Certification, InteRnationalisation and standaRdization in cloUd Security (CIRRUS) aims to 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. with diverse interests in security and privacy issues in cloud computing.

3rd CIRRUS workshop

On November 19th 2013 CIRRUS will hold its third workshop in Vienna, organised by Austrian standards institute at their premises (https://www.austrian-standards.at/en/infopedia-topic-center/infopedia-articles/cirrus/). This third workshop is aimed at preparing a CEN Workshop Agreement (CWE). The proposed CEN Workshop will use the findings of the several projects co-funded by the European Commission, and provide recommendations for the best practice and technical specifications in the area of assurance for continuous monitoring and certification of cloud computing services. The CIRRUS project supports the European Commission, ETSI and ENISA in the implementation of the European Cloud Strategy, but is also expected to link with bodies and institutions outside Europe and to have an impact globally. The Workshop will be open to any interested party in order to allow all parties interested in the activity to discuss and contribute to the development of the future CWA.

Date/time: **Tuesday 19 November** 2013 from 09.00 till 18.00 hrs.

Venue: Heinestrasse 38, Vienna (1001/1003); Austria

Agenda:

08.30 – 09.00	Registration
09.00 – 09.15	Opening of the workshop by Atos and ASI
09.15 – 10.35	First session – **Status overview of standardisation and certification initiatives in Cloud Security** Chair and speakers include Dr. Tobias Höllwarth (Eurocloud), Arjan de Jong (Ministry of Interior, The Netherlands), Daniele Catteddu (Cloud Security Alliance), Dr. Stefan Weisgerber, (Convenor of CEN/CENELEC BT Working Group 6 „ICT Standardization Policy “)
10.35 - 10.50	Networking coffee break & exhibition
10:50 – 12:10	Second session – **Assurance through testing, validation and continous monitoring** – Chair and speakers include Bora Gungoren (PKT), Dr. Eike Wolf (independent consultant, Europrise), Elmar Husman (IBM, TCloud project), Philippe Massonet (CETIC)
12:10 – 12:30	Discussion
12.30 – 14.00	Networking lunch
14.30 – 15.50	Third session – **SLA and security** Chair and speakers include Neeraj Suri (University of Darmstadt), Paolo Mori (CNR), Siad Tabet (EMC), Dominic Mylo (Atos)
15.50 – 16.10	Networking coffee break
16.10 – 17.30	Fourth session – **Hybrid, incremental and multilayer security certification** Chair and speakers include Marian Bubak (AGH), Jean Christophe Pazzaglia (SAP), George Spanoudakis (City University), Eric Hibbard (Hitachi)
17.30 – 18.00	Discussion and Wrap up

The detailed agenda with presentation titles and abstracts are presented on the next pages. To attend the workshop, please register in advance at www.cirrus-project.eu or send an email with your full name and affiliation to k.stumwoehrer@austrian-standards.at. The workshop and lunch are free of charges for registered participants.

The CIRRUS project partners are:

Join the CIRRUS Linkedin group at https://www.linkedin.com/groups/CIRRUS-Cloud-Security-4710127 to stay updated on the first workshop and future CIRRUS events.

Speakers and abstracts

1. Dr. Tobias Höllwarth (Eurocloud, Vienna,. Austria)

Titlte: Cloud Computing -Standards, SLA and Certification - The Main opportunities, challenges and risks for Companies

Abstract:

In his speech, Dr. Tobias Höllwarth will address the following questions: What are the main opportunities, challenges and risks for SMEs on both provider and consumer side? What kind of activities around Cloud-Standards, Cloud-certification, and legal framework can be expected from ISO, the European Community and EuroCloud Europe? What are the main EuroCloud activities? What are the possible solutions to support the challenges of Cloud adoption?

The Speaker

Dr. Höllwarth has worked as a corporate consultant specialised in IT projects for over 20 years. In addition to his work at the Vienna University of Economics and Business he also founded the company Höllwarth Consulting in the year 1991. The main focus of the consulting firm lies in the fields of: IT consulting, IT services and cloud consulting.

