IDENTITY MANAGEMENT

by Jerry Michalski

The topic of identity — personal, organizational and national — plays a starring role at this year’s PC Forum, which has the theme “Let’s Be Clear: Identity, Transparency and the Net,” and is just over a month away. Among other things, Forum speakers and panelists will address what identity is, how it comes into being, how the Net changes it, where identity information is kept, how it can be hidden or broken, and how it can be derived, marketed and manipulated.

This month’s Release 1.0 is a warm-up for the Forum, as well as a follow-up to two issues we wrote in the spring of 1996. That April, we discussed online identity from a sociological perspective, covering people’s expectations about identity in general and the features and behaviors that help determine identity online. The following month, we described the ways that people make their identity visible online by choosing, customizing and using avatars and gestures. In February 1997, we discussed personal data and control of it.

This month, we turn first to some of the technological solutions to the problem of identity online, especially digital certificates and the infrastructure and education needed to make them work. We cover several companies who certify identities or act as trusted holders and dispensers of identity and profile information, including VeriSign, ValiCert and Firefly Network.

We conclude by exploring new business opportunities that may resolve some of the complexity of identity management between certificates, directories, contact-management software and other players who collect such information.

TECHNOLOGICAL SOLUTIONS

Modern cryptographic technology offers a variety of ways to create and protect online identity and protect data. Most of the systems described in this issue depend on it. Unfortunately, crypto is like tofu: By itself, it is formless, tasteless and generally unpalatable to the public, yet it has myriad uses. What it becomes depends entirely on the ingredients someone adds. There are other parallels. Both must be kept fresh to be useful, and their

WELCOME, TRISTA AND PHILENA!
creation is shroud-ed in mysteries understood only by a few specialists — or anyone curious enough to find out.

Depending on how it is used, cryptography can protect privacy; afford anony-mity; authenticate persons, objects, servers, routers or services; guarantee non-repudiation, integrity and more. These features are not isolated from one another. In combination, they can turn into a variety of dishes, each useful in different ways.

Most of the features that certificates and other technologies can pro-vide mirror cues and guarantees that are available to us in the real world, in varying degrees of confidence. Wax seals and signet rings have given way to private transaction networks, bonded couriers, tamper-proof envelopes and digital certificates. Various physical credentials are the traditional signposts of trust. Certificates are their digital counterparts.

In real life

Personal introductions are a generally reliable guarantee of identity. Once you've met someone, you rely on recognizing that person's face in meetings, voice on the phone or handwriting in letters or signatures. Context offers many cues, too. Meeting a guy named Jimmy in a dark alley to discuss a private loan is different from getting a business card from "Mr. Maxwell" at the loan desk in a bank with big columns out front. Granted, some of Mr. Maxwell's environment and manner is a dis-play intended to project con-fi-dence, and nothing guarantees Maxwell won't have higher rates than Jimmy. On the whole, though, our cues guide us well.

But those cues are missing in cyberspace. Most digital denizens' visual vocabulary includes little more than the tiny key or lock symbol that high-lights or "locks" when they have a secure browser connection. Microsoft has done good work developing Internet "zones" that collect sites and resources with similar risk profiles from the user's perspec-tive, but these concepts seldom make it to the interface. They are in the background, out of sight.

What are the semiotics of trust online? What visual cues will indicate that a document is the right document? That a person is who she claims to be? A certificate can be as easy to obtain as a Safeway card or as difficult as a top-secret clearance. How will people know where cer-tificates fall in the trust hierarchy? The problem of identity and authentication online has many variables and many participants, which makes it hard for anyone to create a consistent visual vocabulary. It's important to identify which issues are serious and which are trivial.

How will Zoe know that "Phil" in the chat room is really named Phil, much less whether he is someone she should meet in person? Perhaps some symbols can attest to his veracity. Or maybe, like the ginger questions that dating partners ask at some point about each other's dating histo-ries and habits, Zoe and Phil just have to talk about these things and take risks. Some things will be hard to guarantee or make explicit. Others, such as whether a bank or ATM can be trusted with your deposits, are more straightforward.
Online cues

As in real life, the cues we use online to know things are what they seem (or claim) to be will be subtle and varied. That doesn't mean there should be many different cues from different sources, but rather that there are many things to assure, which will require a variety of online cues. The only way end-users will know what is going on is if these cues are used consistently by all Net applications. If every municipality used a different convention for traffic signs, there would be many more accidents.

