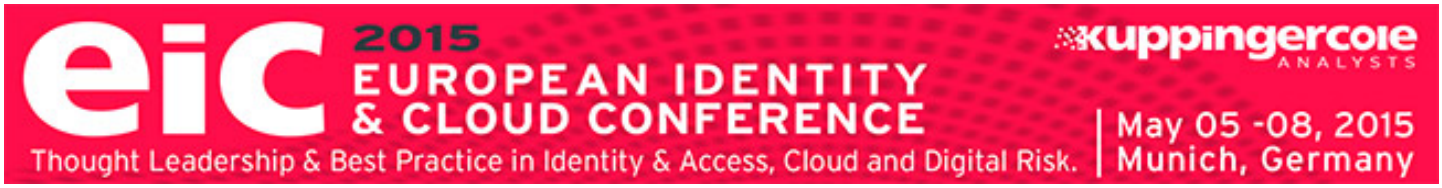

Agenda Overview

Monday, 04.05.2015

14:00-18:00	**Complimentary Seminar** FIDO Alliance Update **Alexei Czeskis**, Software Engineer, Google **Rolf Lindemann**, Senior Director Products & Technology, Nok Nok Labs **Donal O'Shea**, FIDO Alliance

Tuesday, 05.05.2015

08:00-18:00	Check-in & Registration **Room: COUNTER EXPO AREA**			
09:00-13:00	Forum Systems Workshop The Foundations of API Security and API Gateway Technology **Alexei Balaganski**, KuppingerCole **Dr. Dirk Krafzig**, SOAPARK **Jason Macy**, Forum Systems **Mamoon Yunus**, Forum Systems **Room: AMMERSEE I**	OpenID Foundation Workshop Early Insight on Latest Innovations in Online Identity Standards **John Bradley**, OpenID Foundation, Kantara **Jörg Connotte**, Deutsche Telekom AG **Pamela Dingle**, Ping Identity **Roland Hedberg**, ICT Services and System Development (ITS), Umeå University **Eve Maler**, ForgeRock **Nat Sakimura**, Nomura Research Institute **Don Thibeau**, OpenID Foundation **Room: WALCHENSEE**	Kantara Workshop Access Management 2.0 - Consent, Context, and User Engagement **Victor Ake**, ForgeRock **Andre Boysen**, SecureKey Technologies **Joni Brennan**, Kantara Initiative **Ingo Friese**, Deutsche Telekom AG **Dr. Michael Garcia**, National Institute of Standards and Technology (NIST) **Ian Glazer**, Salesforce **Mark Lizar**, SmartSpecies **Dr. Maciej Machulak**, Cloud Identity Limited **Eve Maler**, ForgeRock **Andrea Servida**, European Commission **Michelle Waugh**, CA Technologies **Robin Wilton**, Internet Society **Room: ALPSEE**	Contextual Security Intelligence Getting Smart With Security in the Age of Digital: Moving from Control to Monitoring **Martin Grauel**, Balabit **Péter Gyöngyösi**, BalaBit **Dr. Csaba Krasznay**, BalaBit **Martin Kuppinger**, KuppingerCole **Room: AMMERSEE II**
13:00-14:00	Lunch & Networking **Room: EXPO AREA**			
14:00-14:40	Identity, Access, Security: The Fundaments for Digital Risk Mitigation in the Age of Transformation **Martin Kuppinger**, Principal Analyst, KuppingerCole **Room: AUDITORIUM**			
14:40-15:00	tba **Jan Philipp Albrecht**, Member of Parliament, European Parliament **Room: AUDITORIUM**			
15:00-15:20	Digital Transformation: New Dimensions of Risk and Risk Mitigation **Dr. Scott David, LL.M.**, Fellow Analyst, KuppingerCole **Room: AUDITORIUM**			
15:20-15:40	Digital Risk & the Analog World **Hanns Proenen**, Chief Informaton Security Officer Europe, GE Europe **Room: AUDITORIUM**			
15:40-16:00	eIDAS & Privacy **Andrea Servida**, Head of Task Force "Legislation Team", European Commission **Room: AUDITORIUM**			
16:00-17:00	Coffee & Networking **Room: EXPO AREA**			
17:00-17:20	How to Manage Authorizations in Cloud Services: Getting a Grip on Both Microsoft Azure and Amazon AWS **Patrick Parker**, Founder and CEO, EmpowerID **Room: AUDITORIUM**			
17:20-17:40	The Convergence of IT, Operational Technology and the Internet of Things: How to find a New Balance of Risk and Value **Jackson Shaw**, Identity Management Expert, Dell **Room: AUDITORIUM**			

17:40-18:00	Identity Services 2020 **Kim Cameron**, Creator of the Laws of Identity and Microsoft Identity Architect, Microsoft **Room: AUDITORIUM**
18:00-18:20	User-Managed Identity and Access for the Digitally Transformative Enterprise **Eve Maler**, VP Innovation & Emerging Technology, ForgeRock **Room: AUDITORIUM**
18:20-18:40	Stop Treating your Customers like your Employees **Ian Glazer**, Senior Director, Identity, Salesforce **Room: AUDITORIUM**
18:40-19:00	I Am a Black Swan **Howard Mannella**, Managing Principal, Alternative Resiliency Services Corp **Room: AUDITORIUM**
19:00-19:20	The Good, the Bad and the Ugly of IAM: An Enterprise View **Christian Patrascu**, Director of Product Management, Oracle Corp. **Nick Tuffs**, Principal Delivery Manager, Vodafone
19:30-21:00	Snacks, Drinks & Networking / Evening Reception **Room: EXPO AREA**

Wednesday, 06.05.2015

08:00-18:00	Check-in & Registration **Room: COUNTER EXPO AREA**			
08:30-08:50	Cryptography for the People **Dr. Jan Camenisch**, Scientist, IBM Research **Room: AUDITORIUM**			
08:50-09:10	A smarter, More Secure Internet of Things? **David Mount**, Solutions Consulting Director, NetIQ **Room: AUDITORIUM**			
09:10-09:30	Securing Privileged Identities in OT (Operational Technology) and Industrial Control Systems **Yariv Lenchner**, Senior Product Manager, Operational Technologies, Cyber-Ark Software **Room: AUDITORIUM**			
09:30-09:50	Cybersecurity for Critical Infrastructures and Industry 4.0: Shaping the future of IAM **Ralf Knöringer**, Manager Business Unit IAM, Atos IT Solutions and Services GmbH **Room: AUDITORIUM**			
10:00-11:00	Coffee & Networking **Room: EXPO AREA**			
	The New Risk Landscape: IT, Operational Technology and IoT Moderator: **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole **Room: AUDITORIUM**	**The Future of Identity & Access Management** Moderator: **Martin Kuppinger**, KuppingerCole **Matthias Reinwarth**, KuppingerCole **Room: AMMERSEE I**	**Architecting the Digital Enterprise: Securing Cloud, Data & Mobility** Moderator: **Amar Singh**, KuppingerCole **Mike Small**, KuppingerCole **Room: ALPSEE**	**User Managed Identity & Access** Moderator: **Dr. David Goodman**, KuppingerCole **Mario Hoffmann**, Fraunhofer AISEC **Room: AMMERSEE II**

