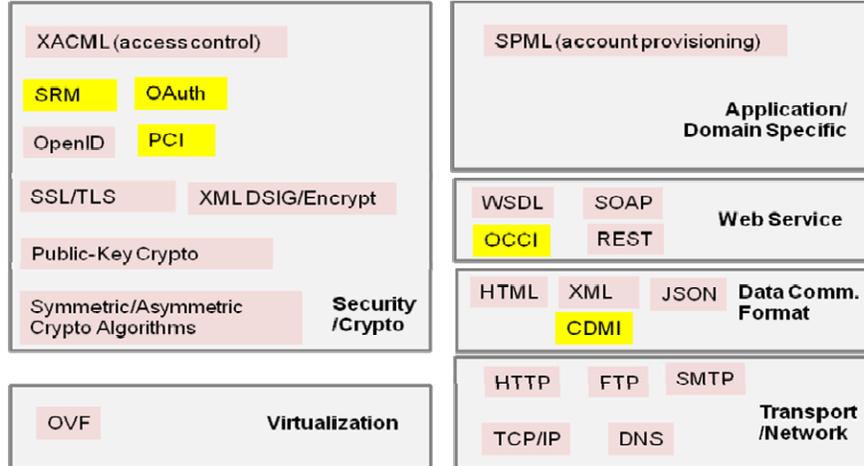


List of Relevant Cloud Computing Standards

1. Overview of the standards related to cloud computing (from Lee Badger’s slides):



2. Standards designed specifically for cloud computing:

Standard Name	Open Virtualization Format (OVF) http://dmtf.org/standards/ovf		
Developed By	Distributed Management Task Force (DMTF) http://dmtf.org/		
Goals	OVF is a packaging standard designed to address the portability and deployment of virtual appliances. OVF enables simplified and error-free deployment of virtual appliances across multiple virtualization platforms. OVF is a common packaging format for independent software vendors (ISVs) to package and securely distribute virtual appliances, enabling cross-platform portability. By packaging virtual appliances in OVF, ISVs can create a single, pre-packaged appliance that can run on customers’ virtualization platforms of choice.		
Stand-Related Work	Document Released	Status	Categorization
	OVF v1.1.0, 01/20/2010	Standard	IaaS, Interoperability

Standard Name	Open Cloud Computing Interface (OCCI) http://www.occ-wg.org		
Developed By	Open Grid Forum http://www.gridforum.org/		
Goals	The OCCI describes APIs which will enable cloud providers to expose their services. It focuses on “Infrastructure as a Service” based clouds and allows the deployment, monitoring and management of virtual workloads (like virtual machines).		
Stand-Related Work	Document Released	Status	Categorization
	Open Cloud Computing Interface - Use cases and requirements for a Cloud API, 01/2010 http://forge.ogf.org/sf/docman/do/downloadDocument/projects.occ-wg/docman.root.drafts/doc15732	Draft	IaaS, Manageability

Standard Name	Cloud Data Management Interface (CDMI) http://www.snia.org/tech_activities/standards/curr_standards/cdmi/		
Developed By	Storage Networking Industry Association (SNIA) http://www.snia.org/home/		
Goals	CDMI defines the functional interface that applications will use to create, retrieve, update and delete data elements from the Cloud. As part of this interface the client will be able to discover the capabilities of the cloud storage offering and use this interface to manage containers and the data that is placed in them. In addition, metadata can be set on containers and their contained data elements through this interface.		
Stand-Related Work	Document Released	Status	Categorization
	Cloud Data Management Interface, v1.0, 04/2010	Standard/SNIA <i>Technical Position</i>	Storage, Interoperability
	Cloud Data Management Interface Reference Implementation, software download, 06/2010	Working Draft	Storage, Interoperability

Standard Name	N/A (Cloud Management Standards ???) http://dmf.org/standards/cloud		
Developed By	Distributed Management Task Force (DMTF) http://dmf.org/		
Goals	DMTF forms workgroups to address interoperability for cloud systems. The workgroup is focused on standardizing interactions between cloud environments by developing specifications that deliver architectural semantics and implementation details to achieve interoperable cloud management between service providers and their consumers and developers.		
Stand-Related Work	Document Released	Status	Categorization
	Use Cases and Interactions for Managing Clouds, 06/18/2010	White paper	Manageability
	Architecture for Managing Clouds, 06/18/2010	White paper	Manageability
	Interoperable Clouds, 11/11/2009	White paper	Interoperability

