Distributed Identification and Consumer Data Protection

Khaja Ahmed – Microsoft Corporation

Threats to Online Safety

- Consumer privacy has steadily declined as internet use grew over the years
- Greater use and greater value attract professional international criminal fringe
  - Exploit weaknesses in patchwork
  - Phishing and pharming at 1000% CAGR
- Identity theft is approaching crisis proportion
- …

There are no simple solutions!

A Holistic approach requiring commitment from all the key players is necessary

Each Must Play a Part

- Thought leaders and Consumer Advocates
- Industry
- Standards Bodies
- Governments
- Relevant NGOs and Quasi-Governmental bodies
- The consumers have already spoken – they want privacy

A PLOT to Protect Consumer Data

- Policies need to be respectful of consumer privacy needs
- Legal framework needs to be conducive to privacy
- Operational practices must evolve to defend and enhance privacy
- Technological solutions must be developed and adopted

Microsoft’s Efforts

The Roles of Microsoft

- Industry leader
- Developer of, Contributor to and Driver of Standards
- Software Product Provider – OS and applications
- Online service provider – MSN & Live ID

The Roles

- Industry leader
  - Thought Leadership
  - Identity Metasystem and the 7 Laws of Identity
- Develop, Contribute to and Drive Standards
  - Drive the right standards
  - The WS* suite
- Software Product Provider – OS and applications
  - The right technology and development practices
  - Windows Vista security features
- Online service provider – MSN & Live ID
  - The right operational practices and technology
  - Information Security Program

What is a Digital Identity?

- Set of *claims* one subject makes about another
- Many identities for many uses
- Required for transactions in real world and online
- Model on which all modern access technology is based

The Laws of Identity

Established through Industry Dialog

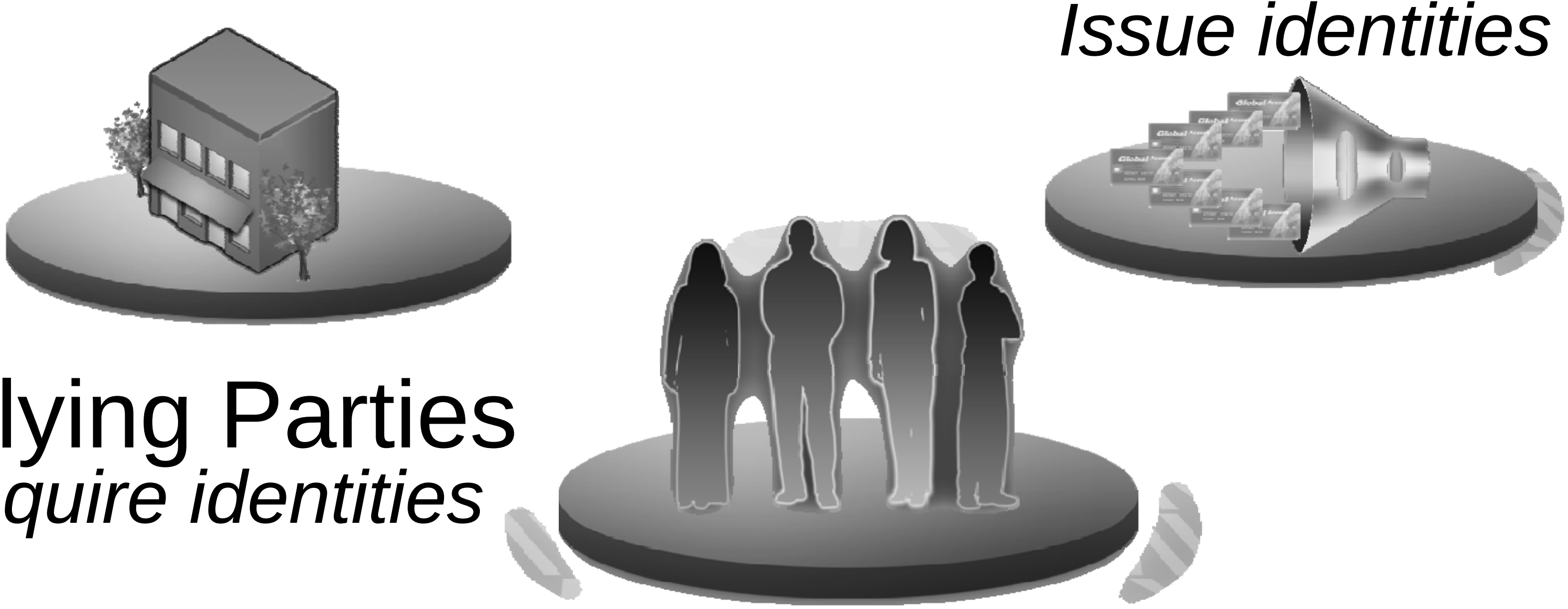
1. **User control and consent**
2. **Minimal disclosure for a defined use**
3. **Justifiable parties**
4. **Directional identity**
5. **Pluralism of operators and technologies**
6. **Human integration**
7. **Consistent experience across contexts**

