Microsoft's Identity and Access Strategy

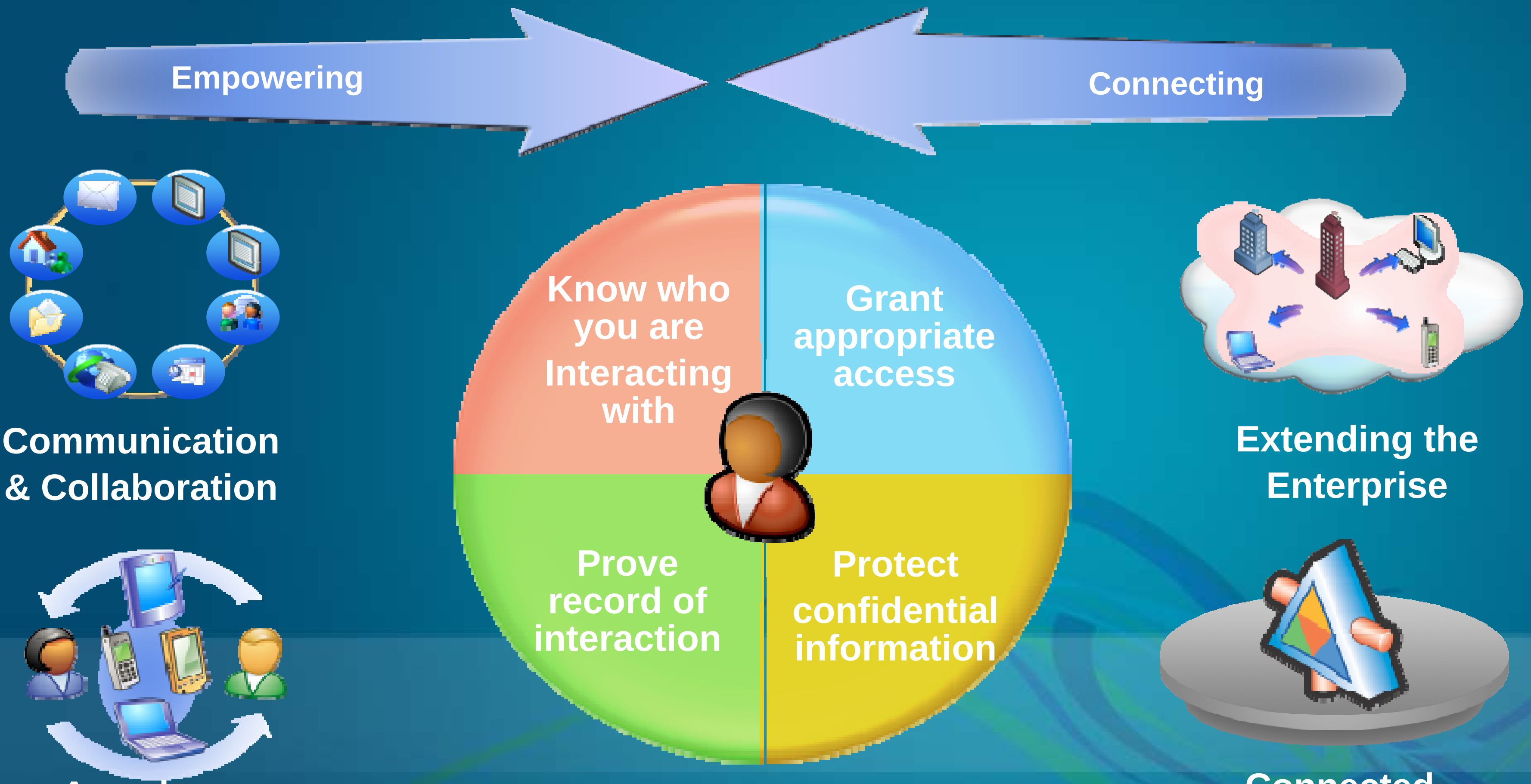
Kim Cameron
Chief Architect of Identity,
Microsoft Corporation

Outline

- The Power of Identity
- Challenges with Identity
- Laws of Identity
- Identity Metasystem
- Microsoft Product Strategy
  - Active Directory
  - InfoCard

