CONFLICTING VISIONS OF CLOUD IDENTITY

Kim Cameron
Architect of Identity, Azure Active Directory, Microsoft

Session ID: IAM-302
Session Classification: Intermediate

Economic Dictates Are Shaking Us

- Current reality is economic contraction
- Enterprises and governments are under increasing pressure to do more with less.
- Long-term implications
- Organizations must become leaner, better focused and more fit-to-purpose.
- Applies to ALL systems of production and distribution, including IT
- We need “breakthrough” changes

THE FIT-TO-PURPOSE ENTITIES THAT SURVIVE NEED “BREAKTHROUGH” CHANGE

The Cloud Brings Breakthrough Change

- Economic benefits come from combined cloud innovations
  - New ways of delivering and operating infrastructure
  - New business processes.
- Infrastructure for *refactoring and redistributing processes to be most efficiently performed.*
- Survivors benefit by specializing in what they do best and most efficiently
- *Multi-sourcing*

SPECIALIZATION BASED ON EXPERTISE AND COST

The Two Tendencies Will Join Up

- The need to become leaner and more fit-to-purpose will drive continuous change. Organizations will:

Substitute inexpensive cloud services when they provide the same functionality as in-house systems

Construct their own systems as cloud services using other ecosystem cloud services as building blocks.

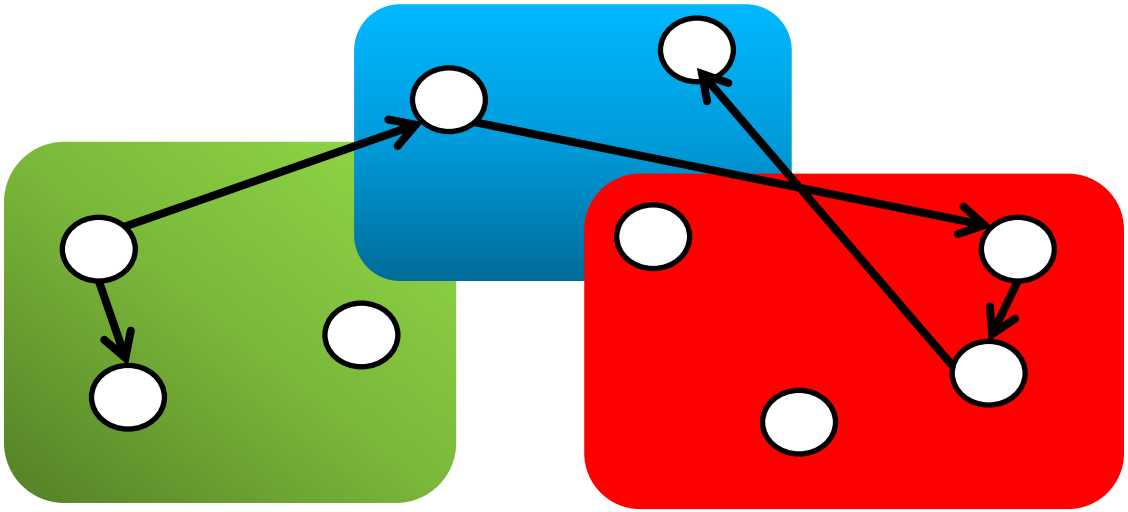
Cross-Cloud Interactions

- Specialized services will expect to hook into other specialized services running anywhere else in the cloud using simple REST APIs.
- Cloud platforms that don't offer this capability will die from "synergy deficiency".
- Enterprise and government data sent to cloud service APIs will be private data
- *The different systems run by different administrations must able to reuse knowledge of identity and policy to adequately protect the data they handle*