Join the discussion at www.identityblog.com

Identity Metasystem

- We need a unifying “Identity metasystem”
  - Protect applications from identity complexities
  - Allow digital identity to be loosely coupled: multiple operators, technologies, and implementations
- Not first time we’ve seen this in computing
  - Emergence of TCP/IP unified Ethernet, Token Ring, Frame Relay, X.25, even the not-yet-invented wireless protocols

Identity Roles



Identity Providers
Issue identities

Relying Parties
Require identities

Subjects
Individuals and other entities about whom claims are made

CardSpace (“InfoCard”)

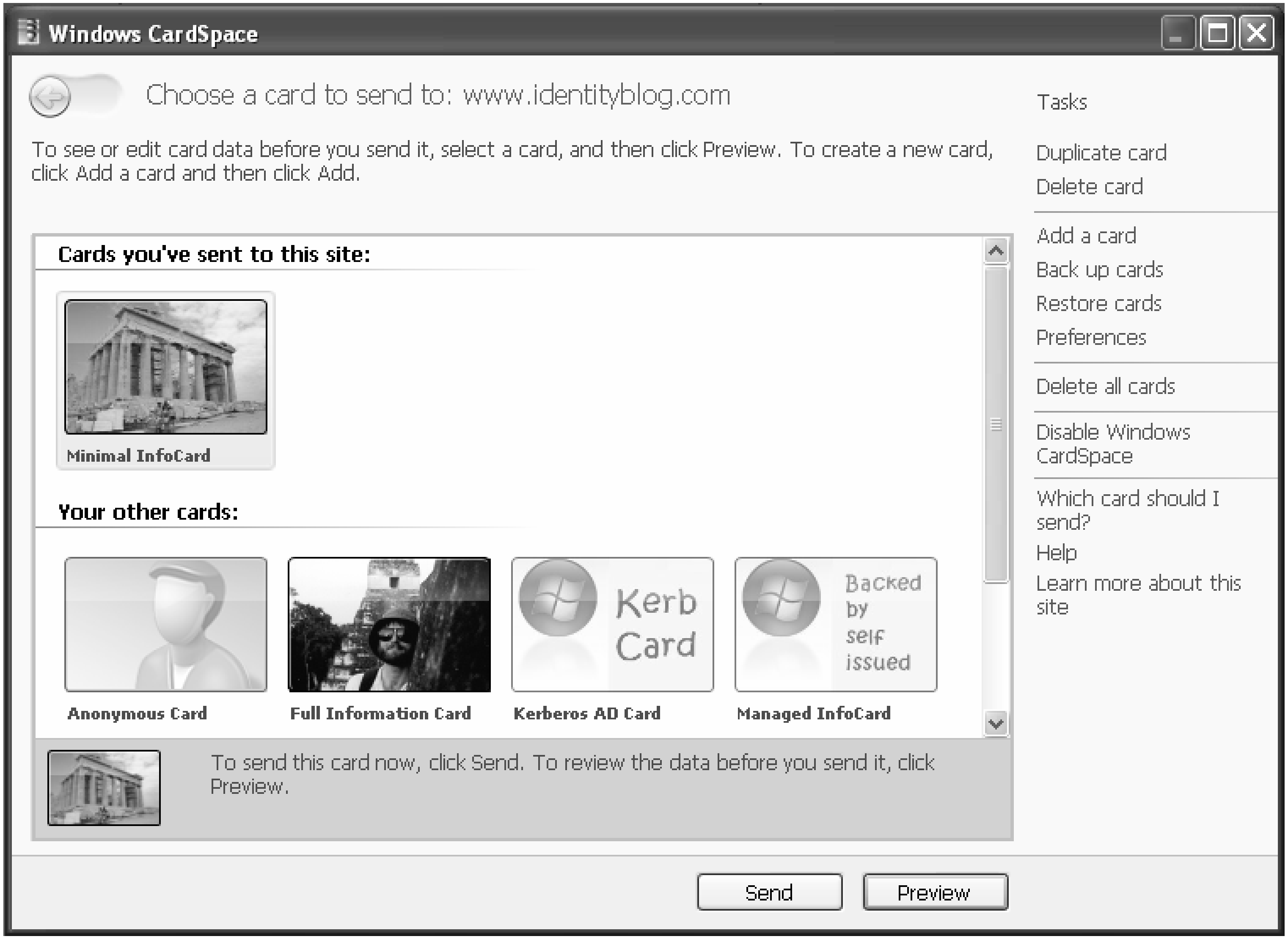
SELF - ISSUED

- Contains self-asserted claims about me
- Stored locally
- *Effective replacement for username/password*
- Eliminates shared secrets
- Easier than passwords

MANAGED

- Provided by banks, stores, government, clubs, etc.
- Cards contain metadata only!
- Claims stored at Identity Provider and sent only when card submitted

CardSpace Experience



Windows CardSpace

Choose a card to send to: www.identityblog.com

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

Cards you've sent to this site:

Minimal InfoCard

Your other cards:

