Secure Identity in Cloud Computing

Michelle Carter
The Aerospace Corporation

March 20, 2013

Agenda

- What is Cloud Computing?
- Defining Identity and Access Management (IAM)
  - *Federated Identity*
    - Open Standards
    - Technologies
    - Trust Agreements
  - *Centralized Authentication and Authorization*
  - *Identity As A Service (IDAAS)*
- Commercial IAM Solutions
- Federated Identify Reference Architecture

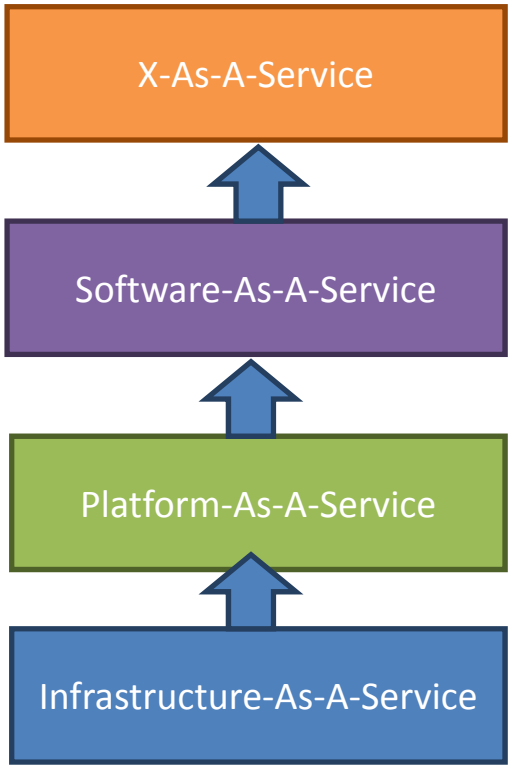
michelle.carter@aero.org
ETG/CSD

What is Cloud Computing?

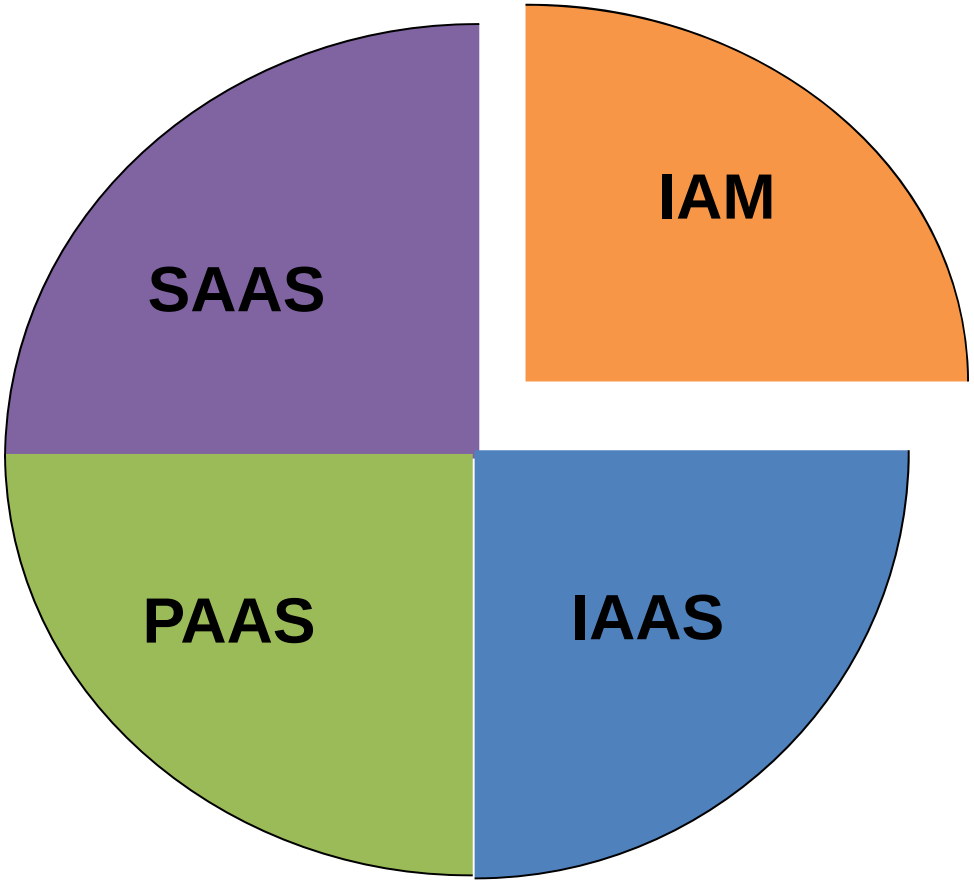
- Cloud computing is the use of computing resources (hardware and software) to deliver a service over the internet
- At its core, cloud technology virtualizes network and computing resources to manage resources and services
- The basis of cloud computing technology is realized by using these fundamental computing services:
  - *Infrastructure as a Service (IAAS)*
  - *Platform as a Service (PAAS)*
  - *Software as a Service (SAAS)*

What is Cloud Computing? (cont.)

- ***IAAS*** provides the foundation for cloud computing services with the implementation of a virtualized platform for managing the interfaces between the hardware and the virtual machine environment
  - *Examples: Amazon (EC2), Windows Azure Virtual Machines*
- ***PAAS*** provides a computing platform that essentially operates as "middleware" software
  - *Examples: RackForce Force.com, Windows Azure Cloud Services, and Google App Engine*
- ***SAAS*** provides cloud users access to software and its functions installed in a cloud environment remotely via a web browser, which allows user flexibility to run multiple tasks and improve support and maintenance of applications
  - *Examples: Google's web-based email and office suite (word processor, spreadsheet, and presentation application)*
- **X-as-a-Service** refers to the increasing number of available services
  - *Example: Identity as a Service , API as a Service, Desktop as a Service, Security as a Service*



Identity and Access Management (IAM)



- Federated Identity
- Single Sign-On (SSO)
- Centralized Authentication/ Authorization
- Identity As A Service

michelle.carter@aero.org
ETG/CSD

Identity and Access Management (IAM)

What is “Federated Identity”

Federated Identity is a means by which an organization can manage users electronic identity and attributes across multiple domains

- In the cloud computing environment, federation of identity plays a key role in enabling allied organizations to authenticate, provide single or reduced sign-on, centralized authentication, and exchange identity attributes between across multiple cloud computing domains
- Realized by:
  - *Open Standards*
    - Security Assertion Markup Language (SAML), Service Provisioning Markup Language (SPML), eXtensible Access Control Markup Language (XACML)
  - *Technologies*
    - Single Sign-On (SSO), Secure Token Exchange, Security Mediation, API Key
  - *Trust agreements between organizations*

Federated Identity

Open Standards

Key IAM related standards:

- Security Assertion Markup Language (SAML)
- eXtensible Access Control Markup Language (XACML)
- Service Provisioning Markup Language (SPML)

Federated Identity

Open Standards (cont.)

- **Security Assertion Markup Language (SAML)** provides an XML based message exchange protocol that specifies the rules for exchanging security assertions
  - *Defines three types of assertions: authorization, authentications, and attributes*
    - **Authorization** is the rights attributed to a user or software program to access a specific resource
    - **Authentication** is the process by with a user or software program is verified at a particular time. This assertion is typically created by the "Identity Provider"
    - **Attributes** provides specific information about a subject (e.g., "Name", "Company Name")

Security Assertion Markup Language (SAML)

Claims Sets

SAML assertions provide an easy means for implementing identity claims-based principles to applications. SAML assertions allow the receiving entity to validate the request before sending a response.

