



# Kerberos as the foundation for the Identity Metasystem

Kim Cameron, Distinguished Engineer  
Microsoft Corporation

<http://www.identityblog.com>

10/21/09 9:30AM

# Agenda

The Landscape: Hard Problems of Identity

The Claims Based Model

Using the Identity Metasystem Architecture

Conversation: What role does Kerberos play?

Minimal Disclosure and Multilateral Security

Possible Directions

# Two hard problems – one answer

## The hardest lines of any application...

- Who are you?
- What are you allowed to do?
- What experience should you have?

## The hardest job of any IT architect

- How do I get **applications** that can work together in an architecture?
- How do I get applications that are securable and manageable?

# Application Developer Inferno

- It's hard to get identity decisions to work out in all the contexts customers require
  - As one developer told me, “You are never done”
- Many choices of identity technology
  - Passwords, Kerberos, X.509, SAML, LDAP, OpenID, etc
  - No easy way to go from ID to auth and personalization
  - Choices imply different representations, user experiences, programming models, fit with scenario
- Applications become limited and “siloed” by technology choices
  - Bound to constraints of technology you choose
  - **Difficult to connect across boundaries** (both technical and organizational) where different choices have been made

# Now the Cloud Brings New Challenges

- Example: Expense Report App
  - Use case: Employees fill out expense reports that are sent to *manager* for approval and charged to *cost centers*...
- On-premise solution:
  - Enterprise buys solution from ISVs like PeopleSoft that leverage enterprise authentication and look-ups in directory and/or HR databases
    -
- Cloud (outsourced service) solution:
  - Service Provider runs Expense Report **Service** in cloud
  - Even if single signon provides authentication, how does cloud access internal systems to discover manager and cost center?
  - Is everything hand configured? Auto-provisioned? How much does *that* cost?
- **Boundaries reveal conflation inherent in current approaches**

# “Claims” Change the Landscape

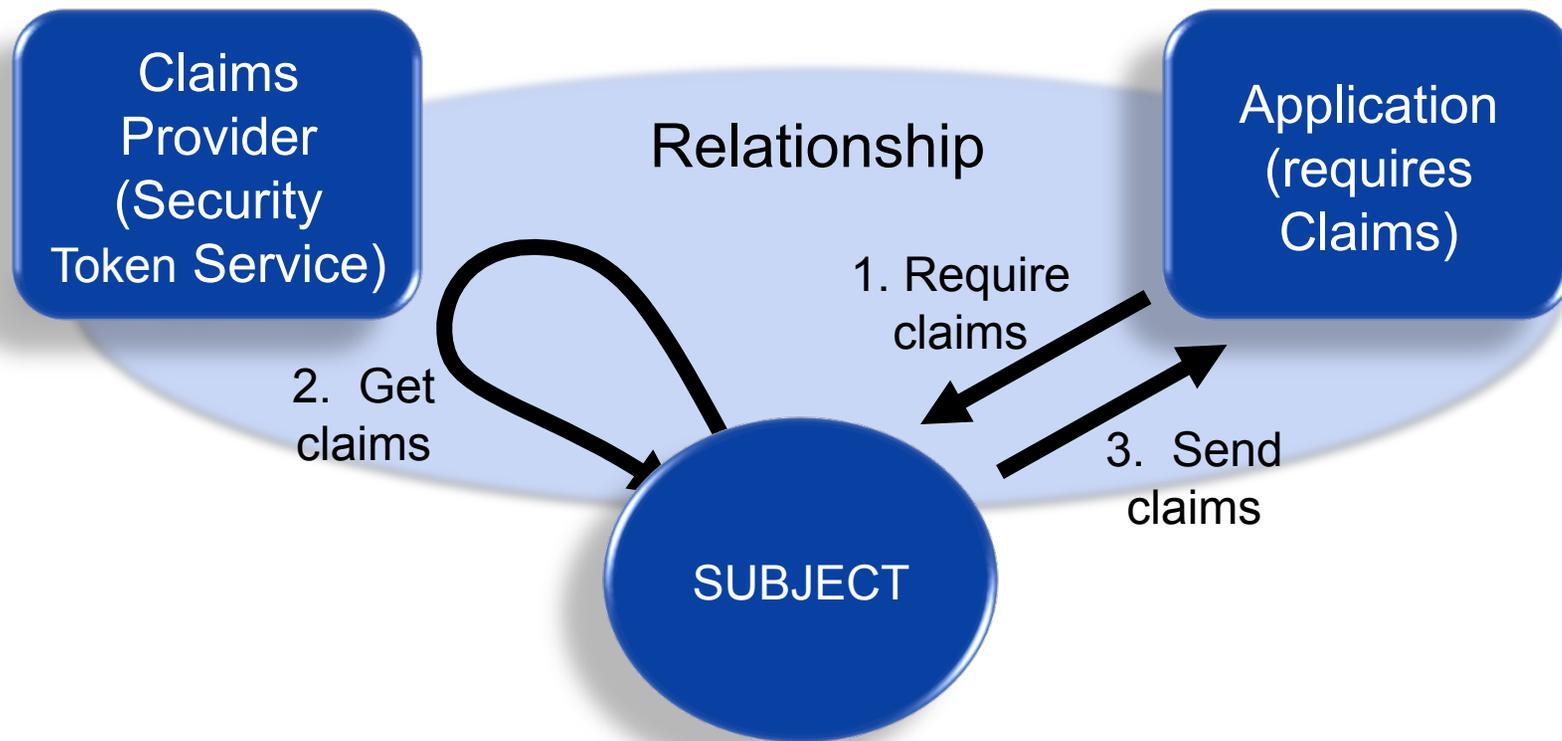
- A new technology that moves us *beyond single sign-on* to “*claim-based*” access across administrative boundaries
  - *Intra and inter-enterprise as well as enterprise-to-cloud*
- Same technology facilitates building and using cloud based services
  - Scaling of services across farms
- Leverage trusted offline proofing in online applications
  - Example – school proofing
  - Sharing data between services.
- Help us cross enterprise administrative and technical boundaries

# The Claims-Based Model

# What is the Claims-Based Model?

- Claims-based model
  - Abstraction layer for authenticating, authorizing, obtaining information about users and services
- Claim: statement made by one subject about another subject
  - Email = [kcameron@microsoft.com](mailto:kcameron@microsoft.com)
  - Age > 21
  - Manager = Craig Wittenberg
  - Role= Architect
- Identity Metasystem: open standards-based architecture for exchange of claims under user control
  - “Claims transformers” that match impedance
  - Write to model, let infrastructure adapt to environment
  - Not a theological exercise

# Claims-Based Model



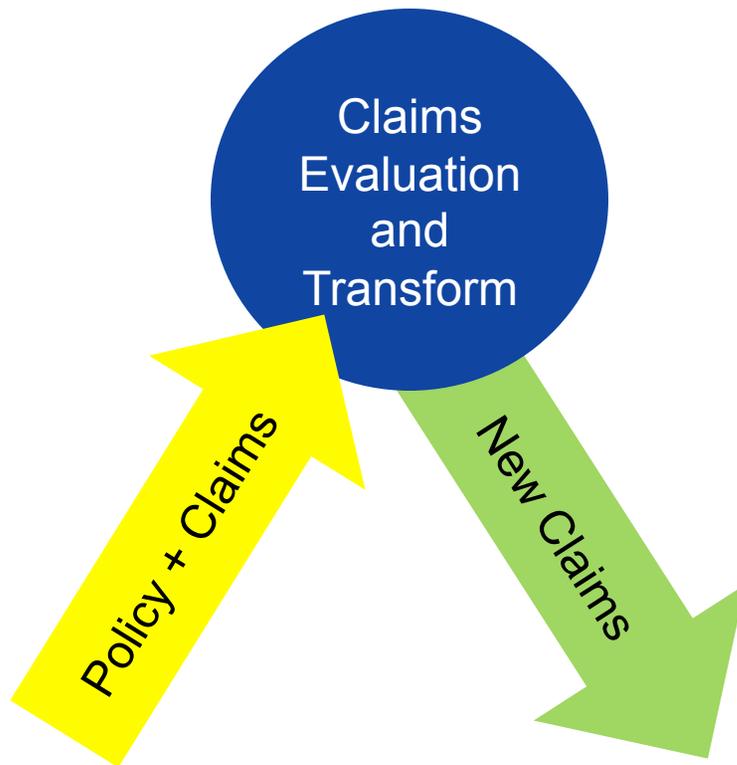
- Application: requires, uses claims to describe users
- Claims provider: supports protocols for issuing claims
- Relationship: context in which meaning of claims is defined

# Laws of Identity

- Users control their release of information, understand, and WANT to participate
- Minimal disclosure necessary for any use
- No hidden SHARING of information
- No global identifiers for private relationships
- Multiple providers in a “claims market”
  - E.g., multiple layers of government, banks, employers, and others who people choose to trust
- Individuals are PART of the system
- They must have a consistent experience so they understand what is happening