Microsoft

The Power of Identity



Empowering

Connecting

Know who you are Interacting with

Grant appropriate access

Prove record of interaction

Protect confidential information

Communication & Collaboration

Anywhere Access

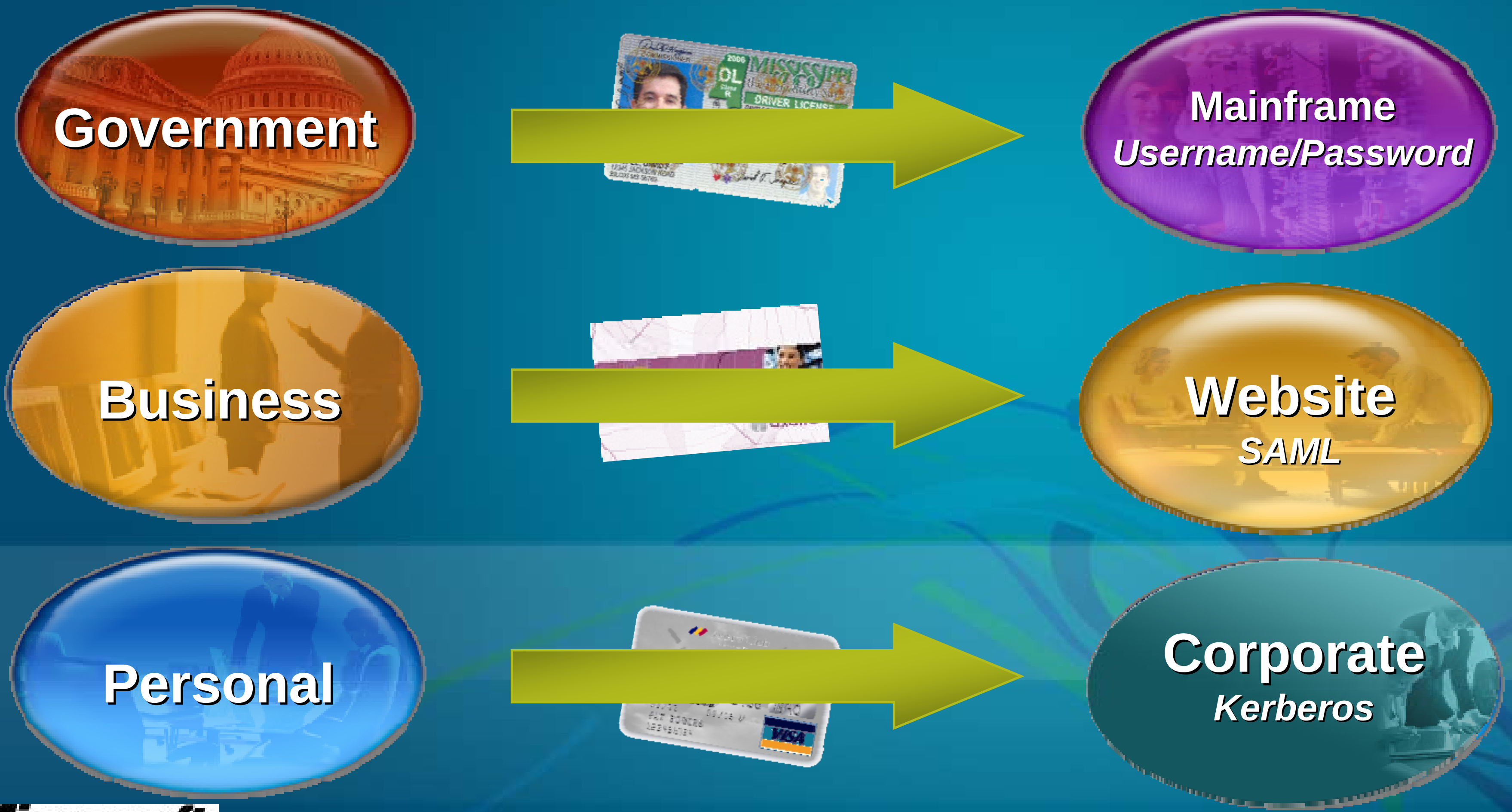
Extending the Enterprise

Connected Systems

Today: Multiple Identities… and Multiple Formats

Identity Providers

Relying Parties



Government

Business

Personal

Mainframe

Username/Password

Website

SAML

Corporate

Kerberos

Threats to Online Safety

- The Internet was built without a way to know who and what you are connecting to
  - Internet services have one-off "workarounds"
  - Inadvertently taught people to be phished
- Greater use and greater value attract professional international criminal fringe
  - Exploit weaknesses in patchwork
  - Phishing and pharming at 1000% CAGR
- Missing an "Identity layer"
  - No simplistic solution is realistic

Microsoft

Lessons from Passport

- Passport designed to solve two problems
  - Identity provider for MSN
    - 250M+ users, 1 billion logons per day
  - Identity provider for the Internet
    - Unsuccessful
- Learning: solution must be different than Passport

