HPCS 2015 TUTORIAL IV

Title: Cloud Security, Access Control and Compliance

http://www.uazone.org/demch/presentations.html
hpcs2015tutorial-cloud-security-access-control-compliance-v02.pdf

Yuri Demchenko
System and Network Engineering, University of Amsterdam

HPCS2015 Conference
20-25 July 2015, Amsterdam

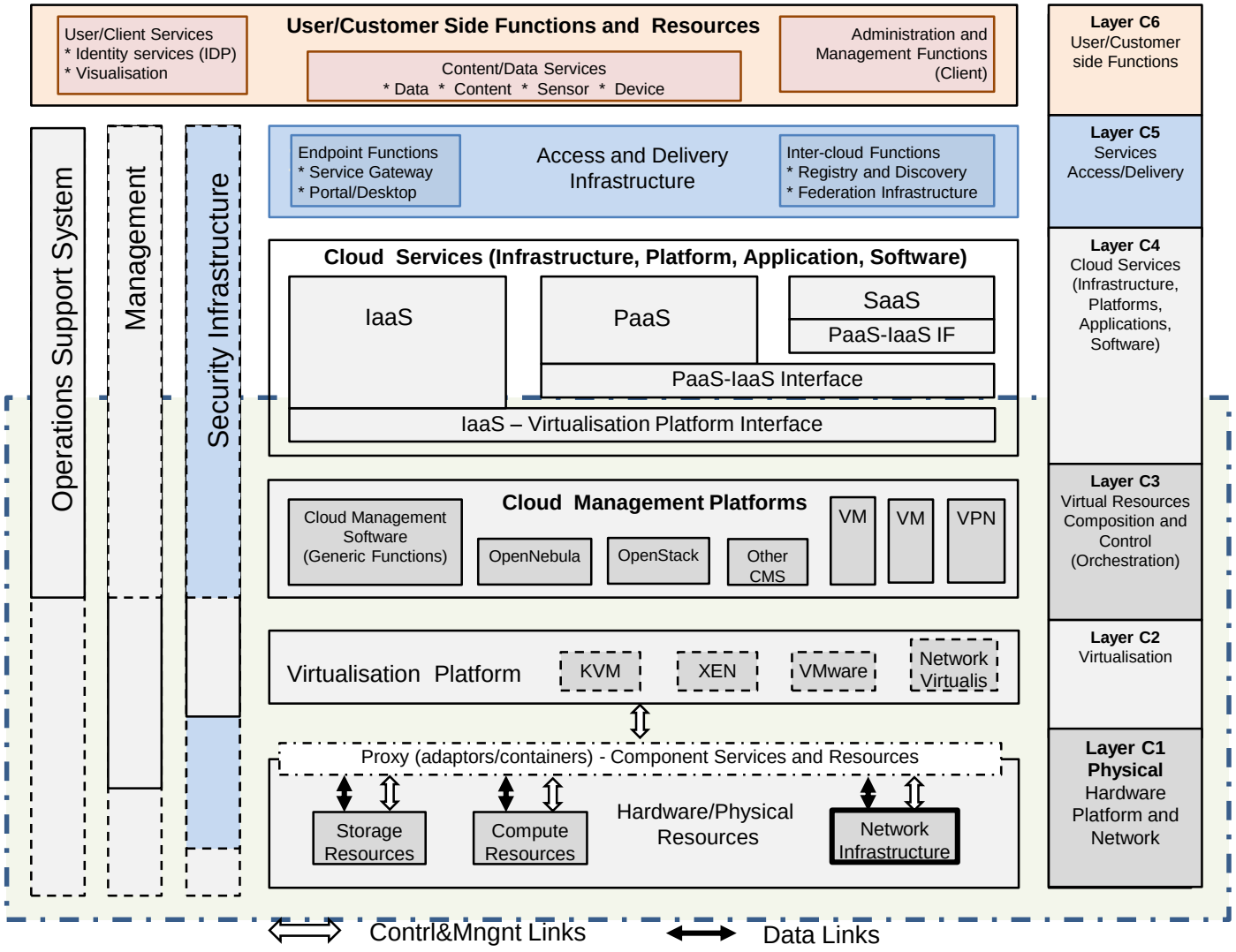
Outline

Part 1. Cloud Security
- Cloud security models, services and mechanisms
- Security Services Lifecycle Management (SSLM) model
- Cloud Security best practices: AWS and Microsoft Azure

Part 2. Authentication and Authorisation Infrastructure (AAI) in cloud
- Basic AAI services, mechanisms and protocols
- Federated security models in cloud
  - Federated Access Control and Identity Management in cloud
- AAI best practices: Amazon IAM and Azure Active Directory (AAD)
- Demo/Hands-on: Identity and policy management in IAM and AAD

Part 3. Cloud Compliance and Certification
- Compliance standards
  - Security Controls and Cloud infrastructure
- PCI DSS Cloud Computing Guidelines
- CSA GRC Stack: Governance, Risk Management and Compliance
- Demo/Hands-on: CSA Consensus Assessment Initiative Questionnaire
- Demo/Hands-on: Microsoft Cloud Security Readiness online tool

Multilayer Cloud Services Model (CSM)



CSM layers

(C6) User/Customer side Functions

(C5) Intercloud Access and Delivery Infrastructure

(C4) Cloud Services (Infrastructure, Platform, Applications)

(C3) Virtual Resources Composition and Orchestration

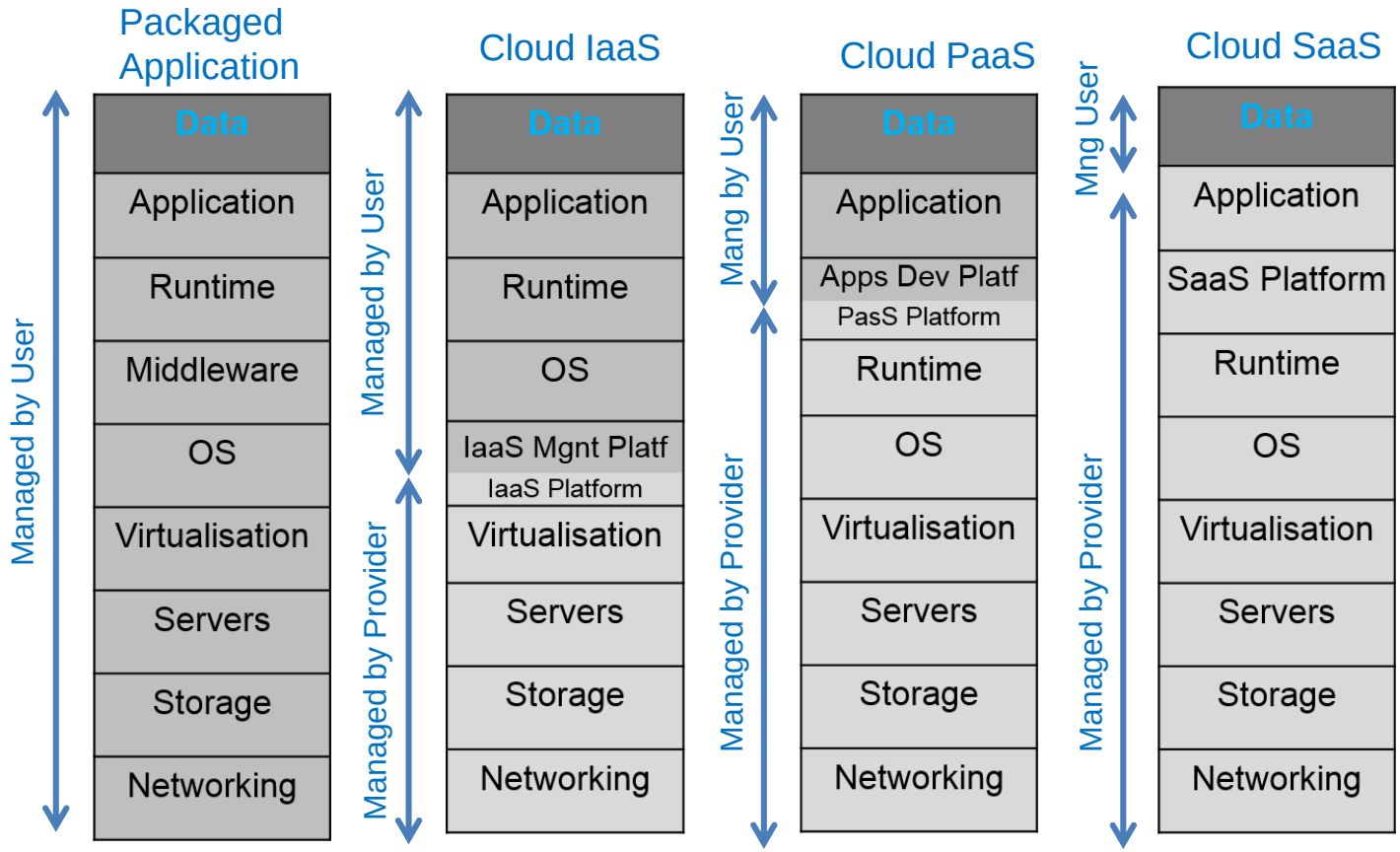
(C2) Virtualisation Layer

(C1) Hardware platform and dedicated network infrastructure

Control/ Mngnt Links

Data Links

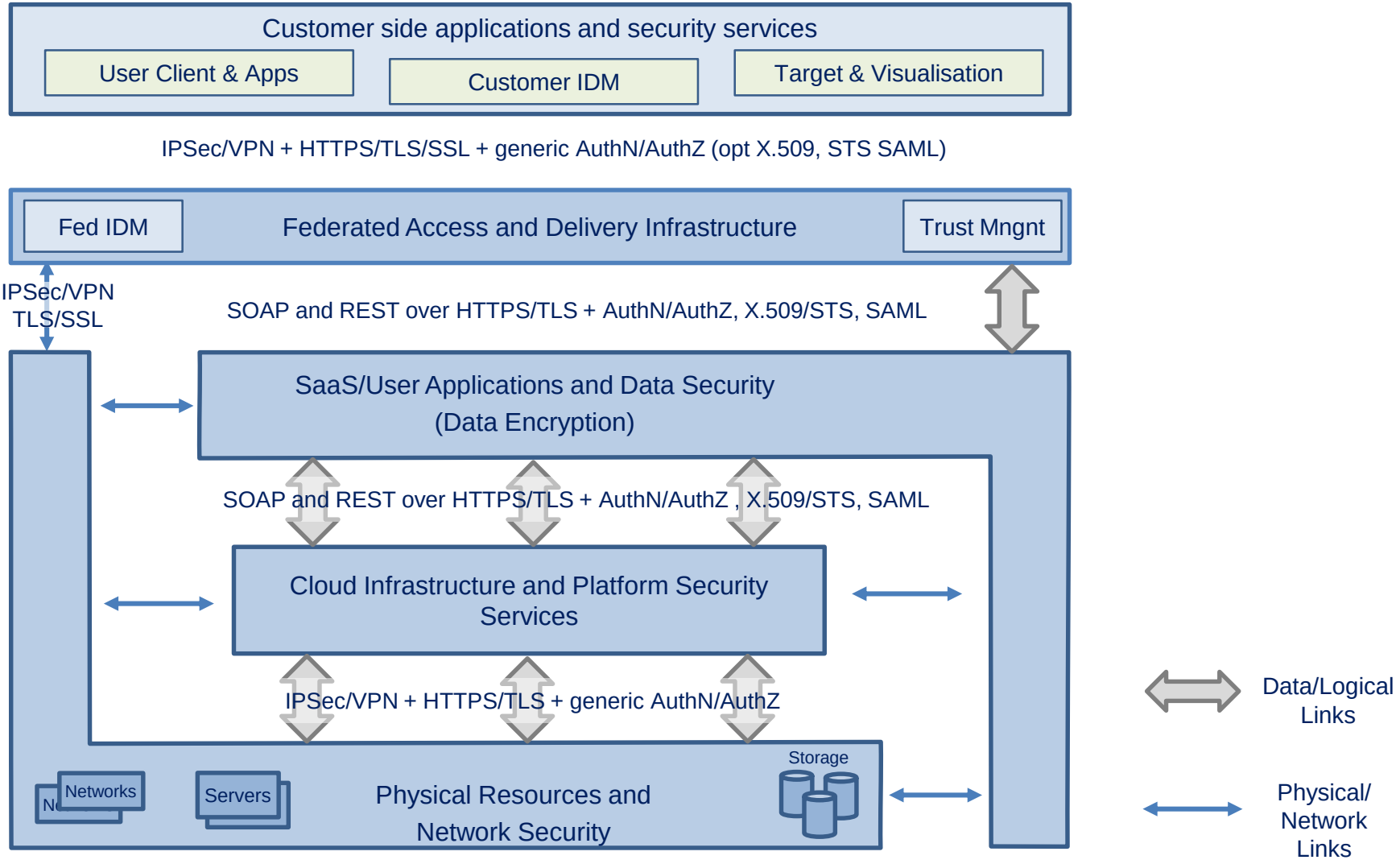
Responsibilities Split in IaaS, PaaS, SaaS



Security management responsibilities split between Customer and Provider for IaaS, PaaS, SaaS service models

- Updating firmware and software for platform and for customer managed components
- Firewall is intrusion prevention is a responsibility of the cloud provider
- Certification and compliance of the cloud platform doesn't imply security and compliance of the customer controlled components

Security Technologies in Cloud: Network and Service Related Security Protocols



What should you know about Security

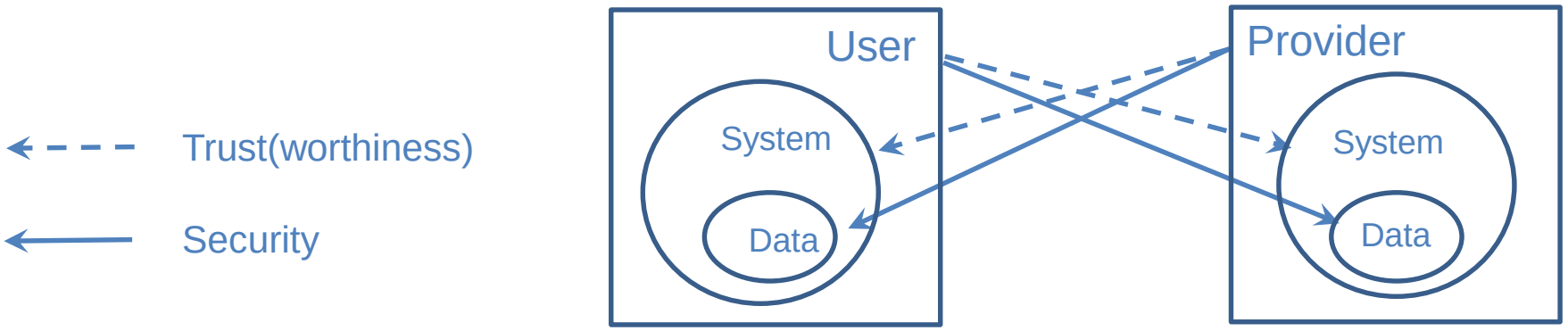
- Password is a basis for secure access but it is not enough to secure your applications and services.
  - There is whole stack of network and infrastructure or platform security services and mechanisms which need to be applied in a consistent way to ensure high system ***dependability*** and ***availability***
- Basis for secure communication and data transfer are the security protocols and security mechanisms
  - Security services are defined for communicating entities and can work at different layers
  - Security mechanisms can be used by services and functional components to achieve one or another aspect of security
    - E.g. VPN is using IPSec and IKE protocol which in their own turn use Diffie-Hellman and shared secret mechanisms;
    - All security protocols use at least one of the basic security mechanisms: encryption, digital signature, authentication, authorisation
    - Where authentication and authorisation can be also services if enacted between interacting parties
- Security is an overloaded term and may mean different aspects

  Network/communication Security - Data Security – Application Security - Operation Security – System Security
- What kind of data to protect
  - **Application Data – Personal Data (User ID, personal information) – Infrastructure management data**
- Data security must be considered for at least 3 aspects

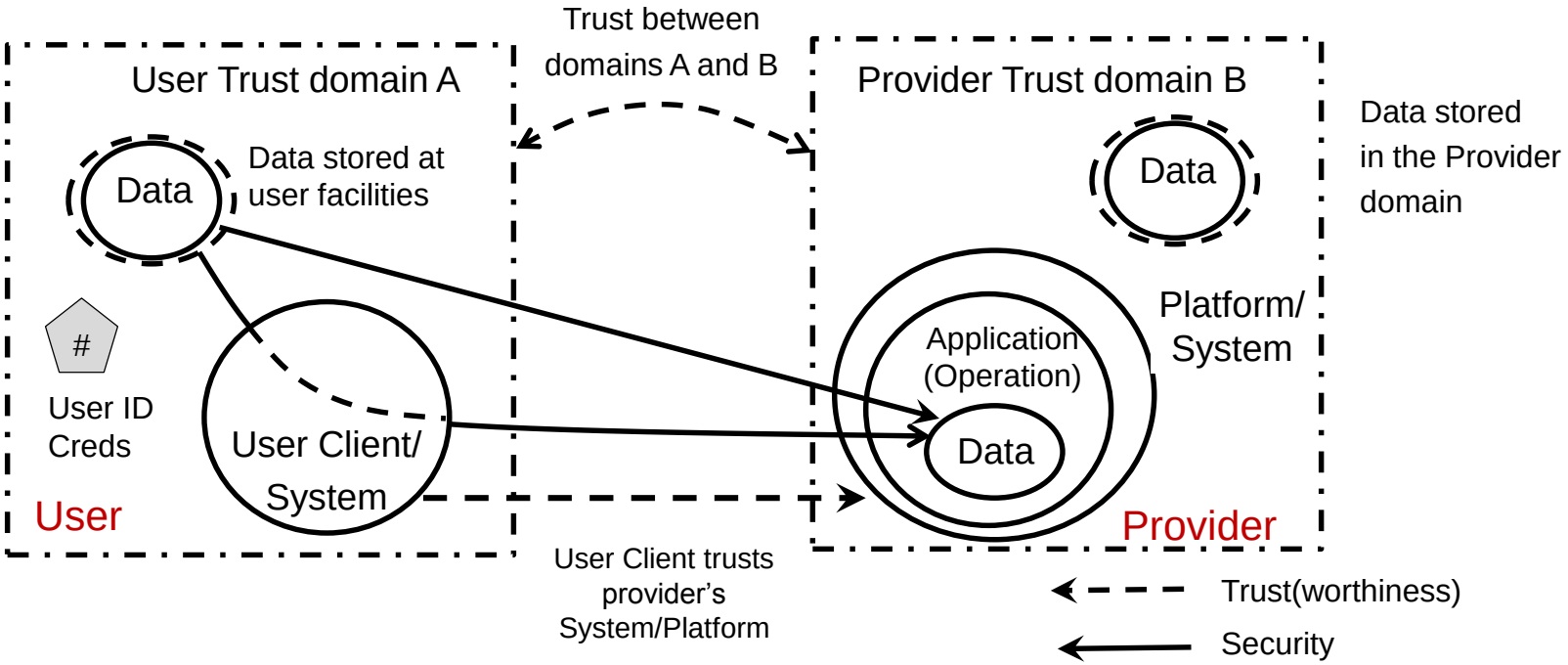
  Data in transfer (Communication) – Data in-rest (Stored) – Data at run-time (Processed)
- Relations between Security and Trust
  - Trust or trust relations is a foundation of the security protocols and services
  - Technical trust is typically based on possession of shared secret or private key in Public Key Cryptography
  - Social trust may include aspects such as reputation and may have different measures for level of trust
  - New methods and mechanisms are intending to combine strictly defined technical trust and system reputation that may be defined by uncontrolled technical factor that are statistically consistent

Different sides of Security and Trust

- Modern paradigm of remote distributed services and online/downloadable digital content provisioning makes security and trust relations between User and Provider more complex
- User and Service Provider – the two actors concerned with own Data/Content security and each other System/Platform trustworthiness
- Two other aspects of security/trust
  - Data stored vs Data processed
  - System Idle vs Active (running User session)



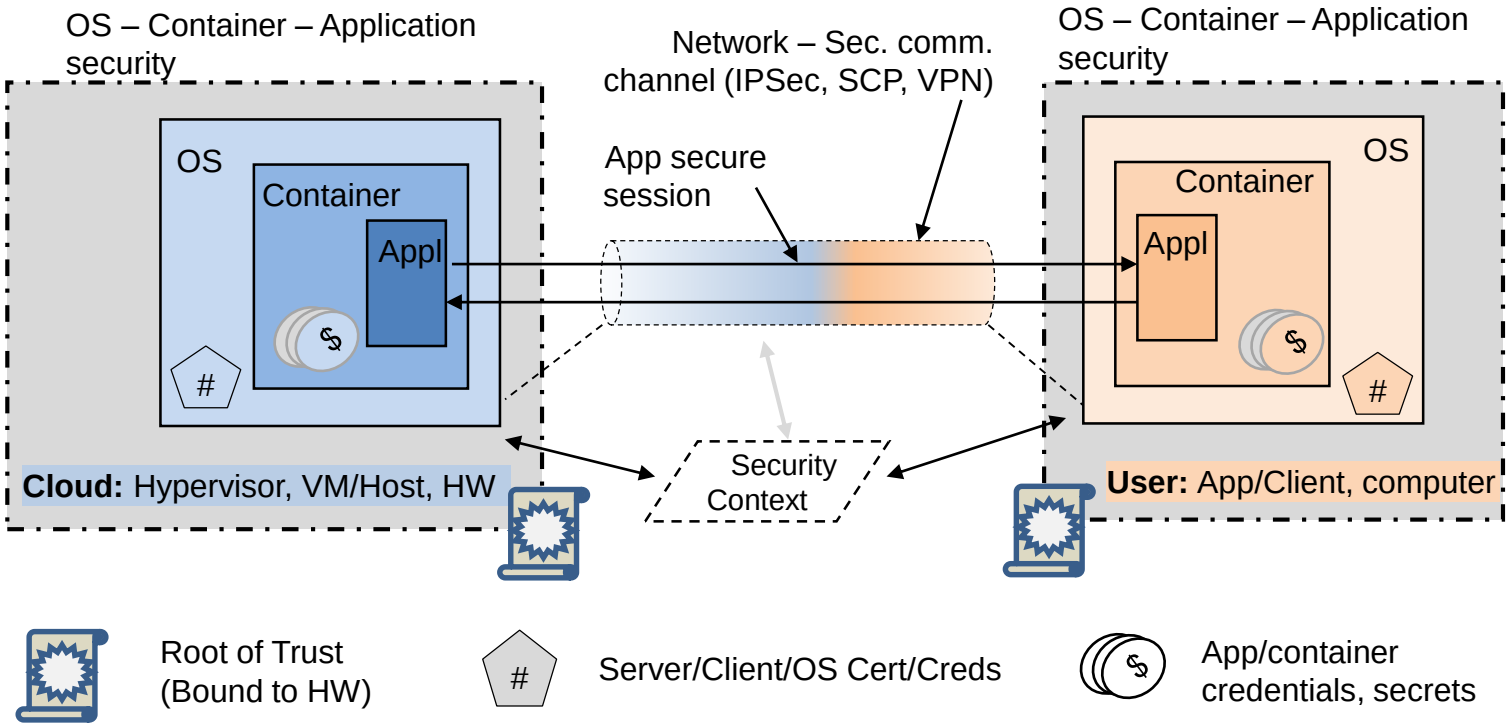
Trust Relations Between Provider and Customer



Components of the trust relations when processing data on the provider platform

- Data stored on user facilities
- Data processed and stored on provider facilities
- User client mast trust provider's system/platform
- Provider knows/trusts user by their ID credentials (e.g. username/password)

Cloud, OS, Network and Applications Trust Layers



- Consistent security must provide security at all layers correspondingly relying on trust credentials at each layer
  - Application – Container - Operating systems (security kernel) + Cloud platform
  - Network/communication – Runtime - Storage
- Two security models: Trusted Computing Base (TCB) for cloud platform and OSI/Internet security cloud based applications
  - Client/server and Service Oriented Architecture vs OS and hypervisor run-time
- Root of trust is based on the security credentials bound to hardware mediated through OS to runtime environment

Cloud Computing Security – Challenges

- Fundamental security challenges and main user concerns in clouds
  - Data security: Where are my data? Are they protected? What control has cloud provider over data security and location?
  - Identity management and access control: Who has access to my personal/ID data?
- Two main tasks in making cloud secure and trustworthy
  - Secure operation of the cloud (provider) infrastructure
  - User controlled access control (security) infrastructure
    - Provide sufficient amount of security controls for competent user
- Cloud security infrastructure should provide a framework for dynamically provisioned cloud security services and infrastructure as a part of the main services

Common Cloud Security Model Elements

- SLA and Provider based security model
  - SLA between provider and user defines the provider responsibility and guarantees
    - Data protection is attributed to user responsibility
    - There is no provider responsibility on user run applications or stored data
  - Providers undergo certification of their cloud infrastructure
    - Current certification and compliance model are not fully applicable to highly distributed and virtualised cloud environment
  - Customer/User must trust Provider
- Using VPN and SSH keys generated for user infrastructure/VMs
  - Works for single cloud provider
  - Inherited key management and scalability problems
- Simple access control, however can be extended with the Federated Identity Management
  - Currently supported by majority of cloud providers
  - Can federate with the customer/tenant SSO and Identity Management service
- Not easy integration with legacy customer/tenant infrastructure and physical resources
- Trade-off between simplicity and manageability on the cloud provider side

Cloud Environment and Issues to be addressed

- Virtualised services and environment
- On-demand provisioning and dynamic scalability
- Multi-tenant platform security and multi-user services access control
  - Tenants' storage and runtime separation in cloud
  - Fine grained access control in the tenants' applications
- New cloud oriented security services models
  - Provider – Customer/Tenant - User
    - Enterprise as a Customer, and employees as Users
- Uncontrolled execution and data storage environment
  - Promising homomorphic/elastic encryption (still at research stage)
- Security services are provisioned on-demand (as part of virtualised infrastructure) and require bootstrapping with the customer services and trust domain
  - Bootstrapping cloud and customer trust domains to ensure trusted environment for data processing and storage
    - Trusted Computing Group Architecture (TCGA)
- Integration with customer legacy security services and infrastructure
  - Campus/office local network/accounts

General Requirements to Cloud Security Infrastructure

- **Data protection during all stages** of a typical data handling process of lifecycle: upload, process, store, deliver/visualize
  - Policies and security requirements must be bound to the data and there should be corresponding security mechanisms in place to enforce these policies
  - Secure data transfer that should be enforced with the **data activation mechanism** for Big Data
  - Data transfer mechanisms should support data partitioning and synchronization.
- **Access control infrastructure virtualisation and dynamic provisioning**, including dynamic/automated policy composition or generation.
- **Security services lifecycle management**, in particular service related metadata and properties, and their binding to the main services.
- **Security context management** during the whole security services lifecycle, including binding security context to the provisioning session and virtualisation platform
  - **Session synchronization mechanisms** that should protect the integrity of the remote run-time environment.
  - **Secure session fail-over** that should rely on the session synchronization mechanism when restoring the session.
- **Trust and key management** in provisioned on demand security infrastructure
  - Support **Dynamic Security Associations (DSA)** to provide fully verifiable chain of trust from the user client/platform to the virtual resource and the virtualisation platform.
  - **Bootstrapping** virtualised infrastructure to virtualisation platform
- **SLA management**, including initial SLA negotiation and further **SLA enforcement** at the planning and operation stages.