# Identity, Capabilities, Authorization

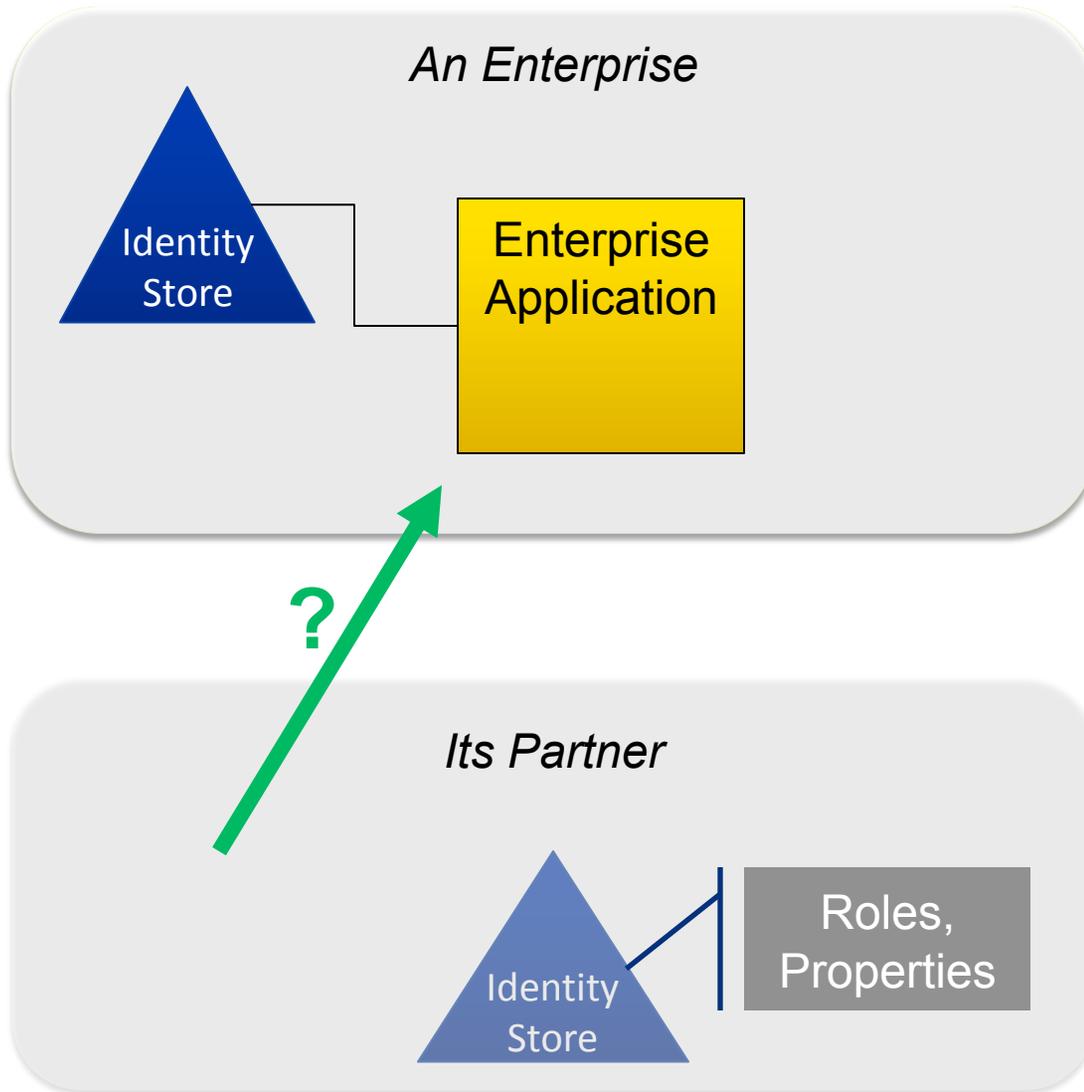
How the Claims Service works



- Claims Transformation
  - New semantics at domain boundaries
  - Different issuer (for example “Local STS”)
  - Transform from Identity to Capabilities
  - Claims Augmentation

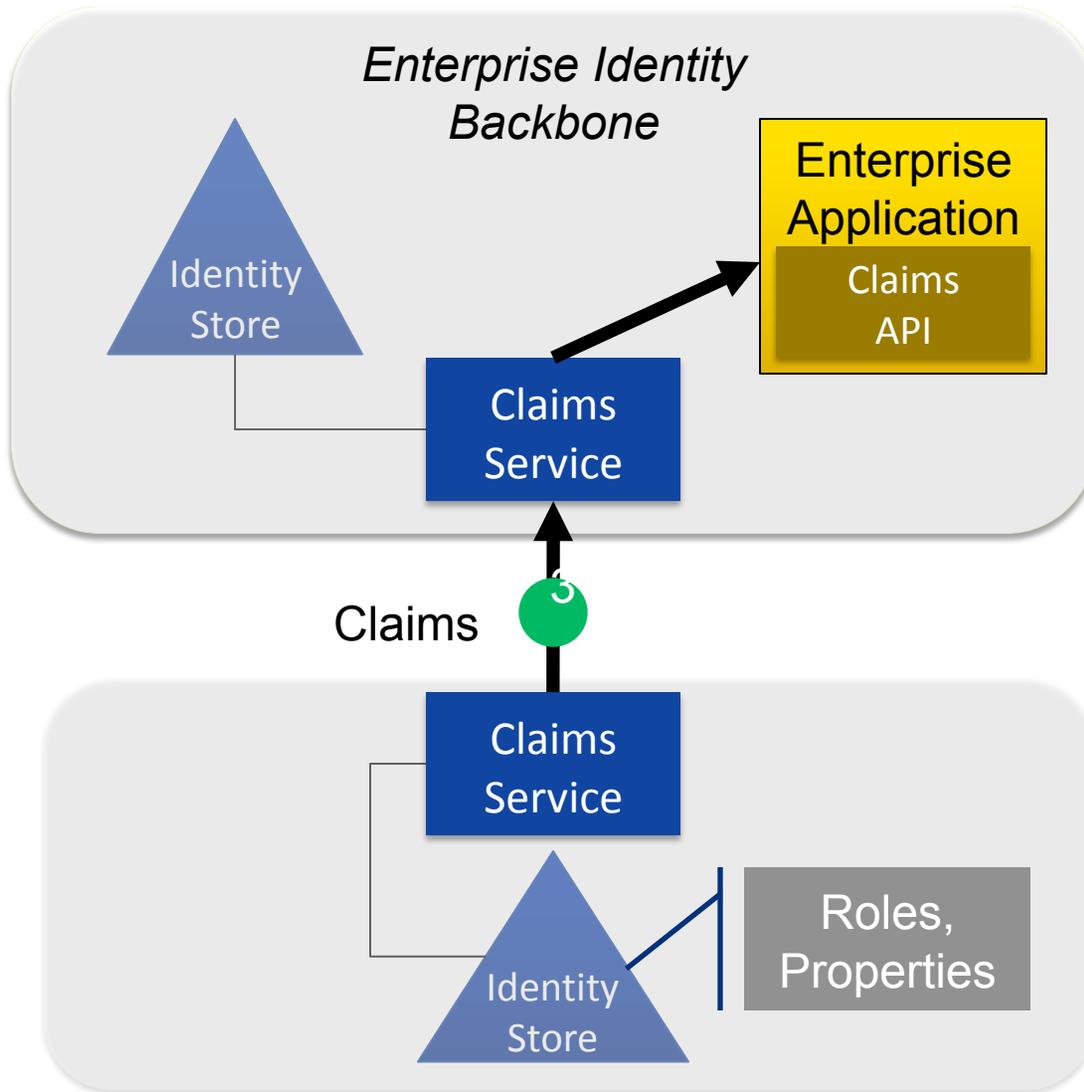
# Using the Identity Metasystem Architecture

# Architecture, Starting with the Enterprise



- How does an enterprise or government department make its application available to more than just employees?

# Industry Standard Components



## Claims API

- Middleware or framework for building claims-aware applications

## Claims Service

- Security Token Service (STS) connecting to an identity store (e.g. KDC)