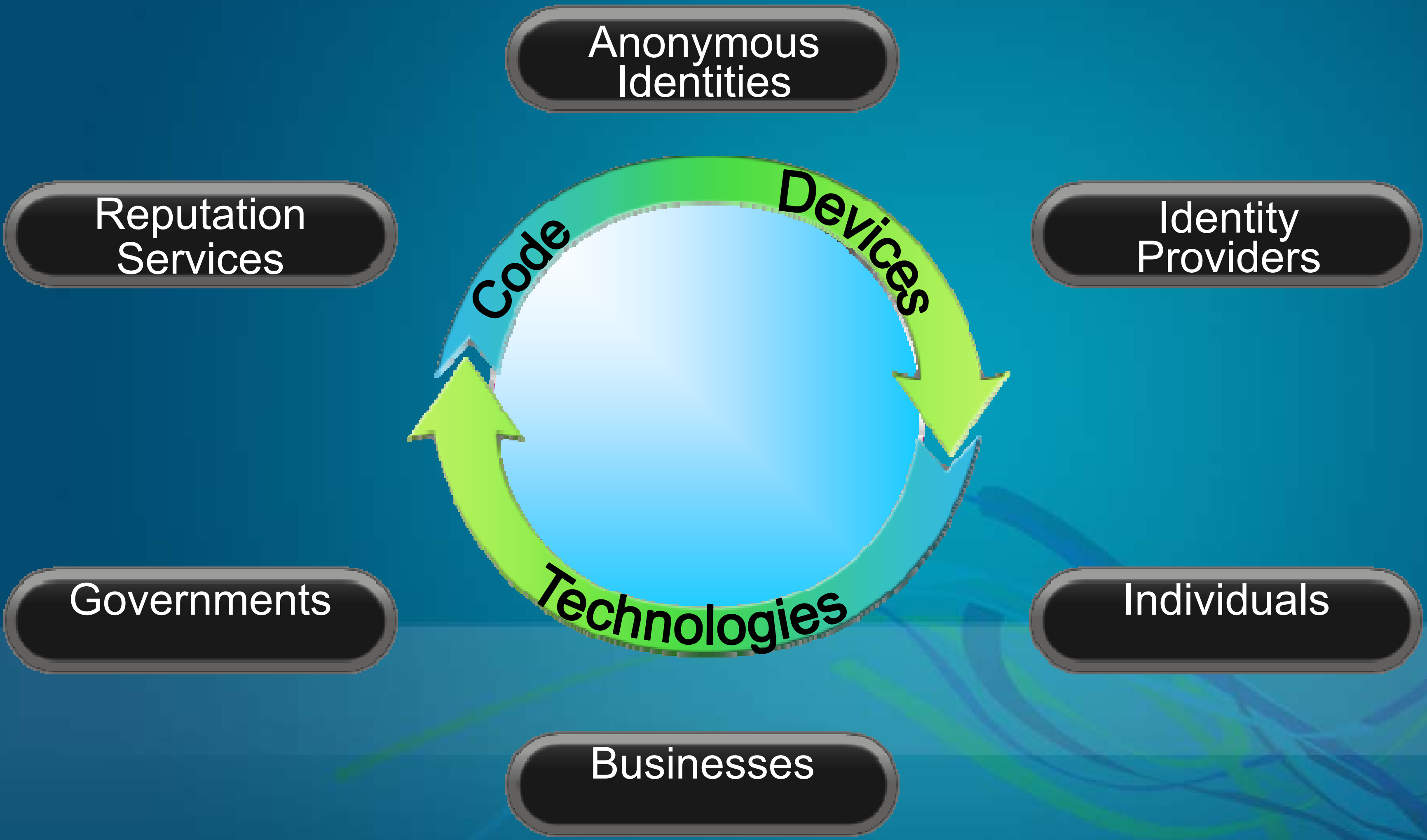
The Laws of Identity

An 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



Anonymous Identities

Reputation Services

Identity Providers

Governments

Individuals

Businesses

Key Characteristics

Requirements for an identity metasystem

Negotiation Driven

Enable relying party, subject, and identity provider to negotiate technical policy requirements

Encapsulation

Technology-agnostic way to exchange policies and claims between identity provider and relying party