Anonymous Card

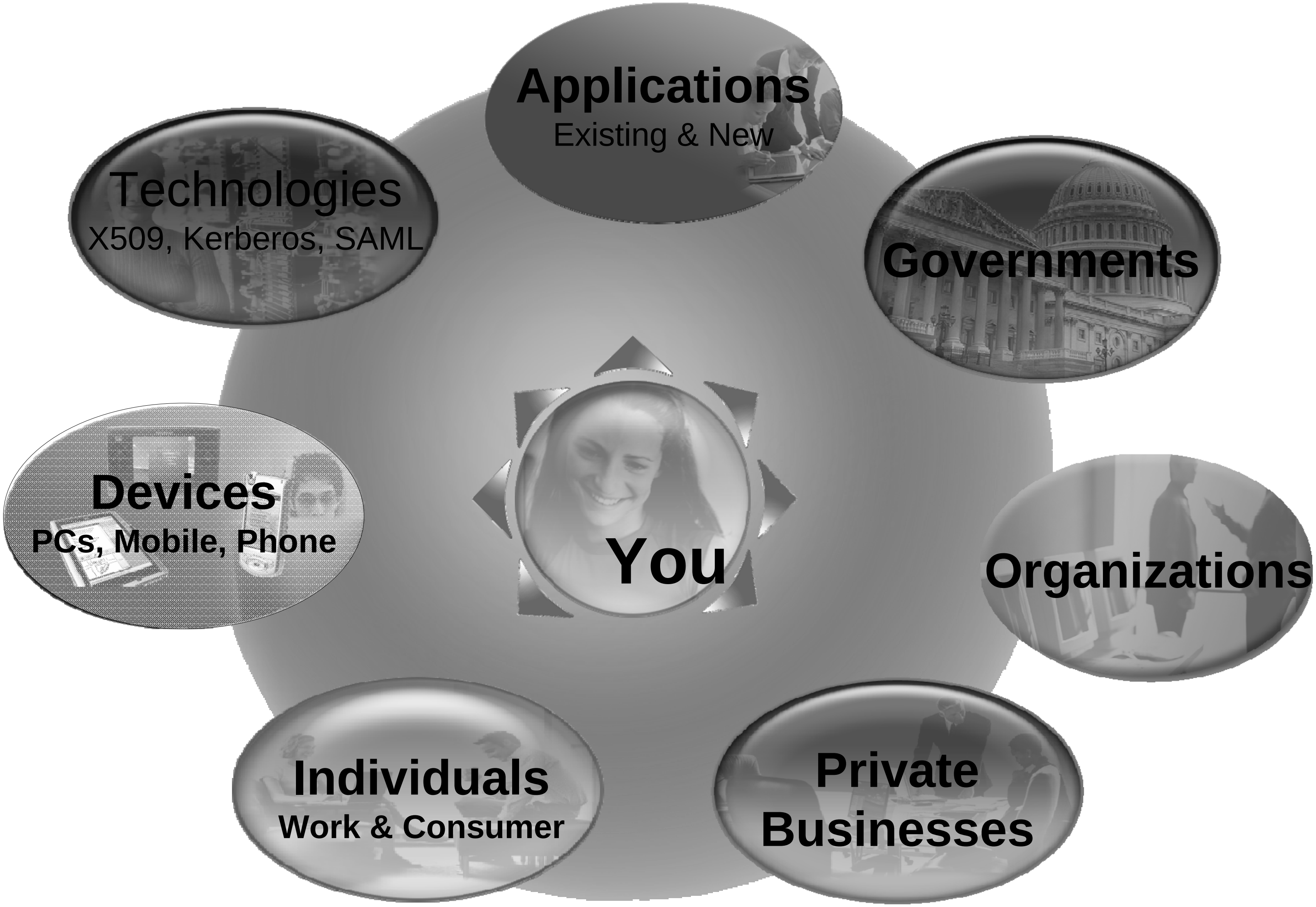
Full Information Card

Kerberos AD Card

Managed InfoCard

To send this card now, click Send. To review the data before you send it, click Preview.