## Identity Selector

- Client component allowing user to select and control identity

# How hard is meta for the Developer?

## 1. *“Who” are you?*

Example Config

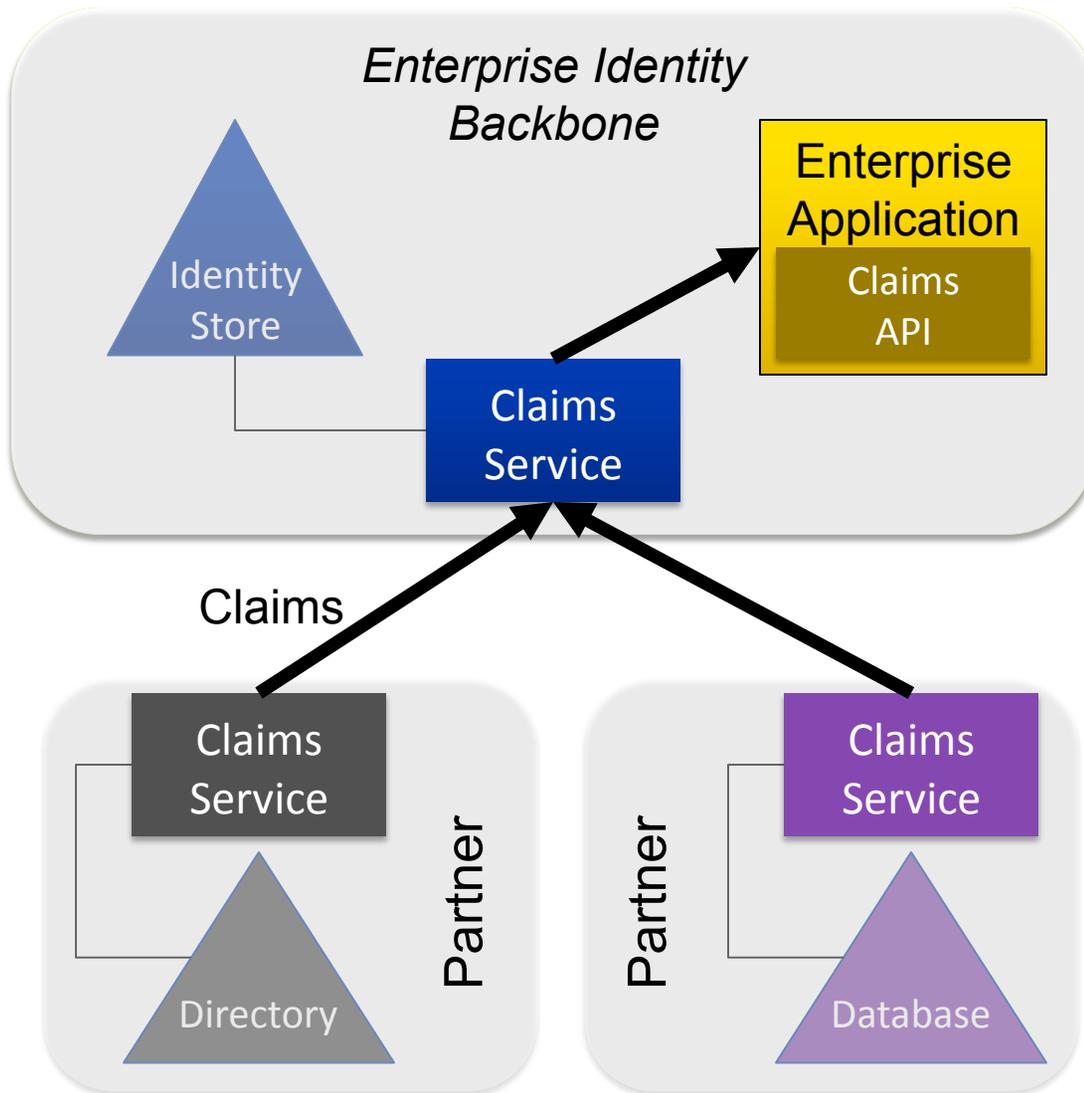
```
<federatedAuthentication enabled="true">
  <wsFederation
    issuer="https://sts1.contoso.com/FederationPassive/"
    realm = "http://web1.contoso.com/MyApp"
    passiveRedirectEnabled = "true"/>
</federatedAuthentication>
```

## 2. *What can you do (Claims API)?*

Example API

```
IClaimsIdentity caller = Thread.CurrentPrincipal.Identity
    as IClaimsIdentity;
string Role = (from c in caller.Claims
    where c.ClaimType == MyClaimTypes.Role
    select c.Value).Single();
```

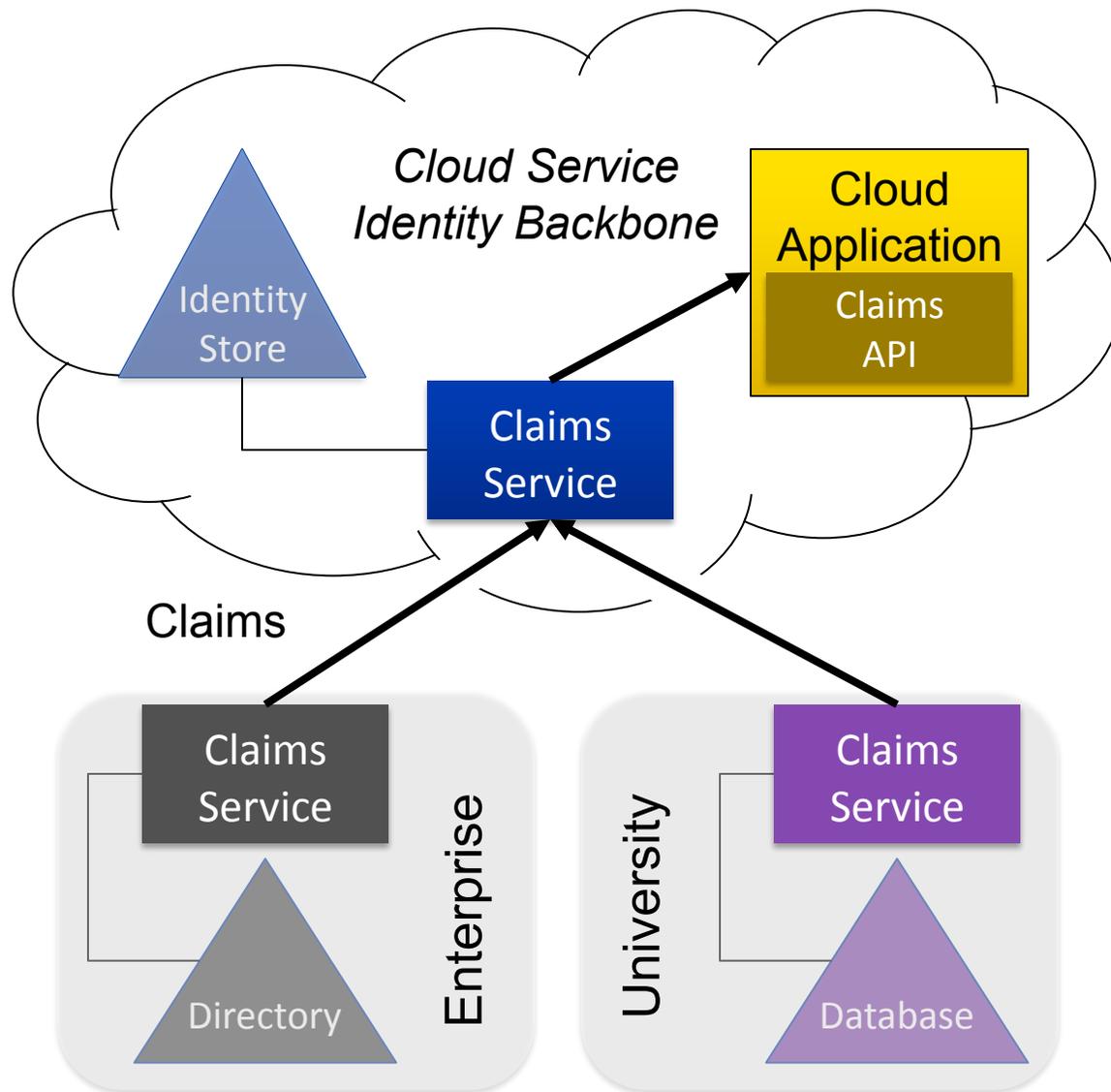
# The Claims Service



## ● Claims Service

- Security Token Service (STS)
- Standard across vendors
- Multiple protocols
  - SAML
  - WS-Federation
  - WS-Trust
- Multiple payloads
- Multiple vendors
  - Open Source, Microsoft, IBM, Novell, Sun, Siemens, etc