The contents of the assertion should include the “claim set” that includes:

- *User name*
- *User role*
- *Purpose of use*
- *User organization*
- *Authorization details*
- *Digital signature*
- *Issuer*

Security Assertion Markup Language (SAML)

Claims Sets (cont.)

SAML provides three methods for validating or confirming the “claim” asserted by an user: sender-vouches, holder-of-key, and bearer.

- ***Sender-vouches*** claims become the attesting entity vouching for the user making the request generally by signing the message with its key. With sender-vouches there is no trust relationship between the requester and the receiving entity, but there is a trust relationship between the attesting entity and the receiver.

- ***Holder-of-key*** claims are signed with a private key corresponding to a digital certificate issued by a trusted authority. Just as in the case of the sender-vouches, the receiver does not have trust relationship between the requester and the receiver, but in the case holder-of-key the receiver does trust the issuer of the requester’s credentials.

- ***Bearer claims*** carry the subject’s identity information, but does not require trust to be verified. It is assumed that the bearer claims are trusted. [4]

Federated Identity

Open Standards (cont.)

- **eXtensible Access Control Markup Language (XAML)** provides a means for organizations to implement a common authorization method across federated clouds
  - *Consists of four policy components: PEP, PIP, PDP, and PAP*
    - Policy Enforcement Point (PEP) – enforces policy decisions and admission control in response to a request for information and/or resource
    - Policy Information Point (PIP) – supplies data that's used for evaluating an authorization policy
    - Policy Decision Point (PDP) – makes decision for entity to gain access to resource and/or information
    - Policy Administration Point (PAP) – creates a policy or a set of policies

Federated Identity

Open Standards (cont.)

- **Service Provisioning Markup Language (SPML)** provides an open standards approach to managing user accounts
  - *Allows organizations with enterprise level platforms (e.g., web portals, application servers, and service centers generate provisioning requests) to generate requests across organizations*

Federated Identity

Technologies

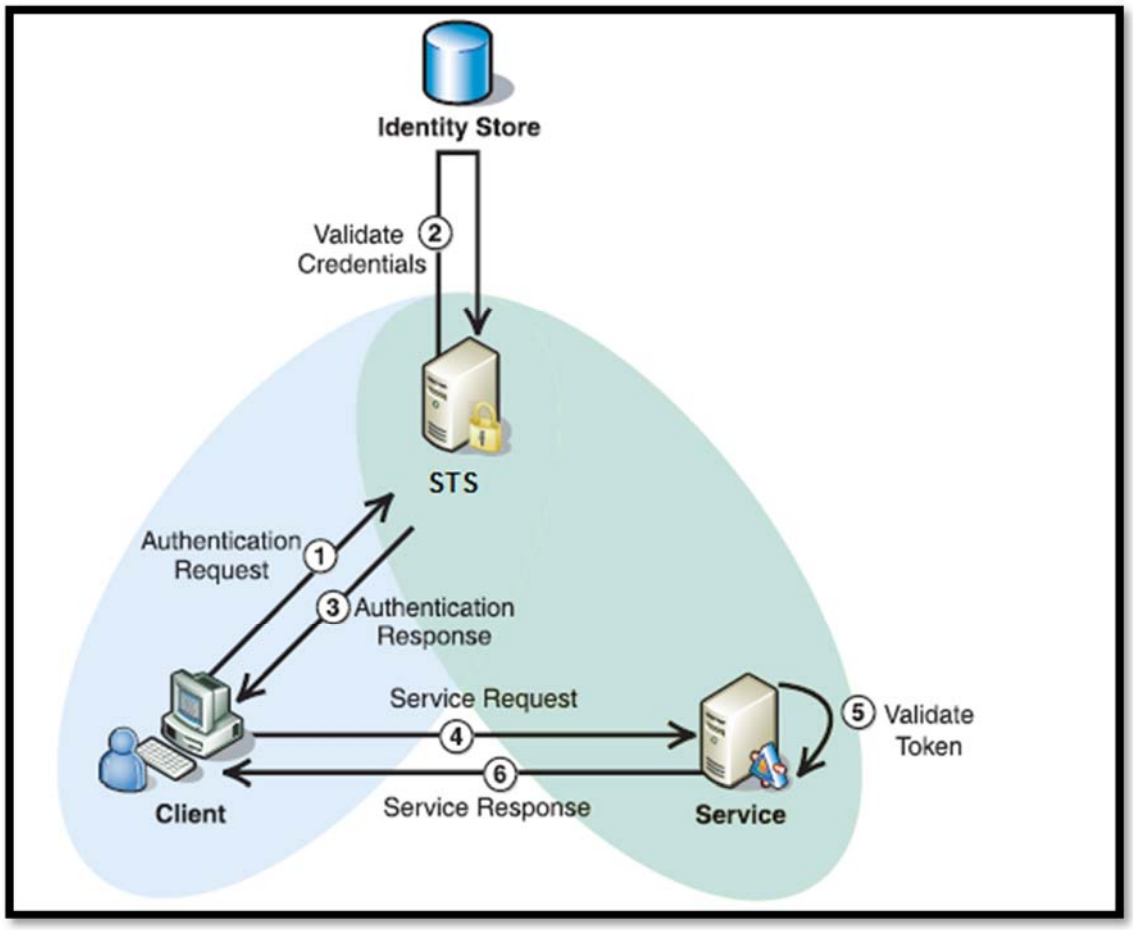
Single Sign-On (SSO) / **Reduced Sign-On (RSO)** enables an organization to implement federated identity between multiple domains.

- Allows a user to authenticate to a single system, while the SSO system manages the user's access to other systems
- Common SSO implementations include:
  - *Kerberos Ticket-Granting Ticket (TGT)*
  - *Smart Card Based (e.g., Government CAC card)*
  - *Two-factor authentication*
    - One-Time Token Password (OTP)
    - Integrated Window Authentication
    - Security Assertion Markup Language (SAML)

Federated Identity

Technologies (cont.)

The implementation of a **Secure Token Service (STS)** is a key aspect to implementing a secure federated cloud environment. STS provides a software based identity provider capability that is responsible for issuing security tokens in a claims-based identity system.