PRIVATE DATA IN THE API ECONOMY

The Cloud Motor Runs on Identity

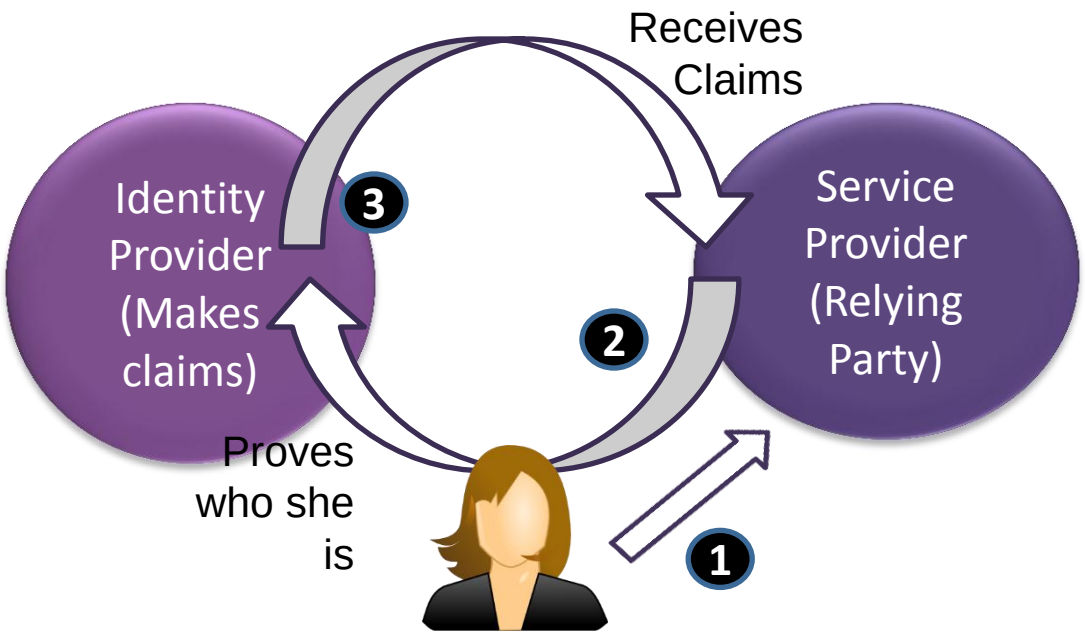
Organizations must be able to reliably identify, authenticate and authorize **across this multi-platform graph of services** before reuse of specialized services becomes practicable and economical and the motor of cloud economics can turn reliably



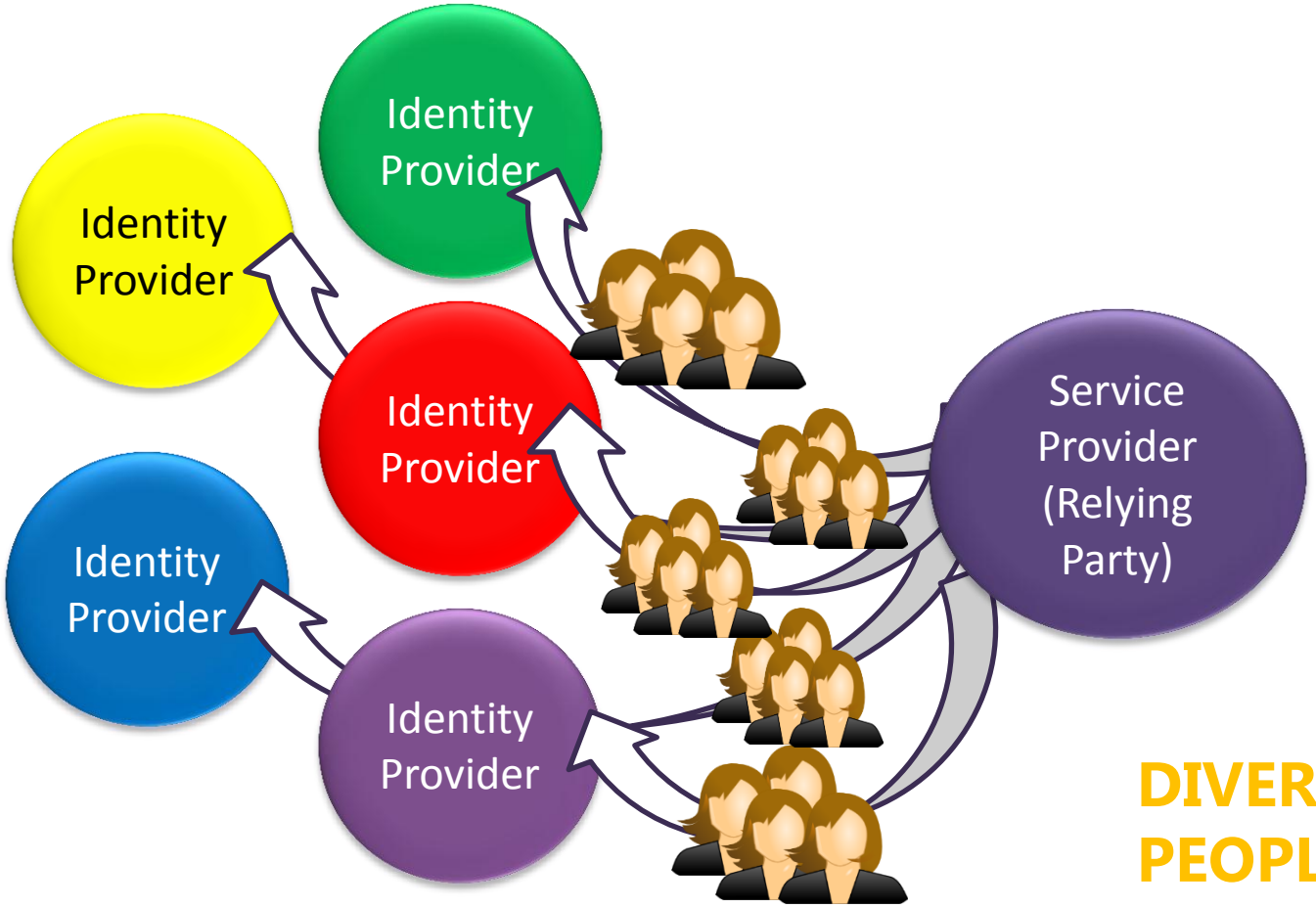
Existing Paradigms Can't Handle Cloud Identity, Security, and Privacy