Tobias Höllwarth was a founding member of EuroCloud.Austria where he is today a member of the Board, a position he also holds with EuroCloud Europe. He acts as an expert for questions pertaining to certification at the Austrian Standards Institute ASI (ÖNORM) and is leader of the Austrian delegation that participates in negotiations with the International Organization for Standardization (ISO) where cloud computing is concerned. In addition to other specialist publications he is also the editor of the book "Migrating to the Cloud" whose second edition came out in 2012. Tobias Höllwarth has organised the Austrian CLOUD Congress that offers both providers and users of cloud solutions a joint platform for the exchange of ideas.

2. Arjan de Jong (Ministery of the Interior and Kingdom Relations, The Netherlands)

Title: Legal and economic aspects of Cloud Security

Abstract:

Understanding market incentives for information security is key to achieve an adequate level of information security for cloud services. Standardisation and certification can play an important role to stimulate the secure uptake of these services, both in the public and the private sector.

In this presentation, first a short overview of the 'information security market' will be given, explaining its unique dynamics and the role that regulation, certification and standardization can play. Second, the current en future EU legal framework for information security in relation to those earlier distinguished economic incentives will be discussed, after which the current developments concerning the Dutch Governmental Cloud and the role of standards therein will be presented.

The Speaker:

Arjan de Jong is a policy advisor on information security at the Ministry of the Interior and Kingdom Relations of the Netherlands. Having studied Law & IT at the University of Groningen, his specialization lies in (EU) privacy and information security law and policy, including electronic identification and trust services.

3. Daniele Catteddu (Cloud Security alliance, UK)

Title: Optimising cloud security, trust and transparency

Abstract:

This session will talk about the impact of security certifications for cloud computing. We'll discuss whether certifications are the solution to current problems such as: optimising security, increasing trust and transparency, facilitating market adoption. Governments and business users do not have simple, cost effective ways to evaluate and compare their providers' resilience, data protection capabilities and service portability. Is certification a way to overcome the barrier?

The Cloud Security Alliance launched in September 2013, in collaboration with the British Standard Institute (BSI) in 2013 and other organisations on the definition of the Open Certification Framework (OCF), an industry initiative that will allow global, trusted certification of cloud providers. How does OCF work? Does it solve the problems?

The Speaker:

Daniele Catteddu, is the Managing Director, EMEA, in Cloud Security Alliance, where he is responsible for the definition and execution of the company strategy in EU, Middle East and Africa. In past worked at ENISA (European Network and Information Security Agency), as Expert, where he was responsible of projects in the areas of Resilience and Critical Information Infrastructure Protection (CIIP). He has also worked within ENISA as a risk management expert, and in particular, having a leading role in developing EU cloud security research. Before joining ENISA, Daniele worked as an Information Security consultant, advising leading player in the banking and financial sector.

Daniele is the author of the study: "Security and Resilience in Governmental Clouds" as well as co-author of the reports: "Cloud Computing: Benefits, risks and recommendations for information security" and "Cloud Computing: Information Assurance Framework". Daniele graduated from the University of Parma (Italy) in Business Administration and Economics, and he is an ISACA Certified Information Security Manager and Certified Information Systems Auditor.

4. Dr. Stefan Weisgerber (DIN Berlin, Germany)

Title: How standards support cloud security

Abstract:

The presentation shows why standards make an essential contribution to the success of cloud computing. It gives an overview of cloud security standardization in the European and international standardization organizations and elaborates how cloud security standardization relates to other standardization work.

The Speaker

Dr. Weisgerber joined DIN Deutsches Insititut für Normung e.V. in 2006, first being responsible for the national standards committees on Information Technology and related fields. Since 2008, he is Head of Technical Department 3 within DIN's standardization division, covering the activities related to fundamental technologies, information technology, machine and plant elements, materials, security and services. Prior to these functions, he held several positions in the telecommunications industry, also with significant exposure to standardization. Dr. Weisgerber holds a Ph.D. in Theoretical Physics.

5. Bora Güngören (Portakal Teknoloji, Turkey)

Title: Interoperability Needs for Systems and Software Asssurance - From Enterprise SOA to Multiple Independent Clouds

The Speaker

Bora Güngören is currently Managing Partner for Portakal Teknoloji, a small sized software development and consultancy company, a PhD student in Management and Organization programme in Baskent University, and a part-time instructor at Bilkent University. He has experience in research, software development, and consulting diverse types of organizations in migrating towards new technologies. He has been active in professional organizations and in particular standardization efforts (JSR and more recent-ly IEEE).