Online cues will be either generic or branded. Internet Explorer, Communicator, Notes and Eudora all have examples of generic symbols (though each uses its own today): the small ribboned seal icon next to an e-mail message that tells you it was signed digitally with a certificate; the lock or key icons that indicate when you have a secure Web connection (without a certificate).

The branded cues are the ones many people use today to determine whether they trust a store or restaurant, including simple things like credit-card stickers on the front door.

Where will they come from?

Today, people already send a lot of e-mail that isn't encrypted or signed. They also buy things from Websites without the benefit of certificates. Why get a certificate at all? In fact, individuals probably won't get and install certificates on their own. They will get certificates from others.

Employers will issue their own certificates and install them in users' machines. Users will occasionally manage the certificates in the "User Setting" or "Preferences" dialogs in their applications or operating system. Ideally, they should seldom have to interact with certificates and then only to approve variations from preset rules that handle most of their secure interactions.

Branded certificates will show up as enhanced features from the major trust, transaction and identity purveyors, such as credit-card issuers, couriers, notaries and insurers. Your next credit card may well include a smart chip that includes a pre-issued certificate. This is likely to be the primary way people receive certificates, unless certificates become a default element of either browser installation or the PC purchase itself.

Individuals aren't the only market. The majority of certificates are likely to run in the background, behind the scenes, as servers and applications authenticate one another with certificates. Before we go too much further into the uses of certificates and the companies that provide them, here's a brief primer on digital certificate technology.

Certificates 101

There are two basic types of encrypted communication systems: secret and public key (most keys are based on prime numbers whose product is large enough to be extra-ordinarily difficult to factor, which is what makes crypto systems secure). In secret-key systems, a pair of identical keys is generated for each secure relationship; both parties hold the same secret...
key. If either party compromises the key, security is lost. Because these keys have to get to both parties, secret-key systems require additional secure key-management infrastructures.

In public-key systems, each participant has a public key and a related but different private one. The public keys can be distributed in the open. Knowing the public key doesn't give another party the power to impersonate its owner. However, she can use the public key to encrypt communications that only the holder of the matching private key can decrypt.

Most of the systems described in this issue use public-key cryptography. The major US supplier of commercial public-key cryptographic technology is RSA Data Security, followed by PGP (Pretty Good Privacy), which is now part of Network Associates.

Certifiable

Certificates bind public keys to other information about the keys' owners, usually to attest to certain facts about the key holders, such as their status as an employee, citizen, good credit risk or dutiful book returner. The certificate contains the public key, which is mathematically linked to the holder's private key; it is signed with the private key of the certificate authority.

Individuals will probably have multiple digital certificates that reflect their many roles and relationships, as well as the brands and privileges that the certificates represent. One may be linked to their private-life identity for sending personal e-mail, another may give them secure access to specific Websites and yet another may link them to their financial institution for transactions. A few of these identities will be public, but many of them will be hidden from view.

Any certificate issuer (also called a certifying authority or CA) can offer several levels of authentication. Some certificates may be issued with little proof of identity, the way library cards are issued; others may be issued only after in-person appearances, biometric recordings (see box, opposite) and deep reference checks.

Certificates can be issued on demand with no proof of identity except an e-mail address. These certificates are used for pseudonymous interactions. You may not know the other party's identity, but his certificate lets you know it's the same mystery person.

Chains and hierarchies

Certificate issuers also attest to one another's ability to issue and safeguard certificate information. This data is often included in certificates, and forms a chain or hierarchy of certificates. At the head of this chain is the root certificate, which is guarded zealously inside hardware systems designed to destroy whatever information they contain if someone tries to tamper with them. If the root certificate issuer is compromised, the entire chain of entities predicated on it is jeopardized. On a much smaller scale, if an individual certificate has expired or been tampered with, it won't work.
Organizations can issue their own certificates, which is a good way to delegate the task of issuance and grow the use of certificates. Even though they issue certificates, companies may outsource the actual generation and management of the certificates. It depends whose technology they use.

