Kantara Initiative Workshop

Identity as Security Glue for the Cloud

Matthew Gardiner

CA Inc.

&

Chris Sharp
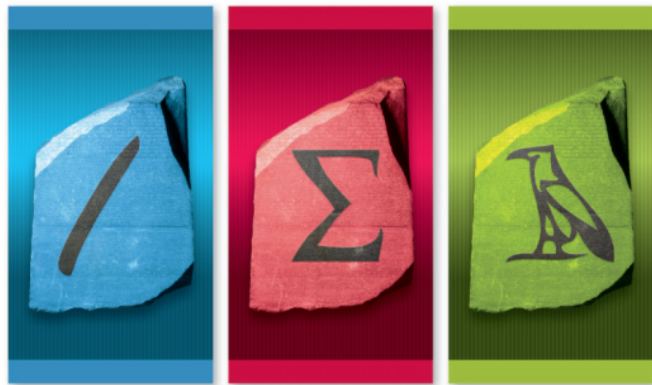
MEDecision

RSACONFERENCE**2010**

SECURITY DECODED
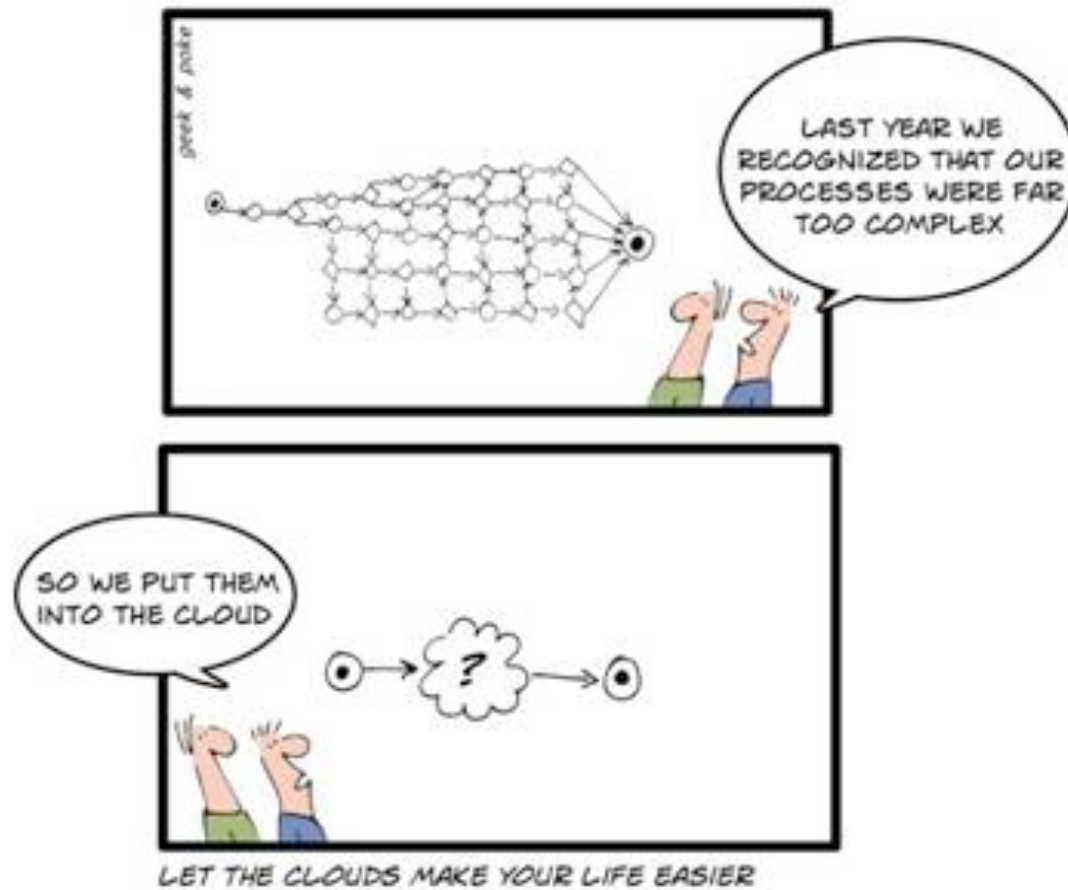
Identity as Security Glue

Health Services From the Cloud

Takeaways

What is the Cloud?