11:00-12:00	Mapping the Changes in Data and Identity Risk Landscapes From Security to Information Security to Digital Risk **Hanns Proenen**, GE Europe Mapping the Changes in Data and Identity Risk Landscapes - From Physical Security to Information Security to Digital Security to Interaction Security **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole	Security for the Digital Business What are the Requirements for your Future IAM to Enable Digital Security? **Martin Kuppinger**, KuppingerCole IAM Under Fire: Best Practices for Protecting the Keys to your Kingdom **Martin Kuppinger**, KuppingerCole **Darran Rolls**, SailPoint The Role of IAM in Hack Prevention **Patrick Parker**, EmpowerID **Matthias Reinwarth**, KuppingerCole	Cloud Identity & Security Top 5 Cloud Security Threats and how to Mitigate the Risk of High Impact **Amar Singh**, KuppingerCole **Mike Small**, KuppingerCole Simplify your IAM – what's first: User Interface, Processes, or Infrastructure? **Marc Bütikofer**, Ergon Informatik AG **Ralf Knöringer**, Atos IT Solutions and Services GmbH **James Litton**, Identity Automation **Mike Nelsey**, Aurionpro Solutions plc **Max Waldherr**, Dell Software	User Empowerment - The Building Blocks Designing the Privacy-Aware Internet: Standards, Trust Frameworks, Encryption, Protocols **Mario Hoffmann**, Fraunhofer AISEC Extending the Power of Consent with User-Managed Access and OpenUMA **Eve Maler**, ForgeRock Crossing The Chasm: Bridging The Divide Between Consumer Identity And Identity In The Enterprise **Robert Lapes**, Capgemini
12:00-13:00	Preconceptions of Risk Data and Identity Systems Risk in the Larger Distributed Risk Context **Thom Langford**, Sapient Negotiating the Risk of Privacy - Understanding Privacy and its Risks **Prof. Dr. Rüdiger Grimm**, University Koblenz-Landau, Faculty of Informatics	Identity Relationship Management (IRM) & the Business Side No Person is an Island: How Relationships Make the IT World More Manageable **Ian Glazer**, Salesforce The business side of IAM – How to Work with the Business to Make IAM Successful in your Organization **Bill Evans**, Dell Software **Matthias Reinwarth**, KuppingerCole **Markus Weber**, ForgeRock **Rudolf Wildgruber**, Atos IT Solutions and Services GmbH	Next Generation (Mobile) Cloud Enterprise Mobility Management: Best Practices & Lessons Learned **Pavlos Makridakis**, Aurionpro Solutions plc **Christian Patrascu**, Oracle Corp. **Dominic Schmidt-Rieche**, AirWatch What's Next in Cloud IAM – Moving Beyond Single Sign-On **Pamela Dingle**, Ping Identity **Dr. Martin Kuhlmann**, Omada **Daniel Raskin**, ForgeRock **Richard Walters**, Intermedia	Internet Scale Encryption, Authentication, Authorization Idemix: Secure, Attribute-Based Authentication **Dr. Jan Camenisch**, IBM Research uProve: The Pricipal of Minimal Disclosure at Work **Ronny Bjones**, Microsoft Qiy Scheme: Trusted Exchange of Personal Information **Marcel van Galen**, Qiy Foundation
13:00-14:30	Lunch & Networking **Room: EXPO AREA**			
	Managing Digital Risk: Mapping the New Distributed Risk Landscapes Moderator: **John Hermans**, KPMG **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole **Room: AUDITORIUM**	**The Future of Identity & Access Management** Moderator: **Matthias Reinwarth**, KuppingerCole **Graham Williamson**, KuppingerCole **Room: AMMERSEE I**	**Architecting the Digital Enterprise: Securing Cloud, Data & Mobility** Moderator: **Amar Singh**, KuppingerCole **Mike Small**, KuppingerCole **Room: ALPSEE**	**User Managed Identity & Access** Moderator: **Joni Brennan**, Kantara Initiative **Dr. David Goodman**, KuppingerCole **Room: AMMERSEE II**

14:30-15:30	Digital Risk Officer & Chief Digital Officer It Takes a Community to Reduce Risk – Company Leadership and Recruitment of Supply Chains Stakeholders in Risk Mitigation Strategies **Amar Singh**, KuppingerCole Recruiting Customers, Suppliers and Even Competitors to Help Reduce Risk **Thom Langford**, Sapient **Dr. Adriana Nugter**, Independant Senior Consultant **Arieh Shalem**, Orange **Amar Singh**, KuppingerCole One Step Closer to the Unhackable Enterprise: Applying an Effective Information Security Strategy **Stefan Van Gansbeke**, CM/MC Health Insurance Fund Belgium	Best Practice Identity @ The Guardian - SSO at Web Scale **Mark Butler**, The Guardian Rethinking Digital Identity: The Australian Government Story **Ben Bildstein**, Department of Industry and Science (Australian Government)	Cloud Encryption; Securing IaaS Customer-Managed Encryption Keys: Controlling Your Data's Privacy in the Cloud **Richard Anstey**, Intralinks **Dan Plastina**, Microsoft Best Practice: From Zero to Secure in 1 Minute **Nir Valtman**, NCR Corporation	Standards & Protocols Protocol meets Architecture: Patterns for Construction of an OAuth Identity Platform **Pamela Dingle**, Ping Identity OpenID Connect Certification **Roland Hedberg**, ICT Services and System Development (ITS), Umeå University **Dr. Michael B. Jones**, Microsoft The Security Stack for Modern Applications: OpenID Connect and OAuth 2.0 **Dominick Baier**, Thinktecture
15:30-16:30	Cloud Risk Assessment Assessing and Mitigating Cloud Risks **John Hermans**, KPMG **Mario Hoffmann**, Fraunhofer AISEC **Olga Kulikova**, KPMG **Mike Small**, KuppingerCole Dynamic Control Selection Framework for Onboarding Cloud Solutions **Olga Kulikova**, KPMG Dynamic Certification of Cloud Ecosystems **Mario Hoffmann**, Fraunhofer AISEC Cloud Risk Assessment – An "Action-Oriented" Approach to Merge Engineering, Economic and Legal Analyses. **Mike Small**, KuppingerCole	FIDO Alliance: Simplifying User Authentication The Death of the Password - Is It Finally Coming True? **Alexei Czeskis**, Google **Tord Fransson**, Yubico **Dr. Michael B. Jones**, Microsoft **Rolf Lindemann**, Nok Nok Labs **Anthony Nadalin**, Microsoft **Donal O'Shea**, FIDO Alliance	Hybrid Cloud & Beyond Best Practice: A Hybrid Enterprise in a Cloud First World **Brian Puhl**, Microsoft Identity-as-a-Service Securing PostNL's 100% Cloud Strategy **Theo Punter**, PostNL	OASIS SAML & XACML for Consumer Identity Securing Sensitive Data While Enhancing Privacy **Dr. Michael Garcia**, National Institute of Standards and Technology (NIST) **Gerry Gebel**, Axiomatics Americas **Karyn Higa-Smith**, U.S. Department of Homeland Security **Soren Peter Nielsen**, NineConsult **Daniel Raskin**, ForgeRock **John Tolbert**, Queralt
16:30-17:30	Coffee & Networking **Room: EXPO AREA**			
17:30-18:30	Think Globally, Act Locally Understanding and Dealing with Macro-Level Risks that Affect your Institution's Risk Profile **Ben Bildstein**, Department of Industry and Science (Australian Government) **Karyn Higa-Smith**, U.S. Department of Homeland Security **Dr. Roy Lindelauf**, Netherlands Defence Academy **Howard Mannella**, Alternative Resiliency Services Corp **Robin Wilton**, Internet Society	Privilege Management Privilege Management Use Cases **Christian Götz**, CyberArk **Serge Ingber**, ObservelT **Amar Singh**, KuppingerCole **Edwin van der Wal**, Everett **Nathan Wenzler**, Thycotic The Snowden Effect: Why seeing is believing **Chris Pace**, Wallix **Wolfgang Roesch**, Tesis Sysware **Michael Yaffe**, BeyondTrust	Business-Critical Infrastructure & Applications The Future of Directory Services: Data Models - Performance - Security **Andrew Ferguson**, KuppingerCole Asia Pacific **Peter Gietz**, DAASI International GmbH **Thorsten Niebuhr**, WedaCon Informationstechnologien GmbH Business Critical Application Security **Christian Patrascu**, Oracle Corp. **Gerhard Unger**, Onapsis Inc.	Telcos & Innovation Identity Strategy for Innovation **Chema Alonso**, Eleven Paths, Telefonica Facing The Future: Identity Opportunities for Telco Operators **Chema Alonso**, Eleven Paths, Telefonica **John Bradley**, OpenID Foundation, Kantara **Jörg Connotte**, Deutsche Telekom AG **Marco Dütsch**, Swisscom **Maarten Louman**, Qiy **Dr. Adriana Nugter**, Independant Senior Consultant **Arieh Shalem**, Orange **Nick Tuffs**, Vodafone
18:30-18:50	RISK is Not a @#$%&! Dirty Word! **Thom Langford**, Director Global Security Office, Sapient **Room: AUDITORIUM**			