Standard Name	N/A (Cloud Security Standards ???) http://www.cloudsecurityalliance.org/Research.html		
Developed By	Cloud Security Alliance (CSA) http://www.cloudsecurityalliance.org/		
Goals	The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing..		
Stand-Related Work	Document Released	Status	Categorization
	Guidance for (Cloud) Identity & Access Management, v2.1, 04/2010	White Paper/Guidance	Cloud Security, IDM and Access Control
	Security Guidance for Critical Areas of Focus in Cloud Computing, v2.1, 12/2009	White Paper/Guidance	Cloud Security in General
	Guidance for (Cloud) Application Security, v2.1, 07/28/2010	White Paper/Guidance	Cloud Security, Application
	Top threats to cloud computing v1.0, 03/2010	Research report	Cloud Security

3. Other relevant standards:

- **Application/Domain Specific**

Standard Name	Service Provisioning Markup Language (SPML) http://www.oasis-open.org/specs/#spmlv2.0		
Developed By	Organization for the Advancement of Structured Information Standards (OASIS)		
Goals	SPML is an XML-based framework for exchanging user, resource and service provisioning information between cooperating organizations. The goal of SPML is to allow organizations to securely and quickly set up user interfaces for Web services and applications, by letting enterprise platforms such as Web portals, application servers, and service centers generate provisioning requests within and across organizations.		
Stand-Related Work	Document Released	Status	Categorization
	SPML v2.0, 04/2006	Standard	Application

- **Web Service**

Standard Name	Simple Object Access Protocol (SOAP) http://www.w3.org/2000/xml/Group/#drafts		
Developed By	The XML Protocol Working Group of the World Wide Web Consortium (W3C)		
Goals	SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.		
Stand-Related Work	Document Released	Status	Categorization
	SOAP v1.2, 06/24/2003	Standard/W3C recommendation	IaaS, Manageability

Standard Name	Web Services Description Language (WSDL) http://www.w3.org/TR/wsdl20/		
Developed By	The World Wide Web Consortium (W3C)		
Goals	WSDL is an XML language for describing Web services. WSDL defines the core language which can be used to describe Web services based on an abstract model of what the service offers. It also defines the conformance criteria for documents in this language.		
Stand-Related Work	Document Released	Status	Categorization
	WSDL v2.0, 06/2007	Standard/W3C recommendation	IaaS, Manageability

REST (Representational State Transfer):

Representational State Transfer (REST) is a style of software architecture for distributed hypermedia systems such as the World Wide Web. The REST architectural style was developed in parallel with the HTTP/1.1 protocol, based on the existing design of HTTP/1.0. The largest known implementation of a system conforming to the REST architectural style is the World Wide Web.

- **Security/Crypto**

Standard Name	eXtensible Access Control Markup Language (XACML) http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml		
Developed By	OASIS		
Goals	XACML is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies. XACML offers a vocabulary for expressing the rules needed to define an organization's security policies and make authorization decisions. XACML has two basic components: (1) an access-control policy language that lets developers specify the rules about who can do what and when; (2) a request/response language that presents requests for access and describes the answers to those queries.		
Stand-Related Work	Document Released	Status	Categorization
	XACML v2.0, 02/2005.	Standard	Security/Access Control

Standard Name	OAuth (Open Authorization Protocol) http://datatracker.ietf.org/wg/oauth/charter/		
Developed By	OAuth working group within the IETF		
Goals	OAuth is an open standard for authorization. It allows users to share their private resources (e.g. photos, videos, contact lists) stored on one site with another site without having to hand out their credentials, typically username and password.		
Stand-Related Work	Document Released	Status	Categorization
	OAuth 1.0, 04/2010	Standard/RFC 5849	Security/Authorization

Standard Name	PCI Data Security Standard https://www.pcisecuritystandards.org/security_standards/index.php		
Developed By	PCI Security Standards Council https://www.pcisecuritystandards.org/		
Goals	PCI Data Security Standard (PCI DSS) provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.		
Stand-Related Work	Document Released	Status	Categorization
	PCI DSS v2.0, 10/28/2010	Standard	Security

Standard Name	OpenID http://openid.net/		
Developed By	PCI Security Standards Council https://www.pcisecuritystandards.org/		
Goals	PCI Data Security Standard (PCI DSS) provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.		
Stand-Related Work	Document Released	Status	Categorization
	PCI DSS v2.0, 10/28/2010	Standard	Security