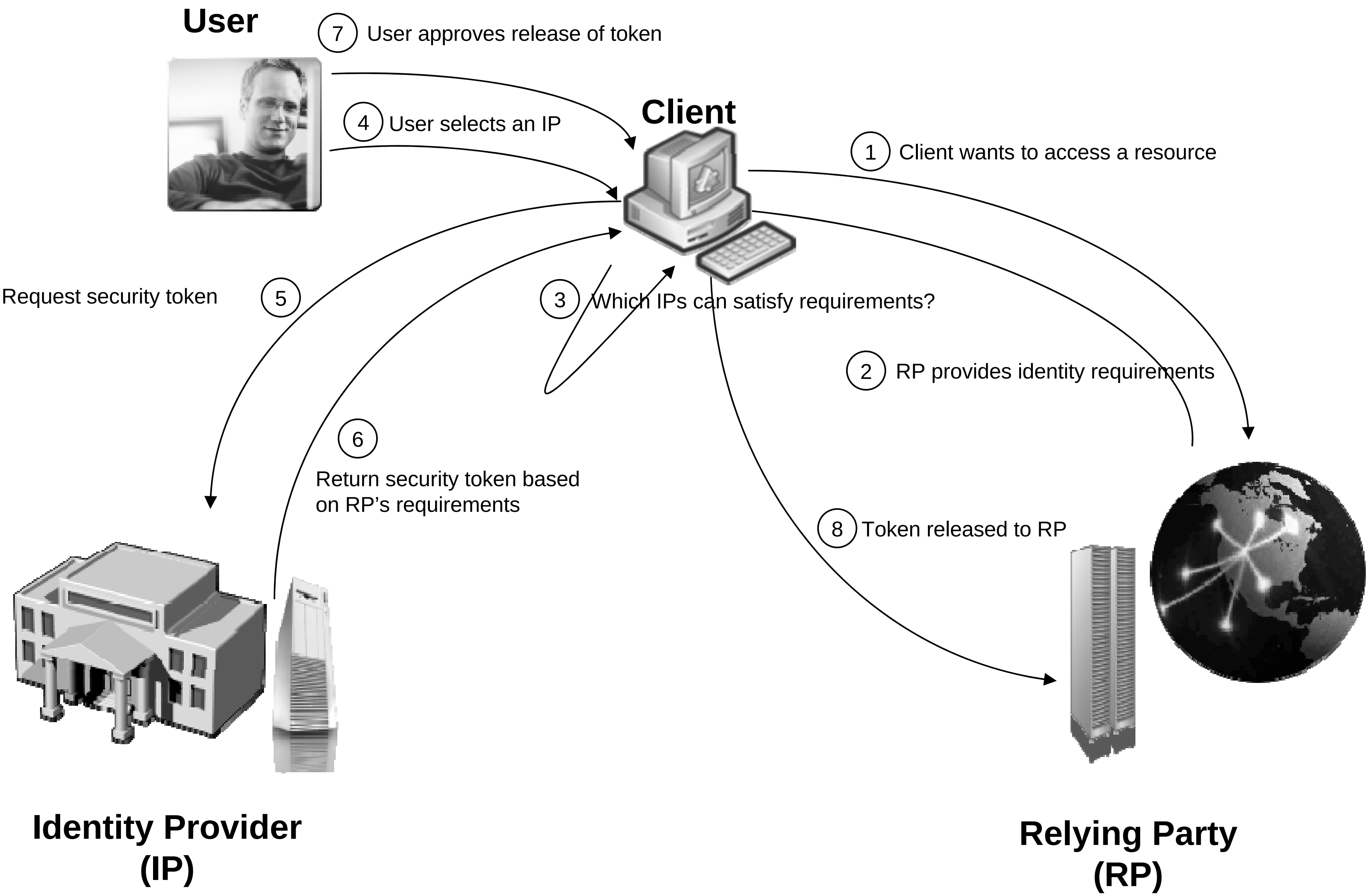
Empowers the User…



CardSpace Overview

- Simple user abstraction for digital identity
  - For managing collections of claims
  - For managing keys for sign-in and other uses
- Grounded in real-world metaphor of physical cards
  - Government ID card, driver’s license, credit card, membership card, etc…
  - Self-issued cards signed by user
  - Managed cards signed by external authority
- Shipped as part of .NET 3.0
  - Runs on Windows Vista, XP, and Server 2003
- Implemented as protected subsystem

Protocol Drill Down


User
7 User approves release of token
4 User selects an IP
Client
1 Client wants to access a resource
Request security token
5
3 Which IPs can satisfy requirements?
2 RP provides identity requirements
6
Return security token based
on RP’s requirements
8 Token released to RP
Identity Provider
(IP)
Relying Party
(RP)

Implementation Properties

- Cards represent references to identity providers
  - Cards have:
    - Address of identity provider
    - Names of claims
    - Required credential
  - Not claim values
- Information Card data not visible to applications
  - Stored in files encrypted under system key
  - User interface runs on separate desktop
- Simple self-issue identity provider
  - Stores name, address, email, telephone, age, gender
  - No high value information
  - User must opt-in

An Identity Metasystem Architecture

- Microsoft worked with industry to develop protocols that enable an identity metasystem: WS-* Web Services
  - Encapsulating protocol and claims transformation: WS-Trust
  - Negotiation: WS-MetadataExchange and WS-SecurityPolicy
- Only technology we know of specifically designed to satisfy requirements of an identity metasystem

Uses Existing Technologies

- Managed Card Authentication Methods
  - X.509 Certificate
  - Kerberos Ticket
  - Self-Issued Information Card
  - Username/Password
- Managed Card Token Type
  - Can be anything (including SAML, X.509, …)
- Self-Issued Card Token Type
  - SAML
- Self-Issued Card Schema
  - Uses LDAP element names