SaaS

PaaS

IaaS

Private Cloud

Public Cloud

Hybrid Cloud
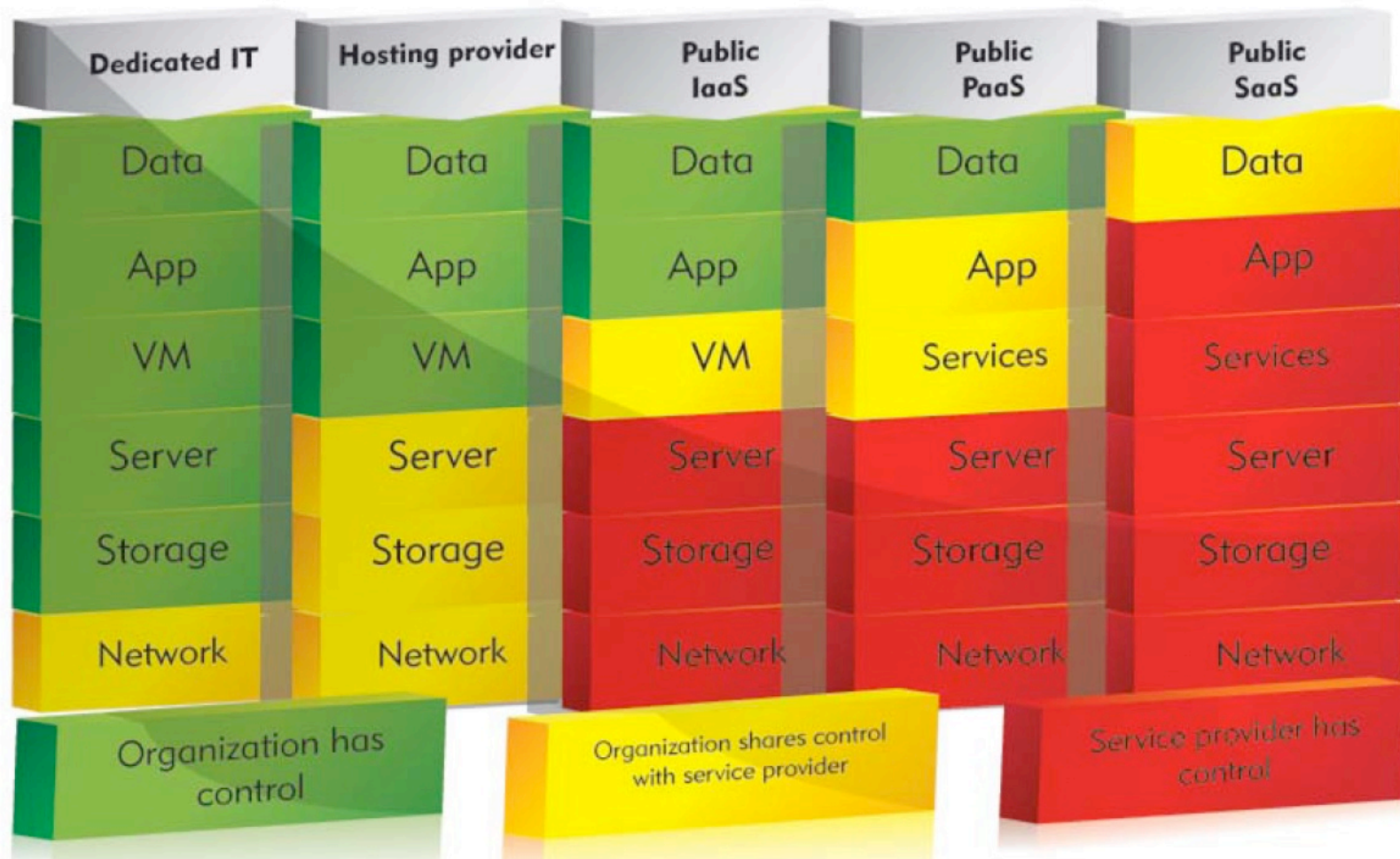
Identity as Security Glue – Points of View

