
DMTF®
distributed management task force, inc.
US Government Driven Cloud Computing Standards
A panel discussion including:
DMTF, Cloud Security Alliance, NIST and SNIA
www.dmtf.org

Lee Badger: Computer Scientist, Computer Security Division, National Institute of Standards & Technology (NIST)

Mark Johnson: Co-Chair, Cloud Management Working Group, Distributed Management Task Force (DMTF), IBM

Mark Carlson: Vice chair of the Cloud Storage Initiative, Storage Industry Networking Industry Association (SNIA), Oracle Corporation

Becky Swain: CIPP/IT, CISSP, CISA – CCM Co-Founder / Chair, Cloud Security Alliance (CSA) Silicon Valley Chapter Board Member, Cisco Systems, Inc.

Winston Bumpus: Co-Chair, Cloud Management Working Group, President, Distributed Management Task Force (DMTF), VMware, Inc.

Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)

Lee Badger
Dawn Leaf

SAJACC Team:

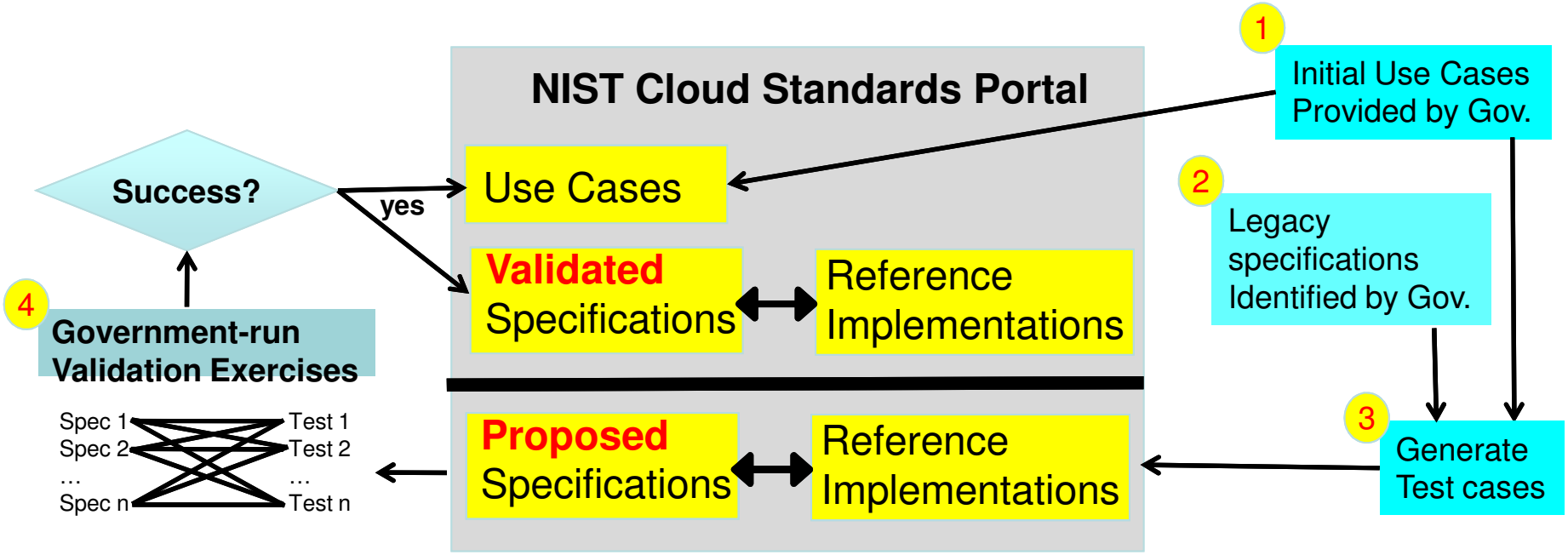
Tim Grance
Tom Karygiannis
Robert Bohn
Jin Tong
Ramaswamy Chandramouli
Robert Patt-Corner
Jeff Voas

March 2, 2011

Important Cloud Computing Requirements

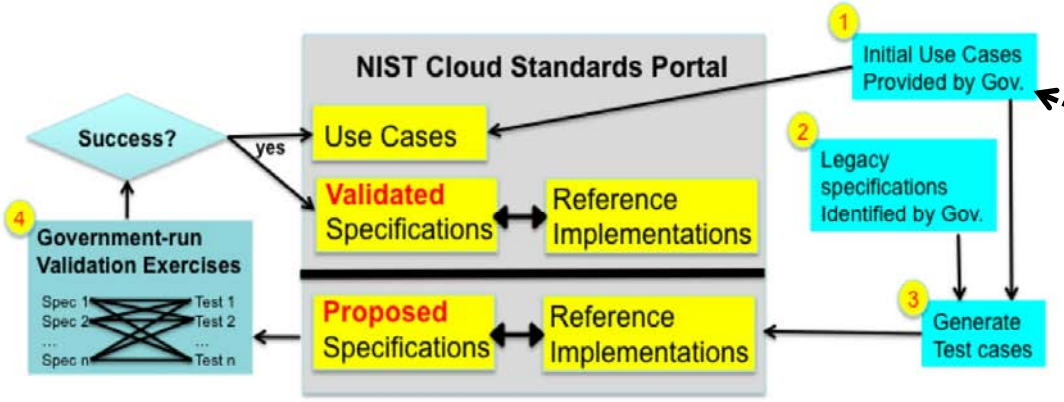
- **interoperability:** clouds work together
- **portability:** workloads can move around
- **security:** customer workloads protected (to the extent possible)

NIST SAJACC Process



- **specifications, use cases:** provide insight on how clouds can work
- **reference implementations**: enable validation exercises
- **continuously growing portal**: new content added over time
- **publically available**: anyone can access

Current Status



✓ 24 use cases described

http://www.nist.gov/itl/cloud/use-cases.cfm

	S3	CDMI
3.4 Copy data objects into a cloud	✓	✓
3.5 Copy data objects out of a cloud	✓	✓
3.6 Erase data objects in a cloud	✓	more on the way...
4.1 Copy data objects between cloud providers (planned by March 15)		

5 use case drivers using two different interfaces

(plan as of Feb. 23)

download at: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/SAJACC

A Use Case

Use Case: a description of how groups of users and their resources may interact with one or more systems to achieve specific goals.

Actors: the active entities
Goals: what the use case tries to achieve
Assumptions: conditions assumed true

Success Scenario 1 (name**, IaaS, PaaS, SaaS**) A step-by-step narrative of what happens to achieve the use case goal
Failure Conditions: what might go wrong
Failure Handling: how to deal with known failures

Success Scenario 2 (name, IaaS, PaaS, SaaS) Another narrative
Failure Conditions: what might go wrong
Failure Handling: how to deal with known failures

...

Credit: any source that inspired us

We are using the approach of A. Cockburn, slightly customized, "Writing Effective Use Cases".

Actors

currently, no taxonomy for actors

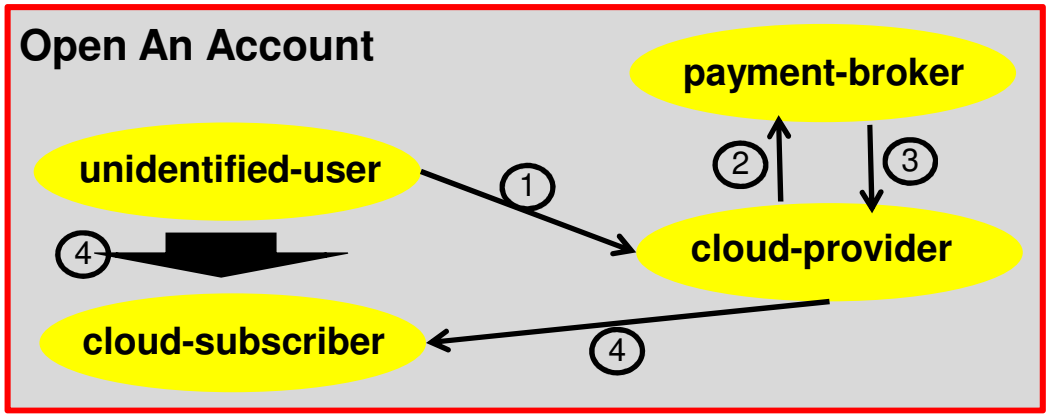
unidentified-user An entity in the Internet (human or script) that interacts with a cloud over the network and that has not been authenticated.

cloud-subscriber A person or organization that has been authenticated to a cloud and maintains a business relationship with a cloud.