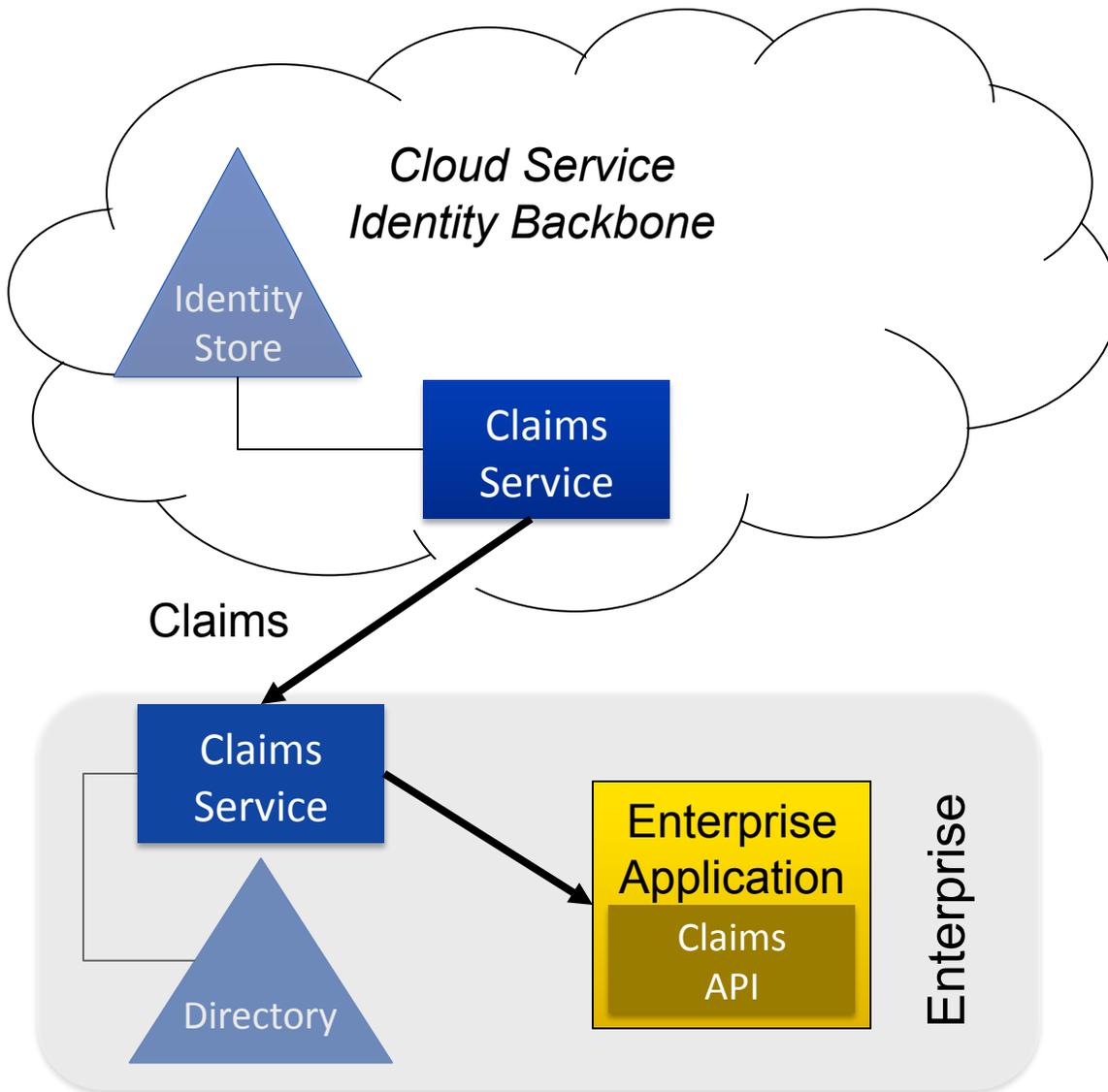
# Architecture Works for Cloud, Too



- **Claims Service**

- “Enterprise” protocols also used by cloud providers
- Additional protocol for providers in Consumer space: OpenID
- Several large cloud service providers already support the model
- Allows single federation agreement to access many services
- No lock-in to any cloud provider

# Architecture is Reversible



- **Claims Service**
  - Claims issued by cloud providers can be used by enterprise applications
  - Pattern: Enterprise outsources consumer identity management
  - Enterprise can accept identities from multiple service providers

**Conversation:  
What role does  
Kerberos play?**

# Kerberos: Constituent Identity System

- Kerberos is the most widely deployed mechanism for authenticating users and providing them with simple claims
  - Consistent with Metasystem model (or visa versa!)
- STS's like ADFS V2 are Claims Transformers that convert Kerberos UPN (and group) claim(s) to SAML and WS-Trust claims
  - Consistent with Claims Transformer architecture
- Kerberos tickets can be sent as “security tokens” within the WS-Trust Claims Transformation protocol
- On the Relying Party Side, we are starting to see examples of claims transformers (“augmenters”) that convert claims back to Kerberos tickets...
  - Poor fidelity...

# Kerberos supporting claims

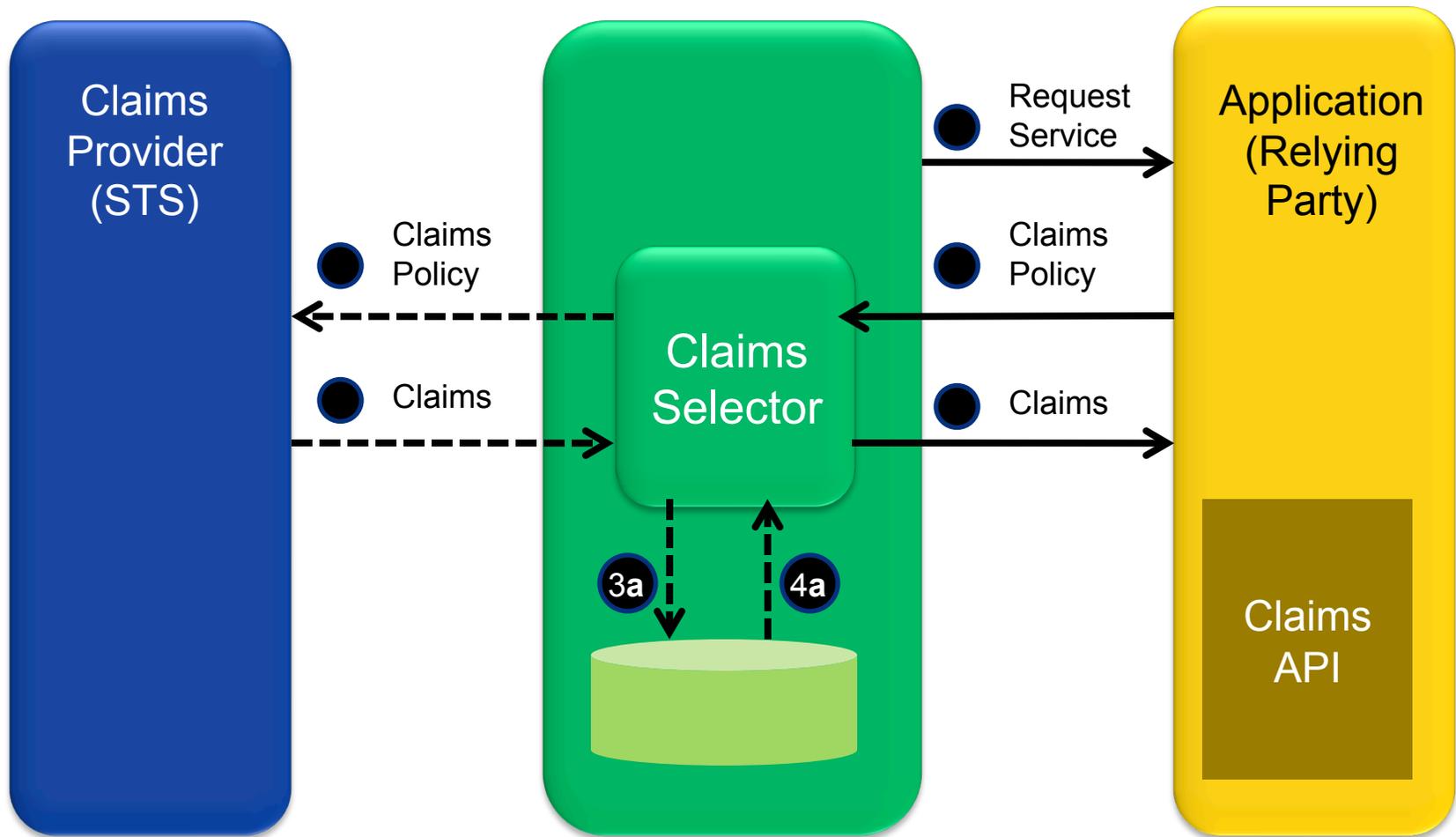
- Possibility of extending Kerberos payload so it supports claims (several ways to do this...)
- Possible “Light-up” scenario on a world scale
- Research project where ACLs are expressed as required claims, and Kerberos vehicles them
- “Inbound” Claims transformer can then become high fidelity
- Huge improvement in manageability is possible
  - Example: “This share can be seen by people in architect roles who report to Joe Long”

# Identity Metasystem Inclusiveness

- The security and privacy problems of the internet will not be solved by a single protocol
  - SAML plays an important role
  - Kerberos plays an important role
  - PKI plays an important role
  - WS-Trust plays an important role
  - OpenID plays an important role
- We need a loosely coupled Metasystem, not a single protocol to Rule the World
  - There is a spectrum of use-cases and we are still seeing innovation
  - U-Prove and other zero knowledge technology

# **Other Frontiers: Minimal Disclosure and Multilateral Security**

# Claims Selector



# Information Card Paradigm

IdentityBlog - Digital Identity, Privacy, and the Internet's Missing Identity Layer - Windows Internet Explorer

http://www.identityblog.com/

File Edit View Favorites Tools Help

IdentityBlog - Digital Identity, Privacy, and the Int...

## Kim Cameron's Identity Weblog

BLOG INTRODUCTION LAWS OF IDENTITY HOME CARDSPACE DOWNLOADS PAPERS BIO DASHBOARD LOG IN RSS FEED

Videos

Why OpenID leads to Information Cards  
Length: 5:41

Add Information Cards with 30 Lines of Code  
Length: 5:49

### My email address

*Is the inferno a part of electronic eternity?*

Posted on Friday 17 July 2009

I'm writing this post in case your version of my email address has "windows.microsoft.com" in it.

The "windows.microsoft.com" domain is being repurposed for some higher good. So going forward, please write to me with the usual address (same local-part) but at "@microsoft.com" instead of "@windows.microsoft.com").

