IDENTITY & ACCESS CONTROL CHALLENGES in the CLOUD

OASIS International Cloud Symposium 2011

Ditton Manor

Tuesday, 11 October 10.45-12.15

Abstract

- The move to Cloud Computing brings with it a number of special challenges when it comes to security. One particular area is that of identity and access management - managing who can access information is fundamental to information security. Cloud computing has introduced two key changes: firstly although responsibility for access management still lies within the organization, the IAM technology is physically distributed; secondly individuals now have significant presence in IT systems outside of the organization. In this session, the panellists will address some of these concerns including:
  - Identity Related risks
  - Privileged User Management
  - Audit and Compliance
  - Authentication and Authorisation

Introductions

- Mike Small,
  - Senior Analyst KuppingerCole
- Felix Gaehtgens,
  - Director of Technology Partnerships, Axiomatics AB
- Tomas Gustavsson,
  - Chief Technology Officer, Primekey
- Brendan Peter,
  - Deputy Commissioner TechAmerica Foundation, CA Technologies
- Matt Rutkowski,
  - Senior Engineer, Master Inventor, IBM

Agenda

- View from the Analyst
  - Mike Small
- Identity Management Issues in the Cloud
  - Brendan M Peter
- PKI and eId Authentication
  - Tomas Gustavsson
- Authorization in the Cloud
  - Felix Gaehtgens
- Audit & Compliance
  - Matt Rutkowski
- Open Discussion (30 Minutes)

IAM Challenges in the Cloud View from the Analyst

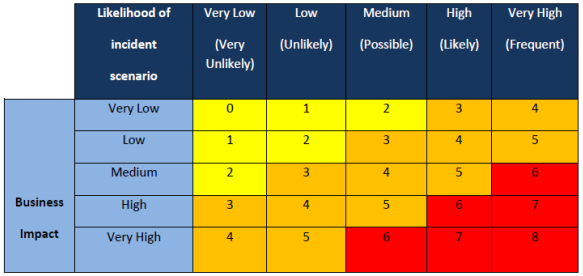
Mike Small CEng, FBCS, CITP

Fellow Analyst

KuppingerCole

Top Cloud Identity Risks

- ENISA Cloud Risk Assessment
  - Compliance Challenges
  - Cloud provider – malicious insider – privilege abuse
  - Management Interface compromise
  - Impersonation



Business Impact \ Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Very Low	0	1	2	3	4
Low	1	2	3	4	5
Medium	2	3	4	5	6
High	3	4	5	6	7
Very High	4	5	6	7	8

We have based the estimation of risk levels on ISO/IEC 27005:2008 (10).

- Cloud Security Alliance - Top Threats
  - Abuse and Nefarious Use of Cloud Computing
  - Malicious Insiders
  - Data Loss/Leakage
  - Account, Service & Traffic Hijacking

enisa European Network and Information Security Agency

ENISA - Cloud Computing - Benefits, risks and recommendations for information security
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Cloud Security Alliance - Top Threats to Cloud Computing V1.0
http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

KUPPINGERCOLE
www.KUPPINGERCOLE.com

Identity – who can you trust?

Facebook and Bebo child sex abuse postman jailed.

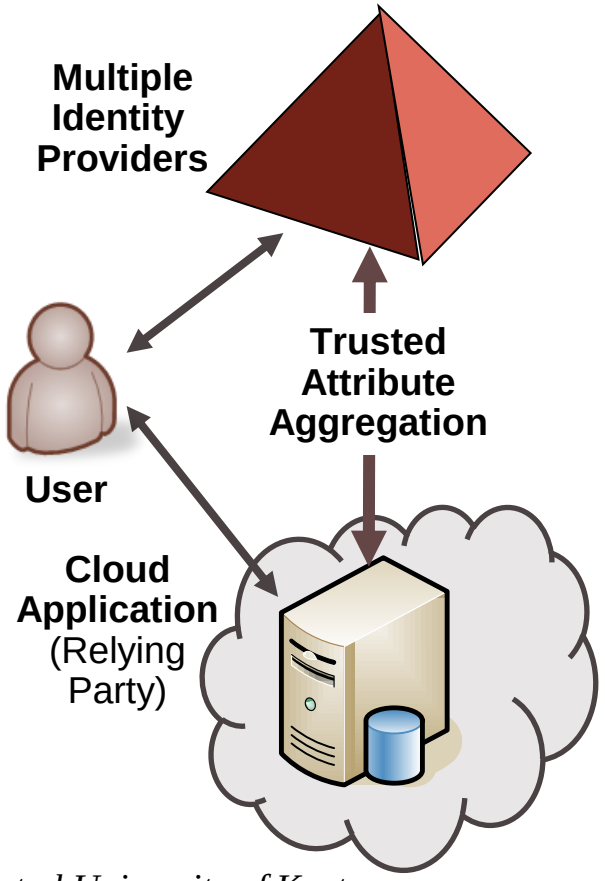
A postman from Cornwall who used social-networking websites to abuse hundreds of children has been jailed for eight-and-a-half years.

The 29-year-old, from Penryn, approached children on Facebook and Bebo, Truro Crown Court heard.

http://www.bbc.co.uk/news/uk-england-cornwall-11403984

Privacy and Attribute Aggregation

- Trusted Identity Providers.
- Privacy vs. Traceability
  - Minimum disclosure
  - Identity Escrow
- Attribute Aggregation. Example – Council Parking Permit:
  - Proof of Car Keeper from DVLA
  - Proof of address from DWP
  - Credit Card



See - Trusted Attribute Aggregation Service, Prof David Chadwick et al University of Kent

Authentication

Carbon Thieves Force European Union to Improve Security, Close Spot Market

www.bloomberg.com
January 21st, 2011

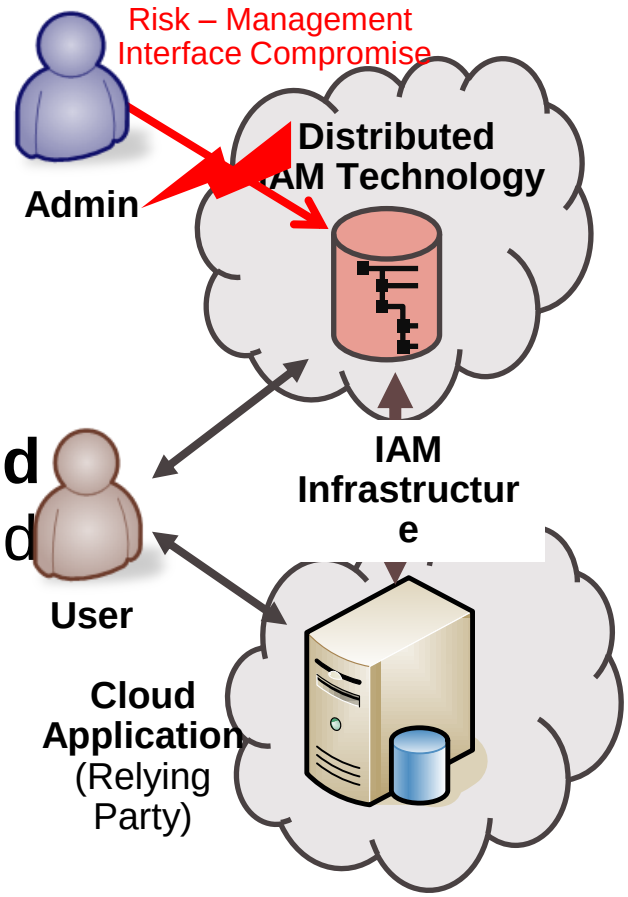
The European Union, whose decision to suspend registries halted the region's spot carbon-emissions market following the theft of permits, said it won't lift restrictions until member states step up identification checks.