6. Dr. Eike Wolf (consultant Europrise, Austria)

Title: The Cloud: IT out of the wall socket? - Design of Cloud Contracts right

Abstract:

- Subject of the contract as main problem for all cloud contracts
- Privacy and data protection according to EU laws and most neglected obligation
- Availability of the service related to data security and protection
- Warranties in respect to data as principal matter
- Indemnifications and most immoral escape clauses
- Conflict Solutions
- Insolvency of the Cloud Supplier (too big to fail?)

The Speaker:

After finishing his doctorate studies at the University of Vienna in 1978 with Doctorate of law he worked as assistance for CEO and as counsellor for a telecom industry, in a bank and for the new General Community Hospital in Vienna. Back as product manager for new networks and broadband technologies for a telecom manufacturer since 1985 and engaged in a law research group concerning software and law and writing in parallel a basic book as co-author concerning software in the Austrian civil right 1991.

Since 1996 working as a independent consultant for civil right, telecommunication and software contracts and certified by EuroPriSe as legal expert for data protection since 2010. He is also Member of the LES Austria, ÖVE, OCG, IEEE and teacher for law at the University of Applied Science at Technikum Wien and at St. Pölten.

7. Elmar Husman (IBM)

Title: Standards in privacy and security critical cloud environments - results from the TClouds EU project

Abstract:

TClouds has investigated different levels and elements of standardisation in detail. We expect to see in thefuture on the one hand interesting point solutions for cloud security and privacy problems as well as more holistic cloud services that offer different levels and packages for security and privacy. The first commercial successes have grown out of TClouds. They include the SA VE technology for security analysis of virtual systems commercialized by IBM and the enhanced Trusted Management Components and Trusted Cloud Nodes in the Trusted Infrastructure by Sirrix. Moreover, open-source toolkits like DepSky are being adopted by academic and commercial users.

The Speaker:

Elmar Husmann has over 10 years experience in running strategic innovation programmes and managing corresponding European policy relations in the domain of ICT innovation. Elmar has been a principal consultant with the German PricewaterhouseCoopers consulting practice as leader of a team on IT organization strategy. Since 2002 he is a senior managing consultant for IBM Business Consulting Services on innovation strategy and change.

In collaboration with IBM Governmental Programmes and IBM Research, he is responsible for EU innovation relations as steering committee member of the Networked European Software and Services ETP (NESSI) and as a member of the cross-ETP Group on the Future of the Internet. Elmar has also been appointed in 2011 Deputy Secretary General of the European Learning Industry Group (ELIG).

Husmann is closely involved with the set-up of a large-scale IBM research programme on the Internet of Services – including several integrated projects funded by the European Commission - jointly with IBM research labs from Haifa and Zurich. Three of these projects have been piloting IBM EU research in the domain of Cloud Computing. Since 2010 he is in particular involved in this context with the TClouds project on trustworthy cloud computing.

8. Philippe Massonet (CETIC, Belgium)

Title: Requirements for Securing Cross Cloud Deployments

Abstract:

With the increasing availablity of commercial cloud services, cloud users now need to decide how to optimaly deploy their applications accross the different cloud offerings. This means for example making decisions about which components need to stay in a private cloud, which components need to be deployed near data sources, or which components need to be deployed near or in clients premises. Security requirements of the application components and the security levels offered by cloud providers should be taken into account in making deployment decisions. This talk will start by introducing the challenges of cross cloud deployments, identify security requirements, and illustrate on a few examples how cloud security standards based on monitoring and reputation could be used in making cross cloud deployments decisions.

The Speaker:

Philippe Massonet is scientific coordinator at CETIC, a Belgian ICT applied research center. His research interest cover the areas of software and security engineering, as well as distributed systems such as Clouds and Grids. He is currently working on the PaaSage FP7 project that aims to provide a platform for optimised cross cloud deployments. He was recently coordinator of the FP7 PONTE eHealth project that investigated building decision support systems for the design of clinical trials. Philippe was responsible for the security and privacy analysis of patient data use. Previously he was responsible for dissemination and security in the RESERVOIR IST European project (Integrated project) led by IBM research. Philippe is experienced in the management of international R&D projects (Eurescom MESSAGE, IST FP6 GridTrust, and FP7 PONTE) and has been involved in many EU FP6/FP7 research projects (RESERVOIR, HPC4U, AssessGrid, CoreGrid, GridTrust, S-Cube and Oldes).