Claims Transformation

Trusted way to change one set of claims regardless of token format into another

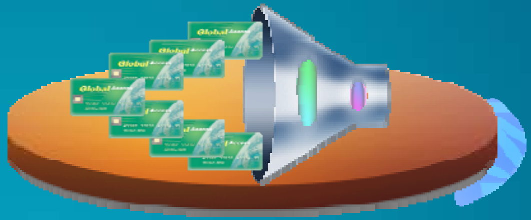
User Experience

Consistent user interface across multiple systems and technologies

Metasystem Players

Identity Providers

Issue identities



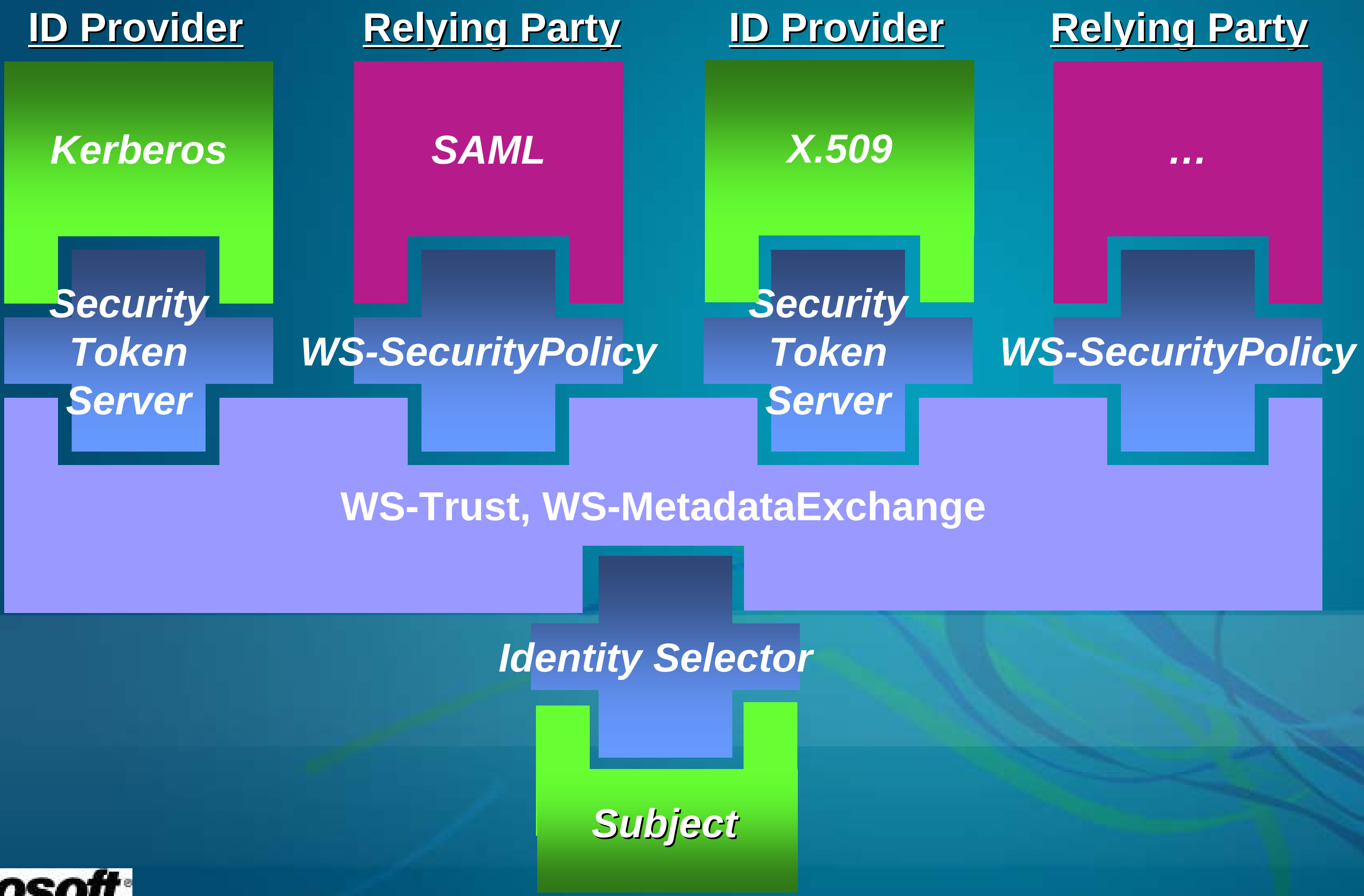
Relying Parties

Require identities

Subjects

Individuals and other entities about whom claims are made

Web Services Metasystem Architecture



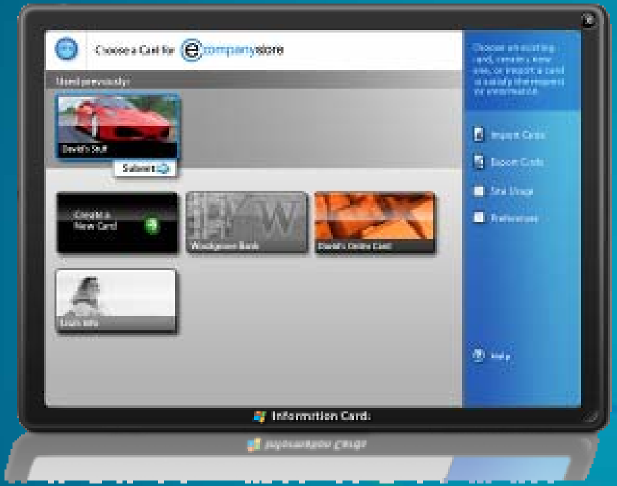
Microsoft

InfoCard

Returning Identity Control to the End User

Easier

- Reduces reliance on usernames & passwords
- Consistent user interface for login and registration
- Grounded in real-world metaphor



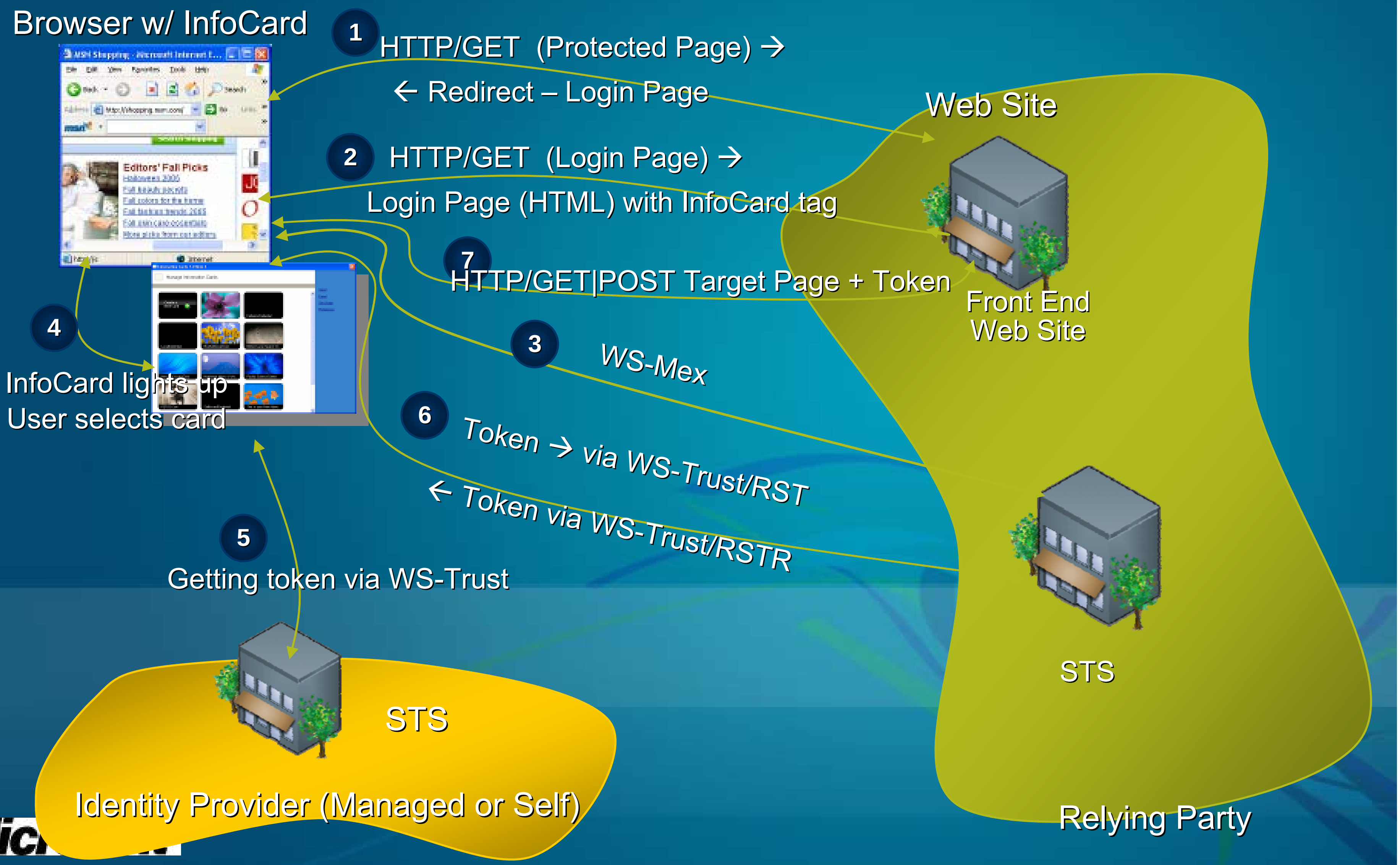
Choose an existing card, create a new one, or import a card to satisfy the request for information.

