Elektronické služby

Ľubo Goryl
Solutions Professional
Microsoft

Modernising Government

“We're asking everyone to change, not only Government itself….

...We are setting a target that within five years, one quarter of dealings with Government can be done by any member of the public electronically - through their television, telephone or computer”

UK Prime Minister Tony Blair, 2000

Scale of the UK Challenge

- Effectively provide Gov't Services online
  - 4,500+ Services online by 2005
  - Ensure 24x7 availability of services
- Address multiple customers/demographics
  - 60m citizens
  - 3m businesses
- Integrate multiple Government 'departments'
  - 20 large dept's, 100s of local/regional gov't
  - 1,800 backend LOB applications
  - 13,000 paper forms -> 5 billion transactions
- Provide convenient, secure access
  - Varying access via PDA, PC …

Agenda

1. Trends in Identity Management
2. IdM Solution Area
3. Features & Benefits
4. Case studies

What impacts our thinking on e-Identity?

Open & Transparent

Privacy

Wikileaks

data ownership

identity theft

CONSUMERIZATION

Cloud Services

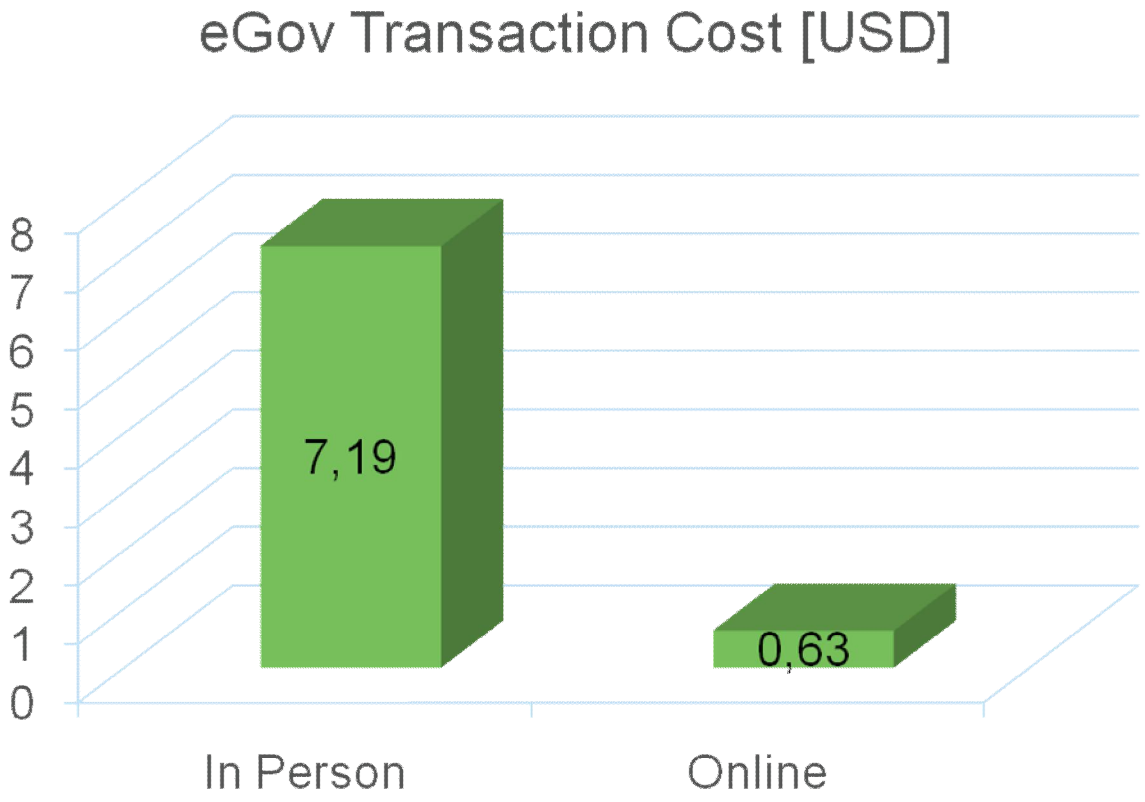
Do More With Less

Mobility

the right to be forgotten

eGov may learn from Internet banking:

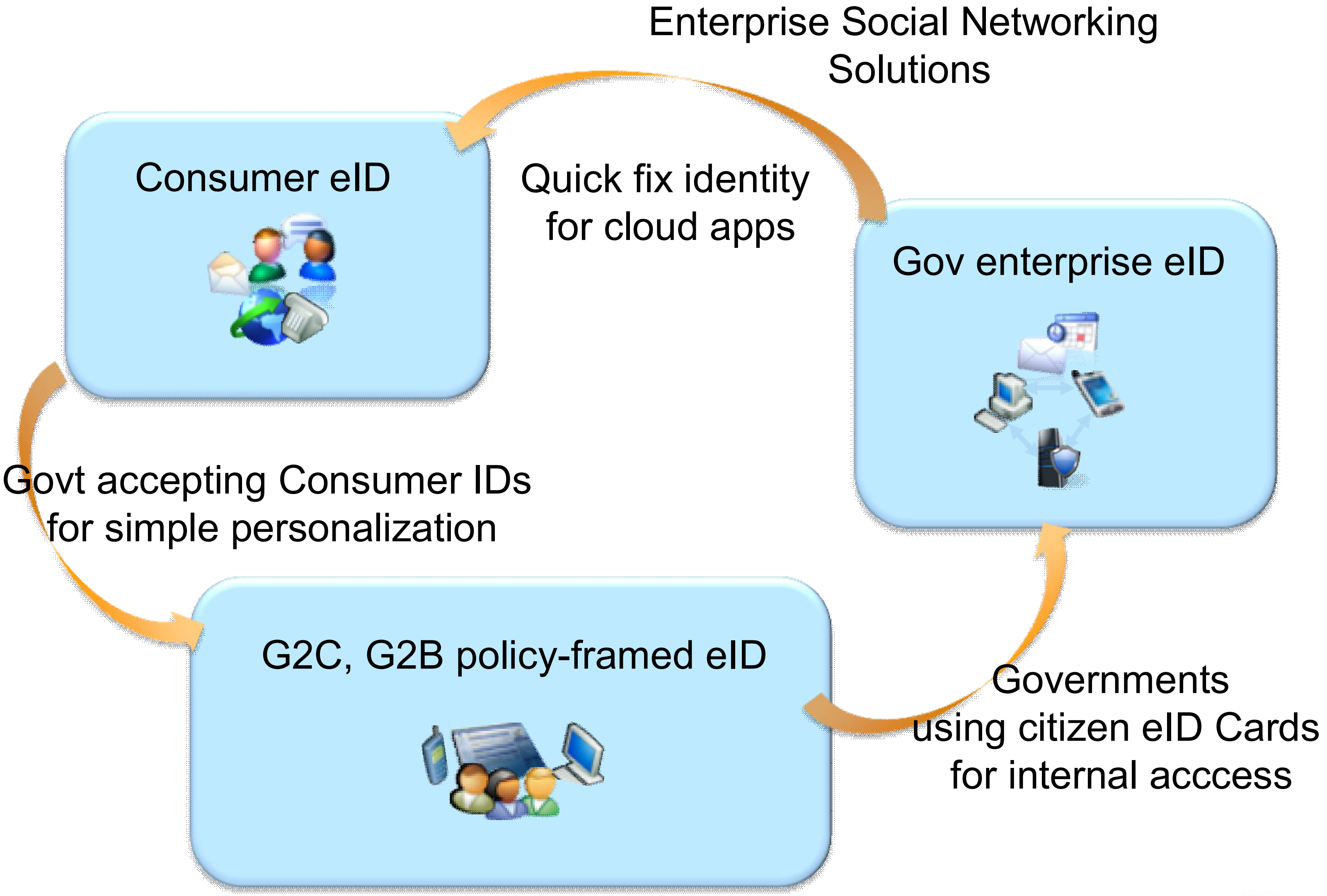
Reduce service delivery cost by moving clients to cheaper channels!



Case presented by U.S. State of Washington Dept. of Licensing CIO, May 2010

Microsoft

Blurring the identity domain borders...



Enterprise Social Networking Solutions

Consumer eID

Quick fix identity for cloud apps

Gov enterprise eID

Govt accepting Consumer IDs for simple personalization

G2C, G2B policy-framed eID

Governments using citizen eID Cards for internal acccess

Microsoft

EU Digital Agenda: “Trust in the Information Society“

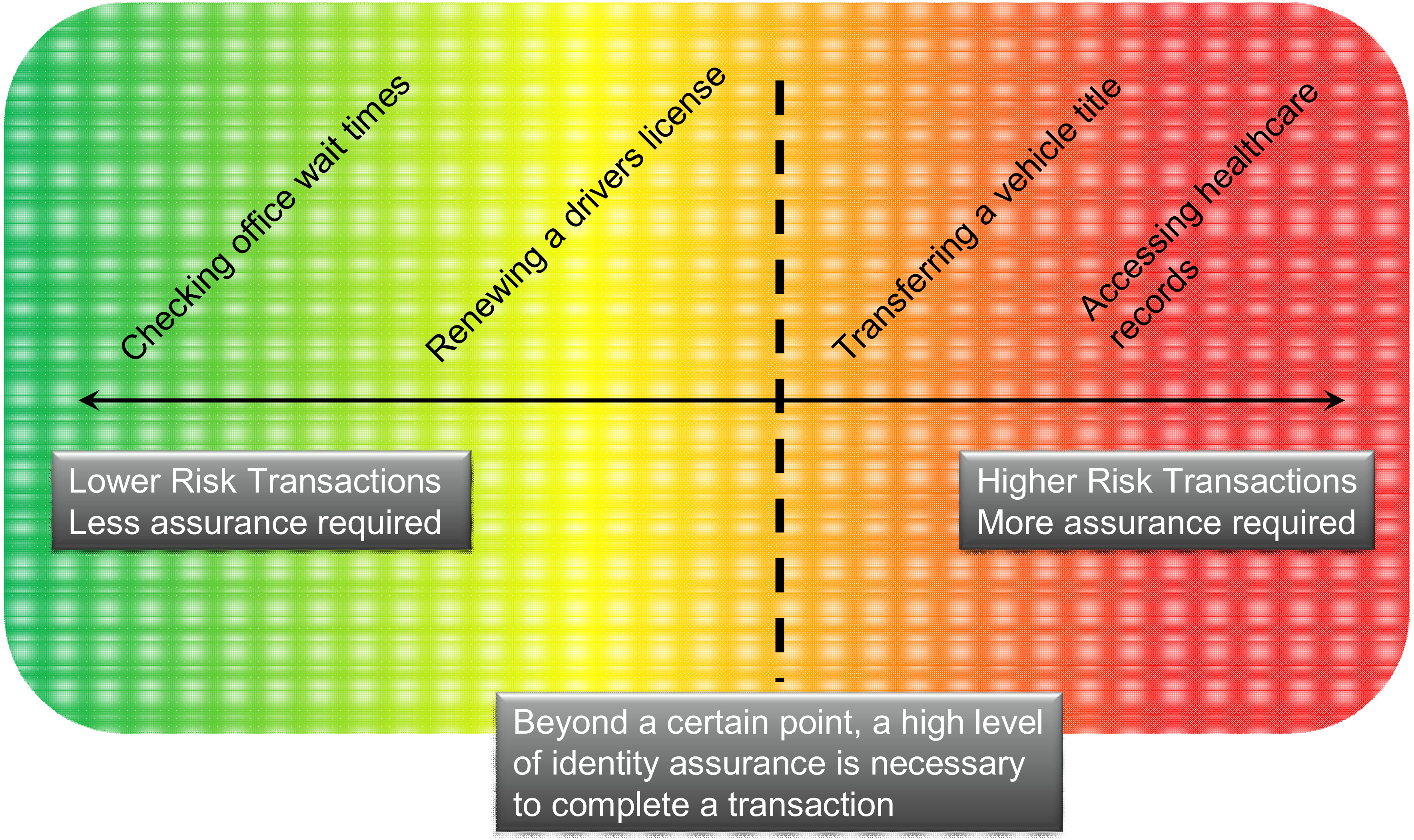
Spanish EU presidency ICT ministerial conference Feb 2010

- Increase trustworthiness, security and interoperability of eGov services and systems in the EU Single Market
- **“Trust by Design“** - Privacy / protection of personal data
- Develop European framework for electronic identity
- Minimal disclosure of personal data
- Make profile aggregation difficult
- eID Framework for interop - eGov, eHealth, and private sector

Europe 2020 Strategy - “Digital Agenda“ from May 2010

- Single market in digital era, enhance trust and security
- Identity as an enabler of trusted eGov services!