Making really sure: hardware and biometrics

As long as private keys and other important information are stored on media that are relatively easy to compromise, such as hard disks, there is always an element of doubt about whether the keys have been compromised. There are two common ways to be more certain that they haven't. The first is with a physical object such as a tamper-proof smart card or ring, which replaces the hard drive in the example above; the second is through physical identification of the user, which replaces the password. Both options offer a robust second layer of protection.

Hardware-based systems are useful only if they are nearly impossible to replicate, if their users report thefts as soon as they take place, and if that leads to immediate revocation of certification. Cards or other devices also require scanners (or readers) wherever they are to be used. It's unclear now what form factor for physical security devices will be most popular in five years.

Biometric systems don't require people to carry anything. They're also pretty foolproof. (Yes, we've heard the grisly stories about fingers being cut off to pass fingerprint-ID systems, but many modern systems actually measure the finger's temperature or look for a natural pulse.) Biometric systems measure and recognize many kinds of unique patterns, from fingerprints to voices, images or retinas and irises, and even DNA. Each is useful under different conditions. In the best action-adventure movies, the hero sits in an escape-proof chamber while the system scans his eye and finger, challenges him with a random question and validates his super-secret ID card.

In less demanding environments, voice recognition could allow access to privileged information with an ordinary telephone, although such a setup would be relatively easy to crack. Retinal scanning is nowhere near as portable, but it's highly reliable. Small, reliable and inexpensive fingerprint-recognition systems now under development should make laptops and the data that live in them safer soon.

Mix and match

It's important to note that certificates can identify much more than people. They can also identify documents, servers, services and more, making certificates a core technology for electronic commerce.

Certificates have many uses, particularly in combination with encryption systems and third-party services. Different combinations could verify — within the limits of the technology and service used — that:

* the person you're dealing with is who she claims to be;
Ease of use: Still a goal


Unless these features get much easier to explain and understand, they won't provide the benefits they promise to the general population. The challenge is to simplify this mess. Ideally, certificates should fade into the background. They should be present but invisible. Early results are mixed. Major software suppliers such as Microsoft, Netscape and Lotus already support digital certificates in their browsers, servers and e-mail clients. Lotus Notes was designed with strong security. For years, it has offered many powerful security and authentication features between Notes users.

Unfortunately, Notes isn't any better than the other applications at managing trusted communications with non-Notes users. Sending signed and encrypted messages is getting easier, but receiving them isn't. In Netscape Communicator's e-mail client, for example, messages with certificates show up in black, with a note that there is a "problem" with them. To open the messages, you have to sort through dialog boxes and follow too many cryptically worded instructions. Among those instructions are important decisions about which certificates to accept automatically in the future that might set you up poorly for a long time.

Weak design seems to be the common theme in software that uses certificates. There is clearly a lot of power at hand here, but to find broad use, software that uses certificates will have to be crafted more carefully and explained more simply.

The issue is broader than just certificates. It also covers other technological advances that promise to reduce a lot of information friction and make people's lives easier, such as HTML e-mail, electronic calling cards and calendar event-exchange protocols (see Release 1.0, 9-93).

In particular, Microsoft and Netscape, the two companies that currently own the software interface that most people will use in the future, have failed
to create clear migration strategies to ensure that these items are easily understood and find broad use. For example, if you send HTML mail to a person whose e-mail client software can't deal with it, she will generally receive a double message: The text will show up once in plain text, then again with all the HTML markup visible — an annoying side effect. This doesn't affect only people without the feature: Those who have it have to keep track of who can and cannot receive HTML mail, and change their authoring behavior accordingly. It's too much to worry about, so many people revert to plain-text e-mail.

Glitches like that have many causes, most of which have to do with old standards meeting new, not bad programming. Yet there is a special educational role that none of these companies has stepped up to play. There is a great deal of missionary work to do alongside the rapid-fire evolution of user-interface designs. The sooner features such as HTML mail and certificates are commonplace, the sooner developers will be able to turn their attention to simplifying larger portions of our computing and communication infrastructure.