Standard Name	Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)		
Developed By	TLS is an IETF standards track protocol. SSL specifications is developed by Netscape Corporation.		
Goals	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that "provide communications security over the Internet". TLS and SSL encrypt the segments of network connections above the Transport Layer, using symmetric cryptography for privacy and a keyed message authentication code for message reliability.		
Stand-Related Work	Document Released	Status	Categorization
	SSL v3.0, 1996 TLS v1.2, 08/2008.	Standard/RFC 5246	Security

Standard Name	XML signature (XMLDSig) http://www.w3.org/TR/xmlsig-core/		
Developed By	World Wide Web Consortium (W3C)		
Goals	XML signatures can be used to sign data—a resource—of any type, typically XML documents, but anything that is accessible via a URL can be signed. An XML signature used to sign a resource outside its containing XML document is called a detached signature; if it is used to sign some part of its containing document, it is called an enveloped signature; if it contains the signed data within itself it is called an enveloping signature.		
Stand-Related Work	Document Released	Status	Categorization
	XML signature v2, 06/10/2008	Standard/W3C Recommendation	Security

Standard Name	XML Encryption Syntax and Processing http://www.w3.org/TR/xmlenc-core/		
Developed By	World Wide Web Consortium (W3C)		
Goals	The mission is to develop a process for encrypting/decrypting digital content (including XML documents and portions thereof) and an XML syntax used to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it.		
Stand-Related Work	Document Released	Status	Categorization
	XML Encryption Syntax and Processing, 12/10/2002	Standard/W3C Recommendation	Security

--	--	--	--

SRM (Security Reference Monitor):

The Security Reference Monitor is the kernel mode component that does the actual access validation, as well as audit generation.

Public-Key Crypto:

Public-key cryptography is a cryptographic approach which involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. The asymmetric key algorithms are used to create a mathematically related key pair: a secret private key and a published public key. Use of these keys allows protection of the authenticity of a message by creating a digital signature of a message using the private key, which can be verified using the public key. It also allows protection of the confidentiality and integrity of a message, by public key encryption, encrypting the message using the public key, which can only be decrypted using the private key.

Examples of well-regarded asymmetric key techniques for varied purposes include: Diffie–Hellman key exchange protocol, DSS (Digital Signature Standard), ElGamal, Various elliptic curve techniques, Various password-authenticated key agreement techniques, Paillier cryptosystem, RSA encryption algorithm (PKCS#1), Cramer–Shoup cryptosystem, etc.

Symmetric-key algorithms:

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption etc. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

Symmetric-key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits and encrypt them as a single unit. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks.

Some examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, TDES, and IDEA.

- **Data Communication Format**

Standard Name	HyperText Markup Language (HTML) http://www.w3.org/TR/html401/
Developed By	World Wide Web Consortium (W3C)
Goals	HTML is the predominant markup language for web pages. A markup language is a set of markup tags, and HTML uses markup tags to describe web pages.

Stand-Related Work	Document Released	Status	Categorization
	HTML v4.01, 12/2009.	Standard/W3C Recommendation	Application/Data format

Standard Name	JavaScript Object Notation (JSON) http://www.json.org/		
Developed By	State Software		
Goals	JSON is a lightweight text-based open standard designed for human-readable data interchange. It is derived from the JavaScript programming language for representing simple data structures and associative arrays, called objects. Despite its relationship to JavaScript, it is language-independent, with parsers available for virtually every programming language.		
Stand-Related Work	Document Released	Status	Categorization
	JSON RFC4627, 07/2006	Standard/RFC 4627	Application/Data format

Standard Name	Extensible Markup Language (XML) http://www.w3.org/TR/xml11/#charset		
Developed By	World Wide Web Consortium (W3C)		
Goals	XML is a set of rules for encoding documents in machine-readable form. XML's design goals emphasize simplicity, generality, and usability over the Internet. It is a textual data format with strong support via Unicode for the languages of the world. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.		
Stand-Related Work	Document Released	Status	Categorization
	XML v1.1 2 nd ed, 08/2006	Standard/W3C Recommendation	Application/Data format

- **Transport/Network**

Standard Name	Hypertext Transfer Protocol (HTTP) http://tools.ietf.org/html/rfc2616		
Developed By	Internet Engineering Task Force (IETF) World Wide Web Consortium (W3C)		
Goals	The Hypertext Transfer Protocol (HTTP) is a networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.		
Stand-Related Work	Document Released	Status	Categorization
	HTTP v1.1, RFC 2616, 06/1999.	Standard/RFC	Transport/Network

Standard Name	File Transfer Protocol (FTP) http://tools.ietf.org/html/rfc959		
Goals	FTP is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server. FTP users may authenticate themselves using a clear-text sign-in protocol but can connect anonymously if the server is configured to allow it.		