Secure eID Enables High-value Transactions Online



Checking office wait times

Renewing a drivers license

Transferring a vehicle title

Accessing healthcare records

Lower Risk Transactions
Less assurance required

Higher Risk Transactions
More assurance required

Beyond a certain point, a high level of identity assurance is necessary to complete a transaction

Some definitions

Term	Meaning
Authentication	Prove that you are eligible for a particular online service (not necessarily revealing your full identity)
Authorization	What are your access rights or access levels
Federated Identity	Trusting on-line users based on some other entity's proof of authentication
Claims-based access	Authorization by means of claims (attributes) Eg. Surname = Jiricek Age>18 = “Yes“
Minimal Disclosure of Personal Information	Reveal the minimal needed set of claims during authentication & authorization
PII	Personal Identifiable Information

Increased Privacy Concerns - Minimize PII Disclosure

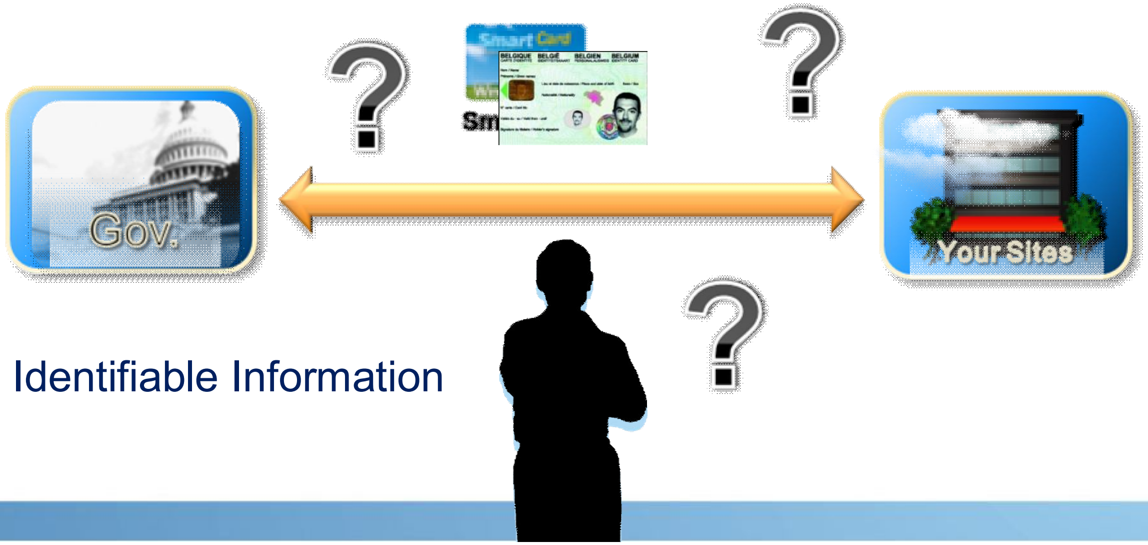
Weakness of the traditional eID authentication:

- Reading X.509 v3 certificate: disclosing all its attributes
- Presented certificate leaves traces at every place visited
- Even in case of Pseudonym log-in, Govt IdP and Service provider may collude and trace citizen transactions

Policy demands both Accountability and Anonymity

- Calling for Minimal PII disclosure and preventing traceability

Need solution supporting both security and privacy

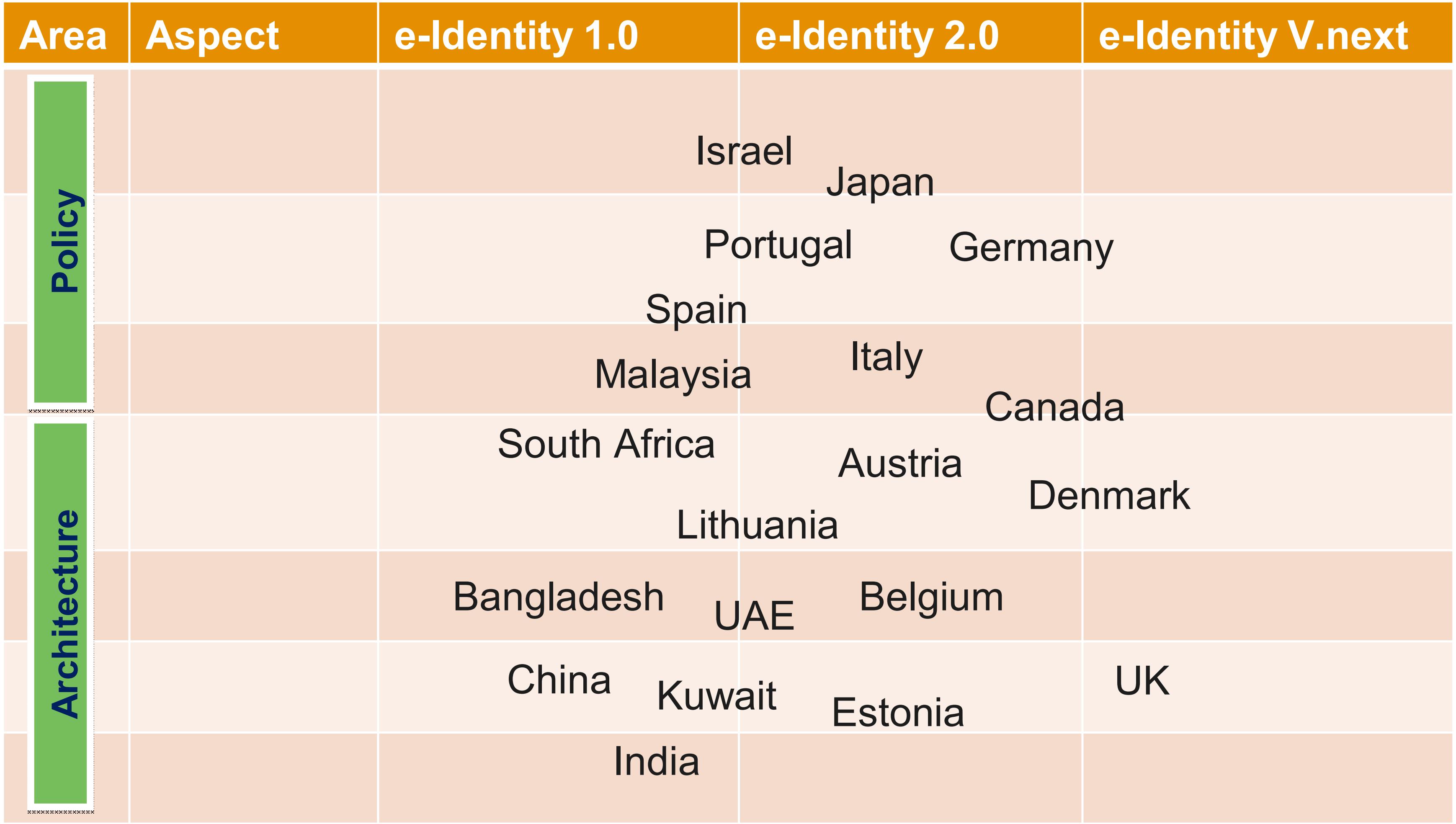


PII = Personal Identifiable Information

Trend: Security & Privacy & Interoperability

Area	Aspect	e-Identity 1.0	e-Identity 2.0	e-Identity V.next
Policy	Privacy	Full disclosure of PII data set in online transactions	Minimal disclosure tokens, but leaving transactions traces	Minimal disclosure tokens without correlation handles
	Citizen data aggregation	Single ID look-up against redundant registries	Aggregating attributes on the fly using single ID	Contextual separation by meaningless IDs
	Interoperability	Single organization	Single constituency	Across countries, gov and commercial
Architecture	Low assurance eIDs	Username & Password separate for each site	Federated ID	Federated ID with anti-phishing features
	Strong assurance eIDs	User data accessible on smartcard or token	IdP federation requiring on-line connectivity	IdP federation – occasionally connected, mobile solutions
	Phishing Protection	Little or no protection by design	User agent, locally installed	User agent as a cloud service
	Biometrics use	Off-line verification (Point of Contact)	On-line verification (Central biom. dbase)	Crypto-biometric authentication