Domain Based IDM Model is a Non-Starter

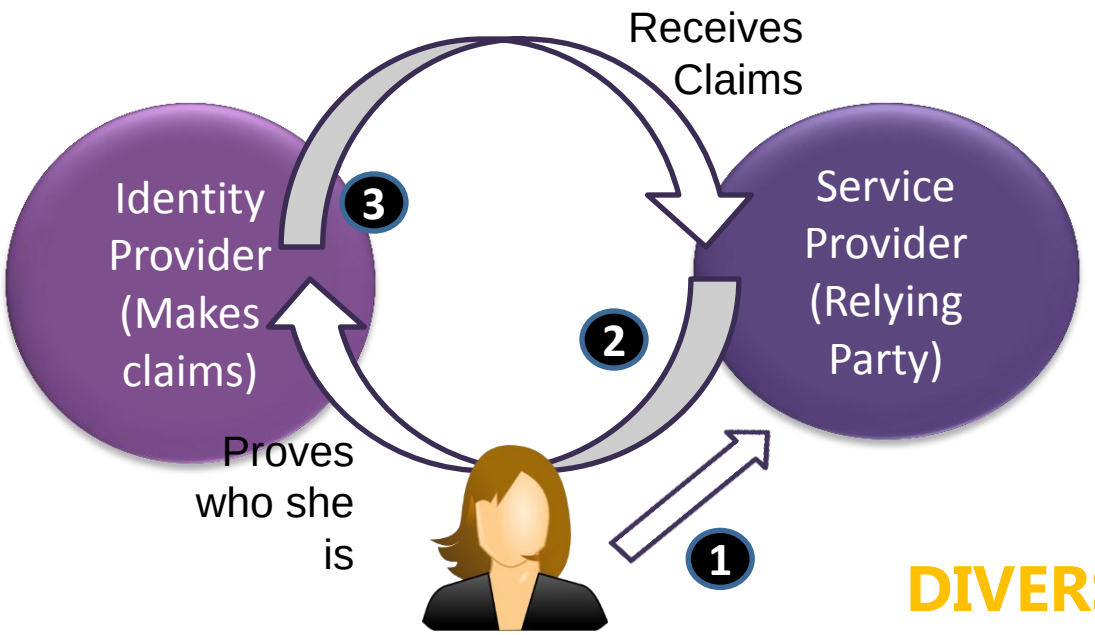
The First-Generation IDM Model Won't Do It Either



The First-Generation IDM Model Won't Do It Either



The First-Generation IdM Model Won't Do It Either



DIVERSE CLAIMS

Necessary Simplification: Identity Management as a Service

Why Identity Management As A Service (IdMaaS)?

- The functional specialization driving cloud economics requires a new model of Identity Management providing cloud era capabilities.
- There is a condition attached: it can't make the cloud so expensive that it loses its reason for being!
- How do you get more capability for less money?
- Use the efficiencies of the cloud to enable efficiencies in identity.