It suspended most operations at Europe's 30 registries for greenhouse-gas emissions on Jan. 19 after a Czech trader reviewing his $9 million account found "nothing was there." The EU estimates permits worth as many as 29 million Euros may be missing.

"At minimum they need to have second authorization in place, such as electronic certificates or ID cards," said Simone Ruiz, European policy director of the Geneva-based IETA.

Administration

- The user's identity and access is **managed by the organization**.
- The IAM processes are internal to the organization.
- The **IAM Technology is distributed** and may be separate from the Cloud Application/Environment.
- **The Management interface is a serious risk**



Authorization

- No single Cloud Authorization Model
- Most SaaS vendors have their own model
- Claims based using SAML
- Claims based from Microsoft (Geneva Server)
- ABAC (Attribute based) - using XACML standard for policy (Axiomatic)

Abuse of High Privilege Role

Database admin steals 2.3M consumer records at Fidelity National subsidiary

A senior database administrator at a subsidiary of Fidelity National Information Services Inc. who was responsible for defining and enforcing data access rights at the company instead took data belonging to about 2.3 million consumers and sold it to a data broker.

Computer World, July 3rd, 2007

The broker in turn sold a subset of the data to other marketing companies. The stolen data included names, addresses, birth dates, bank account and credit card information, the company said in a statement released today.

Audit and Compliance

- "Certain organizations migrating to cloud have made considerable investments in achieving certification either for competitive advantage or regulatory requirements – (e.g. PCI DSS)"

ENISA - Cloud Computing - Benefits, risks and recommendations for information security
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

- CSA Cloud Controls Matrix
- COBIT and the Cloud
- SSAE 16 – Reporting on Controls at a Service Organization
  - SOC Type 1 Report
  - SOC Type 2 Report
- AICPA Trust Services
  - SysTrust/WebTrust

Ten Cloud Questions

1. How is legal and regulatory compliance assured?
2. Where will my data be geographically located?
3. How securely is my data handled?
4. How is service availability assured?
5. How is identity and access managed?
6. How is my data protected against privileged user abuse?
7. What levels of isolation are supported?
8. How are the risks of virtualization “sprawl” managed?
9. How are the systems protected against internet threats?
10. How are activities monitored and logged?

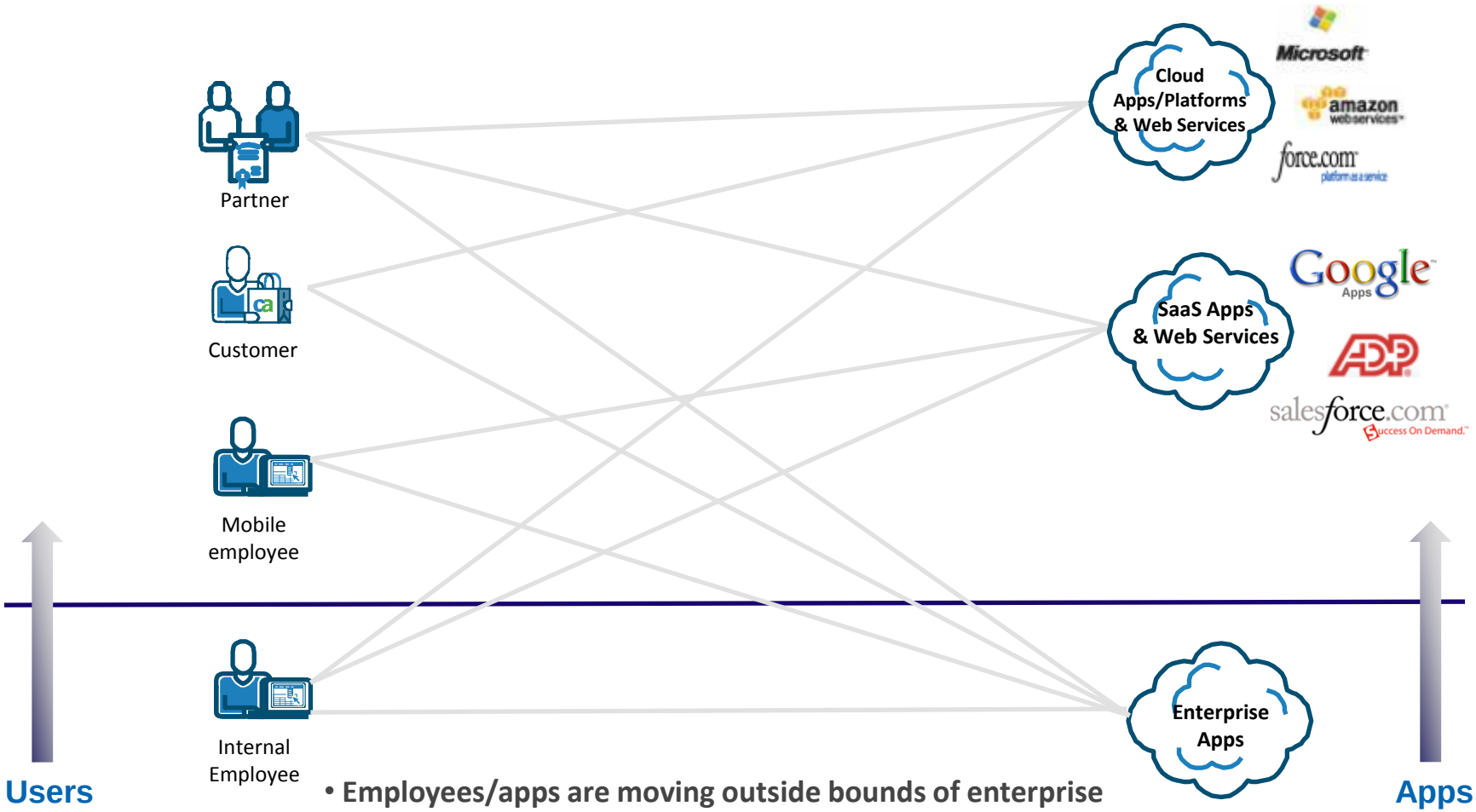
Cloud Computing - Cloud Security Management Advisory Note; KuppingerCole 2011

Identity Management Issues in the Cloud

Brendan M. Peter

Director, Global Government Relations

Management of Identities Becomes More Complex



- Employees/apps are moving outside bounds of enterprise
- Increasing need for secure collaboration
- Cloud-based environments make compliance and policy harder to manage

Security Questions Don't Change Because of Cloud

—Are we compliant?

—What are our security risks?

—What can we do to mitigate these risks?

—What do we deal with first?

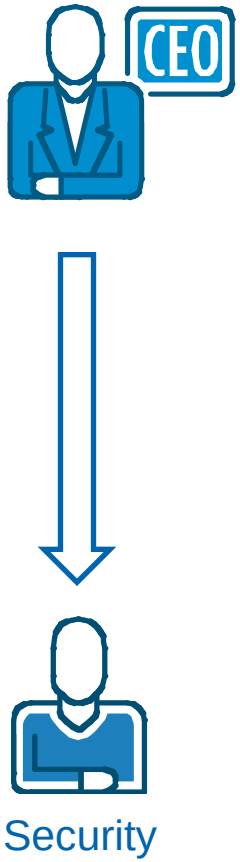
—Who has access to what?