Some Country Examples



Area

Aspect

e-Identity 1.0

e-Identity 2.0

e-Identity V.next

Policy

Architecture

Israel

Japan

Portugal

Germany

Spain

Malaysia

Italy

Canada

South Africa

Austria

Denmark

Lithuania

Bangladesh

UAE

Belgium

China

Kuwait

Estonia

UK

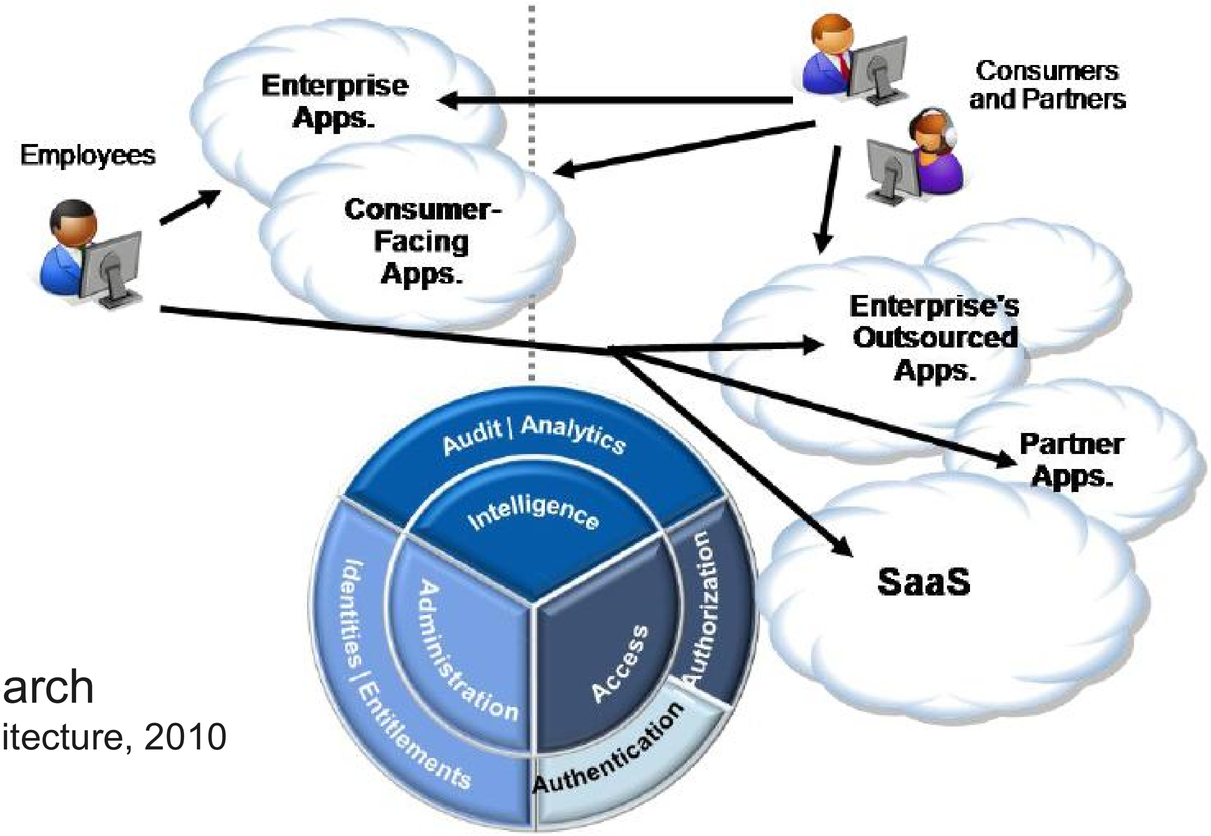
India

Impact of Cloud-Computing Demands on Identity and Access Mgmt

Most large enterprise IAM solutions today are offered as suites, with directory services, user provisioning, role management, Web access management and SSO as common elements of such suites. Recent research confirms concerns regarding IAM integration ability.

Gartner predicts IAM will enter the cloud-computing era with component-based services, not as suites, due to the uneven maturation and availability of suites to fulfill hybrid and cloud-computing needs.

Figure 2. Enterprise IAM Is Being Undone by Cloud Computing



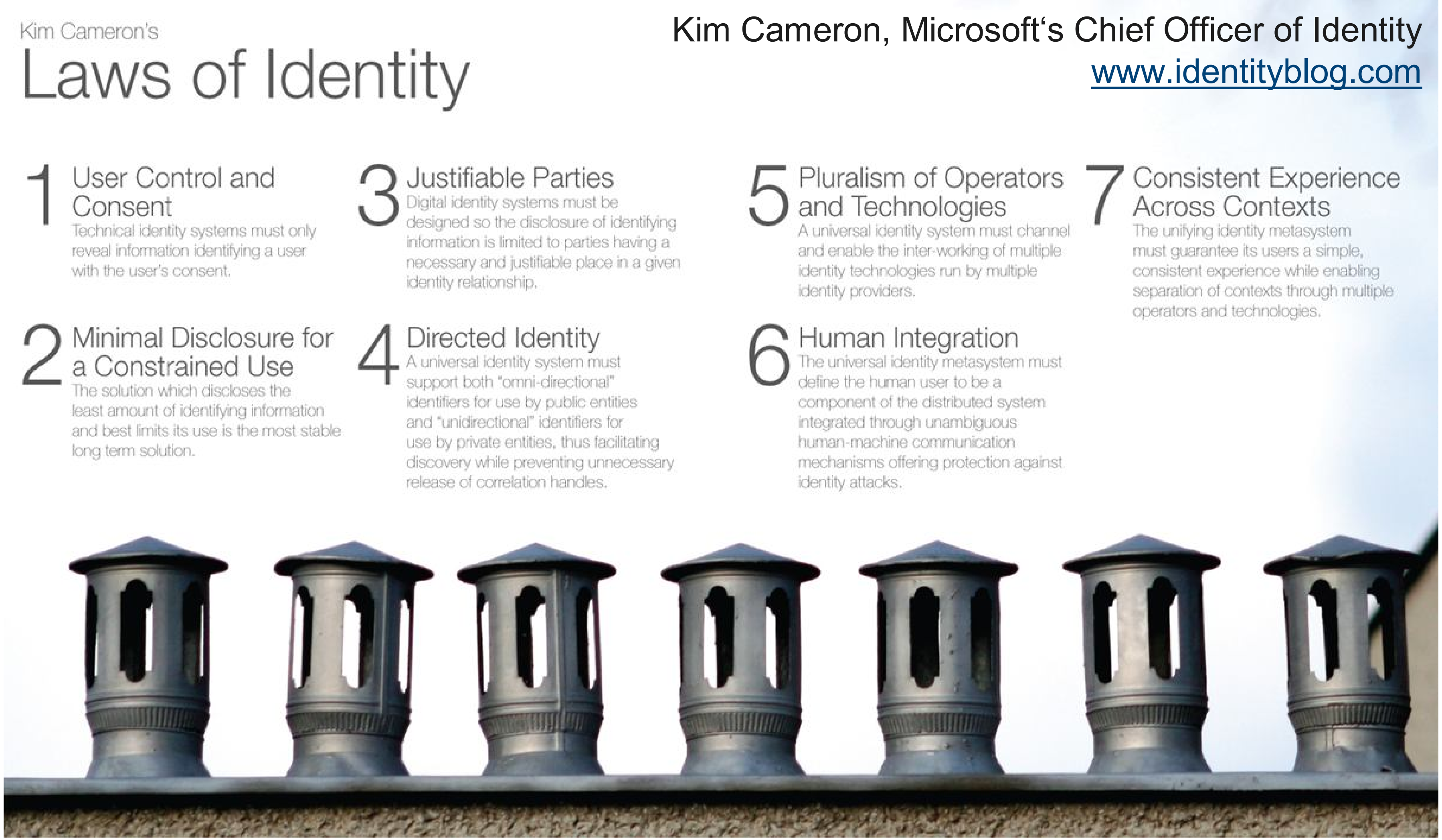
Source: Gartner Research

Identity's Role in Cloud Architecture, 2010

ID Number: G00206421

Microsoft‘s Direction Gets Industry Traction

Kim Cameron, Microsoft‘s Chief Officer of Identity
www.identityblog.com



Kim Cameron's

Laws of Identity

1 **User Control and Consent**
Technical identity systems must only reveal information identifying a user with the user's consent.

2 **Minimal Disclosure for a Constrained Use**
The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3 **Justifiable Parties**
Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4 **Directed Identity**
A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

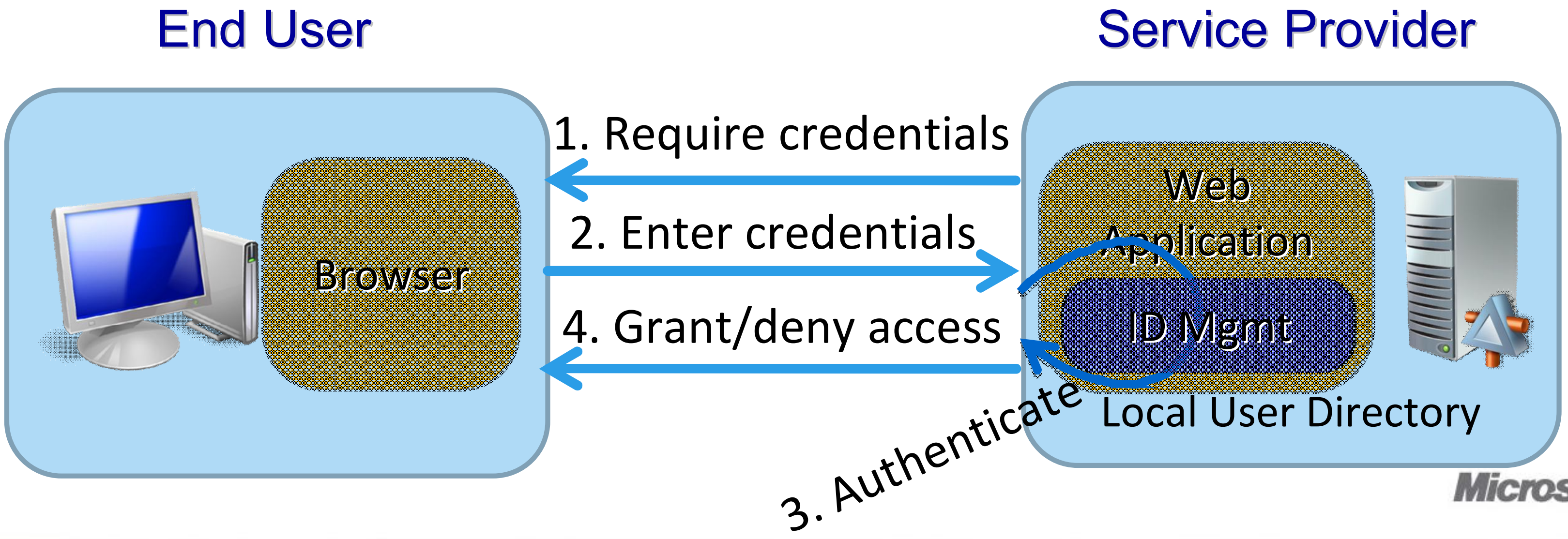
5 **Pluralism of Operators and Technologies**
A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 **Human Integration**
The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7 **Consistent Experience Across Contexts**
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

e-Identity 1.0 Concept

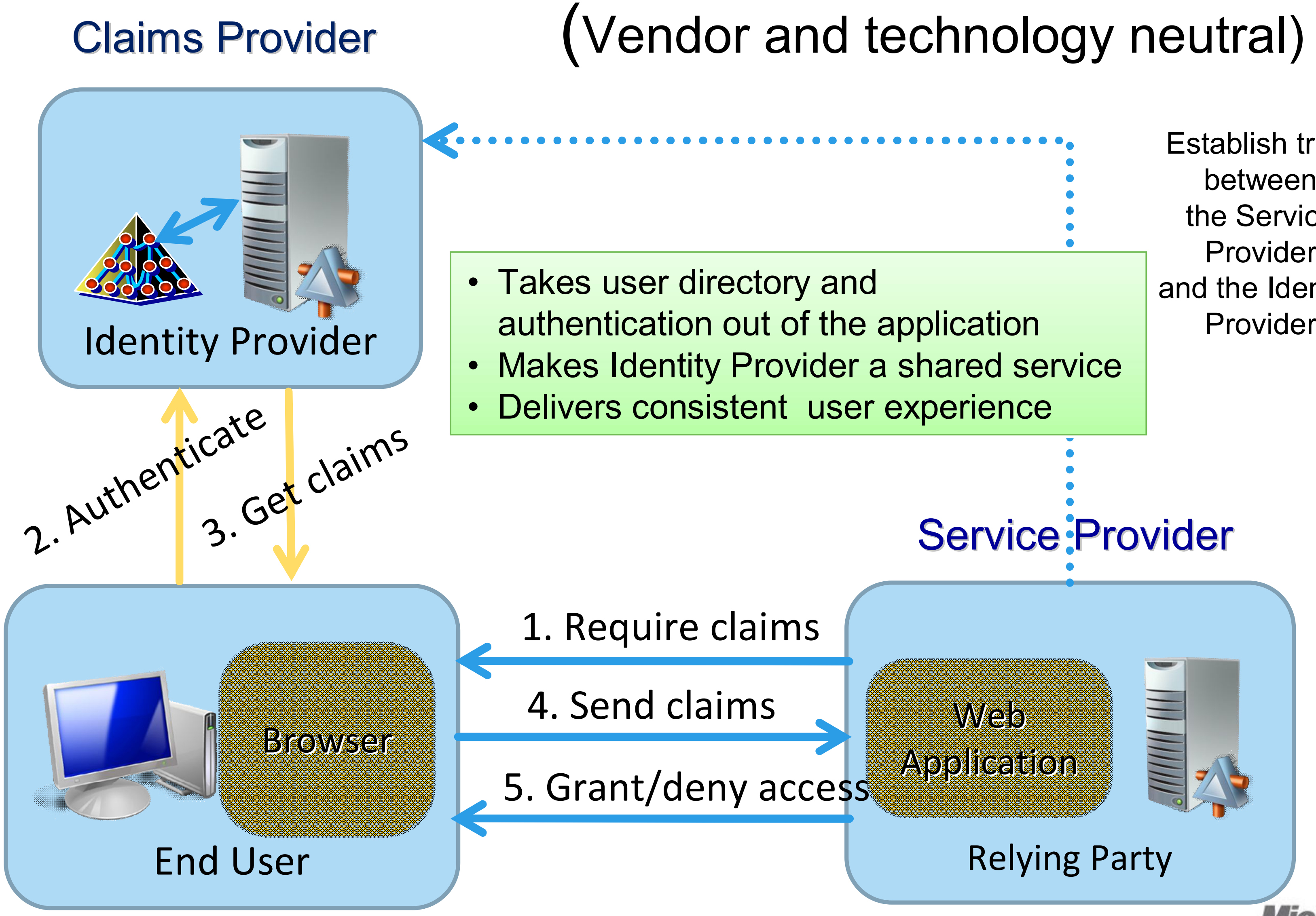
- Identity and Access Management are built into each web service
- User experience is application specific
- PII disclosure follows data in local directory