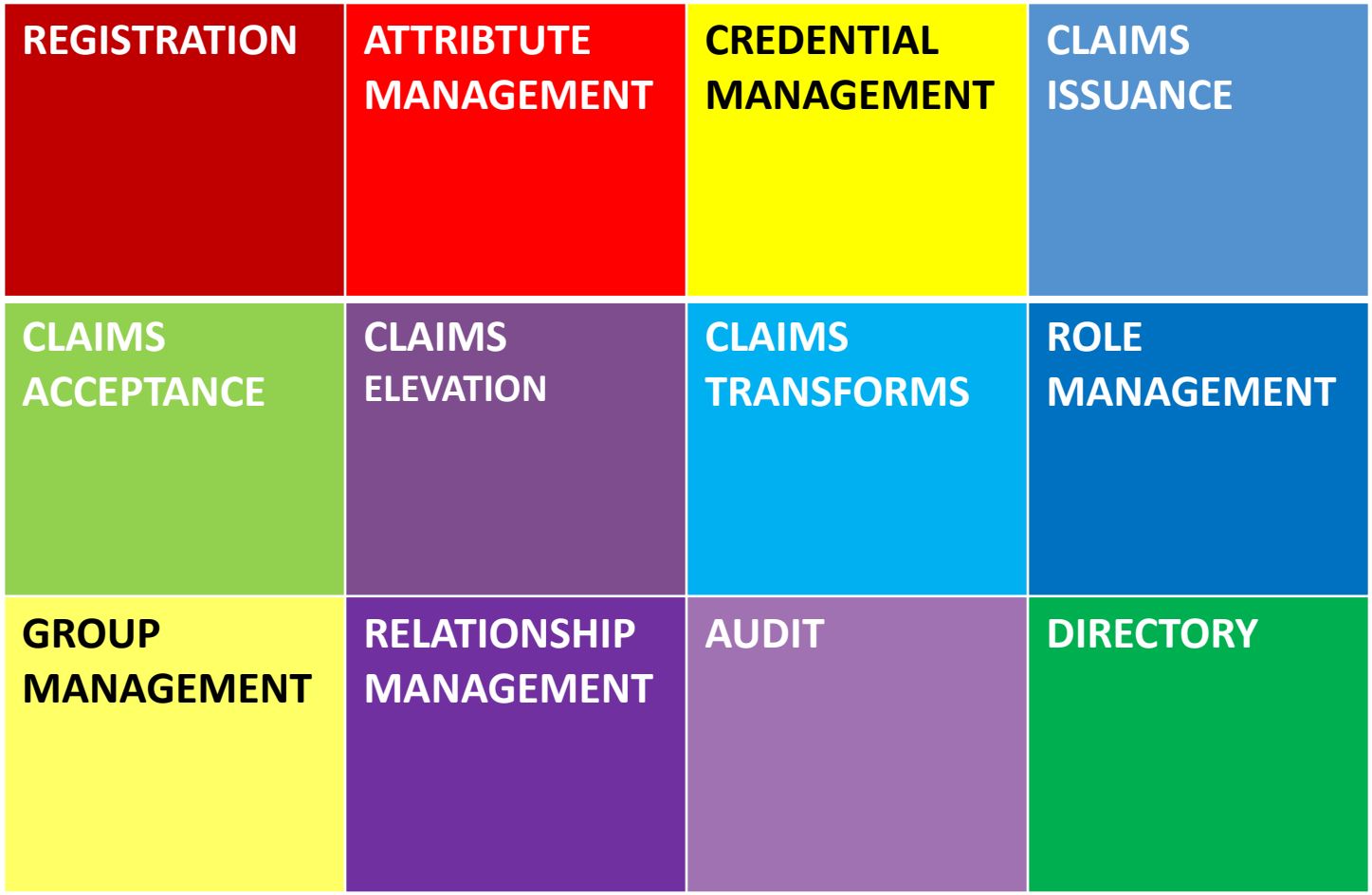
INEVITABILITY OF IDENTITY MANAGEMENT AS A SERVICE

What Is Identity Management As A Service (IdMaaS)?

- Provides cloud services to manage identity relationships for an organization's employees, partners and customers.
- A simple, cost-effective, low-risk, complete solution for connecting members of the enterprise social graph to each other and to their applications and information.

DEFINITION OF IDENTITY MANAGEMENT AS A SERVICE

Composable Capabilities Of IdMaaS



Simplifies, Professionalizes And Lowers Cost

- Deploying cloud applications
- Designing new cloud-based systems
- Federating with small and large partners
  - Credentialing
  - Directory
  - Quality of Service
  - Level of Assurance and Professionalization
- Managing of relationships with individual customers and citizens
- Evolving a Hybrid IT environment

INEVITABILITY OF IDENTITY MANAGEMENT AS A SERVICE

Issues When Identity Is Managed From The Cloud

- Many visions possible for cloud operator
  - Can the cloud operator mine enterprise information?
  - How much visibility does the operator have on enterprise relationships?
  - Can the directory be used by other cloud operators?
  - Will enterprises be treated with the same "contempt" as some say applies to consumers?
- Will governments be able to run rampant "à la Patriot Act"?

WHO'S INFORMATION IS IT?

WHAT ARE THE RULES?

Issues When Identity Is Managed From The Cloud

- Should an IdMaaS Operator assert attributes for which it is not the authoritative source?
  - What are Liability and security implications?
- What about the **honeypot** resulting from huge concentrations of corporate identity?
  - Does it make sense to create this kind of target?
- Can cloud identity reduce the need for backwards compatibility with approaches subject to existing vulnerabilities?

WHO'S INFORMATION IS IT?

WHAT ARE THE RULES?

Example: Directory As IdMaaS

- Organizations selectively expose their directory to other applications, services, customers and partners
- Does the enterprise decide who can see what and in which applications?
- Is the cloud directory a service run on behalf of the enterprise (i.e. IDMAAS) or the operator's cloud directory?
- Are publication of one's own directory and subscription to other directories provided as part of the identity service? Who controls it?
- Does the operator employ Trust Frameworks to simplify legal relationships involved in information sharing?