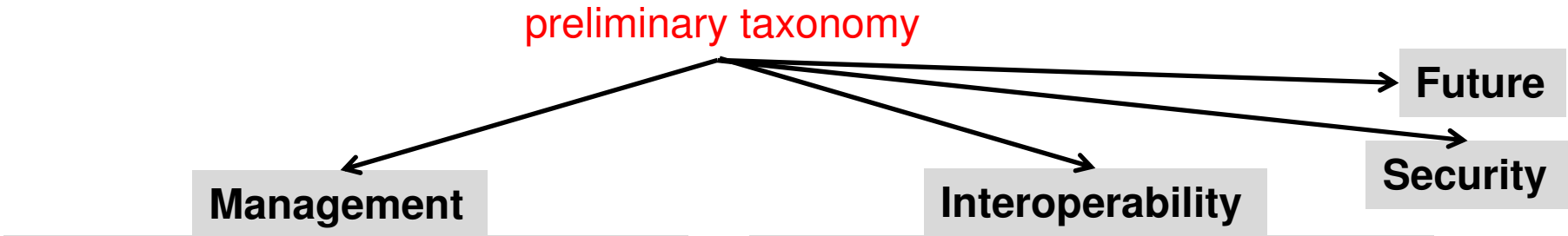
payment-broker A financial institution that can charge a **cloud-subscriber** for cloud services, either by checking or credit card.

cloud-provider An organization providing network services and charging **cloud-subscribers.** A (public) **cloud-provider** provides services over the Internet.

a use case



Current Use Cases



3.1 Open An Account

3.2 Close An Account

3.3 Terminate An Account

3.4 Copy Data Objects Into A Cloud

3.5 Copy Data Objects Out of a Cloud

3.6 Erase Data Objects In a Cloud

3.7 VM Control: Allocate VM Instance

3.8 VM Control: Manage Virtual Machine Instance State

3.9 Query Cloud-Provider Capabilities and Capacities

4.1 Copy Data Objects between Cloud-Providers

4.2 Dynamic Operation Dispatch to IaaS Clouds

4.3 Cloud Burst From Data Center to Cloud

4.4 Migrate a Queuing-Based Application

4.5 Migrate (fully-stopped) VMs from one cloud-provider to another

Current Use Cases

preliminary taxonomy

Management

Interoperability

Security

- **5.1 Identity Management - User Account Provisioning**
- **5.2 Identity Management - User Authentication in the Cloud**
- **5.3 Identity Management - Data Access Authorization Policy Management in the Cloud**
- **5.4 Identity Management - User Credential Synchronization Between Enterprises and the Cloud**
- **5.5 eDiscovery**
- **5.6 Security Monitoring**
- **5.7 Sharing of access to data in a cloud**

Future

- **6.1 Cloud Management Broker**
- **6.2 Transfer of ownership of data within a cloud**
- **6.3 Fault-Tolerant Cloud Group**

A (simple) use case

Open An Account

Actors: **unidentified-user**, **cloud-subscriber**, **payment-broker**, **cloud-provider**.

Goals: **Cloud-provider** opens a new account for an **unidentified-user** who then becomes a **cloud-subscriber**.

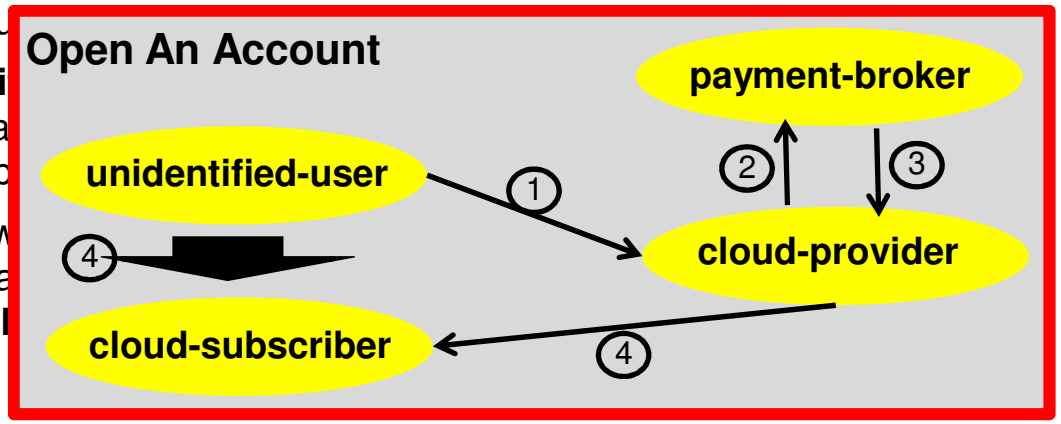
Assumptions: A **cloud-provider**'s account creation web page describes the service offered and the payment mechanisms. An **unidentified-user** can access the **cloud-provider**'s account creation web page.

Success Scenario: **(open, IaaS, PaaS, SaaS):** An **unidentified-user** accesses a **cloud-provider**'s account creation web page. The **unidentified-user** provides: (1) a unique name for the new account; (2) information about the **unidentified-user**'s financial; and (3) when the **unidentified-user** wants the account opened. The **cloud-provider** verifies the **unidentified-user**'s financial information; if the information is deemed valid by **cloud-provider**, the **unidentified-user** becomes a **cloud-subscriber** and the **cloud-provider** returns authentication information that the **cloud-subscriber** can su

Failure Conditions: (1) the **unidenti** financial information is not va **subscriber** the account is op

Failure Handling:For (1) and (2), new below on failure handling rela **subscriber**. **Requirements**

Credit: TBD



A (simple) use case

Open An Account

Actors: **unidentified-user**, **cloud-subscriber**, **payment-broker**, **cloud-provider**.

Goals: **Cloud-provider** opens a new account for an **unidentified-user** who then becomes a **cloud-subscriber**.

Assumptions: A **cloud-provider**'s account creation web page describes the service offered and the payment mechanisms. An **unidentified-user** can access the **cloud-provider**'s account creation web page.

Success Scenario: **(open, IaaS, PaaS, SaaS):** An **unidentified-user** accesses a **cloud-provider**'s account creation web page. The **unidentified-user** provides: (1) a unique name for the new account; (2) information about the **unidentified-user**'s financial; and (3) when the **unidentified-user** wants the account opened. The **cloud-provider** verifies the **unidentified-user**'s financial information; if the information is deemed valid by **cloud-provider**, the **unidentified-user** becomes a **cloud-subscriber** and the **cloud-provider** returns authentication information that the **cloud-subscriber** can subsequently use to access the service.

Failure Conditions: (1) the **unidentified-user** does not provide a suitable name; (2) the financial information is not valid; (3) **cloud-provider** fails to notify the **cloud-subscriber** the account is open.

Failure Handling:For (1) and (2), new account is not created; For (3) See Use Case 3.2 below on failure handling related to notifications from **cloud-provider** to **cloud-subscriber**. **Requirements File:** None.