Filed under: Identity

Kim Cameron @ 1:02 pm

No Comments

### Electronic Eternity

*Digital information should have a half-life unless a good argument can be made for preserving it.*

Error on page.

Internet | Protected Mode: Off 100%

PutIdentityIntoRepo... Inbox - Microsoft O... IdentityBlog - Digma... EIC Folder Camtasia Studio - U... 9:02 AM

# OASIS Standard Approved

The screenshot shows the OASIS website interface. At the top right, there is a link for "English/Other languages". The OASIS logo is prominently displayed on the left, with the tagline "Advancing open standards for the information society" to its right. A navigation bar below the logo includes links for "About", "Members", "Join", "News", "Events", "Members Only", "Cover Pages", and "XML.org", followed by a search box and a "Go" button. A date stamp "16 July 2009" is visible in the top right corner of the page content. On the left side, there are two main menu sections: "CONSORTIUM" and "TECHNICAL WORK". The "CONSORTIUM" section lists "OASIS Standards", "How to Participate", "Policies and Procedures", "OASIS Blogs", and "Site Map". The "TECHNICAL WORK" section lists "Committees by Name", "Committees by Category", and a list of technical areas including "Adoption Services", "Computing Mgmt", "Document-Centric", "e-Commerce", "Law & Government", "Localisation", "Security", "SOA", "Standards Adoption", "Supply Chain", and "Web Services". The main content area features a "OASIS News" header. The primary news item is titled "OASIS Members Approve Open Interoperability Standard for Information Cards" with a subtitle "IBM, Microsoft, CA, EMC, Novell, and Others Advance Personal Digital Identity Standard". A link for "ODT PDF" is provided below the title. The news text states: "Boston, MA, USA; 16 July 2009 — OASIS, the international open standards consortium, today announced that its members have approved Identity Metasystem Interoperability (IMI) version 1.0 as an OASIS Standard, a status that signifies the highest level of ratification. IMI is best known as the technical protocol that enables Information Cards, a new way for people to register, login, and share information with websites without needing a new username and password for each site." A quote follows: "Information Cards offer the best of both worlds—greater privacy and easier access," said Marc Goodner of Microsoft, chair of the OASIS IMI Technical Committee. "As an approved OASIS Standard, IMI assures interoperability across platforms and services, which will result

# US OpenID / Information Card Pilots

The screenshot shows the homepage of the Information Cards website. The top navigation bar includes 'INFORMATION CARDS' with a person icon, 'INFORMATION CENTERS' with links to User, Business, Technical, and Press Information Centers, and 'THE FOUNDATION' with links to Members, Board of Directors, Working Groups, and Local Chapters. A left sidebar contains 'QUICK OVERVIEW', 'FEATURED CARD PROJECTS' (listing AAA Discount Reminders, ChoixVert Information Card, Equifax Over 18 I-Card, Minuteman Library Network I-Card, and Student Advantage RemindMe), and 'FOR GOVERNMENT'. The main content area features a headline: 'YAHOO!, PAYPAL, GOOGLE, EQUIFAX, AOL, VERISIGN, ACXIOM, CITI, PRIVO, WAVE SYSTEMS PILOT OPEN IDENTITY FOR OPEN GOVERNMENT'. Below this is a date 'September 9, 2009' and several tags: 'government', 'Information Card Foundation', 'open trust framework', 'OpenID Foundation', and 'privacy'. A quote reads: '-Government Embraces Innovative Technology to Support Citizen Participation-'. A sub-headline says: '(For more details about this release, please see our [Open Identity for Open Government FAQ](#))'. The main text begins with: 'Washington, D.C. - September 9, 2009 - Ten industry leaders - Yahoo!, PayPal, Google, Equifax, AOL, VeriSign, Acxiom, Citi, Privo and Wave Systems - announced today they will support the first pilot programs designed for the American public to engage in open government - government that is transparent, participatory, and collaborative. This open identity initiative is a key step in President Obama's memorandum to make it easy for individuals to register and participate in government websites - without having to create new usernames and passwords. Additionally, members of the public will be able to fully control how much or how little personal information they share with the government a

# The Provider's Dilemma

The screenshot shows the Equifax website interface. At the top left is the Equifax logo. At the top right is the URL Equifaxcards.com. Below the logo is a navigation bar with the text: Hello, cameron sky@hotmail.com (LOGOUT) | HOME | MANAGE ACCOUNT | ABOUT I-CARDS | CONTACT US. The main content area is titled "Available I-Cards" and features three card options:

- My eID Instant Privacy:** A black card with the Equifax logo and "my eID INSTANT PRIVACY" text. Description: "My eID Instant Privacy is quick and easy to use. No personally identifiable data is on the card, so you can be sure that you are anonymous to websites where you use it. This card meets GSA Level of Assurance 1." A blue button labeled "Get Your Card" is to the right.
- My eID Secure:** A silver card with the Equifax logo and "my eID SECURE" text. Description: "My eID Secure allows you to present a verified identity to websites that need to know who you are in order to protect your information. In order to get a My eID Secure card you will have to be authenticated by Equifax and answer a few questions to verify identity. After that, you will have a verified identity card. This card meets GSA Level of Assurance 2 and 3." A blue button labeled "Get Your Card" is to the right.
- My eID Complete:** An orange card with the Equifax logo and "my eID COMPLETE" text. Description: "My eID Complete card provides the highest level of identity assurance for access to extremely sensitive systems. This card meets GSA Level of Assurance 4." The text "Coming Soon" is to the right.

# Getting past the obvious: We can resolve apparent contradictions

- Example: Multilateral security
  - Each party minimizes what others can learn, so all participants are protected from each other
  - Disclose subsets and \properties of claims without destroying verifiability
    - Age is GREATER than 21 rather than a specific birth date
    - Expiry date AFTER today's date rather than revealing certificate expiration info
    - Prove a person's identifier is NOT on a list without revealing the identifier
- Example: Proof of knowledge
  - Delivers the useful properties of conventional security
  - Differences: issuer's signature and user's public key remain invisible to the issuer itself, proving properties of claims in addition to values

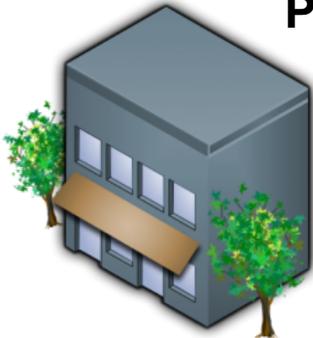
# Example:



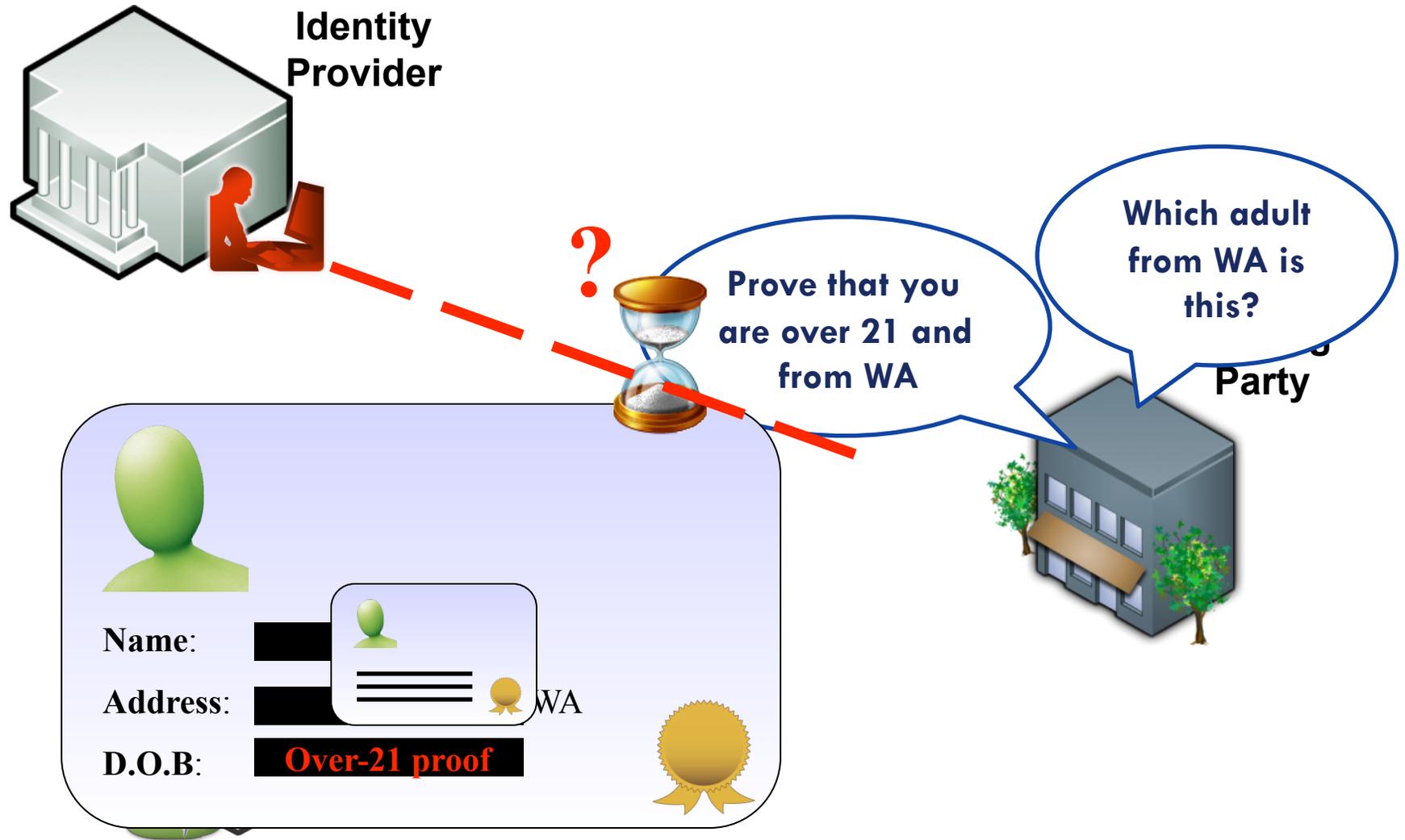
**Name:** Alice Smith  
**Address:** 1234 Pine, Seattle, WA  
**D.O.B.:** 23-11-1955