18:50-19:10	Connected Identity : Benefits, Risks & Challenges **Prabath Siriwardena**, Director, Security Architecture, WSO2 **Room: AUDITORIUM**
19:10-19:30	No Security without Identity **André Durand**, Founder & CEO, Ping Identity **Room: AUDITORIUM**
19:30-22:00	European Identity Awards Ceremony & Buffet Dinner **Room: AUDITORIUM**

Thursday, 07.05.2015

08:00-18:00	Check-in & Registration **Room: COUNTER EXPO AREA**			
08:30-08:50	Finding the Balance Between Secrecy and Operational Efficiency **Dr. Roy Lindelauf**, Military Operations Research, Netherlands Defence Academy **Room: AUDITORIUM**			
08:50-09:10	Identity & Access Process Automation: Improving Business Alignment & Reducing Digital Risk **Dirk Venzke**, Director, Commerzbank AG **Room: AUDITORIUM**			
09:10-09:30	tba **Ravi Srinivasan**, Director, IBM Security Systems **Room: AUDITORIUM**			
09:30-09:50	CISO in the Cloud with Diamonds **Arieh Shalem**, CISO, Orange **Room: AUDITORIUM**			
10:00-11:00	Coffee & Networking **Room: EXPO AREA**			
	Designing, Developing and Deploying Sustainable Distributed Risk Solutions for your Enterprise Moderator: **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole **Room: AUDITORIUM**	**Redefining Access Governance** Moderator: **Matthias Reinwarth**, KuppingerCole **Dr. Horst Walther**, KuppingerCole **Room: AMMERSEE I**	**Secure Information Sharing through Rights Management** Moderator: **Dr. David Goodman**, KuppingerCole **Room: ALPSEE**	**User Managed Identity & Access** Moderator: **Joni Brennan**, Kantara Initiative **Prof. Dr. Sachar Paulus**, KuppingerCole **Room: AMMERSEE II**

11:00-12:00	EU Privacy Regulation The Proposed New European Union Data Protection Regulation - Status and Implications **Rhiannon Davies**, DAC Beachcroft LLP **Kuan Hon**, Queen Mary University of London **Dr. Karsten Kinast LL.M.**, KuppingerCole The Role of Privacy by Design in the New EU Data Protection Regulation **Dr. Karsten Kinast LL.M.**, KuppingerCole **André Lutermann**, Dell Software	Access Governance Best Practice One-Click Insight, Lean Recertification, Improved Compliance: Redefining Access Governance for the Digital Business **Matthias Reinwarth**, KuppingerCole Externalized Access Management (ABAC, RBAC) at Talanx Systeme AG for Bancassurance **Frank Wittlich**, Talanx Systeme AG IAM Processes and their Communication Loops **Stephanie Jaecks**, Bayer BBS	The Future of Collaboration Digital Rights Management – UBS Case Study **Marek Pietrzyk**, UBS Coutts Bank Case Study **Andrew Church**, Coutts Secure Information Sharing - The User Experience **Andrew Church**, Coutts **Marek Pietrzyk**, UBS **Amol Sawarkar**, International Federation of Red Cross and Red Crescent Societies (IFRC)	Life Management Best Practice Life Management in Finance & Insurance Industry **Frank Cooler**, Intrasurance **Marcel van Galen**, Qiy Foundation **Ad van Loon**, X-media Strategies **Dr. Adriana Nugter**, Independant Senior Consultant
12:00-13:00	Cloud Contracting Risks Reaching Compliance Across Jurisdictions: Fundamental Considerations Before Signing a Cloud Services Contract **John Hermans**, KPMG **Dr. Karsten Kinast LL.M.**, KuppingerCole SaaS Contracting: From Risk to Complaince **Edwin Sturrus**, KPMG Advisory N.V.	IAM Standard Processes Roles or no Roles, that's the Question. Two Different Approaches for Compliant IAM Processes. **Matthias Reinwarth**, KuppingerCole **Dr. Horst Walther**, KuppingerCole RBAC & ABAC Hybrid Approaches **Frank Böhm**, FSP **Thorsten Niebuhr**, WedaCon Informationstechnologien GmbH **Patrick Parker**, EmpowerID **Frank Wittlich**, Talanx Systeme AG	Market Maturity Protecting and Tracking Sensitive Data **Dr. David Goodman**, KuppingerCole **Dan Plastina**, Microsoft Information Centric Security; the Way to Go? **Rui Melo Biscaia**, Watchful Software **John Grillos**, Seclore **Henk Van der Heijden**, TecHarbor **Eyal Manor**, Secure Islands **Scott Masson**, TITUS **Dan Plastina**, Microsoft **Jose Manuel Rodriguez**, Prot-On	Bring Your Own Privacy Life Management Use Cases & Business Models **Katryna Dow**, Meeco Empowering the Consumer for Digital Business and the Identity Economy **Prof. Dr. Sachar Paulus**, KuppingerCole
13:00-14:30	Lunch & Networking **Room: EXPO AREA**			
	Managing Digital Risk: Deploying People, Standards, Metrics, and Enforcement. Moderator: **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole **Room: AUDITORIUM**	**Redefining Access Governance** Moderator: **Matthias Reinwarth**, KuppingerCole **Dr. Horst Walther**, KuppingerCole **Room: AMMERSEE I**	**Identity Defined Security** Moderator: **Dr. David Goodman**, KuppingerCole **Dave Kearns**, KuppingerCole **Room: ALPSEE**	**Securing Operational Technology (OT) and the Internet of Things (IoT)** Moderator: **John Sabo**, OASIS Idtrust **Mike Small**, KuppingerCole **Room: AMMERSEE II**