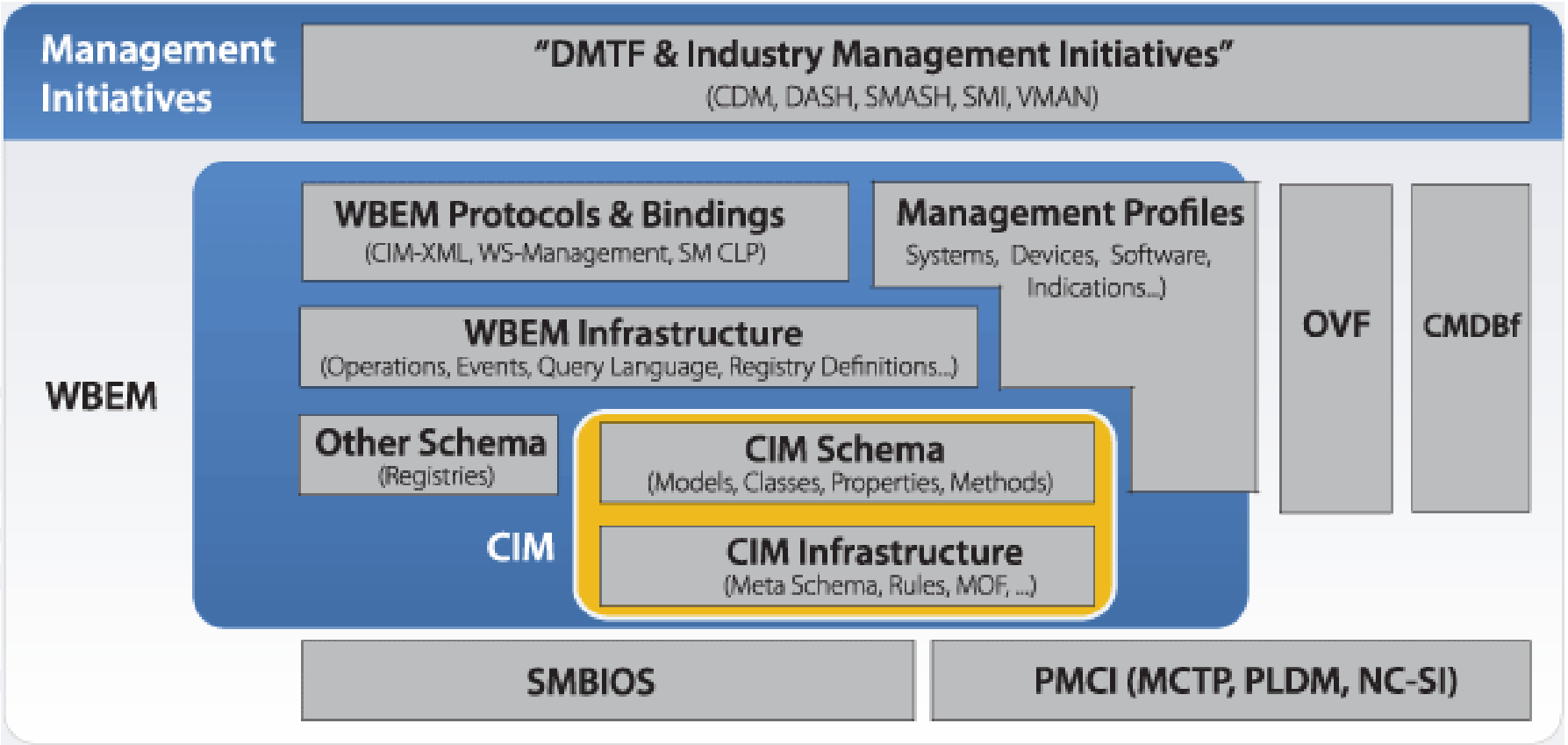
Credit: TBD

Interoperability Standards for Managing Clouds

Mark Johnson
Co-Chair, DMTF Cloud Management Working Group

DMTF Technologies

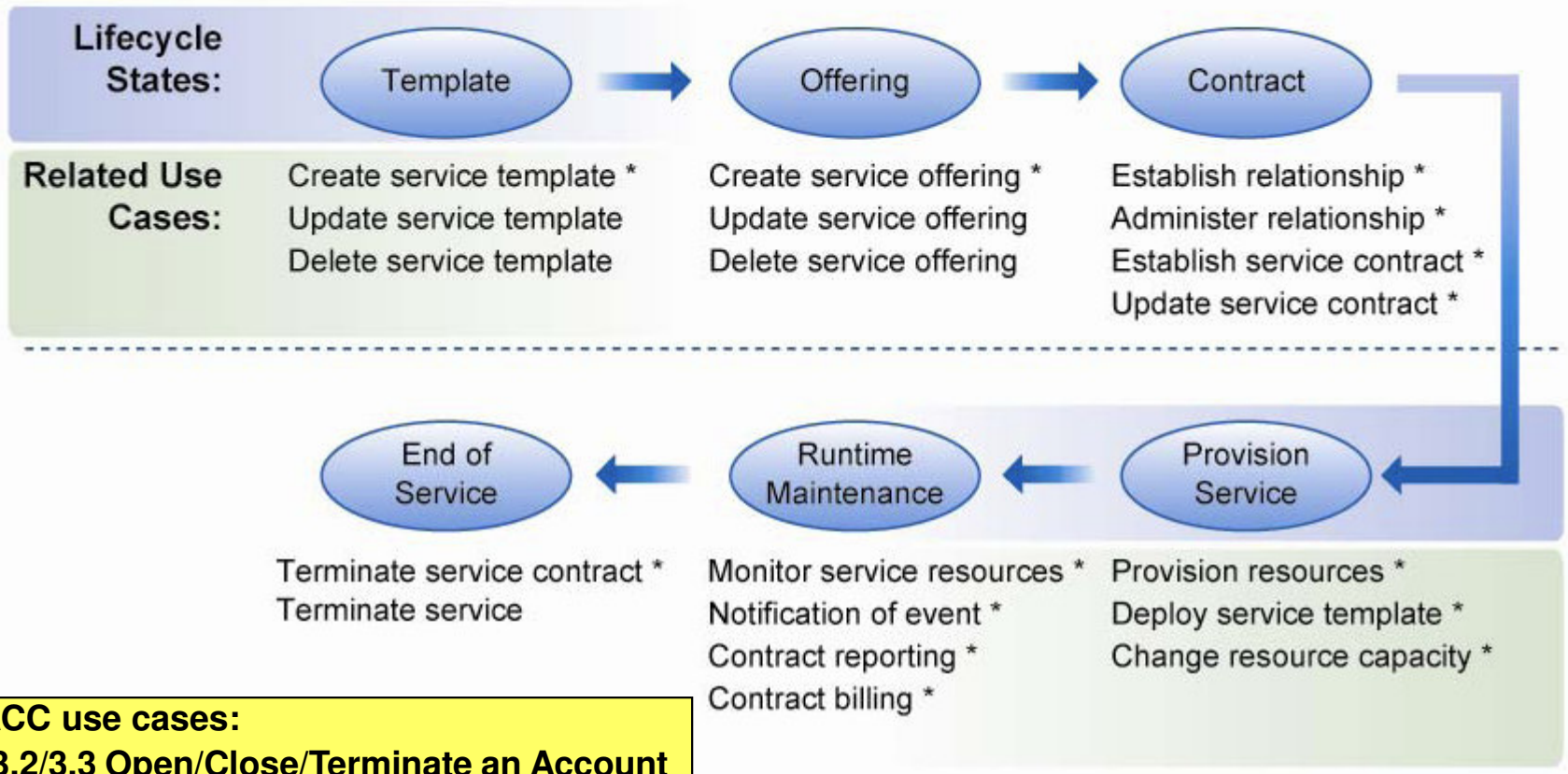
DMTF standards provide well-defined, interoperable interfaces that build upon each other



Cloud Management

- Cloud Incubator (2009-2010) published informational specifications
  - "Interoperable Clouds" white paper
  - Architecture and interfaces
  - Use cases and resource interaction model
- Cloud Management Working Group replaced incubator July 2010
  - Writing formal specifications
  - Focus on IaaS
  - Leverage other standards, e.g., OVF (Open Virtualization Format)
  - 34 actively involved companies + 10 academic or alliance members
- Virtualization and Cloud Management Forum
  - Interoperability and compliance testing
  - Cloud, OVF, and virtualization management