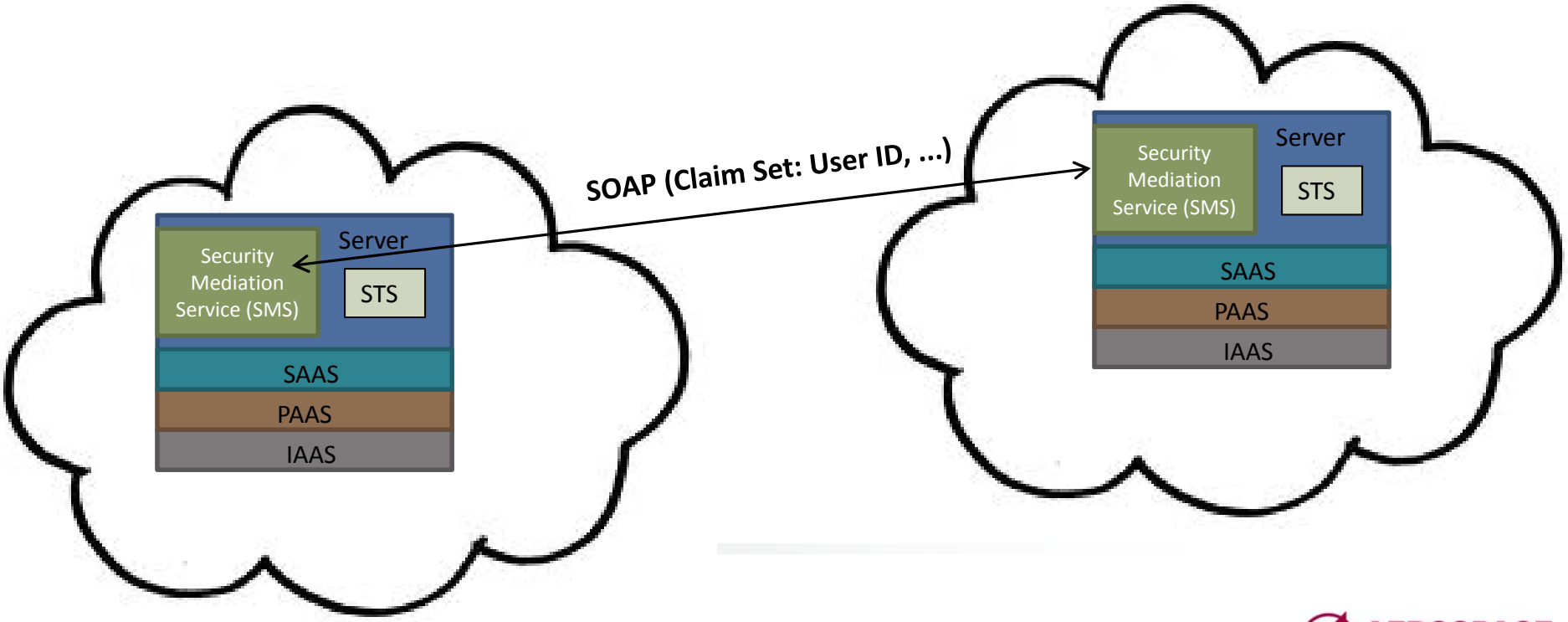


Secure Token Service Implementation

Federated Identity

Technologies (cont.)

The **Secure Mediation Service (SMS)** provides the conduct for subjects (users, systems , services) to request and receive resources and services across cloud computing domains, by providing information required to authenticate and authorized subjects.



Federated Identity

Technologies (cont.)

The **Application Programming Interface (API) Key** provides an additional layer of security for resources or service exchanges.

API key functions serves as a:

- Unique identifier
- Security token for authentication
- Set of access rights on the API associated with it

Federated Identity

Trust Agreements

Trust Agreements are typically defined between two organizations with common needs or goals.

- Three factors to “trust” in a cloud environment:
  - *Agreement (e.g., Service Level Agreements (SLAs))*
    - Used as an enforcement instrument for policies and procedures
  - *Transparency*
    - Insight into the implementation of security practices and how resources are secured and managed
  - *Enforcement*
    - A means of validating users and services

Identity and Access Management (IAM)

Centralized Authentication and Authorization

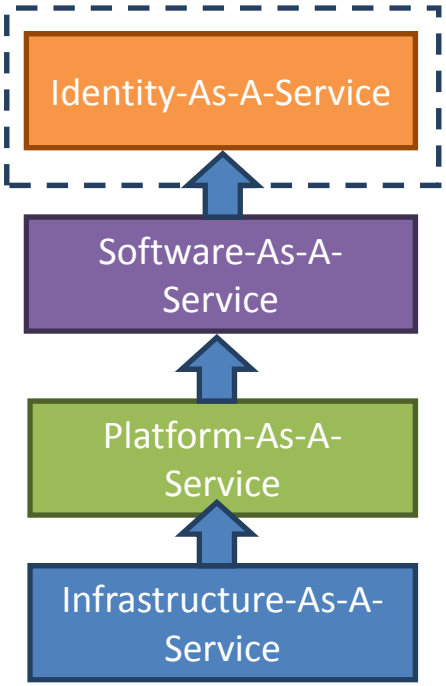
Centralized Authentication and Authorization enables the identity of a process or user to be handled by a centralized service within the cloud.

- Allows organizations to make the process of detecting suspicious activities easier, and reduces the amount of sensitive data transferred in the system (e.g., usernames, passwords)
- Features include:
  - *User Database*
  - *Service Database*
  - *Mediations Service (i.e., SMS)*
  - *Security Token Service*
  - *API Key*

michelle.carter@aero.org
ETG/CSD

User Identity and Access Management (IAM)

Identity As A Service (IDAAS)



Identity as a Service (IDAAS) aims to simplify the management of identity

- Integrates the attributes and functions of a user's identity and manage the data more effectively and efficiently as a part of the overall enterprise service layer. [7]
- Allows applications and other services to consistently reuse:
  - *Identity information*
  - *Identity provider services*
  - *Authentication services*
  - *Authorization services*
  - *Role provider services*
  - *Identity provisioning services*
  - *Auditing and reporting services*

michelle.carter@aero.org
ETG/CSD

Commercial IAM Solutions

Vendor	Product	Security	Interoperability
VMWare	Horizon	• Provides additional user authentication support by employing Open Authentication (Oauth), and multi-factor authentication that includes options from RSA. • Provides a mechanism for implementing policy enforcement • SAML is used for user authentication	• Supports SAML • Provides limited support for other cloud computing software products
OpenStack	Keystone	• Keystone employs security by using a secure token exchange that includes public and private keys	• Supports SAML • Provides an open source option for organizations that chose to add to the existing IAM product or develop an independent IAM solution
Amazon	Elastic Compute Cloud (EC2)	• Organizations that choose to build their own PAAS must have security aware software developers • Addresses security with its multiple user authentication methods for security: AWS access key, public private keys, and multi-factor authentication	• Supports SAML • Limited transparency, thus limiting trust between organizations

Federated Identify Reference Architecture

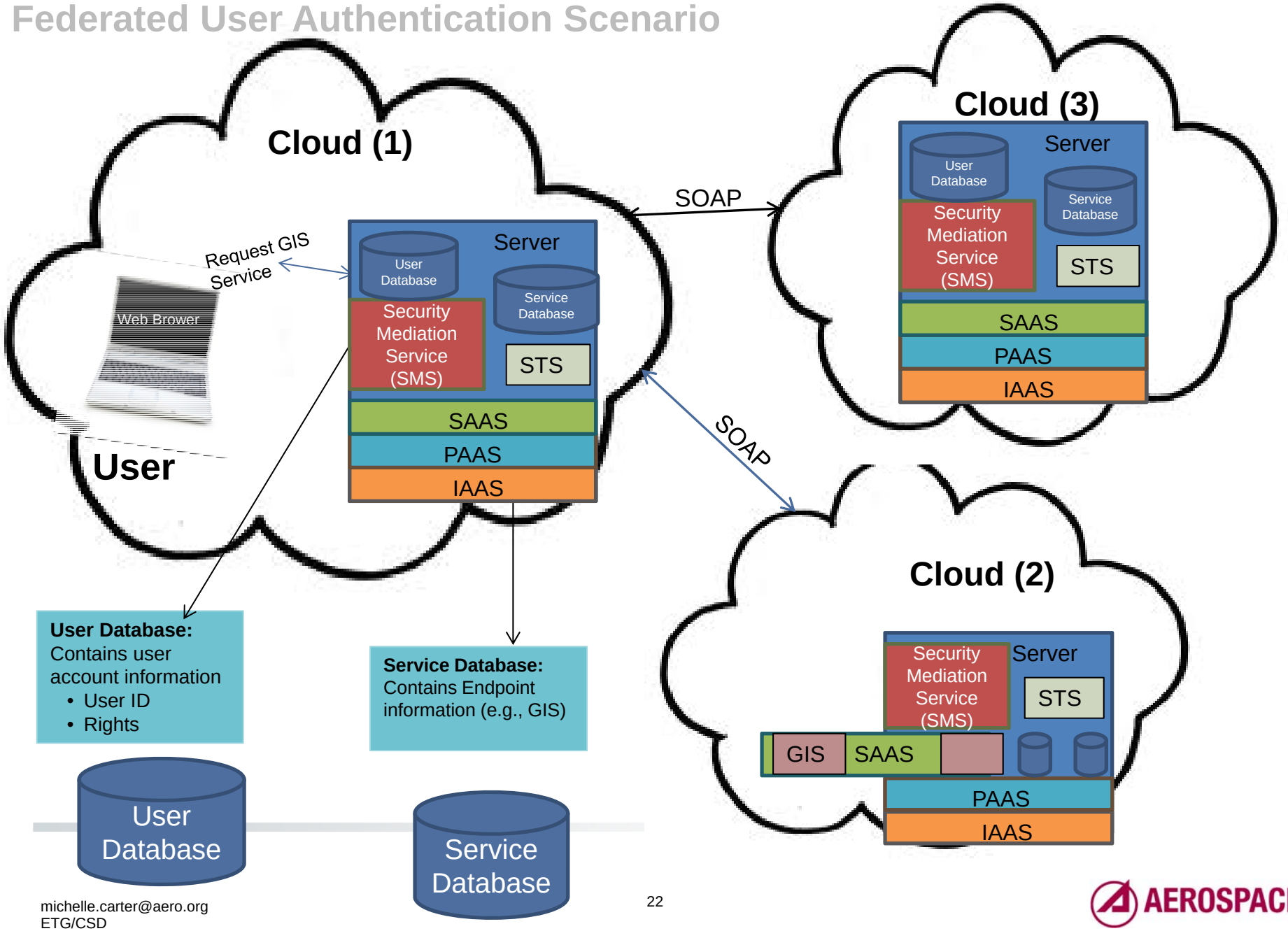
To implement an interoperable federated cloud environment, organizations should implement an identity management solution based open standards such as SAML, SPML and XACML.

