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.

# Second CIRRUS workshop

On July 24th 2013 CIRRUS will hold its second workshop in conjunction with The 37th Annual International Computer Software & Applications Conference Kyoto, Japan July 22-26, 2013. This second workshop is aimed at identifying the status in different countries and world regions regarding the cloud certification and standardisation and will set list of priorities from an international convergence point of view. 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 feature presentations from subject matter experts and will generate an open and interactive discussions between the participants.

**Date/time:** **Wednesday 24 July** 2013 from 09.00 till 18.00 hrs.

**Venue:** Kyoto TERRSA, room 3-B, More info at http://www.kyoto-terrsa.or.jp/floormap.html. CIRRUS wshop is co-located with COMPSAC conference: http://compsac.cs.iastate.edu/

**Agenda:**

| | |
|---|---|
| 08.30 – 09.00 | Registration |
| 09.00 – 09.15 | Opening of the workshop by Atos and IPA |
| 09.15 – 10.15 | First session – **Security and standardisation issues in Cloud Portability and Interoperability**. Chair and speakers include Aljosa Pasic (Atos), Margot Dor (ETSI), Yoshiaki Kiriha, (NEC and GICTF, Japan), Mr. Kiichiro Onishi, (HP and DMTF Japan) |
| 10.15 - 10.45 | Networking coffee break & exhibition |
| 10:45 – 13:00 | **Panel on Governmental clouds and security in Asia** – Chair and speakers include Aloysius Cheang (Cloud Security Alliance), Dr.Sak Segkhoonthod (Electronic Government Agency Thailand), Dr. Hin-Yan Lee (National Cloud Computing Office, Infocomm Development Authority Singapore), Dr Chao-Ming Wu, (New Taipei City Government, Taiwan), Mr. Irwan Rawal Husdi (BPPT, Indonesia), Prof. Dr. Shoji Kajita (Kyoto University, Japan), Mr Alex Lee, (Hong Kong SAR government) |
| 13.00 – 14.30 | Networking lunch |
| 14.30 – 15.45 | Second session – **Incident Management, Information sharing and Global Cooperation,** Chair and speakers include Mark Hoekstra (Grant Thornton), Tarry Singh (O&I services), Ikuo Takahashi and Mayu Arimoto, (CSA) |
| 15.45 – 16.15 | Networking coffee break |
| 16.15 – 17.30 | Third session – **Cloud Certification**. Chair and speakers include Alain Pannetrat (Cloud Security Alliance), Tadashi Nagamiya (Japanese Security Audit Association), Yonosuke Harada (Institute of Information Security and ISO/IEC SC27, Japan), Manuel Garcia Sanchez (Data Protection Agency, Spain) |

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 second workshop and future CIRRUS events.

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 Aljosa.pasic@atos.net. The workshop and lunch are free of charges for registered participants.

## *Speakers and abstracts*

### First session – **Security and standardisation issues in Cloud Portability and Interoperability**

**Aljosa Pasic**

**Title:** Security Issues in Cloud Portability and Interoperability

**Abstract:**

Portability and interoperability are two related although different requirements in cloud computing. While portability generally refers to the ability to migrate applications, virtual machine or data between different clouds, interoperability usually refers to the ability to federate multiple clouds. Therefore interoperability involves interaction between clouds to serve a common purpose and is therefore more complex to achieve than portability. Depending on the entity that coordinates cross-cloud or inter-cloud processes, we can distinguish user-centric or cloud service provider, CSP-centric interoperability scenarios. Several European research projects such as Cloud4SOA, Vision Cloud or Cumulus came with interesting proposals that link to the standardisation efforts in portability and interoperability areas. In this presentation, we will give an overview of the most relevant projects and their possible contributions to build "the chain of confidence-building" in cloud security. This chain refers to standards, certification frameworks and contract terms used, among other things, to ensure the portability and interoperability.