Security Services Lifecycle Management Model (SSLM)

A) Security Service Lifecycle Management (SSLM)

B) On-demand provisioned Service Lifecycle Management (SLM)

Specific SSLM stages and mechanisms to ensure consistency of the security context management

- **Security Service Request** that initiates creation of the dynamic security association and may use SLA security context.
- **Reservation Session Binding** with GRI (Global Reservation ID created at initial SLM stage) that provides a basis for complex security services binding including security policies enforcement
- **Deployment and Bootstrapping** stage (as part of SLM Deployment stage) that allows bootstrapping provider/platform security (creation of the trust anchors) and virtual security infrastructure
- **Registration & Runtime Binding & Synchronisation** stage (as part of the SLM Deployment stage) that allows (1) service registration; (2) binding the local resource or hosting platform run-time process ID to the GRI as a provisioning session ID; and (3) synchronisation of Operation stage processes
  - Specifically targets possible scenarios with the provisioned services migration or restoration.

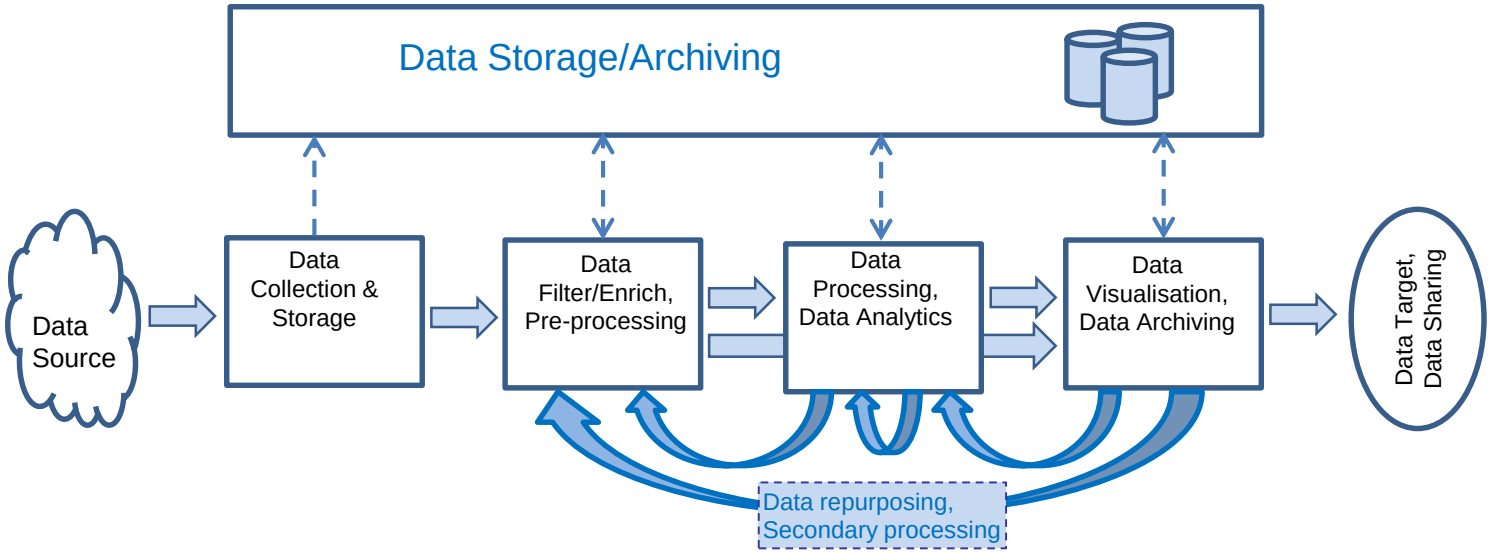
Relation between SSLM/SLM stages and supporting general and security mechanisms

SLM stages	Request	Reservation & Design/Engin.	Deployment		Operation	Decomission ing
Process/ Activity SSLM/SLM	SLA Nego tiation	Service/ Resource Composition Reservation	Composition Configuration		Orchestration/ Session Management	Logoff Accounting
			Bootstrap Sec Serv	Register/ Bind		
SSLM/SLM Mechanisms (M – mandatory; O - optional)						
GRI	**M**					**M**
SLA	**M**				(O)	**M**
Workflow		(O)			**M**	
Metadata	**M**	**M**		**M**	**M**	
Dynamic Security Association (DSA) (instant SSH keypair generation)		(O)	**M**	**M**	**M**	
AuthZ Session Context		**M**	(O)		**M**	
Logging		(O)	(O)		**M**	**M**

Practical Security Services and Mechanisms Used in Cloud

- Virtual Private Network (VPN) Virtual Private Cloud (VPC) for creating virtual cloud infrastructure for each customer
- Secure Shell (SSH) protocol
  - Instant SSH keys generation that takes place during a new account creation
    - Private/secret key must be copied/downloaded by user and securely store; CSP keeps only public linked to account, CSP doesn't store user's private key
- HTTPS and TLS/SSL protocols for secure web access and as a general secure transport protocols
- Public Key Infrastructure (PKI) that provides a basis secure communication protocols (HTTPS, TLS/SSL, SSH) PKI based credentials for entity/user identification and authentication
- Access control that includes Authentication and Authorisation and supported by Identity Management
  - Single Sign On (SSO), federation, delegation, access control policy
  - Secure Token Service (STS) using variety of STS types/formats (e.g. SAML, JSON, X.509 PKI certificates)
- Identity Management service for user accounts management
- Federated Access Control and Federated Identity Management
- Multi-tenant environment mechanisms for virtual customer environments separation
  - Virtualisation, storage and database partitioning, namespace separation, customer session identification and context management, authentication and authorization
- Key escrow to ensure restoration of encrypted data in case key held by data owner is lost

Data Lifecycle Management Model



Data Lifecycle Management (DLM) model stages typically present in majority of user applications:

- Data collection, registration and storage
- Data filtering and pre-processing
- Data processing, data analytics
- Data visualization, data archiving
- Data delivery, data sharing

Majority of scientific and business application require data storage at each transformation stage. Issues to be addressed

- Data Provenance: Data linking and traceability
- Data Deduplications: Avoid duplication of unmodified data
- Data Policy: To be applied and enforced consistently at processing and storage

Data Security and Data Lifecycle Management

- Data security solutions and supporting infrastructure should address the following problems related to the Data lifecycle
  - Secure data transfer (to be enforced with the data activation mechanism)
  - Protection of data stored on the cloud platform
  - Restore from the process failure that may entail problems related to the secure application session and data restoration
  - Data archiving and long term store (policy preservation, container and policy encapsulation)
- Data security services and mechanisms should address the following functionality related to different data management activities
  - Separation: Enable separation of processing and storage services for logically separated data sets and collections such as belonging to different tenants or users
  - Data Storage: Ensure CAP properties (Consistency, Availability, Partitioning)
    - Ensure data availability in case the data handling service goes off-line or failed
  - Transfer: Provide guarantee against compromise in data transfer/communication
  - Migration: Ensure data policy enforcement in case of data migration to another storage service provider
  - Encryption: Guarantee confidentiality and integrity for data storage and transfer

Cryptographically Enforced Data-Centric Security

- On-demand provisioned and distributed character of the cloud based infrastructure and applications, makes it practically unfeasible to achieve full protection of data at all infrastructure layers and during the whole data lifecycle, unless data remain encrypted all time.
- Currently, data could be transferred and stored in encrypted form but they must be decrypted to be processed.
- Recent achievement in developing the homomorphic encryption by Boneh and Waters (2007) made it theoretically possible to process encrypted data.
  - Current homomorphic encryption systems still have limited functionality in the sense of supported operations on data and processed data size
  - Number of academic and industry research are focused on achieving production scale and performance
- Newly developed cryptographic systems allow the following operations on encrypted data: encrypted data comparison, subset queries and arbitrary conjunction of such queries
- Currently well-developed the Identity Based Cryptography (IBC) and attribute based encryption allow combining encryption with access control where only targeted persons can access and decrypt the data.

Cloud Security Standards: NIST and US Federal

NIST Special Publications on Cloud Security include both new cloud focused standards and revised general IT security standards revised to include new cloud related aspects

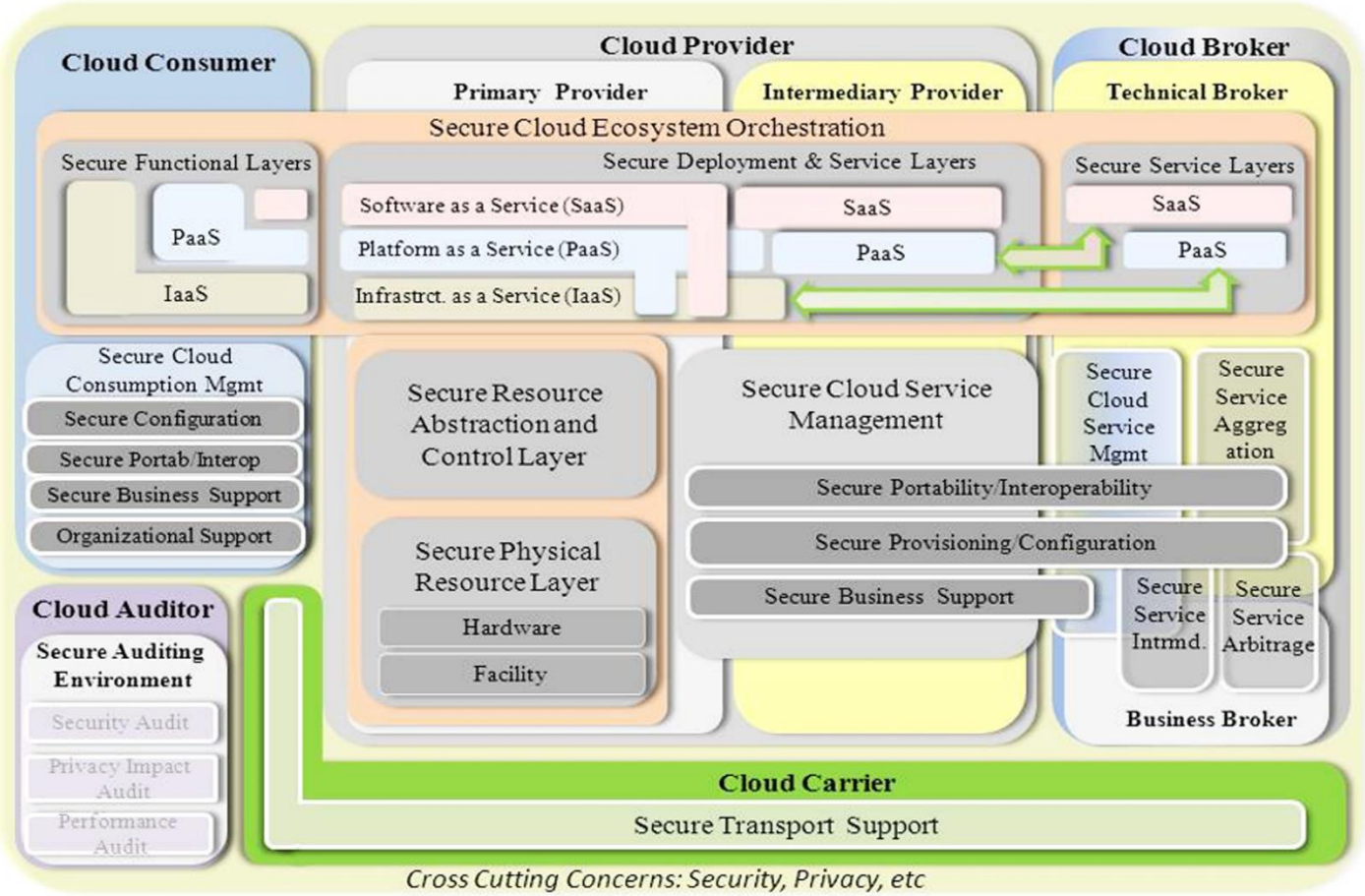
- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing.
  - http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- Draft NIST SP 500-299: NIST Cloud Computing Security Reference Architecture.
  - http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf
- NIST SP 800-125 Guide to Security for Full Virtualisation Technologies
  - http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- Federal Risk and Authorization Management Program (FedRAMP)
  - As of June 6, 2014, US federal agencies must utilize only cloud providers assessed and authorized through FedRAMP
  - Directory of Compliant Cloud Systems - http://cloud.cio.gov/fedramp/cloud-systems
    - AWS East-West US and AWS Governmental Community Cloud, SalesForce, USDA
    - Provisional Authorisation: Akamai, AT&T, IBM, Hewlett-Packard, Lockheed Martin, Microsoft Azure, Oracle

Cloud Security and Big Data Security Standards

Other standardisation bodies and organisations

- Cloud Security Alliance https://cloudsecurityalliance.org/
  - Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2013) https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/
  - Expanded Top Ten Big Data Security and Privacy Challenges. CSA Report, 16 June 2013. https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf
  - CSA Enterprise Architecture: The Security and Risk Management domain. https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/
- European Union Agency for Network and Information Security
  - ENISA Cloud Computing Risk Assessment (2010) http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
  - ENISA Threat Landscape 2013, Overview of current and emerging cyber-threats, 11 December 2013 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport
- CSA and ENISA security standards provides basis for corresponding compliance and certification profiles

NIST Cloud Computing Security Reference Architecture (NIST SP800-299 Draft)



Based on NIST Cloud Computing Reference Architecture NIST SP500-292 (CCRA).

Defines operational and management aspects of security for

- Cloud Consumer
- Cloud Provider
- Cloud Broker
- Cloud Auditor
- Cloud Carrier

Cloud security services integration steps (leveraging NIST SP800-53r4 Risk Management Framework)

1 – Categorise

2 – Identify security requirements

3 – Select architecture

4 – Assess

5 – Authorise

6 – Monitor Cloud Services

CSA3.0 Security Guidance for Critical Area of Focus in Cloud Computing

The CSA3.0 defines 13 domains of the security concerns for Cloud Computing that are divided into two broad categories

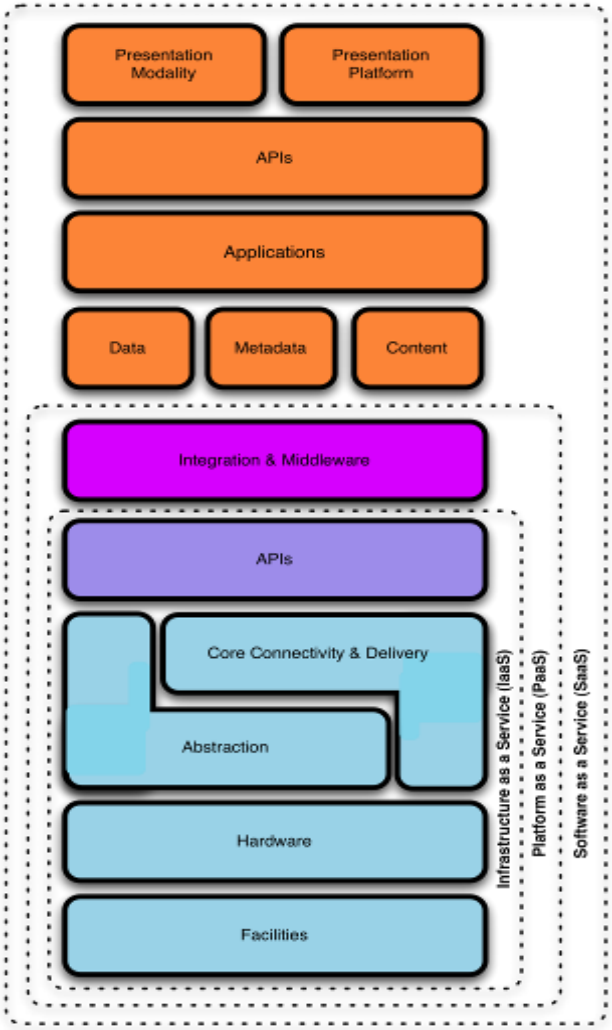
Governance domains

1. Governance and Enterprise Risk Management
2. Legal Issues: Contracts and Electronic Discovery
3. Compliance and Audit
4. Information Management and Data Security
5. Portability and Interoperability

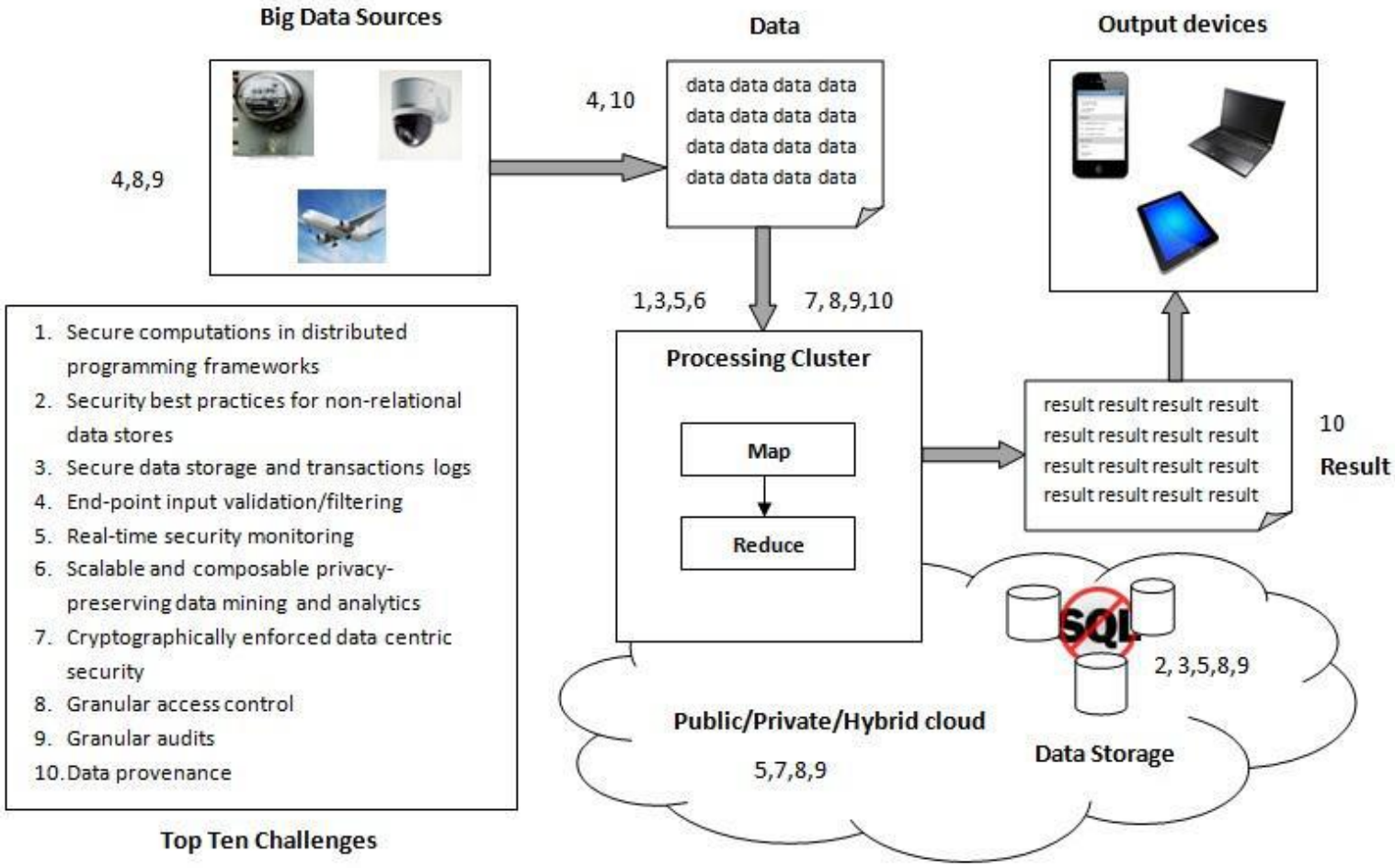
Operational Domains

6. Traditional Security, Business Continuity and Disaster Recovery
7. Data Center Operations
8. Incident Response, Notification and Remediation
9. Application Security
10. Encryption and Key Management
11. Identity and Access Management
12. Virtualization
13. Security as a Service

CSA3.0 Cloud Services Model

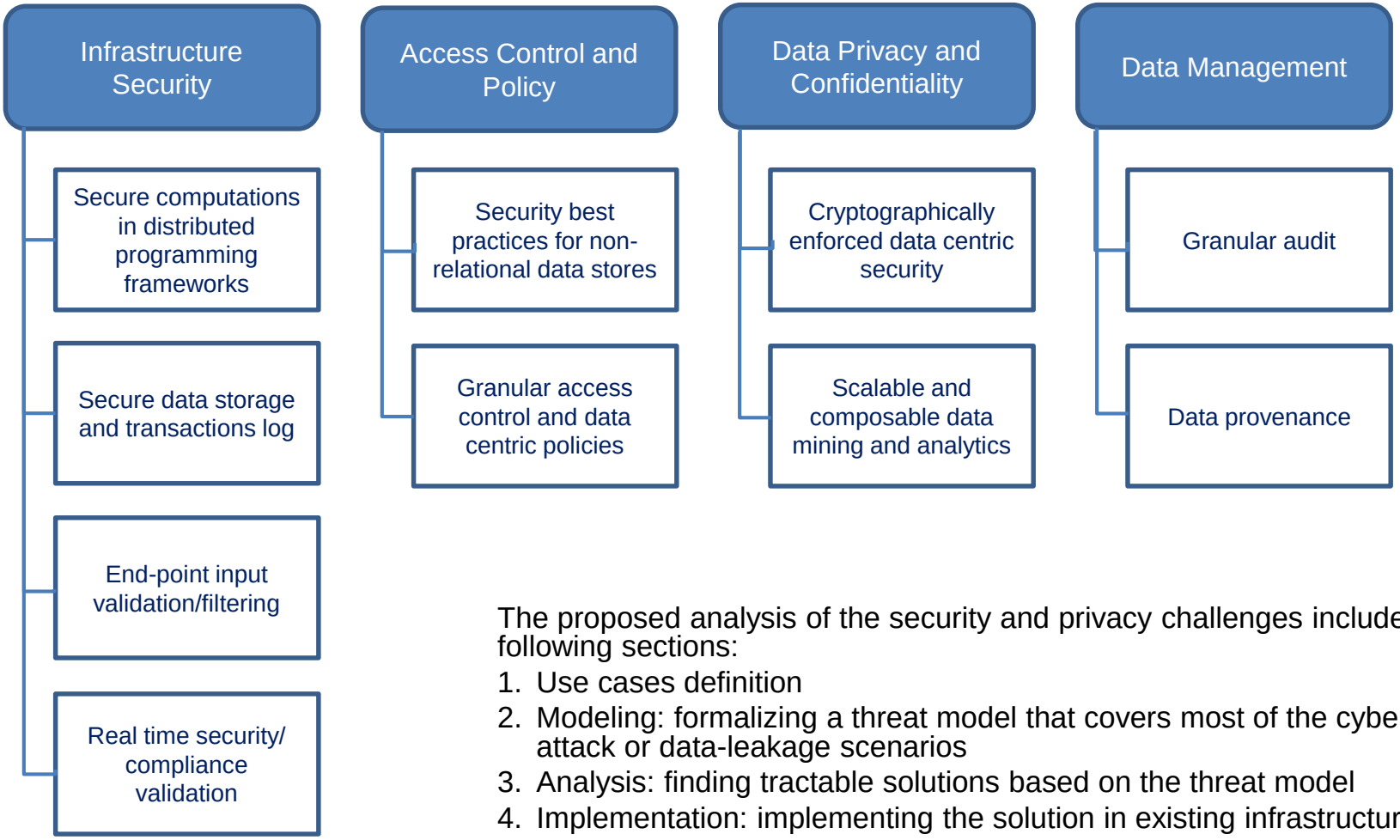


CSA Top Ten Big Data Security and Privacy Challenges



Expanded Top Ten Big Data Security and Privacy Challenges. CSA Report, 16 June 2013.
https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf

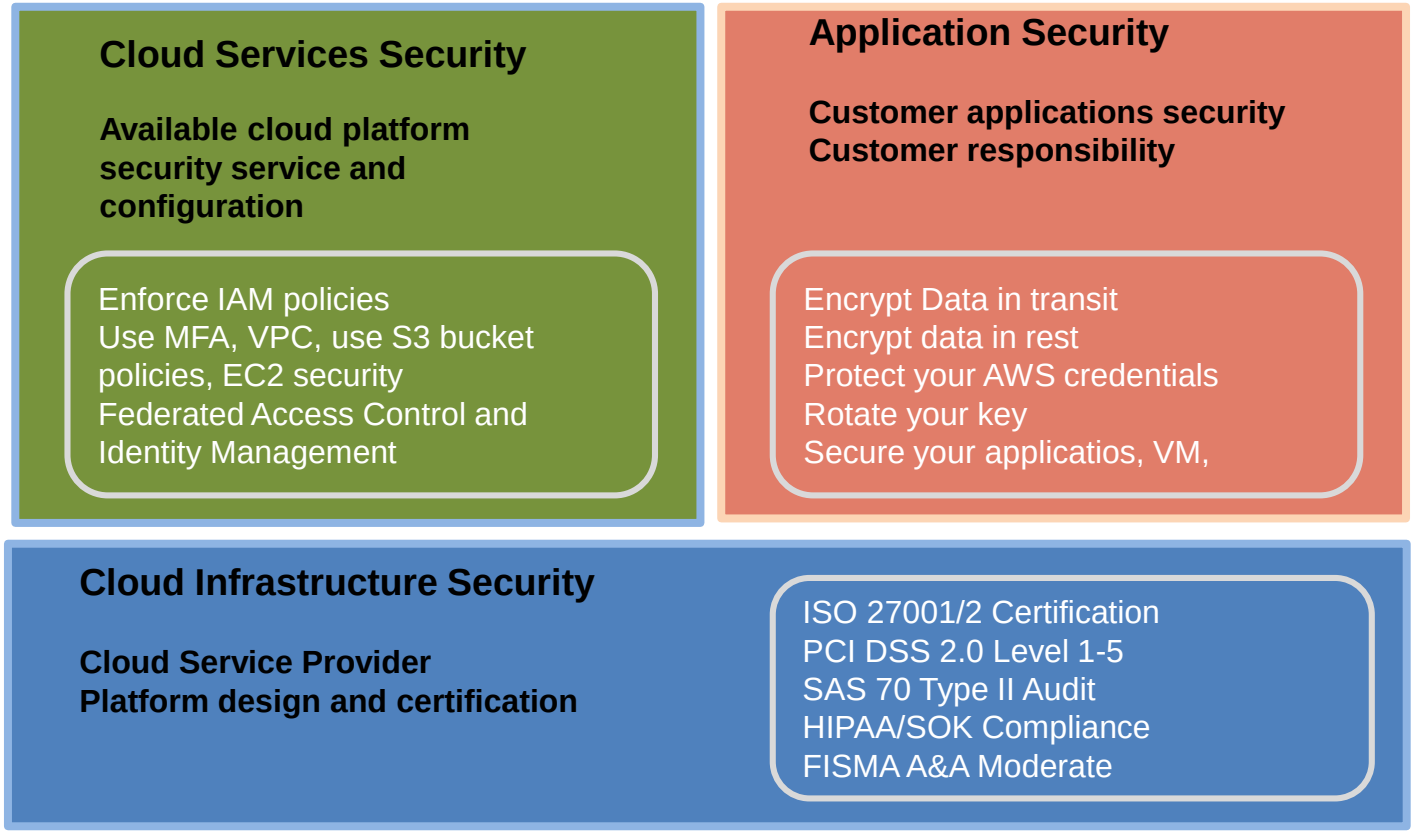
CSA Top Ten Big Data Security Challenges by Functional Groups



The proposed analysis of the security and privacy challenges includes the following sections:

1. Use cases definition
2. Modeling: formalizing a threat model that covers most of the cyber-attack or data-leakage scenarios
3. Analysis: finding tractable solutions based on the threat model
4. Implementation: implementing the solution in existing infrastructures

Amazon Web Services Security Model



Security is declared as one of critical importance to AWS cloud that is targeted to protect customer information and data from integrity compromise, leakage, accidental or deliberate theft, and deletion.