1. **Extend Enterprise Security to Cloud Services [Enterprise <u>to Cloud </u>Providers]**

   • Examples…User provisioning to Cloud, Federated SSO to Cloud, Log collection pulling from Cloud to enterprise

2. **Enable Cloud Providers to better secure their services [<u>For Cloud </u>Providers]**

   • Examples….Controlling the privileged user in the Cloud, Administering the entitlements of all classes of users, Controlling access to Web applications & services in the Cloud, Federating user sessions to other Cloud providers

3. **Enable Cloud Providers to offer Security/IAM services to organizations [Cloud Providers <u>for Enterprise</u>]**

   • Examples….Authentication service from the Cloud, Log management service from the Cloud, DLP service from the Cloud

Identity as Security Glue – Mapping Identity Services to Cloud

Points of View / Identity Services	Enterprise To Cloud Providers	For Cloud Providers	Cloud Providers For Enterprise
Privileged User Management			
Data Leak Protection			
User Provisioning			
Role Management			
User Authentication & Federation			
Web Access Management/SSO			
Web Services Security			
Log Management			

Identity as Security Glue – Areas of Relevance

Points of View ⟍ Identity Services	Enterprise To Cloud Providers	For Cloud Providers	Cloud Providers For Enterprise
Privileged User Management	★	★	★
Data Leak Protection	★	★	★
User Provisioning	★	★	★
Role Management	★	★	★
User Authentication & Federation	★	★	★
Web Access Management/SSO	★	★	★
Web Services Security	★	★	★
Log Management	★	★	★

Identity as Security Glue – Most Immediate Need

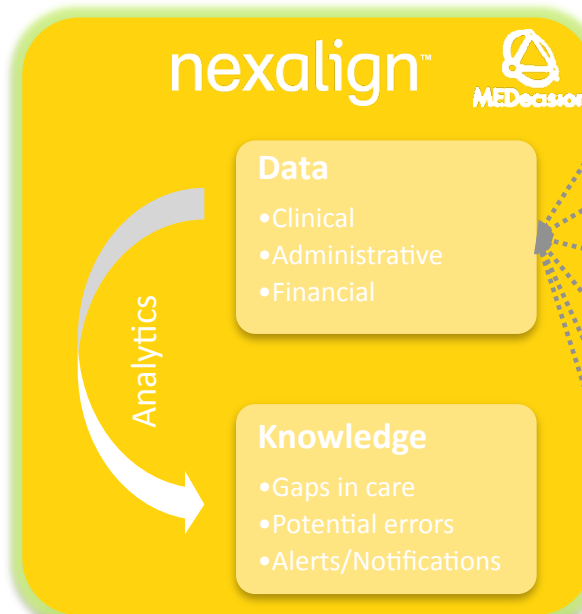| Points of View / Identity Services	Enterprise To Cloud Providers	For Cloud Providers	Cloud Providers For Enterprise
Privileged User Management		★	
Data Leak Protection	★	★	★
User Provisioning	★	★	
Role Management			
User Authentication & Federation	★	★	★
Web Access Management/SSO		★	
Web Services Security			
Log Management		★	★

Health Services From the Cloud

Secure access to Healthcare data

Applications

- Web portal
- Electronic medical record
- Practice management system
- Picture archiving & comm systems
- Personal health record
- Care management system
- Utilization management system
- Disease management system

nexalign™ MEDecision

Analytics

Data
- Clinical
- Administrative
- Financial

Knowledge
- Gaps in care
- Potential errors
- Alerts/Notifications

Provider
Demographics
Lab results
Imaging results
Medical summaries
Scanned documents