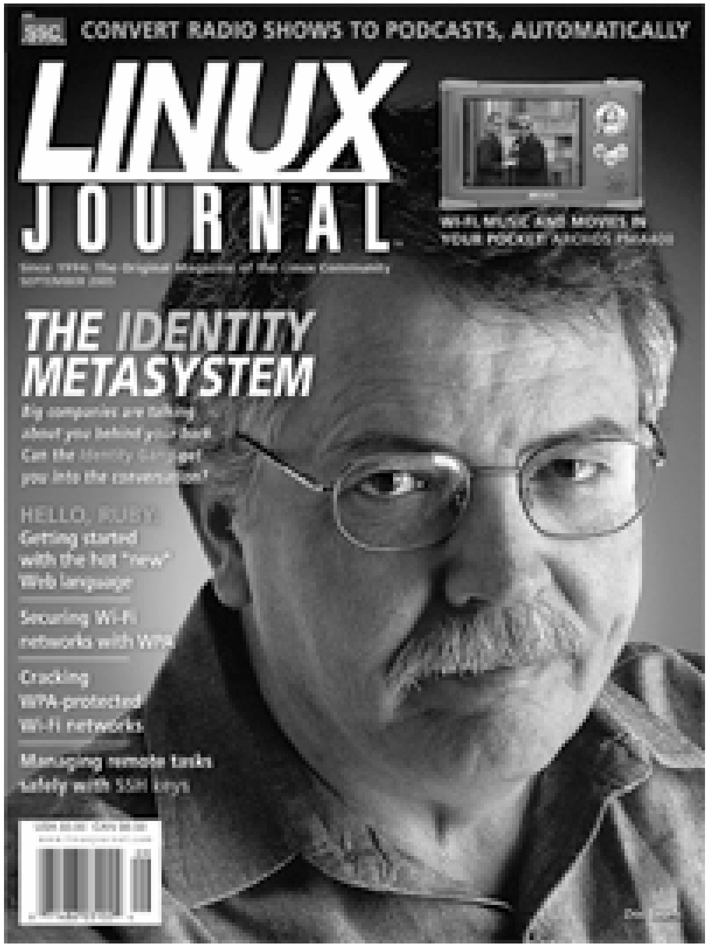
Components Microsoft is Building

- CardSpace identity selector
  - Component of .NET 3.0, usable by any application
  - Hardened against tampering, spoofing
- CardSpace simple self-issued identity provider
  - Self-issued identity for individuals running on PCs
  - Uses strong public key-based authentication – user does not disclose passwords to relying parties
- ADFS V2 managed identity provider
  - Plug Active Directory and other identities into the metasystem
  - Full set of policy controls to manage use of simple identities and Active Directory identities
- Windows Communication Foundation for building distributed applications and implementing relying party services

Not just a Microsoft thing…

- Based entirely on open protocols
- Identity *requires cooperation* – and it's happening…
- Interoperable software being built by
  - Sun, IBM, Novell, Ping Identity, BMC, …
  - For UNIX/Linux, MacOS, mobile devices, …
- With browser support under way for
  - Firefox, Safari, …
- Unprecedented things happening
  - Microsoft part of JavaOne opening keynote
  - Joint Information Card demos with IBM, Novell