Microsoft

Identity Metasystem Concept

(Vendor and technology neutral)

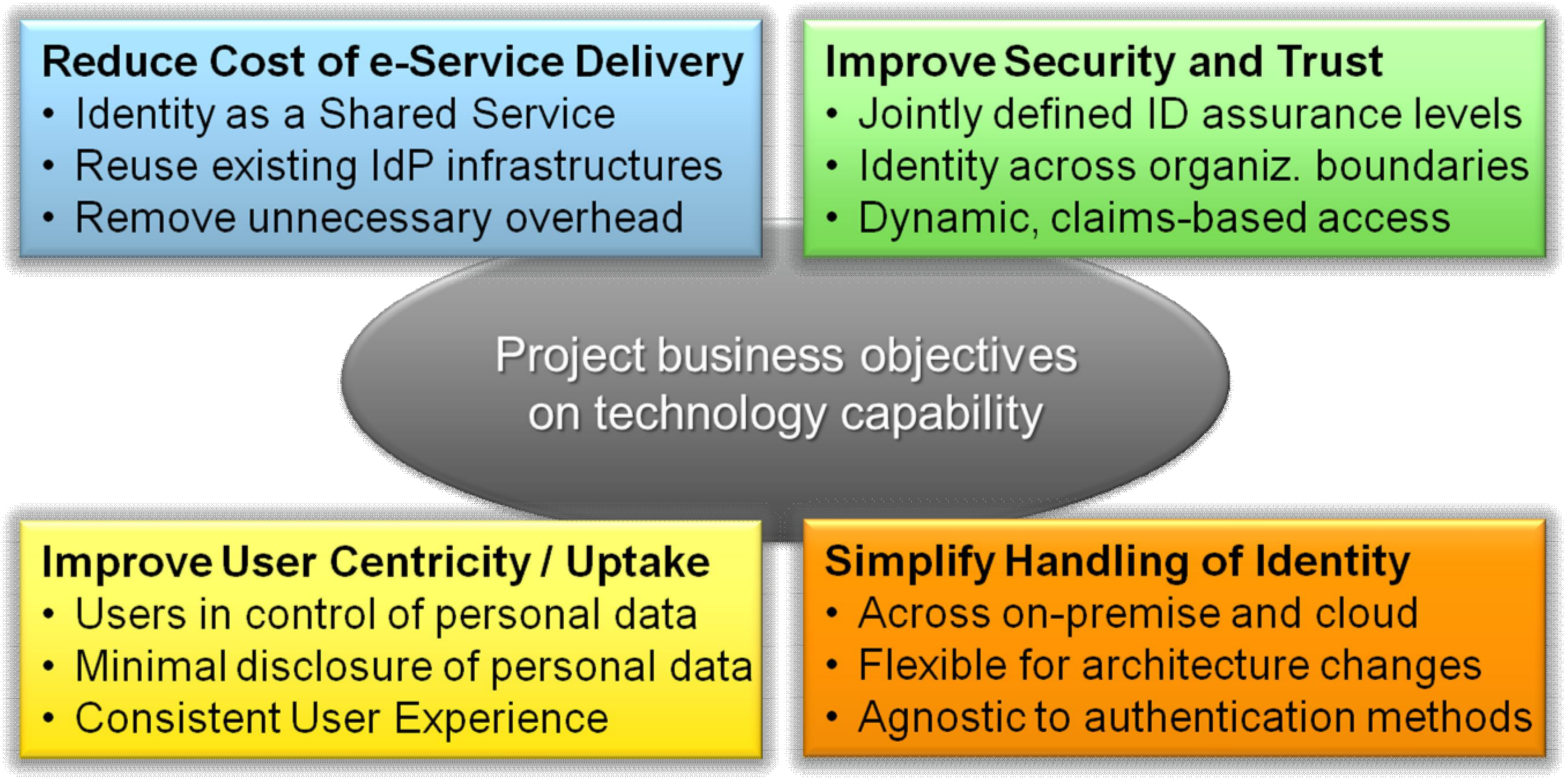


- Takes user directory and authentication out of the application
- Makes Identity Provider a shared service
- Delivers consistent user experience

Agenda

1. Trends in Identity Management
2. IdM Solution Area
3. Features & Benefits
4. Case studies

Requirements of Identity in eGovernment Services



Reduce Cost of e-Service Delivery

- Identity as a Shared Service
- Reuse existing IdP infrastructures
- Remove unnecessary overhead

Improve Security and Trust

- Jointly defined ID assurance levels
- Identity across organiz. boundaries
- Dynamic, claims-based access

Project business objectives on technology capability

Improve User Centricity / Uptake

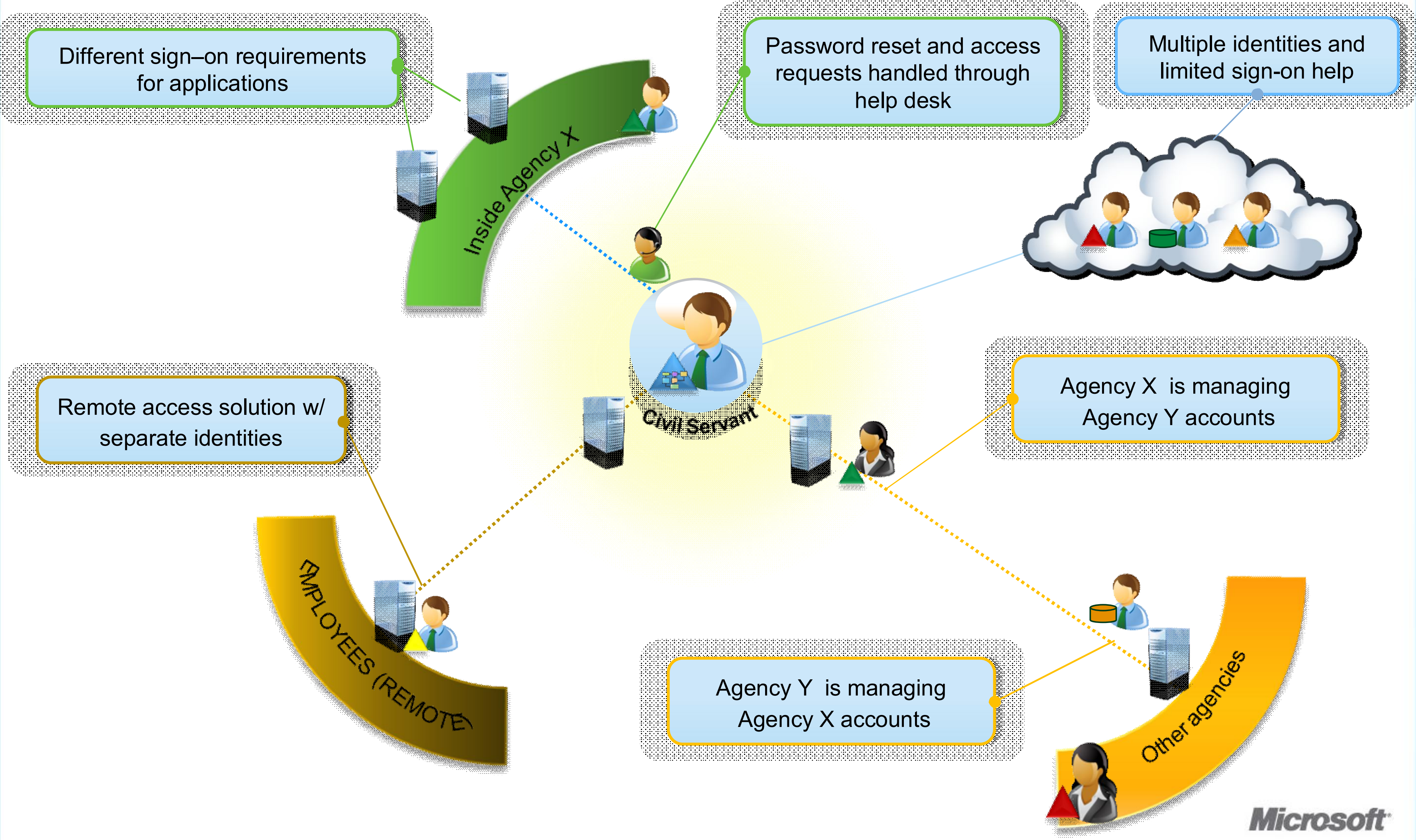
- Users in control of personal data
- Minimal disclosure of personal data
- Consistent User Experience

Simplify Handling of Identity

- Across on-premise and cloud
- Flexible for architecture changes
- Agnostic to authentication methods