Payer
Demographics
Claims

Ancillary
Demographics
Lab results
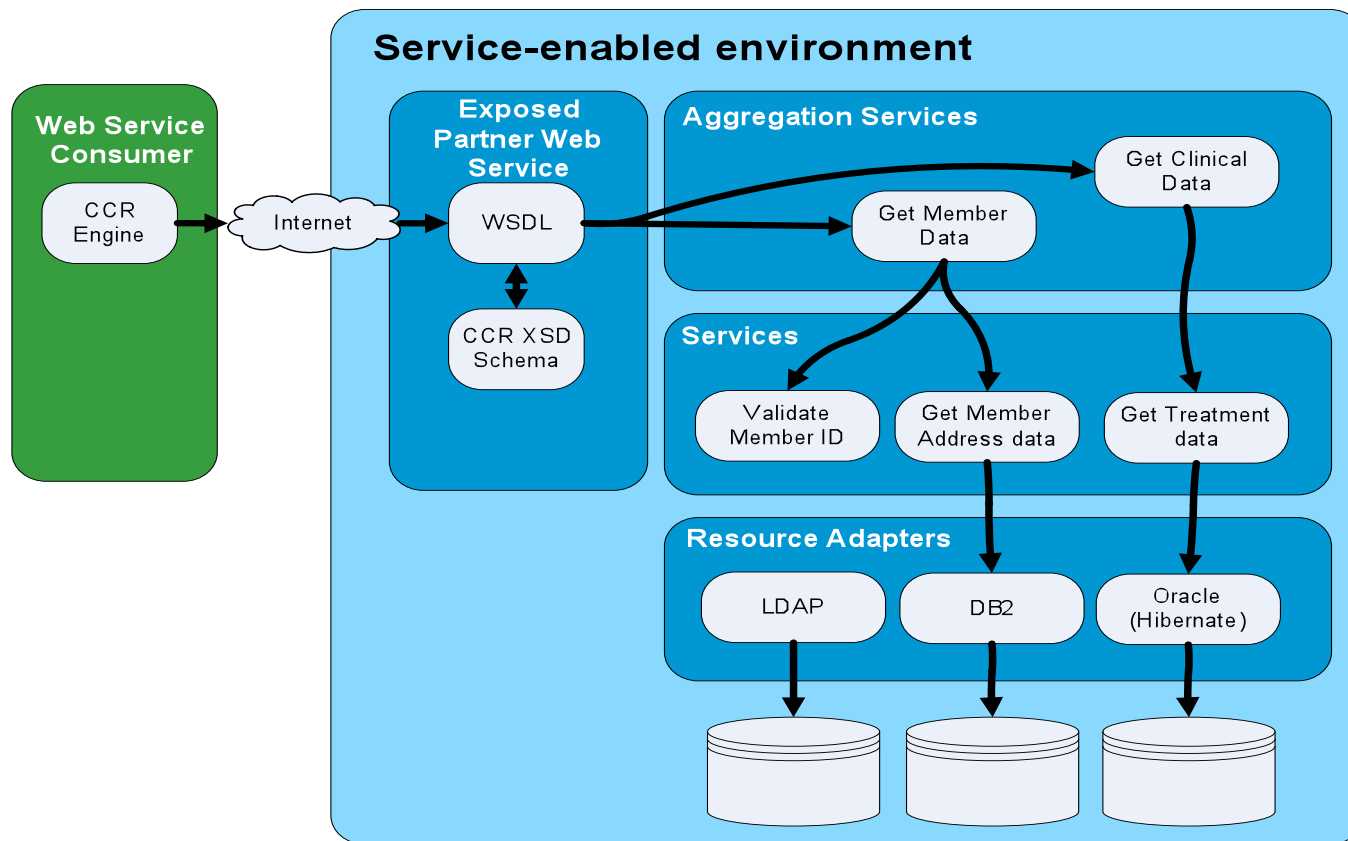Imaging results