IT BELONGS 100% TO THE ENTERPRISE - NOT THE CLOUD OPERATOR.

Example: Service Provider Combining IdMaaS Capabilities

Trust Framework

Facebook
Twitter
Google+
LiveID
Skype
Paypal
Equifax
InCommon

Identity Provider Role

IDMAAS

- Operate
- Integrate
- Configure
- Troubleshoot
- Map Semantics
- Monetize
- Audit and Report

Citi
OTP
Office365
Post Office
DMV
Ministry of Health
Belgian EiD
Law Society

Claims Augmenter Role

The Privacy and Security Imperative

Bar For Security And Privacy

- **Claims enrichment:** Users present applications with verified claims from multiple Claims Providers – in a single request/response or incrementally as required in a session
- Two key uses cases:

Audited

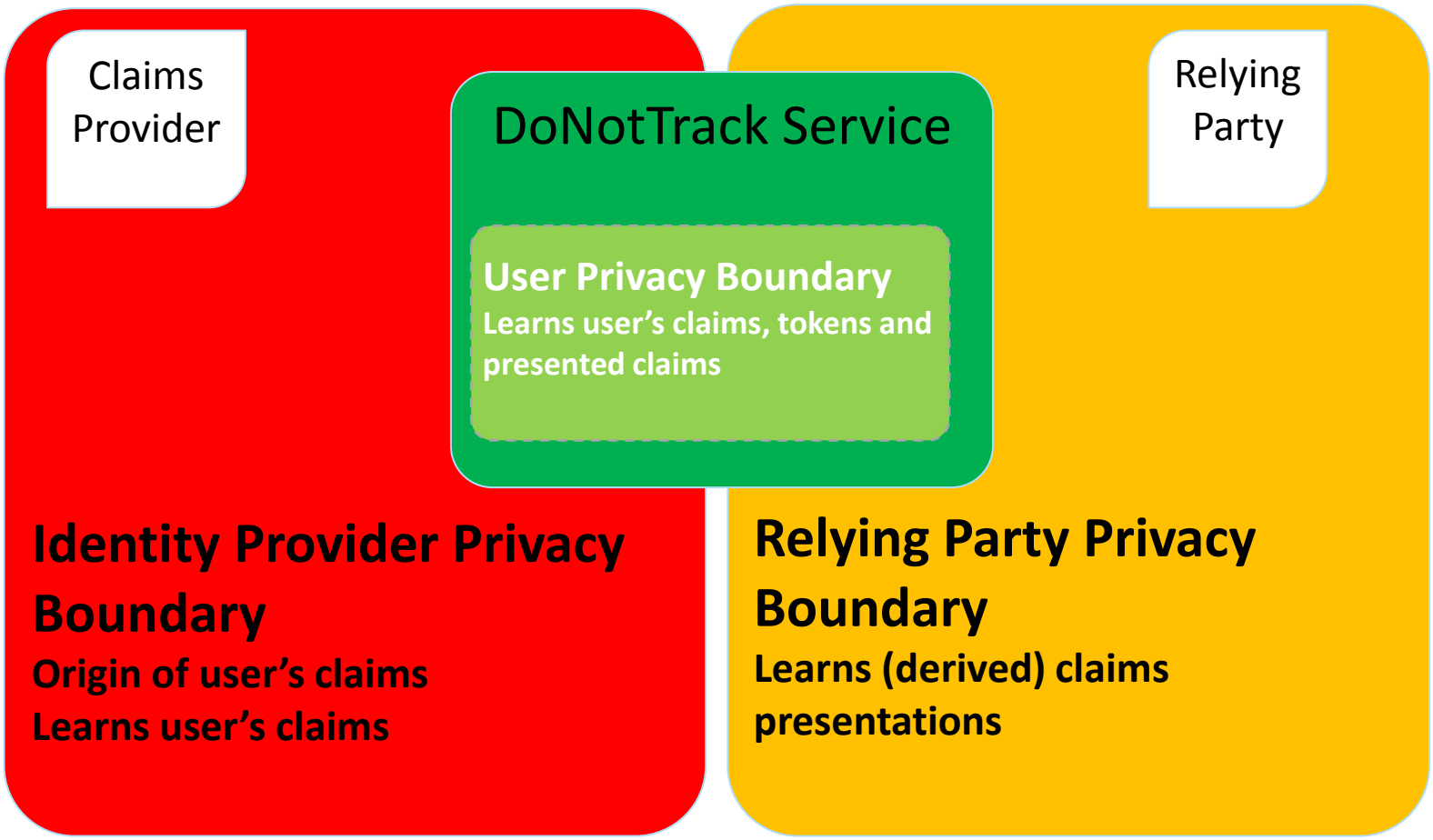
When user tracking and end-end transaction auditing is justifiable, claims can be aggregated while providing cryptographic evidence of every part of a transaction