—Who authorized their access?

—Do they have the right level of access?

—What did they do?

—How do we prove compliance?



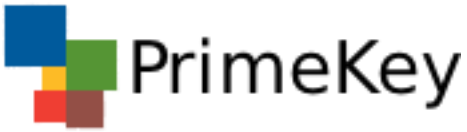
the challenges

Sharing digital identities to enable applications in different security domains to work together securely & seamlessly.

- Security concerns can **slow rollout** of new revenue-enhancing, IT-enabled partner/customer relationships
- Separate security domains are **inconvenient for the users** as security typically becomes burdensome on them
- It is **costly to build & maintain** custom integration with each partner
- Can result in a **burden on the Service Desk** for access support & forgotten credentials
- **Increased IT risk** due to challenge of controlling access to outsourced applications
- Other service providers provide federation today – risk **falling behind competition**

PKI and eld Authentication

- Tomas Gustavsson
- PrimeKey Solutions AB,
- www.primekey.se
- ww.ejbca.org

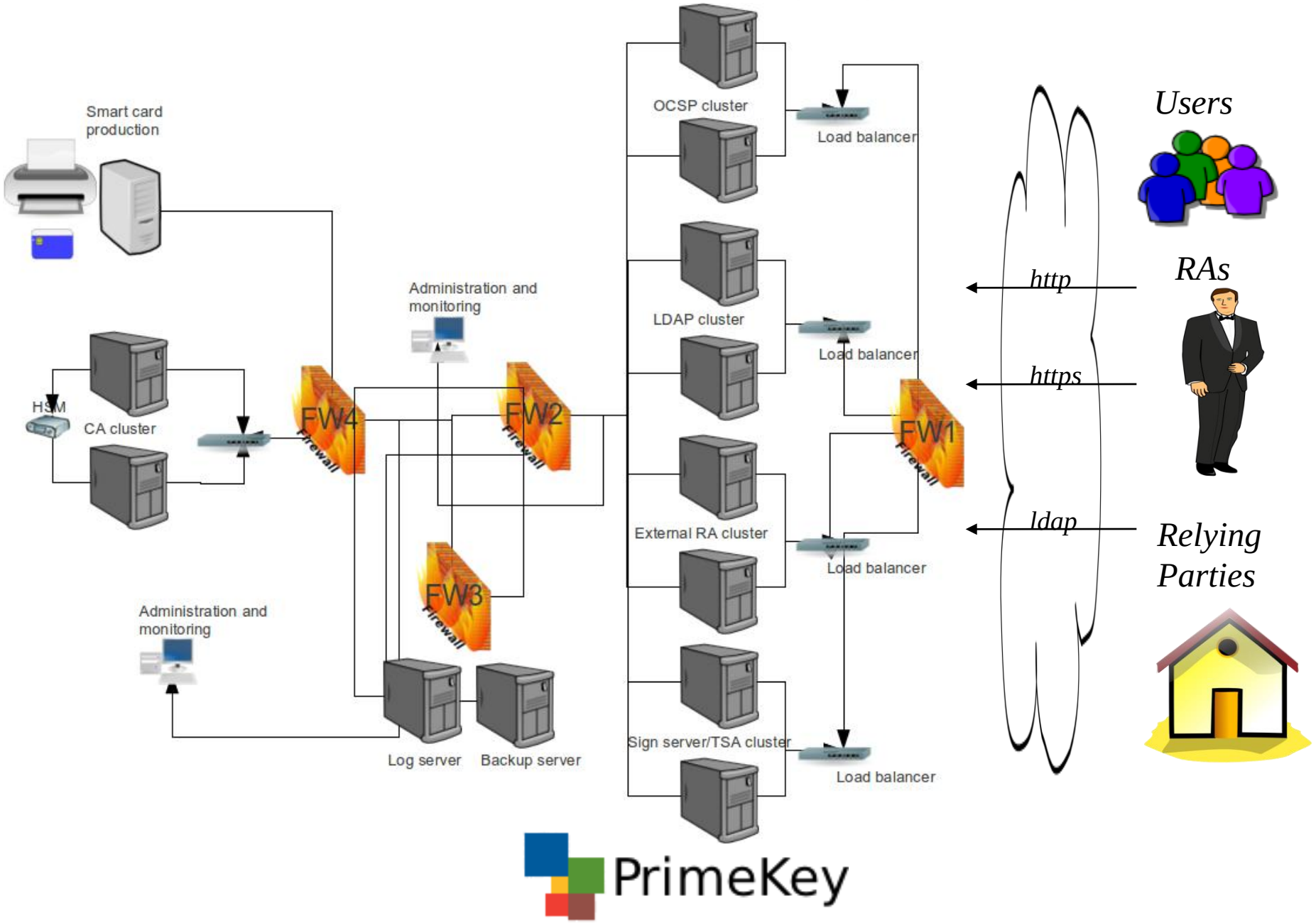


- *PKI is a foundation security infrastructure service*
- *Ubiquitous in securing cloud resources*
  - *TLS secures communication*
  - *Certificates authenticate resources*
  - *Electronic Ids authenticate users*
  - *PKI protects integrity and confidentiality of stored data*

PKI has been around "for ever".
PKI in the cloud is no different from PKI as we know it.

Organizations will want to use their Ids for authentication.
Government and Citizens will want to use eIds for authentication.

PrimeKey


Smart card production
Administration and monitoring
HSM
CA cluster
FW4
Firewall
FW2
Firewall
FW3
Firewall
FW1
Firewall
Administration and monitoring
Log server
Backup server
OCSP cluster
Load balancer
LDAP cluster
Load balancer
External RA cluster
Load balancer
Sign server/TSA cluster
Load balancer
http
https
ldap
Users
RAs
Relying Parties
PrimeKey