- The AWS infrastructure is designed with the high availability and sufficient redundancy to ensure reliable services operation.

AWS Security – Shared Responsibility Model

AWS implements the ***Shared Responsibility Model*** that splits responsibility for the security of different layers and components between AWS as a provider and a customer or tenant.

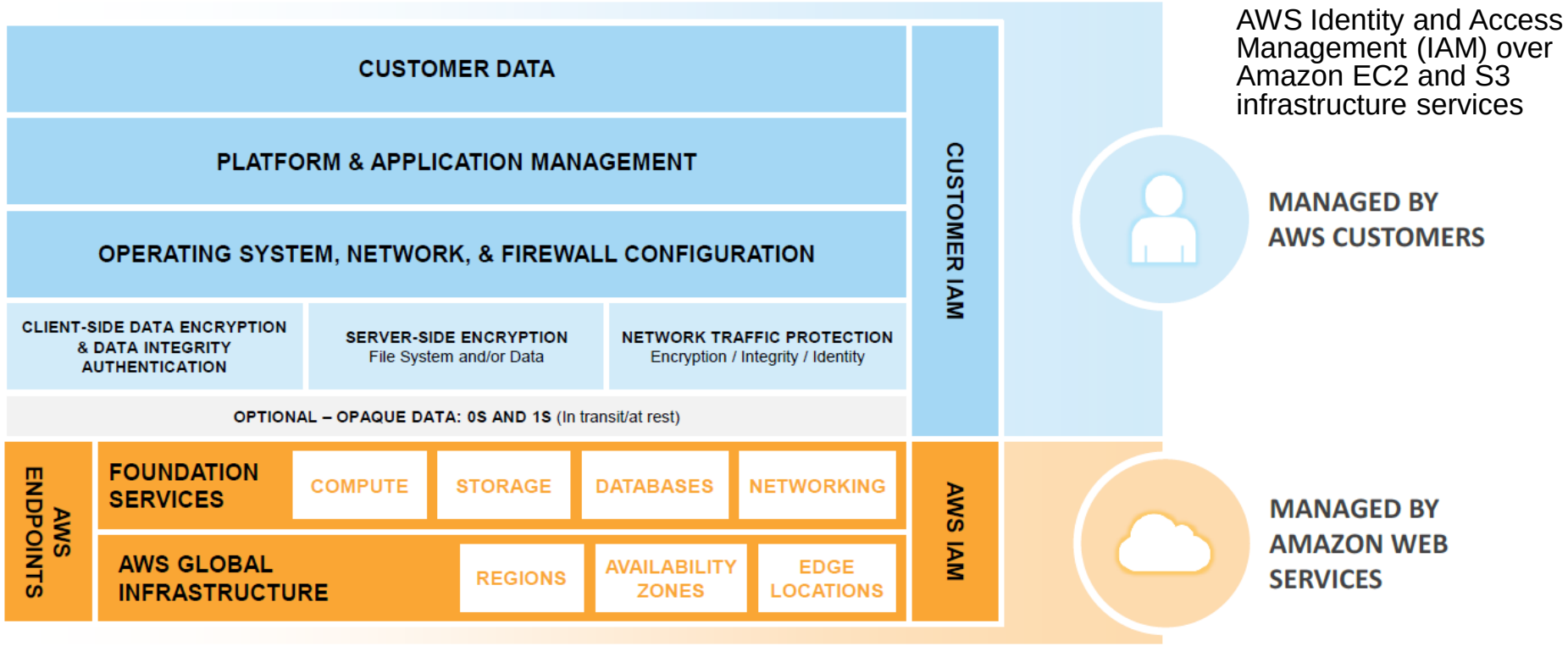
AWS as a cloud provider ensures the security of the cloud infrastructure and cloud platform services:

- Facilities
- Physical security of datacentre
- Network infrastructure
- Virtualisation platform and infrastructure

While **the customer** is responsible for security of the following components:

- Amazon Machine instances, OS, and applications
  - Note, the customer is responsible for security update and patching of the guest OS and installed applications
- Data in transit, data at rest, and data stores
- Credentials, policies and configurations
- Comply with the Acceptable Use Policy (AUP), ensure correct use of the cloud platform

Example: Security responsibility sharing in AWS IaaS infrastructure services



- For other cloud service models PaaS and SaaS the responsibility of AWS goes up to OS, network and firewall for PaaS, and also includes the application platform and container for SaaS.
  - However, the responsibility for data remains with the customer.

[ref] Todorov, D. & Ozkan, Y. (November 2013) 'AWS security best practices', Amazon Web Services [Online]. Available from: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

AWS Security Recommendations: Customer side

Recommended security best practices at each layer

- Protect your Amazon account
- Control internal access to AWS resources
- Limit external access to your cloud
- Protect data in transit and at rest
- Secure data assets
- Secure your compute assets (OS, instances, App)
- Backup for easy recover
- Keep track of your cloud resources (using monitoring service)

Security methods for customer cloud infrastructure

- Virtual Private Cloud (VPC) to create a secure environment for your cloud services in AWS
- Security zoning and network segmentation based on security groups, Network Access Control Lists, host based firewalls
- Network security and secure access for users and applications
- Threats protection layer in traffic flow to ensure protection against Denial of Service (DoS) attacks

[ref] D.Todorov, Y.Ozkan. AWS Security Best Practices. November 2013 [online] http://bit.lu/aws- security-best-practices-new

Security in Amazon EC2 and S3

Amazon Elastic Compute Cloud (Amazon EC2) Security implements

- Multiple levels of security including Guest Operating System, Firewall, API to manage VM instances
- Hypervisor that is a customised version of the Xen hypervisor allows running processes in four privilege modes: host OS is executed Ring 0; guest OS runs in Ring 1, applications run in Ring 3.
- Instances isolation is also provided by hypervisor that forwards all communication for instances via virtual firewall that resides in the hypervisor layer.
  - Such approach ensures that communication paths of instances never intersect.
- Instant SSH keys generation for individual users and groups

Amazon Simple Storage Service (Amazon S3) Security

- S3 storage is accessed via SSL protocol
- Data security in rest is provided by encryption and multi-layer physical security
- AWS adopts a secure and reliable technique for storage device decommissioning

AWS Identity and Access Management (IAM)

AWS IAM provides functionality to securely control access to AWS services and resources for individual users and groups by defining individual and group permissions and policies.

- Manage **IAM users and their access**: Create AIM users and assign them individual security credentials (i.e., access keys, passwords, and multi-factor authentication devices) to provide users access to the AWS Management Console, APIs, services and resources.
  - Create multiple users and groups for the same AWS account/customer
  - Manage permissions in order to control which operations a user can perform.
  - Use customizable URL for accessing AWS Management Console for user groups
    - https://gocxfed.signin.aws.amazon.com/console where "gocxfed" is a group name
- Manage IAM **roles and their permissions**: Create roles and manage permissions to control which operations can be performed by the entity, or AWS service that assumes the role.
- Manage **federated users and their permissions**: Enable identity federation to allow existing identities (e.g. users) in customer enterprise to access the AWS services and resources, without the need to create an IAM user for each identity.
- Enable **Multi-Factor Authentication (MFA)** that augments username and password credentials
  - MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.

Example: Multi-layer Security in AWS

Security Layers are defined similar to 3 Tier Model:

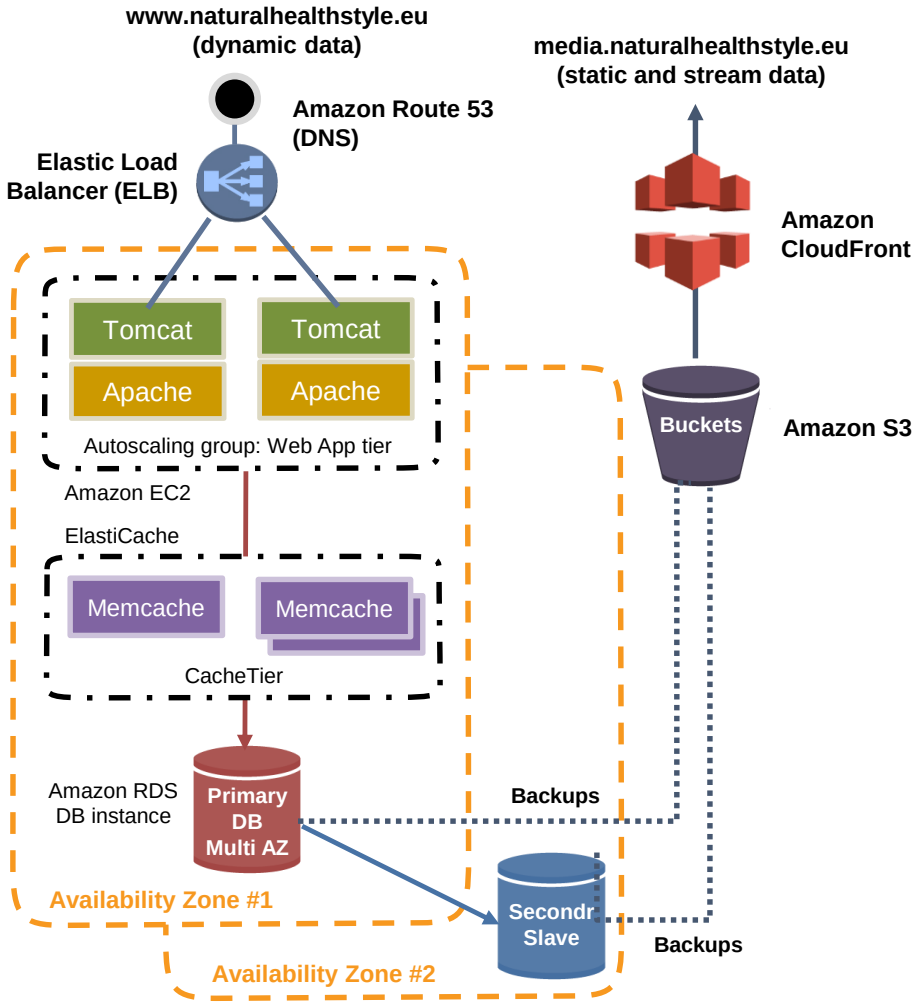
- Presentation/Front end
- Applications
- Data/Database

#Permit HTTP(S) access to Web Layer
From entire Internet
ec2auth Web –p 80, 443 –s 0.0.0.0/0

#Permit Web Layer access to App Layer
ec2auth App –p 8000 –o Web

#Permit App Layer access to DB
ec2auth DB –p 3209 –o App

#Permit admin access SSH to all three layers
First allow connection from office to Web tier, and from there to the other layers
ec2auth Web –p 22 -s <e.g. office network>
ec2auth App –p 22
ec2auth DB –p 22



Microsoft Azure Cloud Security

Microsoft Azure Cloud is built with the security in mind

- Microsoft has long term experience in developing security applications and running large scale service (e.g., Hotmail, MSDN, MSN, Windows Live).
- Azure cloud design claims to follow the widely recognised Microsoft Secure Software Development Lifecycle (SSDL)

SSDL = Security and Privacy by Design

Three components of the cloud environment security

- Cloud infrastructure security
  - Datacenter security, trustworthy design, secure operational procedures
  - Certification and compliance
- Cloud platform security services
  - Serving both platform security and integration with the customer applications
  - Access control, security policies, customer controlled security services
  - Data protection: cloud platform and user controlled
- Customer/tenants applications security
  - Application level access control, security policies
  - Federation with the tenants/users organizational access control

Microsoft Azure Cloud Security Services

Azure Security Services from both the customer's and provider's operational perspectives:

- Federated identity and access management based on Microsoft accounts or organizational accounts, enabled by **Azure Active Directory Service (AADS)**
- Use of mutual SSL authentication.
- Component isolation through a layered environment.
- Virtual Machine state maintenance and configuration integrity.
- Storage redundancy to minimize the impact of hardware failures.
- Monitoring, logging, and reporting on administrative actions.

Built-in data protection

- Control access to customer data and applications
  - Identity and access control with Active Directory based federated access control and Identity Management
- Protect data in transit and at rest
  - Data encryption and isolation
  - Data destruction following string industry standards
- Dedicated network connectivity with Azure ExpressRoute

Microsoft Azure Cloud Security Design Principles

1. SSL mutual authentication for internal control traffic is used for all communications between internal components in Azure cloud.
2. Certificate and private key management is done via a separate mechanism using SMAPI (Service Management API) than code that uses them to avoid key exposure to developers and administrators.
3. Least privilege principle is applied to running customer service on cloud
4. Access control model in Microsoft Azure Storage allows creating one or more accounts and using different accounts to access data of different levels of security.
5. Isolation of hypervisor, Root OS, and Guest VMs is provided by the advanced features of Microsoft Hyper-V hypervisor.
6. Isolation of Fabric Controller (FC) is achieved by implementing secure unidirectional communication between FC and Fabric Agents (FA): FA replies only to FC requests, FA cannot communicate to FC.
7. Packets filtering is implemented at the level of Hyper-V hypervisor to prevent VM of receiving traffic not addressed to them (similar to AWS Xen hypervisor firewalling).
8. VLANs and network segmentation provides isolation between segments that are connected via routers that don't forward not addressed traffic between VLANs.
9. Isolation of customer access is achieved by having a separate management and application networks including using separate Network Interface Cards (NIC) on physical servers
10. Deletion of Data in Microsoft Azure is designed to be instantly consistent: when user executes delete operation all reference to these data are removed and they cannot be accessed via storage API.

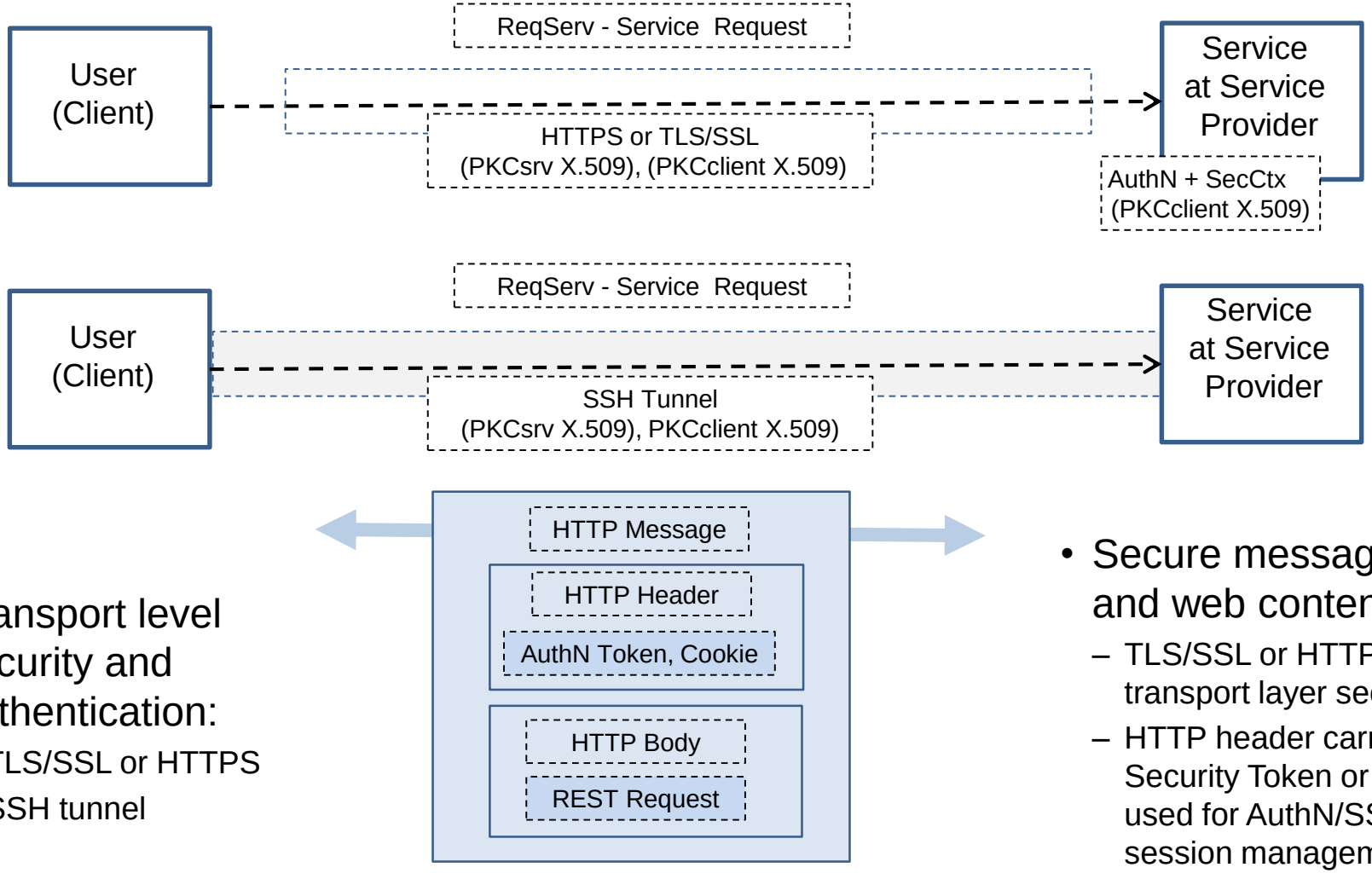
Microsoft Azure Security Controls and Capabilities

- Zero standing privileges
  - Access to customer data by Microsoft operations and support personnel is denied by default.
- Isolation
  - Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users
- Azure Virtual Networks and Encrypted communications
  - ExpressRoute private connection to Azure datacenters to keep traffic off the public Internet
- Data encryption
  - Azure offers a wide range of encryption capabilities up to AES-256
- Identity and access
  - Azure Active Directory enables customers to manage access to Azure, Office 365 and other cloud apps
  - Multi-Factor Authentication and access monitoring offer enhanced security.
- Monitoring and logging
- Patching and Antivirus/Antimalware protection
- Intrusion detection and prevention systems
  - Denial of service attack prevention, regular penetration testing, and forensic tools

Part 2: Federated Access Control and Identity Management in Cloud

- Generic Authentication and Authorisation (AAI) models
- Federated Access Control and Identity Management models and mechanisms
  - OAuth2.0, Shibboleth, OpenID, SAML
- Cloud federation models
  - Client side federation and Provider side federation
- AWS Identity and Access Management (IAM)
- Microsoft Azure Active Directory (AAD)

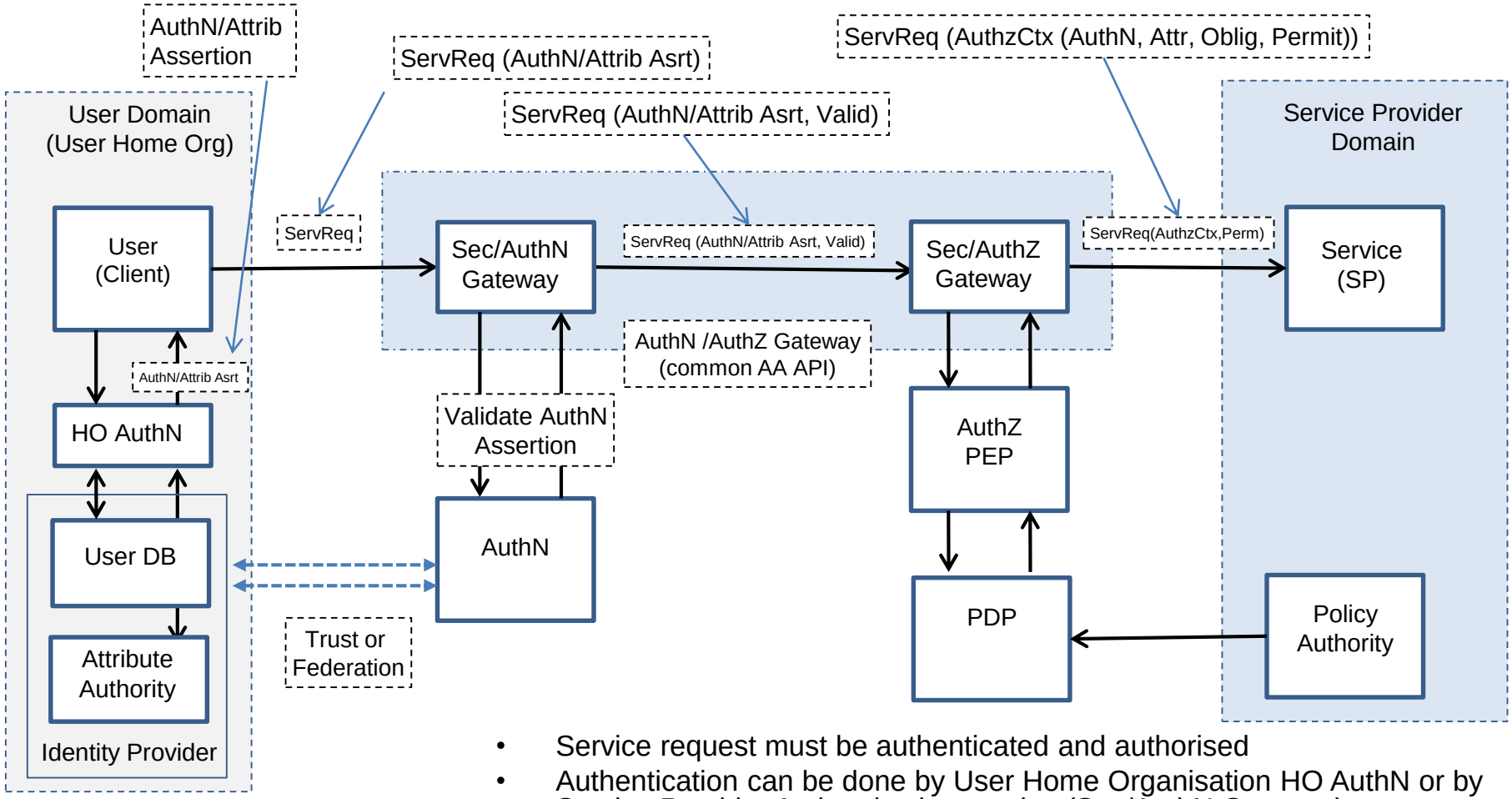
Accessing/Requesting Remote Service: Transport Level Security



- Transport level security and authentication:
  - TLS/SSL or HTTPS
  - SSH tunnel

- Secure messaging and web content
  - TLS/SSL or HTTPS as transport layer security
  - HTTP header carry Security Token or cookie used for AuthN/SSO and session management SecCtx