DoNotTrack

When user tracking is not justifiable, claims enrichment can be done using minimal disclosure so Claims are verifiable but cannot be linked to a user's street identity or leak PII

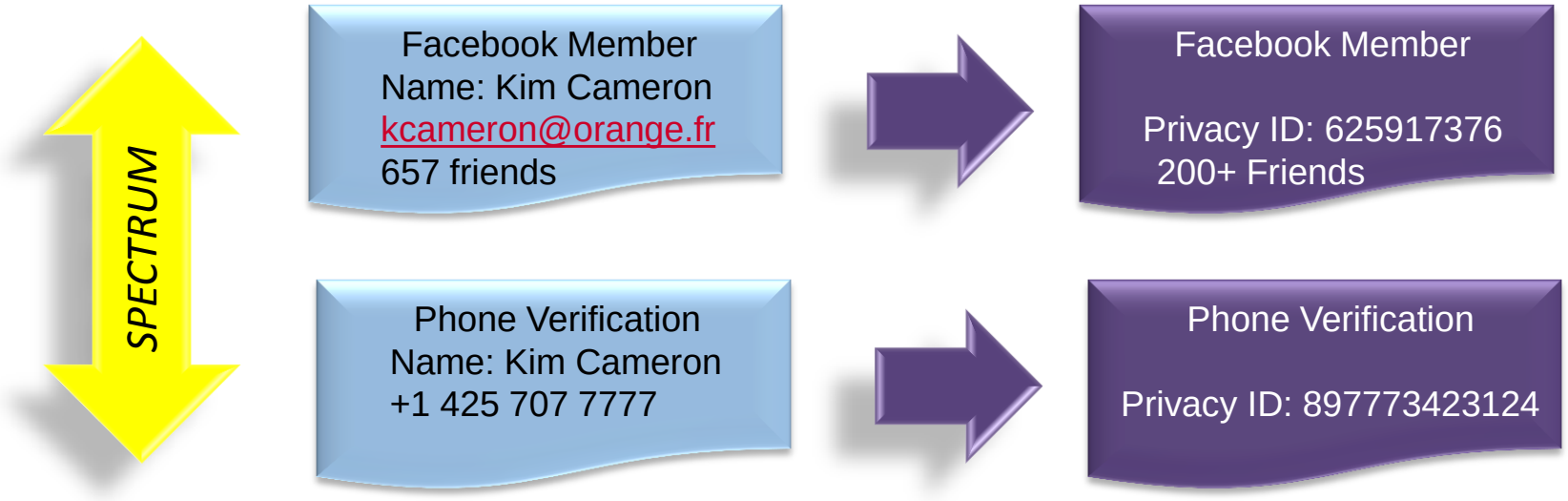
- Combine the Audited and DNT approaches so tracking is impossible for any party except chosen auditors/participants.
- Support standard federation protocols (e.g. SAML, OAuth, OpenID) for interoperability with existing identity ecosystems.