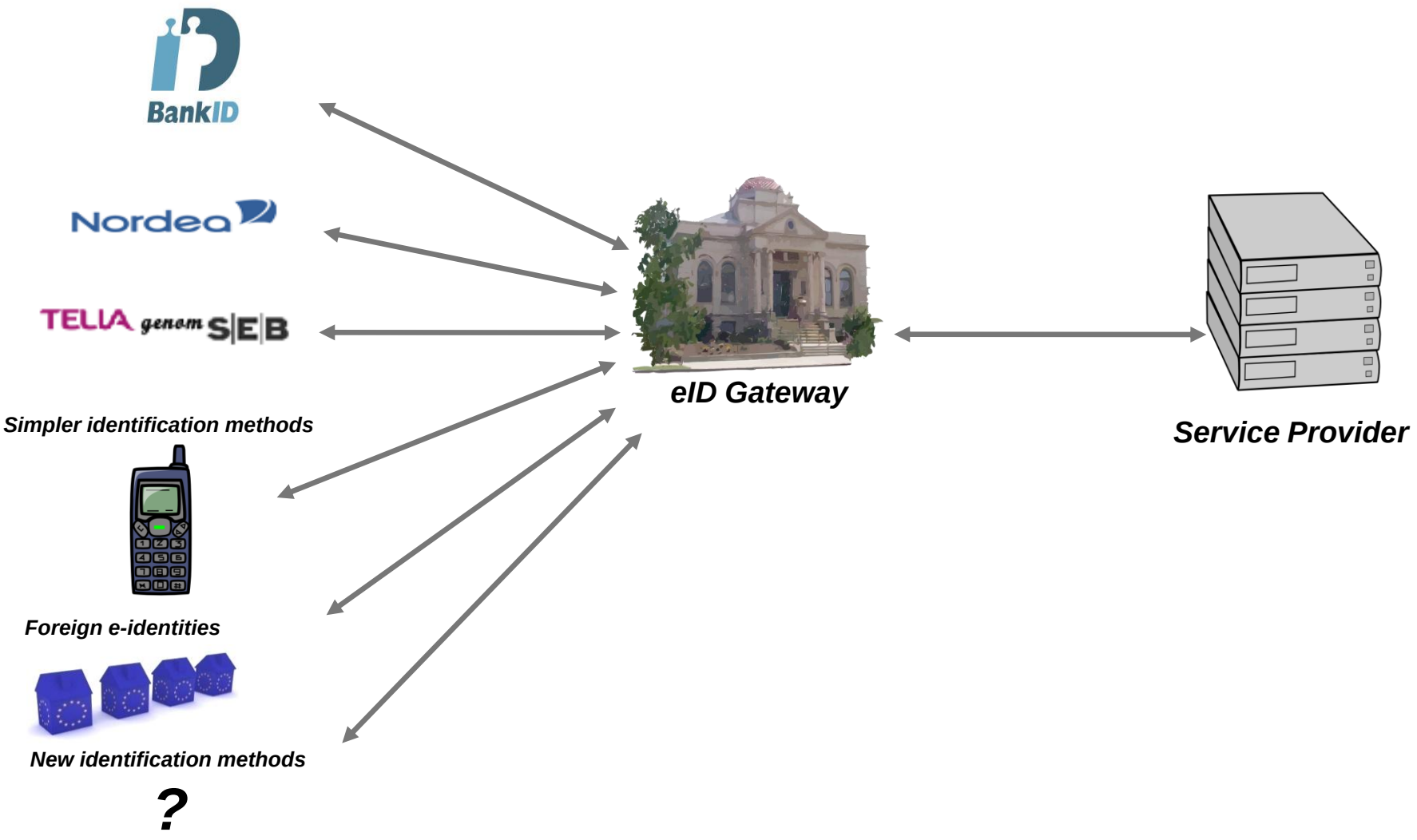
Companies want a solution that:

- *Offers consumers a safe yet simple solution*
- *Enables them to reach all their customers*
- *Is cost-efficient*
- *Is future-proof*

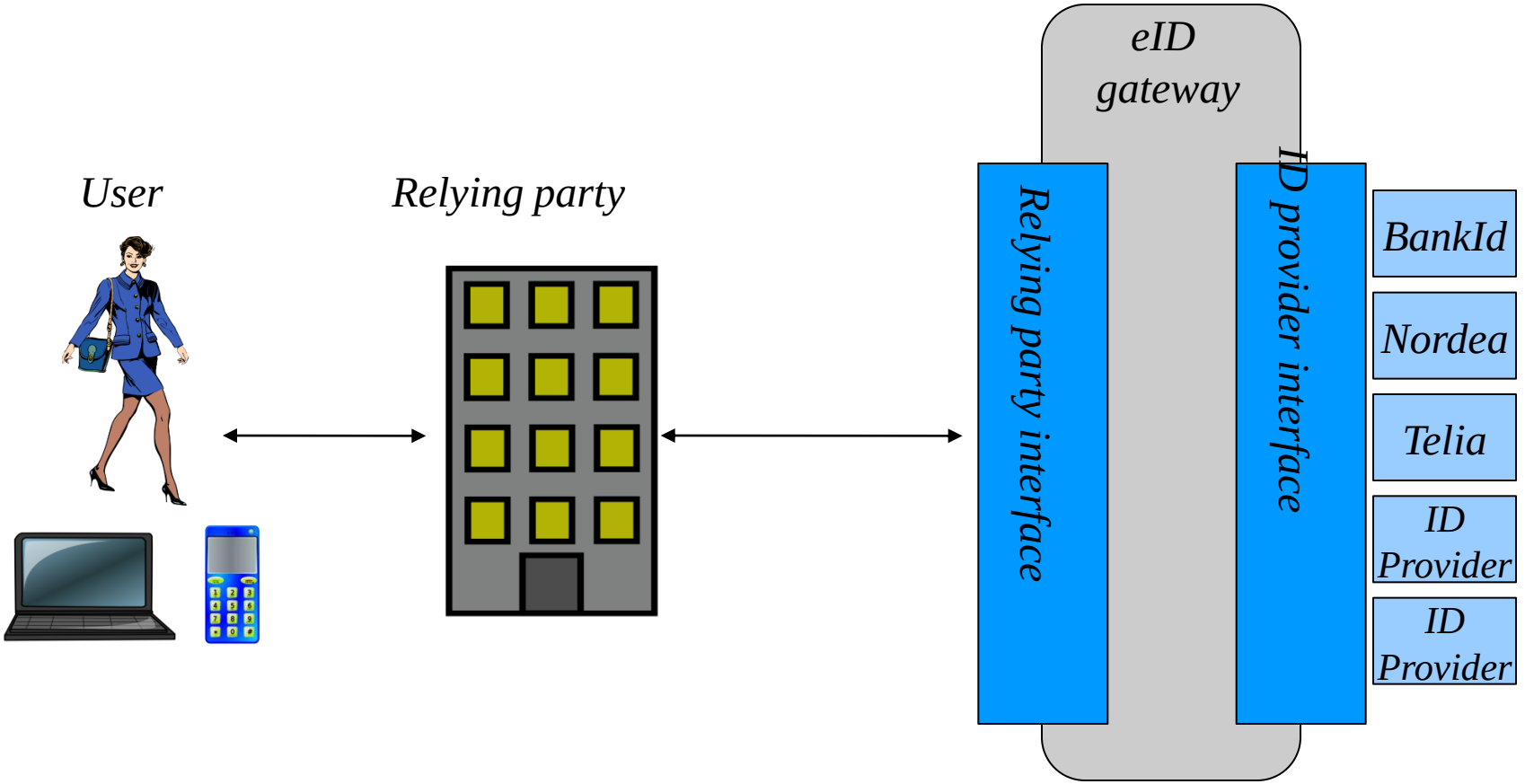
Currently many states are deploying national ID.
In many cases based on cost-effective open source components.

Looking for ways to leverage existing ID infrastructures.

PrimeKey


BankID
Nordea
TELIA genom SEB
Simpler identification methods
Foreign e-identities
New identification methods
?
eID Gateway
Service Provider

PrimeKey


User
Relying party
eID gateway
Relying party interface
ID provider interface
BankId
Nordea
Telia
ID Provider
ID Provider

PrimeKey

EU together with private interests are doing a lot of work to facilitate the use of electronic Ids.

- *STORK*
- *...*
- *CeSecore.eu*
- *…*

Open standards is a pre-requisite for wide deployment of Cloud identity solutions.

