CIRRUS – The 3rd Workshop

Introduction and Project Overview

Aljosa Pasic, Atos

Vienna, 19 Nov 2013

Project Objectives

- Certification, InteRnationalisation and standaRdization in cloUd Security (CIRRUS)

- Bring together stakeholders views : industry organizations, law enforcement agencies, cloud services providers, standard and certification services organizations, cloud consumers, auditors, data protection authorities, policy makers, software component industry etc.

- Address emerging and future challenges for “building the chain of trust”, coming from multiple sources: research project results, policies and legislations, operational agreements, compliance and auditing trends etc

- CIRRUS clouds are among the highest altitude clouds in troposphere: CIRRUS project also aims to provide “high-level, high-impact” support and coordination for European ICT security research projects..

Basic Project Data

ATOS SPAIN SA	ATOS
CLOUD SECURITY ALLIANCE (EUROPE) LBG	CSA
AUSTRIAN STANDARDS INSTITUTE OSTERREICHISCHES NORMUNGSINSTITUT	ASI
Portakal Teknoloji Egitim Danismanlik Yazilim Turizm Taahhut Ve Ticaret Limited Sirketi	PKT
独立行政法人情報処理推進機構	IPA
GRANT THORNTON FORENSIC & INVESTIGATION SERVICES BV	GTFIS

- 24 Months, from 01/10/2012 to 30/09/2014
- EC Funding 679,512 Euros
- Meetings and milestones
  - Kick off 09/10/2012 (Atos offices, London)
  - The first Workshop 28/2/2013 (Cloudscape, Brussels)
  - The second Workshop 24/7/2013 (Compsac, Kyoto, Japan)
  - The third Workshop 19/11/2013 (CEN workshop agreement, Vienna)

Methodology

Digital Agenda, European Cloud Partnership, market trends, EU regulation / directives