PHR
Demographics
HRAs

PBM / Pharmacy
Demographics
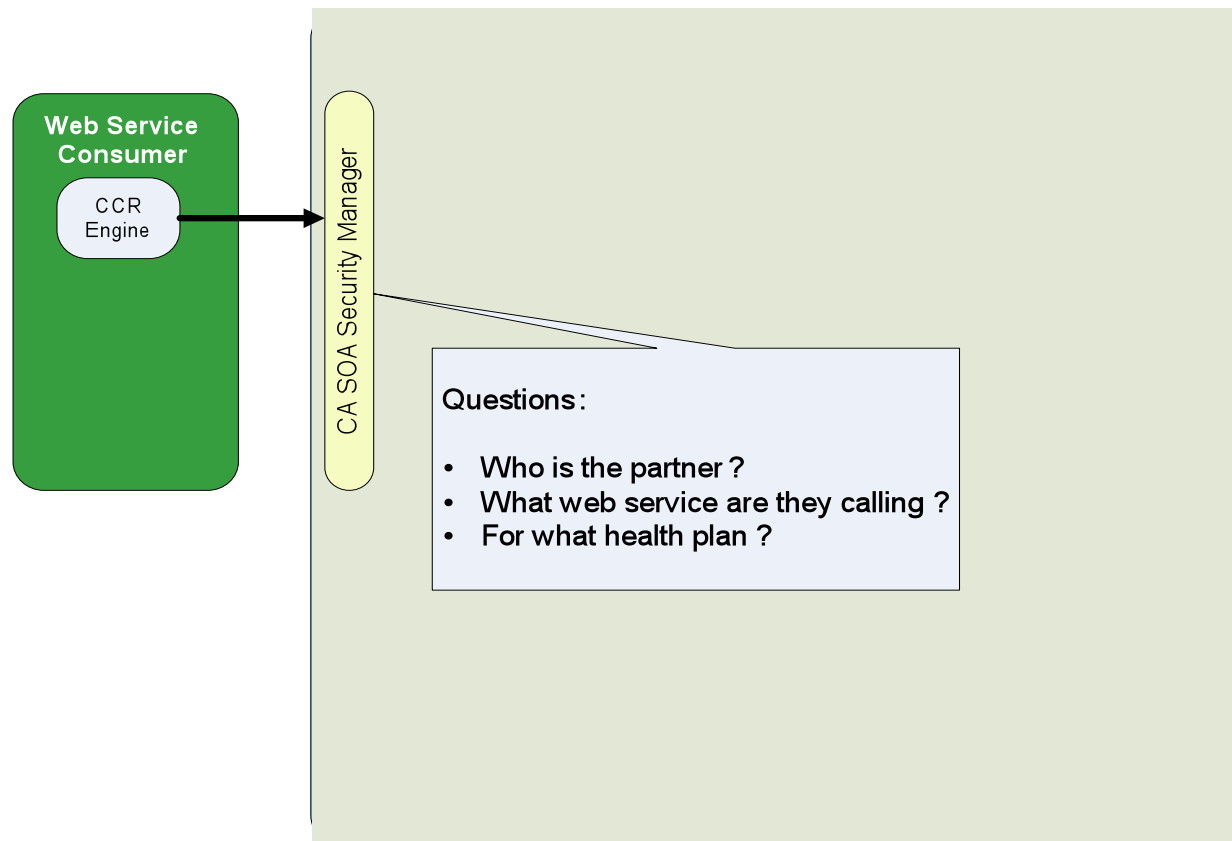Medication history