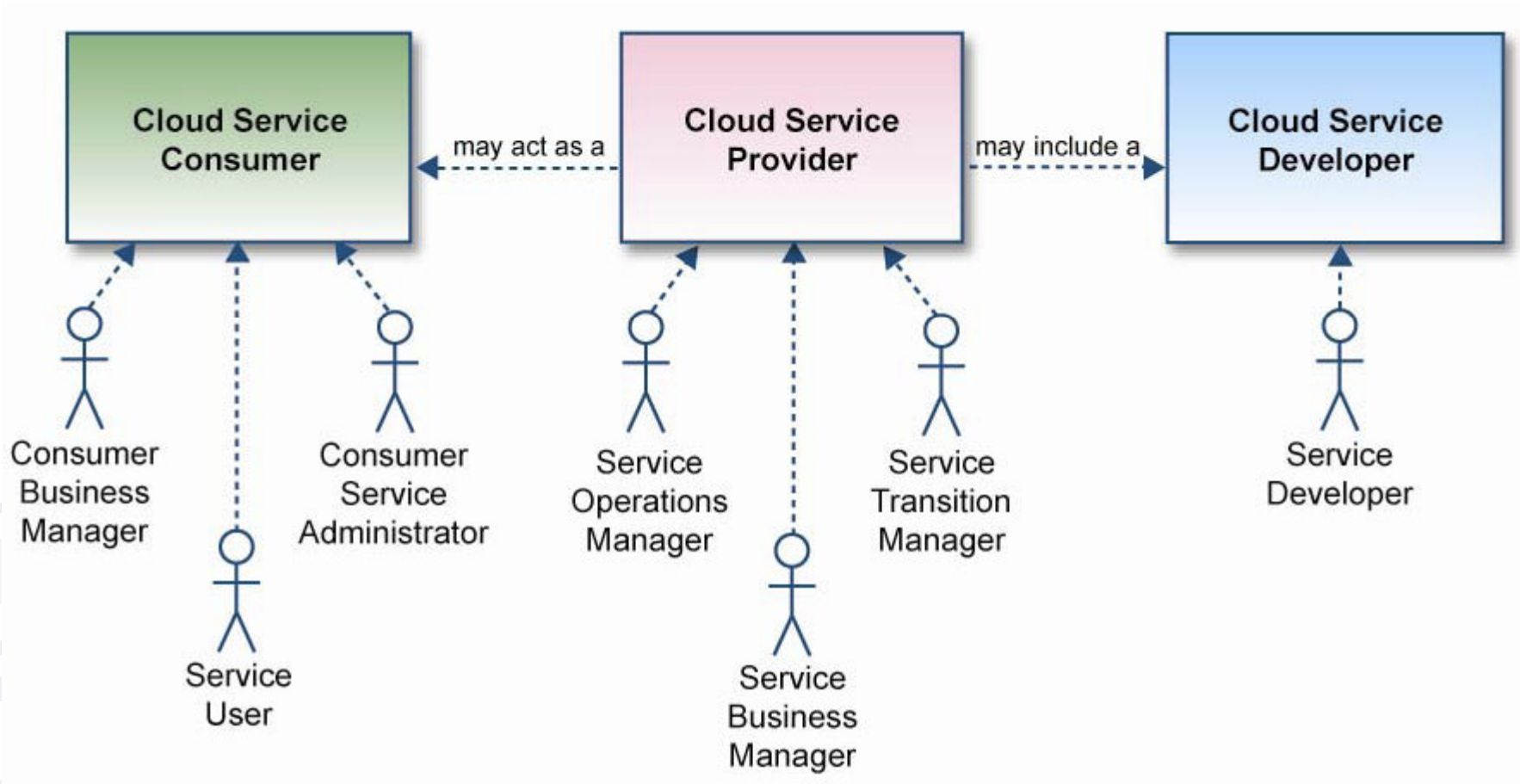
Cloud Service Life Cycle & Use Cases



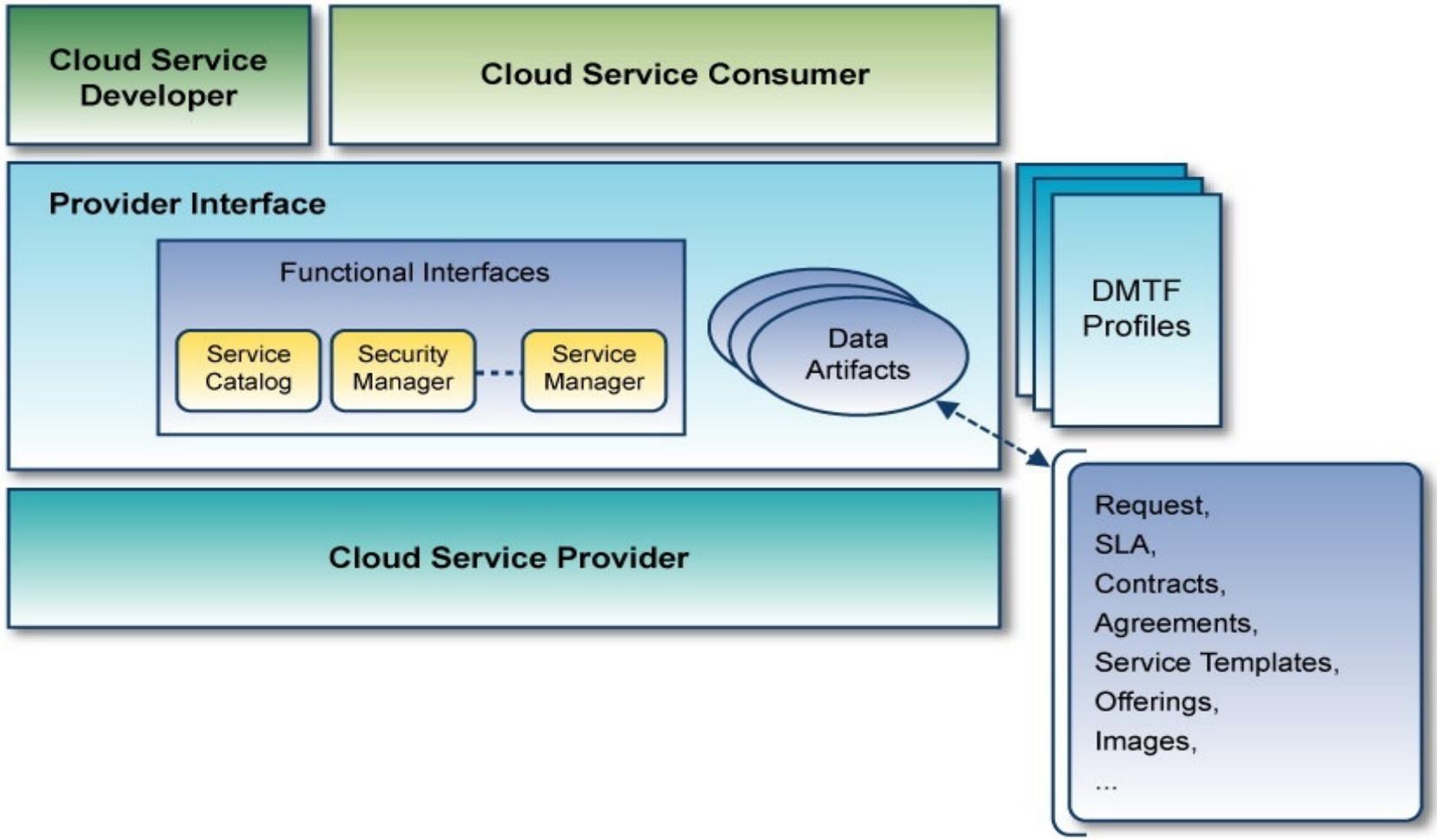
SAJACC use cases:

- **3.1/3.2/3.3 Open/Close/Terminate an Account**
- **3.7 VM Control: Allocate VM Instance**
- **3.8 VM Control: Manage VM Instance State**
- **3.9 Query Cloud Provider Capabilities**