Current Situation

Time and labor intensive process



Different sign–on requirements for applications

Password reset and access requests handled through help desk

Multiple identities and limited sign-on help

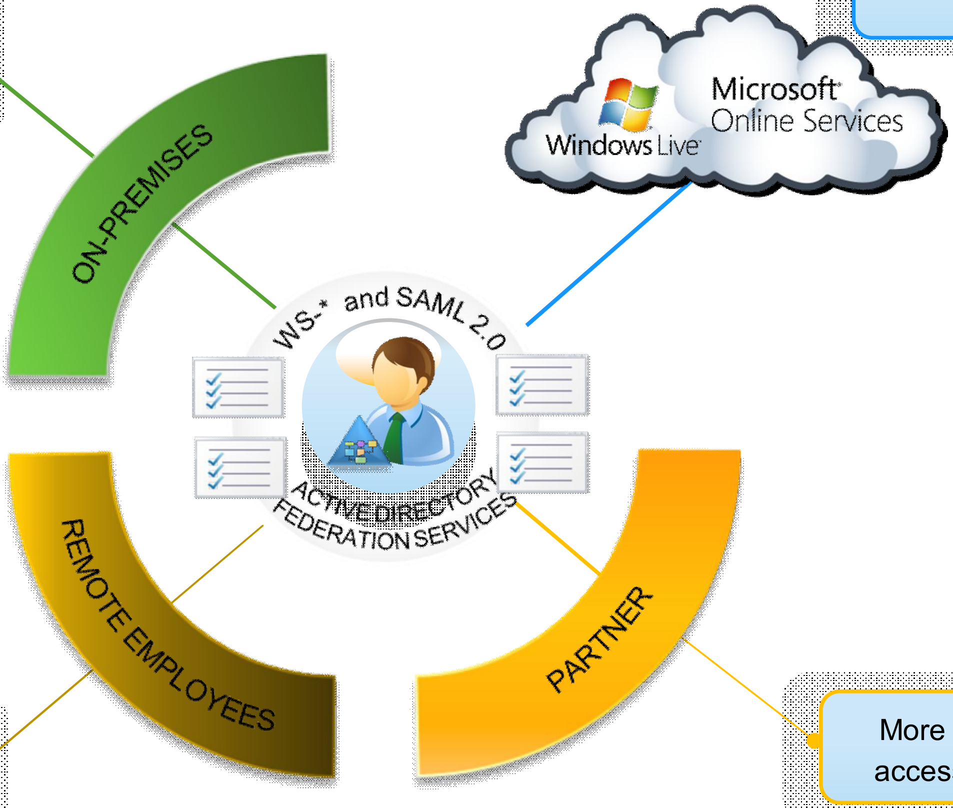
Remote access solution w/ separate identities

Agency X is managing Agency Y accounts

Agency Y is managing Agency X accounts

Identity and Access Management

Simple and easy



Single identity across resources

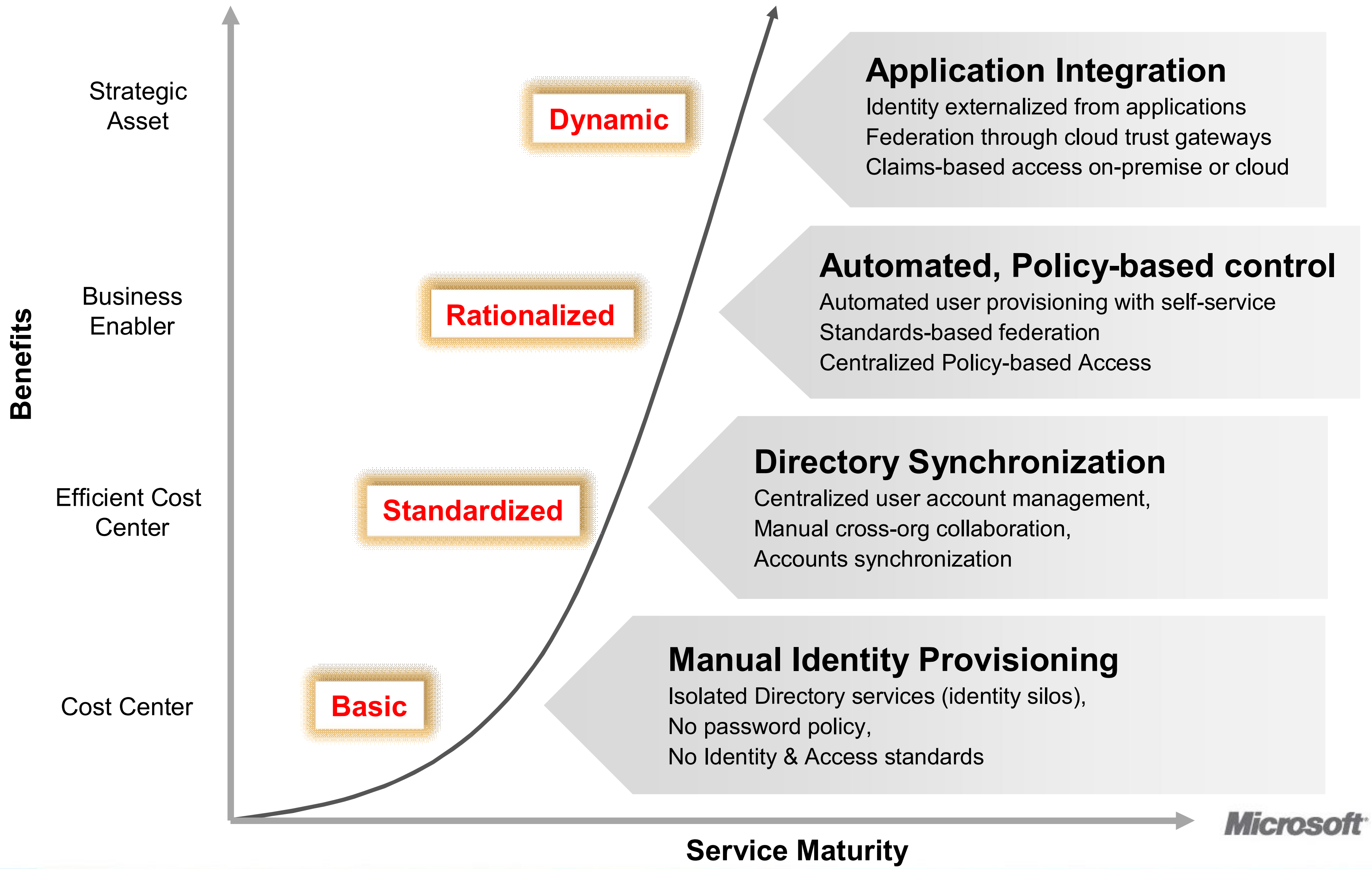
Agency X IDs are used in the cloud

Always-on access built into platform

More secure, simplified access across agencies

Identity Maturity: Technology Capabilities

Microsoft Identity&Access BG view based on Gartner maturity model



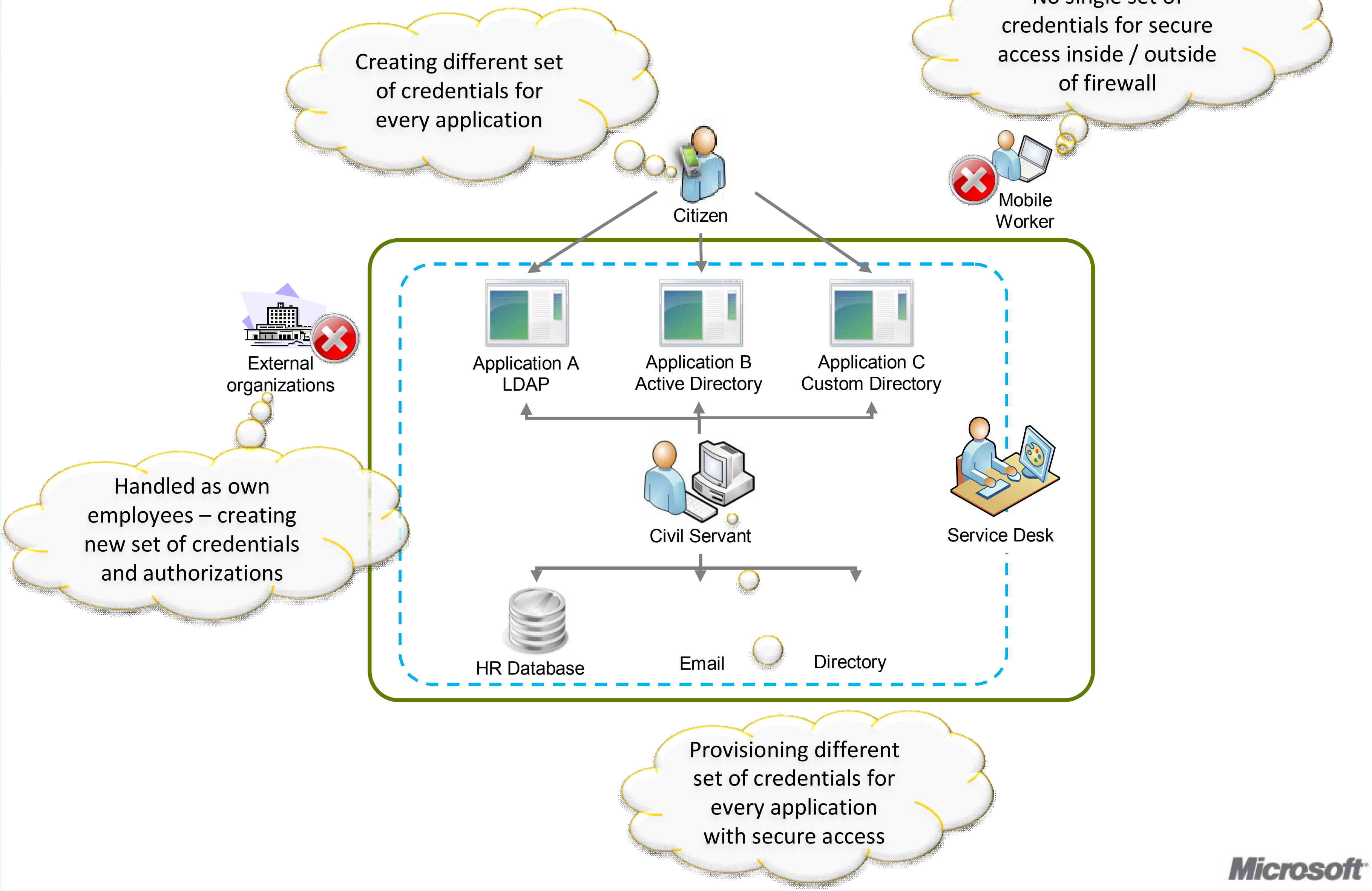
Application Integration
Identity externalized from applications
Federation through cloud trust gateways
Claims-based access on-premise or cloud

Automated, Policy-based control
Automated user provisioning with self-service
Standards-based federation
Centralized Policy-based Access

Directory Synchronization
Centralized user account management,
Manual cross-org collaboration,
Accounts synchronization

Manual Identity Provisioning
Isolated Directory services (identity silos),
No password policy,
No Identity & Access standards