AuthN by User Home Organisation Service



- Service request must be authenticated and authorised
- Authentication can be done by User Home Organisation HO AuthN or by Service Provider Authentication service (Sec/AuthN Gateway)
- User identity is managed by Identity Provider
- Services and applications require session management and Security Context exchange during session

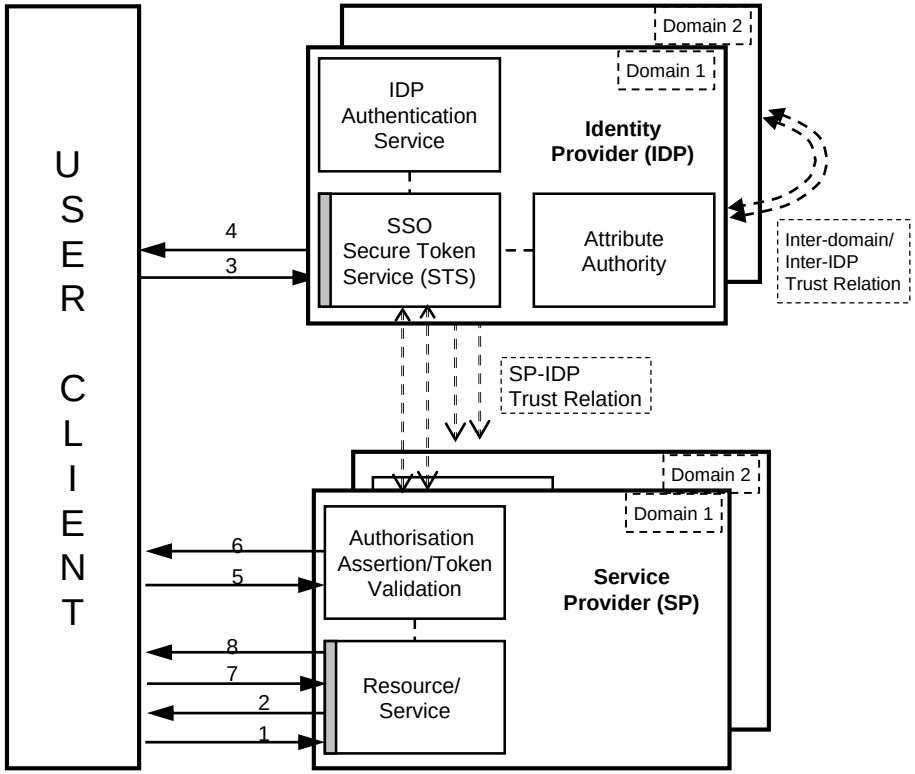
User or Service Request Authentication

- Two options to perform authentication
  - By Service Provider (SP)
    - Authentication is requested after receiving Service Request
    - SP AuthN service request user identity and attribute information from user HO
  - By user Home Organisation (HO) – Federated model
    - User obtains AuthN and Attribute assertions in advance from HO and include it in the Service Request
    - SP AuthN service validates AuthN and Attribute assertions
- User identity information is extracted from the Service Request (ServReq)
  - Username, Password as a simplest option
  - PKI based message authentication (digitally signed message)
- In case of positive authentication
  - AuthN assertion (AuthnAssert) is issued by Identity Provider (IDP)
  - Attribute assertion (AttrAssert) is issued by Attribute Authority Service (AAS)
  - All assertions need to be integrity protected and include IDP and AAS credentials

Authorisation

- Generic Authorisation model includes 3 basic functions or components
  - Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Authority Point (PAP)
- PEP receives AuthZ related information from AuthZ/Security gateway
- PEP creates Authorisation Request and sends it to PDP
  - PEP checks validity of the provided AuthN and Attribute assertions (AuthN context)
    - PDP retrieves policy from PAP and evaluates request, and makes decision – Permit, Deny or conditional Permit/Deny
  - PDP typically has standard implementation and uses specific policy language, e.g. XACML
- PEP in case of Permit
  - Either simply relies ServReq or creates AuthZ assertion containing AuthZ context

General Federated Access Control Model



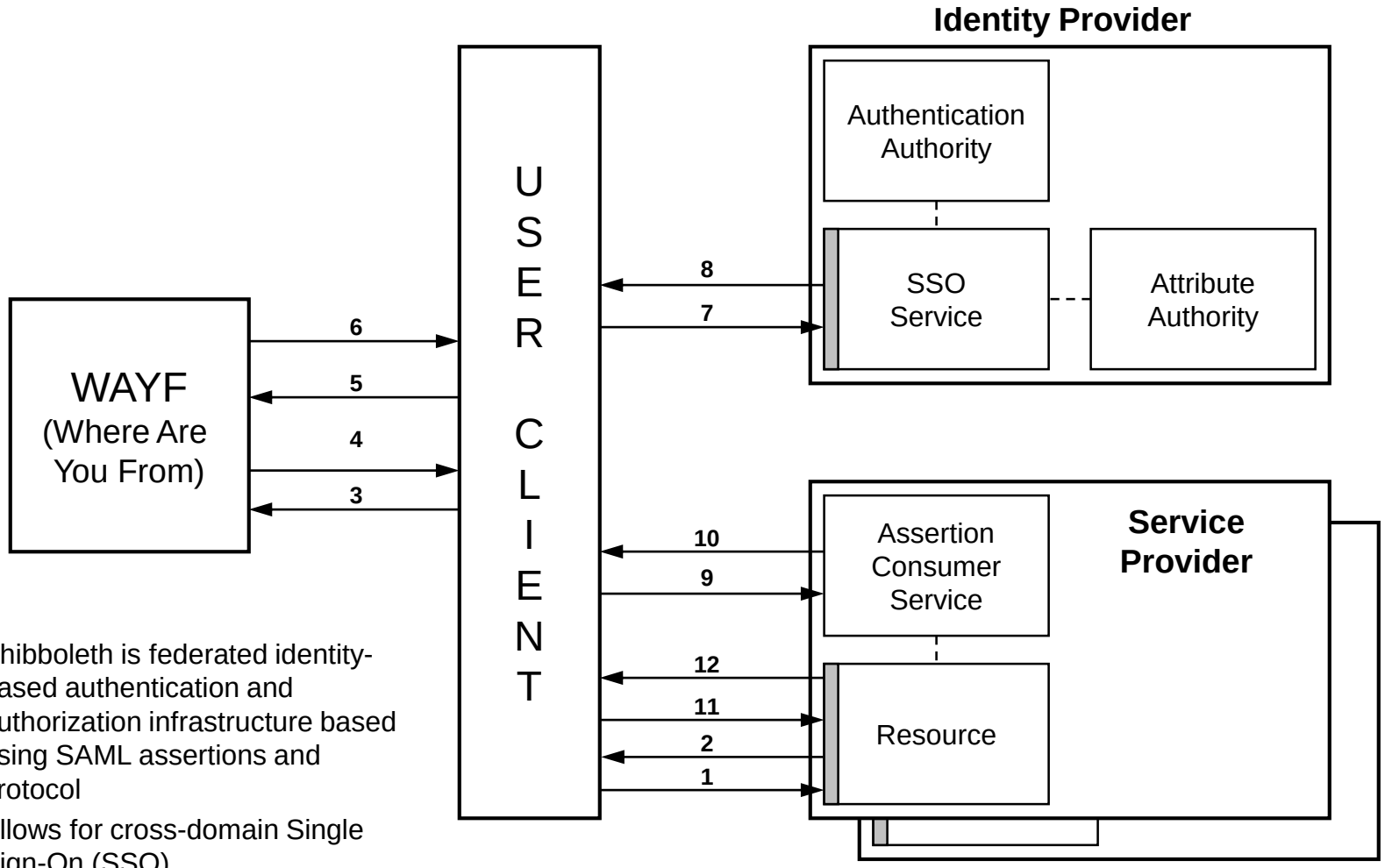
General identity federation and federated access control sequences and trust relations:

- Trust relation exists between a SP and IDP in the same domain
- For federated access control and identity provisioning, there must trust relations established between IDPs in different domains.
- Trust relations in federation mean that that the federation members trust each other assertions and will accept each other security/authentication tokens as valid.

The following steps usually take place during the federated access control:

- 1 – Client/user requests access to a resource or service
- 2 – Service Provider replies with the list of trusted IDPs and/or Authentication services (AuthN)
- 3, 4 – Client authenticates to the trusted IDP and obtains an Authentication assertion (AuthnAssert) or a Secure Token (ST);
  - E.g. web cookie for browser based client
- 5, 6 – Client presents AuthnAssert or ST/cookie to the Service Provider's Authorisation service that validates presented credentials and evaluates the request against the access control policy.
  - Decision Permit or Deny
  - Authorisation service may issue an Authorisation assertion (AuthzAssertion)
- 7, 8 – Client presents AuthzAssertion to the Resource and gets access to it.

Example Sequence SSO + IDP (multi-domain): Shibboleth Operation with WAYF Service

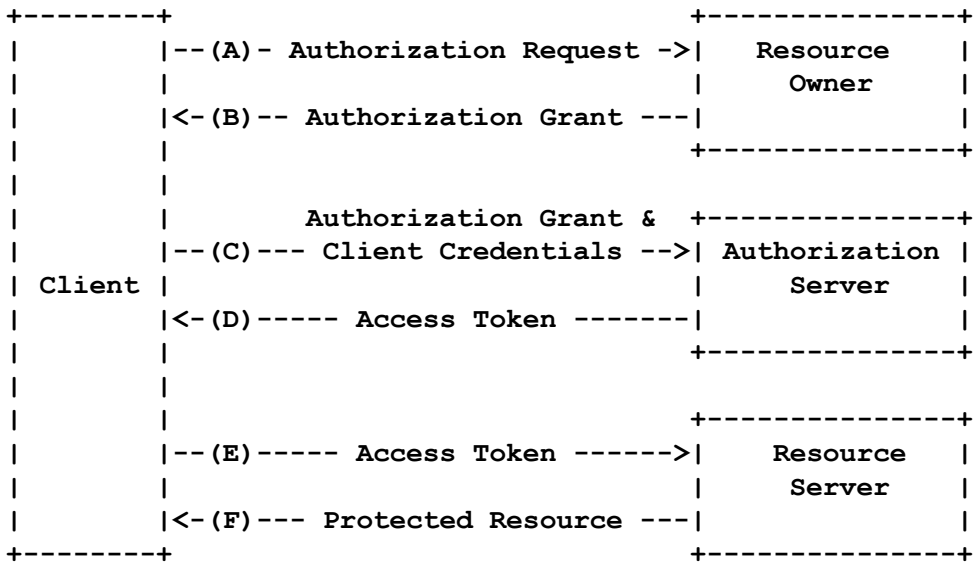


- Shibboleth is federated identity-based authentication and authorization infrastructure based using SAML assertions and protocol
- Allows for cross-domain Single Sign-On (SSO)

OAuth2.0 – Open Authentication Protocol

Functionally OAuth2.0 is the Authorisation and Delegation Protocol

- RFC6749 The OAuth 2.0 Authorization Framework http://tools.ietf.org/rfc/rfc6749.txt
- Initially proposed by Facebook, currently also implemented in Windows 8



(A) The client requests authorization from the resource owner.
  - The authorization request can be made directly to the resource owner, or preferably indirectly via the authorization server as an intermediary.

(B) The client receives an authorization grant, which is a credential representing the resource owner's authorization, expressed using one of four grant types defined in this specification or using an extension grant type.
  - The authorization grant type depends on the method used by the client to request authorization and the types supported by the authorization server.

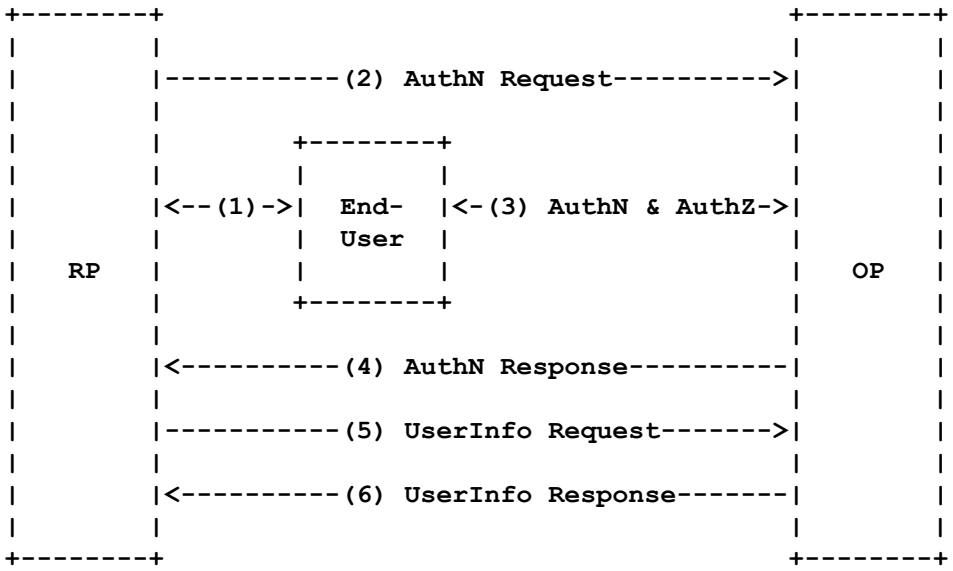
(C) The client requests an access token by authenticating with the authorization server and presenting the authorization grant.

(D) The authorization server authenticates the client and validates the authorization grant, and if valid, issues an access token.

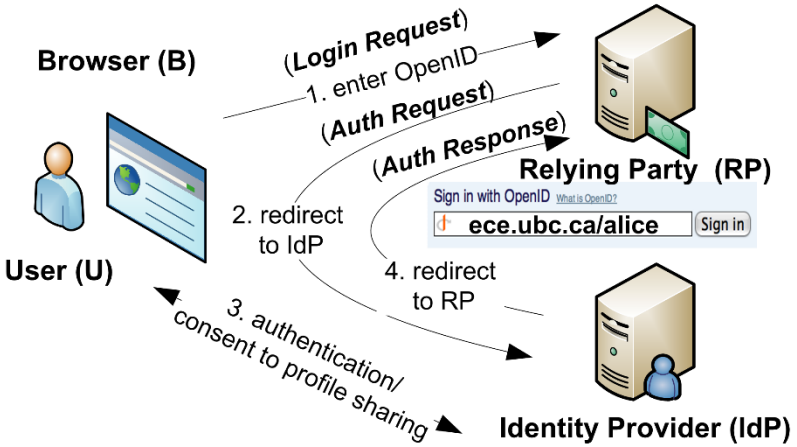
(E) The client requests the protected resource from the resource server and authenticates by presenting the access token.

(F) The resource server validates the access token, and if valid, serves the request.

OpenID Connect Protocol



[ref] http://openid.net/specs/openid-connect-core-1_0.html

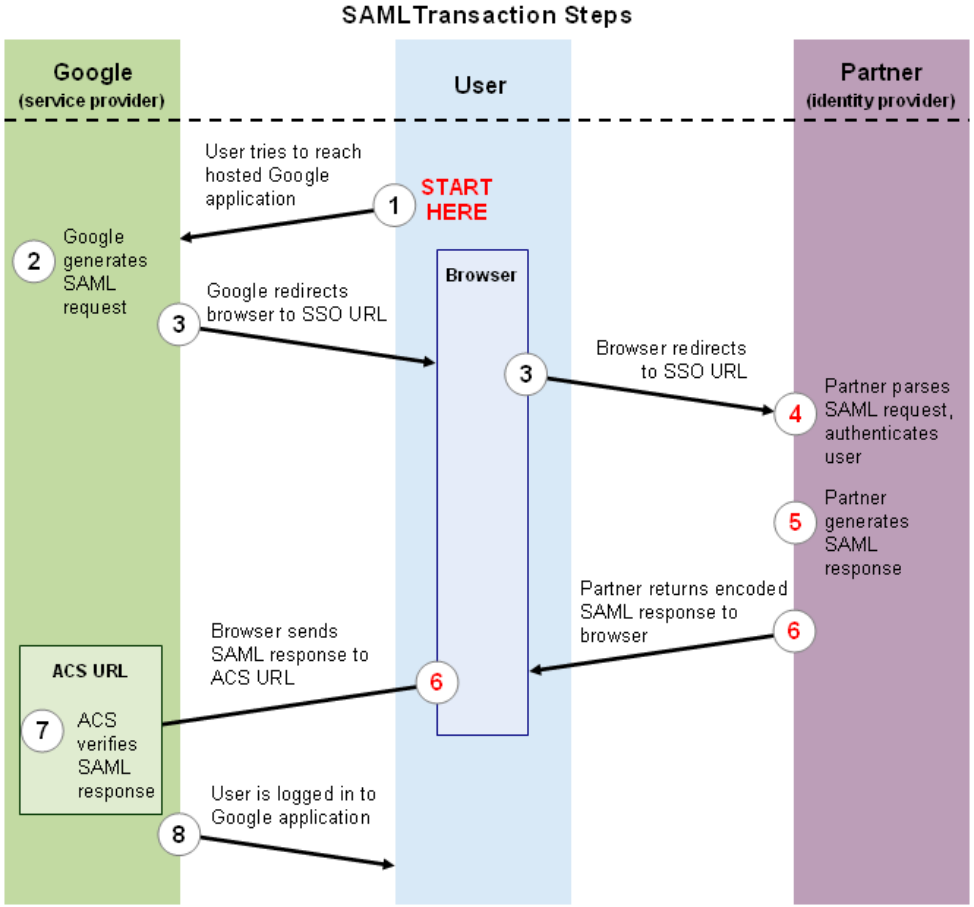


[ref] http://konstantin.beznosov.net/professional/archives/241

OpenID Connect protocol sequence

1. User send OpenID URL to Relying Party (RP) in order to access service
2. The RP (Client) sends a request to the OpenID Provider (OP).
3. The OP authenticates the End-User and obtains authorization.
4. The OP responds with an ID Token and usually an Access Token.
5. The RP can send a request with the Access Token to the UserInfo Endpoint.
6. The UserInfo Endpoint returns Claims about the End-User.

SAML Assertions and Federation Protocol



OASIS SAML specification defines SAML Security Assertion and SAML protocol to exchange security assertions during Authentication and Authorisation

- SAML defines 3 types of assertions: Authentication, Authorisation, Attribute
- SAML Protocol defines binding to HTTP and SOAP protocols
- SAML assertions can be communicated as browser cookie

Example illustrates using SAML protocol to obtain SAML based access token from the trusted Identity Provider for Google Apps

- Requires off-line established trust between Service Provider (Relying Party) and Identity Provider

Cloud Federation – Scaling up and down

- Scalability is one of the main cloud feature
  - To be considered in the context of hybrid cloud service model
    - Cloud burst and outsourcing enterprise services to cloud
    - Cloud services migration and replication between CSP
- Scaling up
  - Identities provisioning
  - Populating sessions context
- Scaling down
  - Identity deprovisioning: Credentials revocation?
  - Sessions invalidation vs restarting
- Initiated by provider and by user/customer

Federation in Grid and Clouds: Grid VO vs Cloud Virtual Infrastructure

- Grid federates resources and users by creating Virtual Organisations (VO)
  - VO membership is maintained by assigning VO membership attributes to VO resources and members
  - Resources remain under control of the resource owner organisation Grid Centers
  - Users remain members of their Home Organisations (HO)
    - AuthN takes place at HO or Grid portal
    - To access VO resources, VO members need to obtain VOMS certificate or VOMS credentials
- In clouds, both resources and user accounts are created/provisioned on-demand as virtualised components/entities
  - User accounts/identities can be provisioned together with access rights to virtual resources

Cloud Federation: Actors and Roles

- Cloud Service Provider (CSP)
- Cloud Customer (organisational)
  - Multi-tenancy is provided by virtualisation of cloud resources provided to all/multiple customers
- Cloud User (end user)
- Cloud (Service) Broker
- Identity Provider (IDP)
- Cloud Carrier
- Cloud Service Operator
- Cloud Auditor

Cloud Federation – Scaling up and down

- Scalability is one of the main cloud feature
  - To be considered in the context of hybrid cloud service model
    - Cloud burst and outsourcing enterprise services to cloud
    - Cloud services migration and replication between CSP
- Scaling up
  - Identities provisioning
  - Populating sessions context
- Scaling down
  - Identity deprovisioning: Credentials revocation?
  - Sessions invalidation vs restarting
- Initiated by provider and by user/customer

Cloud Federation Models – Identified models

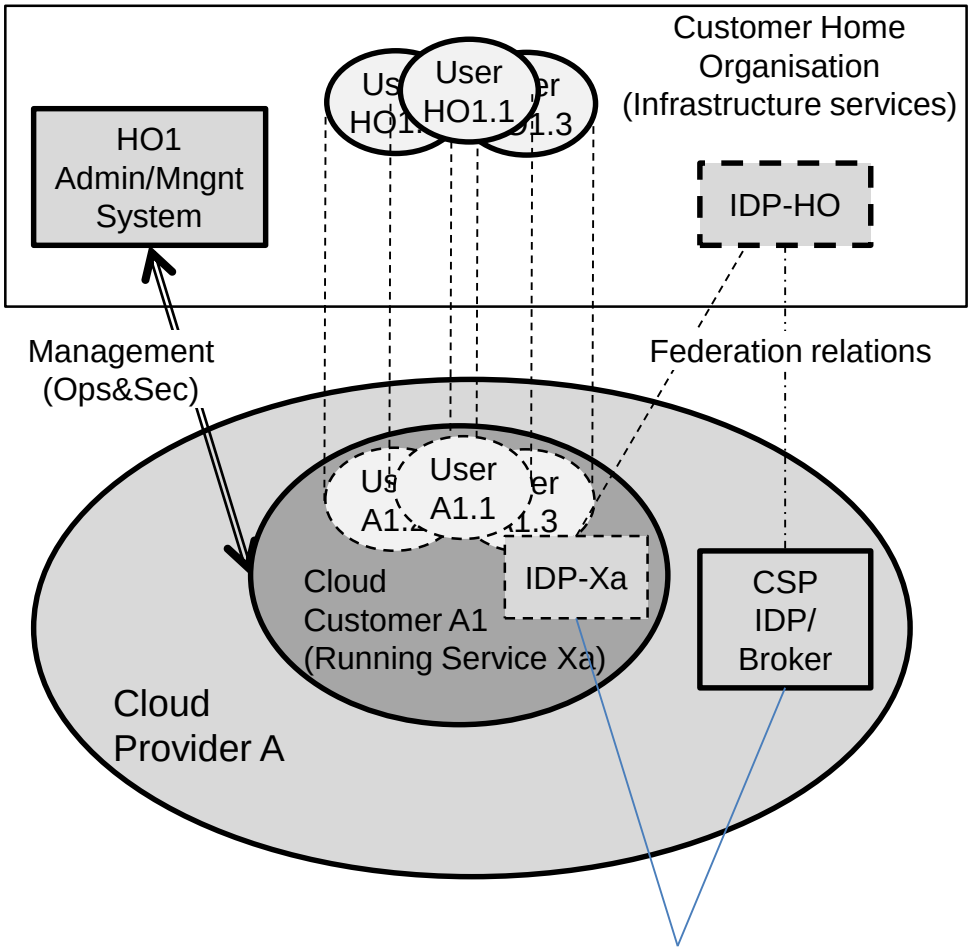
User/customer side federation

- (1.1) Federating users/HO and CSP/cloud domains
  - Customer doesn't have own IDP (IDP-HO)
  - Cloud Provider's IDP is used (IDP-CSP)
- (1.2) Federating HO and CSP domains
  - Customer has own IDP-HO1
  - It needs to federate with IDP-CSP, i.e. have ability to use HO identities at CSP services
- (1.3) Using 3rd party IDP for external users
  - Example: Web server is run on cloud and external user are registered for services

Provider (resources) side federation

- (2.1) Federating CSP's/multi-provider cloud resources
  - Used to outsource and share resources between CSP
  - Typical for community clouds

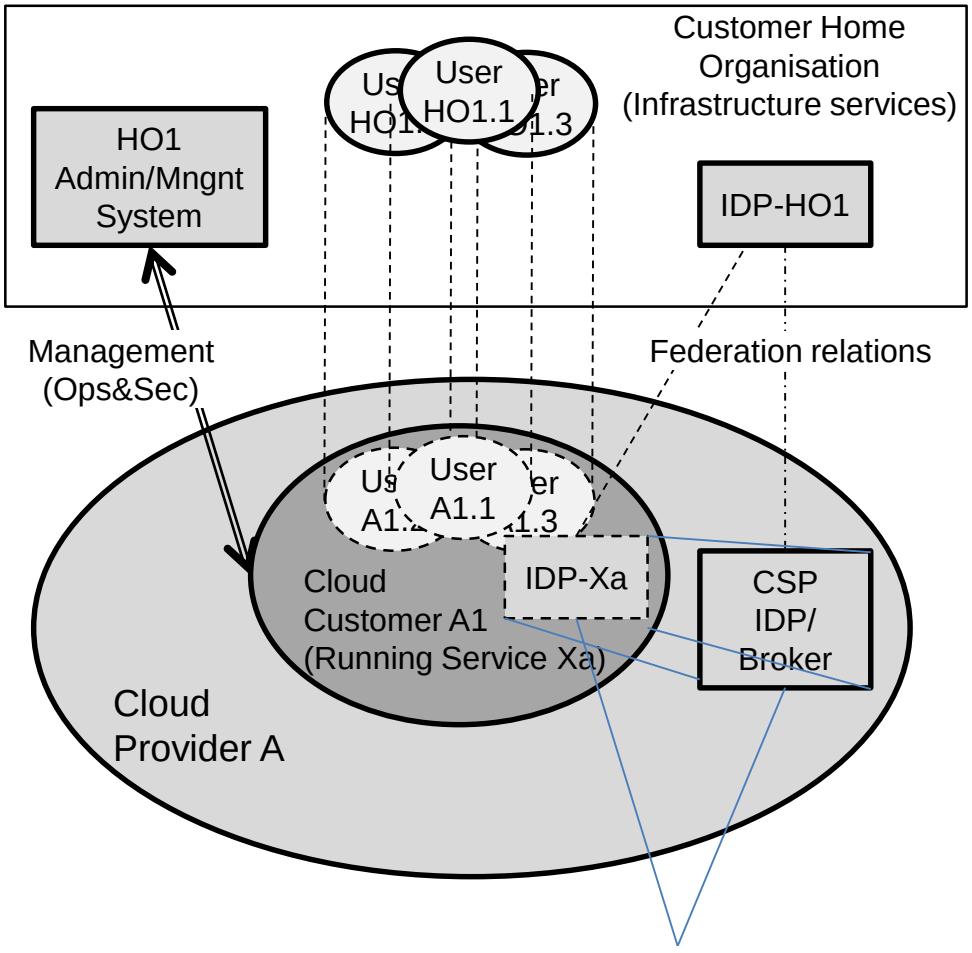
Basic Cloud Federation model (1.1) – Federating users/HO and CSP/cloud domains (no IDP-HO)