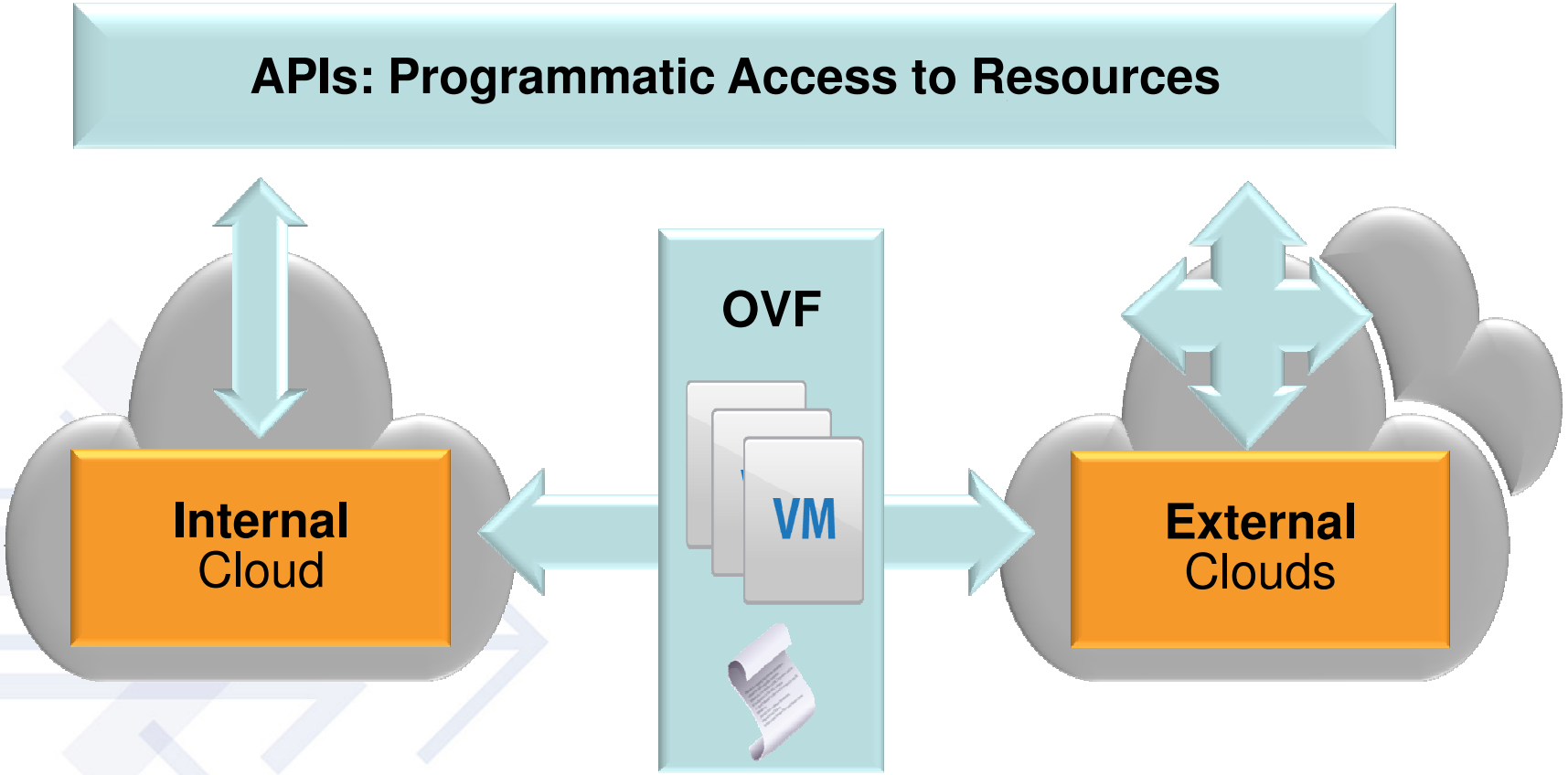
Use Case Actors Taxonomy



Cloud Management Architecture

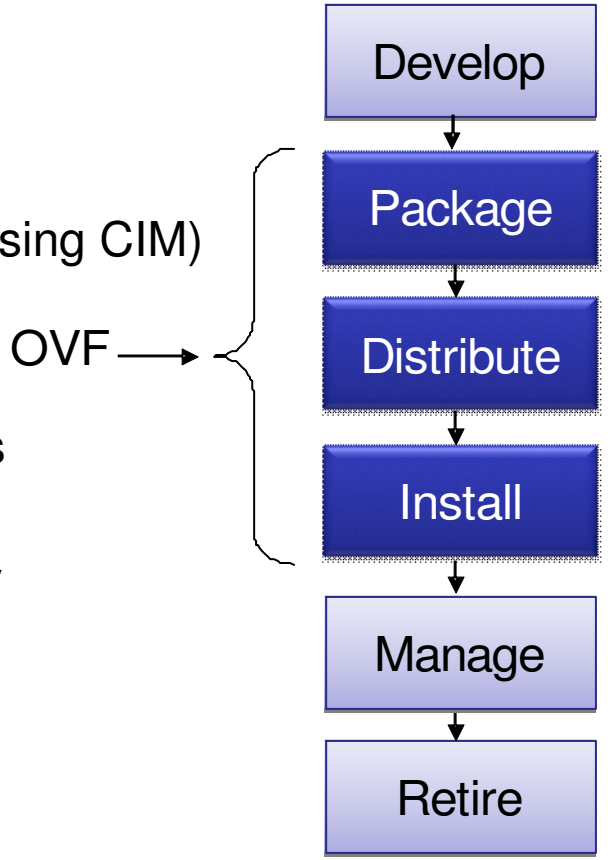


OVF and Clouds



OVF – Open Virtualization Format

- Summary
  - Packaging format for virtual appliances
  - Metadata describing environment requirements (using CIM)
  - Activation logic and artifacts
- Benefits
  - Deliver software through portable virtual machines
  - Streamlined installations
  - Virtualization platform independence and flexibility
  - Single-system and multiple-system services
- History
  - OVF 1.0 & 1.1: published 2009 & 2010
  - OVF 2.0: under development



Addressing US Government interoperability requirements

The SNIA Cloud Data Management Interface Standard

BrightTalk Session March, 2011

SNIA
Cloud Storage

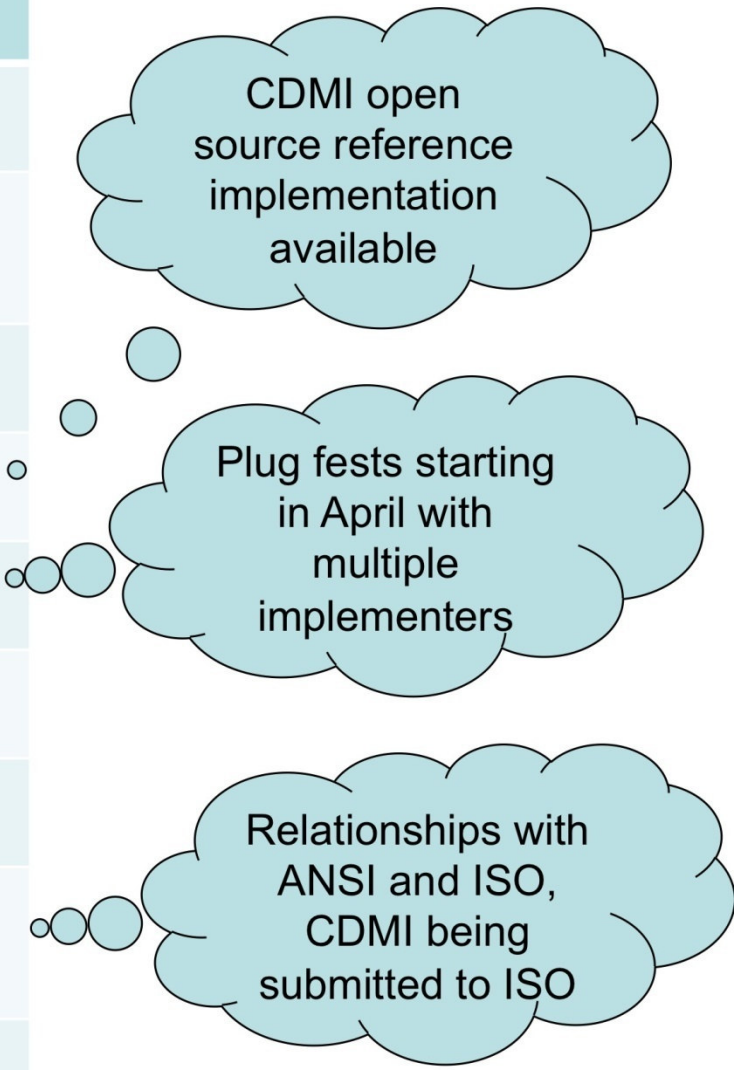
SNIA Cloud Activities

- Storage Networking Industry Association (SNIA) is a Standards Development Organization (SDO)
  - Published the Cloud Data Management Interface as a SNIA Architecture (April 2010) – also moving to De Jure standardization
- SNIA is also a trade association for the storage industry
  - Promoting the Cloud Storage market overall
  - Promoting the adoption of the CDMI standard
    - Tutorials, Whitepapers, Cloud Events, Magazine Articles, Blogging, Tweeting. etc.
  - Promoting interoperability between implementations
    - Plug-fests, test suites, conformance programs
- SNIA also produces open source software
  - CDMI reference implementation available under BSD license