Safer

- Helps end users avoid many phishing attacks
- Support for two-factor authentication
- Secure subsystem
- Self-asserted and "managed" identities

Built on Web Services Protocols

InfoCard Protocol Flow



Browser w/ InfoCard

1 HTTP/GET (Protected Page) →

← Redirect – Login Page

2 HTTP/GET (Login Page) →

Login Page (HTML) with InfoCard tag

7 HTTP/GET|POST Target Page + Token

3 WS-Mex

4 InfoCard lights up
User selects card

6 Token → via WS-Trust/RST

← Token via WS-Trust/RSTR

5 Getting token via WS-Trust

Web Site

Front End
Web Site

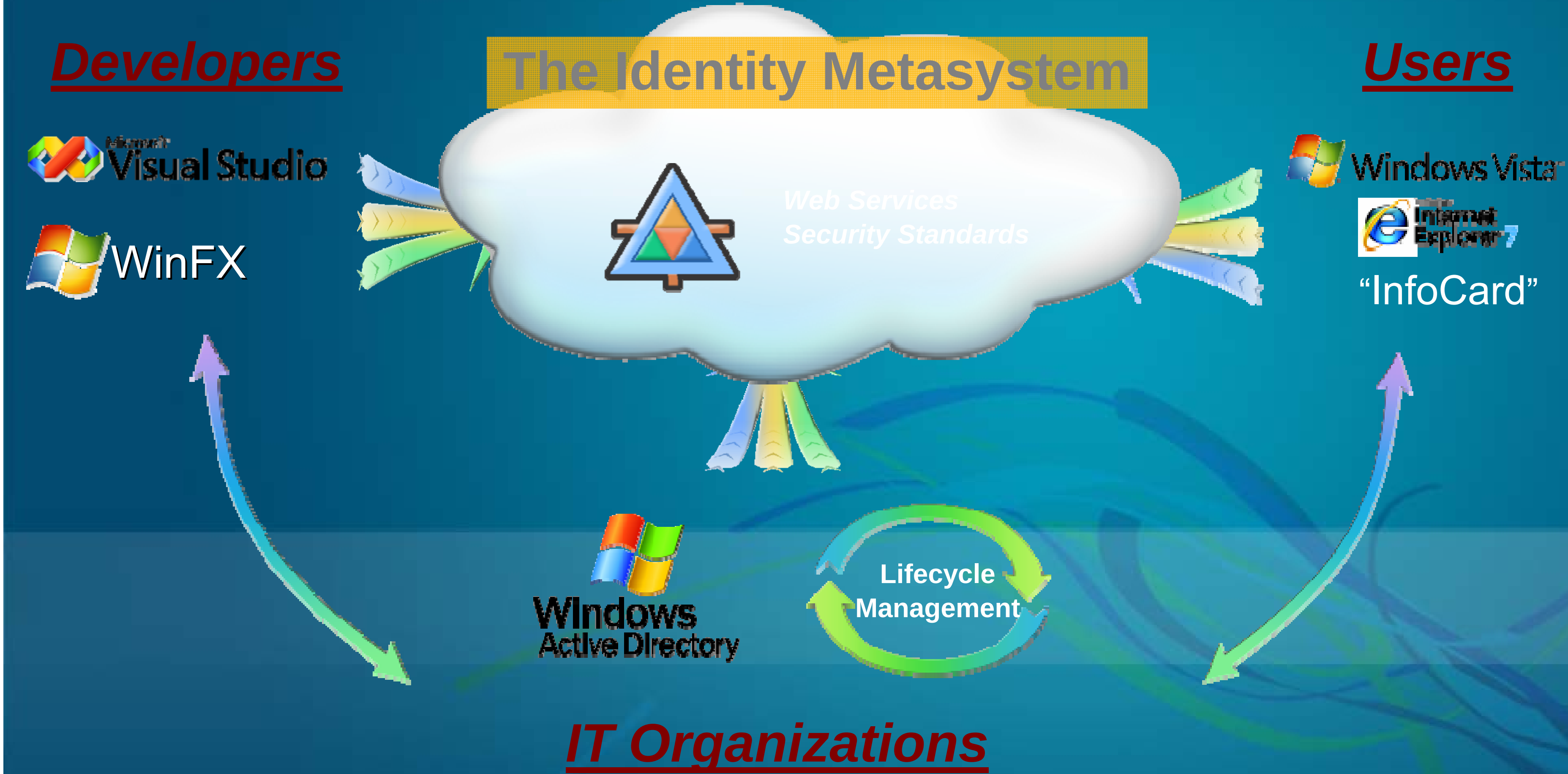
STS

Relying Party

STS

Identity Provider (Managed or Self)