**The speaker:**

ALJOSA PASIC current position is Technology Transfer Director in Atos Research & Innovation (ARI), based in Madrid, Spain. He graduated Information Technology at Electro technical Faculty of Technical University Eindhoven, The Netherlands, and has been working for Cap Gemini (Utrecht, The Netherlands) until the end of 1998. In 1999 he moved to Sema Group (now part of Atos) where he occupied different positions. During this period he was participating in more than 50 international research, innovation or consulting projects, mainly related to the areas of information security or e-government. His current interests include Secure Software and Service Engineering (he is the chairman of NESSOS industry advisory group), electronic identity and privacy, GRC (governance, risk and com-

pliance) as well as cybersecurity. He is member of EOS (European Organisation for Security) Board of Directors, and collaborates regularly with organisations such as ENISA, IFIP, IARIA, FI-PPP and others. Currently, he is also the project coordinator of CIRRUS (Cloud Security Certification) project.

**Mr. Kiichiro Onishi**

**Title:**

Customer Major Concerns on Enterprise Use of Cloud and DMTF Activities to Address Them

**Abstract:**

Cloud services are in new stage where enterprises and business units start using them as their production environment. However, enterprise customers still have strong concerns on such use of cloud. The concerns include, (1) integrated operation and management of services across various cloud delivery model such as private cloud, managed cloud and public cloud, (2) flexible and agile migrate between cloud services providers without any vendor lock-in, and (3) securely storing their data and information assets including customer privacy information under conformance to their own security policy. In this session, identifying these customer concerns, DMTF activities and standards to address these concerns will be presented.

**The Speaker:**

Kiichiro Onishi is a Distinguished Technologist - Information Systems Architect in Hewlett-Packard Japan. Since joined in HP in 1990, Kiichiro have engaged in many large system integration projects as well as architecture initiatives for various customers. Kiichiro also took major role in starting up of HP Enterprise Cloud Services - Virtual Private Cloud in HP Japan. Currently, Kiichiro is working with customers to plan to migrate their infrastructure from on-premise environment to external cloud services. Kiichiro's activity outside HP includes having led localization of TOGAF8 and TOGAF9 specifications as an enterprise architect. Kiichiro is an OpenCA Master certified architect. In DMTF, Kiichiro is one of the startup member of DMTF Japan charter.

**Margot Dor**

**Title**

Cloud standards, one is too many, a thousand is not enough

**Abstract**

**The speaker**

ETSI is an ICT standards organization whose mission is to enable the emergence of global open standards for networks and services. The 750+ members (60% European based) design the work programme with their input and participation to technical committees. ETSI is located in Sophia Antipolis, France.

Margot worked in the IT and bank industry prior to joining ETSI to launch a market intelligence unit. She is today in charge of strategy development. Born and raised in Marseille, Margot graduated in Political Science and International Public Law (Aix-Marseille III) and holds a post-graduate degree in Strategic Marketing (HEC Paris).

**Yoshiaki Kiriha**

**Title**

Inter-Cloud Computing and Networking for Secure Social Infrastructure

**Abstract**

Evolving cloud systems become more and more distributed and complex in order to deal with large amount of data processing in coming Big-Data and M2M era. As a next generation of Cloud, inter-cloud is promising for various kind of social cloud applications, and will have an important role to realize an secure social infrastructure.

This talk introduces requirements, use-cases, system models and protocols for Inter-cloud collaboration which are discussed in GICTF (Global Inter-Cloud Technology Forum), as well as a mission, scope, organization, activities of GICTF. Especially, the inter-cloud models and protocols are now under standardization discussion in ITU-T SG13. Future direction will be discussed as a summary of this talk.

**The speaker .**

Yoshiaki Kiriha is a senior manager in the Cloud System Research Laboratories, NEC. He then joined NEC in 1987, where he has worked in the R&D division for over 20 years. He has been involved in many projects in NEC and has transferred core technologies to the product division. His research interests include distributed systems, real-time systems, as well as Future internet service and management. He has continuously contributed as a TPC for almost of all IM/NOMS/DSOM conferences from 2000 and has served as a chair of TC on Information Communication Management, IEICE, 2010-2011.