Public Health
Demographics
Immunizations

ca. MEDecision®

RSA CONFERENCE 2010

Creating a service-enabled environment

Service-enabled environment

Web Service Consumer
- CCR Engine

Internet

Exposed Partner Web Service
- WSDL
- CCR XSD Schema

Aggregation Services
- Get Member Data
- Get Clinical Data

Services
- Validate Member ID
- Get Member Address data
- Get Treatment data

Resource Adapters
- LDAP
- DB2
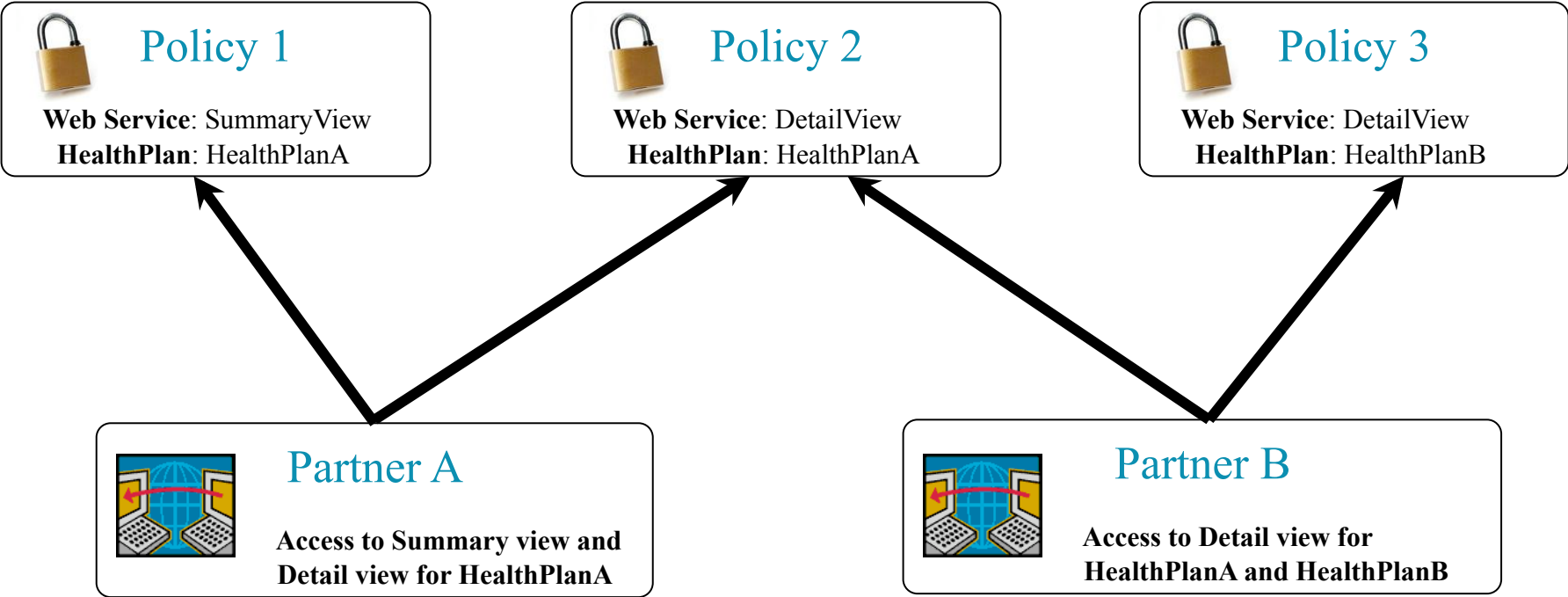- Oracle (Hibernate)