The issue of interface design plagues all of the efforts to create identity-management systems that we are about to describe. We take this as an indication that this is still a young industry, and we hope that it will improve markedly — and soon.
VERISIGN: GET YOUR DIGITAL CHOP

For thousands of years, people in Eastern cultures have used chops — personalized stamps carved in wood or stone — as marks of identity, much as Western cultures have used signatures and signet rings. Stone and paper don’t travel well through data networks, so these modern times require electronic equivalents.

VeriSign, founded in April 1995 as a spinout from RSA Data Security, is currently the principal issuer of chops for cyberspace. With these digital certificates (VeriSign calls them Digital IDs), individuals and companies can sign messages, documents, applications, services and more.

When corporations want to issue their own certificates, VeriSign licenses them front-end software that allows them to configure and run their own CA, but it still generates the certificates on its own servers. Companies that want to bring the whole process in-house can purchase certificates from VeriSign’s competitors, such as Nortel subsidiary Entrust Technolo-gies and GTE Cybertrust.

Since it began issuing certificates in the third quarter of 1997, VeriSign has issued over 2 million IDs to individuals, plus over 40,000 enterprise certificates.

The bumpy ride

If you are an employee of a company that uses Digital IDs, you will end up using them some way or another. As we mentioned earlier, they will be generated for you, assigned to you and installed in your systems. But getting one voluntarily is no simple matter.

Even figuring out whether you want to get one at all is difficult. The demo on VeriSign's site requires that you get and install a Digital ID in order to see what it can do for you. If you're not willing to take however long that might take (it doesn't say) and risk messing up your system, you’ll have to piece together what you can from text around the site. There's no mockup or walkthrough emphasizing the steps and the benefits.

For people who “walk” in off the street, VeriSign offers two kinds of Digital IDs: A $10-a-year Class 1 ID (a free, less-powerful version is available now for a short introductory period) and a Class 2 ID for $20 a year. The Class 1 ID gets you a unique registry in VeriSign’s repository, lets you use certificates with Web browsers and e-mail, and offers $1000 protection from economic loss underwritten by USF&G.

The Class 2 ID requires you to submit more information about yourself and checks that information against Equifax’s database. The Class 2 ID has the same features as Class 1, plus $25,000 in coverage. Potential added functionality includes password replacement, software validation and online subscriptions.

Class 3 IDs are for servers and include proof that the server has the right to use a particular organization’s name, encrypted communications and a $100,000 NetSure warranty.
What to choose?

Before you get to added benefits, you'll have to get past some simple design problems in VeriSign's Web registration process. For example, the process also forced us to choose which browser to get a certificate for (a browser compatibility problem that affects VeriSign's functionality) and what cryptographic service provider to use. Don't people have enough trouble figuring out what Internet service provider to use? After we submitted the registration form, the system replied that we shouldn't have put spaces in the credit-card field (there was no example to follow). When we clicked the button to go back to the form again, all of the information we had entered was gone. Small stuff, but each barrier keeps potential users out.

After receiving a confirming e-mail message from VeriSign and getting the ID installed, we realized that there is room in the system for us to have multiple certificates and to choose which ones to use for different occasions (we hadn't had our morning coffee yet and we were taking the Website literally). Although that feature promised future excitement, it also introduced some confusion. Finally, we went to the VeriSign ID test page and were told our ID was in working order... but for what?

We would also have liked to know how to tell if our certificate had been compromised and what to do in that situation. Many of these doubts and questions come from lack of familiarity with the process and its outcomes. There's clearly plenty of need for education.

Would you like a cert with your fries?

One of the ways that VeriSign is marketing the benefits of Digital IDs (and begin to establish some brand presence) is with a list of VeriSign Authentic Sites, which now numbers over 2000.

One of the principal ways that VeriSign Digital IDs will get propagated quickly is by piggybacking on other Websites' and Net services' registration procedures. For example, today, when you register for Netscape's Netcenter, you can also get a VeriSign certificate. Expect to see many more such arrangements. Also, many certificates will be included transparently in other interactions, such as getting a smart credit card.