PrimeKey

AXIOMATICS

Authorization in the Cloud

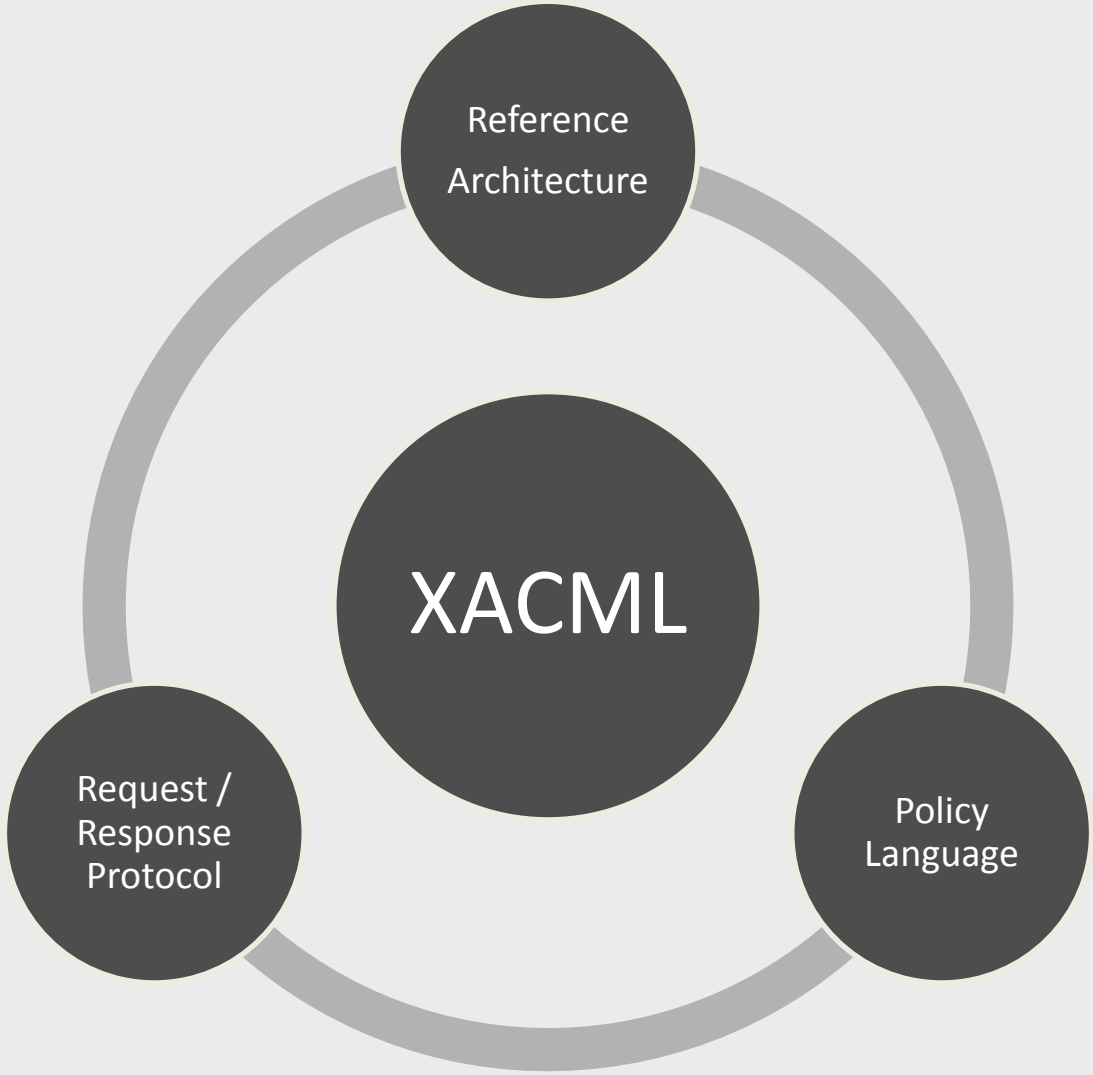
(There's more to security than authentication!)