## Panel on Government and Cloud Security

**Dr. .Sak Segkhoonthod**

Dr. Sak is director of Government Information Technology Services and a special instructor in Data Communications of Telecommunication Engineering, Suranaree University of Technology.

He has been a researcher of NECTEC, since 1997-2000 working on projects such as Information Superhighway Testbed Project, ThaiSARN Project, GINet Project, SchoolNet@1509 Project, Public Key Infrastructure Project etc. He is Thailand's Representative in NAM (Non Alliance Movement) 's ICT Meeting, Thailand's Representative in APT (Asia Pacific Telecommunication) Meeting, Thailand's Representative in APAN (ASIA Pacific Advanced Network)Meeting as well as Network Expert for APEC TEL.

Dr. Sak studied electronics Systems Engineering, University of Essex (Ph.D). He obtained M..S. in Computer Studies, University of Essex, B.S. electronics , King Mongkut's Institute of Technology Ladkrabang.

**Dr. Hing-Yan Lee**

Dr. Hing-Yan LEE is Program Director of National Cloud Computing Office at the Infocomm Development Authority of Singapore, where he oversees the national programme in cloud computing. Under his purview are initiatives such as grid service provisioning, SaaS incubation centre, cloud innovation centre, SaaS Enablement Programme, Technology Evaluation Programme, Data-as-a-Service Programme, development of cloud security standards as well as collaboration in Open Cirrus and IBM Cloud Lab Singapore. Prior to this, Hing-Yan was Deputy Director of National Grid Office at the Agency of Science, Technology and Research as well as Principal Scientist at the Institute for Infocomm Research. He also held senior management and technical positions at Kent Ridge Digital Labs, Japan-Singapore Artificial Intelligence Centre, Information Technology Institute (applied R&D arm of the National Computer Board) as well as two high-tech start-ups.

Hing-Yan serves or has served on the School of Digital Media & Infocomm Technology advisory panel at the Singapore Polytechnic, co-chair of National Infocomm Competency Framework (NICF) technical committee on Cloud Computing, vice chair of Special Interest Group on Enterprise Cloud Computing & Virtualisation (Singapore Computer Society), Cloud Computing Standards Coordinating Task Force (IT Standards Committee), NatSteel Corporate R&D advisory panel, Singapore National Archives Board, and the Australia-Singapore Joint ICT Council.

He graduated from the University of Illinois at Urbana-Champaign in USA with PhD and MS degrees in Computer Science, specializing in artificial intelligence and software reuse. He previously studied at Imperial College London in UK where he obtained a BSc (Eng.) with 1st Class Honours in Computing and MSc in Management Science.

**Dr Chao-Ming Wu**

Dr Wu is the chairperson of Research, Development and Evaluation Commission, New Taipei City Government, Taiwan (R.O.C.). He is also professor at Information Management Department, Chung Yuan Christian University, Taiwan. He obtained Ph.D. from Information Management, Central University, Taiwan (1995-1999). His working experience includes also position of Chief Secretary at Information Management Department, Chung Yuan Christian University, Taiwan and the director of the research institute, Information Management Department, Chung Yuan Christian University, Taiwan

**Mr. Irwan Rawal Husdi (BPPT, Indonesia)**

Irwan Rawal Husdi position is the Head of Science & Technology Network Center in Indonesia. He obtained BSc, in Physics, University of Henri Poincare (France), 1993 and M.Eng, Electronics, Tokyo Institute of Technology (Japan), 2004. Previously , he was involved in Research & Development related to control and sensors, as well as in Research & Development on fiber optic amplifier in communications, aeronautical navigation and in development of set-top-box standard especially for Early Warning System feature for Indonesian digital broadcasting system as part of migration to digital broadcasting. Currently he is working on development of services based on cloud computing to provide solutions for government institutions and local governments in developing e-Government

**Dr. Shoji KAJITA, (Kyoto University)**

Professor at IT Planning Office, Institute for Information Management and Communication Academic Center for Computing and Media Studies, Kyoto University

Shoji Kajita is a researcher and practitioner on Infield Information Informatics defined as study of the ways in which community dynamics and information and communication technologies mutually shape each other as a stakeholder of community. He is currently a Professor of IT Planning Office, Institute for Information and Management Communication, Kyoto University. He was an Associate Professor of Strategic Planning Office in Information Communication Technologies and Services, and also Department of Systems and Social Informatics, Graduate School of Information Science, Nagoya University. His current main interests include e-Learning and e-Science to actualize scalable information environment for higher educational institutions.