Key factors to a federated, secure, interoperable approach to cloud computing:

- Open Standards Implementation (SAML, SPML, XACML)
- Web Services/Web portal
- Security Mediation Service (SMS)
- SAML claims based implementation
- SOAP and SSL for message transmission
- Secure Token Service (STS)

Federated Identify Reference Architecture

Federated User Authentication Scenario



michelle.carter@aero.org
ETG/CSD

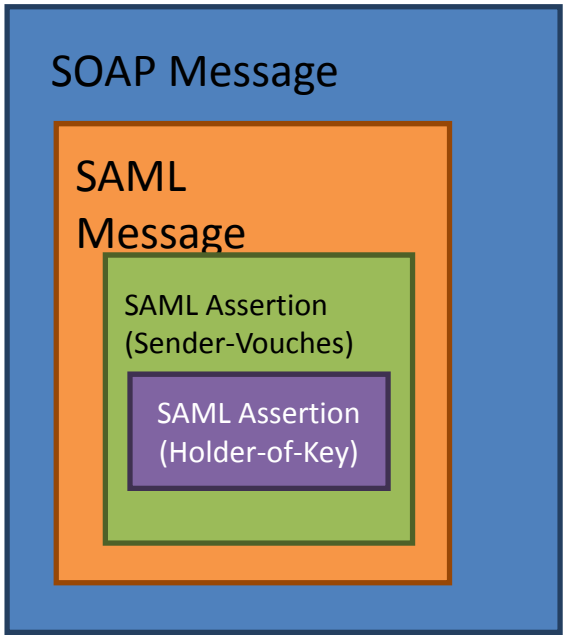
Federated Identify Reference Architecture

SAML Claims Based Approach

The use of the open standard SAML, allows organizations the flexibility of implementing an IAM solution that's suited for the organization's needs while allowing each federated cloud to easily define the identity assertions required to securely expose services and share data.

This implementation of SAML uses both holder-of-key and sender-vouches assertions:

- Sender-Vouches implementation provides a means for the receiving organization to verify the sender with the public key exchange, and confirms the requester by the use of the "requester confirmation" process.
- Adding the requester information for messages sent between federated clouds is an added security measure.

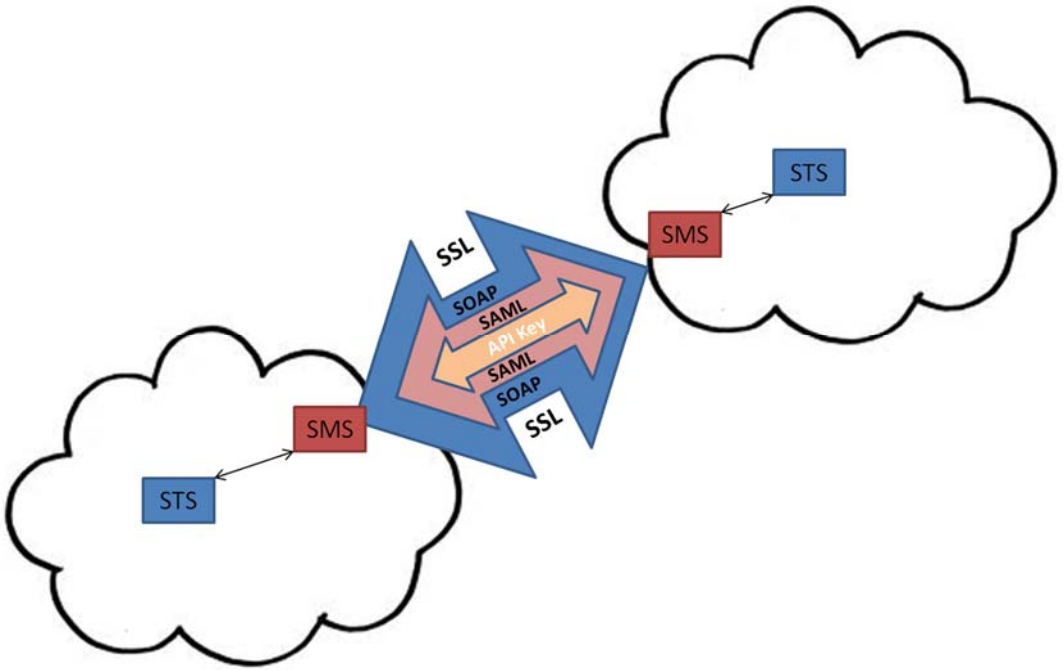


Nested SAML Assertion

Federated Identify Reference Architecture

Secure Authentication/Authorization

The diagram provides a visual representation of how data in the proposed IAM system will exchange information using security assertions within a trusted environment. The two domains will send and receive data via a SSL connection, and the information is further protected with the SAML with encryption.



Security Mediation Service (SMS): Perform the exchange of security assertion between the requester and the federated cloud. Additional task: manage provisioning, implement/enforce policies, generate API Key

Security Token Service (STS): Generates the tokens based on username and certificate.