14:30-15:30	Software Defined Everything The Role of Policy Management in the Software-Defined Era **Tim Grance**, NIST **Andy Land**, IBM **Anthony Nadalin**, Microsoft **Ken Owens**, Cisco Systems **Hemma Prafullchandra**, HyTrust	Dynamic Authorization Adaptive Policy-Based Access Management: Beyond ABAC and RBAC **Martin Kuppinger**, KuppingerCole The Future of Authorization **Gerry Gebel**, Axiomatics Americas **Martin Kuppinger**, KuppingerCole **Darran Rolls**, SailPoint **Markus Weber**, ForgeRock **Frank Wittlich**, Talanx Systeme AG	New Security Solutions for the Enterprise What If the Future of Security Means Not Knowing It's There? **Kim Cameron**, Microsoft **Nishant Kaushik**, CA **Christian Patrascu**, Oracle Corp. **Jackson Shaw**, Dell User Discovery: Changing Best Practices and Protocol Convergence **Pamela Dingle**, Ping Identity	IoT/OT Privacy & Security Security and the Internet of Everything and Everyone **Mike Small**, KuppingerCole IoT Privacy Risks, Legislation and Solutions **Kuan Hon**, Queen Mary University of London **Yariv Lenchner**, Cyber-Ark Software **Peter Niblett**, IBM **John Sabo**, OASIS Idtrust **Erik Sucksdorff**, GlobalSign
15:30-16:30	Risk Metrics What Gets Measured Gets Done – Identifying New Metrics for Distributed Digital System Performance to Evaluate and Mitigate Risk. **Dr. Roy Lindelauf**, Netherlands Defence Academy **Nathan Wenzler**, Thycotic How to Measure the Real Access Risk? **Niels von der Hude**, Beta Systems Software **Wolfgang Roesch**, Tesis Sysware	Best Practice IAM/IAG @ Continental AG: Clearing Process as a Basis for Identity Management **Theodor Heindl**, Continental Corporate Infrastructure Identity Relationship and Access Management and Dynamic Authorisation Management as a Driver for New Business Opportunities **Laura Lätti**, DNA Finland	IAM as a Managed Service IAM as a Service Best Practice: B.Braun Melsungen AG **Martin Oberlies**, B.Braun Melsungen AG Experiences with IAM as a Service and/or IAM Managed Service **Martin Oberlies**, B.Braun Melsungen AG **Theo Punter**, PostNL **Darran Rolls**, SailPoint **Maarten Stultjens**, iWelcome **Yso Vonk**, NXP Semiconductors **Peter Weierich**, iC Consult GmbH	Identity of Things Putting Identity at the Center of IoT- Kantara IDoT Strategic Review **Victor Ake**, ForgeRock **Andre Boysen**, SecureKey Technologies **Ingo Friese**, Deutsche Telekom AG **Hannes Tschofenig**, ARM Process Control, Production IT and Operational Technology - No Go Areas for IDM? **Eleni Richter**, EnBW
16:30-17:00	Coffee & Networking **Room: EXPO AREA**			
17:00-18:00	Adopting the New Thinking on Digital Risk Bringing it All Together – Distributed Strategy Solutions for Distributed Risk **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole	Access Intelligence Access Intelligence, User Activity Monitoring, Recertification: What do we Really Need? **Ramses Gallego**, Dell **Dr. Michael B. Jones**, Microsoft **Rainer Knorpp**, Devoteam **Thierry Winter**, Evidian	Behavioral Analytics The Anthem Breach and how it could have been Avoided **Dave Kearns**, KuppingerCole Risk Based Realtime Security Through Behavioral Intelligence: Concepts and Market Maturity **Martin Kuppinger**, KuppingerCole	Integration Mastering IoT Privacy and Security Risks Without Losing the Benefits of IoT **Gershon Janssen**, OASIS Open Standards Group **Peter Niblett**, IBM **Jeff Stollman**, Secure Identity Consulting **Dirk Wahlefeld**, ITConcepts **Souheil Ben Yacoub**, Verisign
18:00-18:30	Closing Keynote **Prof. Dr. Sachar Paulus**, Scientific Advisor, KuppingerCole **Room: AUDITORIUM**			

Friday, 08.05.2015

08:30-10:00	Check-in & Registration **Room: COUNTER HOTEL**		
	Workshop Stream I **Room: AMMERSEE I**	**Workshop Stream II** **Room: AMMERSEE II**	**Workshop Stream III** **Room: ALPSEE**
09:00-12:30	Roles, Recertification, Access Governance: The Lean Approach **Matthias Reinwarth**, KuppingerCole	Cloud Risk Assessment **Mike Small**, KuppingerCole	Industry Focus Workshop: Insurance & Financial Services Prepare your Organization for the Digital Transformation: Enable the Agile, Connected Business **Martin Kuppinger**, KuppingerCole **Wolfgang Rupprath**, FSP

12:30-13:30	Lunch Break **Room: RESTAURANT**		
13:30-16:00	Roles, Recertification, Access Governance: The Lean Approach **Matthias Reinwarth**, KuppingerCole	Beyond your On-Premise IT: Privilege Management for Cloud, Virtualization, SDE, OT, and IoT **Dave Kearns**, KuppingerCole **Edwin van der Wal**, Everett **Nathan Wenzler**, Thycotic	Identity Mixer, uProve, Qiy Trust Framework, UMA: Providing Control to the Individual **Ronny Bjones**, Microsoft **Joni Brennan**, Kantara Initiative **Dr. Maria Dubovitskaya**, IBM Research **Marcel van Galen**, Qiy Foundation **Bram Neuteboom**, Qiy Foundation **Daniel Raskin**, ForgeRock

Agenda Details

Monday, 04.05.2015

14:00-18:00	**Complimentary Seminar** FIDO Alliance Update **Alexei Czeskis**, Software Engineer, Google **Rolf Lindemann**, Senior Director Products & Technology, Nok Nok Labs **Donal O'Shea**, FIDO Alliance

Tuesday, 05.05.2015

08:00-18:00	Check-in & Registration **Room: COUNTER EXPO AREA**
09:00-13:00	**Forum Systems Workshop** **The Foundations of API Security and API Gateway Technology** **Alexei Balaganski**, KuppingerCole **Dr. Dirk Krafzig**, SOAPARK **Jason Macy**, Forum Systems **Mamoon Yunus**, Forum Systems This workshop will explore API gateway technology. What it is, how it's applied today, the benefits of API gateway technology, and implementation examples. As enterprise architectures become increasingly complex, organizations are challenged with creating a modern and secure infrastructure. In this workshop, you will learn how API gateway technology is a fundamental component to achieving business agility and information security. Additional topics covered: • How to modernize legacy and existing services • Centralizing identity enforcement, including SAML and OAuth • Modern access control strategies and best practices Presentations will include sessions from industry leaders as well as an implementation showcase where attendees have the opportunity to participate in hands-on exercises. **Agenda** **Dienstag, 05.05.2015** 09:00-10:00 — How to Implement Multifactor Single Sign-On (SSO) **Dr. Dirk Krafzig**, CEO, SOAPARK 10:00-11:00 — Foundations of API Security **Jason Macy**, CTO, Forum Systems 11:00-11:30 — Coffee Break 11:30-12:30 — Implementation Showcase **Jason Macy**, CTO, Forum Systems **Mamoon Yunus**, CEO, Forum Systems 12:30-13:00 — Technical Round Table Discussion **Dr. Dirk Krafzig**, CEO, SOAPARK **Jason Macy**, CTO, Forum Systems **Matthias Reinwarth**, Senior Analyst, KuppingerCole **Mamoon Yunus**, CEO, Forum Systems
09:00-13:00	**OpenID Foundation Workshop** **Early Insight on Latest Innovations in Online Identity Standards** **John Bradley**, OpenID Foundation, Kantara **Jörg Connotte**, Deutsche Telekom AG **Pamela Dingle**, Ping Identity **Roland Hedberg**, ICT Services and System Development (ITS), Umeå University **Eve Maler**, ForgeRock **Nat Sakimura**, Nomura Research Institute **Don Thibeau**, OpenID Foundation This OpenID Foundation Workshop provides early insight and influence on important new online identity standards like the EIC Award-winning OpenID Connect. We will provide updates on the OpenID Connect Self Certification Test Suite and Mobile Profile Working Groups of OpenID Connect as well as other protocols in the pipeline like Account Chooser and Native Applications. Leading technology experts from Microsoft, Google, Ping Identity and others will update developments with these key protocols, review work group progress and discuss how they help meet enterprise business challenges. ◦ OpenID Connect Self Certification and Registration by Don Thibeau of the OpenID Foundation ◦ OpenID Connect Conformance Testing by Roland Hedberg of the Umea University of Sweden ◦ OpenID Connect by Co Chairs Mike Jones and Nat Sakimura of the NRI ◦ Mobile Profile for OpenID Connect by Chair Torsten Lodderstedt of Deutsche Telekom ◦ Account Chooser by TBD Google Identity Team and/or Pam Dingle of Ping Identity ◦ "HEART" Health Care Profile of OpenID Connect by Co Chair Eve Maler of Forgerock ◦ Native Applications Work Group by Co Chair John Bradley of Ping Identity