Stand-Related Work	Document Released FTP, RFC 959, 10/1985.	Status Standard/RFC	Categorization Transport/Network
---------------------------	--	-------------------------------	--

Standard Name	The Internet Protocol Suite (TCP/IP)		
Developed By	DARPA		
Goals	The Internet Protocol Suite is the set of communications protocols used for the Internet and other similar networks. It is commonly also known as TCP/IP, named from two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first two networking protocols defined in this standard.		
Stand-Related Work	Document Released RFC 675, 12/1974. RFC 1180, 01/1991.	Status Standard/RFC	Categorization Transport/Network

Standard Name	Domain Name System (DNS) http://tools.ietf.org/html/rfc1034 , http://tools.ietf.org/html/rfc1035		
Developed By	Internet Engineering Task Force (IETF)		
Goals	DNS is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.		
Stand-Related Work	Document Released RFC 1034, RFC 1035, 11/1987.	Status Standard/RFC	Categorization Transport/Network

Standard Name	Simple Mail Transfer Protocol (SMTP)		
Goals	Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.		
Stand-Related Work	Document Released SMTP RFC 5321, 2008.	Status Standard/RFC	Categorization Transport/Network

4. Other cloud standards related activities (work in progress, no published work yet):

- **Organization for the Advancement of Structured Information Standards (OASIS)**
 - **OASIS Identity in the Cloud (IDCloud) TC**, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud
 - The OASIS IDCloud TC works to address the serious security challenges posed by identity management in cloud computing. The TC identifies gaps in existing identity management standards and investigates the need for profiles to achieve

interoperability within current standards. It performs risk and threat analyses on collected use cases and produces guidelines for mitigating vulnerabilities.

- Focus: *Security/ID Management*

- **Cloud Audit**, <http://www.cloudaudit.org/>
 - The goal of CloudAudit is to provide a common interface and namespace that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology.
 - The entire organization is dedicated to cloud computing security, the audit aspects. Launched in 01/2010. It is now CSA (Cloud Security Alliance) project.
 - The group uses <http://groups.google.com/group/cloudaudit>, as the main communication forum.
 - Focus: *Security (providers to automate the Audit, Assertion, Assessment, and Assurance (A6))*

- **The Cloud Computing Interoperability Forum** <http://www.cloudforum.org/>
 - The Cloud Computing Interoperability Forum (CCIF) is an open, vendor neutral, not for profit community of technology advocates, and consumers dedicated to driving the rapid adoption of global cloud computing services. CCIF shall accomplish this by working through the use open forums (physical and virtual) focused on building community consensus, exploring emerging trends, and advocating best practices / reference architectures for the purposes of standardized cloud computing.
 - CCIF is working on *Unified Cloud Interface (UCI)*. UCI is an attempt to create an open and standardized cloud interface for the unification of various cloud api's. A singular programmatic point of contact that can encompass the entire infrastructure stack as well as emerging cloud centric technologies all through a unified interface. One of the key drivers of the unified cloud interface is to create an api about other api's. A singular programmatic point of contact that can encompass the entire infrastructure stack as well as emerging cloud centric technologies all through a unified interface.
 - Focus: *Interoperability*

- **European Telecommunications Standards Institute(ETSI)**, <http://www.etsi.org/>
 - **Technical Committee/TC CLOUD** (previously TC GRID)
 - The goal of TC CLOUD is to address issues associated with the convergence between IT (Information Technology) and Telecommunications. The focus is on scenarios where connectivity goes beyond the local network. Since TC CLOUD has particular interest in interoperable solutions in situations which involve contributions from both the IT and Telecom industries, the emphasis is on the Infrastructure as a Service (IaaS) delivery model. TC CLOUD focuses on interoperable applications and services based on global standards and the validation tools to support these standards. TC CLOUD will address interoperability aspects of end-to-end applications and develop formal test specifications to support them. The technical scope of TC CLOUD is broad. It includes: resource and service access, protocols and middleware, security.
 - Focus: *Network (?)*

- Document released:
 - Research report: **CLOUD: Initial analysis of standardization requirements for Cloud services**, 04/2010