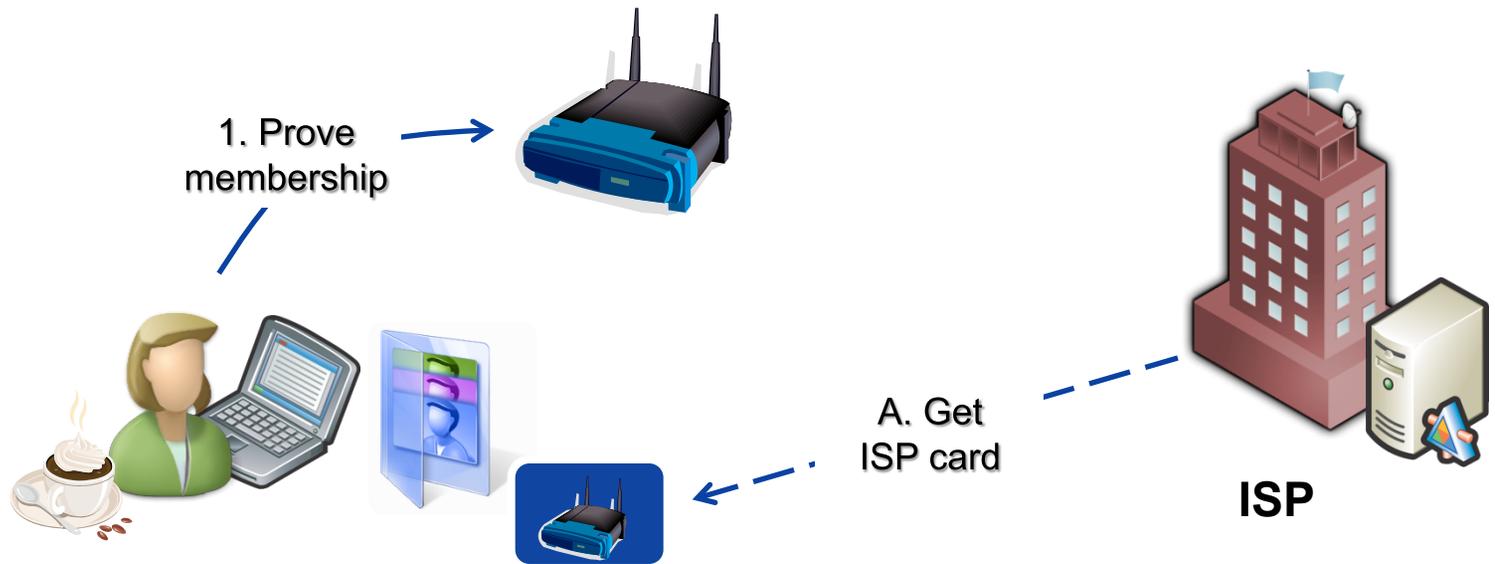
**Relying  
Party**



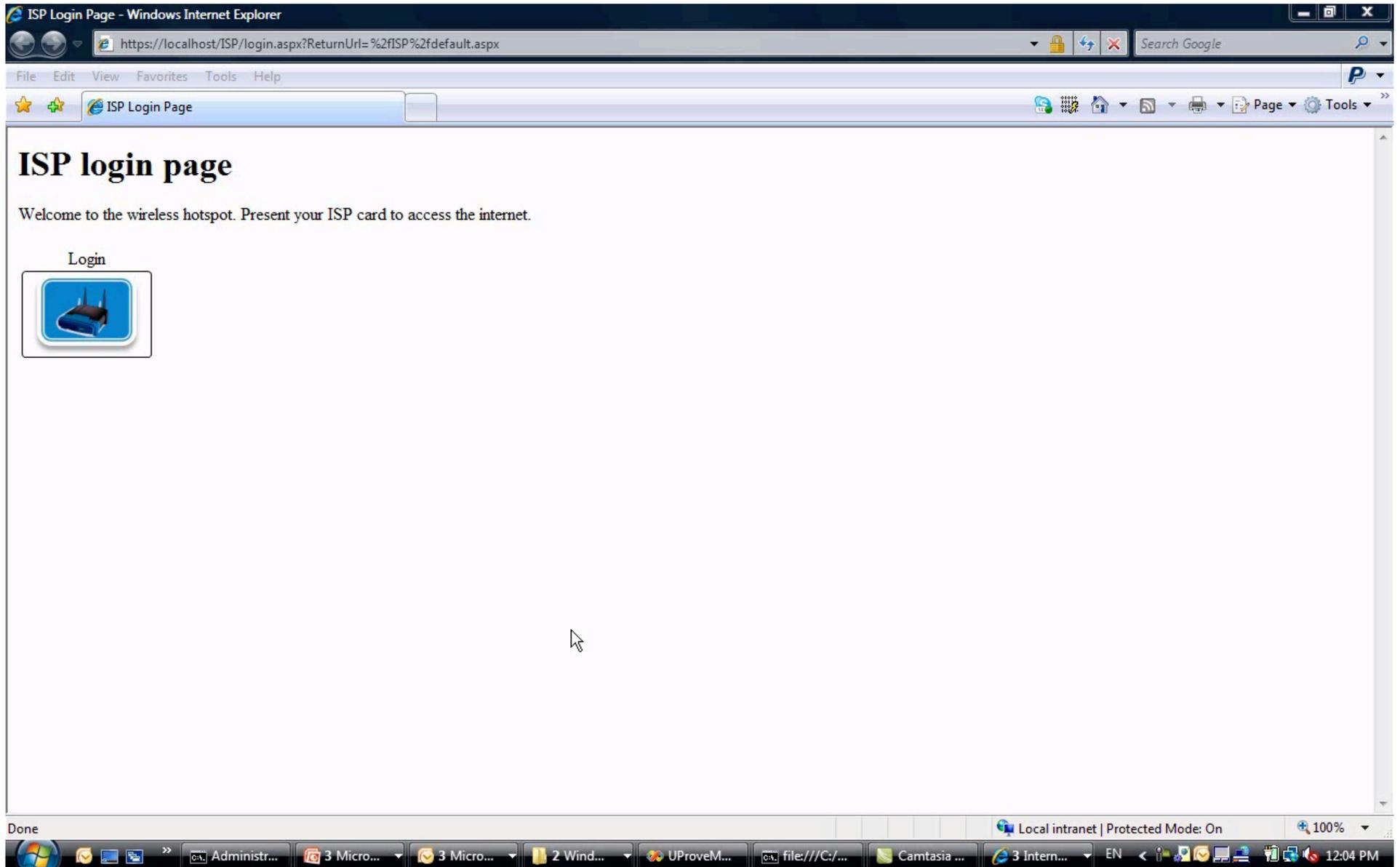
# Minimal Disclosure Token



# Scenarios



# Signing on to a Hot Spot



The screenshot shows a Windows Internet Explorer browser window titled "ISP Login Page - Windows Internet Explorer". The address bar displays the URL: `https://localhost/ISP/login.aspx?ReturnUrl=%2fISP%2fdefault.aspx`. The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The address bar also features a search box with "Search Google" and a "Page" dropdown menu. The main content area of the browser displays the following text:

## ISP login page

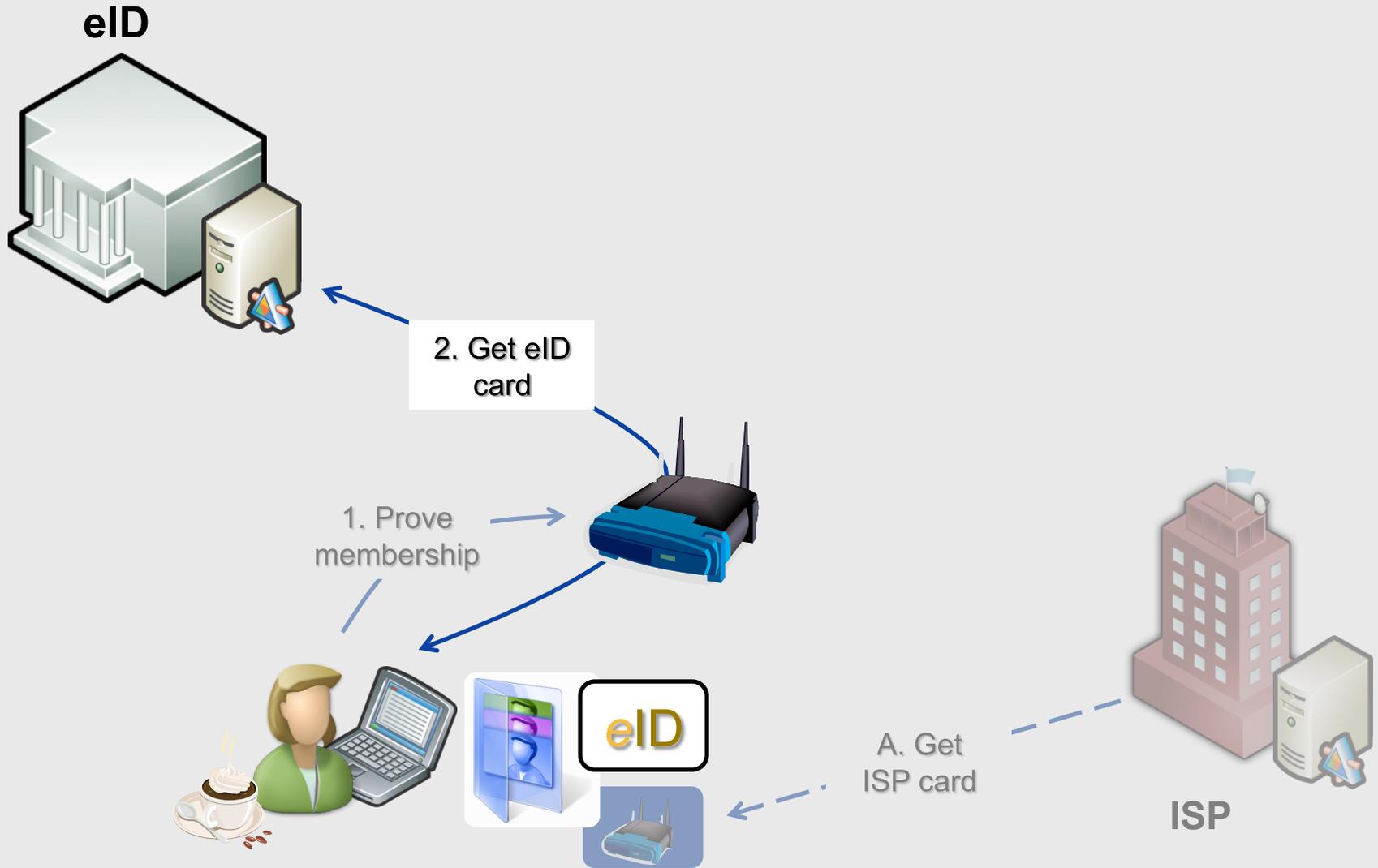
Welcome to the wireless hotspot. Present your ISP card to access the internet.

Login



The button is labeled "Login" and is positioned below the welcome message. The browser's status bar at the bottom shows "Done", "Local intranet | Protected Mode: On", and "100%". The Windows taskbar at the very bottom displays several open applications, including "Administr...", "3 Micro...", "2 Wind...", "UProveM...", "file:///C:/...", "Camtasia ...", and "3 Intern...". The system clock in the bottom right corner shows "12:04 PM".

# Scenarios



# Getting an eID Information Card

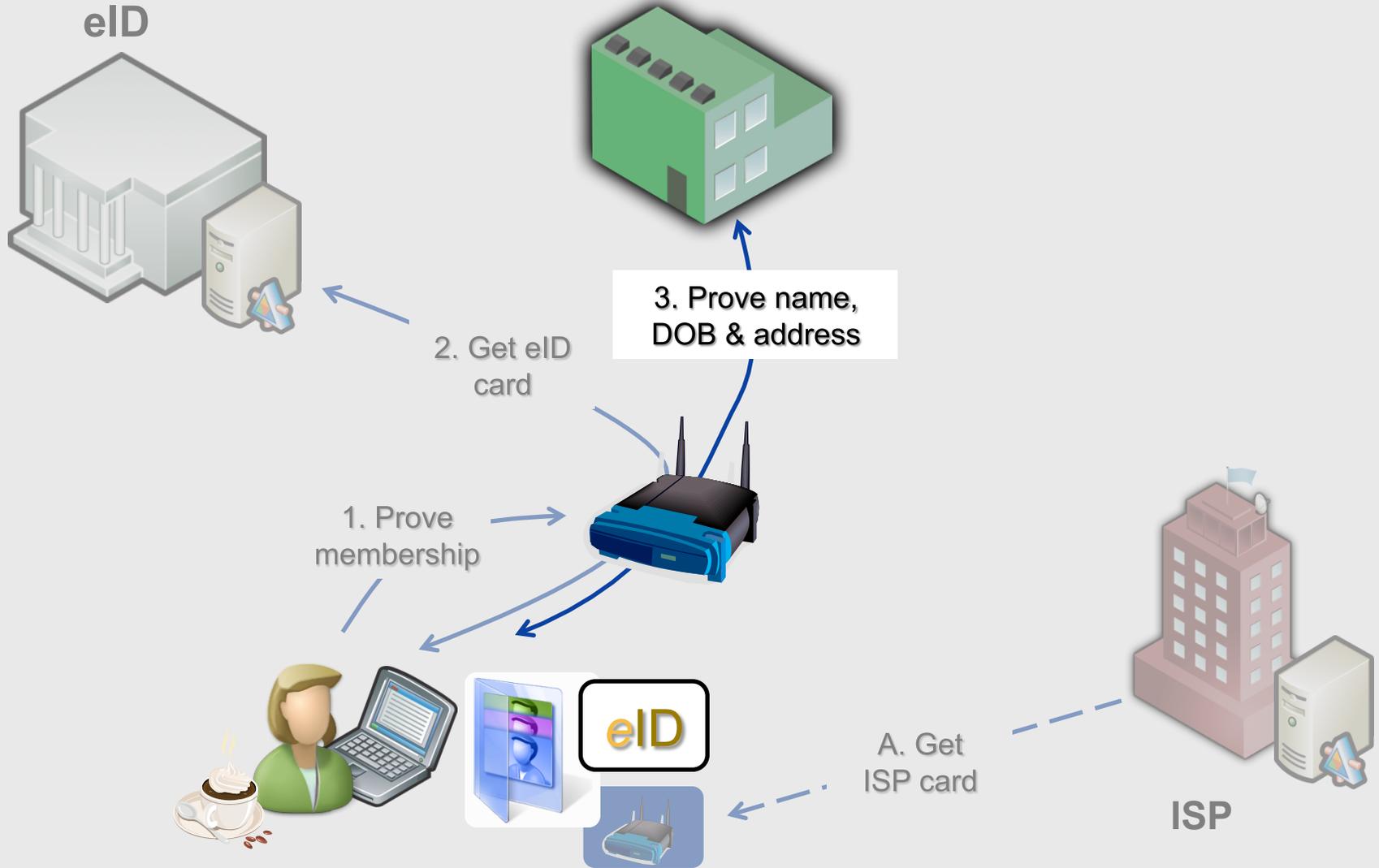
The screenshot shows a Windows Internet Explorer browser window with the following content:

- Address Bar:** <https://localhost/eID/Default.aspx>
- Page Title:** eID
- Logo:** BRITISH COLUMBIA The Best Place on Earth
- Section Header:** Welcome to eID
- Section Header:** Begin registration
- Text:** To begin registration, you need to fill out some information below and visit a point of service to obtain an activation code.
- Text:** [Begin registration.](#)
- Section Header:** Complete registration
- Text:** If you have an activation code, [click here to get your eID card.](#)

The browser's status bar at the bottom indicates "Local intranet | Protected Mode: On" and "100%". The Windows taskbar at the very bottom shows several open applications, including "2 Micro...", "3 Micro...", "2 Wind...", "Camtasia ...", "UProveM...", and "file:///C:/...", along with the system clock showing "12:46 PM".

# Scenarios

## Birth certificate RP



# Ordering a Birth Certificate

Vital Statistics Agency - Windows Internet Explorer

https://localhost/RP1/default.aspx

Search Google

File Edit View Favorites Tools Help

Vital Statistics Agency

 **BRITISH COLUMBIA**  
The Best Place on Earth

## Welcome to the Vital Statistics Agency

### Order your birth certificate

Present your eID card to order your birth certificate (don't have one? get it [here](#)).