09:00-13:00	**Kantara Workshop** **Access Management 2.0 - Consent, Context, and User Engagement** **Victor Ake**, ForgeRock **Andre Boysen**, SecureKey Technologies **Joni Brennan**, Kantara Initiative **Ingo Friese**, Deutsche Telekom AG **Dr. Michael Garcia**, National Institute of Standards and Technology (NIST) **Ian Glazer**, Salesforce **Mark Lizar**, SmartSpecies **Dr. Maciej Machulak**, Cloud Identity Limited **Eve Maler**, ForgeRock **Andrea Servida**, European Commission **Michelle Waugh**, CA Technologies **Robin Wilton**, Internet Society The Kantara Initiative annual EIC workshop will focus on the Kantara Initiative strategy for Connected Life & Access Management 2.0.
09:00-13:00	**Contextual Security Intelligence** **Getting Smart With Security in the Age of Digital: Moving from Control to Monitoring** **Martin Grauel**, Balabit **Péter Gyöngyösi**, BalaBit **Dr. Csaba Krasznay**, BalaBit **Martin Kuppinger**, KuppingerCole Behaviour-based approaches to detecting intrusions have recently gained importance and momentum as a complementary model to the purely knowledge based approach. Behavioural intrusion detection is based on the assumption, that intrusions regularly create deviations from the normal behaviour, which is defined by reference models. In permanently comparing network activity with the reference model, such deviations can be detected and used to create an alarm. Using the behavioural context to detect intrusions is proposing an exciting side-effect: In permanently comparing network activity with reference models, it is possible to discover and learn previously unknown attack patterns and provide "intrusion intelligence". In this workshop, KuppingerCole´s Principal Analyst Martin Kuppinger will at first introduce you to the concept of Contextual Security Intelligence and describe the challenges you will have to master, like • keeping false alarms low • extending behavioural approaches beyond vulnerability-attacks to the area of privilege misuse • keeping your reference model up-to-date with changing behaviours • avoiding privacy concerns and then will hand over to Dr. Csaba Krasznay and Péter Gyöngyösi from BalaBit, who will give you a deep and intense overview on state-of-the-art Contextual Security Intelligence, devided into the core areas of • Privileged Activity Monitoring and • User Behavioural Analysis
13:00-14:00	Lunch & Networking **Room: EXPO AREA**
14:00-14:40	Identity, Access, Security: The Fundaments for Digital Risk Mitigation in the Age of Transformation **Martin Kuppinger**, Principal Analyst, KuppingerCole **Room: AUDITORIUM**
14:40-15:00	tba **Jan Philipp Albrecht**, Member of Parliament, European Parliament **Room: AUDITORIUM**
15:00-15:20	Digital Transformation: New Dimensions of Risk and Risk Mitigation **Dr. Scott David, LL.M.**, Fellow Analyst, KuppingerCole **Room: AUDITORIUM**
15:20-15:40	Digital Risk & the Analog World **Hanns Proenen**, Chief Informaton Security Officer Europe, GE Europe **Room: AUDITORIUM**
15:40-16:00	eIDAS & Privacy **Andrea Servida**, Head of Task Force "Legislation Team", European Commission **Room: AUDITORIUM**
16:00-17:00	Coffee & Networking **Room: EXPO AREA**
17:00-17:20	How to Manage Authorizations in Cloud Services: Getting a Grip on Both Microsoft Azure and Amazon AWS **Patrick Parker**, Founder and CEO, EmpowerID **Room: AUDITORIUM**
17:20-17:40	The Convergence of IT, Operational Technology and the Internet of Things: How to find a New Balance of Risk and Value **Jackson Shaw**, Identity Management Expert, Dell **Room: AUDITORIUM**
17:40-18:00	Identity Services 2020 **Kim Cameron**, Creator of the Laws of Identity and Microsoft Identity Architect, Microsoft **Room: AUDITORIUM**

18:00-18:20	User-Managed Identity and Access for the Digitally Transformative Enterprise **Eve Maler**, VP Innovation & Emerging Technology, ForgeRock **Room: AUDITORIUM**
18:20-18:40	Stop Treating your Customers like your Employees **Ian Glazer**, Senior Director, Identity, Salesforce **Room: AUDITORIUM**
18:40-19:00	I Am a Black Swan **Howard Mannella**, Managing Principal, Alternative Resiliency Services Corp **Room: AUDITORIUM**
19:00-19:20	The Good, the Bad and the Ugly of IAM: An Enterprise View **Christian Patrascu**, Director of Product Management, Oracle Corp. **Nick Tuffs**, Principal Delivery Manager, Vodafone
19:30-21:00	Snacks, Drinks & Networking / Evening Reception **Room: EXPO AREA**

Wednesday, 06.05.2015

08:00-18:00	Check-in & Registration **Room: COUNTER EXPO AREA**
08:30-08:50	Cryptography for the People **Dr. Jan Camenisch**, Scientist, IBM Research **Room: AUDITORIUM**
08:50-09:10	A smarter, More Secure Internet of Things? **David Mount**, Solutions Consulting Director, NetIQ **Room: AUDITORIUM**
09:10-09:30	Securing Privileged Identities in OT (Operational Technology) and Industrial Control Systems **Yariv Lenchner**, Senior Product Manager, Operational Technologies, Cyber-Ark Software **Room: AUDITORIUM**
09:30-09:50	Cybersecurity for Critical Infrastructures and Industry 4.0: Shaping the future of IAM **Ralf Knöringer**, Manager Business Unit IAM, Atos IT Solutions and Services GmbH **Room: AUDITORIUM**
10:00-11:00	Coffee & Networking **Room: EXPO AREA**
11:00-12:00	**Mapping the Changes in Data and Identity Risk Landscapes** **From Security to Information Security to Digital Risk** **Hanns Proenen**, GE Europe Hanns Proenen will take you on a small journey through traditional IT security, as it was until recently, and how he is observing and experiencing the shift to information security and IT risk. He will talk about the tasks for the IT Risk Officer and how to build a firewall between the digital and the analogue world. **Mapping the Changes in Data and Identity Risk Landscapes - From Physical Security to Information Security to Digital Security to Interaction Security** **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole Well-managed organizations address unique and emerging risks, such as networked data and identity-related risks in the context of their overall risk profile, and seek to implement solutions that can cost-effectively address organizational risk at multiple levels. As new online and networked system risks associated with data and identity handling systems have surfaced, pre-existing risks still remain relevant; and together they vie for the attention of managers around the world, causing them many sleepless nights. How are emerging risks similar to and different from traditional risks faced by enterprises? How can traditional risk mitigation strategies inform, or mislead, managers seeking to address emerging risks?