9. Prof. Dr. Neeraj Suri (TU Darmstadt, Germany)

Title: Making Security SLA's Useful

Abstract:

SLA's, as a base technique, are widely adopted in the ICT community. However their usage for security is still very much evolving. The talk discusses the specification, composition and negotiation of SLA's for Security.

The Speaker

Suri is a Chair Professor of "Dependable Systems and Software" at TU Darmstadt, Germany and is affiliated with Microsoft Research. Following his PhD at the Univ. of Massachusetts at Amherst, he has held both industry and academic positions across the US and Europe, and receiving extensive trans-national funding from the EC, German DFG, NSF/DARPA/ONR/AFOSR, NASA, Microsoft, IBM, Hitachi, GM and others. He is a recipient of the NSF CAREER award, as well as Microsoft and IBM Faculty Awards. Suri's professional services span associate Editor-in-Chief for the IEEE Trans. on Dependable and Secure Computing, editorial boards for IEEE Trans. on SW Engg., IEEE TPDS, ACM Computing Surveys, IEEE Security & Privacy and many others. He serves on advisory boards for Microsoft (Trustworthy Computing Academic Advisory Board, Strategy Advisor for MSR-ATL's) and multiple other US/EU/Asia industry, policy and university advisory boards. Suri chaired the IEEE Technical Committee on Dependability and Fault Tolerance, and it's Steering Committee.

10. Dr. Paolo Mori (Istituto di Informatica e Telematica - Consiglio Nazionale delle Ricerche, Pisa, Italy)

Title: Usage Control in Cloud Services

Abstract:

Cloud services are aimed to provide to authorized users several kind of resources on demand, and users exploit these resources to carry out their business and research processes for the time they need.

Since the usage of these resources could last a long time, i.e., many hours or even days, the corresponding access rights could expire while the accesses are still in progress.

Hence, a proper access control model, such as the Usage Control (UCON) one, must be adopted in the design of the security support for Cloud services, in order to deal with long lasting accesses.

The Speaker:

Paolo Mori is currently a researcher of the Information Security group of Istituto di Informatica e Telematica – Consiglio Nazionale delle Ricerche in Pisa. His main research interests involve trust, security and privacy, focusing on access and usage control, trust and reputation management in distributed environments, such as Grid, Cloud, and mobile devices. His interests also include security and privacy in the e-health scenario. He is co-author of more than 50 scientific papers and has been/is involved in a number of European and Italian projects on information and communication security

11. Siad Tabet (EMC, United States)

Title: Accelerating Cloud adoption with Security Level Agreements automation, monitoring and industry standards compliance

Abstract:

One of the most critical factors in the deployment of trustworthy cloud ecosystems is cloud service providers security assurance (CSP). Cloud customer expectations are getting harder to meet with the ever increasing number of CSPs and the emerging concept of cloud service composition. CPSs need to provide standard security SLAs and support their audit and reporting to enable their customers to self-manage and self-audit their cloud provisioned applications. The trust relationship in such scenarios is a many to many relationship

and requires automation and agility. There are efforts in both industry and academia with a number of encouraging initiatives including the integration of cloud-adapted risk management frameworks, SLA automation and use of public repositories. This talk will discuss these issues, the requirements for cloud security assurance and risk management frameworks, illustrated with some specific examples and scenarios. We will also provide an overview of the current standardization landscape.

The speaker:

Dr. Said Tabet is a Senior technologist and industry standards strategist in the Corporate Office of the CTO at EMC. Said is the principal representative to INCITS CS1, co-chair of the Secure Cloud Computing Ad-Hoc group, and a member of the US delegation to SC27. Dr. Tabet is also a member of the Cloud Security Alliance (CSA) International Standardization Council, co-Chair of the SME Council and co-Chair of the Cloud Security SLA working group. Dr. Tabet is a regular speaker and panelist at industry conferences and international standards meetings, authors and editor of book series and articles.