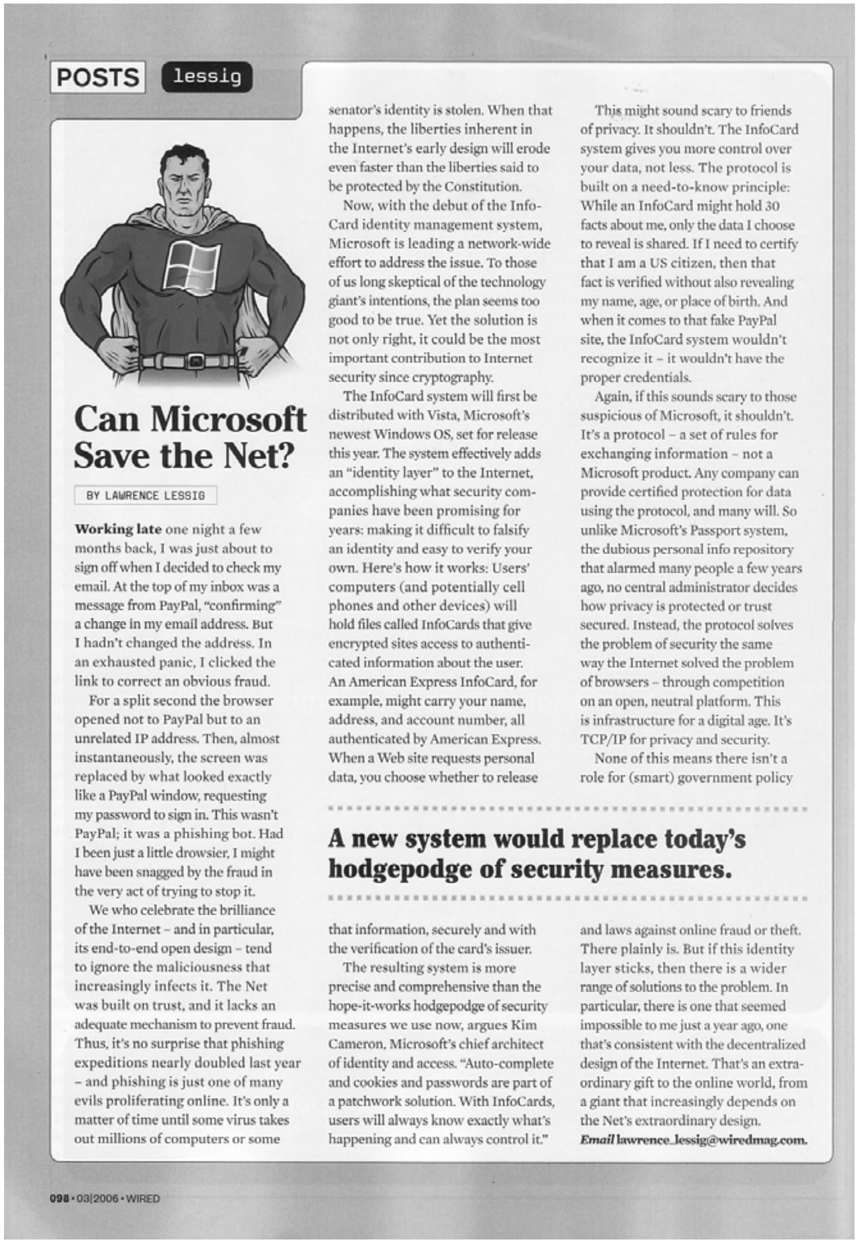
LINUX Journal Sep ’05 Cover


CONVERT RADIO SHOWS TO PODCASTS, AUTOMATICALLY
LINUX
JOURNAL
Since 1994: The Original Magazine of the Linux Community
SEPTEMBER 2005
WI-FI MUSIC AND MOVIES IN YOUR POCKET ARCHOS PMA400
THE IDENTITY METASYSTEM
Big companies are talking about you behind your back. Can the Identity Gang get you into the conversation?
HELLO, RUBY
Getting started with the hot "new" Web language
Securing Wi-Fi networks with WPA
Cracking WPA-protected Wi-Fi networks
Managing remote tasks safely with SSH keys

- By Doc Searls
- Linux Journal Editor
- Author of the “cluetrain manifesto”

- Introducing “The Identity Metasystem”

WIRED Magazine - Mar ’06



POSTS lessig

Can Microsoft Save the Net?

BY LAWRENCE LESSIG

Working late one night a few months back, I was just about to sign off when I decided to check my email. At the top of my inbox was a message from PayPal, “confirming” a change in my email address. But I hadn’t changed the address. In an exhausted panic, I clicked the link to correct an obvious fraud.

For a split second the browser opened not to PayPal but to an unrelated IP address. Then, almost instantaneously, the screen was replaced by what looked exactly like a PayPal window, requesting my password to sign in. This wasn’t PayPal; it was a phishing bot. Had I been just a little drowsier, I might have been snagged by the fraud in the very act of trying to stop it.

We who celebrate the brilliance of the Internet – and in particular, its end-to-end open design – tend to ignore the maliciousness that increasingly infects it. The Net was built on trust, and it lacks an adequate mechanism to prevent fraud. Thus, it’s no surprise that phishing expeditions nearly doubled last year – and phishing is just one of many evils proliferating online. It’s only a matter of time until some virus takes out millions of computers or some senator’s identity is stolen. When that happens, the liberties inherent in the Internet’s early design will erode even faster than the liberties said to be protected by the Constitution.

Now, with the debut of the InfoCard identity management system, Microsoft is leading a network-wide effort to address the issue. To those of us long skeptical of the technology giant’s intentions, the plan seems too good to be true. Yet the solution is not only right, it could be the most important contribution to Internet security since cryptography.

