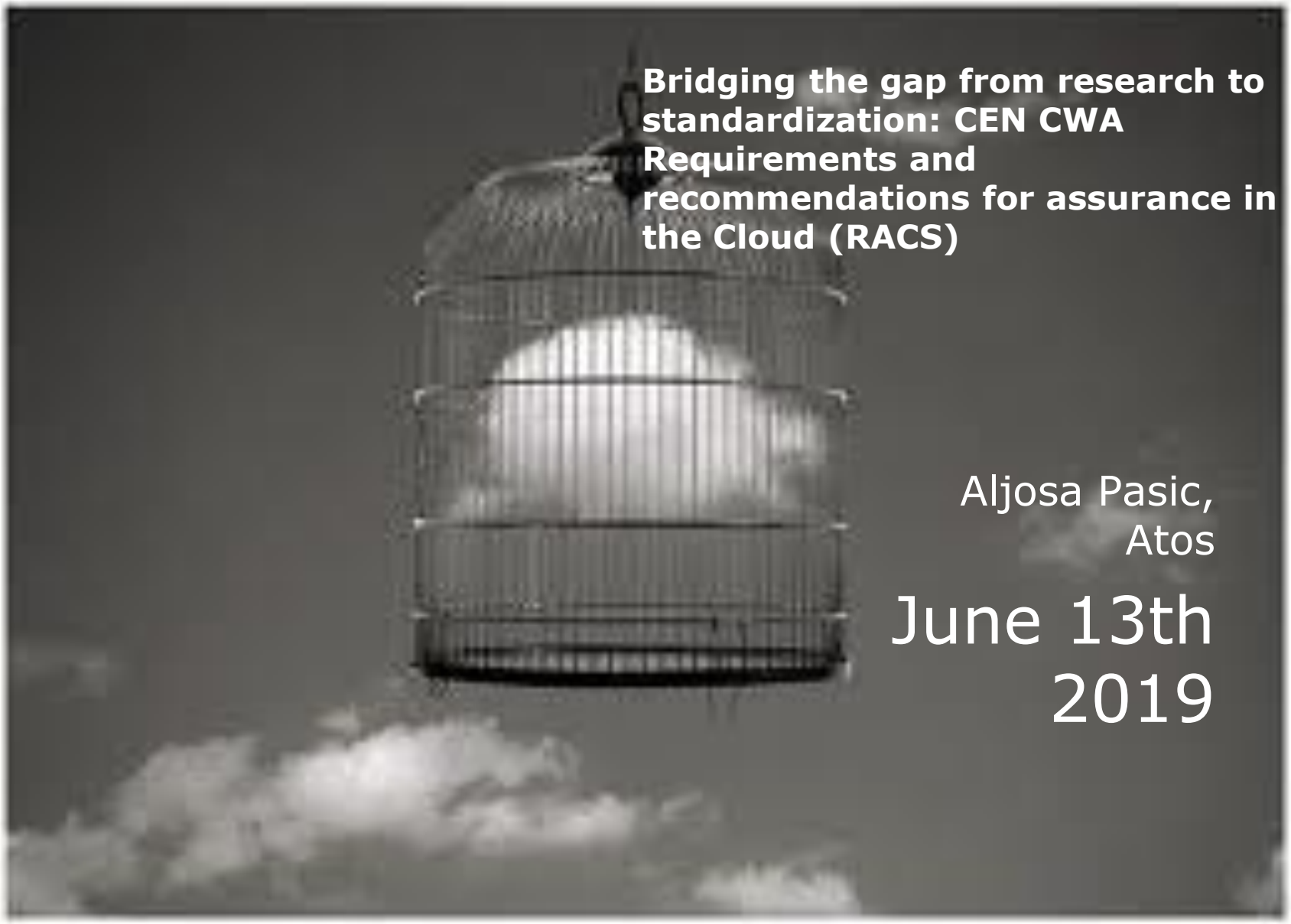

Bridging the gap from research to standardization: CEN CWA Requirements and recommendations for assurance in the Cloud (RACS)

Aljosa Pasic,
Atos

June 13th 2019

Atos

Context: CIRRUS Project Outline

- Certification, InteRnationalisation and standaRdization in cloUd Security (CIRRUS)
- **Bring together** representatives of 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 future** cloud security challenges, coming from multiple sources: national legislations, operational agreements, compliance auditing, certification, control, confidentiality, 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..