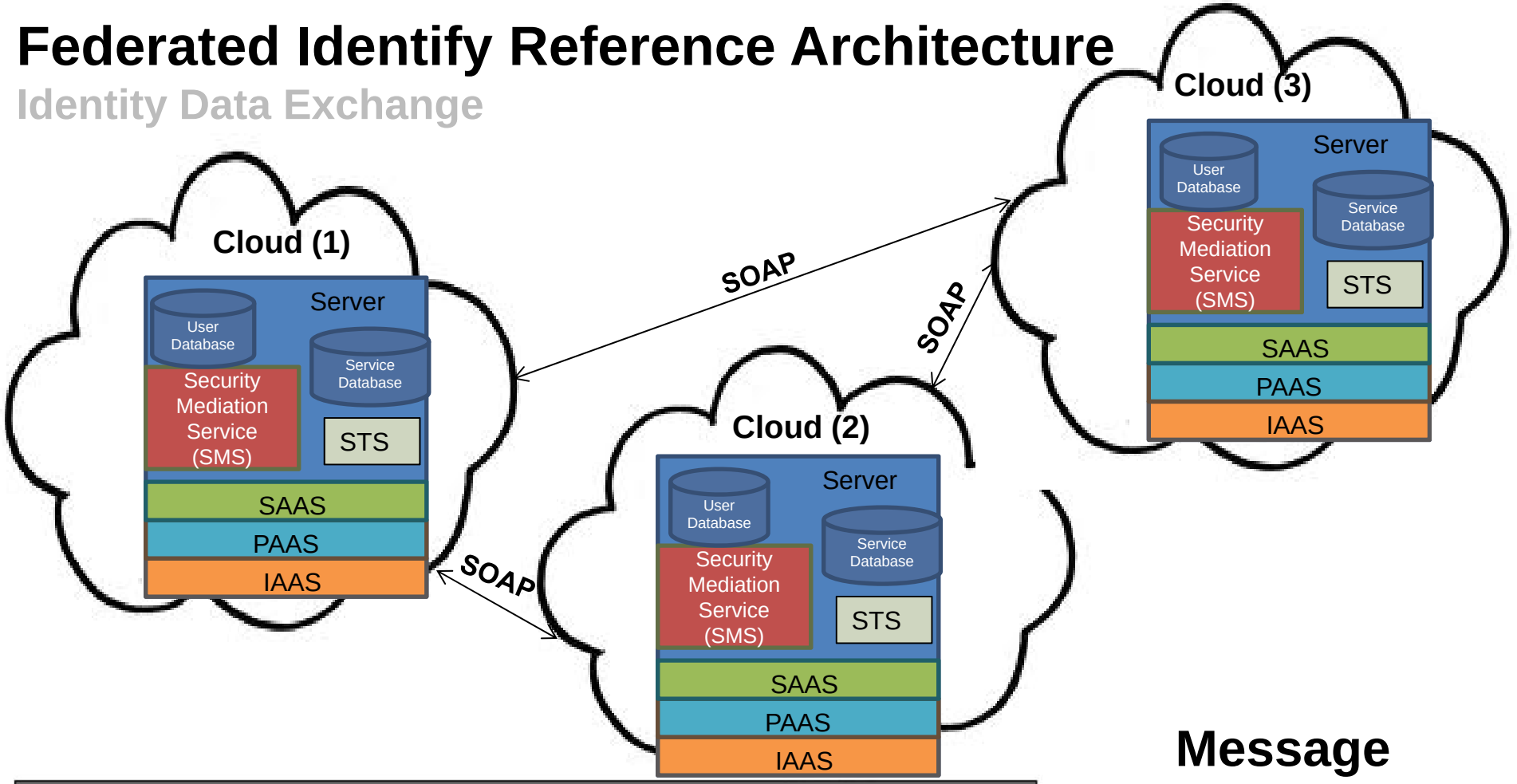
Secure Socket Layer (SSL): SSL used to secure the data exchange between the cloud domains

API Key: Secret key is sent by SMS and validated by external SMS used to authenticate the service request

Simple Object Access Protocol (SOAP): SOAP will be used to transport the SAML assertions

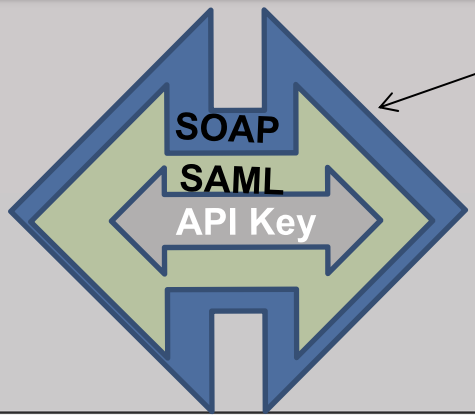
Federated Identify Reference Architecture

Identity Data Exchange



Authentication SOAP Message Contents:

- ***SAML Assertion***
  - ✓user name
  - ✓user role
  - ✓purpose of use
  - ✓user organization
  - ✓authorization details
  - ✓digital signature
  - ✓ issuer
- ***API Key***