Felix Gaehtgens

Director of Technology Partnerships

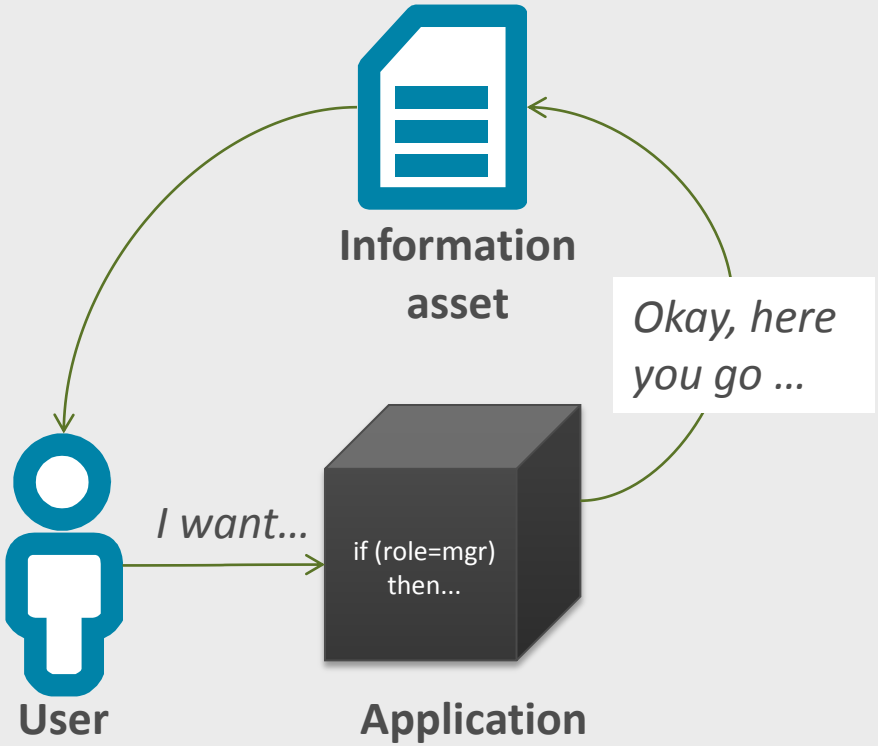
Axiomatics AB

XACML – The Standard for Authorisation

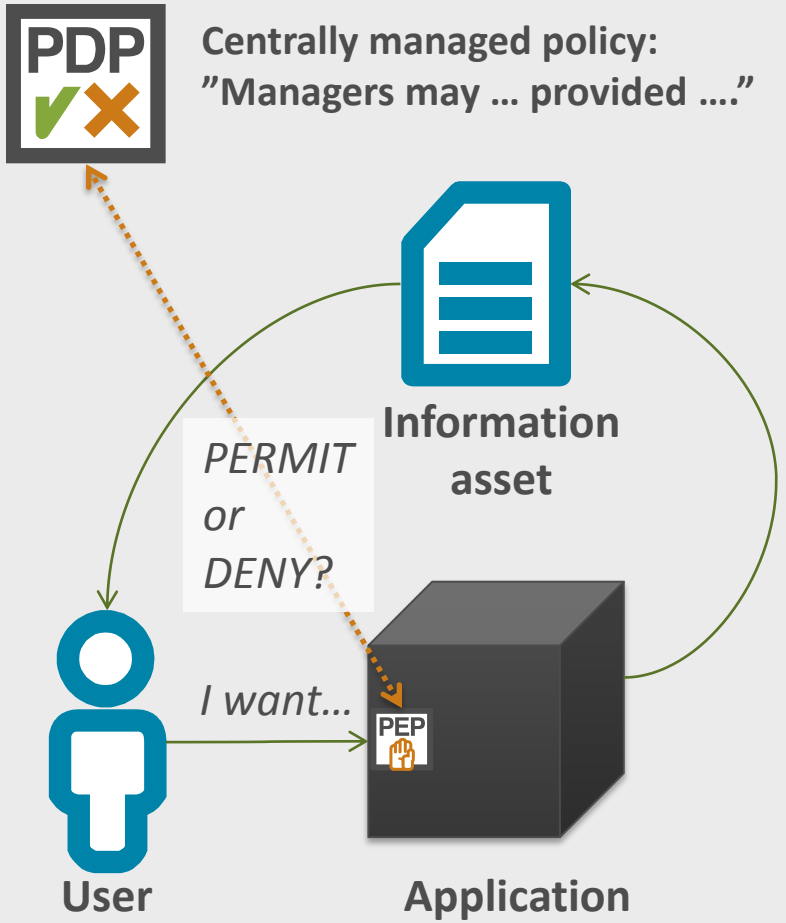


The black box challenge

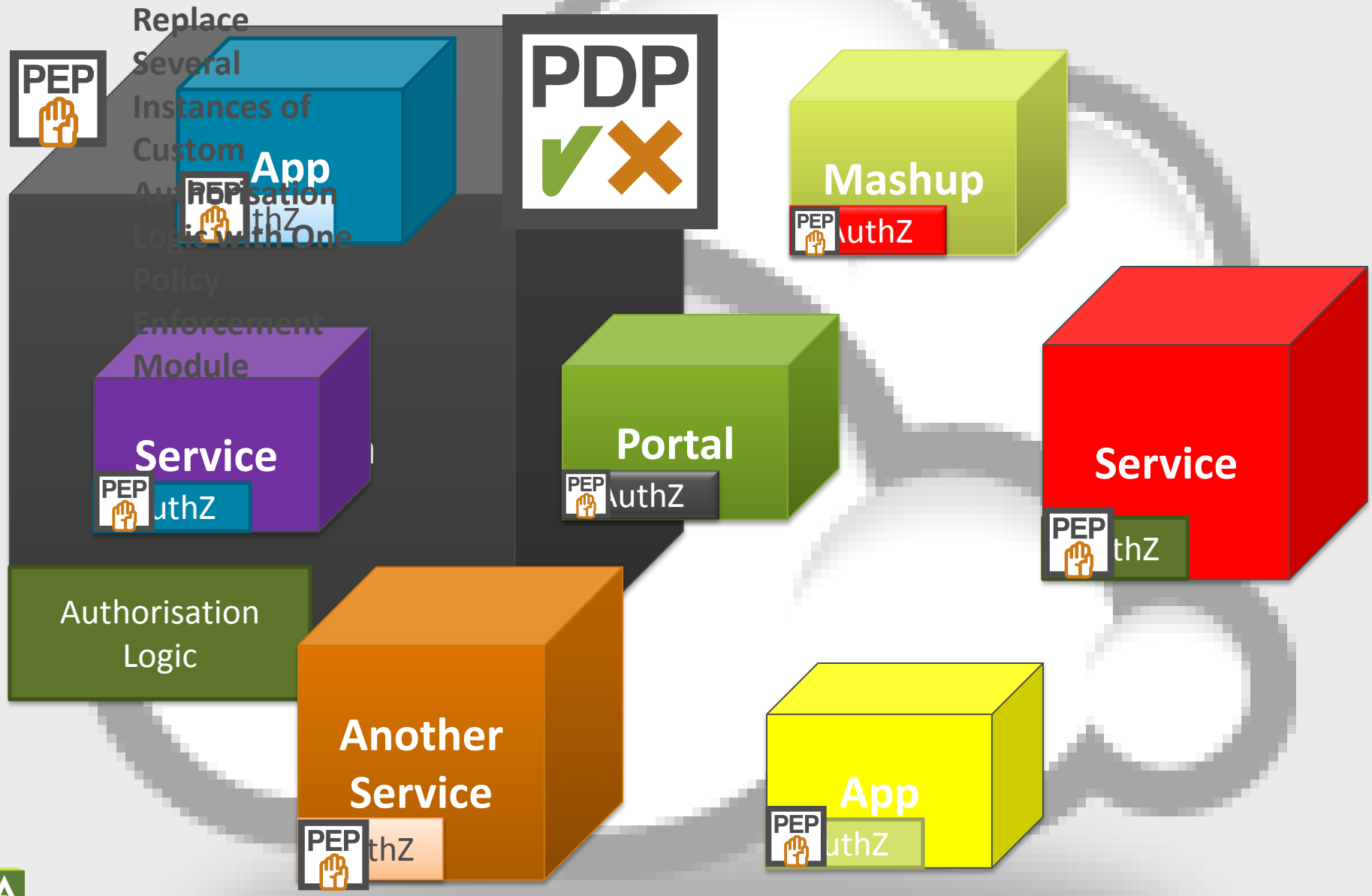
- Current situation



- Externalized authorization



...in the cloud...

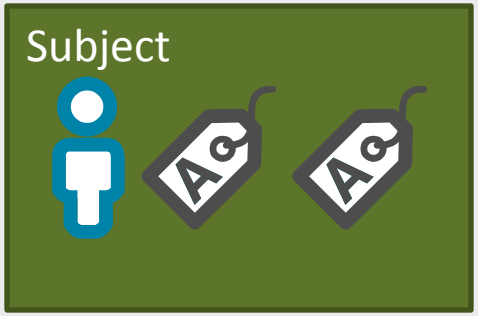

Replace Several Instances of Custom Authorisation Logic with One Policy Enforcement Module
PEP
PDP
App
Mashup
Service
Portal
Service
Authorisation Logic
Another Service
App

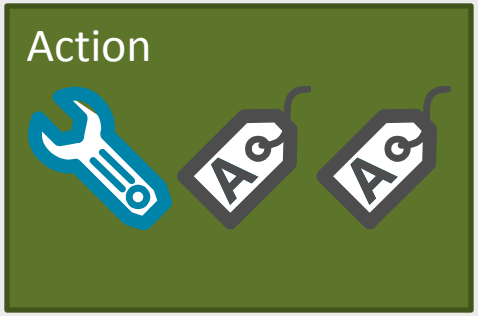
XACML Policy Language

Subject	Action	Resource	Context
A user…	…wants to do something…	…with information assets…	… in a given environment…
Example:			
A physician…	…wants to open and edit…	…Joe's health care record…	… in the emergency room at 3 pm
A bank client wants to …	…withdraw € 5000…	… from his account…	…at an ATM machine in Stockholm at 8 pm
A consultant…	… wants to check out the functional specification …	…from the document management system…	… at 2 a.m from a hotel lobby in Milano…

XACML Concepts

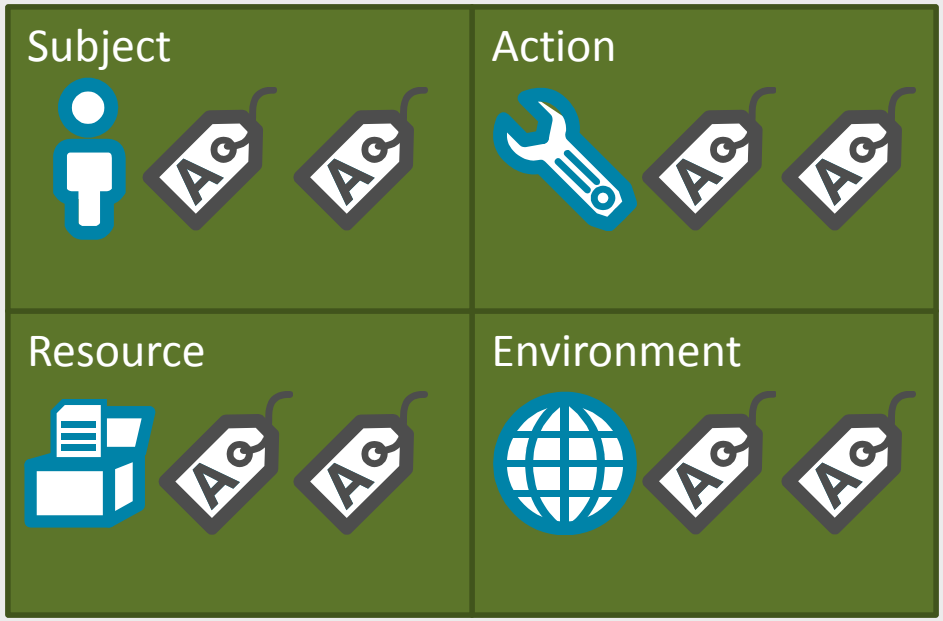
It’s all about Attributes!
ABAC = Attribute Based Access Control