Problem Statement and Objectives

- The lack of trust is one of the main constraints for a wider cloud adoption
- The aim was to reach an **acceptable trade-off** between different views or perspectives (e.g. consumers request of transparency and the provider need to protect business, between privacy and accountability) and provide consolidated opinion as an input to EU policy making
- Need to **support ongoing research** projects by coordinated dialogue that will lead to convergence of efforts on e.g. Cloud Security Taxonomy, collection of inputs to Certification and Standardization efforts

Project Partners

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

- 24 Months, from 01/10/2012 to 30/09/2014
- EC Funding 679,512 Euros
- Kick off 09/10/2012 at Atos offices in London
- First Workshop on 28/2/2013 in Brussels
- Last workshop in 2015 at ASI premises in Vienna

How did we get to CWA ?

- Inputs from FP6 and FP7 Research projects and initatives: Reservoir, Siena (Cloudscape), Optimis, Passive, Tclouds, Vision-Cloud, OGF, FI-WARE (FI-PPP), CUMULUS etc
- Link to 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+ etc
- Advisory Board feedback
- Input/Output from/to revisions of EU Directives (e.g. on Critical Infrastructure Protection or Privacy Directives), EU policy and strategy (e.g. Digital Agenda, European Cloud Partnership)

CWA content

- All requirements are also recommendations, but not all recommendations can be translated into operational requirements for cloud security assurance
- Security controls (sometimes referred as countermeasures or safeguards) are standard mechanisms or actions that correspond to one or more security requirements

CWA content

- Cloud reference models provide abstract synopses of the cloud infrastructure. Models can be classified according to different criteria (e.g. distinguishing between business-oriented and architecture models).
- The most important "general purpose" security control frameworks are ISO/IEC 27001/27001, the Information Security Forum's Standard of Good Practice for Information Security, NIST SP 800-53, ISACA COBIT, PCI, NIST, Jericho Forum and NERC. The CSA CCM is the most well-known cloud specific control framework that gives detailed understanding of security concepts and principles in 13 cloud computing domains.
- Audit
  - What: which evidences are feasible?
  - How: attestation, the auditor does not determine whether the standards are valid. Certification, the result of an audit has to measure compliance with prescriptive standards. Next Big Thing: automation and continuous monitoring

Recomendations

- RACS recommendations or requirements include:
  - Which components must or should generate events to be monitored?
  - Which types of events must or should be monitored?
  - Which data characteristics must or should have been stored for each type of event (e.g., username and source IP address for authentication attempts)?
  - How the confidentiality, integrity, and availability of each type of event must or should be protected while in transit through monitoring infrastructure?
  - Possibility to have machine-readable policies for event collection?

Lessons learned

- Selection of topic
  - 100% trending topic at that time…
  - Which caused many to work on this in paralel (ENISA, ETSI, CSA, Eurocloud, International…)
- Selection of instrument (CWA)
  - Good visibilty for EU projects
  - Standardisation coordination was an issue
- Collection of contributions from EU projects:
  - Many projects were happy to contribute
  - Few projects were not cooperative. Why?
- Consolidation and editing
  - Great work from several persons
  - Wrong selection of (some) partners
- Publishing and use of RACS CWA
  - ASI and CEN support was crutial
  - Publishing is not sufficient – promotion is needed

Thank you

Aljosa Pasic
aljosa.pasic@atos.net

14/06/2019

Atos

Initiative	Status at CWA publication date	Relation with CWA
ISO standards (27009, 27017, 27018)	ongoing	CWA RACS is providing input regarding future emerging requirements
ENISA CCSM and CCSL projects	Draft results presented on November 12th 2014	These projects are mainly focused on certification schemes. They will identify controls used in cloud certification schemes
ETSI CSC	Finished in 2013. A new project expected to start in 2015	Input was given to the CSC in 2013 from CIRRUS members.
European Cloud Partnership ECP and Select industry groups (SIG)	Ongoing, draft code of conduct and SLA delivered	CWA RACS will provide requirements to these groups