For more information, visit: http://shojikajita.jp/ShojiKajita-CV_en.html

**Moderator: Aloysius Cheang (Cloud Security Alliance)**

Aloysius Cheang is Managing Director APAC of Cloud Security Alliance. He also heads up the Standards Secretariat. Aloysius brings to the Alliance extensive experience gained from running business units and multi-million enterprise security and technology programs for Global 500 organizations worldwide in his previous roles as a CSO for a Telco and APAC practice leader with leading management consulting firms. He is an active community leader, having founded and mentored various information security projects, forums, groups and associations in Singapore and many parts in APAC. He is also active in standardization and was most recently a co-editor for ISO/IEC 27032 "Guidelines for Cybersecurity", having contributed towards many other security standards such as ISO/IEC 24762 et al in the past. Aloysius holds a B. Sc (Hons) and Master's degrees in Computer Science from the National University of Singapore and is currently a doctorate candidate. His professional certifications include CISA, CISSP and GCIH. His views are valued by global media such as Times, Wall Street Journal and CIO Magazine as a trusted independent source of specialist opinion over the last decade.

## Second session – Incident Management, Information sharing and Global Co-operation,

### Mark Hoekstra

**Title:** Forensic Challenges in the Cloud

**Abstract:**
Forensic Technology is getting more and more important within the investigative world, both public and private. Since technology evolves very fast in the last couple of decades the Forensic IT experts are used to technical challenges with respect to their daily operations. Cloud environments however, generate more than technical challenges alone; also organisational and legal challenges are influencing the work of a Forensic IT expert in a rather drastic way.

Since there is growing need in investigating data within all sorts of fact finding missions, these problems are highly relevant for all stakeholders in cloud environments: the cloud provider community, cloud users and third parties such as law enforcement and private investigators. Each of them is in need of reliable and legal access to the data in the cloud, whilst privacy and security remain safeguarded.

Based on the ongoing efforts within the framework of the CIRRUS project, Mark will share an overview of the main challenges identified and will discuss potential avenues on how these challenges may be addressed in the future.

**The speaker**

Mark joined Grant Thornton in 2010 as partner at the Forensic & Investigating Services Department. Mark's is specialised in Forensic Technology / E-discovery services. Mark is an Investigations and Forensic IT Specialist with over 20 years of experience involving complex (Forensic IT) Investigations predominantly working in The Netherlands and elsewhere in the world.

Mark is involved in setting international standards regarding Forensic IT Investigations and has lectured at different Universities in Europe on this subject.

After a successful career within some law enforcement agencies both national and international, especially regarding his involvement setting up High Tech crime units, Mark founded his privately held company on this subject. After some years Mark decided to combine the Forensic Technology skills of his company with Forensic Accountant specialists.

Together with his Colleague Peter Schimmel Mark now heads the Forensic & Investigation Services unit within Grant Thornton Netherlands.

**Tarry Singh**

**Title:**

**Cloud governance: Who has the control in the cloud?**

**Abstract:**

IT is typically troubled with mundane tasks while the business wants to have a faster go-to-market strategy and wants to implement key solutions to remain competitive. In this competitive space, Cloud computing offer attractive benefits to business stakeholders especially around agility and cost.

Moving from on-premise to a cloud environments involves more than just outsourcing a component of the technology stack, it also subtly out-tasks many duties. Roles, processes, and authentication technologies need to be reconfigured to fit a distributed stack where parts of the IT solution space reside on-premise while the rest are in the Cloud and it is also managed by several vendors.

Adopting cloud means accepting loss of control. A Cloud vendor will address the needs of most constituents and any high degree of customization which counteracts their business model. This makes integration a complex initiative involving two separate parties trying to align.