- Certificates on a Web server were a good start but…
  - It does not easily allow for role-base access
- Implementation of role-based access to web services allows for:
  - Secure Web services using partner certificates
  - Identify partners based on the digital signature
  - Apply additional role-based access rules
  - Encrypt/Decrypt the message
- We chose to use WS-Security because of the partners we're dealing with
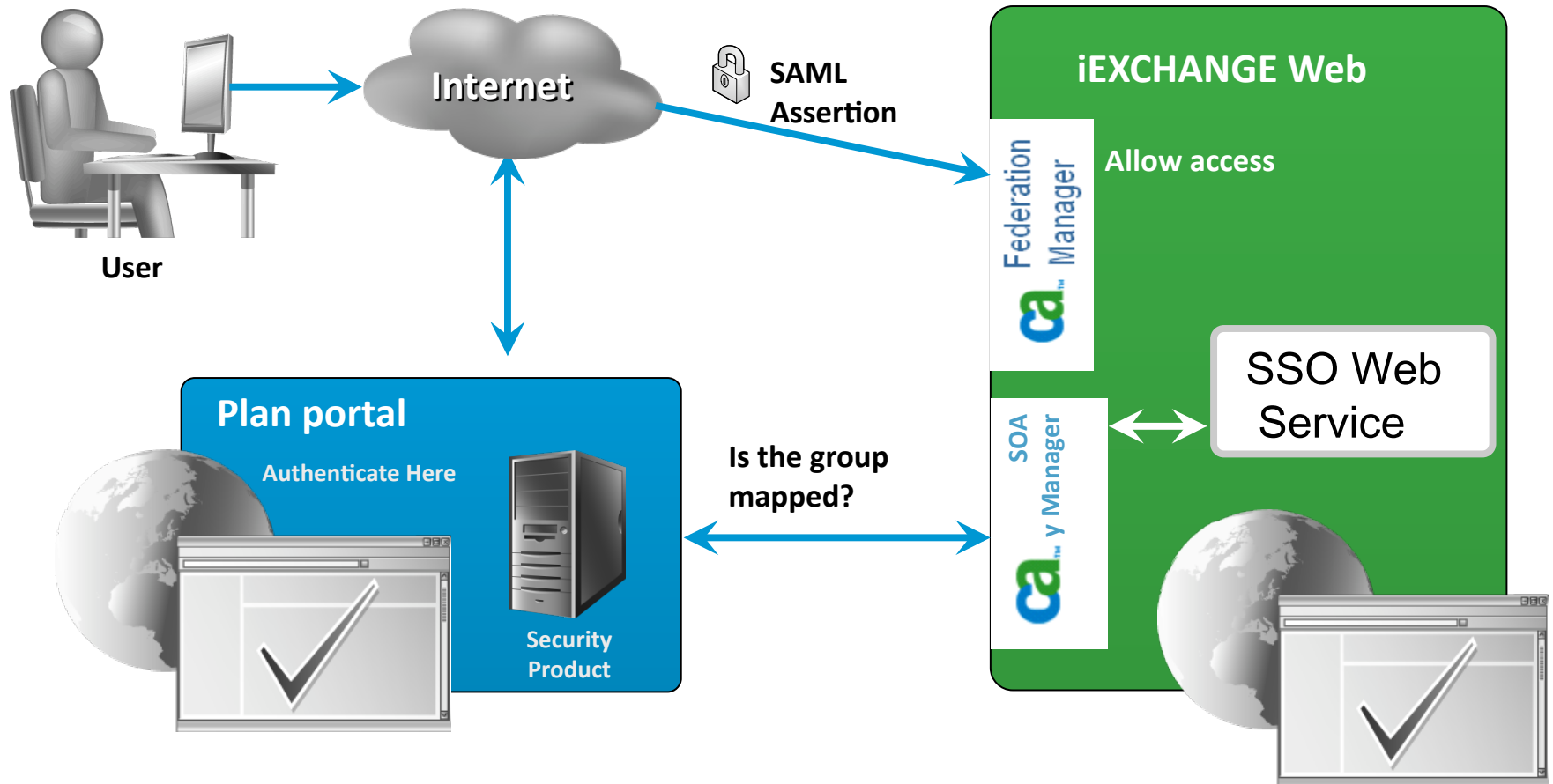- Change to other authentication schemes (like SAML) is simply a change in configuration

Applying authorization rules

Web Service Consumer

CCR Engine

CA SOA Security Manager

Questions:

- Who is the partner ?
- What web service are they calling ?
- For what health plan ?

Applying role-based access

Policy 1
Web Service: SummaryView
HealthPlan: HealthPlanA

Policy 2
Web Service: DetailView
HealthPlan: HealthPlanA

Policy 3
Web Service: DetailView
HealthPlan: HealthPlanB

Partner A
Access to Summary view and Detail view for HealthPlanA

Partner B
Access to Detail view for HealthPlanA and HealthPlanB

Combining SAML and web services

Takeaways

- Identity is key security glue for the cloud

- Federation standards are central
  - SAML, WS-Security, OpenID, IMI, XACML, SPML….
  - Fortunately the security industry foresaw the cloud
  - But we must recognize new players need to be educated

- Challenges remain the same
  - Privacy, liability, contracts, economics, interoperability…

- Harness the "cloud hype" to continue to progress our identity mission