XACML Concepts

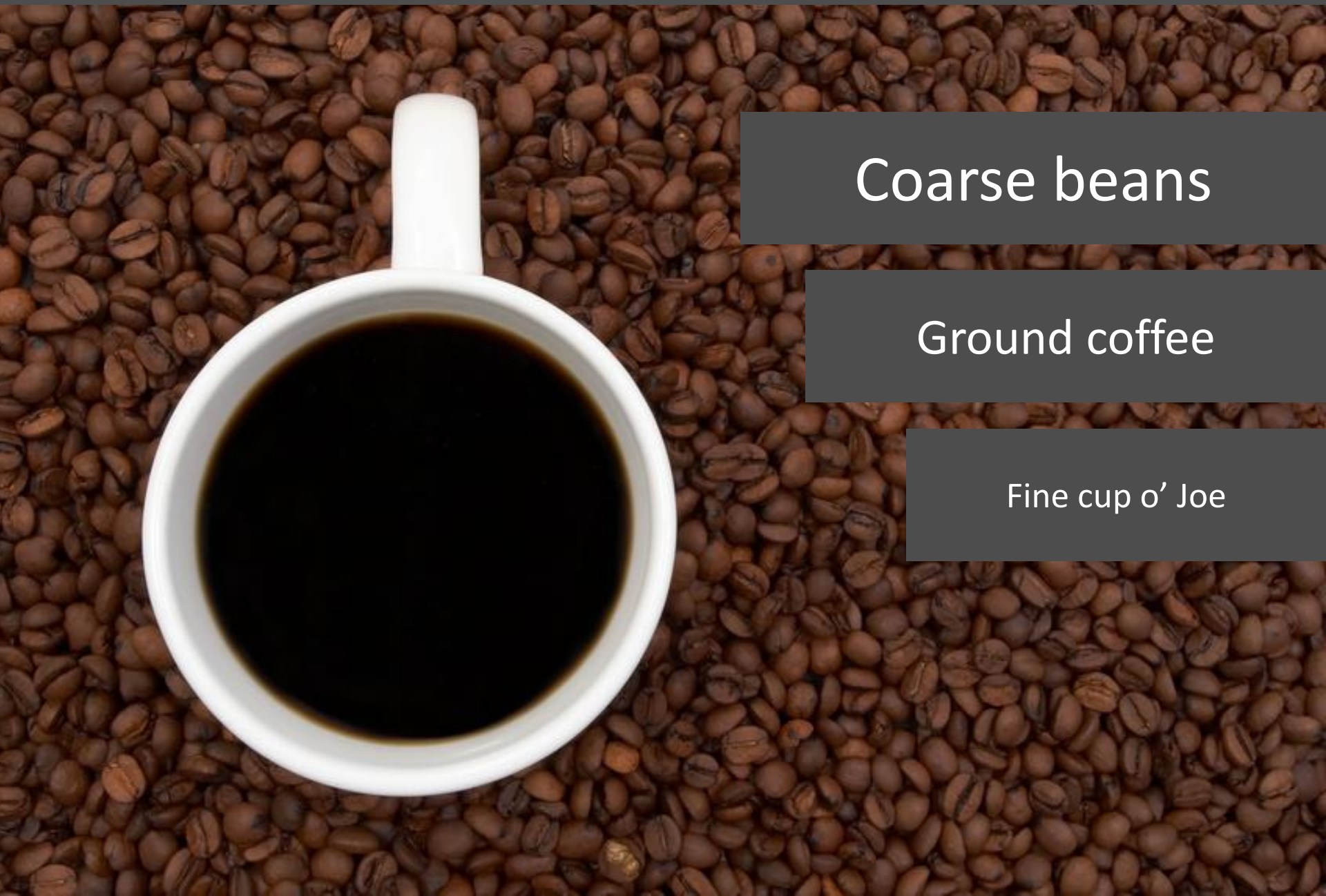
It's all about Attributes!
ABAC = Attribute Based Access Control



XACML Policies

XACML Request

XACML and ABAC… from coarse to fine-grained AC



Welcome to the Future

OASIS

Identity & Access Control Challenges in the Cloud

Audit & Compliance

Matt Rutkowski
OASIS Identity in the Cloud TC, Editor
Senior Engineer and Master Inventor
IBM Software Group, Emerging Standards

Audit & Compliance Challenges in the Cloud

How can an organization using "The Cloud" ensure compliance with the laws and regulations that they are subject to?

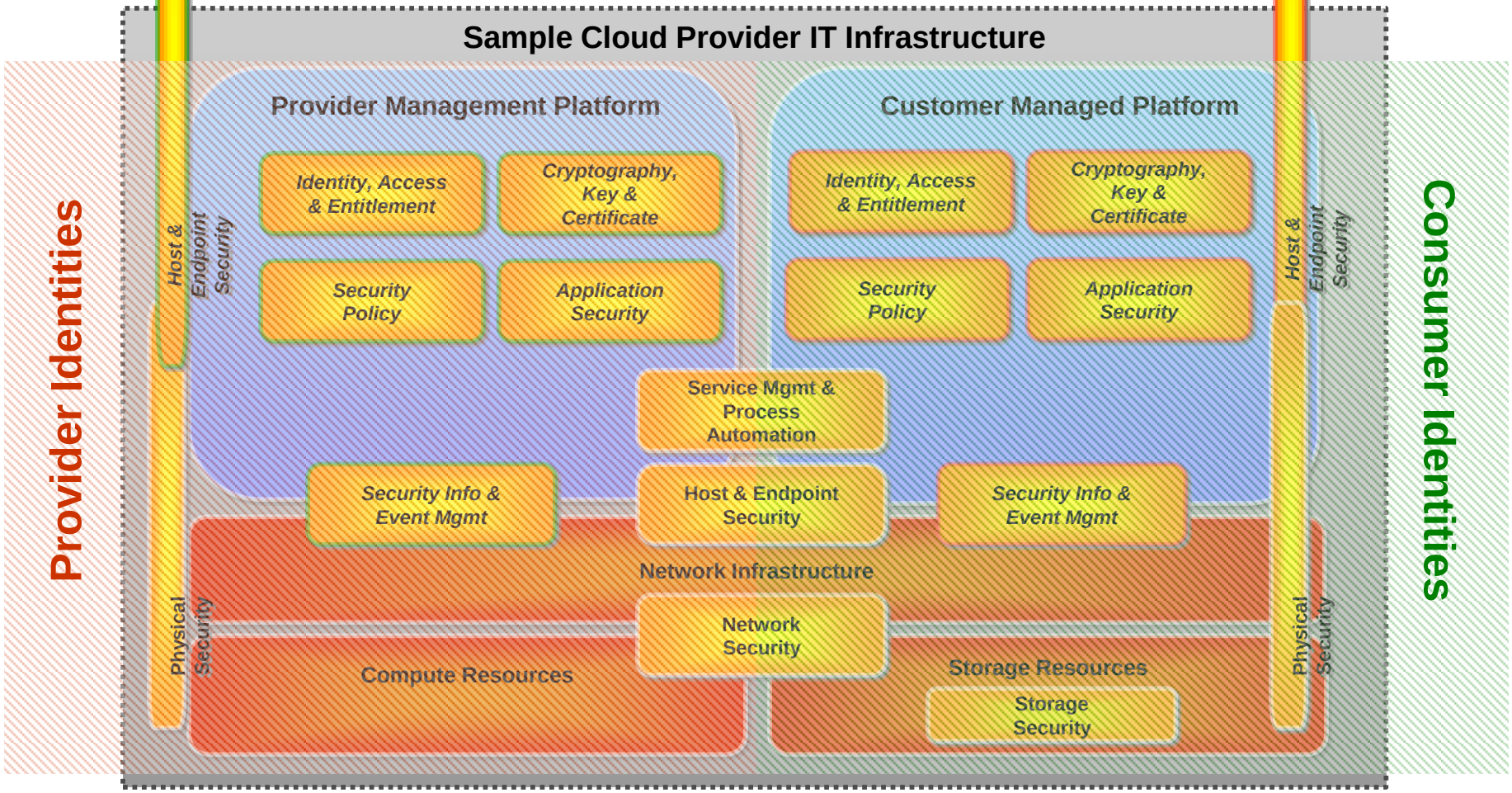
- **How Can a Cloud Provider**
  - **Provide Assurance that Tenants' Compliance and Security Policies are Consistently Managed and Enforced "in the cloud" as they would be if Managed Locally?**
    - Applies to Applications, Configurations and Data whether "Static" (in storage) or "Dynamic" (in network or in process)