DoNotTrack: Privacy Boundaries



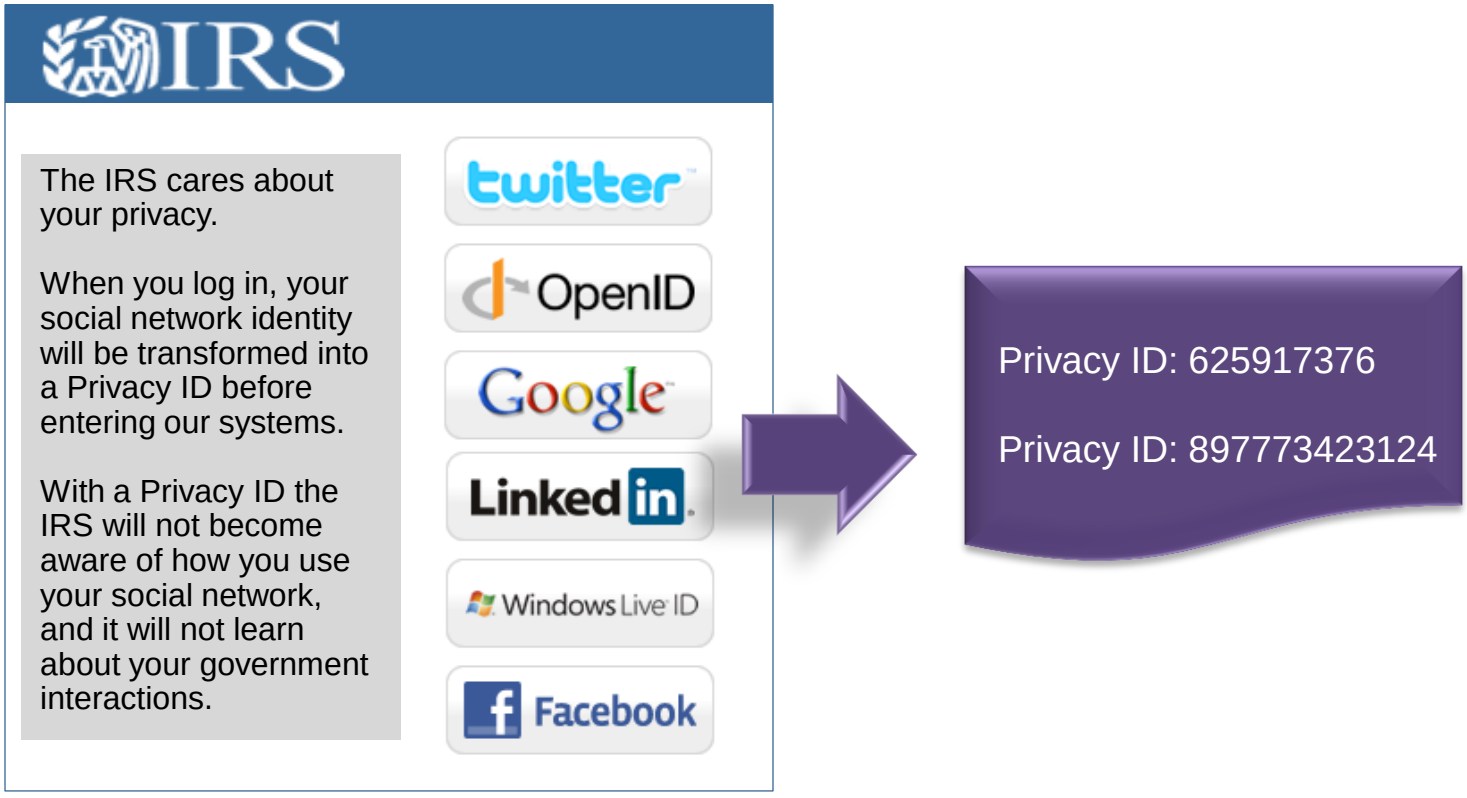
Example of Privacy IDs

- Leverage authentication done by Identity Providers and relevant substantive claims BUT:
  - Strip IP identifier and replace with “Privacy ID” that can’t be linked to original ID*
  - Minimize claims (e.g. birth date to age category) as appropriate
  - Establish a reassuring mental model for users
  - Special ID that protects your privacy but lets RP know what it needs to know



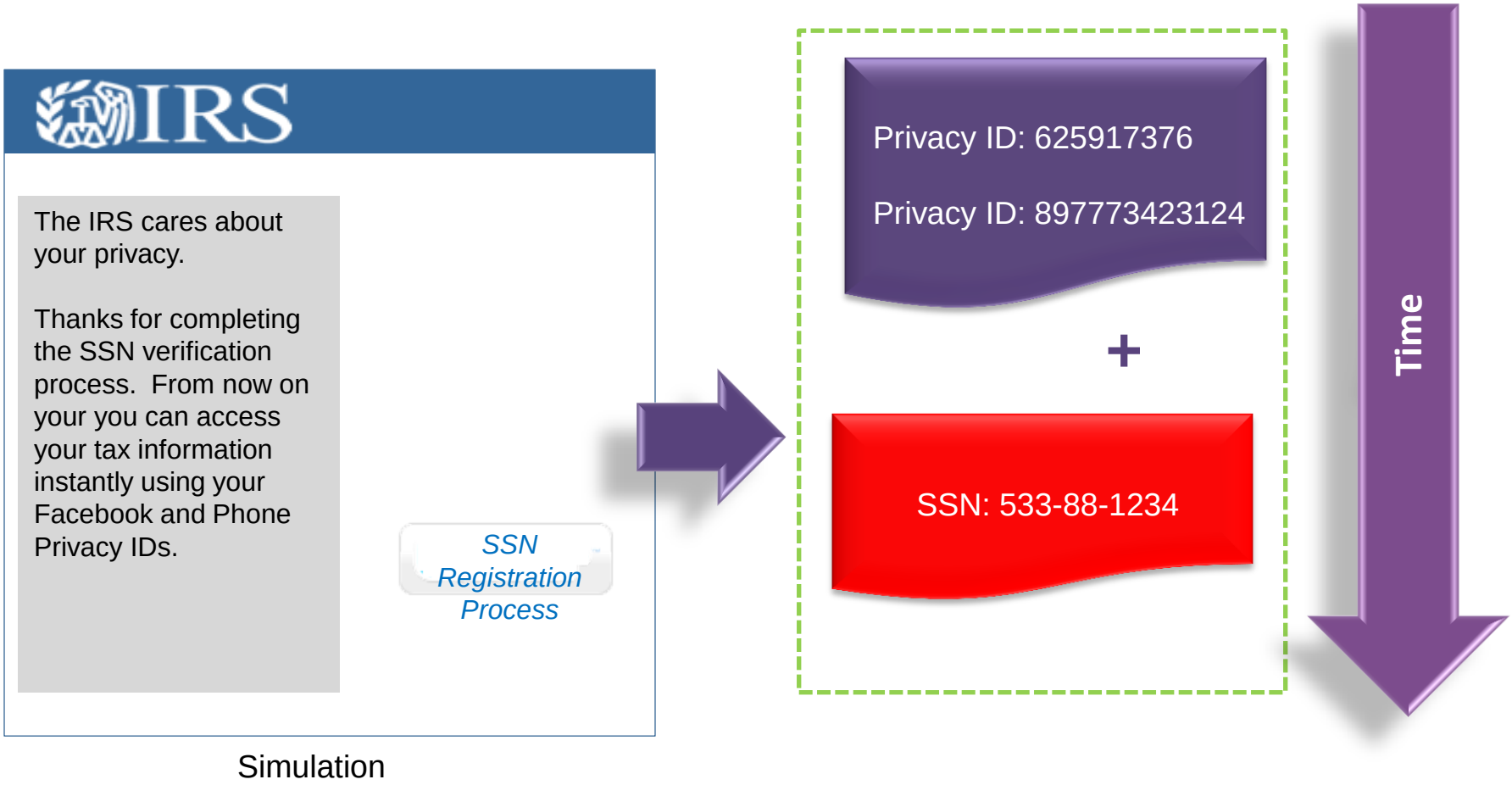
* Different qualities of guarantee are possible