User side Federation

- Simple/basic scenario 1: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for users from HO1 and managed by HO1 Admin/Management system
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those created for Service Xa

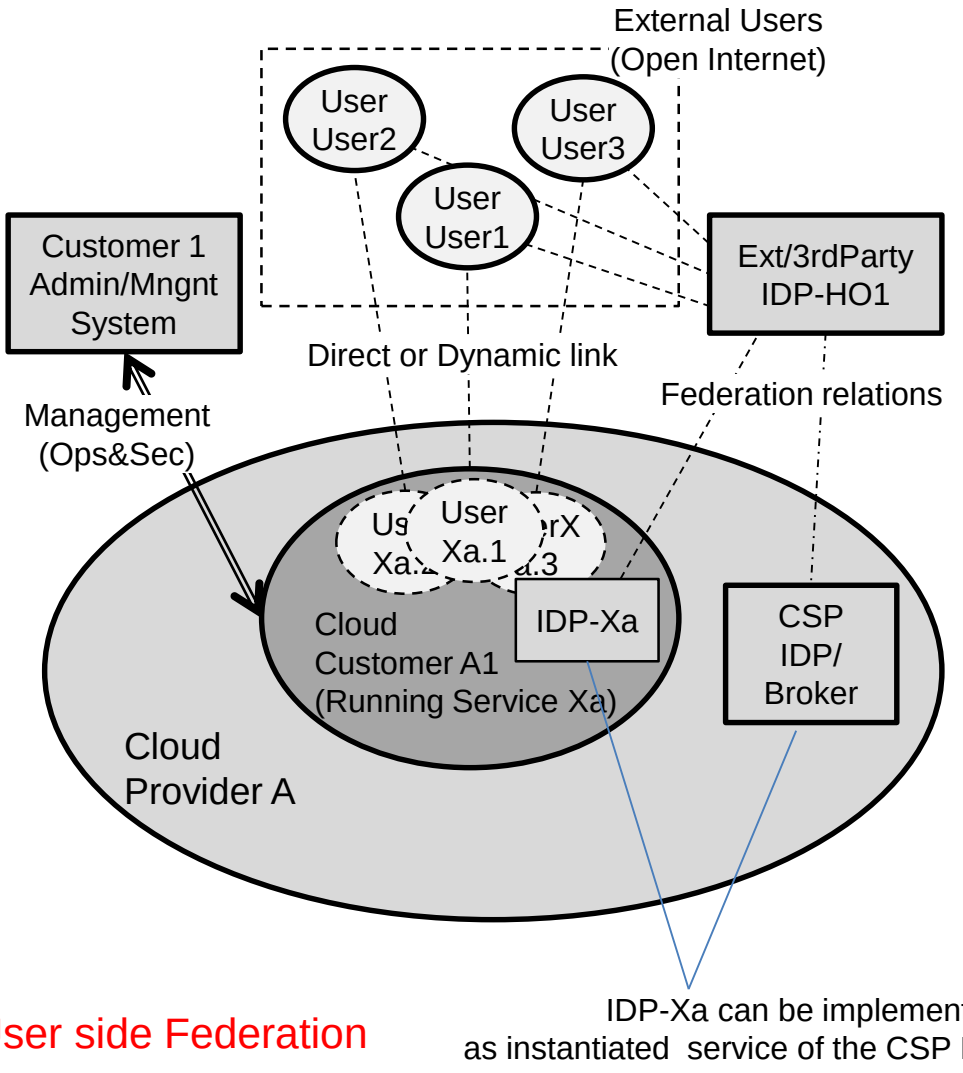
Basic Cloud Federation model (1.2) – Federating HO and CSP domains (IDP-HO1 and IDP-CSP)



User side Federation

- Simple/basic scenario 1: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for users from HO1 and managed by HO1 Admin/Management system
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those created for Service Xa

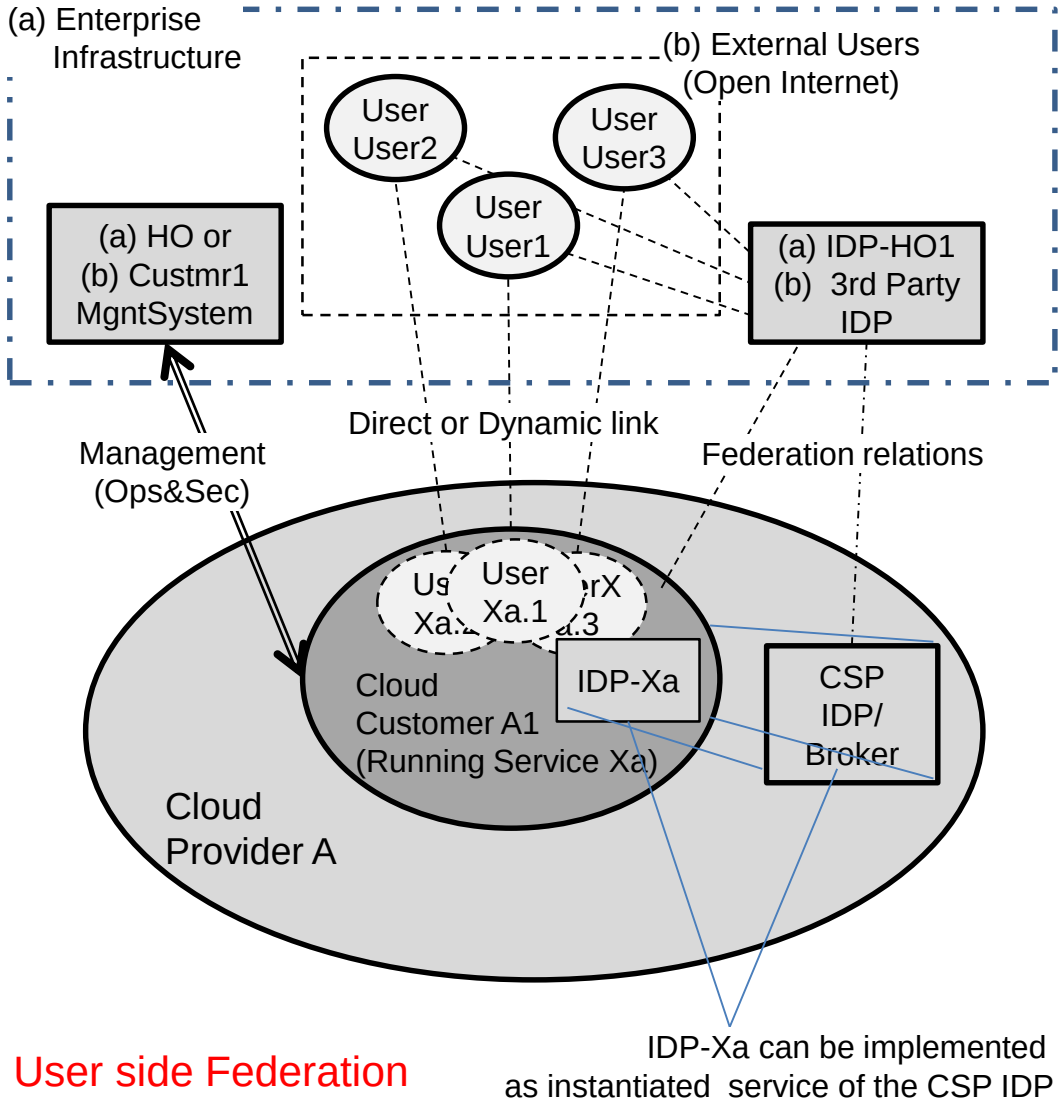
Basic Cloud Federation model (1.3) – Using 3rd party IDP for external users



User side Federation

- Simple/basic scenario 2: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for external users (e.g. website) and managed by Customer 1
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those IDP-Xa created for Service Xa

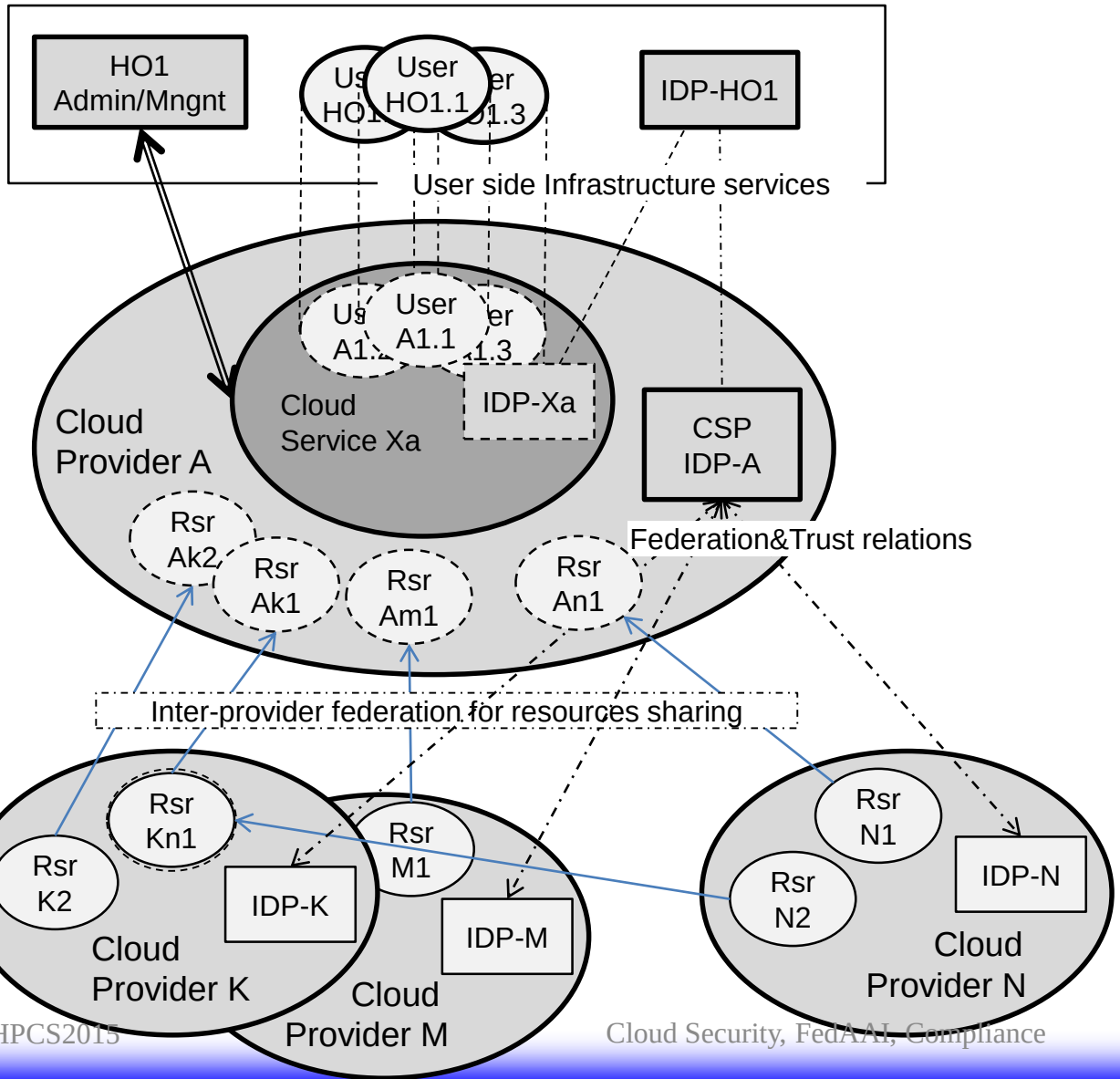
Basic Cloud Federation model – Combined User side federation



User side Federation

- Simple/basic scenario 2: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for external users (e.g. website) and managed by Customer 1
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those IDP-Xa created for Service Xa

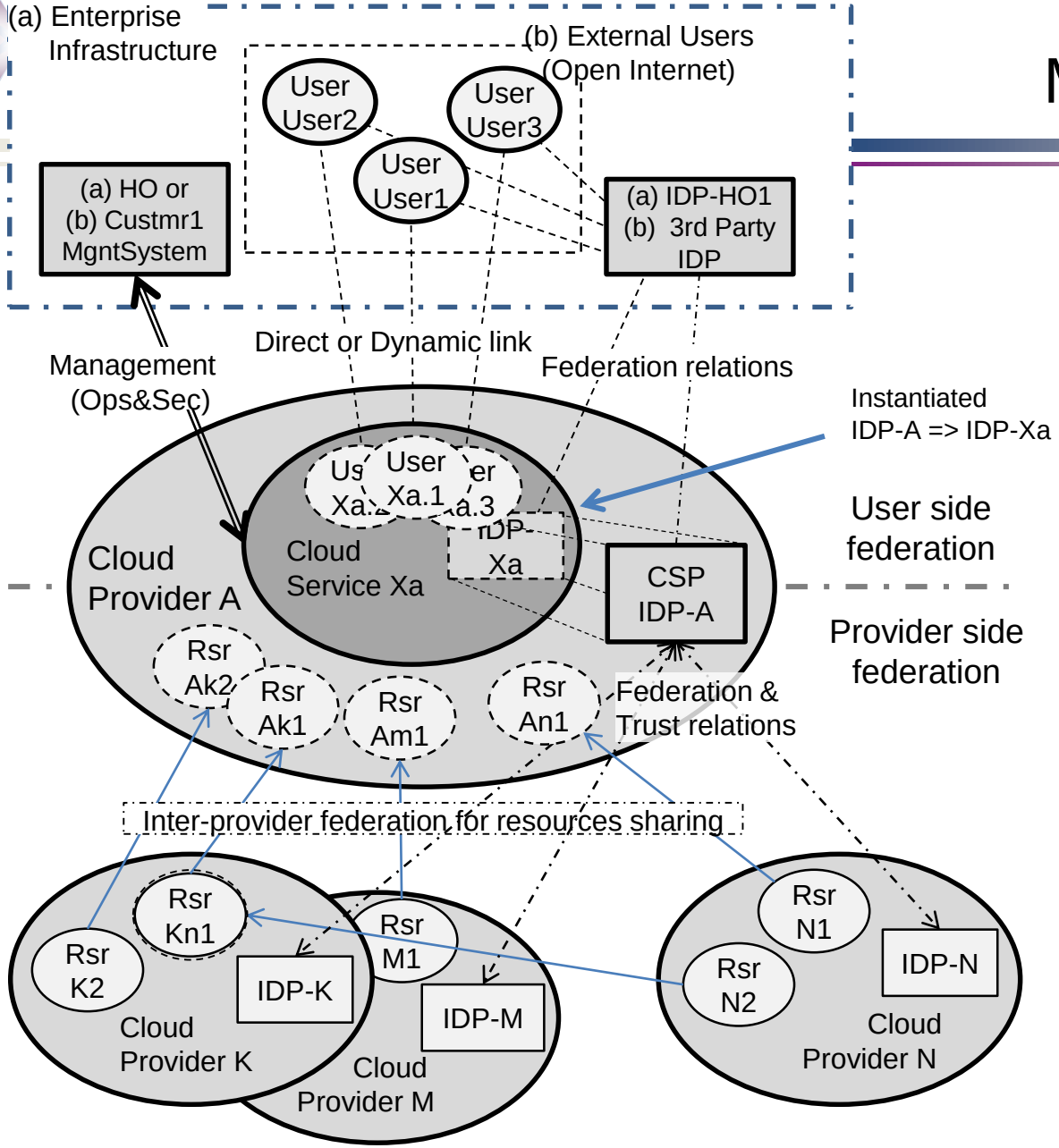
Basic Cloud Federation model (2.1) – Federating CSP's/multi-provider cloud resources



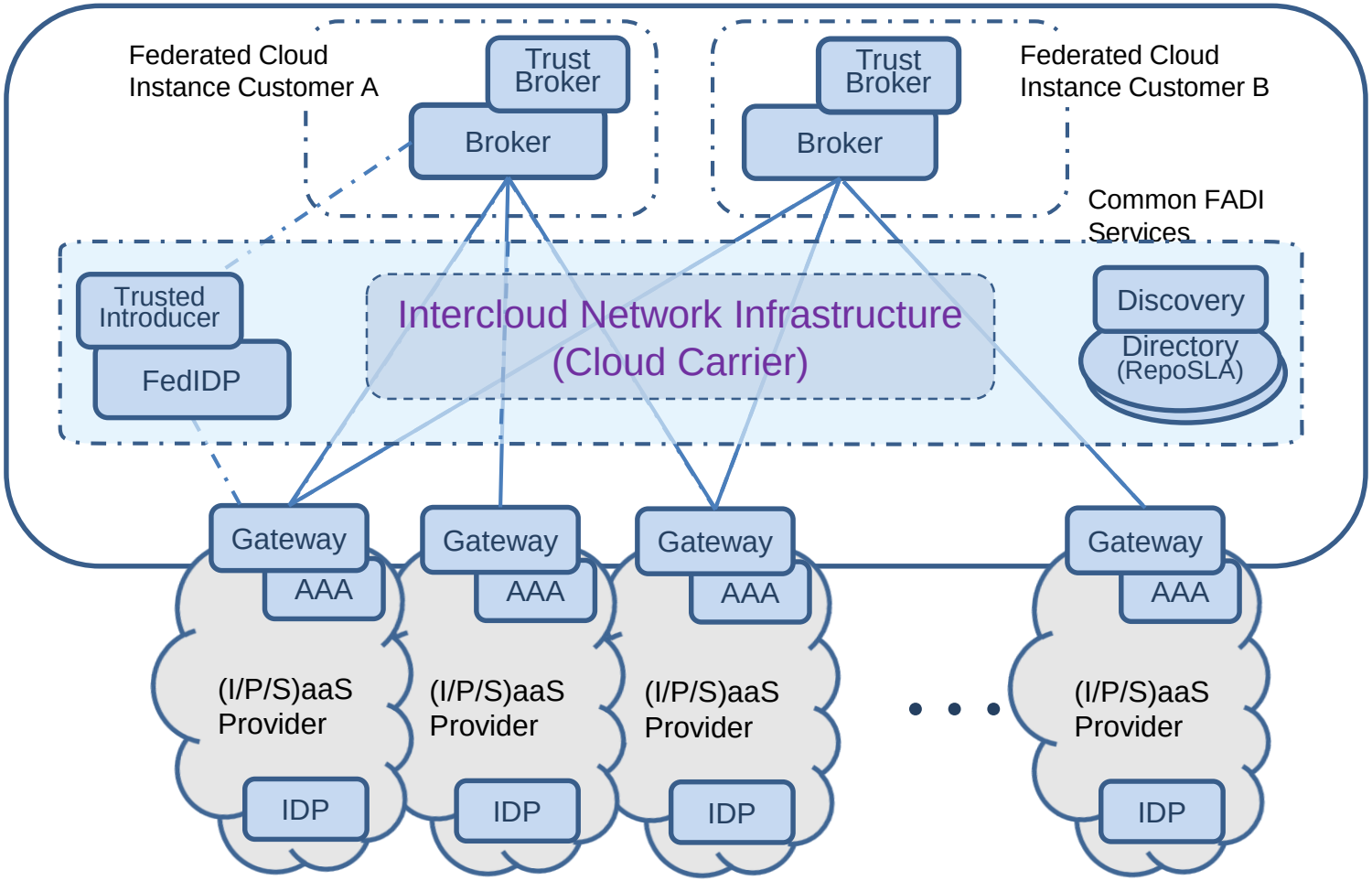
- Cloud provider side federation for resources sharing
- Federation and Trust relations are established between CSP's via Identity management services, e.g. Identity Providers (IDP)
  - May be bilateral or via 3rd party/broker service
- Includes translation or brokering
  - Trust relations
  - Namespaces
  - Attributes semantics
  - Policies
- Inter-provider federation is transparent to customers/users

Provider side Federation

Cloud Federation Model - Combined



Intercloud Federation Infrastructure



AWS Identity and Access Management (IAM)

AWS IAM provides functionality to securely control access to AWS services and resources for individual users and groups by defining individual and group permissions and policies.

- **Manage IAM users and their access:** Create AIM users and assign them individual security credentials (i.e., access keys, passwords, and multi-factor authentication devices) to provide users access to the AWS Management Console, APIs, services and resources.
  - Create multiple users and groups for the same AWS account/customer
  - Manage permissions in order to control which operations a user can perform.
  - Use customizable URL for accessing AWS Management Console for user groups
    - Default https://34629057537.signin.aws.amazon.com/console where “3462905737” is an account ID
    - Customised https://gocxfed.signin.aws.amazon.com/console where “gocxfed” is a group name
- **Manage IAM roles and their permissions:** Create roles and manage permissions to control which operations can be performed by the entity, or AWS service that assumes the role.
- **Manage federated users and their permissions:** Enable identity federation to allow existing identities (e.g. users) in customer enterprise to access the AWS services and resources, without the need to create an IAM user for each identity.
- **Enable Multi-Factor Authentication (MFA)** that augments username and password credentials

Examples of using AWS IAM

Fine-grained access control to AWS resources

- IAM enables your users to control access to AWS service APIs and to specific resources. IAM also enables you to add specific conditions to control how a user can use AWS, such as time of day, their originating IP address, whether they are using SSL, or whether they have authenticated with a multi-factor authentication device.

Manage access control for mobile applications with Web Identity Providers

- You can enable your mobile and browser-based applications to securely access AWS resources by requesting temporary security credentials that grant access only to specific AWS resources for a configurable period of time.

Integrate with your corporate directory

- IAM can be used to grant your employees, and applications federated access to AWS Management Console and AWS service APIs, using your existing identity systems like Microsoft Active Directory.
- You can use any identity management solution that supports SAML 2.0 or feel free to use one of our federation samples (AWS Console SSO or API federation).

Multi-Factor Authentication for highly privileged users

- Protect your AWS environment by using AWS Multi-Factor Authentication (MFA), a security feature available at no extra cost that augments username and password credentials.
- MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.

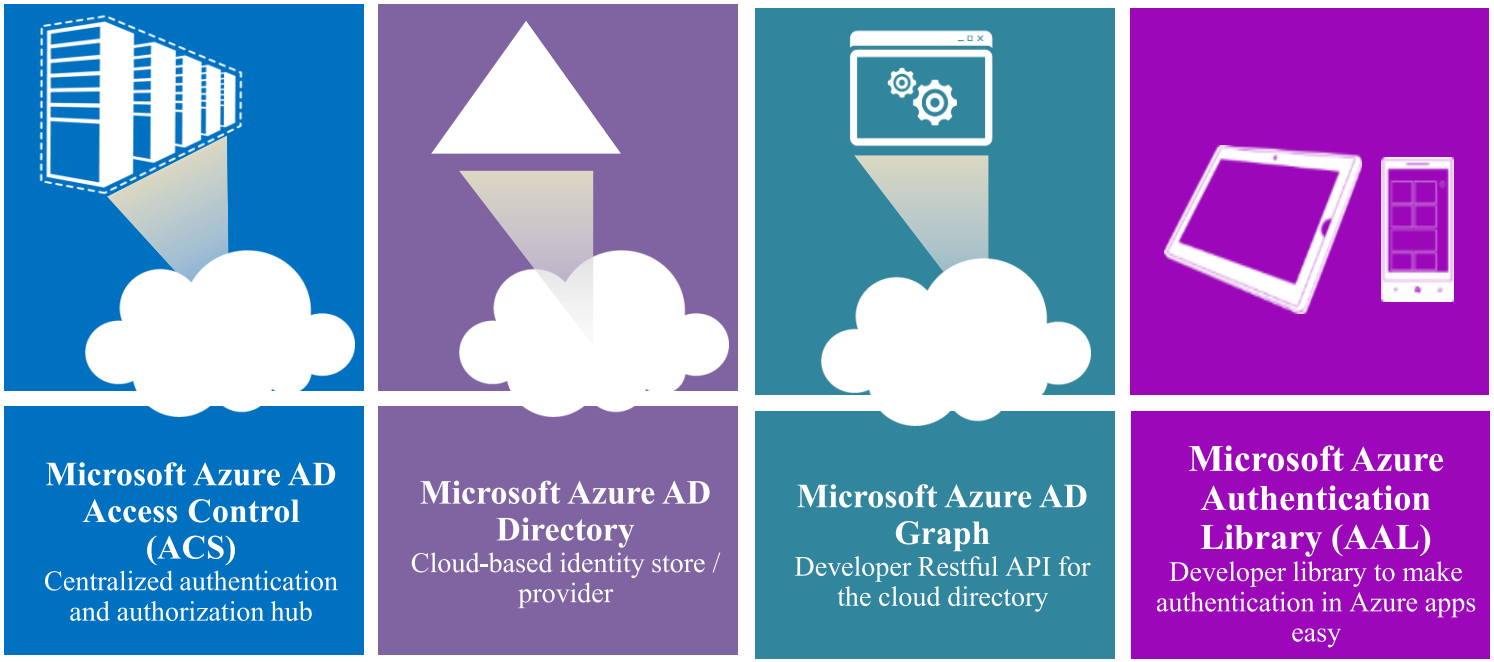
Top Ten IAM Best Practices

AWS has a list of best practices to help IT professionals and developers manage access control without losing flexibility or resiliency

1. Users – Create individual users
2. Groups – Manage permissions with groups
3. Permissions – Grant least privilege
4. Password – Configure a strong password policy
5. Multi Factor Authentication – Enable MFA for privileged users
6. Roles – Use IAM roles for EC2 instances
7. Sharing – Use IAM roles to share access
8. Rotate – Rotate security credentials regularly
9. Conditions – Restrict privileged access further with conditions
10. Root – Reduce/remove use of root

[ref] Top Ten IAM Best Practices http://www.everytalk.tv/talks/2521-Amazon-Web-Services-re-Invent-SEC-303-Top-10-AWS-Identity-and-Access-Management-IAM-Best-Practices

Microsoft Azure Active Directory (AAD)



Microsoft Azure Active Directory is a modern cloud service providing Identity Management and Access Control capabilities to cloud applications.