ETSI SotA, NIST Roadmap, ENISA , BMWI

FP7 research project results, technology trends etc

Privacy by Design, "notified ID", multi-cloud settings, breach notification…

Continous monitoring, automation, machine readible policy…

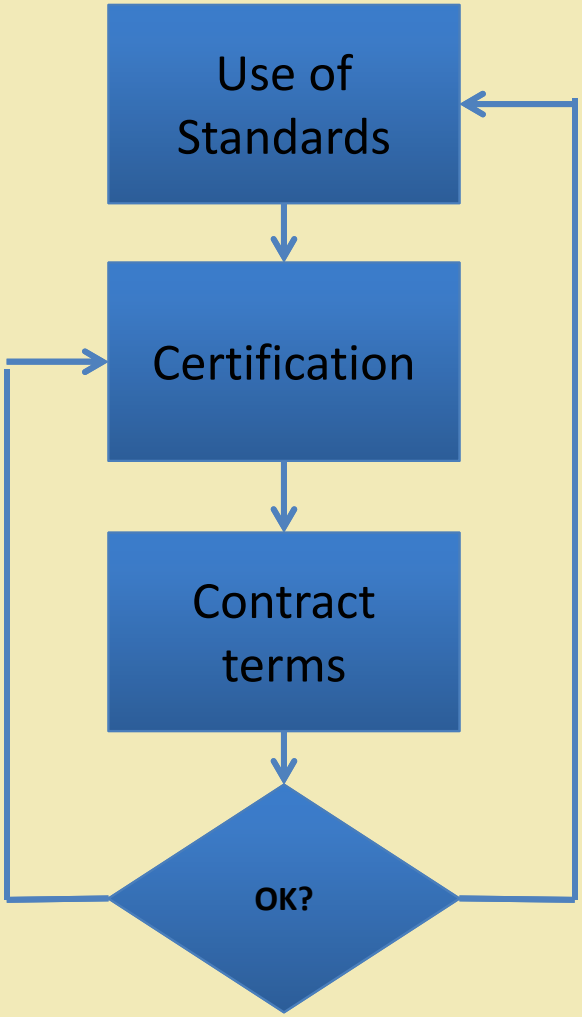
CIRRUS Contribution

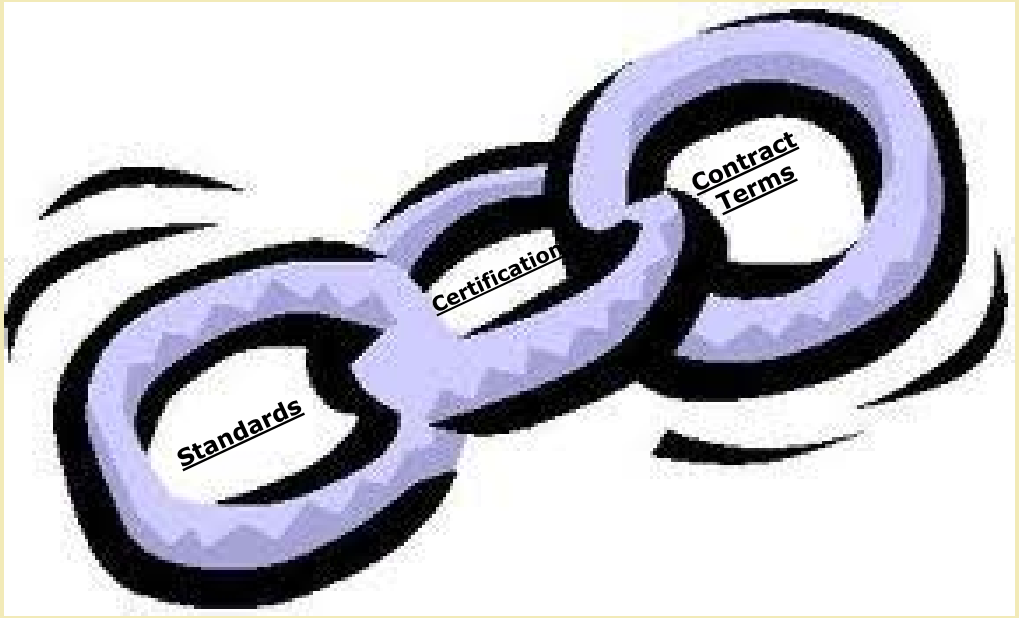

Connecting top-down
and bottom-up clouds

O1: Bring together different stakeholders and views

- Inputs/Outputs from/to Research projects : Reservoir, Siena (Cloudscape), Optimis, Passive, Tclouds, Vision-Cloud, OGF, FI-WARE (FI-PPP), CUMULUS, Cloud4SOA, Artist, TRESSCA, A4Cloud, Assert4SOA…
- Inputs from initiatives such as Trust in Digital Life, EOS, Trusted Computing, EP3R, EIT-ICT Labs, EFIA Consultation Group, Digital Europe, Business Software Alliance, Eurocloud Association, Thematic Network SSEDIC, Networks of Excellence (Nessos, Syssec), FI-WARE project, BIC, INCO-Trust, Effect+, **NIS Platform** etc
- Inputs from **Advisory Board**
- Input/Output from/to revisions of EU Legislation revision process (e.g. eIDAS, NIS or Privacy Directives/Regulations), EU policy and strategy (e.g. Digital Agenda, **European Cloud Partnership**)
- Inputs from National and International initiatives (Trustcloud, Japan, Singapore…)
- Inputs/Outputs from/to related efforts **(ETSI, ENISA, CEN)**
- Others (surveys, questionnaires…)
- http://www.cirrus-project.eu/

O2: (Connected) Challenges of the chain of trust





- Certification linked to assurance process (e.g. audit), assurance process to standards etc
- Trust linked to certification of compliance with privacy policy, policy linked to requirements, requirements linked to XXX level agreements, agreements linked to contract…