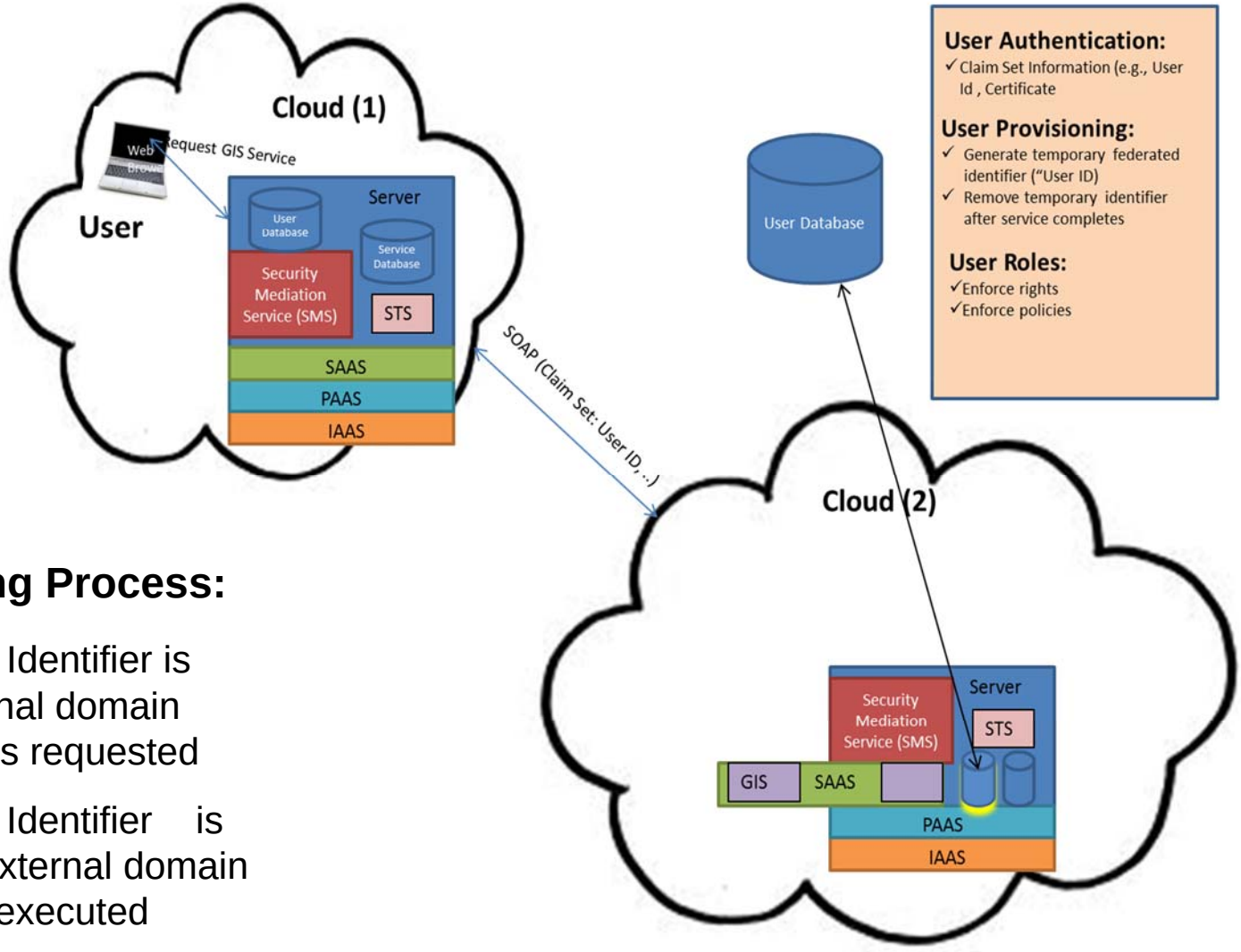


Message Layers

AEROSPACE

Federated Identify Reference Architecture

User Provisioning

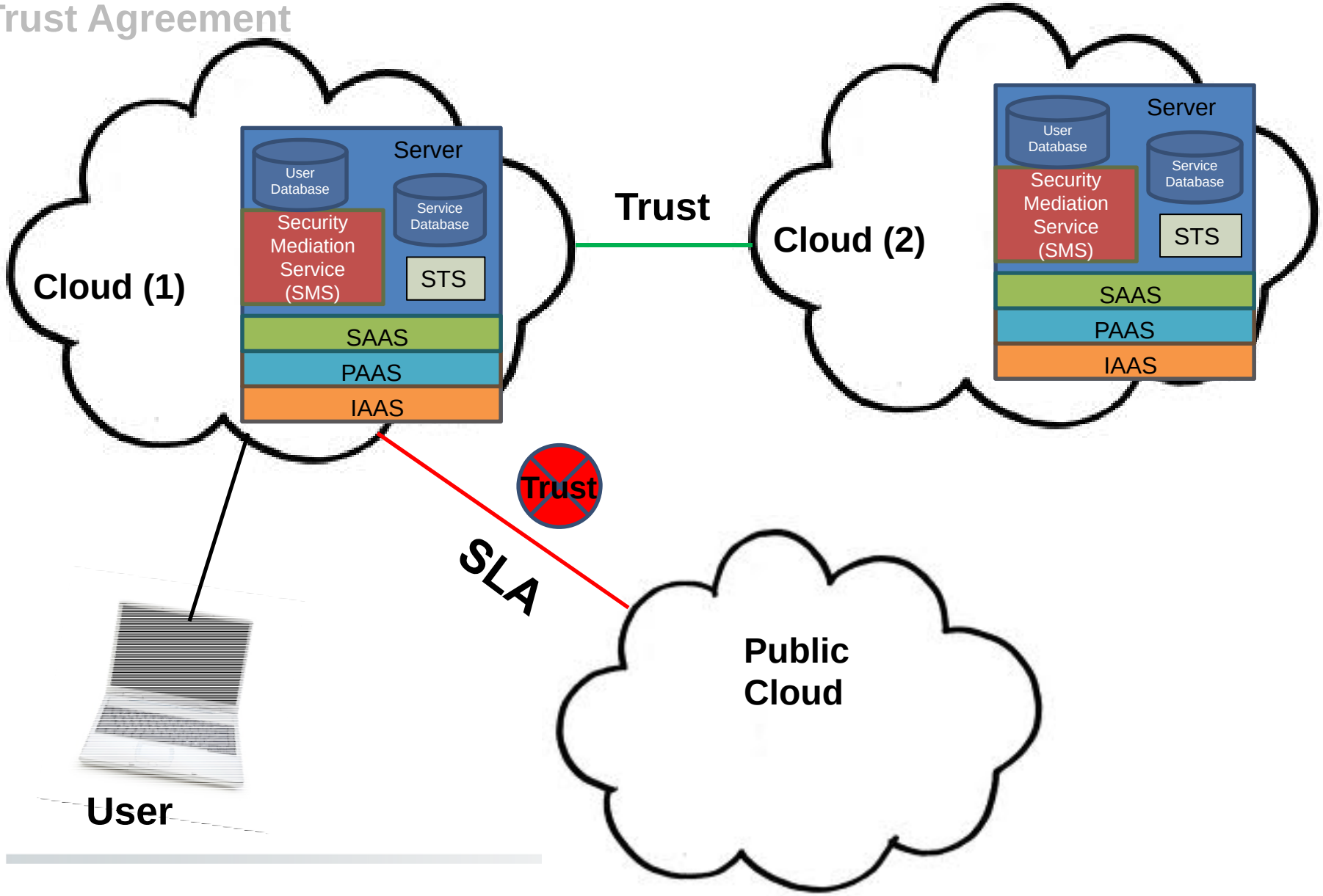


User Provisioning Process:

- Federated User Identifier is created in external domain when resource is requested
- Federated User Identifier is removed from external domain after request is executed

Federated Identify Reference Architecture

Trust Agreement



Summary

- Organization's striving to have a comprehensive Identity and Access Management (IAM) solution should consider three key items:
  - *Interoperability*
  - *Security*
  - *Trust*
    - Transparency
    - Enforcement

- **Key Architectural Features:**
  - *Centralized authentication/ authorization*
  - *Secure Mediation Service (SMS)*
    - Provisioning
    - Policy based user enforcements
  - *Security Token Service (STS)*
  - *Subject (users, systems, services) account management*
  - *Open Standards (SAML, XACML, SPML)*
  - *SAML claims based subject validation*
  - *Secure Messaging*
  - *Application Programming Interface (API) Key*
  - *Secure Socket Layer SSL*

AEROSPACE
Assuring Space Mission Success

Questions?

March 20, 2013
michelle.carter@aero.org
310-336-1278

Backup

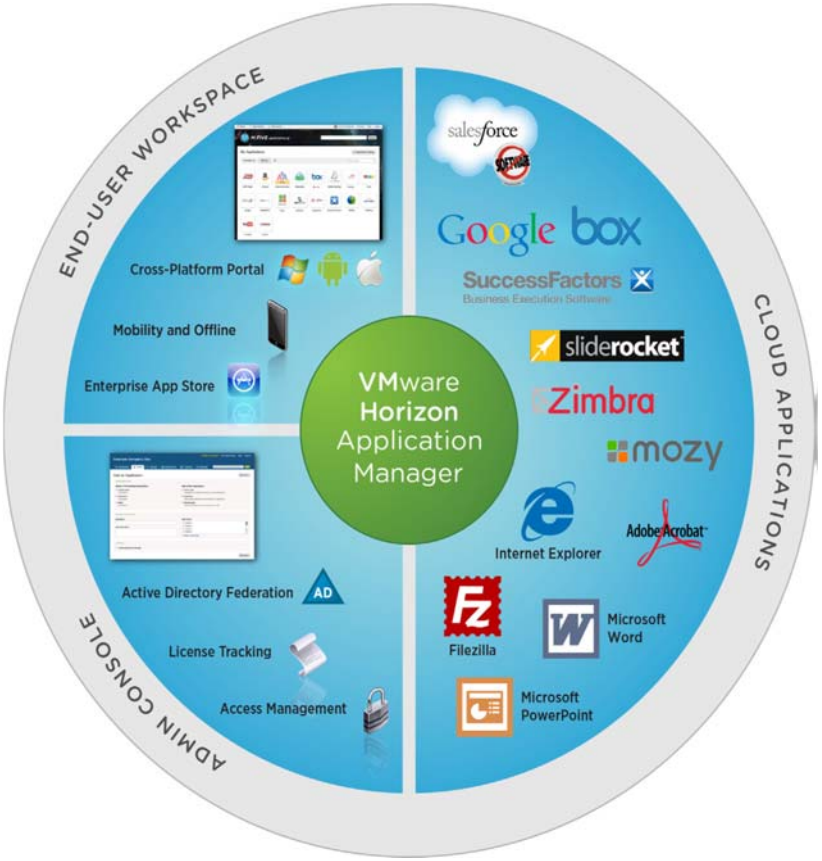
Commercial IAM Solutions

VMWare Horizon

VMware's vCloud is an IAAS public and private cloud computing product that's built on their existing virtualization architecture.

Horizon is VMWare's Identity and Access Management (IAM) product.