CDMI is maturing as a standard

Cloud Storage SNIA

Maturity Level*	Description	Recommendation
1.No Standards	Standardization needed	Encourage standards development
2.Under Development	Discussions within standards groups. Open source project launched.	Monitor and provide feedback to standards development
3. Specification Document Published	Initial specification posted for public review	Review specification and plan testing
4.Initial Reference Implementation	Reference implementation available	Evaluate reference implementation
5.Early Third Party Testing	Evaluation in test environments	Pilot Projects should consider use
6.Initial Production Implementations	Successful use in production	Mainstream projects should consider use
7.Many Deployments	Widespread use by many groups	Projects should use the standard as a default
8.Accepted Standard	De facto or de jure acceptance as a standards	Projects should use unless special circumstances require exemption
9.Aging Standards	Newer standards are under development	Projects should explore alternatives

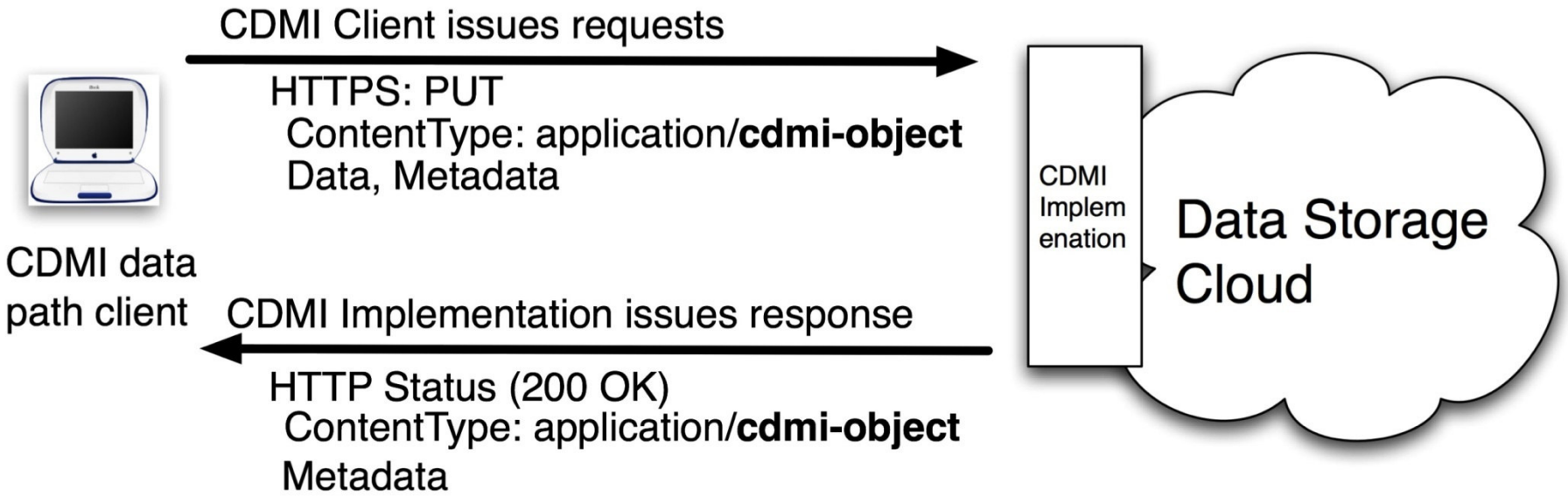


*Source: Draft NIST Cloud Standards Roadmap

CDMI addresses SAJACC Use Cases

- CDMI is an HTTP/RESTful protocol with TLS support for securing the data, metadata and communications
  - CDMI Content Types (MIME) are standardized by IANA (IETF RFC)
  - Message body is encoded in JSON (JavaScript Object Notation)

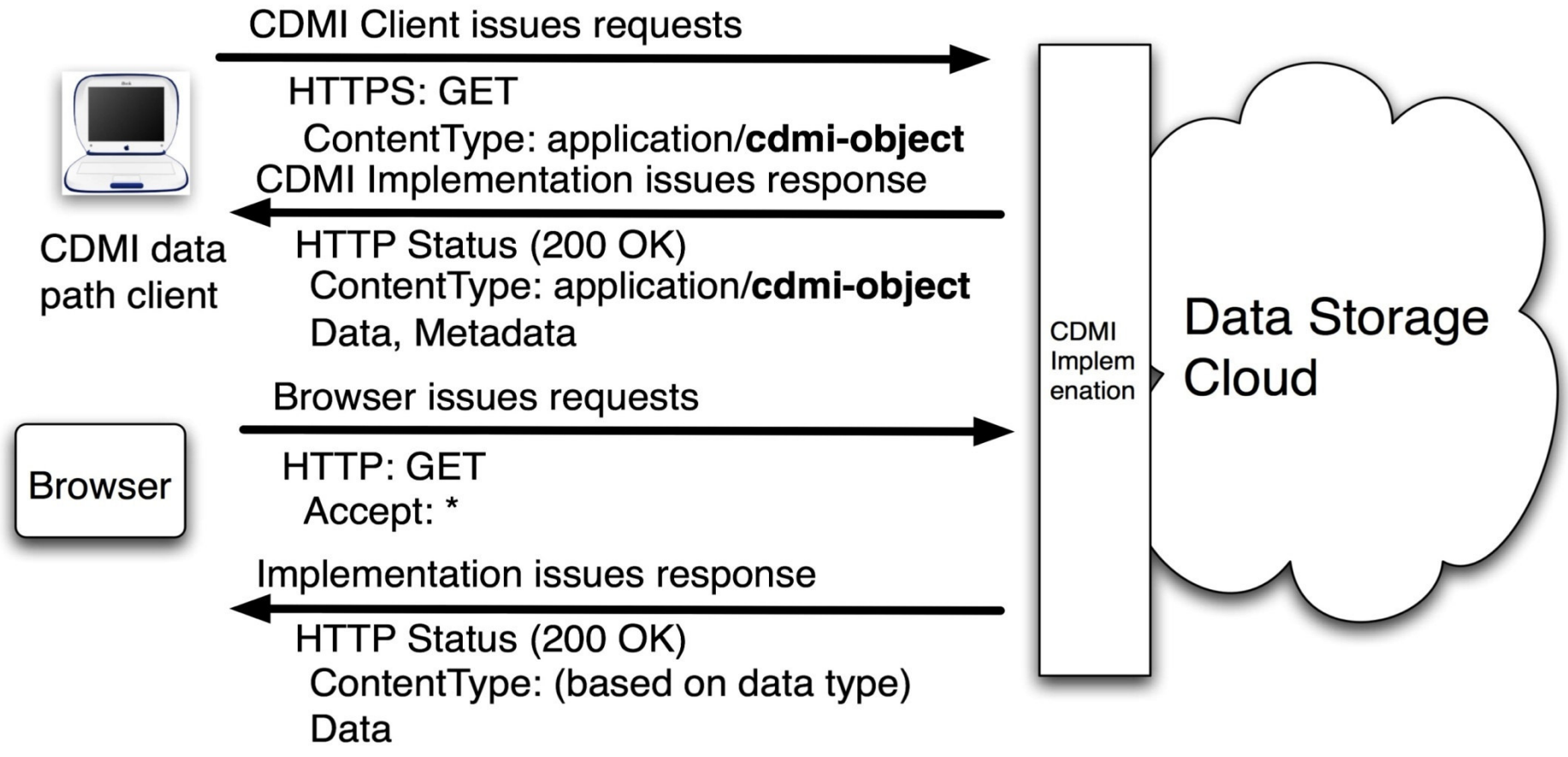
SAJACC Use Case **3.4**: *Copy Data Objects into a Cloud*