- Provides Identity and access management in the cloud
- Can be integrated with on-premises AD
- Supports Integration with cloud applications

Microsoft Azure Active Directory provides 4 basic services

- Microsoft Azure AD Access Control (ACS)
- Microsoft Azure AD Directory
- Microsoft Azure AD Graph
- Microsoft Azure Authentication Library (AAL)

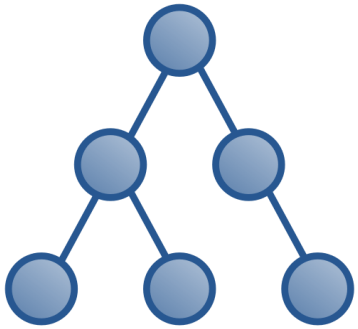
Windows AD Server vs Microsoft Azure AD

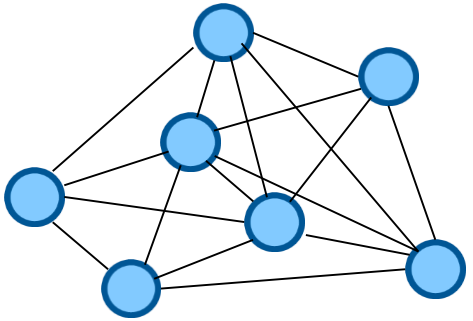
Windows Active Directory

- AD Domain Services
- AD Lightweight Directory Services
- AD Federation Services
- AD Certificate Services
- AD Rights Management Services
- Corporate environment
- Kerberos, LDAP, DNS

Microsoft Azure Active Directory

- Azure Active Directory
- Azure Access Control Service
- AD RMS (Preview)
- Cloud based and cloud oriented
- REST, SAML-P, WS-Federation, OAuth, Graph API

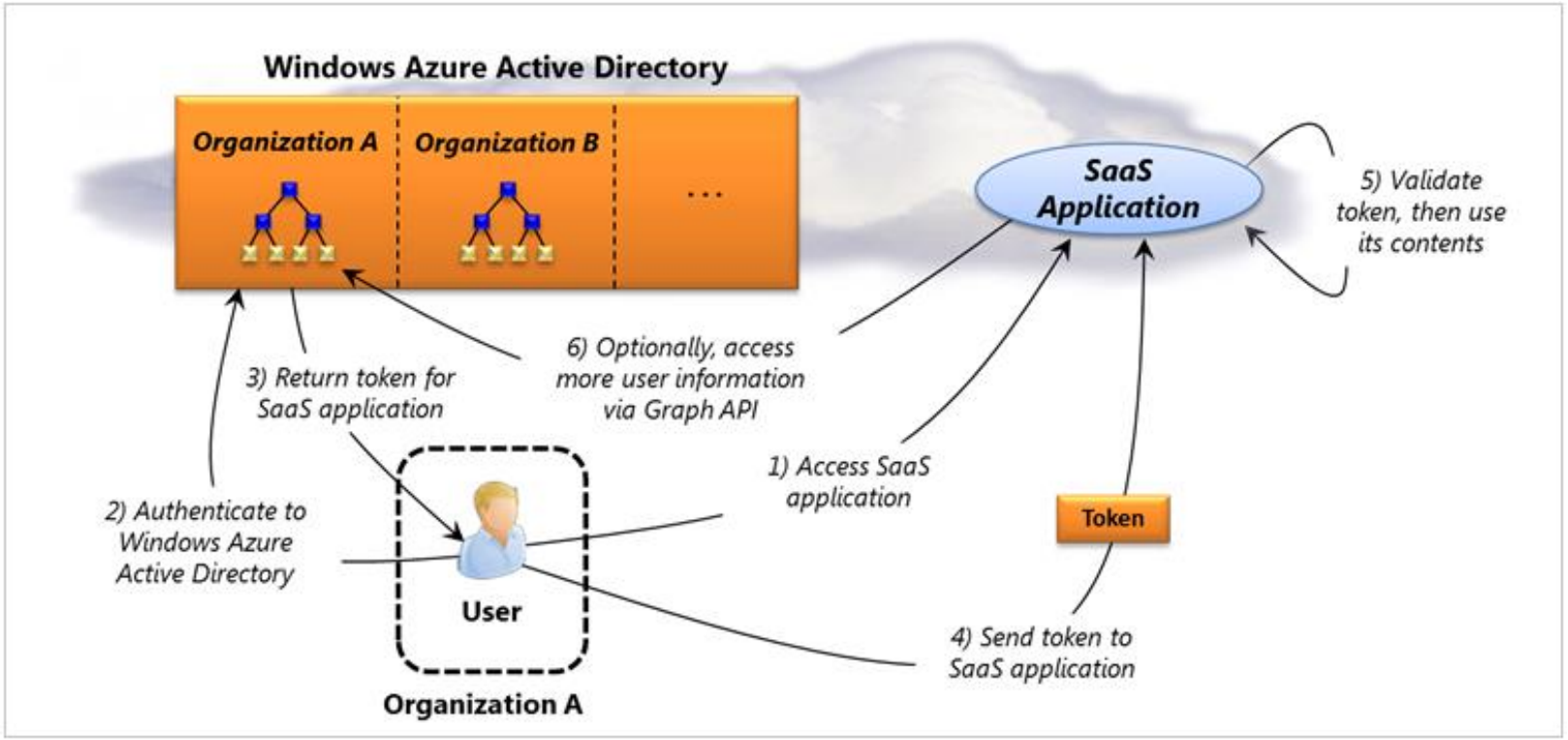




Microsoft Azure AD Access Control

- A cloud federation service for your cloud applications and services
  - Federates on-premises and cloud identity services
- Prerequisites
  - Demands federated authentication
  - AD on-premises and AAD on cloud synchronisation
- Supports multiple identity providers
  - Facebook, Google, Microsoft, Windows Server AD FS, Yahoo!
- Supports multiple protocols
  - WS-Federation, WS-Trust, OAuth 2.0 (draft 13)
- Supports multiple tokens
  - JWT, SAML 1.1/2.0, SWT

Example: AAD based Access Control and Federation



Two main options for using this directory service in the cloud:

- Individuals and organizations that use only cloud based SaaS applications can rely on Azure Active Directory as their sole directory service.
- Organizations that run Windows Server Active Directory can connect their on-premises directory to Azure Active Directory, then use it to give their users single sign-on to SaaS applications.
- Azure Graph Query are used for requesting information from AAD

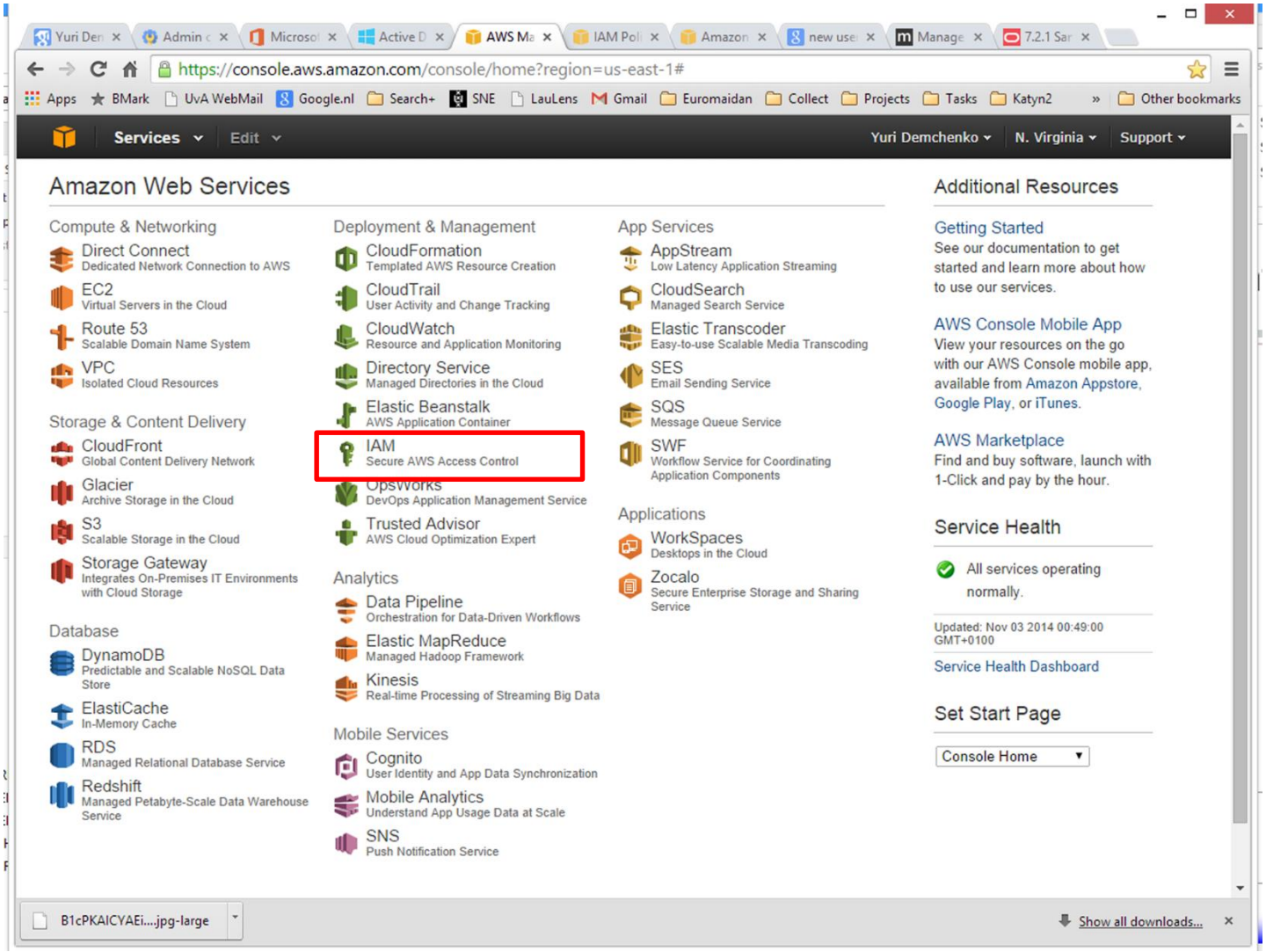
[ref] http://azure.microsoft.com/en-us/documentation/articles/fundamentals-identity/

Demo/Hands on Amazon IAM

This demonstration will show

- How to work with AWS Access Management (IAM)
- How to create users and groups in IAM
- How to configure Access Policy for groups
- How to establish identity and access federation in IAM with organizational or 3rd party Identity provider and authentication service

AWS Identity and Access Management (IAM)

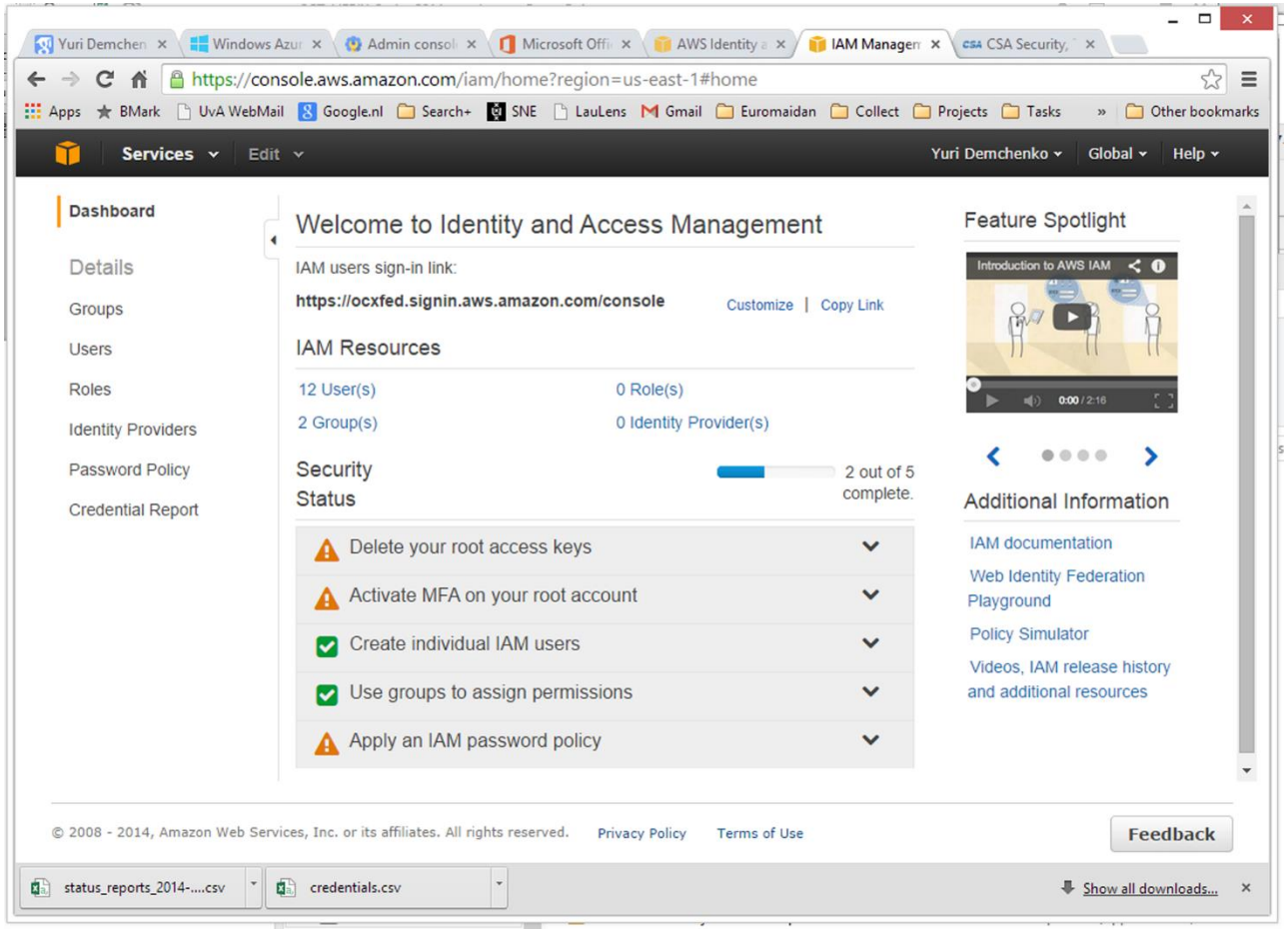


IAM is one of AWS services

Accessible from AWS Management Console

Accessible also via API and CLI

IAM Dashboard



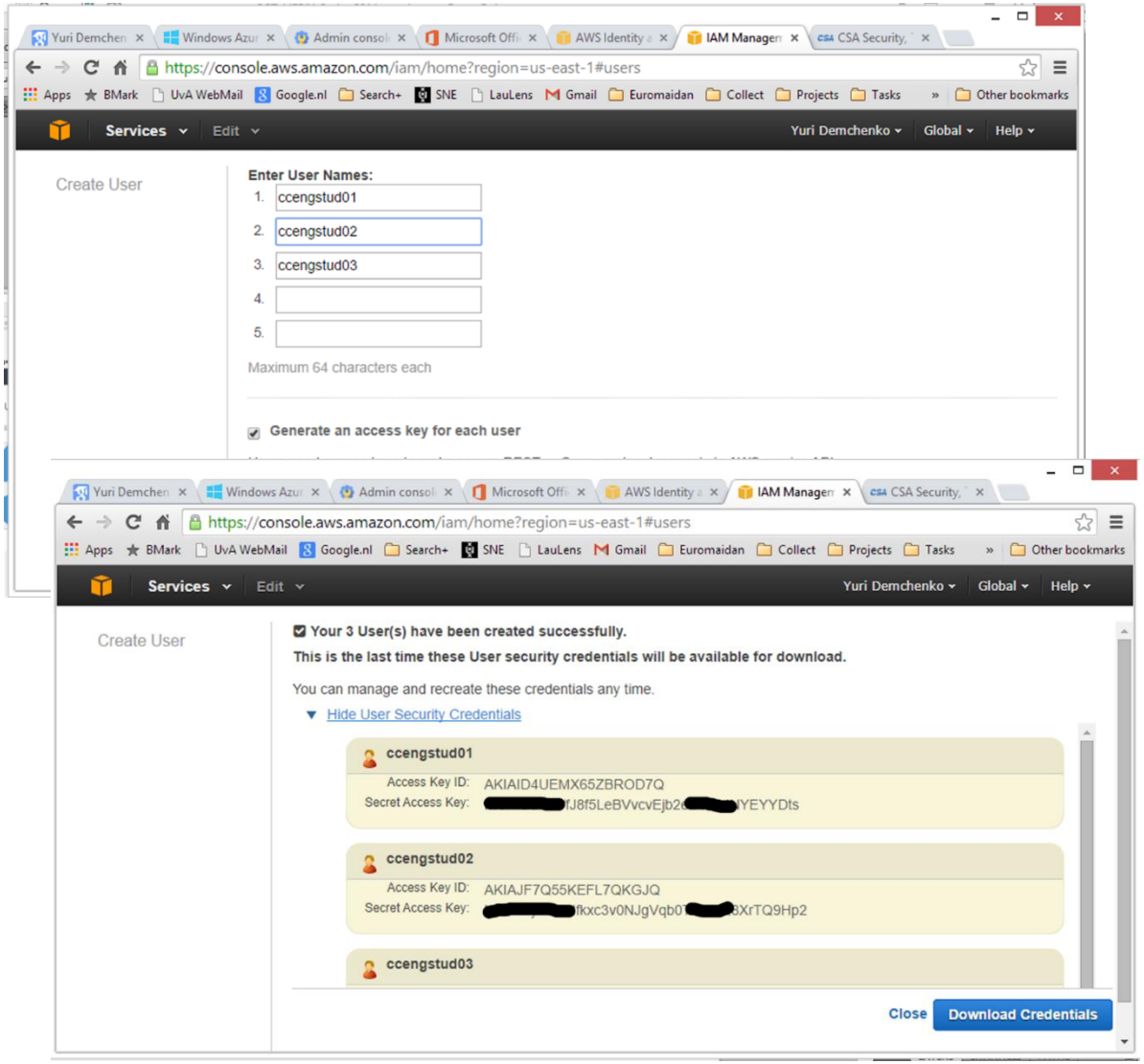
IAM Dashboard allows the following functions

- Create individual IAM users
- Create groups and assign access policies
- Define roles
- Define IAM password policy
- Configure federation by adding trusted IDP

Customise IAM users signin link

- Default signin link is created by account number
- You can customize it by creating **account alias** and selecting user friendly name, e.g. by the project name “OCXfed” https://ocxfed.signin.aws.amazon.com/console
- Name selection “first come, first selected”
  - No conflict arbitrage

Creation of Users: Storing Generated Access Key



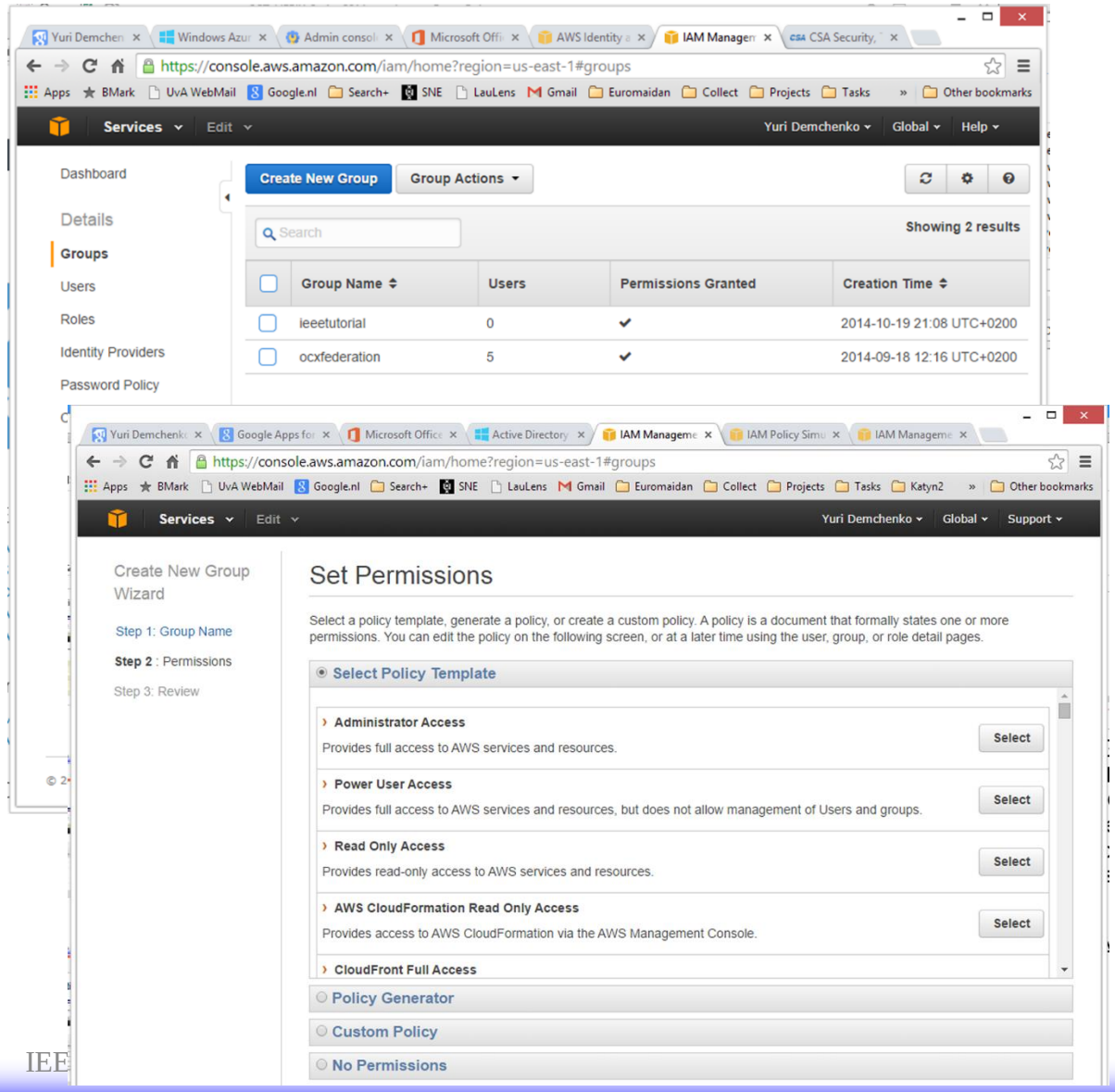
Create new users

- Can be done for list of up to 5 users
- Includes generation of access key for each user

Saving user access keys

- User access key is created instantly during user creation and not storage by IAM/AWS
- User or administrator can download access key and securely store on own computer
- Access key is required when using SSH to access AWS services

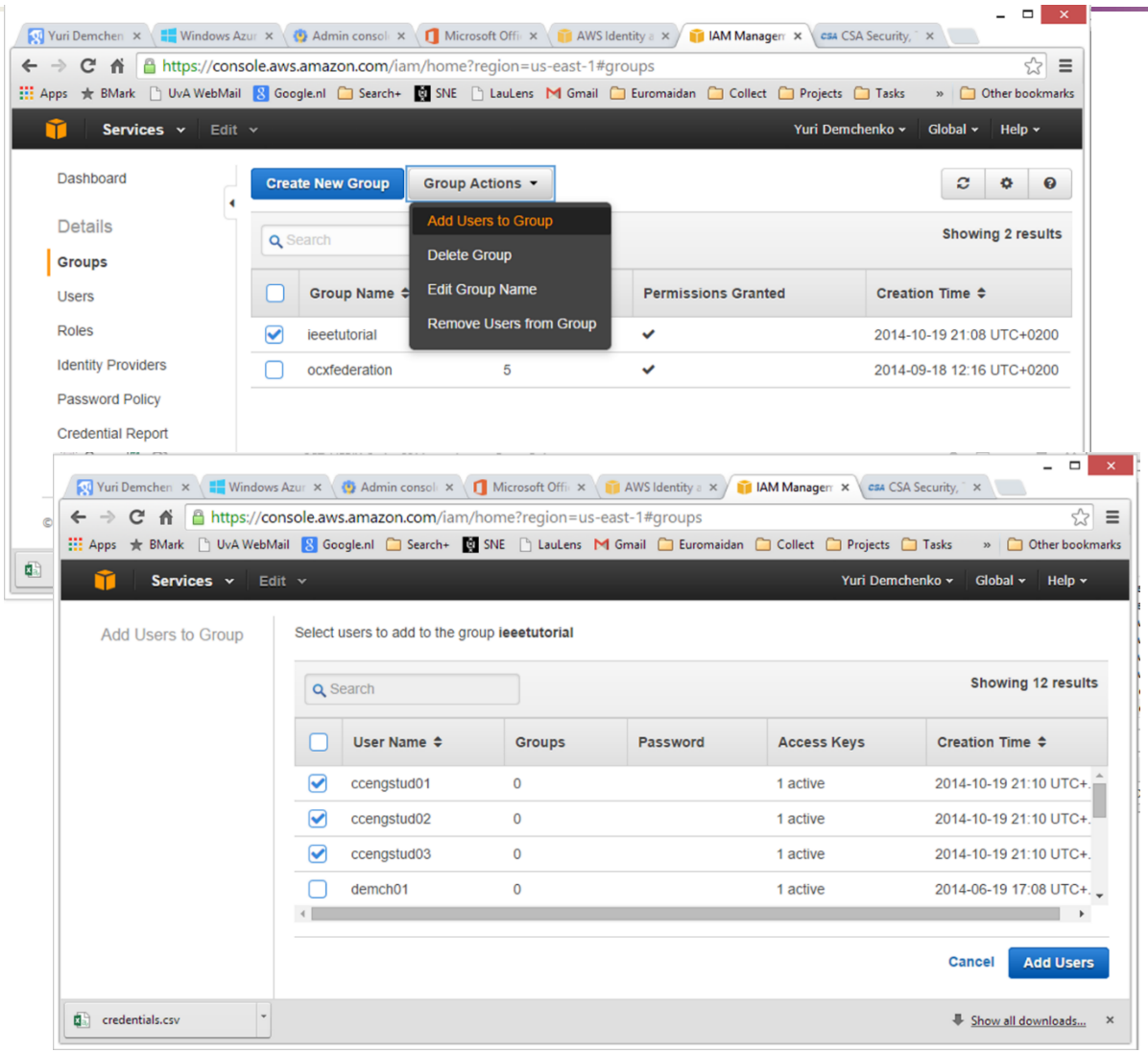
Create new Group



Create new Group:

- In Groups tab select Create New Group
- Step 1: Select Group name
- Step 2: Set Permission or define Policy
  - Can be changed later via Policy configuration
- Step 3: Review and confirm
- Next step: Add users to group

Add users to existing group



Add Users to existing/ created Group:

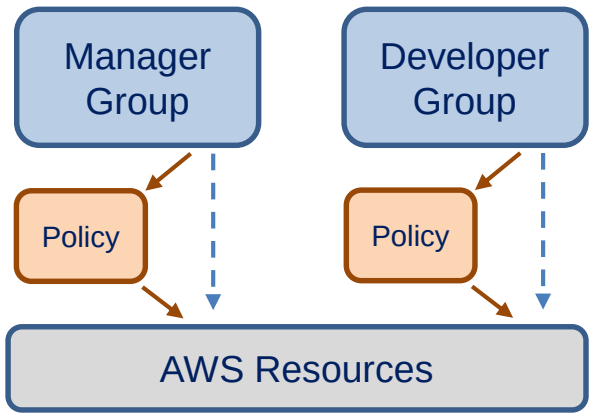
- Select group from the table
- In Groups tab select Group Action: Add Users to Group
- Select Users from the table
- Click button Add Users
- Step 3: Review and confirm
- Other actions:
  - Edit Group Name
  - Remove Users from Group

Note: Group is used to define permissions for a groups users

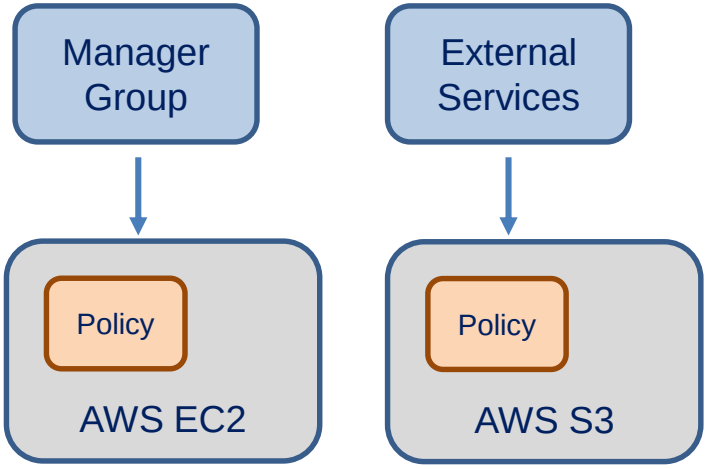
User based and Resource Based Policies

- Besides Users and Groups, Policies can be assigned to Resources
- E.g. S3 buckets and SQS queues can be applied policies
  - Configuring a bucket to be only accessible from a certain IP addresses

User based Access Policies



Resource based Access Policies



Access Policy Configuration

Sample IAM Policy for a user that can access single S3 resource “mybucket”:

Access is allowed if a request comes from user client with IP address 193.23.31.34

```
{
  "Statement": [
    {
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::mybucket",
          "arn:aws:s3:::my-bucket/*"]
    },
    {
      “Condition”:
      “StringEquals”: {
      “AWS.SourceIP”:
      [“193.23.31.34”] }
    }
}
```

Statement defines Actions and Permissions

Action(s)/Operation(s)
Wildcard is allowed

Resource:
Target of Operation

Condition Statement

Action and Resources

"Action" specifies permission to execute operation, e.g.

- RunInstances
- ViewInstances
- AttachVolume
- CreateBucket
- CreateObject
- In total more than 150 AWS management commands

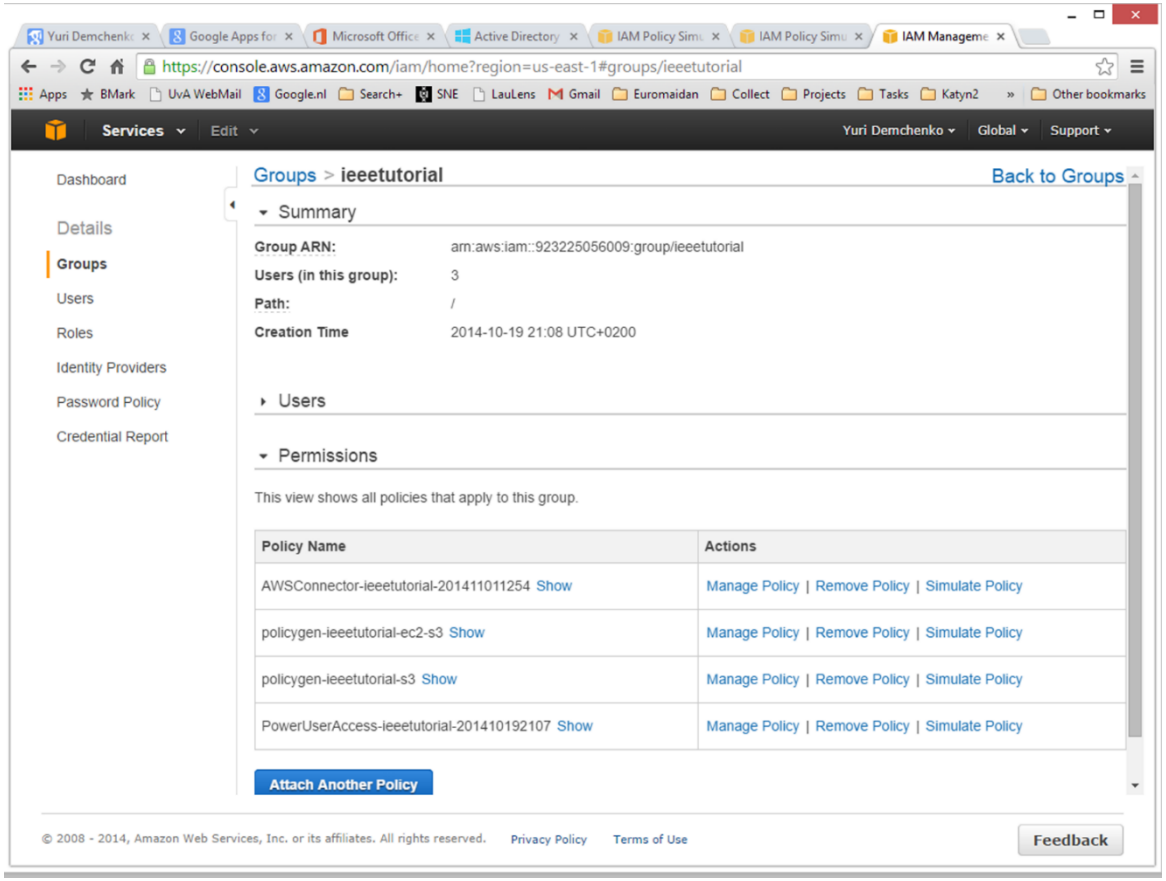
"Resource" specifies permissions for target of operation

- EC2 Instance
- EBS volume
- S3 Bucket, or Object

Available condition statements

- Text string comparison:
  - StringEquals, StringNotEquals, StringEqualsIgnoreCase, StringNotEqualsIgnoreCase, StringLike, StringNotLike
- Number
- Date
- Boolean
- IP Address
  - IPAddress, NotIPAddress

Policy Configuration on IAM Management Console



Options to set policy

- Select policy from templates containing more than 80 preset policies
- Use policy generator
- Upload custom policy

Policy format is JSON notation

Administrator Access: All is permitted

Power User Access: All is permitted except creating accounts

Multi-user Environment scenarios in AWS

Scenario 1: Individual Server Environments

Suitable for labs and other classwork that requires users to access their own pre-provisioned Linux or Windows servers running in the AWS cloud.

Scenario 2: Limited User Access to AWS Management Console

Suitable for users that require control of AWS resources, such as students in cloud computing or high performance computing (HPC) classes.

Scenario 3: Separate AWS Account for Each User with optional consolidated billing

Provides an environment for users who need a completely separate account environment, such as researchers or graduate students. It is similar to the “Limited User Access to AWS Management Console” scenario, except that each IAM user is created in a separate AWS account, eliminating the risk of users affecting each other’s services.

[ref] Setting up multiuser environment in the AWS Cloud (for classroom training and research)
https://media.amazonwebservices.com/AWS_Setting_Up_Multiuser_Environments_Education.pdf

Scenario 1: Individual Server Environments

Scenario 1: Individual Server Environments

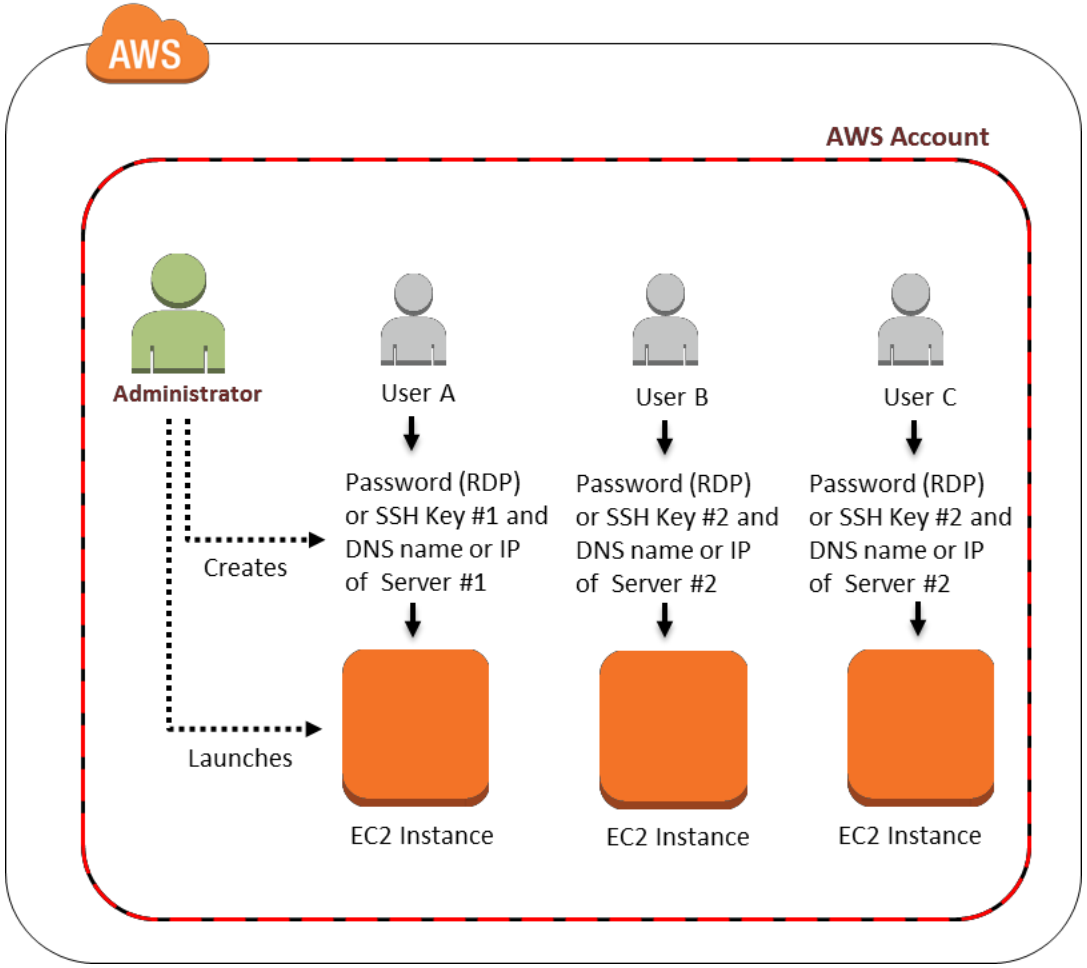
Suitable for labs and other classwork that requires users to access their own pre-provisioned Linux or Windows servers running in the AWS cloud.

- The servers are Amazon Elastic Compute Cloud (Amazon EC2) instances that can be created by an administrator with a customized configuration that includes applications and data needed to perform tasks for labs or assignments.

As an example, consider a class with 25 students.

- The administrator creates 25 private keys (or one shared private key) and launches 25 Amazon EC2 instances; one instance for each student.
- The administrator shares the appropriate key or password with each student and provides instructions on how to log in to their instance. Students do not have access to the AWS Management Console, APIs, or any other AWS service.
- Each student gets a unique private key (in case of Linux) or a username and password (in case of Windows) along with the public hostname or IP address of the instance that they can use to log in.

Scenario 1: Individual Server Environments



User accounts setup and configuration

- Administrator creates a new AWS account or uses existing AWS account for the user groups and assigns permissions
  - For example, this can be a shared account for a professor, class, department, or school.
- Administrator must explicitly grant them permissions to access the AWS resources that they need for their work.
  - By default, IAM users don't have access to any AWS resources.
- Administrator can give users their own unique access keys, for security and separation between users.

Administrator then launches the required AWS services for each user and provides resource access credentials to the users.

[ref] Setting up multiuser environment in the AWS Cloud (for classroom training and research)
https://media.amazonwebservices.com/AWS_Setting_Up_Multiuser_Environments_Education.pdf

Scenario 2: Limited User Access to AWS Management Console

Scenario 2: Limited User Access to AWS Management Console

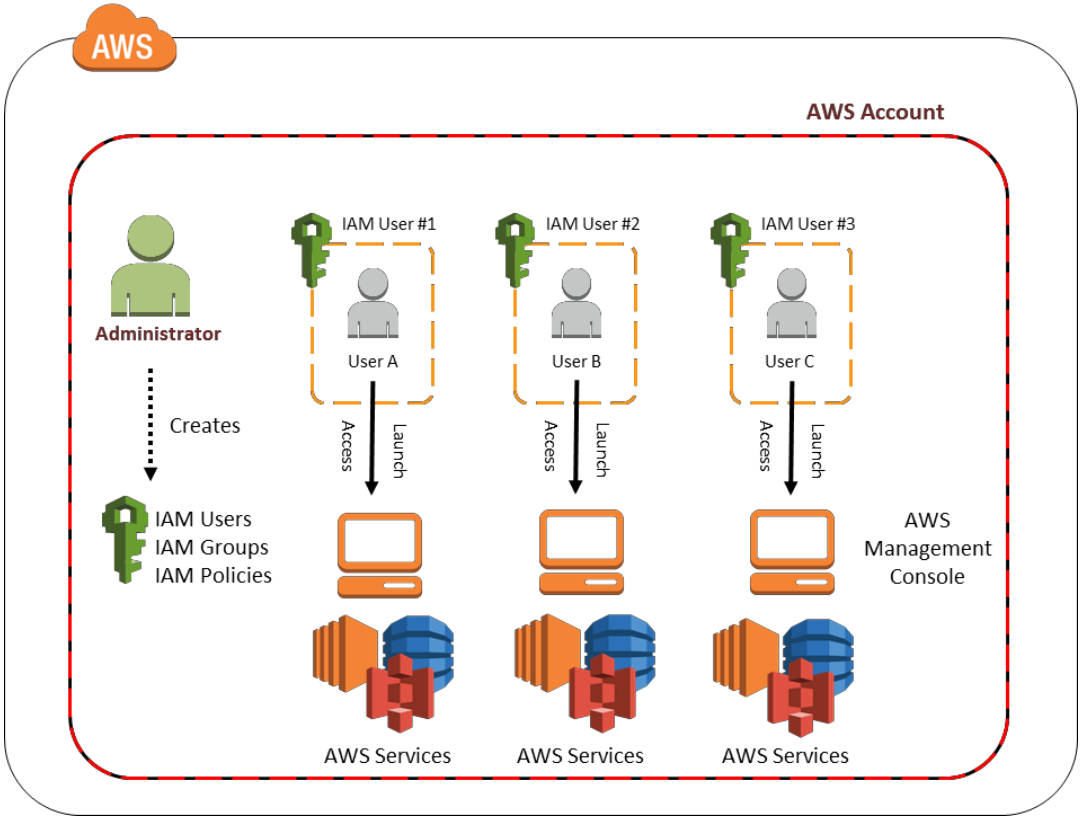
Suitable for users that require control of AWS resources, such as students in cloud computing or high performance computing (HPC) classes.

- With this scenario, users are given restricted access to the AWS services through their IAM credentials.

As an example, consider a class with 25 students.

- The administrator creates 25 IAM users using the AWS Management Console or APIs, and provides each student with their IAM credentials (username and password) and Login URL to the AWS Management Console.
- The administrator also creates a group policy or individual user policies that allow or deny access to different services.
- Each student (IAM user) has access to resources and services as defined by these access control policies set by the administrator.
- Students can log in to the AWS Management Console to access different AWS services as defined the policy, for example, launch Amazon EC2 Instances and store objects in Amazon S3.

Scenario 2: Limited User Access to AWS Management Console



User accounts setup and permissions assignment

- Administrator creates IAM users and give each one access credentials.
- Administrator can create and manage AWS users and groups and use permissions to allow and deny access to AWS resources.
- Users can log into the AWS Management Console and then they can launch and access different AWS services, subject to the access control policies applied to their account.
- Users have direct control over the access credentials for their resources.

[ref] Setting up multiuser environment in the AWS Cloud (for classroom training and research)
https://media.amazonwebservices.com/AWS_Setting_Up_Multiuser_Environments_Education.pdf

Scenario 3: Separate AWS Account for Each User

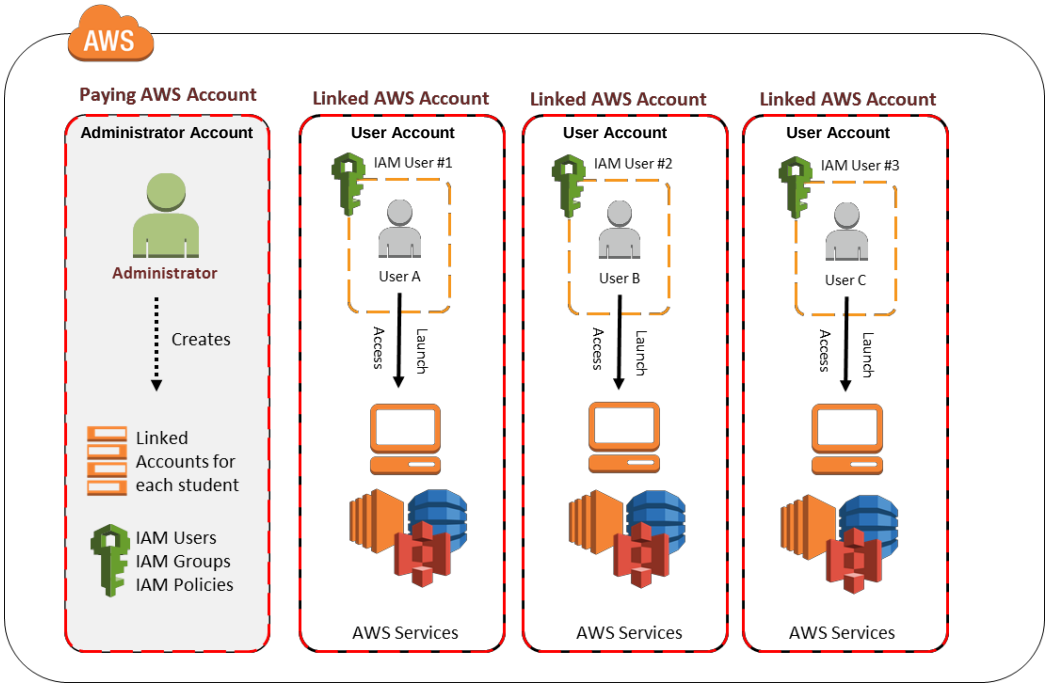
Scenario 3: Separate AWS Account for Each User with optional consolidated billing

Provides an environment for users who need a completely separate account environment, such as researchers or graduate students. It is similar to the “Limited User Access to AWS Management Console” scenario, except that each IAM user is created in a separate AWS account, eliminating the risk of users affecting each other’s services.

As an example, consider a research lab with 10 graduate students.

- The administrator creates one paying AWS account, 10 linked student AWS accounts, and 1 restricted IAM user per linked account.
- The administrator provisions separate AWS accounts for each user and links the accounts to the paying AWS account.
- Within each account, the administrator creates an IAM user and applies access control policies.
- Users receive access to an IAM user within their AWS account.
  - They can log into the AWS Management Console to launch and access different AWS services, subject to the access control policy applied to their account.
  - Students don’t see resources provisioned by other students.

Scenario 3: Separate AWS Account for Each User



Create AWS accounts and assign permission

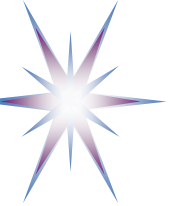
- Administrator creates separate AWS accounts for each user who needs a new AWS account.
  - These accounts can optionally be linked together to enable the consolidated billing.
- The administrator then creates an IAM users and groups in each AWS account and applies an access control policy to each user or group.
- Users are given access to the IAM user within their AWS account, but do not have access to the root credentials of the AWS account.
- Users can log into the AWS Management Console with their IAM credentials and then they can launch and access different AWS services, subject to the access control policies applied to their account.
- Users have direct control over the access credentials for their resources and they can also share these resources with other users as necessary.

[ref] Setting up multiuser environment in the AWS Cloud (for classroom training and research)
https://media.amazonwebservices.com/AWS_Setting_Up_Multiuser_Environments_Education.pdf

Summary and further reading

- Cloud Security impose new security challenges
  - Based on the core security principles and models
  - Security and Trust in cloud
- Multiple dimensions of security
- Cloud Federation models and security
  - Two general cloud federation models: client side and provider side, - provide a framework for user access federation and inter-cloud resources sharing
- AWS IAM services provides a solution for federated access control and Identity Management in AWS and federates
- Microsoft Azure Active Directory is a powerful platform for FedIDM and federated access control that naturally integrates with enterprise Active Directory services

- Read standards and industry best practices
- EGI Federated Cloud and security



Part 3. Cloud Compliance

Security and Compliance

- Security and compliance are related and in some cases interchangeable
  –
- Security is commonly defined as a set of technical, physical, and administrative controls in order to ensure normal operation of a system or application
  – Security is often associated with the CIA triad Confidentiality, Integrity, Availability
  – Appropriate level of security requires organizations to take measures and comply to the numerous security controls
- Compliance is a certification or confirmation that the system or an organization meets the requirements of specified standards, established legislation, regulatory guidelines or industry best practices that can be jointly defined as compliance framework
  – A compliance framework can includes business processes and internal controls the organization has in place to adhere to these standards and requirements
  – The framework should also map different requirements to internal controls and processes to eliminate redundancies
- Why it is important for cloud?
  – When moving to cloud, the organization moves from internal security and operational environment/context (that may not be formally defined) to external operational security that will become a part of SLA (or business requirement) with CSP
- Problem with achieving compliance for cloud based applications/solutions
  – Audit requirements are not designed for virtualised distributed environment
  – Lack of visibility in cloud: large CSP such as Amazon and Google are “walled/curtained gardens”
  – Requirements to allow CSP audit may involve Non-Disclosure Agreement (NDA) and risk of provider lock-in

Regulatory requirements to be considered for cloud compliance

General standards and recommendations

- ISO/IEC 27001:2005 Certification on security infrastructure
  - Industry standard: the risk-based information security management program that follows a plan-do-check-act process
- NIST SP 800-53 Security Controls and ISO/IEC 15408 Evaluation Cirteria
- Service Organisation Control SOC 1 (SSAE 16/ISAE 3402) and SOC 2 and 3 (AT 101)
  - SOC 2 is a detailed attestation report (often restricted) for service organizations that contains strict standards for security, availability, processing integrity, confidentiality, and privacy.
  - SOC 3 is a general purpose report which summarizes the SOC 2 audit
- NIST SP 800-144 Guidelines for Security and Privacy in Cloud Computing
- Cloud Security Alliance (CSA) Security Guidance for Critical Area of focus in Cloud Computing
- ENISA Cloud Computing Security Risk Assessment
- European Union Data Protection Directive

Industry and government related

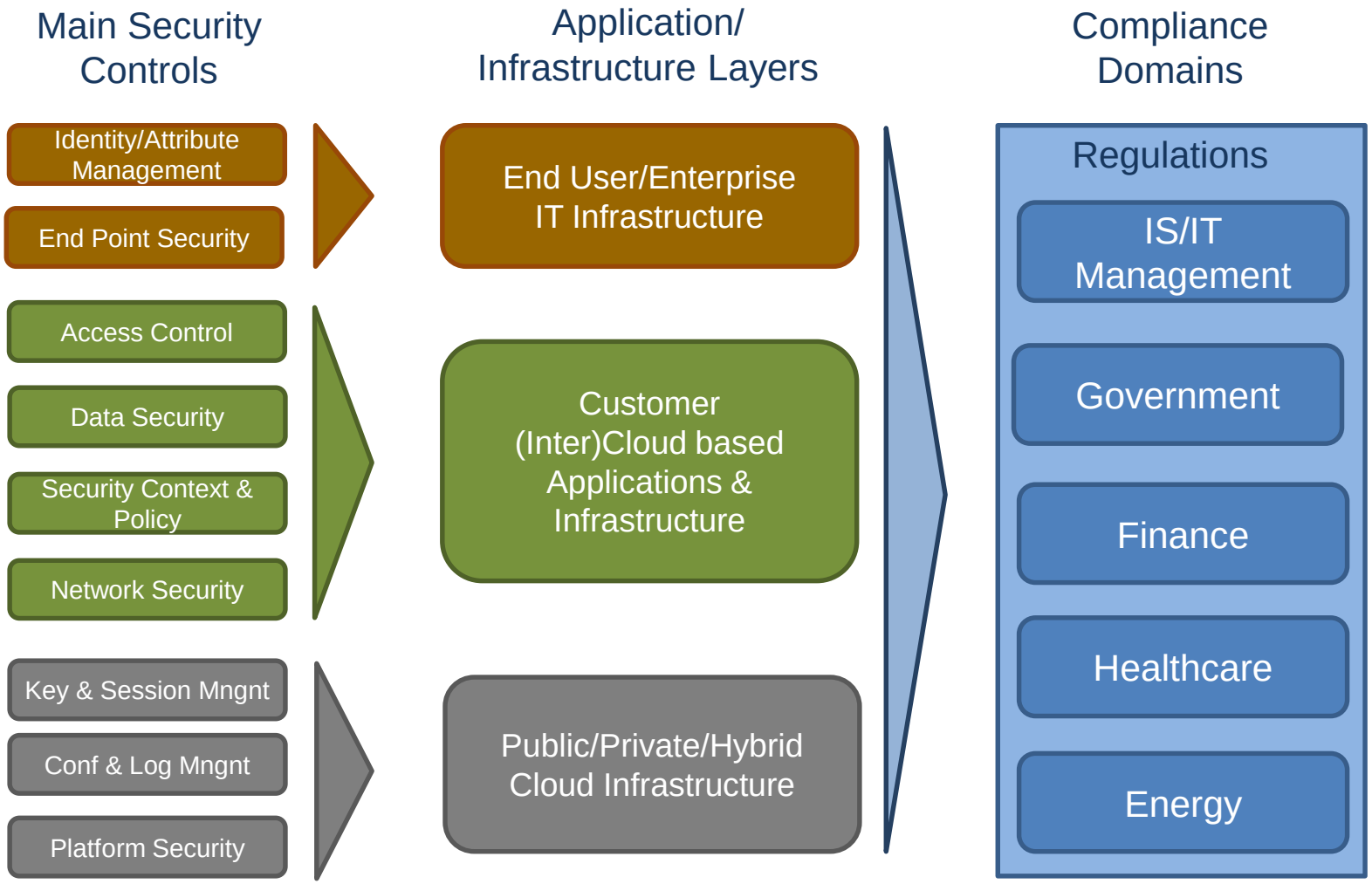
- Payment Card Industry Data Security Standard (PCI- DSS)
- Sarbanes Oxley Act (SOX)
- HIPAA/HITECH - The U.S. Health Insurance Portability and Accountability Act (**HIPAA**) and HITECH (Health Information Technology for Economic and Clinical Health)
  - Act created by the US federal government include provisions to protect patients' private information.
- The Federal Information Security Management Act of 2002 (FISMA)
  - Describes security requirements for the protection of information and information systems in Federal systems
- Gramm-Leach-Bliley Act (FGLBA)
- Federal Risk and Authorisation Management Program (FedRAMP)
- Department of Defense Information Certification Accreditation Process (DIACAP)

EU Regulations on Cloud Computing

2 main documents published in 2012

- Unleashing the Potential of Cloud Computing in Europe, Brussels, 27.9.2012, COM(2012) 529 final
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
- Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final.
  http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- EU cloud regulation framework to fully emerge by 2015

Mapping Compliance and Cloud Infrastructure Components



Security and Compliance Questions

The main questions that security and compliance auditors would ask you

- Where is our data going to reside?
- Who is going to look after it?
- Who is going to be able to see it?
- Is it going to be the people that manage the infrastructure for us?
- Is it going to be internal and external people?
- And if we use a public cloud how secure is that cloud platform for us?
- Is the cloud going to be segregated from other organisations' data?