- Provides organizational management access via SAAS or web applications
- Leverages an organization's existing directory services by pulling user authentication into the cloud
  - *Metadata is used to associate a user's identity with the cloud management product [28]*

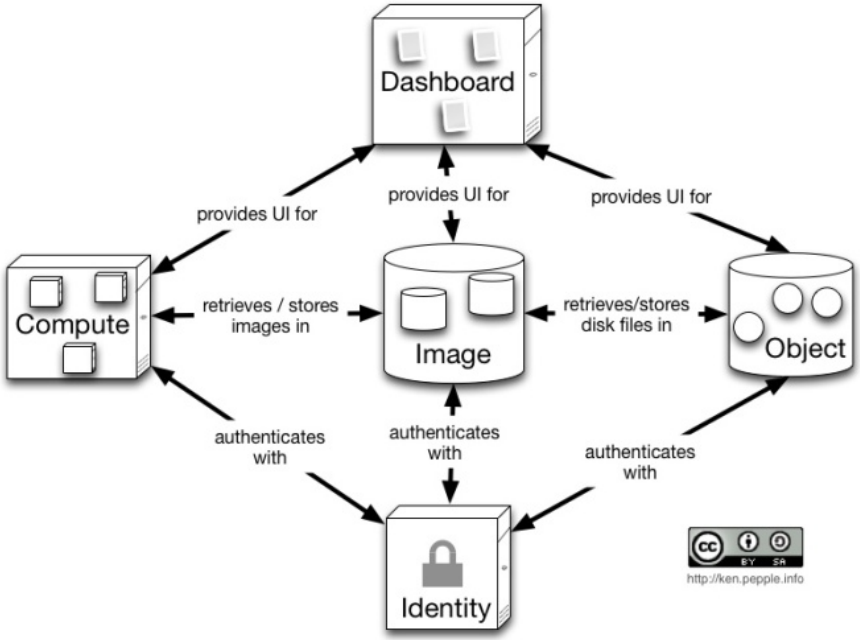


VMWare Architecture with Identity [28]

Commercial IAM Solutions

OpenStack Keystone

- Provides a means for the software to integrate with an existing backend directory service such as Lightweight Directory Access Protocol (LDAP)
- Provides authentication and authorization services for all OpenStack components
- Token generation is used to authorize users
- Provides a catalog of available services

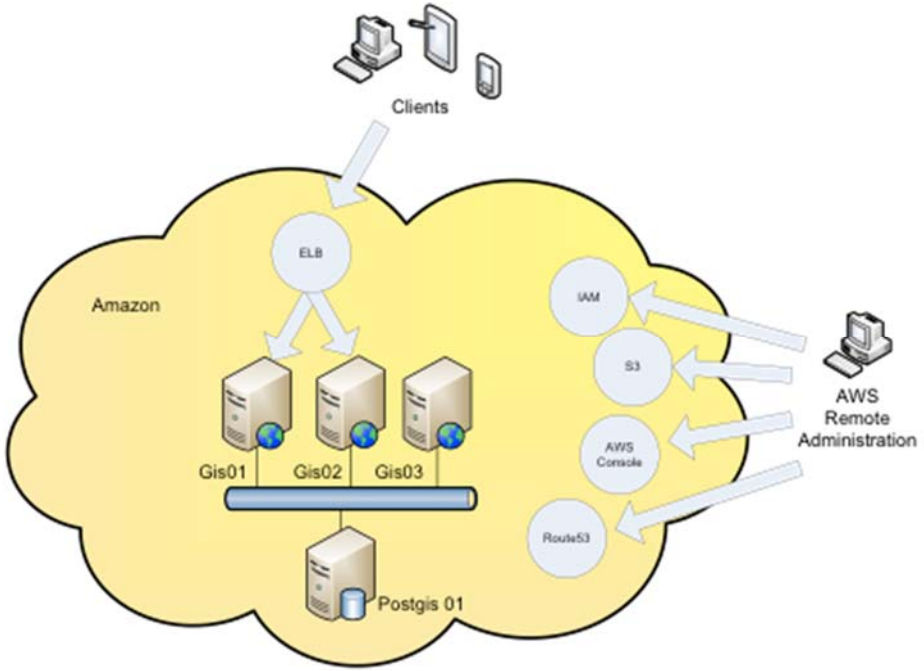


OpenStack Architecture with Identity [10]

Commercial IAM Solutions

Amazon Elastic Compute Cloud (EC2)

- Provides support for identity and access management that implements user security credentials, manages permission assignments, and allows organizations to set up IAM functionality via APIs
- Allows organizations to build their own platforms
- Provides SAML support
- Addresses security with its multiple user authentication methods for security: AWS access key, public private keys, and multi-factor authentication
- Creates trust challenges for organizations seeking to employ an interoperable IAM solution



Amazon EC2 Architecture with Identity [29]

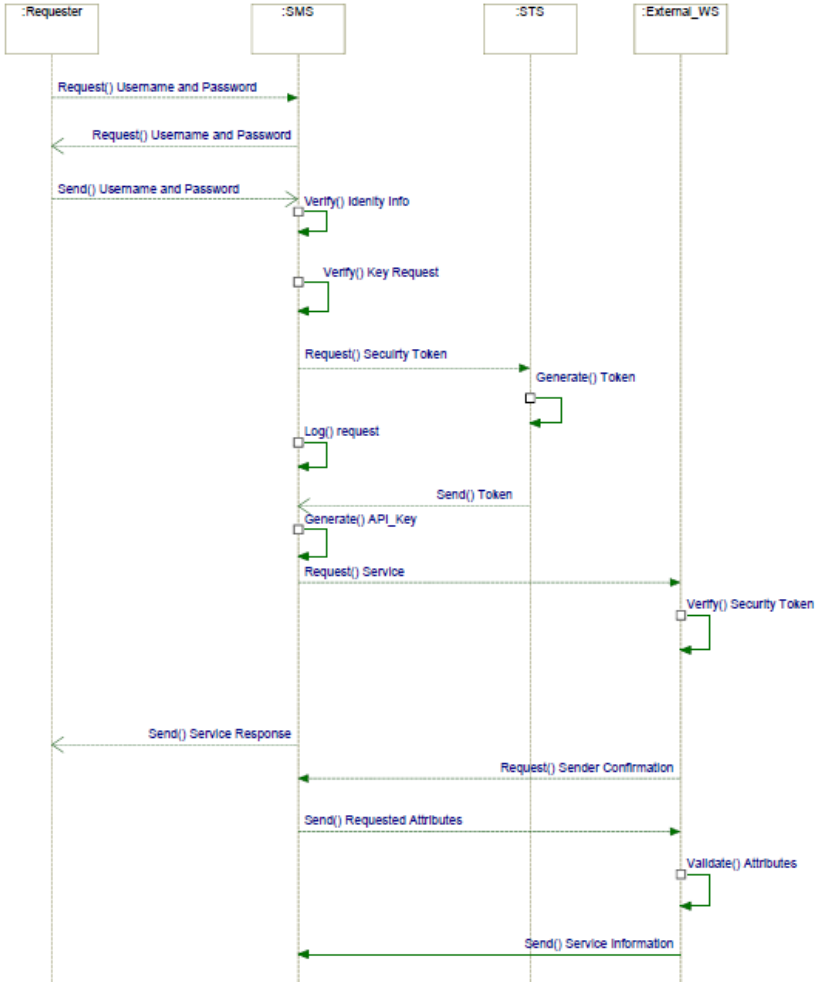
Identity and Access Management

Security Challenges/Vulnerabilities

- **Man-in-the-Middle (MITM)**
  - *MITM exposure risk is common when SSL connections are not properly set up, thus allowing an attacker to retrieve security credentials [24]*
- **Distributed Denial of Service Attacks (DDoS)**
  - *Public cloud multi-tenant infrastructure*
    - An attack against a single service/client is a possible attack against all the services and shared resources on a system
    - Cloud computing environment can have a multiplying effects across public clouds because of the following common infrastructures: network, computing infrastructure, memory, and storage [23]
- **Application Program Interface (API) Attacks**
  - *Elevated concern due to common use of APIs for executing cloud interoperability*
  - *Poses a security gap for Identity and Access Management [25]*
    - Cloud Security Alliance study defines the use of anonymous access, reusable security tokens or passwords, and clear-text authentication are all examples of how insecure APIs are a threat to cloud security [1]

Federated Identify Reference Architecture

SAML Assertion



User Authentication/Authorization Sequence Diagram

The sequence diagram provides a detailed view of the internal IAM process:

1) The user makes a request to the SMS and the SMS verifies the requestor's rights to the requested data.
2) SMS checks the type of claims required and then makes a request to the STS for creation of the user token.
3) After receiving the token, the SMS generates a API key for added security.
4) Request for service is submitted to external web service.
5) Sender confirmation is requested by external STS to validate requester.
6) Requested attributes are sent , and external STS validates the entitlements before proceeding with the execution of the data or service request.