CDMI uses existing standards

- CDMI data objects can be accessed by standard browsers and internet tools (subject to owner's access control lists)

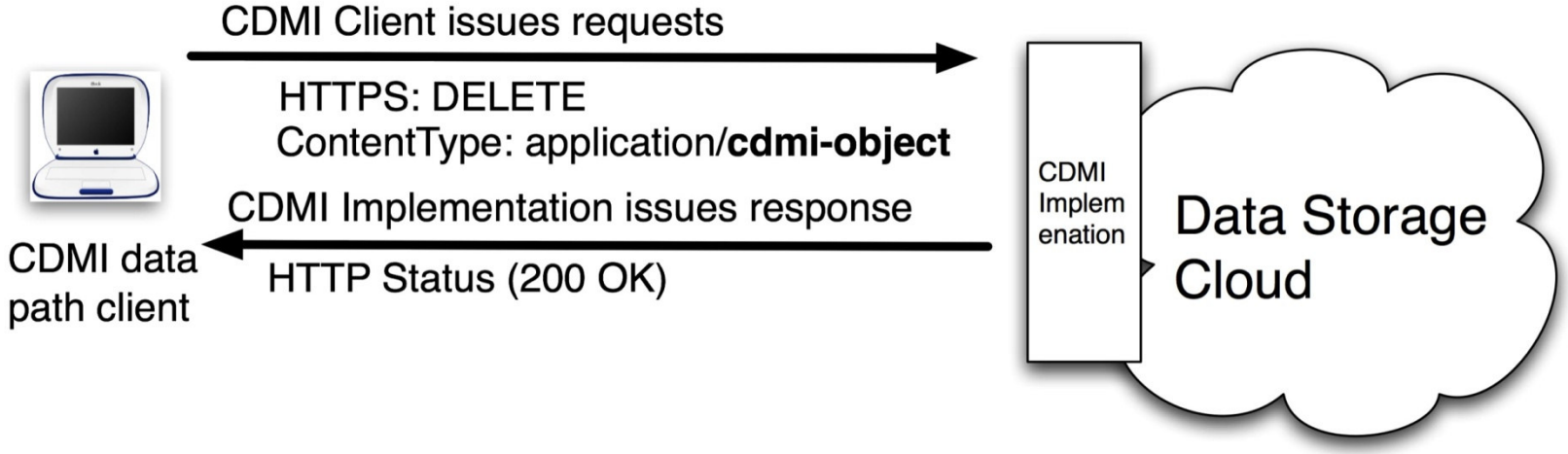
SAJACC Use Case **3.5**: *Copy Data Objects out of a Cloud*



CDMI defines interoperable services

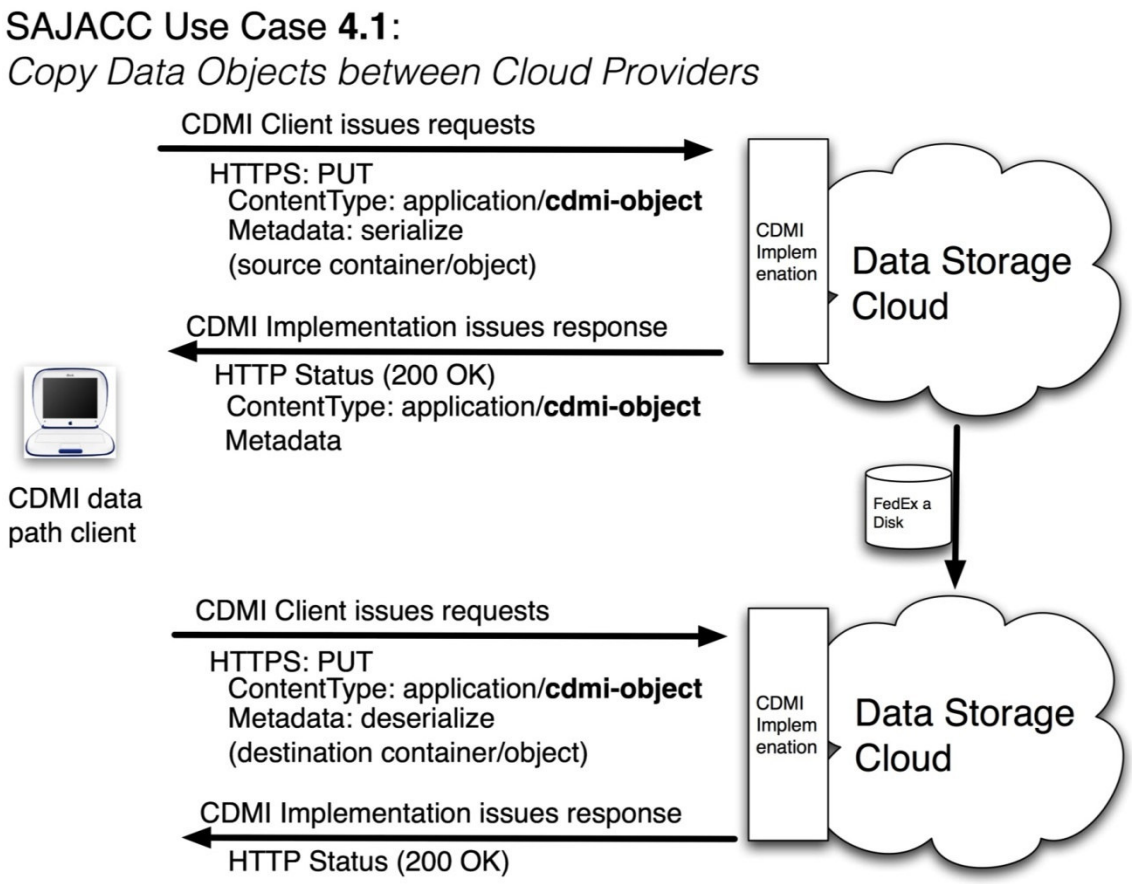
- CDMI data objects may "order" data services from the cloud
  - Secure Erasure, Encryption, Replication, Retention, Backup/ Restore, Tiering, Hashing, Preservation, etc. (extensible)
  - Done through Data System Metadata (key/value) on the Containers or Objects

SAJACC Use Case **3.6**: *Erase Data Objects in a Cloud*



CDMI enables Data Portability

- CDMI standard defines an interoperable format for moving data and associated metadata between cloud providers interoperably
  - And ensuring that the new cloud provides the same services