Reporting then becomes a key issue in such deployments. We will discuss issues such as What should be reported and when must it be reported? How should risk be mitigated and how will it be allocated across the cloud? SLA integration is key but must be implemented to have a check on controls and metrics.

**The speaker**

Tarry has over 20 years of experience in multiple industries. He is thought-leader and respected technology professional on emerging trends and technologies such as Cloud Computing, Virtualization and Social Computing. Currently, he is Managing Partner/CEO, O&I Services in Amsterdam, The Netherlands It is a European firm based in Netherlands (with offices in Germany) with sole focus on knowledge, growth, quality, flexibility and team-spirit for European clients. Previously, he was Engagement Director Europe, QS Advisory; London, United Kingdom. QS Advisory is a management-consulting firm specifically focusing on outsourcing of IT services. He was also director - EMEA Business Development, at ATOS (formerly Atos Origin/KPMG) ; Utrecht, The Netherlands, where he established Sourcing strategy to execute projects/operations by utilizing Virtual Teams from EMEA & APAC. He established and further developed virtualization division and grew team to 70 certified professionals in EMEA and up to 40 in India, pioneering Cloud Computing program and assessing existing Data Centers globally to develop a SaaS strategy for global customers. In 2009 he got award and a personal recognition as VMware vExpert 2009 for 10 years of contribution to virtualization community. Prior to 2007, he was Senior Manager working in Infrastructure, University Groningen, The Netherlands, as well as Senior

Consultant at Pecoma; Amsterdam, The Netherlands , Project Manager at Royal Wagenborg Shipping; Groningen, The Netherlands. In the period 1991 -2000 he had various Operational Management roles in Oil, Gas & Transportation Sector for Employers such as SeaTrade (Netherlands), NYK (Japan), AEL/NSSPL (Singapore/USA), AP Moller Maersk (Denmark/Brasil) etc. He received B.Sc degree from LBS School of Advanced Research and Development, Mumbai University, India.

**Ikuo Takahashi & Mayu Arimoto**

**Title:**

Data Loss and Leakage by Cloud Providers (Legal Studies on FirstServer Case)

**Abstract:**
More and more companies are using cloud as storage for their data in recent years. It is not limited to private sectors, but governmental organizations are also beginning to commit in cloud computing like "G Cloud" in Britain.

Under such circumstances, in June 2012, FirstServer, a rental server provider operated by Yahoo! Japan lost data belonging to more than 5,000 companies when the firm attempted to upgrade the servers. The firm also lost the backup data and was unable to rebuild the system. According to the investigation committee, the loss was caused by the bug in the upgrading program against security vulnerability and the inappropriate update operating procedure.

Although there are no lawsuits filed against the firm regarding this data loss up until now, we have to look into legal challenges in these data loss cases: in which case cloud providers are held liable for the damages, to what extent, etc. Besides, privacy issues arise in case of data leakage.

We are going to discuss these legal challenges and the measures to address these problems in Japan and other countries.

**The speaker**

Ikuo Takahashi is one of the founders of Cloud Security Alliance Japan Chapter and also joins the Information Network Law Association, based in Tokyo, Japan. He is the Leader Lawyer in Chief of BLT Legal Chambers and CEO of research firm IT Research Art.

Mayu is a member of Cloud Security Alliance Japan Chapter and also joins the Information Network Law Association, based in Tokyo, Japan. She graduated the University of Tokyo, Faculty of Law, and has been an attorney.

## Third session – Cloud Certification

**Alain Pannetrat**

**Title:**

Can monitoring be used to create a "permanent certified cloud"?

**Abstract:**

Cloud Security Alliance recently entered in a partnership with the British Standards Institute with a goal of providing a third party cloud certification framework by the end of the year. If successful, this scheme could be a strong enabler for the development of cloud services, as it answers a long standing demand from cloud customers. Yet like any traditional certification scheme, it also raises questions. In the world of rapid technology changes and agile supply chain management, what is the value of a certificate one month or one year after it has been delivered? We propose to investigate the idea of coupling third party certification with constant monitoring tools to provide a permanent certified cloud. We discuss some ideas and challenges that lie along the way.