Microsoft Support For The Metasystem



Microsoft

Active Directory As An Evolving System

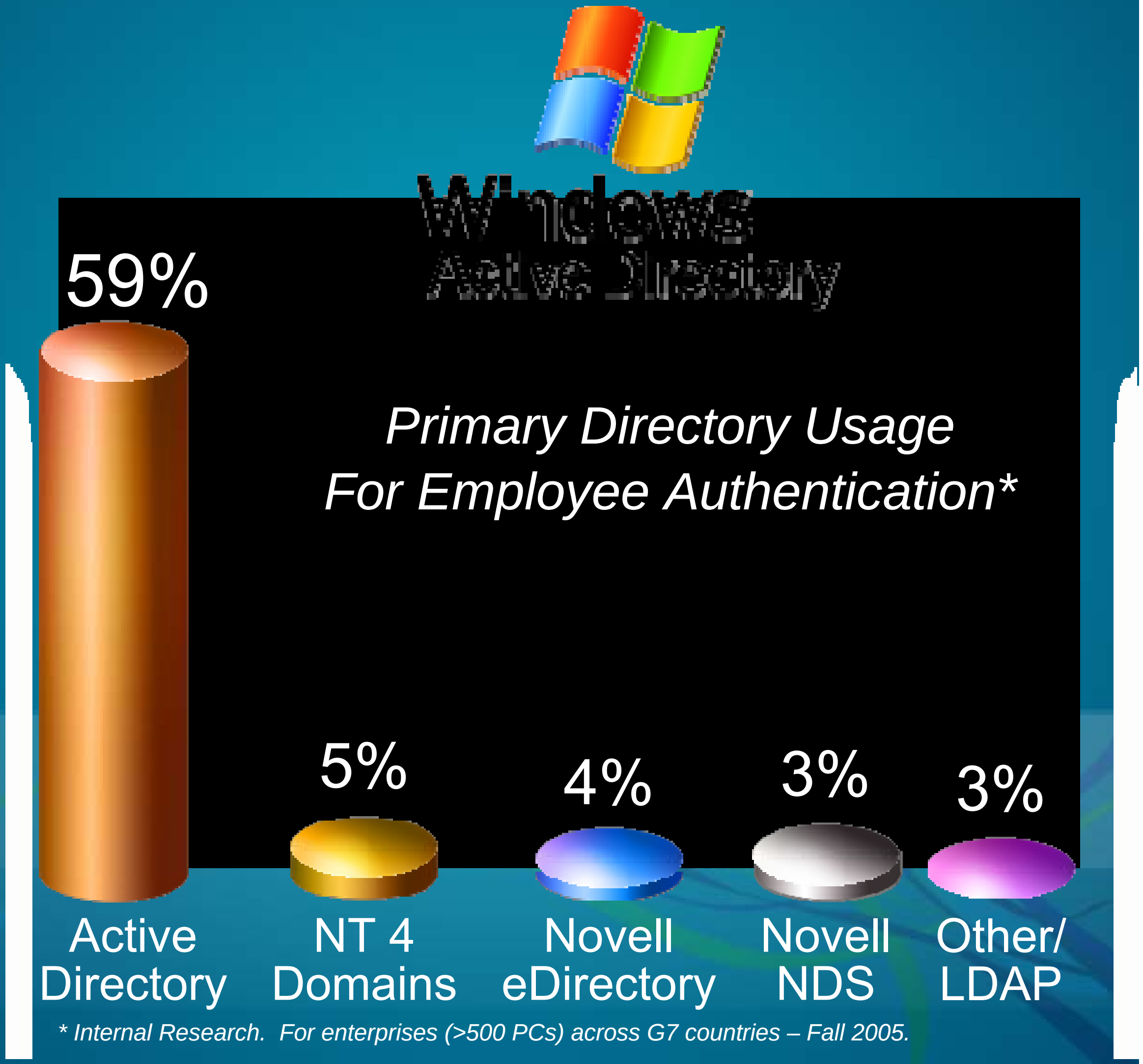
Strong Credentials
Certificate Services

Information Rights
Rights Management Services

Federated Identity
Active Directory Federation Services

IDA Management
Microsoft Identity Integration Server

Domain and Directory Services
Windows Active Directory



*Primary Directory Usage For Employee Authentication**

** Internal Research. For enterprises (>500 PCs) across G7 countries – Fall 2005.*

Microsoft’s Active Directory Vision

Unleash The Power of Identity

Unified

- ► Simplified deployment of a broad set of capabilities
- ► Consistent policy and access control model
- ► Unified management experience