Last December, VeriSign closed $30 million in private financing from strategic partners including Cisco, Comcast, First Data, Gemplus, Intuit and Microsoft (the first round of funding was $10 million). These companies are building VeriSign technology into a variety of systems, primarily for electronic commerce.

Earlier this month, VeriSign made a well-received initial public offering. Opening at $14, its stock rose to over $30 and has remained there in the few days since. With the IPO behind him, VeriSign's president and CEO Stratton Sclavos (formerly at Taligent and MIPS) can focus some attention on the many small things that will help make Digital IDs as ubiquitous as he would like them to be.
There are many circumstances in which you would want to revoke a certificate in a hurry. The obvious ones are when you lose your secure ID card or you fire an employee and want her access privileges stopped immediately. As long as the number of people using certificates is relatively small, it's relatively easy to create a flat file that contains all of the revoked ID numbers (called a Certificate Revocation List or CRL). Any application can check the file before checking the certificate itself.

However, the flat-file approach is relatively slow and doesn't scale well. It also runs into problems when certificates cut across corporate boundaries. Corporations are unlikely to allow other companies to read such sensitive files inside their firewall or even outside in any place that might be compromised.

To solve this problem, ValiCert created a high-performance revocation architecture that is effectively a clearinghouse for certificates. At its core is a carefully crafted hashing routine designed by Paul Kocher, the company's chief scientist, and Chini Krishnan, the company's founder and cto. Kocher developed the cryptographic elements of SSL (Secure Sockets Layer) and used a timing attack to crack the RSA algorithm and others. The hash algorithm lets the system grow large Certificate Revocation Trees, yet delivers very compact and hard-to-crack codes that represent the results of a ValiCert check.

The system scales non-linearly, allowing it to cover trillions of certificates without significantly increasing the speed to process queries or the size of the validation code. The codes are typically 600 to 800 bytes long, depending on the size of the list of revoked certificates. ValiCert creates these codes by collecting CRLs and other relevant revocation data from participating certificate authorities.

ValiCert licenses Enterprise Validation Servers to customers to add to their existing certificate servers. If the companies wish to use the revocation with partners outside their firewall, they can use the Validation Servers to periodically synchronize their list of revoked codes through ValiCert's Certificate Validation Service, a distributed server hierarchy based on a central Certificate Revocation Tree that ValiCert maintains.

Companies don't have to license the enterprise server to participate in the ValiCert system. They can synchronize their revocation information with a simple server plug-in.

Freshness guaranteed

ValiCert's system can also help reduce network traffic related to assurances. Given the number of certificates that might be part of a transaction, there could be an order of magnitude more traffic generated by overhead to make sure that the transaction elements are authentic than the simple transaction itself. One way to cut down on that traffic is to use freshness certificates, which state that various elements are trustworthy as of a particular point in time. If you trust the issuer of the freshness certificate, you can trust the transaction.
To be successful, a revocation system has to be as ubiquitous and inexpensive as possible. ValiCert is already working with several issuers of certificates to make sure that it can interoperate with them. It is also pricing its service reasonably. Corporations that want to use the ValiCert toolkit to enable their applications to work with the ValiCert system pay only $1000 per application per year; the Certificate Validation Server costs $10,000.

ValiCert already has agreements with BBN Planet, Entrust, GTE, Entegrity Solutions and Netscape to incorporate its technology in their systems, but they are just a start. Other partners include Baltimore Technology, Thawte, BelSign and Xcert. In order for ValiCert to thrive, certificates have to become enormously popular.

There is much more to managing identity than getting a digital certificate and knowing whether it is valid or not. What about payment information, personal preferences and demographic data? What about information that is more dynamic, such as where you are and what you're doing right now?

**FIREFLY AND YOUR PRIVATE INFO**

To average Internet users, Firefly Network is probably most familiar for its music-recommendation Website based on collaborative-filtering technology. Not for long. All along, Firefly has worked on systems that track, maintain and share user information, while it participated in key public-policy development groups related to the rights and uses of such information. Now, with viable online privacy standards emerging and new networking capabilities available, Firefly is breaking trail in the important application area of identity management (see Release 1.0, 2-97 and 11-96; disclosure: Esther Dyson is an investor in Firefly.)