Cloud Security Alliance: Supporting Standards with GRC Assurance

Becky Swain, Co-founder and Co-chair
CSA Cloud Controls Matrix Working Group

March 2011

About the Cloud Security Alliance

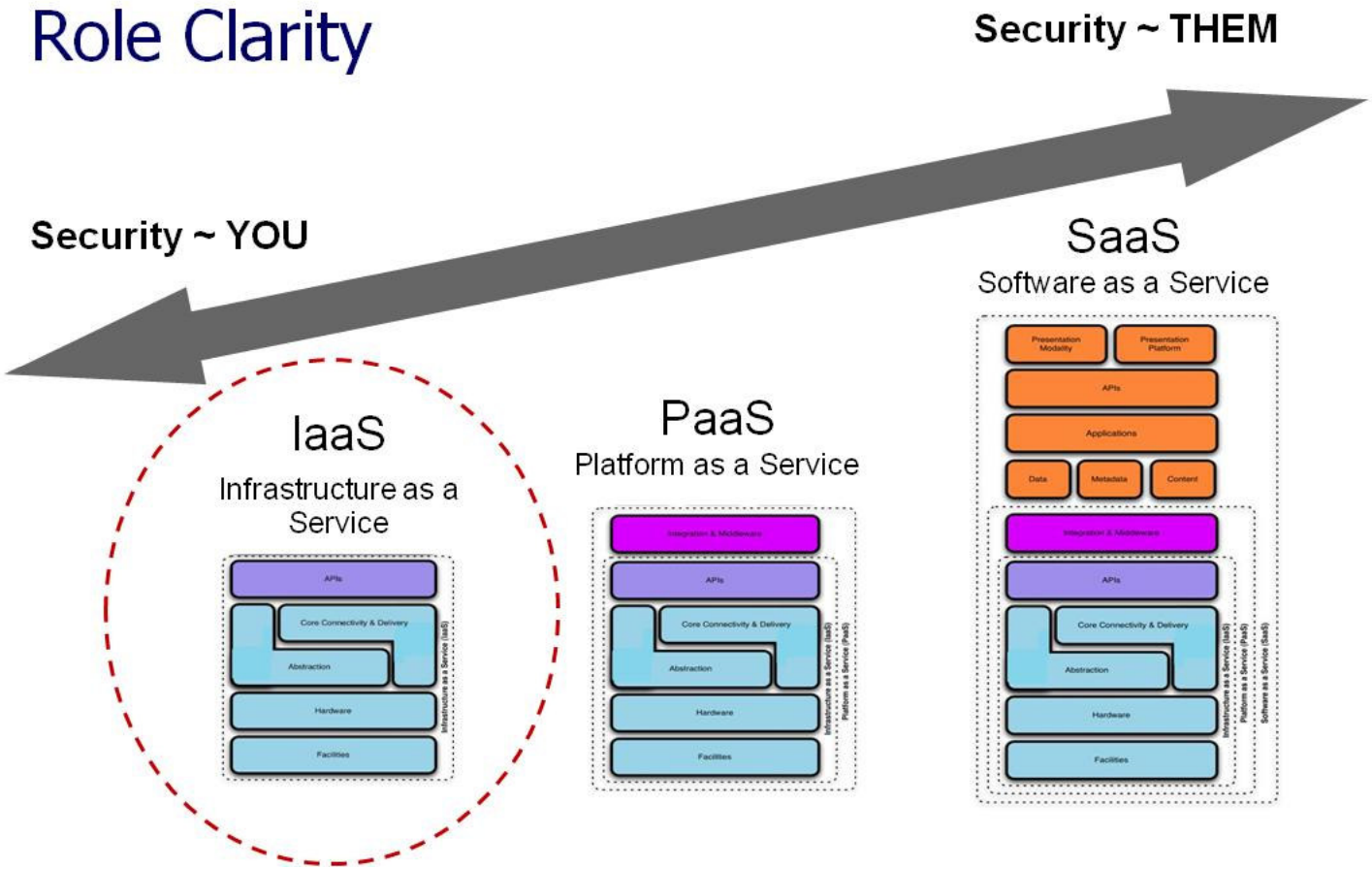
- Global, not-for-profit organization
- Over 17,000 individual members, 100 corporate members
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
  - GRC: Governance, Risk management and Compliance
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Advocacy of prudent public policy

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

cloud security alliance℠

www.cloudsecurityalliance.org

Cloud: New Challenges for GRC



www.cloudsecurityalliance.org

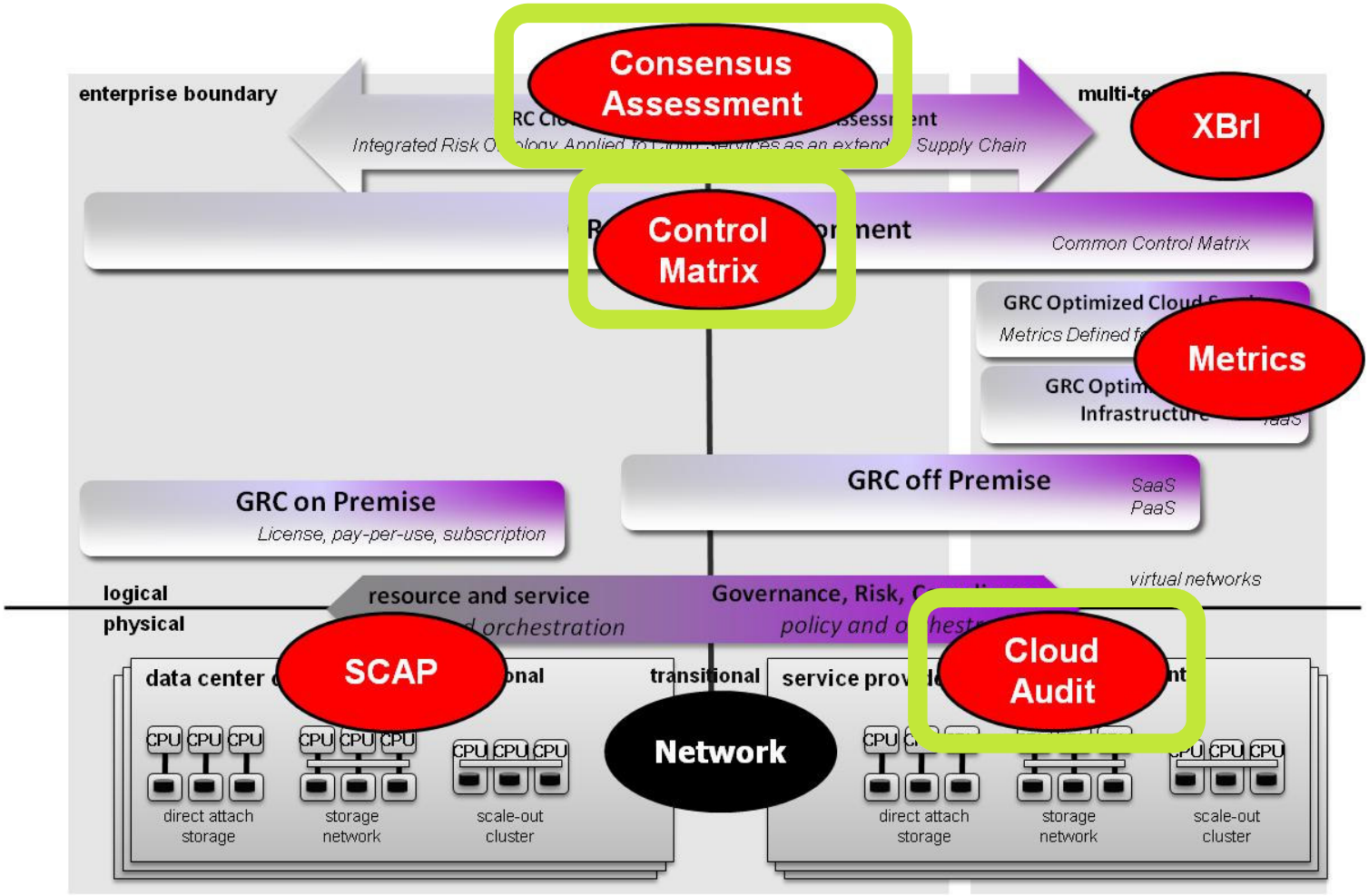
CSA GRC Stack

- Integrated suite of CSA Initiatives to enable GRC assurance of cloud computing
- Designed to support all delivery models and deployment modes as defined by NIST
- Leveraged and aligned with existing standards whenever possible
- "Actor-aware" – tool usage for different roles in cloud use cases
- www.cloudsecurityalliance.org/grcstack

CSA GRC Stack

- Cloud Controls Matrix – Controls framework for all different cloud types with articulated actor responsibilities. Mapped to FISMA, ISO 27001, PCI, COBIT and more.
- Consensus Assessments Initiative – Questionnaire for identification of security controls, appropriate for assessments, RFPs, contracts
- CloudAudit – specification for automatic assertion of controls, enabling continuous GRC & audit scalability in cloud environments

CSA GRC Stack
Bringing it all together…



SAJACC and CSA

- CSA tools can highlight critical control requirements in SAJACC use cases and reference implementations
- Actor responsibilities for GRC assurance can be identified
- Instrumentation within provider infrastructure for proactive, repeatable and continuous assurance
- Some minor work to harmonize nomenclature needed

Questions?

www.nist.gov/itl/cloud/

www.dmtf.org/cloud

www.snia.org/cloud

www.cloudsecurityalliance.org

www.cloud-standards.org