Security Mediation Service (SMS): Perform the exchange of security assertion between the requester and the federated cloud. Additional task: manage provisioning, implement/enforce policies, generate API Key

Security Token Service (STS): Generates the tokens based on username and certificate.

Requester: Sends request for data or service to SMS

Sender Confirmation: A certificate check is performed which includes: revocation list check, expiration date check, signature from trust certificate authority, and key usage

API Key: Secret key is sent by SMS and validated by external SMS used to authenticate the service request

michelle.carter@aero.org
ETG/CSD

Acronym List

- **API** – Application Programming Interface
- **DDoS** – Distributed Denial Of Service
- **EC2** – Elastic Compute Cloud
- **IAAS** – Infrastructure As A Service
- **IAM** – Identity And Access Management
- **IDMS** – Intelligent Distributed Denial Of Service Mitigation Systems
- **JDBC** – Java Database Connectivity
- **IDAAS** – Identity As A Service
- **LAN** – Local Area Network
- **LDAP** – Lightweight Directory Access Protocol
- **MITM** – Man-In-The-Middle
- **NIST** – National Institute of Standards and Technology
- **OTP** – One-Time Token Password
- **PAAS** – Platform As A Service
- **RSA** – Rivest-Shamir-Adleman algorithm
- **SAAS** – Software As A Service
- **SAML** – Security Assertion Markup Language
- **SLA** – Service Level Agreement
- **SMS** – Security Mediation Service
- **SOAP** – Simple Object Access Protocol
- **SPML** – Service Provisioning Markup Language
- **SRTBH** – Source-Based Remote Triggered Black Hole
- **SSO** – Single-Sign-On
- **SSL** – Secure Socket Layer
- **STS** – Security Token Service
- **SV** – Sender Vouches
- **TLS** – Transport Layer Service
- **TGT** – Ticket Granting Ticket
- **WAN** – Wide Area Network
- **XACML** – eXtensible Access Control Markup Language

References

- [1] Cloud Security Alliance, Top Threats to Cloud Computing V1.0", https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Mar. 2010.
- [2] R. McMillan, "Hackers find a home in Amazon's EC2 cloud" Infoworld, http://www.infoworld.com/d/cloud-computing/hackers-find-home-in-amazons-ec2-cloud-742, Dec. 2009.
- [3] Tivoli Federated Identity Manager, IBM, http://www-01.ibm.com/software/tivoli/products/federated-identity-mgr/.
- [4] "Security Assertion Markup Language (SAML) V2.0 Technical Overview", OASIS, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.html, Mar. 2008
- [5] K. Marko, "Understanding Private Cloud Stacks", InformationWeek Reports, http://reports.informationweek.com/abstract/5/8682/cloud-computing/fundamentals-understanding-private-cloud-stacks.html, Feb. 20 12.
- [6] VMware. "VMware vCloud® Architecture Toolkit Public VMware vCloud Implementation Example" October 2011.
- [7] N. Kaushik, "Understanding Identity as a Service", Oracle, https://collaboration.opengroup.org/jericho/presentations/fall2007/kaushik.pdf.
- [8] "Ping Federate:Tech Specs", Ping Identity, https://www.pingidentity.com/products/pingfederate/.
- [9] **"**How to Use a Hypervisor in Cloud Computing Virtualization" http://www.dummies.com/how-to/content/how-to-use-a-hypervisor-in-cloud-computing-virtual.html.
- [10] "Conceptual Architecture", OpenStack, http://docs.openstack.org/essex/openstack-compute/admin/content/conceptual-architecture.html.
- [11] P. Mell and T. Grance, "The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology". NIST Special Publication 800-145, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, Sep. 2011.
- [12] "Defined Categories of Service 2011", Cloud Security Alliance, https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf. Oct. 2011.
- [13] "WS-Security Profile of the OASIS Security Assertion Markup Language (SAML)", OASIS, https://www.oasis-open.org/committees/security/docs/draft-sstc-ws-sec-profile-04.pdf, Sep. 2002.
- [14]. "Cloud Computing Synopsis And Recommendations", NIST, http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf, May 2011.
- [15] "Defined Categories of Service 2011", Cloud Security Alliance, https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf, 2011.
- [16] "eXtensible Access Control Markup Language (XACML)", OASIS, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf, Feb. 2005.
- [17] **"**IBM Tivoli Federated Identity Manager", IBM**,** http://www-01.ibm.com/software/tivoli/products/federated-identity-mgr/features.html?S_CMP=rnav.
- [18]. "Keystone Architecture", Openstack, http://docs.openstack.org/developer/keystone/architecture.html, Aug. 2012.
- [19] "VMware® ThinApp Reviewers Guide", VMWare, http://www.vmware.com/files/pdf/VMware-ThinApp-Reviewers-Guide.pdf, 2011.
- [20]. "Symplified Trust Cloud™ Enables EC2 Security" Symplified**,** http://www.thetrustcloud.com/features.html.
- [21] "Cloud Identity Buyer's Guide", Symplified, www.symplified.com.
- [22]" Cloud Security Alliance Security as a Service Implementation Guidance Version 1.0", Cloud Security Alliance, http://www.cloudsecurityalliance.org, 2012.
- [23] T. Lohman. "DDoS is Cloud's security Achilles heel", http://www.computerworld.com.au/article/401127/ddos_cloud_security_achilles_heel/#closeme. Sep. 2011.
- [24] "SANS Institute InfoSec Reading Room", http://www.sans.org/reading_room/whitepapers/threats/ssl-man-in-the-middle-attacks_480. Feb. 2002.
- [25] "Cloud Computing", Armorize Technologies Inc., http://www.malware-info.com/cloud_computing.html.
- [26] "CSA Security, Trust & Assurance Registry (STAR)", Cloud Security Alliance, https://cloudsecurityalliance.org/star/.
- [27] B. Doerr "Cloud Insecurity: Not Enough Tools, Experience or Transparency", Tech News World, http://www.technewsworld.com/story/74890.html, Apr. 2012.
- [28] "VMware Horizon Application Manager", VMWare**,** http://www.vmware.com/files/pdf/horizon/VMware-Horizon-App-Manager-Datasheet.pdf, April 2012.
- [29] "AWS Case Study: Junta de Extremadura and Sadiel", Amazon Web Services, http://aws.amazon.com/solutions/case-studies/sadiel/.
- [30] Service Provisioning Markup Language (SPML) Version 1.0, OASIS, https://www.oasis-open.org/committees/download.php/4137/os-pstc-spml-core-1.0.pdf, Oct. 2003.

Federated Identify Reference Architecture

User Authentication Message

- IAM system exchanges information using security assertions within a trusted environment.
- Information between the two domains is exchanged via a SSL connection, and the information is further protected with SAML encryption.