The Firefly Passport gives users an application with which to control their personal information, such as bookmarks, demographic and contact information, and payment details, and can dispense it selectively to other parties when authorized to do so. For example, Barnes and Noble could offer a Passport user an extra 10 percent discount in exchange for registering at its site or answering a detailed demographic questionnaire. The user could accept the offer and complete the transaction by hitting one button. It makes sense: Why retype your billing and mailing address or take yet another survey if your Passport has all that info?

That example benefits mostly the Website requesting information. The Passports get interesting for users when companies that support Passports band together into networks, which involves running Firefly Passport Offices, linking them up through Firefly's central hub, which acts as the intermediary, and adhering to Firefly’s privacy policy.

A Passport Office costs $15,000. It can recognize visiting Passport holders and can issue new ones to people who don't have them, as well as support privacy policies and link to other Passport Offices. Firefly’s Catalog Navigator, which helps publish Web catalogs as well as do collaborative filtering, is $25,000 per server. It connects to the Passport Office, where it can benefit from all the information that users have released.
Companies in the same Passport network should be able to treat customers better and more consistently. Passport users can login once at any of the sites and have their identity information preserved as they travel to other sites in that network. If given permission, the Passport sites can also avail themselves of user-preference information derived by the collaborative filtering capability or stated explicitly by users, in addition to standard profile information. There are two levels of permissions. The information can be shared only if the individual users and their host Passport sites agree to release it.

In use, the current Passport pops up as a small, menu-less browser window that can float above your normal browser. It has buttons that can take you to different parts of the Passport service, which includes messaging, notification that your friends are online and profile information – all features that Firefly's recommendation system already had. Other buttons take you to other Websites.

In which we take the test drive...

Firefly calls this combination of services “networked personalization with privacy.” Customers that use Passports should get more things they want, more conveniently. At least that's the way it's all supposed to work. In practice, it's not quite that easy. Although the Passport is a few weeks short of supporting privacy policies or offering easy mobility, we decided to test-drive it anyway, as other curious passers-by might.

We started our Passport by visiting Firefly's site, logging in (having registered there in pre-Passport days) and hitting “Click here to launch your Passport.” The small Passport window popped up; so far, so good. Then we visited the Barnes and Noble site, which is featured on the Passport as one of Firefly's Passport partners. Nothing happened. No signs of Passport activity. If the site hadn't been set up to handle Passports yet (which was true and quite understandable), it should probably have been left off the Passport buttons. Its presence there implied more than it should have and left us puzzled in what was billed as a demo of Passport utility.

So we headed for MyLaunch, another site highlighted on our Passport, and it did invite us to enter our Firefly Passport name and password – but hadn't we just entered it? When we did type it in, MyLaunch told us that our name and password didn't match the ones we had just used to bring up our Passport and wouldn't log us in. Drat. A visit to another affiliated site, My Yahoo!, took us to a Firefly-driven Website recommendation system interface, but the site gave no indication that it knew about us or the Passport. Sigh.

BostonEats.com, billed as the best demo site for Passports, rejected us the way MyLaunch did. It looked as if nothing else had happened, but the small Passport browser window, now obscured behind the BostonEats site, did seem to know we were visiting BostonEats. Unfortunately, following its instructions didn’t log us into the site, either.

Despite these shakedown problems, we're fans of the Passport idea, and we can't wait to see it work transparently.
Better living through acronyms: OPS, P3P and ICE

In early 1997, Firefly developed the Open Profiling Standard (OPS), a relatively simple information-exchange standard based on the vCard spec. OPS allowed for the trusted exchange of profile information while protecting profile owners' privacy. Firefly's main objective in creating OPS was to improve Websites' personalization capabilities without violating their visitors' or members' privacy.