11:00-12:00	**Security for the Digital Business** **What are the Requirements for your Future IAM to Enable Digital Security?** **Martin Kuppinger**, KuppingerCole When it comes to security for the digital enterprise, we have good reason to get nervous, understanding current breaches like Sony as the first signs of a dark future, where cyber criminals and even terrorists lurk and create serious damage. In this session, Martin Kuppinger will first define, what "digital security" means, what the real risks are that need to be faced and mediated, and which roles IAM will play in this context. **IAM Under Fire: Best Practices for Protecting the Keys to your Kingdom** **Martin Kuppinger**, KuppingerCole **Darran Rolls**, SailPoint Understanding the criticality of IAM infrastructure (delivered as software or as a service) and securing the service and its lifecycle. **The Role of IAM in Hack Prevention** **Patrick Parker**, EmpowerID **Matthias Reinwarth**, KuppingerCole As witnessed by a seemingly non-stop onslaught of public breaches of prominent organizations (Sony, Anthem, Target, etc.), it appears that the gloves have come off in the battle being waged in cyberspace. Nations have become heavily involved in industrial hacking for the purpose of enriching their government-owned enterprises. Hacktivists are out in force to publicly expose and shame corporations for perceived public wrongs. Unfortunately, Enterprise IT is caught in the middle and must defend from, detect, and respond to these threats. This session will discuss the role of IAM in preventing breaches, limiting their scope, and permitting faster detection and response.
11:00-12:00	**Cloud Identity & Security** **Top 5 Cloud Security Threats and how to Mitigate the Risk of High Impact** **Amar Singh**, KuppingerCole **Mike Small**, KuppingerCole Although cloud computing has left the early adopter stage, there are still quite a few organizations hesitant to migrate services and data into the cloud due to security concerns, not only in Europe. Many of the security and privacy concerns heard when listening to IT professionals, are not just fears - they are real amd meed to be treated. In this presentation, KuppingerCole Analysts Mike Small and Eric Cole will guide you through the top 5 Cloud Security & Privacy concerns and propose measures to mitigate the risks originating from those threats. **Simplify your IAM – what's first: User Interface, Processes, or Infrastructure?** **Marc Bütikofer**, Ergon Informatik AG **Ralf Knöringer**, Atos IT Solutions and Services GmbH **James Litton**, Identity Automation **Mike Nelsey**, Aurionpro Solutions plc **Max Waldherr**, Dell Software Too many companies suffer from complex IAM implementations. Lack of user acceptance due to overly complex user interfaces; massive workloads for business people in recertification; failed projects due to complex infrastructures; the list of challenges is long. On the other hand, the need for a well-working IAM has never been as large as today. Support for more users and other types of identities than ever before, with more and more business users being involved in access requests and identity management; detecting abuse of access rights and excessive entitlements as soon as possible; simple implementation of more than just basic identity provisioning; that's what companies need today. Time to simplify IAM infrastructures. But where to start? Or does it require completely rethinking and re-implementing everything? And how to move from what you have to a simplified IAM infrastructure with broader reach? The panelists will discuss the business and IT demand for simplifying IAM and how to reach that goal.
11:00-12:00	**User Empowerment - The Building Blocks** **Designing the Privacy-Aware Internet: Standards, Trust Frameworks, Encryption, Protocols** **Mario Hoffmann**, Fraunhofer AISEC The lack of control over the flow of personally identifiable data is becoming the most serious inhibitor for the digital economy, further strenghtening the need for standards, technologies and frameworks for secure and transparent data sharing methods. In this session we will move together through the existing building blocks for empowering the user to take full control over his data and create an image on how they fit together. **Extending the Power of Consent with User-Managed Access and OpenUMA** **Eve Maler**, ForgeRock Existing notice-and-consent paradigms of privacy have begun to fail dramatically — and as recent Pew surveys have demonstrated, people have begun to (ahem) notice. The discipline of privacy engineering aspires to "craft", but finds it hard to break out the "compliance" rut. The User-Managed Access (UMA) standard and the OpenUMA open-source project are stepping into the breach with two essential elements that change the game: asynchronous consent and centralized consent management. **Crossing The Chasm: Bridging The Divide Between Consumer Identity And Identity In The Enterprise** **Robert Lapes**, Capgemini Consumer identity marches to the beat of a different drum. It does its own thing regardless of enterprise norms and expectations. So how do you solve a problem like consumer identity? This session take an insightful look at the changing identity landscape and explores the widening gap between consumer and enterprise identity. It talks about the challenges we face as we try to bridge the gap between the carefully controlled enterprise and the complexity of consumers.

12:00-13:00	**Preconceptions of Risk**
	Data and Identity Systems Risk in the Larger Distributed Risk Context
	Thom Langford, Sapient
	
	Risk is often seen as a dirty word in business. It is a thing that needs to be reduced to nothing, and has no possible good use in an organization, especially a security programme. This couldn't be more wrong! Risk is an inherent part of any business, and yet it is often poorly recognized and leveraged in the security organisation.
	
	In this presentation Thom will look at three areas of the risk conundrum to open the veil on the elusive art of understanding and ultimately measuring risk:
	
	1. The initial interpretation of risk and how it is often misunderstood.
	2. The measurement of risk, and how some systems work and other don't.
	3. The effective treatment of risk, and how sometimes the obvious thing to do can be the wrong thing to do.
	
	With the use of analogies and examples, the audience will appreciate that risk assessment, measurement and management is not always as straightforward as it might first seem. The audience will leave with a new appreciation of how risk can be leveraged for good, and not just perceived as bad.
	
	Negotiating the Risk of Privacy - Understanding Privacy and its Risks
	Prof. Dr. Rüdiger Grimm, University Koblenz-Landau, Faculty of Informatics
	
	The growing of volume, velocity and variety of Big Data creates new business models for the exploitation of data, for example individual marketing synchronously created out of clickstream data and background knowledge. However, these opportunities arouse privacy concerns. Users lose control over their privacy, and services are uncertain how to keep the trust of their customers in their decent personal data handling.
	
	In this presentation the risk of privacy in the modern communication technology, both Internet and mobile networks, is analyzed. It turns out, that users have to negotiate the risk of privacy between refraining from services, trusting services, using self-data-protection methods and trusting privacy enhancing technologies. Services, on the other hand, have to present themselves as trustworthy with respect of their competent and decent way to handle user data. This presentation identifies the privacy principles and related trust areas and protection means.
	
	Topics of presentation
	
	• The privacy challenge in the Internet and mobile networks
	  ◦ Privacy principles
	  ◦ Privacy invading and enhancing technologies
	  ◦ esp. permission rights management with mobile apps
	• Risk management
	  ◦ Trust and control
	  ◦ Trust factors in technical environments
	  ◦ Trust factors in IT privacy
	• Negotiating the risk between trust and control mechanisms
	  Privacy risk factors and related trust areas
	  ◦ Weaknesses, measures, and remaining trust areas
	  ◦ Role and perspectives of self and system data protection

12:00-13:00	**Identity Relationship Management (IRM) & the Business Side** **No Person is an Island: How Relationships Make the IT World More Manageable** **Ian Glazer**, Salesforce **The business side of IAM – How to Work with the Business to Make IAM Successful in your Organization** **Bill Evans**, Dell Software **Matthias Reinwarth**, KuppingerCole **Markus Weber**, ForgeRock **Rudolf Wildgruber**, Atos IT Solutions and Services GmbH Everyone knows someone who is dealing with the aftermath of a failed IAM project and as a result, everyone knows someone struggling to move forward with the next phase of IAM. As a result, identity experts are struggling to overcome their organizations' fear of commitment to IAM. In this session, we'll share strategies for re-engaging with the business on its terms to enable you to secure funding for your project, protect the business, and add value to the organization.