Basic: The Traditional Identity Silo Approach



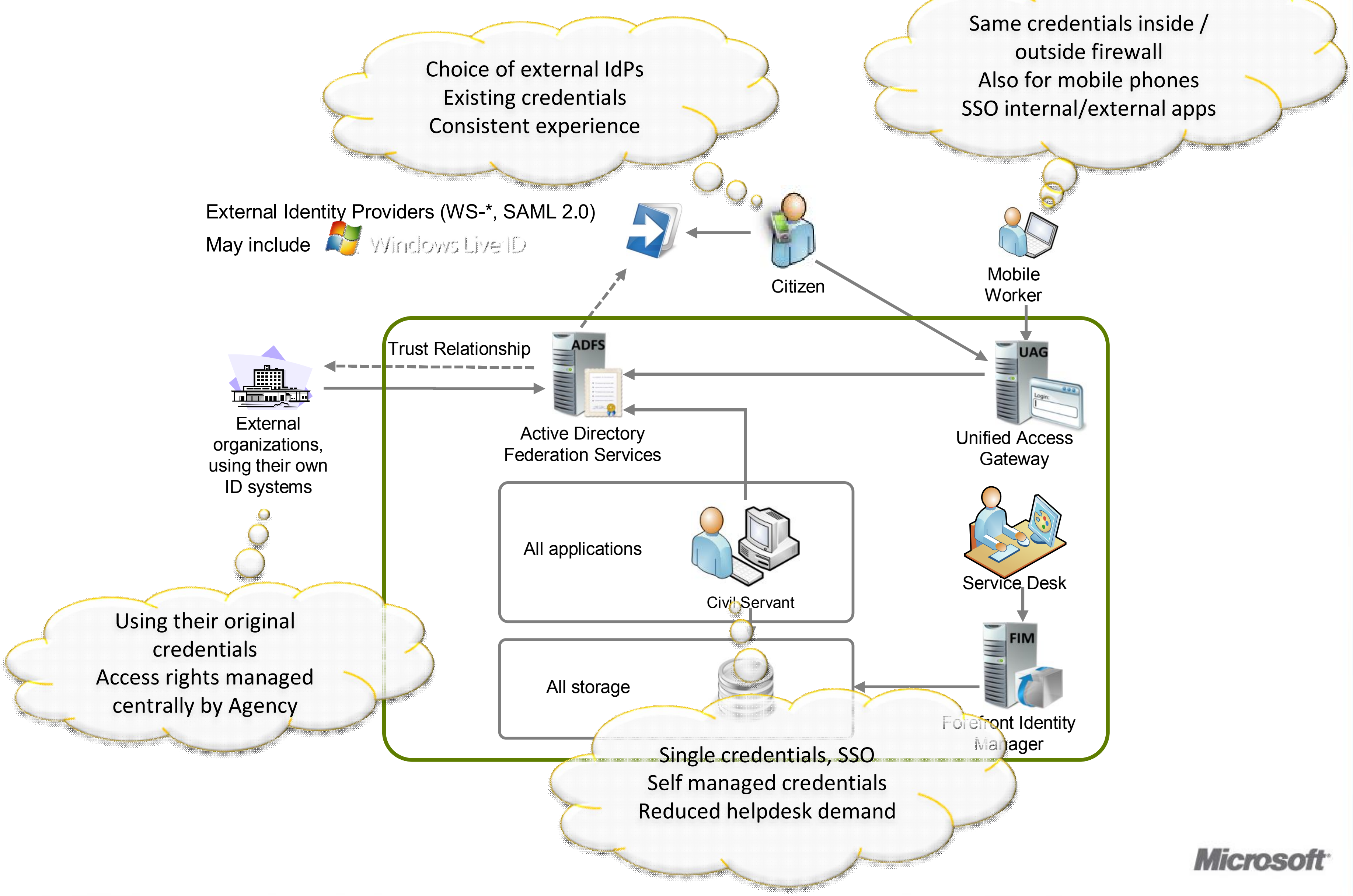
Creating different set of credentials for every application

No single set of credentials for secure access inside / outside of firewall

Handled as own employees – creating new set of credentials and authorizations

Provisioning different set of credentials for every application with secure access

Rationalized: Streamlined IdM and Federated Access



Choice of external IdPs
Existing credentials
Consistent experience

Same credentials inside / outside firewall
Also for mobile phones
SSO internal/external apps

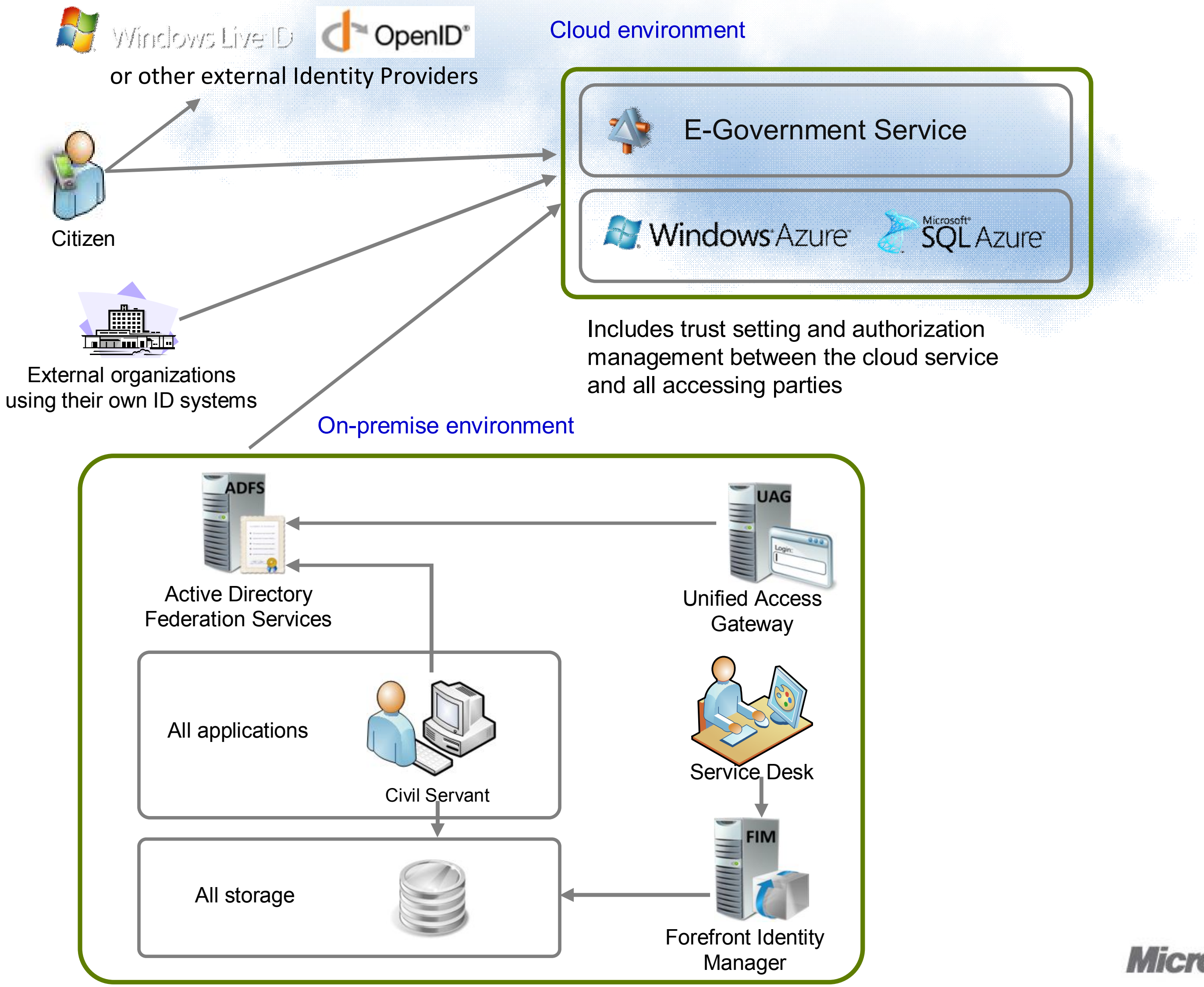
External Identity Providers (WS-*, SAML 2.0)
May include Windows Live ID

Using their original credentials
Access rights managed centrally by Agency

Single credentials, SSO
Self managed credentials
Reduced helpdesk demand

Microsoft

Dynamic: Opening Up to Cloud Services, External IdP‘s



Windows Live ID
OpenID
or other external Identity Providers
Cloud environment
E-Government Service
Windows Azure
Microsoft SQL Azure
Citizen
External organizations using their own ID systems
Includes trust setting and authorization management between the cloud service and all accessing parties
On-premise environment
ADFS
Active Directory Federation Services
UAG
Unified Access Gateway
All applications
Civil Servant
Service Desk
FIM
All storage
Forefront Identity Manager

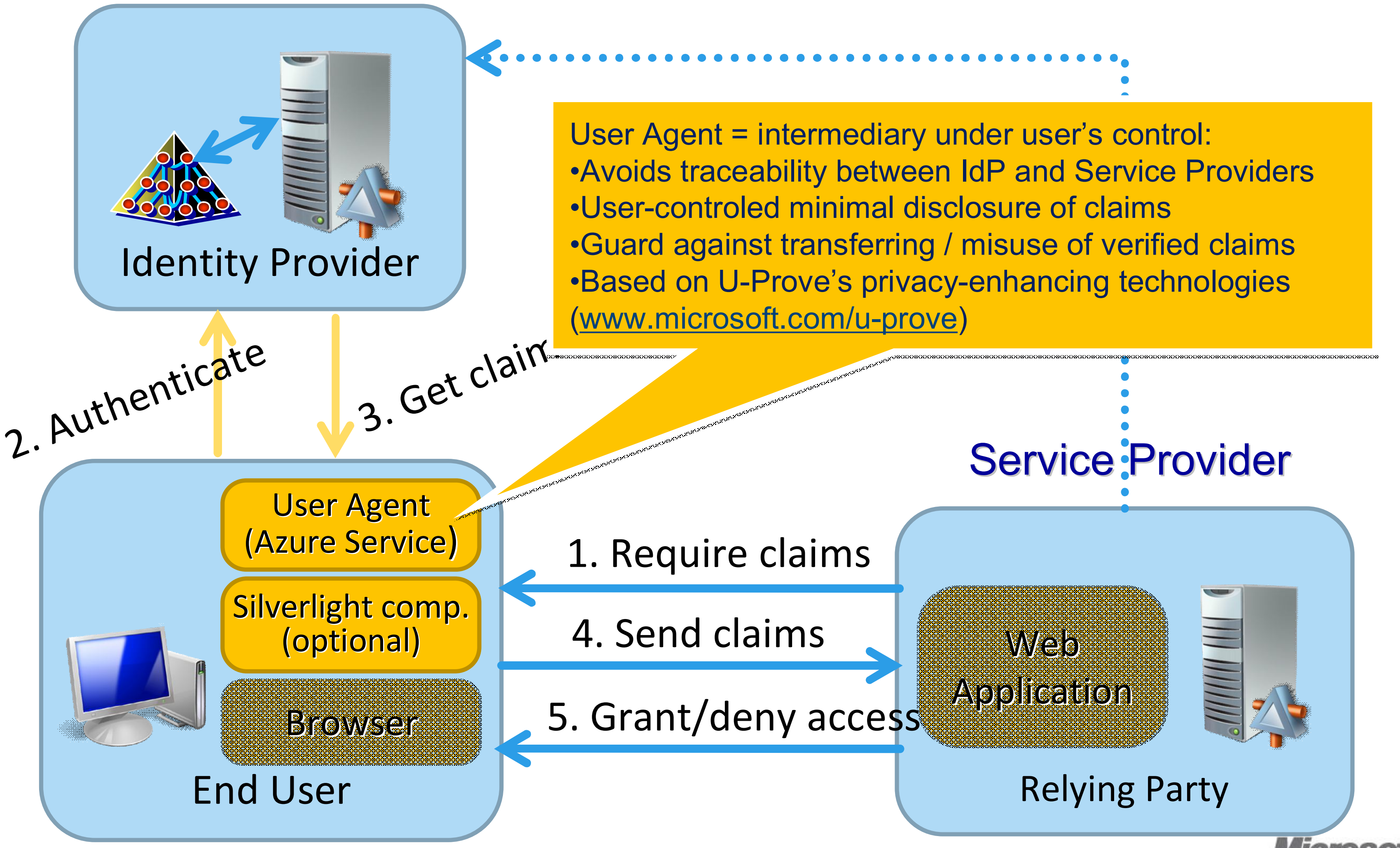
Microsoft

Agenda

1. Trends in Identity Management
2. IdM Solution Area Requirements
3. IdM Solution Area
4. Features & Benefits
5. Case studies