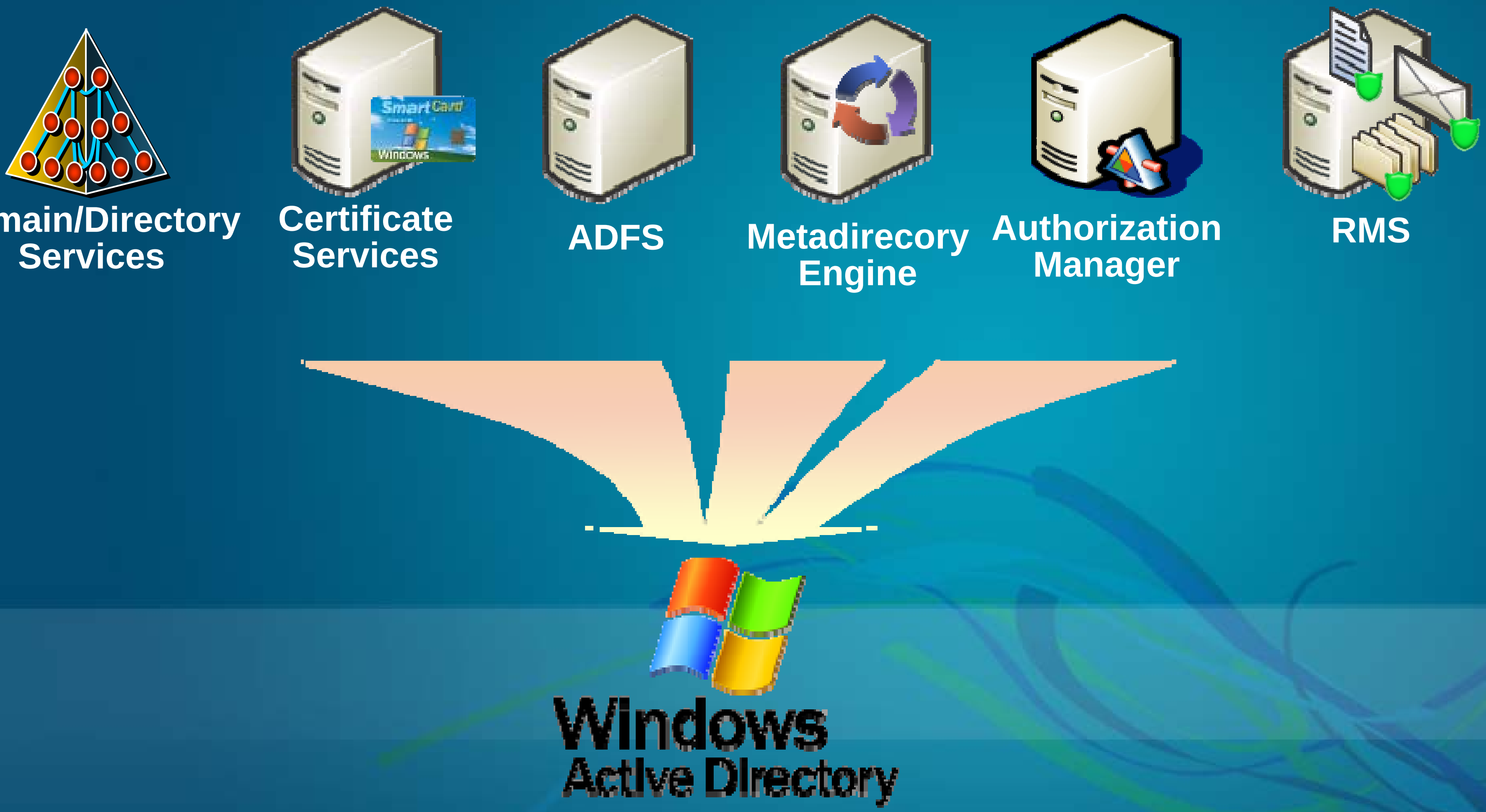
Connected

- ► Frictionless customer and partner interactions
- ► Easy access to Internet services
- ► Extends the reach of apps and information workers

Integrated

- ► Seamless user experience across applications
- ► Common identity across all applications & services
- ► Simplified development of identity aware applications