Case study: Certification/Compliance by Amazon AWS Cloud

The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best-practices including:

- ISO/IEC 27001:2005
- SOC 1, SOC2, SOC3
- FIPS 140-2
- CSA
- PCI DSS Level 1
- HIPAA
- ITAR
- DIACAP and FISMA
- FedRAMP (SM)
- MPAA

Amazon Cloud is certified for hosting US Governmental services

http://aws.amazon.com/compliance/

Case study: Certification/Compliance by Microsoft Azure

Microsoft services/infrastructure meets the following key certifications, attestations and compliance capabilities

- ISO/IEC 27001:2005 Certification on security infrastructure
- SOC 1 (SSAE 16/ISAE 3402) and SOC 2 and 3 (AT 101)
  - Obtained in 2008 and 2012
- Cloud Security Alliance (CSA) Cloud Controls Matrix
- NIST SP 800-144 Guidelines for Security and Privacy in Cloud Computing
- PCI Data Security Standard Certification level 1
- HIPAA and HITECH
- FISMA Certification and Accreditation – since 2010
- Various state, federal, and international Privacy Laws(95/46/EC, e.g. EU Data Protection Directive, California SB 1386, etc.)

http://www.windowsazure.com/en-us/support/trust-center/compliance/

PCI DSS Cloud Computing Guidelines

Information Supplement: PCI DSS Cloud Computing Guidelines, February 2013 (https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf)

Content:

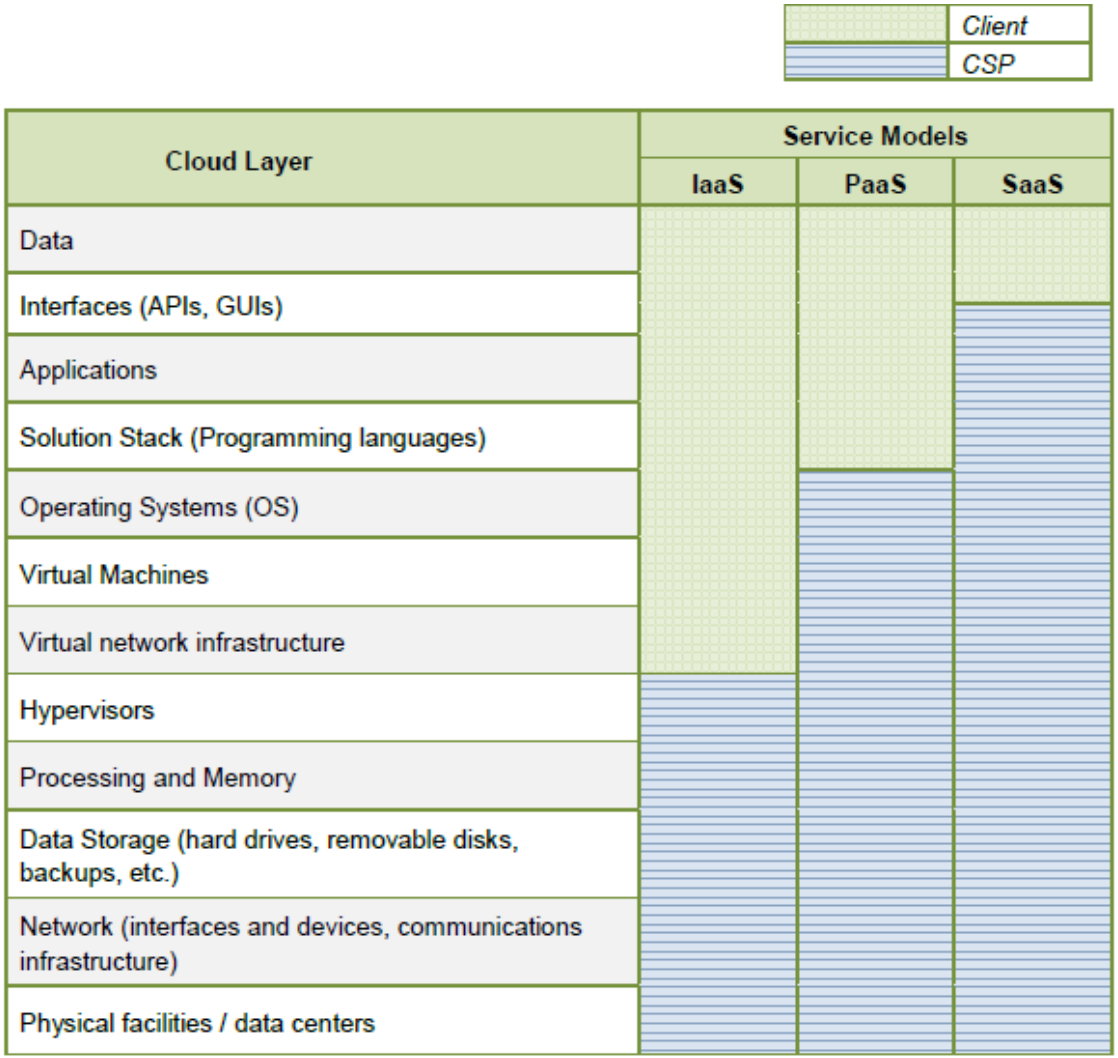
- Cloud Overview – provides explanation of common deployment and service models for cloud environments, including how implementations may vary within the different types.
- Cloud Provider/Cloud Customer Relationships – outlines different roles and responsibilities across the different cloud models and guidance on how to determine and document these responsibilities.
- PCI DSS Considerations – provides guidance and examples to help determine responsibilities for individual PCI DSS requirements, and includes segmentation and scoping considerations.
- PCI DSS Compliance Challenges - describes some of the challenges associated with validating PCI DSS compliance in a cloud environment.
- Additional Security Considerations – explores a number of business and technical security considerations for the use of cloud technologies.

Audience: Involved parties/stakeholders

Cloud customers, cloud service providers and regulators must work together to determine the solutions that best meet the needs of stakeholders:

- **Merchants:** Enterprise and public sector cloud customers must be able to achieve their compliance obligations while using cloud services
- **Individuals** using the cloud have an expectation that their personal information will be protected and used appropriately
- **Cloud service providers** must have clear mechanisms to evaluate and communicate capabilities
- **Assessors:** Regulators and industry governing bodies need to have confidence that their requirements are met and verified

Example: Controls assignment for different cloud service models (PCI DSS)



CSP facility/ infrastructure must be certified/compliant with PCI DSS and relevant standards

- Provided mapping between PCI DSS and other standards

Note: Data is always responsibility of the customer/client

Source: PCI DSS Cloud Computing Guidelines, February 2013 (https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf)

Example: PCI DSS Responsibilities sharing

PCI DSS Requirement	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1: Install and maintain a firewall configuration to protect cardholder data	Both	Both	CSP
2: Do not use vendor-supplied defaults for system passwords and other security parameters	Both	Both	CSP
3: Protect stored cardholder data	Both	Both	CSP
4: Encrypt transmission of cardholder data across open, public networks	Client	Both	CSP
5: Use and regularly update anti-virus software or programs	Client	Both	CSP
6: Develop and maintain secure systems and applications	Both	Both	Both
7: Restrict access to cardholder data by business need to know	Both	Both	Both
8: Assign a unique ID to each person with computer access	Both	Both	Both
9: Restrict physical access to cardholder data	CSP	CSP	CSP
10: Track and monitor all access to network resources and cardholder data	Both	Both	CSP
11: Regularly test security systems and processes	Both	Both	CSP
12: Maintain a policy that addresses information security for all personnel	Both	Both	Both
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

Segmentation considerations

Segmentation on a cloud based infrastructure must ensure similar level of segmentation as with physical infrastructure

- Mechanisms to ensure appropriate segmentation may be applied at the network, operating system and application layers
- Cardholders data isolation must be ensured
- (Multi-tenant) Cloud environments must be isolated from each other

Examples of correctly segmented cloud environments:

- Traditional Application Service Provider (ASP) model where physically separate servers are provided for each client's environment
- Virtualized servers that are individually dedicated to a particular client, including any virtualized disks such as SAN, NAS or virtual database servers
- Environments where clients run their applications in separate logical partitions using separate database management system images and do not share disk storage or other resources

Examples of not correct segmentation

- Environments are separated only by access control at the application or operating system level
- Data are stored at the same of the database

Segmentation technologies

- Physical firewalls and network segmentation at the infrastructure level
- Firewalls at the hypervisor and VM level
- VLAN tagging, in addition to firewalls
- Intrusion prevention system
- Data loss prevention tools at the hypervisor and/or VM level
- Controls to prevent out-of-band communications
- Isolation of shared processes and resources from client environments
- Segmented data storage for each client
- Strong, two-factor authentication
- Separation of duties and administrative oversight
- Continuous logging and monitoring of perimeter traffic

What does PCI DSS Compliance means?

- Cloud service validation for certain PCI DSS requirements does not automatically transfer to the client environments within the cloud service
  - For example, a CSP's validation may have included use of up-to-date anti-virus software on the CSP's systems; however, this validation might not extend to the individual client OS or VMs (such as in an IaaS service).
- Client's PCI DSS compliance does not result in any claim of compliance for the CSP, even if the client's validation included elements of the service managed by the CSP.

In general, one party's compliance doesn't solve the overall compliance

a) If a CSP is compliant, this does not mean that their clients are.

b) If a CSP's clients are compliant, this does not mean that the CSP is.

c) If a CSP and the client are compliant, this does not mean that any other clients are

SLA and compliance

- SLA and other written agreements should clearly delineate responsibility between parties
- PCI DSS compliance validation and testing (with associated controls and permissions) should be clearly detailed in SLA

CSA GRC Stack: Governance, Risk Management and Compliance

The GRC Stack provides a toolkit for enterprises, cloud providers, security solution providers, IT auditors and other stakeholders to assess both private and public clouds against industry established best practices, standards and critical compliance requirements.
https://cloudsecurityalliance.org/research/grc-stack/

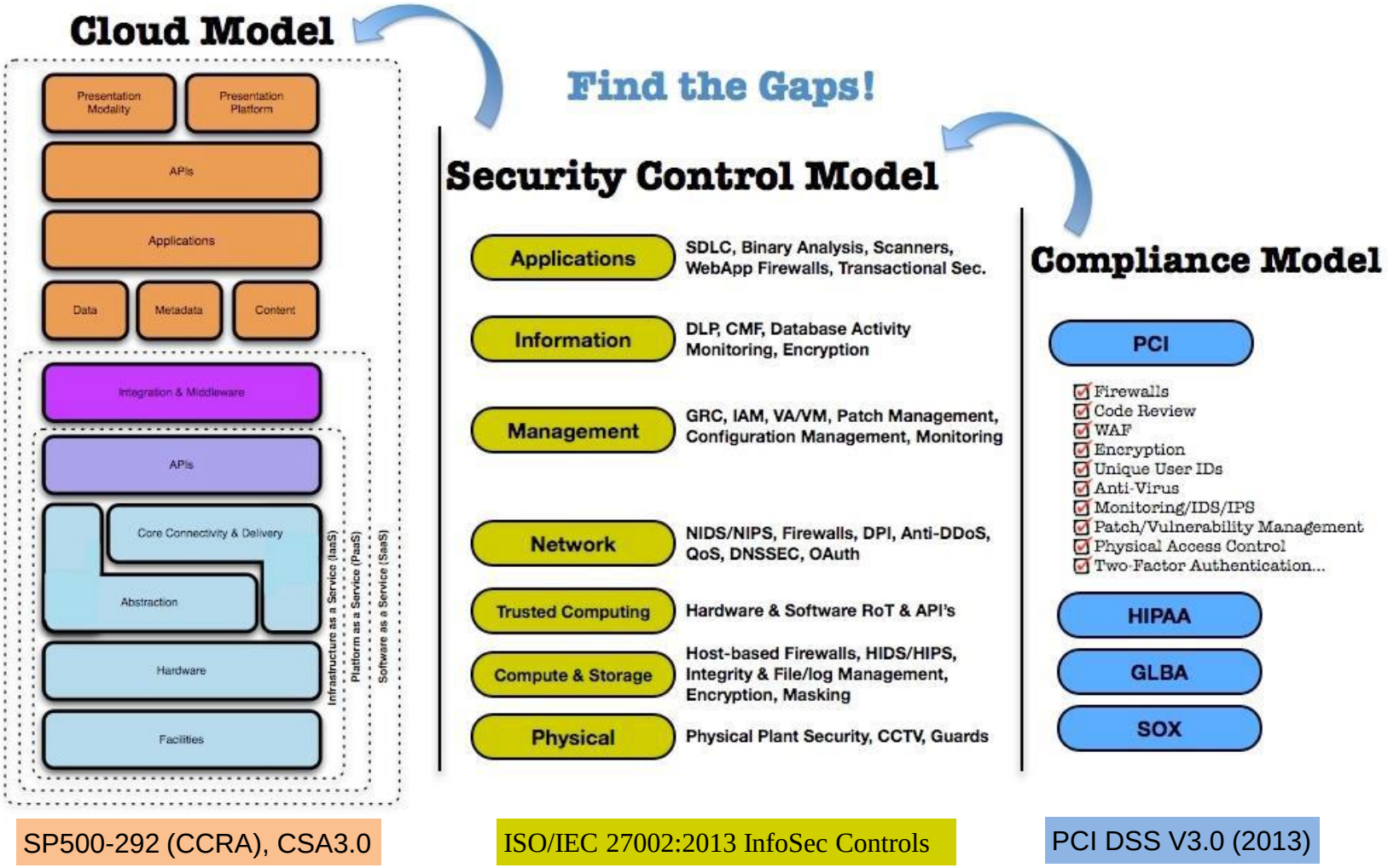
- **Cloud Controls Matrix (CCM)** is designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider (https://cloudsecurityalliance.org/research/ccm/)
  - The CCM gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains
  - Defined in accordance to industry-accepted security standards, regulations, and controls frameworks such as the HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI, HIPAA and NIST.
- **Consensus Assessments Initiative Questionnaire (CAIQ)** provides an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency (https://cloudsecurityalliance.org/research/cai/)
  - Provided in a form of questionnaire in the spreadsheet format, a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.
  - Questions are formulated to answer “yes or no” what should help to tailor each unique cloud customer’s evidentiary requirements.
- Other initiatives (currently dormant)
  - CloudAudit to provide a common interface and namespace that would allow cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their cloud environments and provide a foundation for transparency and trust in private and public cloud systems.
  - Cloud Trust Protocol (CTP) to provide mechanism by which cloud service consumers ask for and receive information about the elements of transparency as applied to cloud service providers.

A Complete Cloud Security Governance, Risk, and Compliance (GRC) Stack

https://cloudsecurityalliance.org/research/grc-stack/

Delivering	← Stack Pack →	Description
Continuous monitoring … with a purpose		Cloud Trust Protocol (CTP) • Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers
Claims, offers, and the basis for auditing service delivery		• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
Pre-audit checklists and questionnaires to inventory controls		Consensus Assessments Initiative (CAI) • Industry-accepted ways to document what security controls exist
The recommended foundations for controls		Cloud Control Matrix (CCM) • Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider

CSA3.0: Mapping the Cloud Model to the Security Control & Compliance



SP500-292 (CCRA), CSA3.0

ISO/IEC 27002:2013 InfoSec Controls

PCI DSS V3.0 (2013)

[ref] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2013)
https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

What is the Cloud Controls Matrix (CCM)?

- Baseline control framework specifically designed for managing risk in the Cloud Supply Chain:
  - Addressing the inter and intra-organizational challenges of persistent information security by clearly delineating control ownership.
  - Providing an anchor point and common language for balanced measurement of security and compliance postures.
  - Providing the holistic adherence to the vast and ever evolving landscape of global data privacy regulations and security standards.
- Serves as the basis for new industry standards and certifications.

CCM Control Groups:

1. Compliance (CO)
2. Data Governance (DG)
3. Facility Security (FS)
4. Human Resources (HR)
5. Information Security (IS)
6. Legal (LG) .
7. Operations Management (OM)
8. Risk Management (RI)
9. Release Management (RM)
10. Resiliency (RS)
11. Security Architecture (SA)

98 security controls in total

CSA Consensus Assessment Initiative

- A cloud supply chain risk management and due diligence questionnaire
- ~ 200 yes/no questions that map directly to the CCM, and thus, in turn, to many industry standards.
- Can be used by both CSPs for self-assessment or by potential customers for the following purposes
  - to identify the presence of security controls and practices for cloud offerings
  - procurement negotiation
  - contract inclusion
  - to quantify SLAs
- For potential customers, the CSA Consensus Assessment Initiative Questionnaire (CAIQ) is intended to be part of an initial assessment followed by further clarifying questions of the provider as it is applicable to their particular needs.
  - v1.1 published in Sept 2011; v3.0.1 is available from 2014

CAIQ Guiding Principles

The following are the principles that the working group utilized as guidance when developing the CAIQ:

- The questionnaire is organized using CSA 13 governing & operating domains divided into “control areas” within CSA’s Control Matrix structure
- Questions are to assist both cloud providers in general principles of cloud security and clients in vetting cloud providers on the security of their offering and company security profile
- CAIQ not intended to duplicate or replace existing industry security assessments but to contain questions unique or critical to the cloud computing model in each control area
- Each question should be able to be answered yes or no
- If a question can’t be answered yes or no then it was separated into two or more questions to allow yes or no answers.
- Questions are intended to foster further detailed questions to provider by client specific to client’s cloud security needs. This was done to limit number of questions to make the assessment feasible and since each client may have unique follow-on questions or may not be concerned with all “follow-on questions

CAIQ Questions and Mapped Standards

- Control Group, Control Group ID (CGID) and Control Identifier (CID) all map the CAIQ question being asked directly to the CCM control that is being addressed.
- Relevant compliance and standards are mapped line by line to the CAIQ, which, in turn, also map to the CCM. The CAIQ v1.1 maps to the following compliance areas – HIPPA, ISO 27001, COBIT, SP800_53, FedRAMP, PCI_DSS, BITS and GAPP. V1.2 will additionally include mappings to Jericho Forum and NERC CIP.
- Each question can be answered by a provider with a yes or no answer.

CSA STAR: Security, Trust and Assurance Registry

- Public Registry of Cloud Provider self assessments
- Leverages GRC Stack Projects
  - Consensus Assessments Initiative Questionnaire
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
- Documents the security controls provided by various cloud computing offerings
- Encourage transparency of security practices within cloud providers
- Permanent effort to drive transparency, competition, innovation and self regulation with agility – crowdsourcing cloud security

CCM™ Cloud Controls Matrix

CAI™ Consensus Assessments Initiative

CSA STAR Compliance Levels

LEVEL ONE: CSA STAR Self-Assessment

- CSA STAR Self-Assessment is a free offering that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with.
- Cloud providers either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), or to submit a report documenting compliance with Cloud Controls Matrix (CCM).
- This information then becomes publicly available, promoting industry transparency and providing customer visibility into specific provider security practices. www.cloudsecurityalliance.org/star/self-assessment/

LEVEL TWO: CSA STAR Attestation

- CSA STAR Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix.
- STAR Attestation provides for rigorous third party independent assessments of cloud providers. www.cloudsecurityalliance.org/star/attestation/

LEVEL TWO: CSA STAR Certification

- The CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider.
- The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2005 management system standard together with the CSA Cloud Controls Matrix. www.cloudsecurityalliance.org/star/certification/

LEVEL THREE: CSA STAR Continuous Monitoring

- Currently under development and scheduled for 2015 release, CSA STAR Continuous Monitoring enables automation of the current security practices of cloud providers.
- Providers publish their security practices according to CSA formatting and specifications, and customers and tool vendors can retrieve and present this information in a variety of contexts. www.cloudsecurityalliance.org/star/continuous/

STAR Listing Process

- Provider fills out CAIQ or customizes CCM
- Uploads document at /star
- CSA performs basic verification
  - Authorized listing from provider
  - Delete SPAM, “poisoned” listing
  - Basic content accuracy check
- CSA digitally signs and posts at /star
- Does not provide automation, 3rd party assessment, relative/absolute scoring, real-time controls monitoring, etc
- Ultimate assurance is real time GRC (enabled by CloudAudit) complemented by CSA STAR and 3rd party attestation.

Why not certification or 3rd party assessment?

- Complex to do certification right
  - Many uses of cloud, many customer needs
  - Different risk profiles for each
- CSA supporting broad industry consortia and standards bodies
  - ISO, ITU-T
  - Common Assurance Maturity Model (CAMM – 3rd Party assessment)
  - GRC Stack aligns with common requirements (e.g. PCI/DSS, HIPAA, FedRAMP, 27001, CoBIT, etc)
- Self assessment & transparency complements all
  - STAR could be part of SSAE 16 SOC II report (SAS 70 replacement)

Demo/Hands on

Cloud Compliance Assessment tools

- Microsoft Cloud Security Readiness tool

  https://roianalyst.alinean.com/msft/AutoLogin.do?d=5636122870850885 25

- CSA CAIQ and PCI DSS Dashboard
  - CSA **Cloud Controls Matrix (CCM) v3.0.1**

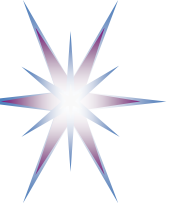
    https://cloudsecurityalliance.org/research/ccm/

    https://downloads.cloudsecurityalliance.org/initiatives/ccm/ccm-v3.0.1.zip
  - CSA Consensus Assessment Initiative Questionnaire (CAIQ) v3.0.1

    https://cloudsecurityalliance.org/research/cai/

Summary and take away

- Cloud compliance provides a basis for wider cloud services adoption and inter-cloud integration.
  - Cloud compliance provides a basis for risk assessment, SLA definition and decision making when moving services to cloud
- Compliance is supported by numerous standards, legislation, regulatory guidelines and industry best practices that jointly define a compliance framework
  - Knowing major cloud compliance standards is necessary for correct cloud services, design, deployment and operation
- PCI DSS Cloud Computing Guidelines provides invaluable source best practices information and practical recommendations for all categories of cloud specialists and practitioners
- Data Protection and Privacy in cloud is regulated by not less numerous group of standards and regulatory document
  - Personal data protection is an important area of governmental and inter-governmental regulation. EU-US Safe Harbor Framework is one of such international frameworks



Notes