O3: High Impact for EU research projects

- Communication from EC to the European Parliament on “unleashing the potential of CC”, three cloud-specific actions
  - Cutting through the Jungle of Standards
  - Safe and Fair Contract Terms and Conditions
  - Establishing a European Cloud Partnership to drive innovation and growth from the public sector
- Links to European Cloud Partnership (ECP) and SIG, ISO 27017/18 process, ETSI and ENISA
- EESC comments on EC communication: from cloud-active to cloud-productive, from top-down to bottom up

CIRRUS D4.1 Standardisation and Certification Status

- Formal standards
- Specifications
- Workshop agreements
- Conformance/test
- Reports/best practise

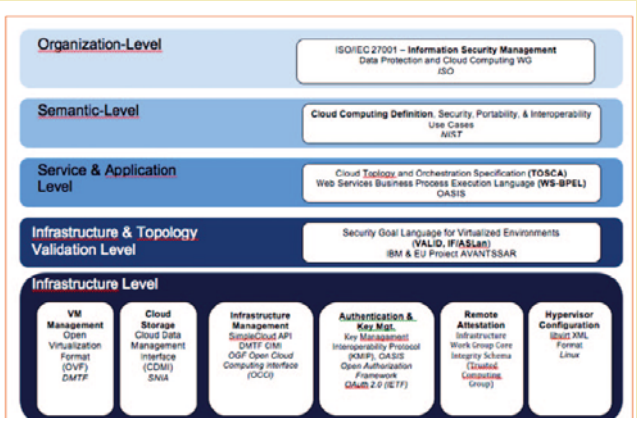
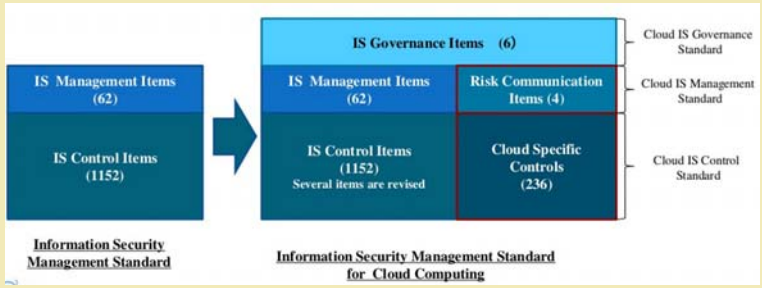


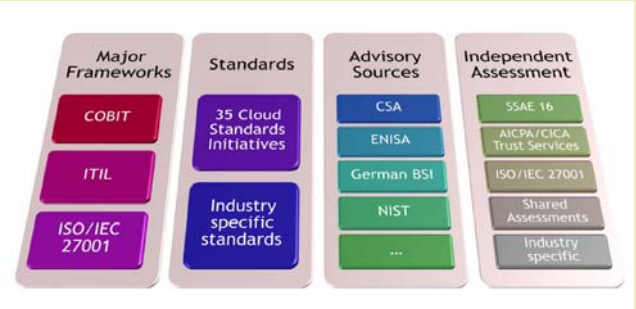
Figure 11: TClouds Map of Open Standards

Field	Type of standard	Examples
Technology	File & exchange format	*OVF, EC2, USDL, CIM SVM...*
	Programming models	*MapReduce, JAQL, PIG, HIVE*
	Protocols & interfaces	*OCCI, CDMI, CloudAudit, Google DLF, ...*
	Standard components & reference architectures	*OpenStack, OSGI, NIST RM, IBM RM, DMTF, CTP, ...*
	Benchmarks & tests	*Benchmarking Suites, Security Assessment, ...*
Management	Business models	*IaaS, PaaS, SaaS operating models, ...*
	Service Level Agreements	*WS-Agreement, Business SLAs, ...*
	Condition of contracts	*EVB-IT, EU SVK, components for AGB, EULA*
	Management models & processes	*ISO 27001/27002, ITIL, COBIT, ...*
	Controlling models & processes	*SSAE, SAS 70, ...*
	Guidelines	*BSI requirements, NIST UC, EuroCloud LRD&C*
Legal	Legal requirements	*EU data protection directive, BDSG, Safe Harbor*
	Voluntary commitments	*Open Cloud Manifesto, ...*
	Company policies	*Internal policies, ...*