12:00-13:00	**Next Generation (Mobile) Cloud** **Enterprise Mobility Management: Best Practices & Lessons Learned** **Pavlos Makridakis**, Aurionpro Solutions plc **Christian Patrascu**, Oracle Corp. **Dominic Schmidt-Rieche**, AirWatch The mobile cloud era represents a tectonic shift and executives are increasingly recognizing the opportunity at stake as they map out the role technology plays in their organizations' future. Workflows are becoming synergized with the elements of mobile and cloud, as field workers are accessing cloud services for their day to day operations. However, this presents security challenges for enterprises when mobile users access sensitive information through email and applications across personal smartphones and tablets. In this session we will discuss how the mobile cloud era can be optimized through agility and automation, while employee & customer privacy and sensitive corporate information remain ensured. **What's Next in Cloud IAM – Moving Beyond Single Sign-On** **Pamela Dingle**, Ping Identity **Dr. Martin Kuhlmann**, Omada **Daniel Raskin**, ForgeRock **Richard Walters**, Intermedia While an imperative component to a truly comprehensive Cloud Identity and Access Management strategy, Single Sign-On (SSO) is not the only factor for enterprises to consider when evaluating the proper long term solution. Other critical factors to keep in mind include advanced trust-based access control, authorization management and audit intelligence for compliance. As enterprises look to take advantage of cloud adoption, these structured best practices will allow companies to leverage existing IAM investments, retain control and meet compliance requirements. In addition, this session will provide a blueprint for secure cloud adoption and a roadmap to an integrated cloud application management – without requiring companies to sacrifice current governance needs and data security. Key Takeaways: • How to retain control and meet compliance requirements in IAM • Actionable tips on secure cloud adoption • Balancing governance and security needs while creating additional value through cloud investments
12:00-13:00	**Internet Scale Encryption, Authentication, Authorization** **Idemix: Secure, Attribute-Based Authentication** **Dr. Jan Camenisch**, IBM Research Identity mixer allows users to authenticate without identifying themselves by revealing only the required attributes. In this talk, we will present the different features of identity mixer, and give an overview on the possible cryptographic realisations of these features. **uProve: The Pricipal of Minimal Disclosure at Work** **Ronny Bjones**, Microsoft U-Prove is a cryptographic technology that allows users to take control over their data and minimally disclose certified information about themselves when interacting with online resource providers. U-Prove provides a superset of the security features of Public Key Infrastructure (PKI), and also provide strong privacy protections by offering superior user control and preventing unwanted user tracking. In his presentation, Ronny Bjones from Microsoft will describe uProve and talk about the deployment of uProve in Life Management use cases **Qiy Scheme: Trusted Exchange of Personal Information** **Marcel van Galen**, Qiy Foundation
13:00-14:30	Lunch & Networking **Room: EXPO AREA**

14:30-15:30	**Digital Risk Officer & Chief Digital Officer** **It Takes a Community to Reduce Risk – Company Leadership and Recruitment of Supply Chains Stakeholders in Risk Mitigation Strategies** **Amar Singh**, KuppingerCole To help stakeholders balancing their needs to protect the organization against the needs to run the business - this is the new role IT professionals have to take over in the era of digital business. Moving forward, security people aren´t the "defenders against cyber threats" anymore. They are becoming the facilitators of a balance between the needs to protect and the needs to run a business. In digital Business, we are moving things into the cloud. We are moving things into software-as-a service. We don´t have control of them anymore. A lot of the traditional technologies just don´t apply. So we have to start looking at other things like contract clauses and the new types of controls which come along with the new breed of digital risks. During this session, we will talk and discuss about the new skills required from IT Leadership. **Recruiting Customers, Suppliers and Even Competitors to Help Reduce Risk** **Thom Langford**, Sapient **Dr. Adriana Nugter**, Independant Senior Consultant **Arieh Shalem**, Orange **Amar Singh**, KuppingerCole Various types of shared economic interests and risks create communities of interest where separate organizations work together such as in myriad supply chains worldwide. How can COIs come together in structured settings such as technical and policy standards initiatives, government programs, markets and other regulatory and self regulatory contexts to identify common needs and design, develop and deploy mutually acceptable solutions? **One Step Closer to the Unhackable Enterprise: Applying an Effective Information Security Strategy** **Stefan Van Gansbeke**, CM/MC Health Insurance Fund Belgium The threat landscape became wicked and rougher. Governments are desperately trying to fight the cyber threats. But their efforts will never satisfy the needs. As a company, community or individual you remain a vulnerable target. Applying a layered information security strategy can effectively reduce your risk exposure. Define your drivers and long term security goals; involve your stakeholders; engage your customers, employees and suppliers; clearly communicate and achieve your targets by implementing the security roadmap are the key steps for becoming a security intelligent company who will be better protected against the next attack. In this revealing presentation, we will share our experiences about building such an effective security strategy.
14:30-15:30	**Best Practice** **Identity @ The Guardian - SSO at Web Scale** **Mark Butler**, The Guardian The Guardian's web and mobile application usage rates are experiencing explosive growth. This growth is driven by an increased consumption of news online. Today's users have high expectations in terms of usability, security and performance. This session aims to highlight the challenges that Identity faces and will discuss the technology that can be used to keep pace in this fast moving development environment. Topics covered will be: • Cloud technology and the importance of scalability. • Security versus usability trades offs and compromises. • Multi device Identity support. • Continuous delivery. • Data driven development and lean principles. **Rethinking Digital Identity: The Australian Government Story** **Ben Bildstein**, Department of Industry and Science (Australian Government) The Australian Government's coordinated approach to digital identity started in the business-to-government domain, with the creation of a whole-of-government credential (AUSkey) and trust broker (VANguard) in 2007. A separate process occurred in the citizen-to-government domain (myGov) in 2013. This case study examines the policy decisions leading to the creation of these systems, and the technical challenges and compromises that followed. This includes the decision to use digital certificates for business transactions, but username/password-based credentials for citizens. It also explains the delay between centralizing business-to-government and citizen-to-government authentication, partly due to the Australian public's rejection of nationalized identity in the Australia Card. At a more technical level, it also discusses multiple exposed and exploited security flaws, which threatened the security benefits of this centralized authentication. Finally, the case study details the changing environment of digital identity, and the technical and policy questions currently being uncovered by the Australian Government in its quest to have all 50,000+ transaction-per-annum systems available end-to-end digitally. Key takeaways: 1. Understanding Australia's approach to digital identity and where it is heading under the Australian Government's digital policy agenda, with comparisons to other countries 2. Appreciation of the hidden security costs of centralized authentication, and the effect of failures 3. Demonstration of how the differences between various authentication and identity domains can necessarily lead to significantly different outcomes and technologies, in the whole-of-government space