- **Clouds Must Provide for the Fundamental Tenets of Auditing**
  - ***Every Action that Affects a Resource being Governed by a Compliance Policy Must be Recorded***
    - Includes Security, Regional, Industry and Tenant or Account Specific Policies
  - **That Record (Log, Event, etc.) Must Contain the *Auditable Identities* of the**
    - ***Humans or Entities*** *- involved in Initiating each Action*
    - ***Target Resource*** *– that was the intended target of the action*
    - ***Management Resources*** *– that manage / control access to the intended Target Resource*

- **Audit Records Should Be Available to Tenant Customers As Needed**
  - **The Identities Contained in these Records Must provide an *Audit Trail* into the Cloud**
    - *The "Trail" Maps to the Actual Resources Used to perform the Action in the Provider's Infrastructure*

A Cloud Provider IT Datacenter - View of Security Controls & Identities

- Separation of Provider & Consumer Identities Used for Audit & Compliance
  - Security Controls Potentially Implemented with Different Products & Standards
- Identity Representation & Format May Change at Each Layer
  - e.g. Account, User ID, Service ID, Security Token, Transaction ID, etc.



Some Specific Identity Management Challenges

- **Identity Management "Services" for Cloud May Be Distributed**
  - **May be Hosted Internal or External to the Cloud Deployment**
- **Distributed Nature of Cloud Permits Multiple Identity Providers, Authentication and Authorization Services**
  - **Multiple Identity Providers, Both Internal and External to Cloud Deployment**
  - **Different Identity Credentials / Representations / Formats Used at Different Layers of the Cloud Platform and Infrastructure**
- **Providers Need to Correlate Identity Across Infrastructure Layers**
  - **As Identity Representations Change, Providers must Maintain an Auditable Trail to the Original Identity Provider at Any Point in a Transaction**
    - *Including Cloud Applications that Cross Deployment Boundaries (Hybrid Cloud)*
- **Cloud Providers Need to be "Region" Aware for Compliance**
  - **Cloud Providers MUST be able to Associate Geographic & Temporal Location to Each Identity**
    - *Identities May Need to be Governed / Managed by Geography to enforce Regional Compliance Policies, Regional Times (e.g. Concept of "Business Hours")*

Ultimately, the Consumers of Cloud are Responsible for the Security and Integrity of their Own Data, Even when it is held by a Cloud Service Provider

Misconceptions About Cloud Audit & Compliance

- **Cloud Architectures that Apply Identity Mgmt. Standards Are Not Necessarily Auditable**
  - **Many Security Standards and Identity Representations Work "Point-to-Point" or Within One Layer of the Architecture Limiting Auditability**
  - ***Piecing Together Proven Security Standards & Products Together in a Cloud Infrastructure Does Not Guarantee Auditability***
- **Traditional Compliance Certifications on Provider Datacenter Do Not Generally Extend to Tenant Customer Applications and Data**
  - **Primarily Exist to Assure the Provider of their Own Cloud Infrastructure Security**
  - **May Not Account for Customer Regional, Industry and Corporate Policies**
    - Difficult to permit the Consumer to Manage these Granular Policies Remotely
  - **Do Not Account for Tracking the Use of Virtualized Resources, Co-Tenanted Data**
- **Negotiating Custom Service License Agreements (SLAs) to Assure Compliance and Access to Audit Data…**
  - **Can Negate the Cost Savings Promised by a Cloud Marketplace**
  - **Once Customer Adapts Auditing Tools & Processes to a Single Provider they can become "Locked In"**

Identity in the Cloud Technical Committee

TC Sponsors

Alfresco Software
Axway Software
CA Technologies
Capgemini
Cisco Systems
IBM
Jericho Systems
Lieberman Software
Microsoft
Ping Identity Corporation
Red Hat
SafeNet, Inc.
SailPoint Technologies
SAP AG
Skyworth TTG Holdings Ltd.
Symantec Corp.
The Boeing Company
TRUSTe
US Dept. of Defense (DoD)
Vanguard Integrity

Charter

- Describe security challenges posed by identity management in cloud through use cases
- Perform standards gap analysis against use cases and existing identity management standards
- Investigate the need for IdM profiles to achieve interoperability within current standards

Published Committee Note Draft - *27 June 2011*

- "*OASIS Identity in the Cloud TC - Use Cases Version 1.0*"
  - 32 Identity Management Use Cases
  - Covering 13 Defined Categories of Identity Management
  - **7 Have Clear Focus on Audit & Compliance Issues**
  - However…

Nearly all Use Case Submissions Listed

"Audit & Compliance" as a Key Security Area Regardless of the Scenario

Meeting the Challenge

- **To Realize the Promise of a "Cloud Marketplace"**
  - ***Cloud Providers and Consumers Must Work Together to Create the Standards and Profiles needed to Provide Consistent Audit and Compliance Management***
    - *Approach Audit & Compliance as Critical to Cloud Adoption*
- **Every Component of a Cloud Provider's Infrastructure MUST be accountable for the Resources they Manage**
  - *Each Able to Produce Auditiable Records that Contribute to the Complete Audit Trail*
  - ***Linked at All Points to Identities and additionally to Associated Access Rights and Entitlements***
- **Develop Consistent Open Standards for Cloud Auditing That Can Be Utilized By Cloud Providers in Their Management Platforms**
  - **Create Profiles of Existing Security Standards for Cloud Identity Management that Include Audit Considerations**
    - *Including Standards for Interfaces, Identity Formats, Protocols and Audit Data that state the Requirements for Creating Valid Audit Records*

These Standards Based Profiles would Essentially Define

Comprehensive Cloud Security Management Service Standards for Auditing

DISCUSSION

SUMMARY

THANK YOU