Title	Acronym	Organisation	Description	Status	Type of initiative
Transport Layer Security	SSL/TLS	IETF	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. The SSL protocol allows mutual authentication between a client and server and the establishment of an authenticated and encrypted connection. TLS is a protocol from the IETF based on SSL.	Operational	II - Technical specification
XML Http Request	XHR	W3C	XHR stands for XML HTTP Request. XHR is an API that is used to enable the request/response process over the HTTP communication protocol. It is normally implemented as part of the javascript engine of web browsers allowing developers to write code that synchronously or asynchronously make http requests and handle http responses. The API is very flexible and supports several data formats for the representation of the requests and responses such as JSON, HTML and XML. That diversification of the data that can be used sets XHR a highly adopted technology allowing for the development of more user friendly interfaces that offer a richer and more easy to use web applications.	Operational	II - Technical specification
Javascript Object Notation	JSON	IETF	JSON is a text-based open standard designed for human-readable data interchange. It is derived from the JavaScript scripting language for representing simple data structures and associative arrays, called objects.		I Formal Standards
Cloud Application Management for Platforms	CAMP	OASIS	CAMP: Cloud Application Management for Platforms: defines the artifacts and APIs that need to be offered by a Platform as a Service (PaaS) cloud to manage the building, running, administration, monitoring and patching of applications in the cloud	Early stage Working Group, no publications yet.	II - Technical specification
-	ODCA Usage Model: Platform as a Service (PaaS) Interoperability	ODCA	The ODCA PaaS Interoperability Usage Model was written to encourage operation of cloud applications across providers, rapid integration with consumer orchestration engines, and automatable configuration and operation of both the PaaS container and the execution of the application itself	Public	V - Technical reports
Open Virtualisation Format	OVF	DMTF/ISO /ANSI	Open Virtualization Format (OVF) is an open standard for packaging and distributing virtual appliances or more generally software to be run in virtual machines. OVF is a common packaging format that enables cross-platform portability.	Operational	I Formal Standards
Virtual Machine Disk	VMDK	VMWare	Standard format for virtual storage volumes	Operational	II - Technical specification
Virtual Disk	VDI	Oracle	Virtual storage volume format	Operational	II - Technical specification
-Hard	VHD	Microsoft	Virtual storage volume format	Operational	II - Technical specification
-vices -ion -ge	WSDL (for the SaaS layer)	W3C	WSDL is a standard way of describing web services that enhances and makes possible service integration. It is based on XML and provides a formal way of defining information such as service invocation parameters, service name and type of the expected result. WSDL makes it possible for completely heterogeneous services to integrate irrespective of the programming language or the platform that they run on.	Operational	I Formal Standards
-sed -se -ment	WBEM	DMTF	A set of management and Internet standard technologies developed to unify the management of distributed computing environments.	Operational	II - Technical specification
-n -tion	CIM suite of standards - e.g. CIM-	DMTF	CIM provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. CIM's common definitions enable vendors to exchange semantically rich management	Operational	II - Technical specification

D2.2 Green Paper Draft





- Idenity Management Services : One size does not fit all
  - Policy: Include PIA in the loop
  - Standards: for new (or improved) services (fine grained auth, delegation/mandates etc)
  - Cert: (Risk based) Mapping of QAA/LoA to service levels and user types
  - Business: Emerging decoupling of IdM services e.g. Assurance as a service
- Data Protection and Privacy
  - Policy: Deeper analysis of complex models (joint ownership, joint controllers)
  - Standards: audit trail formats and runtime events
  - Cert: Machine readible PLA, con-mon audit based
  - Business: Link privacy to “trust as a service”
- Runtime monitoring
  - Business: Decouple signalling from monitoring
  - Standards: “generic” data, used in multiple assessments
  - Research: Quality of MonData: integrity, timeliness, trustworthiness, confidentiality…
  - Research: Resilience of monitoring services


Enjoy your CIRRUS
cloud today!!!