12. Mr. Dominic Mylo (Atos, Germany)

Title: Security threats and controls for cloud management

Abstract:

As a national security agency, the goal of the Federal Office for Information Security (BSI) is to promote IT security in Germany. The BSI is first and foremost the central IT security service provider for the federal government in Germany. The BSI has the ambition to address current technology and their security recommendation in their IT security methodology, which is called IT-Grundschutz.

The IT-Grundschutz standard provides security recommendations for baseline protection meant for ordinary protection requirements. The standard includes a risk based approach to enhance the baseline protection with specific security controls based on a risk assessment. For several platforms, standard applications, networks, buildings and IT-systems the IT-Grundschutz catalogues are structured in security templates called “Baustein” (means for instance a module with security measures for a Windows 2003 Server). For Cloud topics several new templates are developed in 2013 for the IT-Grundschutz catalogues.

Atos has created the security template “cloud management” for the secure operation of cloud services with a focus on private clouds. Cloud management introduces security controls established under consideration of cloud security standards (ENISA, CSA, IETF) to create confidence in the security of cloud services. The focus is on cloud users from the environment of the authorities and SMEs

The developed security template includes a list of threats and detailed security controls for cloud management. With this new security templates it is possible to certify cloud computing environments by ISO27001 with the german IT-Grundschutz standard.

The Speaker:

Dominic Mylo is working as Security Consultant for Atos Information Technolgy in Meppen, Germany since 2005. He graduates as Bachelor of Science in July 2008 and worked in parallel in SI Security Unit.

Dominic Mylo has his focus on Security Strategy and Consulting tasks where he can bring in both, the consulting and solution view as well as the auditors opinion. He is able to complement his consulting skills with technichal assessments like penetration tests and vulnerability scans. Since 2013 he is responsible for the Security Offering (GKO ISRM) in Germany and develops new security offerings.

His projects demanded knowledge in very different areas of IT security and he showed that he is able to gain highly specific knowledge in several branches (e.g. UMTS Security or Cloud Security). Dominic Mylo continuously develops his skills and competencies and is able to prove that with his certifications as CISSP and CISA. Furthermore he is certified as ISO/IEC 27001 Auditor and BSI IT-Grundschutz Lead-Auditor.

In 2013 Dominic Mylo developed the security template for cloud management („IT-Grundschutz Baustein“) for the Federal Office for Information Security in Germany.

13. Marian Bubak (AGH)

Title: Federating cloud resources for medical (VPH) applications

Abstract:

The VPH-Share platform provides tools which enable the developer to interact with the cloud resources and create new application components (Atomic Services). VPH-Share is building a safe, online facility in which medical simulation developers can produce workflows - chains of processing tasks - to allow raw medical data to be refined into meaningful diagnostic and therapeutic information. Via an easy to use graphical interface, all the functions needed by workflow developers will be provided, including design, construction, data-access and storage, high-speed computations, sensitivity analyses and results presentations.

The Speaker:

Marian Bubak has a M.Sc. degree in Technical Physics and Ph.D. in Computer Science. He is an adjunct at the Institute of Computer Science and ACC Cyfronet AGH University of Science and Technology, Kraków, Poland, and a Professor of Distributed System Enginnering at the Universiteit van Amsterdam.

His research interests include parallel and distributed computing, grid systems, and e-science; he is the author of about 200 papers in this area, co-editor of 28 proceedings of international conferences and the Associate Editor of FGCS Grid Computing.

14. Jean-Christophe Pazzaglia (SAP, Assert4SOA,France/Germany)

Title: ASSERT4SOA: a toolkit for certification schemes.

Abstract:

The term "certification" has several different meanings in ICT. Software practitioners can earn a certificate for expertise in a certain hardware or software technology. The maturity of crucial IT processes, such as software development, can be and is often certified. Even individual software systems can be certified as having particular non-functional properties, including safety, security or privacy. However, the latter type of certification (e.g. Common Criteria) has had only a limited use to this day. Current trends in the IT industry suggest that software systems in the future will be very different from their counterparts today, due to wider spread of the deployment of the cloud stack.

These trends point to large-scale, heterogeneous ICT infrastructures hosting applications that are dynamically built from loosely-coupled, well-separated services, where key non-functional properties like security, privacy, and reliability will be of increased and critical importance. In such scenarios, certifying software properties but also running platform and management processes will be crucial. Current certification schemes, however, are either insufficient in addressing the needs of such scenarios or not applicable at all and thus, they cannot be used to support and automate run-time security assessment.