Identity Metasystem with User Agent

(Vendor and technology neutral)



User Agent = intermediary under user's control:
- Avoids traceability between IdP and Service Providers
- User-controled minimal disclosure of claims
- Guard against transferring / misuse of verified claims
- Based on U-Prove's privacy-enhancing technologies (www.microsoft.com/u-prove)

Microsoft

How Identity Metasystem Contributes

Policy objectives	Identity Federation	Claims-based Access:
Reducing Cost	Identity = shared service	Less cost for developers
User Centricity	Consistent user experience	Minimal disclosure of personal information
Security & Trust	Common Identity Assurance levels	Dynamic effect of identity attributes (claims)
Simplicity & Flexibility	ID externalized from applications – agnostic to IdPs / authN	Same for on-premise and cloud

Agenda

1. Trends in Identity Management
2. IdM Solution Area Requirements
3. IdM Solution Area
4. Features & Benefits
5. Case studies

UK Government Gateway

www.gateway.gov.uk

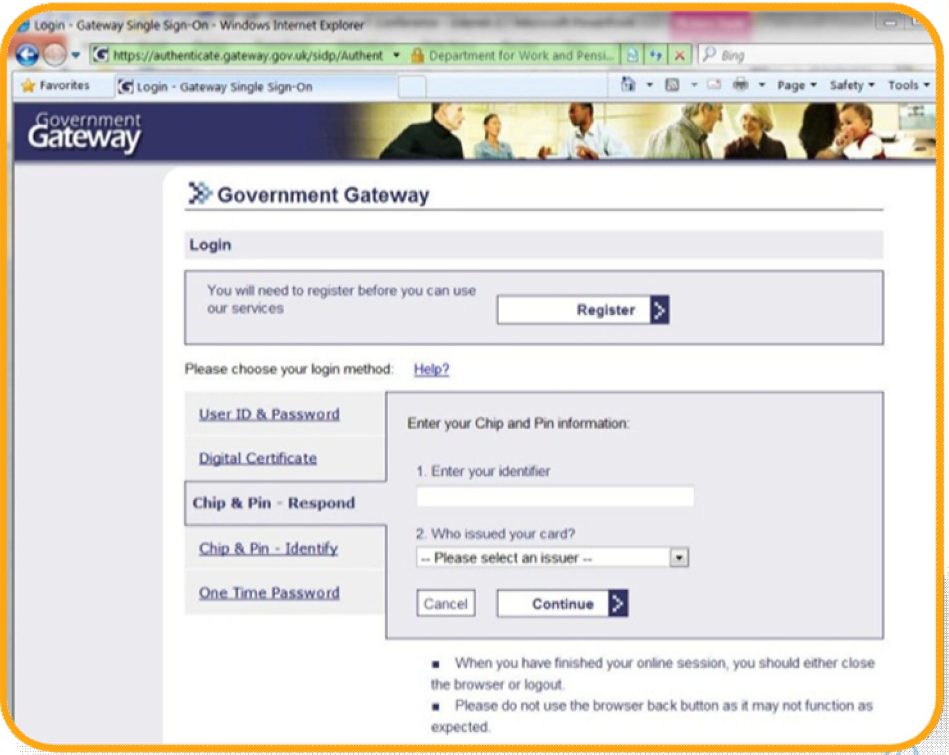
- The main eGov transactional hub
  for 18+ millions UK citizens and businesses
- Probably the first widely used federated identity provider to other departments‘ e-Services
- 2006 Custom-built WS-* and SAML federation services

Uses **Identity federation** to allow other departments to authenticate, offering protocols

- WS-Federation
- Liberty Alliance
- SAML 1.1 and SAML 2.0

Supports **multiple levels of identity assurance** via

- Pin activated password
- X.509 Certificates
- Chip&Pin cards
- One-Time Password (OTP)


Login - Gateway Single Sign-On - Windows Internet Explorer
https://authenticate.gateway.gov.uk/sidp/Authent
Department for Work and Pensi...
Bing
Favorites
Login - Gateway Single Sign-On
Page
Safety
Tools
Government Gateway

Government Gateway

Login

You will need to register before you can use our services

Register

Please choose your login method: Help?

- User ID & Password
- Digital Certificate
- Chip & Pin - Respond
- Chip & Pin - Identify
- One Time Password

Enter your Chip and Pin information:

1. Enter your identifier

2. Who issued your card?
   -- Please select an issuer --

Cancel | Continue

- When you have finished your online session, you should either close the browser or logout.
- Please do not use the browser back button as it may not function as expected.

UK Ministry of Defence Federating with UK Gateway

Customer Profile
Ministry of Defence, UK - Central Government;
Seats: 320,000 personnel, approx 10,000 of them are remote users

Customer Challenge

- 10,000 of their „orphaned users“ without online access to Line of Business applic‘s.
- E.g. field users‘ expense claims took weeks to send and process on paper forms
- Identified 20 routine HR applications as a priority for secure remote access to save operating costs.

Solution

- Used UK Govt Gateway for Chip&PIN authentication, MS Intelligent Apps Gway (IAG) for secure remote access, Internet Security and Acceleration Server (ISA), Identity Lifecycle Manager 2007 etc.
- Identity & Access custom solution by Capgemini, EDS, Gemalto, Avaleris, MCS

Customer Results/Benefits

- Remote worker expense claims settled in 24 Hours instead of days or weeks
- Saves taxpayers “Many Millions of Pounds” in 10 yrs
- Secure access via One-Time Passwords (OTP)
- Integrates well with other Oracle based applications
- Consolidates multiple forms of Digital Identity

“We wanted to give all of the remote staff secure access to the MOD systems from any industry or home based browser, from an Internet café, or even an i-Touch phone or personal digital assistant.”

- David Longhurst, an Adviser to the Chief Information Officer at the MOD

http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?casestudyid=4000003478

Microsoft

Vancouver Coastal Health: Federated Access

BRITISH COLUMBIA
The Best Place on Earth

Customer Profile
The Province of British Columbia, Canada, provides public services, such as healthcare, education, and transportation, to the residents of British Columbia. Vancouver Coastal Health is one of the health agencies.

Customer Challenge

- Multiple health agencies and hospitals needed secure access to patient health records, stored in the provincial systems.
- Traditionally, that would involve creating and maintaining new user accounts with access rights for authorized personnel.

Solution

- The Province decided to implement a shared service “eHealth Viewer“, based on Windows Identity Foundation infrastructure.
- Authorization managed by claims-based access and federation with employees home Active Directory Federation Services 2.0.

Customer Results/Benefits

- Solved the problem taking advantage of existing AD credentials
- Only one user account management process
- Dynamic access rights – immediate update effect
- System open for broader federation with other health organizations

> *“Identity federation is a key enabler in delivering public services. By using Active Directory Federation Services 2.0, we can start right away by using existing IT infrastructure.”*
>
> ***- Patricia Wiebe, Senior Identity Architect, Province of British Columbia***

http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?casestudyid=4000007158

Microsoft

Vancouver Coastal Health: What was achieved

Health record keepers rely on other health agencies‘ authentication

- Dropped idea of building and maintaining an aggregated (and redundant) access list of all health personnel with access rights
- Agreed on a trusted model, where record keepers trust SAML authentication of doctors‘ hospitals or agencies

Flexible model to grow in the future

- Federation enables scaling – number of participating agencies is principally unlimited

Federated Identity and Access = Shared Service

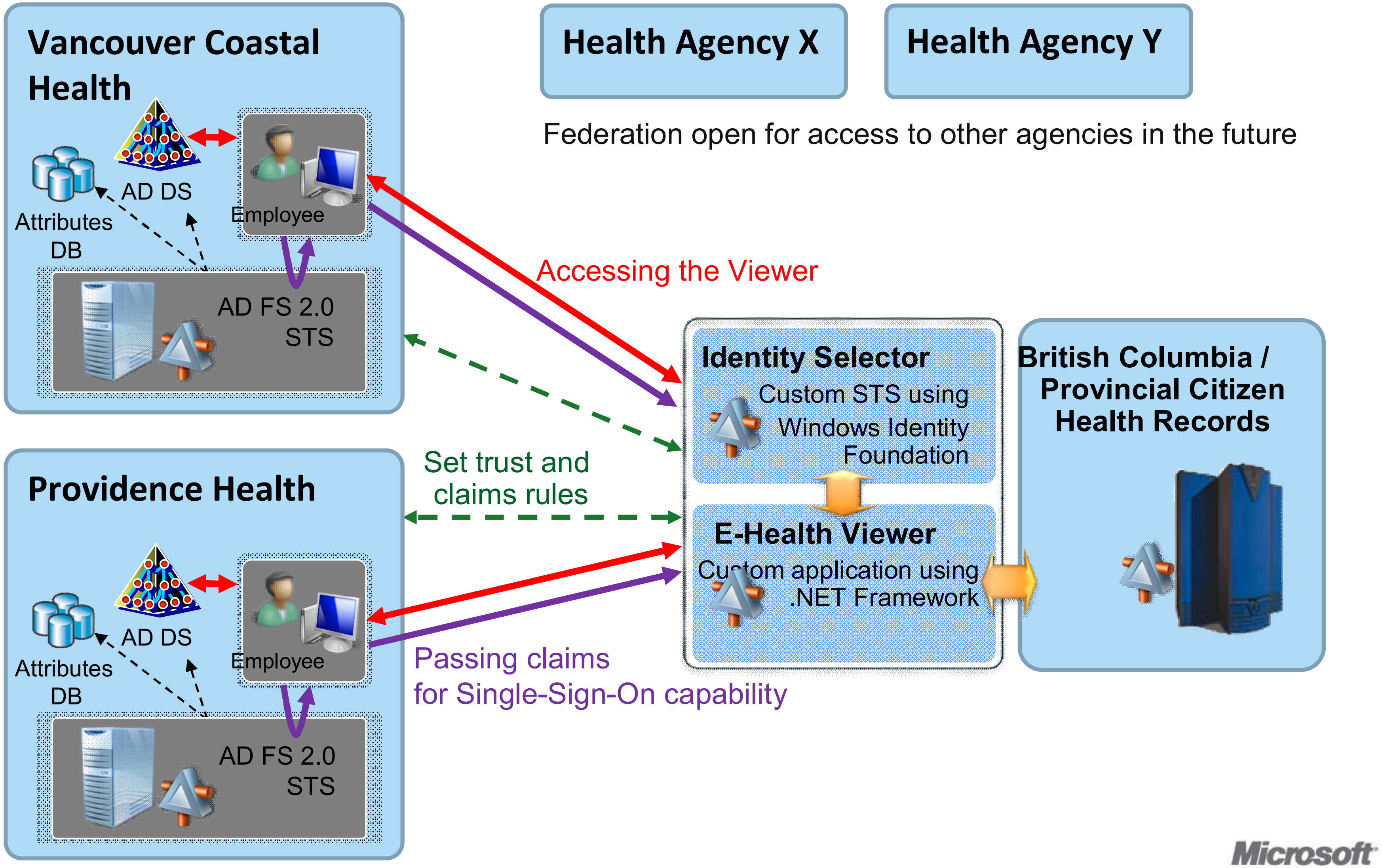
- The same schema can be used for other e-Services in the future, eliminating further eID cost and complexity