At around the same time, the Internet Privacy Working Group (IPWG) began to develop the Platform for Privacy Preferences (P3P). P3P extends the Platform for Internet Content Selection (PICS) standard with notice and consent capabilities to enable automatic negotiation of preferences, policies and information exchange. If P3P settings are accurate, Web surfers should be able to surf at will, and see P3P notices only as they stray out of bounds of what is already approved in the profile.

P3P and OPS have common goals, but P3P incorporates a higher-level grammar to facilitate negotiations and other more complex activities. A few months ago, the P3P and OPS working groups unified their projects; the governing term is now P3P (see Release 1.0, 2-97). Today, Firefly Passports manage simple profile information; soon they will include electronic payment information, richer profiles based on P3P and more.

Enter ICE

P3P addresses communication between users and sites. Now, with Vignette, Microsoft, Sun and others, Firefly is helping create an XML (eXtensible Markup Language) specification called ICE: Information and Content Exchange.

ICE will add structure and semantics to the kinds of information that commercial Websites in an alliance might want to exchange regularly, including (but by no means limited to) P3P content. By adhering to the ICE spec, companies will be able to strike such alliances more easily. It'll be a business decision, not a major integration project. For example, Vignette is building site-syndication software designed around ICE that it has code-named Site-To-Site.

Saul Klein, Firefly's senior vp of brand and strategy, hopes that the company's aggressive involvement in developing these standards and in creating networks of Firefly client sites will give it a significant head start. He also wants to establish Firefly and its clients as well-known assurance brands in cyberspace. More powerful semantic content, better negotiation grammars and trusted brands will together help cyberspace citizens overcome the various doubts and risks of doing business online.

Honey, I shrunk the certificates!

When Firefly first launched its music-recommendation site, some Passport-style information existed in members' Web pages or in the Firefly server. Over time, that information has started moving from the server to the desk-top, where the new Passport floats above whatever you are doing. One of Firefly's next initiatives is to move this information to the pocket. Imagine this information on smart cards or affinity cards that let you plug in anywhere and be treated better.
A final note about interacting with other members through Firefly that also
dates back to the original Website: When members would log into the serv-
iece, they would see a list of member names that had logged in just before
them across the top of the screen. At the time, this was a simple and
clever way to show that other people were around, too, and it helped make
Firefly a social, personal experience.

One of the reasons we're so enthusiastic about buddy lists is that they
give a much better sense of presence than seeing names on Web pages, even
if the environments are the same in both cases. Seeing a picture of a
tech-support person on a Web page with a caption underneath that says, “Let
me know if you have any questions” gives us far less sense that someone’s
around than having a name pop onto our buddy list explicitly labeled as a
tech-support person — as long as we've allowed that to happen, of course.

SHORT SUBJECT

Clearly, all this information about people is valuable to someone. So
valuable, in fact, that it is becoming a strategic asset. Companies are
beginning to consolidate and ally around directories. The question needs
to be asked from the individual's side, though: Who should hold your iden-
tity information? Direct marketers? Directory services? Financial insti-
tutions? Communication service providers? Whom can you trust? How can
companies develop this trust?

All that data

There's a pragmatic side to this issue, too. Databases, electronic
orga-niz-ers and other gadgets are replacing paper Rolodexes, albeit slow-
ly. We can now scan business cards and get reasonable results from OCR
(Optical Character Recognition) software. Sometimes, though, the work we
must go through to collect contact information about others and put it to
work gives us nostalgia for the days of paper tools. Life is full of dou-
ble- and triple-entry of data, or awkward exports and imports, never mind
endless de-duping of lists. Nothing talks to anything else. Isn't there a
better way to keep this information?

Four11, WhoWhere? and other large directories already have many people's
names and addresses, though they're all too often woefully inacc-urate. So
do the major credit-card, credit-rating and long-distance compan-ies, and
others that have national and international customer bases. When different
people refer to one individual, they need access to the same information,
plus some custom information of their own. They also want se-curity:
Nobody else can know that that person is their customer, and so on.

Of course, it's heresy to suggest that any company would put its most valu-
able asset — its client list — outside its walls. Nor are we big fans of
centralized, monolithic databases. Yet we can't help but feel that there's
an opportunity here for one company to stake some central ground.