In this talk we will highlight how the ASSERT4SOA infrastructure (i) developed enhanced methods for the certification of complex and continuously evolving SOA–based software systems and services and make use of existing certification processes within the SOA context (where possible), (ii) developed mechanisms and tools for the assessment of SOA–based systems' and services' trustworthiness, both at design time and runtime, based on systems and service certification, (iii) integratee the methods, mechanisms and tools of (i)–(ii).

The Speaker

Since July 2010, Jean-Christophe is the director of the SAP Security Product Research Center Sophia Antipolis - France. He is managing the team focusing on Security Engineering from the Security and Trust Practice. Jean-Christophe worked on international environments since 1997 in 4 European countries France, UK, Italy and Cyprus where he held several positions in research labs (Institut Eurécom, CRS4, Cardiff University, I3S) but also private companies (Albourne Partners, Mediatech and Softeam). He started to work on ICT Security 12 years ago and worked on different topics (eg. IDS/ Identity Management/ PKI/Policy/Architecture As-

sessment/Certification) and his know-how enabled to mentor researchers and to take the lead of several research projects (e.g. CYSPA, Serenity, Politess, PrimeLife and TAS3). He was also the principal investigator for SAP on various successful proposals (e.g. PrimeLife, CESSA, ASSERT4SOA). His current research interests encompass IT security from the user and citizen perspective, with a strong emphasis on adaptative and contextual security, traceability and privacy aware architecture.

Jean-Christophe holds a Ph.D. from the University of Nice-Sophia Antipolis (1997) and graduates the Essentials of Management program of University of St Gallen (2009).

15. Prof. George Spanoudakis (Research School of Informatics City University, London; UK)

Title: Incremental Certification of Cloud Service Security

Abstract:

Recent incidents related to the security of cloud services demonstrate that we are still not in a position to fully guarantee cloud security or provide a systematic assessment of it. Thus, security is rightly one of the major concerns of enterprises and the general public regarding the use of the cloud. As a step towards addressing this problem, this presentation provides an overview of the problem and outlines a novel approach for certifying the security of cloud services.

This approach is based on the incremental certification of security properties for different types of cloud services, including IaaS, PaaS and SaaS services, based on operational evidence for the provision of such services that is gathered through continuous monitoring.

The Speaker:

George Spanoudakis (BSc, MSc and PhD) is Professor of Computer Science and Associate Dean for Research in the School of Informatics at City University London. He is also a member of the Council of the University of Piraeus in Greece, and has held visiting positions at the Universities of Essen, Malaga and Crete, and the London School of Economics. His research focuses on service oriented and cloud computing, and software systems security. In these areas, he has published extensively and attracted research funding in excess of €5m. His research grant portfolio includes several R&D projects funded by the EU, national research councils and directly by the industry. Currently, he is the technical coordinator of the F7 EU project CUMULUS (2012-15) that focuses on security certification of cloud services. Professor Spanoudakis has served in the program and organisation committees of more than 130 international conferences and workshops, and co-chaired some of them (SEKE '06, SEKE '07 and NTMS '14). He is also a member of the editorial boards of several journals including the Int. J. of Software Engineering and Knowledge Engineering, Int. J. of Advances in Security and Int. J of Advances in Software. Beyond research, he has been providing consultancy advice to private companies, universities, public funding and standardisation bodies in the UK and overseas.

16. Eric Hibbard (Hitachi Data Systems)

Title: Security and Privacy *(in preparation)*

The speaker

Eric Hibbard is Hitachi Data Systems' CTO Security & Privacy and is responsible for storage security strategy, identifying and defining new storage security architectures and designing new storage networking infrastructures. Hibbard is also a senior security professional who serves as the INCITS/CS1 (Cyber Security) International Representative to ISO/IEC JTC1 SC27, the Vice Chair of IEEE P1619 Security in Storage Working Group and the Chair of the SNIA Security Technical Work Group. His involvement in organizations like INCITS/T11, ISACA, ISSA, the Trusted Computing Group, the IEEE-USA Critical Infrastructure Protection Committee (CIPC) and the American Bar Association afford him a unique perspective on issues germane to information assurance.