**The speaker:**

Alain Pannetrat is a Senior Researcher at Cloud Security Alliance. He supports CSA's research contributions in national and EU funded projects as well as in cross-industry European R&D initiatives. He is a security and privacy expert, specialized in cryptography, cloud computing and smart-cards. He previously worked as a IT Specialist for the CNIL, the French data protection authority, and was an active member of the Technology Subgroup of the Article 29 Working Party, which informs European policy on data protection. He started his career as an IT Security consultant specialized in bank smart-card systems. He received a PhD in Computer Science after conducting research at Institut Eurecom on novel cryptographic protocols for IP multicast security.

**Yonosuke Harada**

**Title**

Something missing in Cloud Provider Certification

**Abstract**

Business user faces with difficulty for outsourcing IT environment. It is not easy how to select cloud provider by price, quality of service, information security measures, brand name, company reputation, and/or SLA. One of the best selection ways is to check the certification/qualification of the provider before contracting. ISMS certification is widely used as the criteria for users to trust providers. Now many cloud providers such as Microsoft, Amazon, Google Aps are already certified with ISMS.

Last June, more than 6,000 Japanese SMEs experienced unintended disruption of their service by troubles of a cloud provider service. The provider reported that they deleted all

the stored data including backup by a serious mistake on operation, although the provider is certified with both ISMS and P-mark (domestic certification for private information protection controls). Some SMEs were not able to continue their e-services due to lack of backup in local environment. They trust providers' ISMS and P-mark certification which require backup control procedures at the contract. however, the providers' certifications have not been banned immediately nor stopped.

Many potential SMEs seeking cloud services have hesitated to contract with such providers because of lack of information security management for data deletion and exposure. Those users have very disappointed against "Certification" as assurance and clear accountability to their customers with outsourcing.

This paper first Introduces the incident stated above and states its impact to existing certification schemes. We also surveyed existing certifications, assuring services (e.g. STAR by CSA) and assurances (e.g. SOC). Then we discusses perception gaps existing between user expectation and reality of those services. We conclude that certification services are inevitable for user to know its achieved level of security. Thus certification service provider should more focus on filling the gaps between user perception and expectation.

**The speaker**

Current Job Title: Professor of the Graduate School of Institute of Information Security

Yonosuke Harada has started his carrier as IT research engineer at Research Labs of NTT (Nippon Telephone and Telegraph) after finishing post-graduate course at Kyoto University Faculty of Engineering. His major concern area was to remotely monitor and control of Exchange System from congestion of calls. He also had participated in several research activities as well as services and products development projects for Telecommunication Networks In 90s, his major activity areas are to develop Information security architecture which includes Information Security Management and Information Security Technologies. In late 1999, he moved to InfoCom Research Labs, which is the think tank and research arm of NTT, where he participated in Information security consulting and auditing.

For academic carrier, he teaches Risk Management at Osaka University Graduate Course and Meiji University from 2005, before he became full time professor at the Graduate School of Institute of Information Security in 2010. He is now teaching Information Security Management, IT and Security Auditing, IT Assurance and IT Governance as well as business management for Information security. He is also teaching Information Security related topics at other universities such as Graduate School of Nippon University, Cyber University and, Ferris Girls University.

Also, he was the president of ISACA Tokyo chapter from 2001 to 2003, and the International Vice president from 2008 to 2010. He is also contributing ISO/IEC SC27 Information Security standardization activities since 2008 until now.

**Manuel Garcia Sanchez**

**Title: Cloud Certification and Personal Data Protection**

## The speaker

Manuel García holds a Degree in Economics and a Master Degree on ICT Management. He joined the Spanish Data Protection Authority in 2002, first as a Data Inspector and IT Auditor and, after a secondment in Brussels working with the European Data Protection Supervisor, as a member of the International Department with responsibilities in police and judicial cooperation and issues related to new technologies. He regularly attends meetings of formal working groups at European and international level dealing with privacy and data protection issues, particularly those linked with the tasks of the Article 29 Working Party.