The InfoCard system will first be distributed with Vista, Microsoft’s newest Windows OS, set for release this year. The system effectively adds an “identity layer” to the Internet, accomplishing what security companies have been promising for years: making it difficult to falsify an identity and easy to verify your own. Here’s how it works: Users’ computers (and potentially cell phones and other devices) will hold files called InfoCards that give encrypted sites access to authenticated information about the user. An American Express InfoCard, for example, might carry your name, address, and account number, all authenticated by American Express. When a Web site requests personal data, you choose whether to release that information, securely and with the verification of the card’s issuer.

The resulting system is more precise and comprehensive than the hope-it-works hodgepodge of security measures we use now, argues Kim Cameron, Microsoft’s chief architect of identity and access. “Auto-complete and cookies and passwords are part of a patchwork solution. With InfoCards, users will always know exactly what’s happening and can always control it.”

This might sound scary to friends of privacy. It shouldn’t. The InfoCard system gives you more control over your data, not less. The protocol is built on a need-to-know principle: While an InfoCard might hold 30 facts about me, only the data I choose to reveal is shared. If I need to certify that I am a US citizen, then that fact is verified without also revealing my name, age, or place of birth. And when it comes to that fake PayPal site, the InfoCard system wouldn’t recognize it – it wouldn’t have the proper credentials.

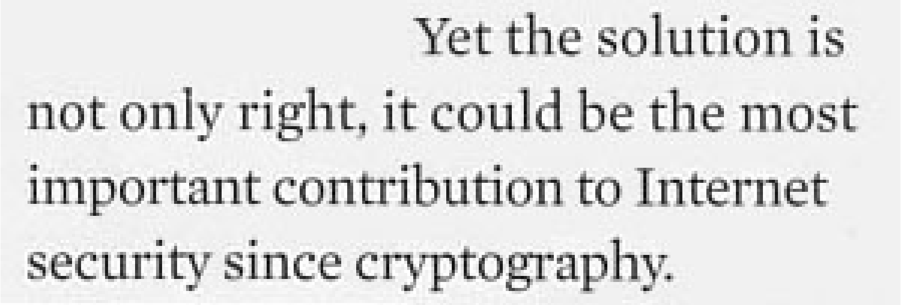
Again, if this sounds scary to those suspicious of Microsoft, it shouldn’t. It’s a protocol – a set of rules for exchanging information – not a Microsoft product. Any company can provide certified protection for data using the protocol, and many will. So unlike Microsoft’s Passport system, the dubious personal info repository that alarmed many people a few years ago, no central administrator decides how privacy is protected or trust secured. Instead, the protocol solves the problem of security the same way the Internet solved the problem of browsers – through competition on an open, neutral platform. This is infrastructure for a digital age. It’s TCP/IP for privacy and security.

None of this means there isn’t a role for (smart) government policy and laws against online fraud or theft. There plainly is. But if this identity layer sticks, then there is a wider range of solutions to the problem. In particular, there is one that seemed impossible to me just a year ago, one that’s consistent with the decentralized design of the Internet. That’s an extraordinary gift to the online world, from a giant that increasingly depends on the Net’s extraordinary design.

Email **lawrence_lessig@wiredmag.com.**

A new system would replace today’s hodgepodge of security measures.

- By Lawrence Lessig
- Influential Internet & Public Policy Lawyer
- Special Master in antitrust case against Microsoft
- Quotation:



Yet the solution is not only right, it could be the most important contribution to Internet security since cryptography.

Microsoft Open Specification Promise (OSP)

- Perpetual legal promise that Microsoft will never bring legal action against anyone for using the protocols listed
  - Includes all the protocols underlying CardSpace
- Issued September 2006
- http://www.microsoft.com/interop/osp/

WS* Standards

- Developed cooperatively by industry partners
- Submitted to standards bodies (OASIS) and adopted
- Interoperable implementations from multiple parties exist

SDL

- A major step towards more secure software
  - Now recognized as an industry leading best practice
- SDL tools being made available to third parties
- Tools, Training, Development Methodology and Corporate Commitment

Information Security Program

- MSN has an ISP that provides for
  - Data Classification into MBI, HBI, LBI
  - Different and appropriate handling and security measures are applied
  - Separation of duties and restricted access policies mitigate risk of administrator abuse

(Backup Slides)