AD for Unified Identity & Access



Domain/Directory Services

Certificate Services

ADFS

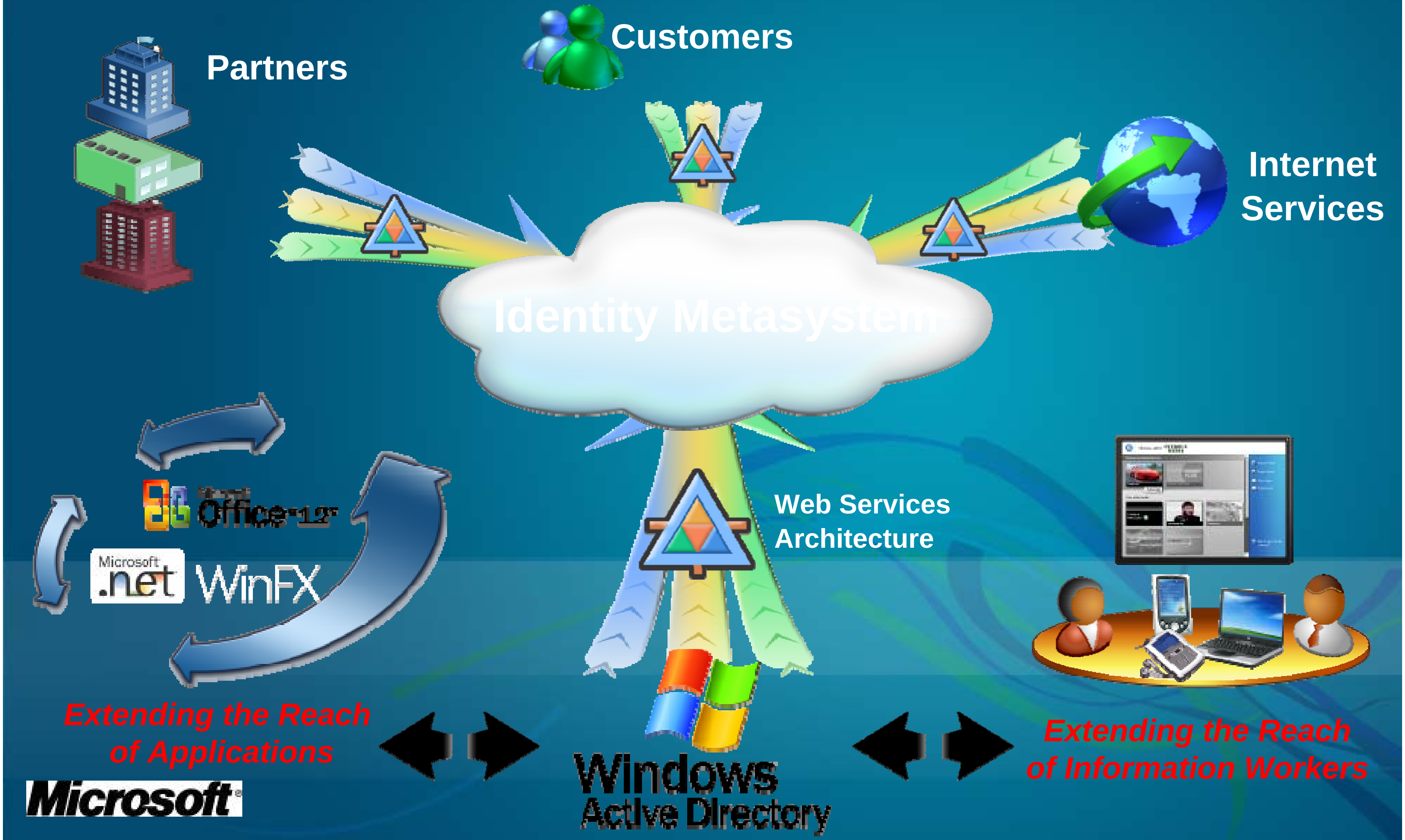
Metadirecory Engine

Authorization Manager

RMS

Unified architecture, policy model, and management experience

AD for Outward-Facing Connected Identity



Partners

Customers

Internet Services

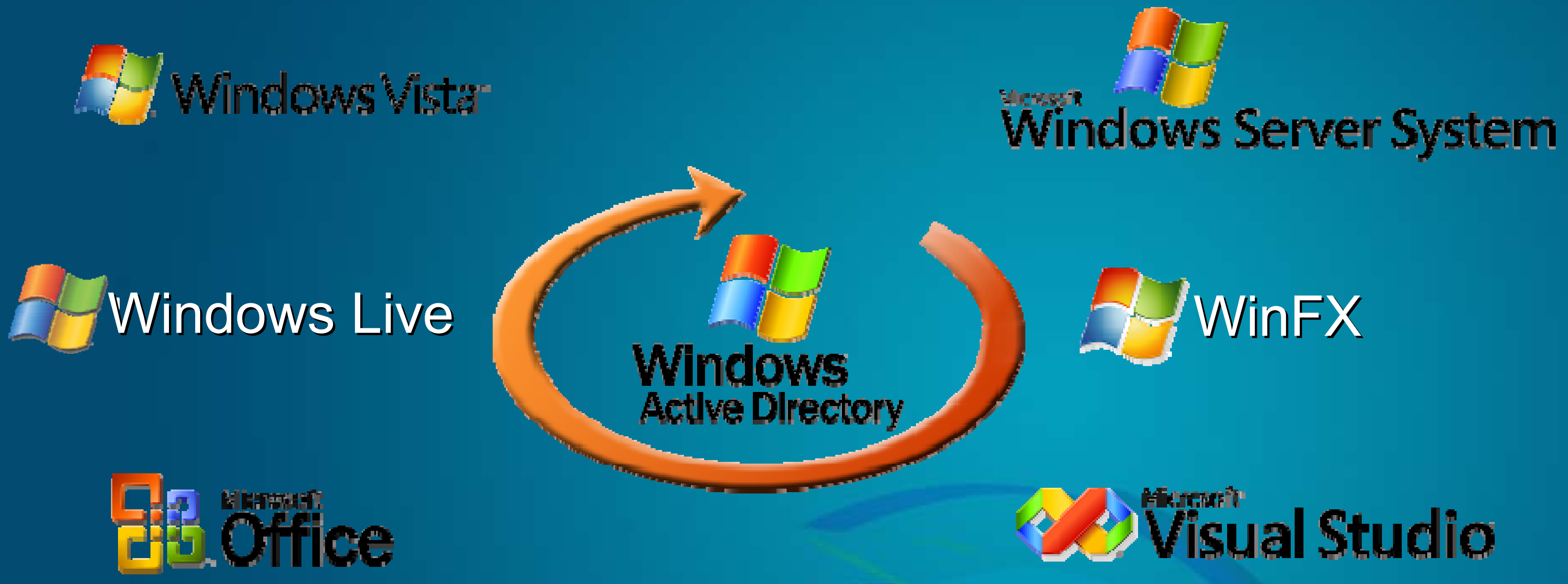
Identity Metasystem

Web Services Architecture

Extending the Reach of Applications

Extending the Reach of Information Workers

Integrating Identity Across Our Offerings



Common Infrastructure and Experiences Access…

Access Control **Information Rights** **Federation** **Auditing**

Directory **Smartcard Logon** **Single Sign-on**

Managing Identity and Access

- Heterogeneous Identity Aggregation
- Policy-Driven Workflow
- Automated Provisioning

- Simplified Credential Management
- Smart Card Integration
- Policy-Driven Workflow

Summary

- We are proponents of an Identity, Privacy and Trust Ecosystem where everyone is welcome
- We are adopting a holistic approach making identity easy and safe for end users, application developers, web sites and IT professionals
- Microsoft sees an Identity Metasystem based on Web Service Standards as the way to reach across devices, platforms and applications
- We are planning to unleash the Power of Identity by making all our products identity aware
- We have an inclusive vision, we are executing on it, and we look forward to working with everyone in the industry to build an Identity Metasystem for the Internet
- Contact me at http://www.identityblog.com

Microsoft®

Your potential. Our passion.™

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Microsoft®