Vancouver Coastal Health – Multi-Agency Service Delivery

Federated Identity & Claims-based access to Health information

http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=4000007158

BRITISH COLUMBIA
The Best Place on Earth



Vancouver Coastal Health

AD DS

Attributes DB

Employee

AD FS 2.0 STS

Health Agency X

Health Agency Y

Federation open for access to other agencies in the future

Accessing the Viewer

Identity Selector

Custom STS using Windows Identity Foundation

E-Health Viewer

Custom application using .NET Framework

British Columbia / Provincial Citizen Health Records

Set trust and claims rules

Providence Health

AD DS

Attributes DB

Employee

AD FS 2.0 STS

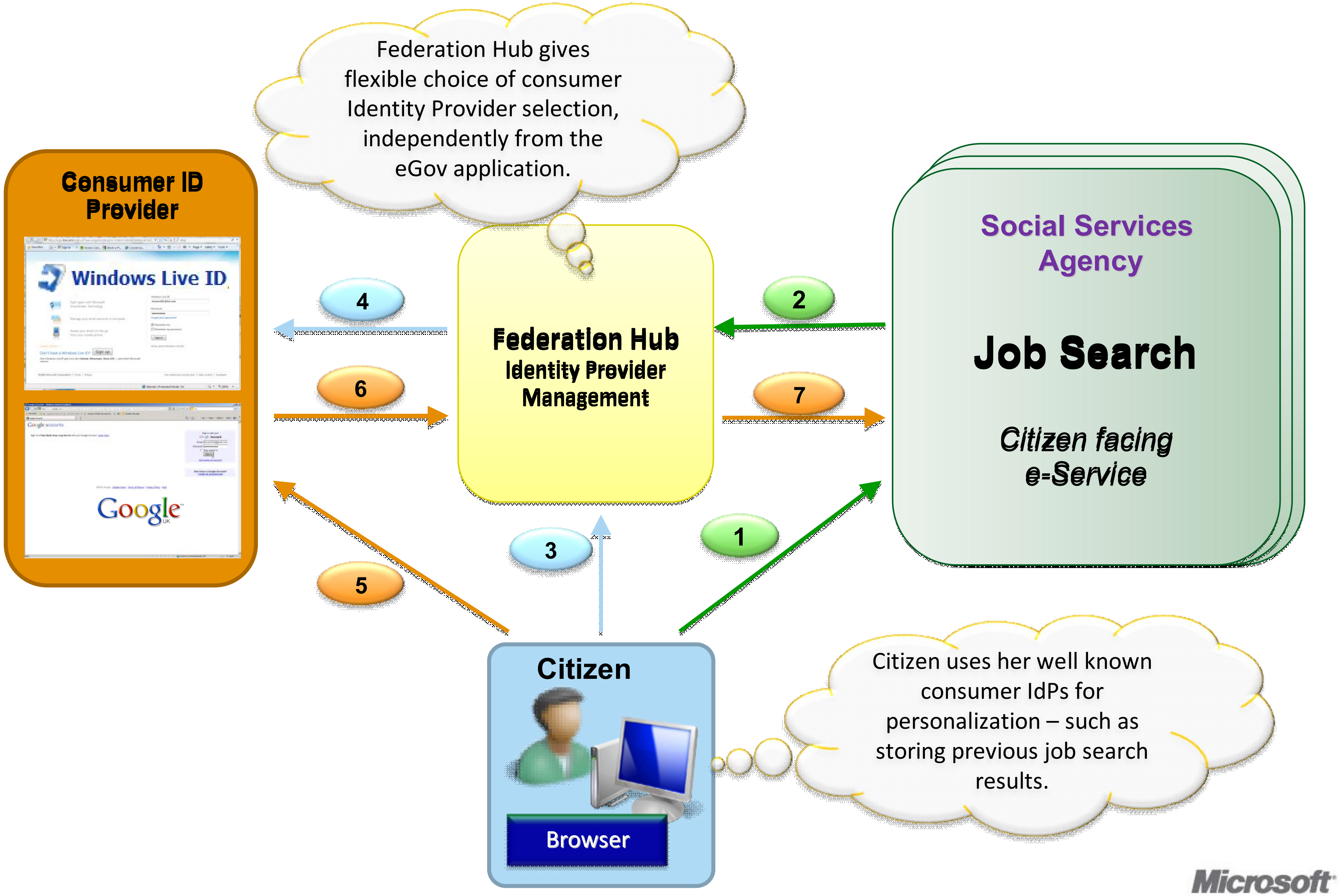
Passing claims for Single-Sign-On capability

Microsoft

UK – Reusable Solution for Local Councils

- Under deployment 2010/2011 in several councils
- Objective: “Citizen Channel shift“
  - Move high value transactions online in order to reduce costs
- Tiered identity assurance service with 3 levels:
  - Bronze – no ID verification = personalization only
  - Silver – Medium verification
  - Eg. Social benefit listing, Parking permit
  - Gold – Passport, Drivers license, Credit card verification
  - Eg. Health records, Social benefits application and approval
- Choice of 3rd party Identity Provider services
- Choice of 2-factor authentication
  - One-Time Passwords to cell phone, RSA token etc.
- Open, standards-based, industry-proven solution
  - Based on COTS products
  - Common identity mgmt platform for all e-Services

Cost Effective Personalization Through Consumer IdPs



Federation Hub gives flexible choice of consumer Identity Provider selection, independently from the eGov application.

Consumer ID Provider

Federation Hub
Identity Provider Management

Social Services Agency

Job Search

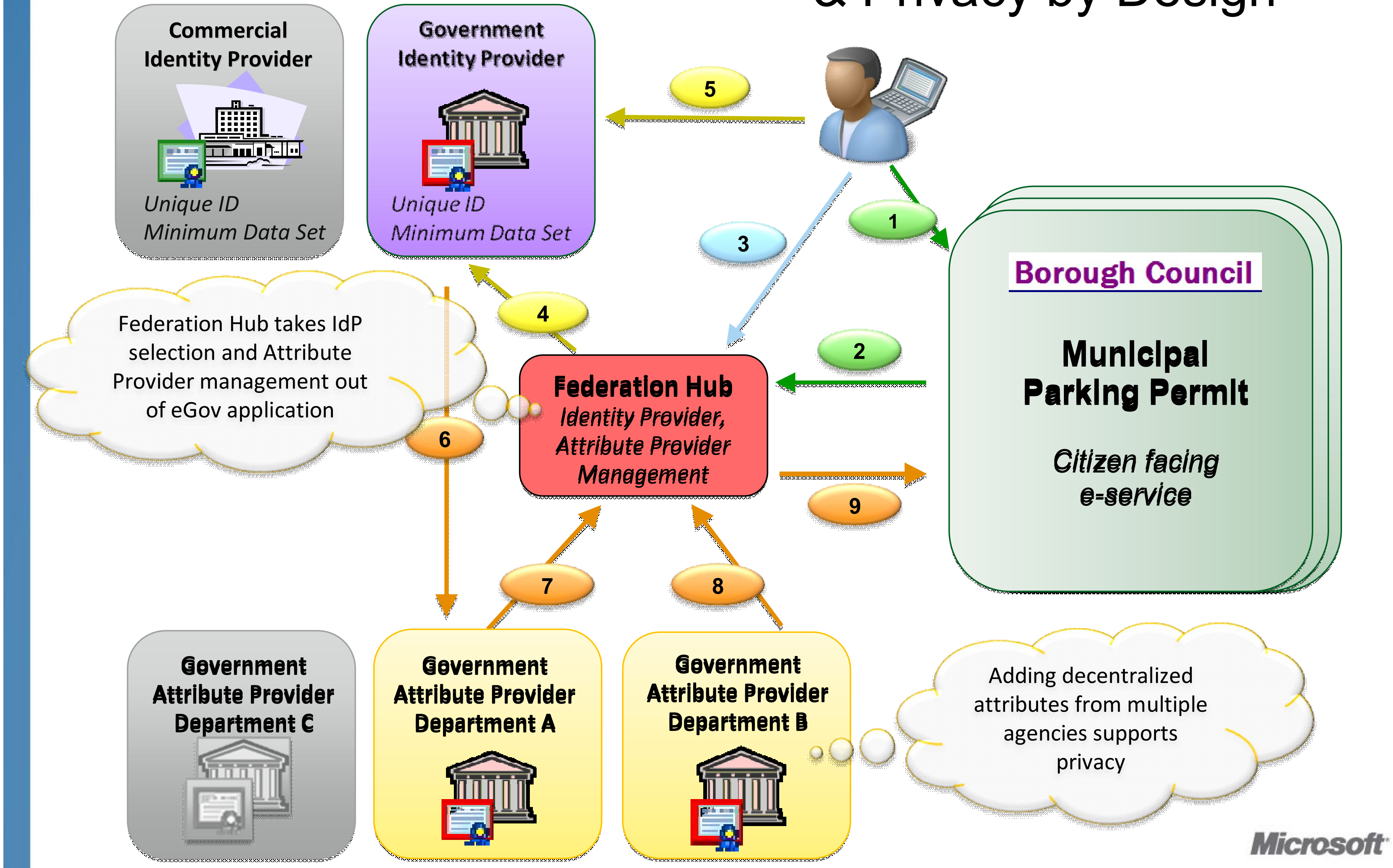
Citizen facing e-Service

Citizen

Browser

Citizen uses her well known consumer IdPs for personalization – such as storing previous job search results.

UK Local Government – Advanced e-Services & Privacy by Design



Commercial Identity Provider
Unique ID
Minimum Data Set
Government Identity Provider
Unique ID
Minimum Data Set
5
3
1
Borough Council
Municipal Parking Permit
Citizen facing e-service
4
2
Federation Hub
Identity Provider, Attribute Provider Management
6
9
7
8
Government Attribute Provider Department C
Government Attribute Provider Department A
Government Attribute Provider Department B

Federation Hub takes IdP selection and Attribute Provider management out of eGov application

Adding decentralized attributes from multiple agencies supports privacy

Summary: Identity Management

Microsoft, together with solutions partners, delivers Identity Management solutions that:

- Enable citizens, businesses, and employees to securely access information they need to be more productive
- Integrate with the existing infrastructure and accelerate application development
- Are able to dynamically adapt to changing needs, threats, and legal requirements

Identity Management for SW Architects (Customer ready material)

- Microsoft IAM Platform entry point on MSDN
  Blogs, videos, webcasts, whitepapers: http://msdn.microsoft.com/en-us/security/aa570351.aspx
  Geneva Team Blog on MSDN – good summary of external content - link

- Windows Azure AppFabric – Access Control Service
  All AppFabric overview: http://www.microsoft.com/windowsazure/appfabric/
  Access Control Service video on MSDN Channel9
  Access Control Service sample code: http://acs.codeplex.com/

- Identity Developer Training Kit – downloadable pack (March 2010 update):
  Contains a set of hands-on labs, documents and references that will help you to learn how to take advantage of Microsoft's latest identity and access control developer's products and services.
  http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=c3e315fa-94e2-4028-99cb-904369f177c0

- Identity Developer Step-By-Step Claims Based Access
  Explains how claims-based access works in common scenarios:
  http://blogs.msdn.com/vbertocci/archive/2009/05/15/more-details-about-the-identity-developer-training-kit.aspx

Microsoft®

Your potential. Our passion.™

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.