noss: “The larger the user
base and the more ‘mature’ the credential, the greater the external utility. Anything over a million certificates starts to get interesting.”

Obviously, some details, including legal and ICANN issues, remain to be worked out, and the service is not especially proprietary – no more proprietary than a brand name, which also must be earned. In this case, Tucows will need to make its offering easy to understand to all parties and workable in practice. Nor is trust binary: Tucows/Geotrust will probably have to work out different levels of trust and figure out exactly what they are vouching for.

Nonetheless, it’s a start at addressing the big challenge of digital certificates – verification of individuals with no official standing but with some kind of link to the real world. In a world where money shouldn’t mean everything, a domain name – and the related reputation – is a convenient asset to serve as the bond behind one’s word.

<table>
<thead>
<tr>
<th>COMING SOON</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Personal identity management.</td>
</tr>
<tr>
<td>• Grid computing.</td>
</tr>
<tr>
<td>• Large-group collaboration.</td>
</tr>
<tr>
<td>• The standards game.</td>
</tr>
<tr>
<td>• And much more. . . (If you know of any good examples of the categories listed above, please let us know.)</td>
</tr>
</tbody>
</table>
Resources & Contact Information

Kelly Richdale, Artiom Yukhin, A4Vision, 41 (22) 849-1050; kelly.richdale@a4vision.com, artiom.yukhin@a4vision.com

America Online, http://my.screenname.aol.com
Jamie Lewis, Burton Group, 1 (404) 257-4153; jlewis@burtongroup.com
Jonathan Curtiss, ComSense, 44 (7730) 982-554; jonathan@locipartners.com
Eric Leach, Critical Path, 1 (415) 541-2571; eric.leach@cp.net
Mike Serbinis, Critical Path, 1 (416) 408-5250; ms@cp.net
IBM, 1 (888) 426-1001 or 44 (208) 818-4705; analyst@us.ibm.com or analyst-relations@uk.ibm.com
Eric Dean, c/o Michele Cerza, Liberty Alliance, 1 (415) 984-6158; michele.cerza@ketchum.com, http://projectliberty.org (not libertyalliance.org!)
Jim Bodenbender, Madison, 1 (312) 759-5030; jbodenbender@madison-info.com
David Goodman, Metamerge, 44 (141) 423-2844; david.goodman@metamerge.com
Michael Knagenhjelm, Metamerge, 47 (41) 27-44-33; michael.knagenhjelm@metamerge.com
Charles Fitzgerald, Microsoft, 1 (425) 882-8080; charlesf@microsoft.com
Shawn Dickerson, Novell, 1 (800) 453-1267; crc@novell.com
Gordon Eubanks, Nand Mulchandani, Oblix, 1 (408) 861-6800; geubanks@oblix.com, nand@oblix.com
Mary Ann Davidson, Oracle, 1 (650) 506-5464; mary.ann.davidson@oracle.com
Paul Barrett, Real User, (202) 331-7727; paul@realuser.com
Jim Melonas, Real User, (202) 331-7729; jim@realuser.com
Kristian C. Lehment, SAP, 49 (6227) 743-931; kristian.lehment@sap.com
Elliot Noss, Tucows, 1 (416) 538-5494; enoss@tucows.com

For further reading:
Dan Geer, “Federated Identity Management: Sorting out the possibilities,”
http://www.simc-inc.org/archive0002/February02/Speakers/geer-keynote.htm
Brendan Dixon, “Building the Internet Trust Network,”
http://www.simc-inc.org/archive0002/February02/Speakers/dixon/index.htm
Digital ID World, October 12-14, Denver, CO. See calendar.
### Calendar of High-Tech Events

#### 2002

**JULY 15 - 17**

**Burton Group Catalyst North America 2002** – San Francisco, CA
Virtual Enterprise Networks: Embracing the New Reality. An annual three-day event focusing on relevant, critical network and applications infrastructure issues. Register online. For more information call 1 (801)304-8100 or email catalyst@burtongroup.com. www.burtongroup.com/catalyst.

**JULY 20-21**

**ThinkQuest – Exploring the Future of Learning** – Seattle, WA
This ThinkQuest Live Event, in conjunction with the University of Washington and other partners, is a hands-on exploration of today’s most promising emerging technologies and educational ideas and applications, followed by in-depth conversations about their application to future learning. Register online or email Andrea Justham, ajustham@learningspace.org. http://www.thinkquestlive.org/event.html

**JULY 21-23**

**Digital Spectrum** – La Jolla, CA

**JULY 21-26**

**SIGGRAPH 2002** – San Antonio, TX
The 29th International Conference on Computer Graphics and Interactive Technics. The world’s annual gathering of the international computer graphics community, where the digital future is defined and revealed. To register, print out the online registration form and fax to 1(312)321-6876. For additional information, contact 1(312)321-6830. www.siggraph.org/s2002.