Done

Local intranet | Protected Mode: On 100%

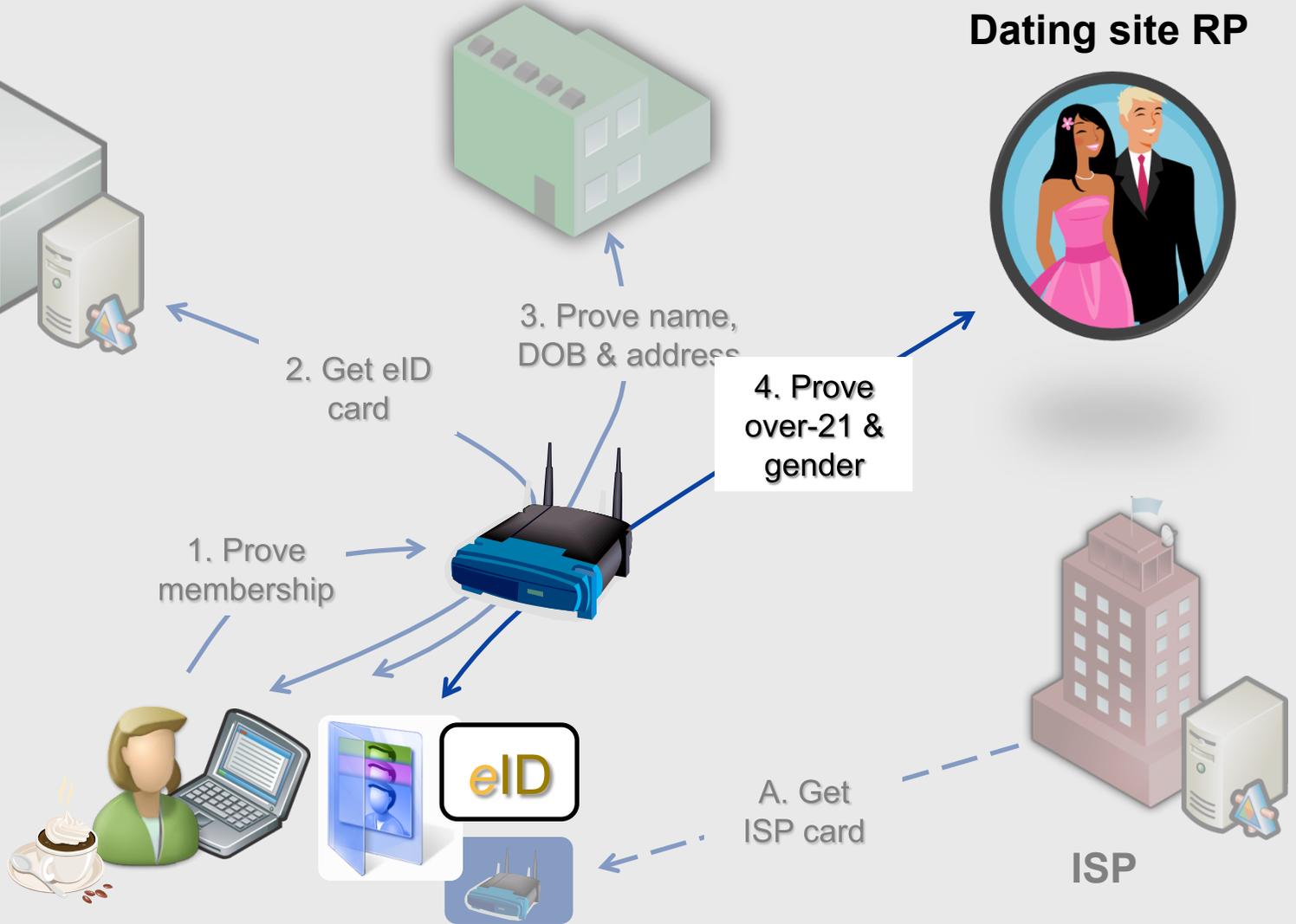
Administr... 3 Micro... 3 Micro... 2 Wind... UProveM... file:///C:/... Camtasia ... 2 Intern... EN 12:07 PM

# Scenarios

Birth certificate RP

eID

Dating site RP



2. Get eID card

3. Prove name, DOB & address

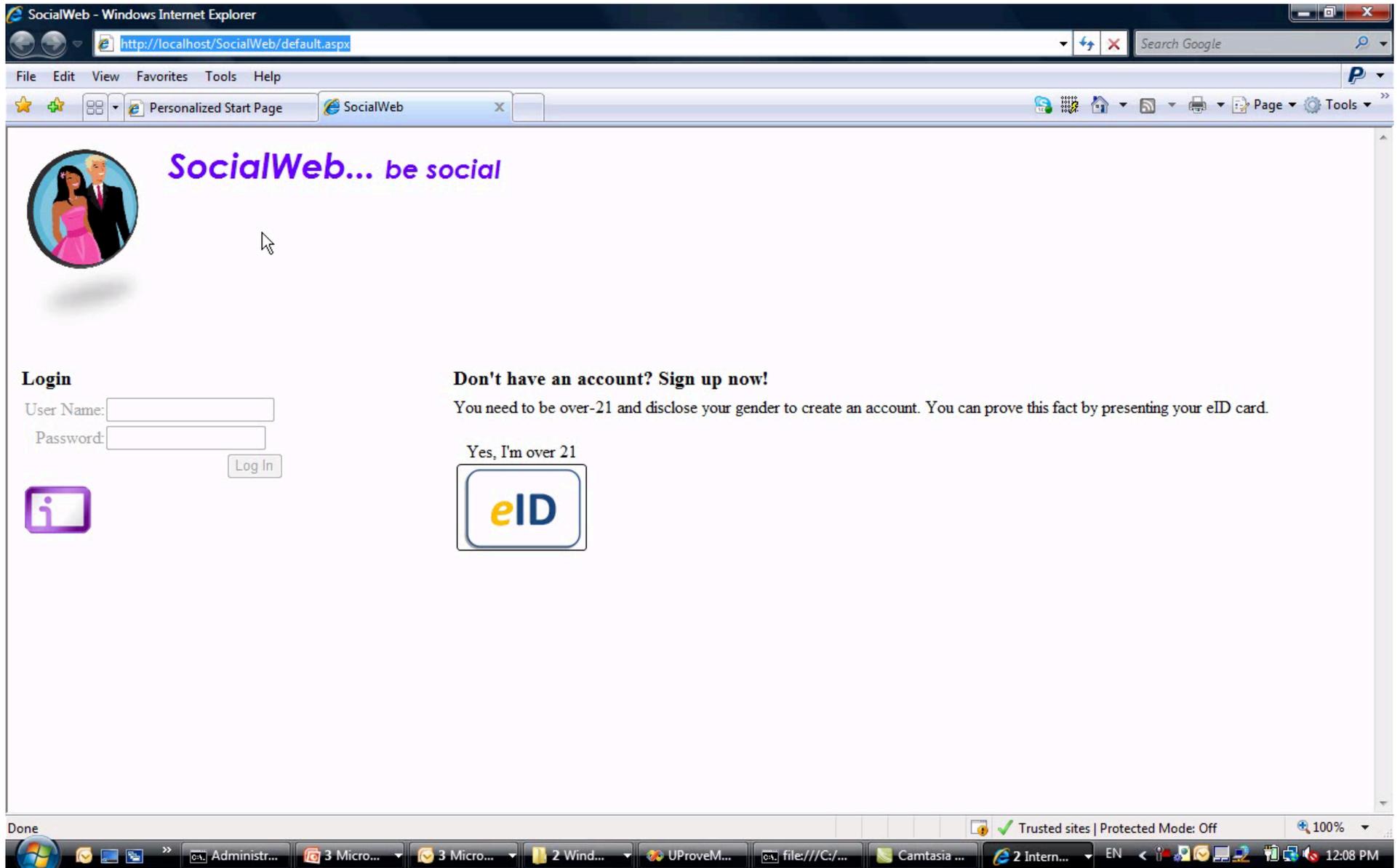
4. Prove over-21 & gender

1. Prove membership

A. Get ISP card

ISP

# Visiting a Social Website



The screenshot shows a Windows Internet Explorer browser window displaying a social website. The address bar shows the URL `http://localhost/SocialWeb/default.aspx`. The page features a logo with a couple and the text "SocialWeb... be social". Below the logo, there is a "Login" section with input fields for "User Name:" and "Password:", and a "Log In" button. To the right, there is a "Don't have an account? Sign up now!" section with a text box for "Yes, I'm over 21" and an "eID" button. The browser's taskbar at the bottom shows several open applications, including "Administr...", "3 Micro...", "2 Wind...", "UProveM...", "file:///C:/...", "Camtasia ...", and "2 Intern...". The system tray shows the time as 12:08 PM.

SocialWeb - Windows Internet Explorer

`http://localhost/SocialWeb/default.aspx` Search Google

File Edit View Favorites Tools Help

Personalized Start Page SocialWeb

 **SocialWeb... be social**

**Login**

User Name:

Password:

Log In



**Don't have an account? Sign up now!**

You need to be over-21 and disclose your gender to create an account. You can prove this fact by presenting your eID card.

Yes, I'm over 21



Done

Trusted sites | Protected Mode: Off 100%

Administr... 3 Micro... 3 Micro... 2 Wind... UProveM... file:///C:/... Camtasia ... 2 Intern... EN 12:08 PM

# Contact:

<http://www.identityblog.com>

**kcameron at microsoft.com**

**Chat with Microsoft's identity  
and access at the exhibit**