The key is to create dynamics that motivate people to keep their own infor-
mation fresh. It's not all that difficult to do. For example, if we knew
before undertaking a household move that our (paper) magazine subscriptions
would be changed sooner and all together by registering at such a ser-
vice, we'd be there in a minute. If it also helped us block paper and electronic junk mail, it would score bonus points.

Human-resource departments have discovered that employees are motivated to keep their own information up-to-date. Employee self-service applications also save the time and expense of data entry.

On from there

That's just the start. It's easy to brainstorm dozens of functions we would want to perform with up-to-date, custom-enhanced address information. Depending on how intimate or frequent our association with different people are, we would want to maintain them in our mailing list on someone else's server (a task we would happily outsource) or synchronize them with all the other things we use that have contact information: Outlook 98's address book, our PalmPilot, our dumb cellular phone, our ICQ and AIM buddy lists and our Wildfire personal phone assistant — all of which we wish knew about one another (see Release 1.0, 6-97, 10-94 and 4-93).

There's more consolidation brewing in the directory and identity business. The company that ends up holding the principal list of names and attributes will have a special advantage. That may or may not be the company that has the trusted relationship and holds the profile and payment records, though it's easier to envision one entity holding all that information.
RESOURCES & PHONE NUMBERS

Nick Grouf, Firefly Network, (617) 528-1000; fax, (617) 577-7220; nick_grouf@firefly.net
Stratton Sclavos, VeriSign, (650) 429-3460; fax, (650) 961-7300; stratton@verisign.com
Yosi Amram, Chini Krishnan, ValiCert, (650) 849-9860; fax, (650) 849-9866; yosia@valicert.com, chini@valicert.com

COMING SOON

• What advertisers measure.
• Online governance.
• Market-based security
• And much more... (If you know of any good examples of the categories listed above, please let us know.)

Release 1.0 is published monthly, except for a combined July/August issue, by EDventure Holdings, 104 Fifth Ave., New York, NY 10011-6901; (212) 924-8800; fax, (212) 924-0240; http://www.edventure.com. It covers software, the Internet, electronic commerce, computer-telephone integration, online services, group-ware, text management, con-nec-tivity, messaging, wireless communications, intel-lect-ual property law and other unpredictable topics. Editor: Esther Dyson (edyson@edventure.com); publisher: Daphne Kis (daphne@edventure.com); managing editor: Jerry Michalski (spiff@edventure.com); office manager: Helen Martin (helen@ed-ven-ture.com); marketing manager: Mari Katsunuma (mari@edventure.com); cir-cu-la-tion mana-ger: Scott Giering (scott@edventure.com); assistant: Trista Schroeder (trista@ed-ven-ture.com); receptionist: Philena Taylor (philena@edventure.com). Copy—right 1998, ED-ven-ture H-oldings Inc. All rights re-served. No mater-ial in this pub-li-cation may be re-pro-duc-ed with-out written permission; however, we gladly arrange for re-prints or bulk purchas-es. Subscriptions cost $695 per year, $750 over-seas.

Release 1.0

23 February 1998
Please enter my subscription to Release 1.0 at the rate of $795 per year in the U.S. and Canada. Overseas subscriptions are $850, airmail postage included. Payment must be enclosed. Satisfaction guaranteed or your money back.

Name__________________________
Title__________________________
Company_______________________
Address________________________
City___________________________ State_________ Zip__________
Country________________________

Telephone_______________________ Fax_______________________
E-mail___________________________ URL_______________________

☐ Check enclosed
☐ Charge my
  ☐ American Express    ☐ Master Card    ☐ Visa
  Card Number____________________ Expiration Date_______
  Name and Billing Address_______________________________
  Signature_____________________________________________

☐ Please send me information on your multiple copy rate.

Please fill in the information above and send to:

EDventure Holdings Inc.
104 Fifth Avenue, 20th Floor
New York, NY 10011

If you have any questions, please contact us at 1 (212) 924-8800; fax 1 (212) 924-0240; e-mail us@edventure.com; www.edventure.com.

Daphne Kis
Publisher