**JULY 22-26**

**O’Reilly Open Source Convention** – San Diego, CA
A central gathering place for the open source community. Register online, or call Andrew Calvo, 1(707) 827-7176, or by email andrewc@oreilly.com. www.conferences.oreillynet.com/os2002.

**SEPTEMBER 9-12**

**IDF Fall 2002** – San Jose, CA
Intel Developer Forum is a year-round program including multiple worldwide events for hardware and software developers. This year’s second US Conference features four days of technical sessions, keynote speeches, and various leaders and experts. For information contact Wendy Laugesen, (650) 372-7968, or email wendy.laugesen@key#media.com. http://intel.com/idf/us.

**SEPTEMBER 9-13**

**Networld+Interop Fall 2002** – Atlanta, GA
The data networking industry’s semi-annual showcase of the newest gear. Details on the Web at http://www.key3media.com/interop/lv2002/.

**SEPTEMBER 18-20**

**DEMOmobile - Unwiring the Planet** – La Jolla, CA
DEMOmobile is the annual conference that focuses exclusively on products and technologies shaping the mobile and wireless marketplace. Register on line. For information, contact Lavayne Harris, 1 (800) 633-4312, or + (650)577-7801 (outside the US), or via email at registrar@idgexecforums.com www.idgexecforums.com/demomobile.
Calendar of High-Tech Events

SEPTEMBER 23-25  International IT Service Management Summit – Boston, MA Dedicated to educating IT and business executives on how standardized processes and best practices can be applied across IT support and delivery functions, to deliver superior services while reducing risks and managing costs. For information, contact Juliet Sigmann, jsigmann@internet.com, call 1(508)870-5858 or register online. www.itsmfevent.com.

SEPTEMBER 23-25  eBusiness Integration Conference Series – New York, NY BrainStorm and Giga Information Group have joined forces to co-produce the 2002 eBusiness Integration Conference Series. For information, email Linda O’Donnell at info@brainstorm-group.com, or call her at (1 508) 393-3266. www.brainstorm-group.com.

SEPTEMBER 24-26  Privacy2002 – Cleveland, OH This year’s theme is Information, Security and New Global Realities as participants try to bridge the gap between the needs of business and government, and the concerns of consumers and privacy advocates. Register online, or contact Sol Bermann 1(614)688-4578,bermann@osc.edu. www.privacy2000.org.


OCTOBER 9-11  Digital ID World Conference 2002 – Denver, CO “Identity Crisis: Taming the Network” is the theme of the first major event designed to drive the emerging digital identity industry. Register online or email sales@digitalworld.com for more information. www.digitalidworld.com/conference/2002.

NOVEMBER 3-5  EDventure’s High-Tech Forum – Berlin, Germany Save the date for our 12th European conference! For details, call Daphne Kis, 1 (212) 924-8800; fax, 1 (212) 924-0240; daphne@edventure.com; www.edventure.com.

Events Esther plans to attend.

Events Kevin plans to attend.

Lack of a symbol is no indication of lack of merit. The full, current calendar is available on our Website, www.edventure.com. Please contact Irene Lawrence (irene@edventure.com) to let us know about other events we should include.

---

**Release 1.0 Subscription Form**

Complete this form and join the other industry executives who regularly rely on *Release 1.0* to stay ahead of the headlines. Or if you wish, you can also subscribe online at [www.release1-0.com](http://www.release1-0.com).

Your annual *Release 1.0* subscription costs **$795** per year (**$850** outside the US, Canada and Mexico), and includes both the print and electronic versions of 11 monthly issues; 25% off the cover price when you order from our online archives; a *Release 1.0* binder; the bound transcript of this year’s PC Forum (a **$300** value) and an invitation to next year’s PC Forum.

**NAME**

**TITLE**

**COMPANY**

**ADDRESS**

**CITY**

**STATE**

**ZIP**

**COUNTRY**

**TELEPHONE**

**FAX**

**EMAIL**

*personal email address required for electronic access.*

**URL**

☐ My colleagues should read *Release 1.0*, too!

*Send me information about multiple copy subscriptions and electronic site licenses.*

☐ Check enclosed  ☐ Charge my (circle one): AMERICAN EXPRESS MASTER CARD VISA

**CARD NUMBER**

**EXPIRATION DATE**

**NAME AND BILLING ADDRESS**

**SIGNATURE**

Please fax this form to Natasha Felshman at 1 (212) 924-0240.

Payment must be included with this form. Your satisfaction is guaranteed or your money back.

If you wish to pay by check, please mail this form with payment to: EDventure Holdings, 104 Fifth Avenue, 20th Floor, New York, NY 10011, USA. If you have any questions, please call us at 1 (212) 924-8800; email us@edventure.com; www.edventure.com.