EXAMPLE: IRS



Simulation

IRS (Later That Year)



Simulation

Two Visions of Cloud Identity

- THE IDMAAS model makes it feasible for service providers to assemble claims from multiple sources while respecting the individual's "mental model" of a direct relationship
- Fundamentally different from pushing the user back to a monolithic identity provider that eventually knows all about her ("Register your street address and SSN with Google?")
- With the IDMAAS model we can embrace the cloud without giving up our commitment to "contextual separation".

THE USER'S RELATIONSHIP IS WITH THE SERVICE PROVIDER (RP), NOT AN ALL-SEEING IDENTITY PROVIDER

Apply

- Within three months, brainstorm and be able to discuss:
  - What “Refactoring and Distribution of IT” could mean for your organization
  - The role your enterprise could play in the API economy?
    - As a service provider?
    - As a service consumer?
  - How value would flow if you refactored IT and offered RESTful services?
  - The privacy, security and compliance requirements of your enterprise and customers in the API economy?

Apply

- Within Six Months
  - Develop an analysis of the component IdMaaS capabilities that make sense for your organization
  - Look into the Cloud service landscape as it pertains to support for the API economy
  - Familiarize yourself with the IdMaaS offerings and the extent to which service-offerings satisfy your need to interact with customers and services without regard to the clouds they run on or identities they use…
  - Familiarize yourself with binding promises around organizational control of information by cloud and IdMaaS operators (“right to switch or delete”)

Apply

- Visit http://www.identityblog.com and similar blogs and participate in the discusion

Appendix

Composable Capabilities of IdMaaS

REGISTER	Registration of people, organizations, devices and services	• Distinguishing entities, assigning them identifiers, and publishing in a directory • Based on knowledge of natural people and things; or • Based on federation – accepting digital claims made by others
ATTRIBUTE	Collection and proofing of attributes	• Collecting attributes • Determining that they actually describe an entity registered in a directory • Recording that these attributes belong to that entity
CREDS	Primordial credential management	• Registration of keys, biometric and other information an entity may use to prove it is a unique entity
ISSUE	Claims issuance	• Using primordial credentials or some set of received claims to locate an entity in a directory and issue claims describing the entity
ACCEPT	Claims acceptance	• Accepting claims from a federated source by locating the source in a directory and verifying that trust framework and policy allows the claims to be acted upon
AUGMENT	Claims augmentation	• Using a set of accepted claims to locate the attributes of an entity in a directory and issue an expanded set of claims
TRANSFORM	Claims transformation	• Using a set of accepted claims to issue another set of claims based on sets of rules
ROLE	Management of roles	• Managing a catalog of roles • Registering roles associated with entities
GROUP	Management of groups	• Managing a catalog of groups • Registering groups to which an entity belongs
RELATIONSHIP	Cataloging of relationships	• Managing a catalog of relationship types • Registering the relationships one entity has with another
AUDIT	Identity Auditing	• Maintaining an appropriate record of changes and accesses visible only to auditors
COMPLIANCE	Assurance of compliance	• Complete sets of procedures ensuring compliance with mandated frameworks