14:30-15:30	**Cloud Encryption; Securing IaaS** **Customer-Managed Encryption Keys: Controlling Your Data's Privacy in the Cloud** **Richard Anstey**, Intralinks **Dan Plastina**, Microsoft Businesses put a lot of trust in the cloud, believing that, as paying customers, they will enjoy total protection from hackers and law enforcement agencies trying to access their private data. But the majority of cloud providers who encrypt data have full control over encryption keys and could – if required to – access and share the data. This is a risk many businesses are unaware of. It also means CISOs in industries handling very sensitive data cannot take advantage of the benefits of cloud technology, as their enterprise policies and regulatory compliance requirements prohibit them from having implementations where providers have full access to their data. Customer-managed encrypted keys (CMKs) offer a solution to this problem, putting the data owner in full control of the encryption being used within the cloud service regardless of where it is stored. This combined panel & presentation session will explore how implementing CMKs will give customers back the control of their data as well as promoting cloud adoption. You will become familiar with cryptography systems available now that use CMKs to protect data held by cloud vendors, how they work, when it is necessary to implement, and how it can enable highly regulated industries to operate securely beyond the firewall. **Best Practice: From Zero to Secure in 1 Minute** **Nir Valtman**, NCR Corporation Cloud instances lifecycles are accelerating fast. Cloud providers are competing among them by switching to by-the-minute server billing instead of hourly billing. This means that servers should be installed, launched, process and terminate and all within a range of minutes. This new accelerated life cycle makes traditional security processes such as periodic patches, vulnerability scanning, hardening and forensics impossible. In this accelerated lifecycle, there are no maintenance windows for patches or ability to mitigate a vulnerability, so the security infrastructure must adapt into new thinking. In this new thinking we must adopt new methods for server's security configuration, evaluation and termination. Servers must be patched before they boot up, security configuration and hardening procedures should be integrated with server installation, vulnerability scanning and mitigation process should be automatic and operating systems should not even include user's ability to login directly. In the presentation we announce on a new open source tool named "Cloudefigo" and explain about techniques that enables this new accelerated security lifecycle. We demonstrate how to launch a pre-configured, already patched instances into encrypted storage environment automatically while evaluating their security and mitigating them automatically if a vulnerability is found. In the live demo we leverage Amazon Web Services EC2 Cloud-Init scripts and object storage for provisioning automated security configuration, integrating encryption, including secure encryption keys repositories for secure server's communication. The result for those techniques are cloud servers that are resilient, automatically configured and secure without any attack surface for hacker to explore.
14:30-15:30	**Standards & Protocols** **Protocol meets Architecture: Patterns for Construction of an OAuth Identity Platform** **Pamela Dingle**, Ping Identity For the most part, OAuth 2.0 and other REST-based protocols for identity transactions are ratified and ready to use. But how can they be combined to solve the actual business problem of operating in an identity infrastructure? This session will cover the top 20 patterns of interaction for SSO, mobile, API, and provisioning use cases, showing how a practical combination of clients and scopes can result in a tightly secured identity architecture that leverages combinations of OAuth 2, SCIM, OpenID Connect, JWT assertion flow, JOSE and other protocols, including SAML. Pamela will discuss the pros and cons of solving different problems with different patterns, with the goal of naming and documenting the patterns so that they can be adopted in the industry at large. **OpenID Connect Certification** **Roland Hedberg**, ICT Services and System Development (ITS), Umeå University **Dr. Michael B. Jones**, Microsoft The OpenID Connect protocol has quickly gained widespread adoption, enabling easy-to-use login and API access for both Web and native applications. During its development, extensive interoperability testing was performed on a voluntary basis to ensure that different implementations would actually work together. Now that the OpenID Connect protocol is final, the OpenID Foundation is working to ensure even better interoperation between implementations by creating a self-certification program for OpenID Connect implementations, with early participants including Google, Microsoft, NRI, Salesforce, and Ping Identity. This session will describe the certification test suite software developed by Roland Hedberg of Umeå University and how OpenID Connect implementers use it to certify their implementations to the OpenID Foundation. **The Security Stack for Modern Applications: OpenID Connect and OAuth 2.0** **Dominick Baier**, Thinktecture We need a modern, mobile first and API friendly security stack for building the current and next generation of applications and services. This includes authentication, authorization and delegated API access. OpenID Connect and OAuth2 provide an unprecedented alignment in providing one unified solution for the above problems and have reached excellent true cross-platform and –vendor adoption in very short time. This talk walks you through the mechanics of the protocols and how they solve common application scenarios – especially when combined.

15:30-16:30	**Cloud Risk Assessment** **Assessing and Mitigating Cloud Risks** **John Hermans**, KPMG **Mario Hoffmann**, Fraunhofer AISEC **Olga Kulikova**, KPMG **Mike Small**, KuppingerCole The modern reality is that even the most technology conservative companies are thinking to shift some of their valuable assets to the cloud. However, since anyone with a credit card can purchase cloud services with a single click, the governance and control of organisations are frequently being circumvented. This can create various challenges for organisations that wish to adopt the cloud securely and reliably. This session will lead you through various approaches on how to assess and mitigate risks for onboarding cloud solutions. Key Takeaways: 1. understanding of information risks related to cloud usage. 2. understanding of the concept of dynamic selection of controls, based on data profile, to mitigate cloud risks. 3. application of the proposed framework in daily practice (e.g. by turning it into a software tool that allows quick and easy control selection for employees responsible) **Dynamic Control Selection Framework for Onboarding Cloud Solutions** **Olga Kulikova**, KPMG This talk will propose a data-driven selection of organisational, technical, contractual and assurance requirements, so secure usage of cloud solutions within the enterprise can be guaranteed. The importance of data oriented control selection will be outlined and key control domains will be introduced. **Dynamic Certification of Cloud Ecosystems** **Mario Hoffmann**, Fraunhofer AISEC Cloud ecosystems are dynamic and flexible enablers for innovative business models. Some business models, especially for the European cloud market, however, still face challenges in security, privacy, and trust. A common approach among cloud providers addressing these challenges is proving one's reliability and trustworthyness by audit certificates. Basically, audit certificates are based on national and/or international as well as business and/or governmental compliance rules. The most prominent certifications in cloud computing are the "Open Certification Framework (OCF)" of Cloud Security Alliance, EuroCloud's "Star Audit", and "Certified Cloud Service" provided by TÜV Rheinland as well as more general certifications following ISO 27001, BSI Grundschutz, ENISA, and NIST. This session will discuss the state of the art of auditing and certifying cloud ecosystems and how current certification catalogues and schemes have to be enhanced to meet future requirements - requirements such as dynamic certification, on-demand-audits, and automatic monitoring and evaluations. **Cloud Risk Assessment – An "Action-Oriented" Approach to Merge Engineering, Economic and Legal Analyses.** **Mike Small**, KuppingerCole When moving to the use of cloud services it is most important to take a risk based approach. However the process involved is often manual and time consuming; a tool is needed to enable a more rapid and consistent assessment of the risks involved. This session describes why a risk based approach to the use of cloud services is needed. It introduces the KuppingerCole Cloud Rapid Risk Assessment Tool developed by KuppingerCole to help organizations assess the risks around their use of cloud services together in a rapid and repeatable manner. After attending this session you will be able to: • Describe why a risk based approach is needed. • Describe the KuppingerCole Cloud Rapid Risk Assessment Tool • Describe the benefits from the use of this tool.
15:30-16:30	**FIDO Alliance: Simplifying User Authentication** **The Death of the Password - Is It Finally Coming True?** **Alexei Czeskis**, Google **Tord Fransson**, Yubico **Dr. Michael B. Jones**, Microsoft **Rolf Lindemann**, Nok Nok Labs **Anthony Nadalin**, Microsoft **Donal O'Shea**, FIDO Alliance "Death of the Password" announcements have been around for a decade or more, but none of them have come true. The FIDO Alliance (Fast Identity Online), founded in 2012, with a member list reading like the Internet Who-isWho, has been gaining so mcuch traction with its proposed standard security protocol, that this time chances are great that the password based authentication will be killed. In this session we will talk about the concept behind the FIDO protocol and understand the benefits the FIDO standard can create inside and outside the enterprise.

15:30-16:30	**Hybrid Cloud & Beyond** **Best Practice: A Hybrid Enterprise in a Cloud First World** **Brian Puhl**, Microsoft You'll laugh, you'll cry, and you might even pick up a useful nugget or two listening to a real-world enterprise IT architect share the experiences of the past year trying to support his business migrating to cloud services, and sharing the lessons learned from trying to integrate 2 hybrid enterprises into a single, streamlined company. You'll hear where the cloud came through for us, and how we often had to fall back to on-prem services such as FIM, Ping Federate, and ADFS to make the glue which binds it all together. Key Takeaways: • Migrating to the cloud can be hard; mergers and acquisitions of companies is hard; M&A of hybrid cloud enabled companies is very hard. • How to manage the cloud vendor relationships through integrations • Identity and Security planning to make integrations successful in a cloud world **Identity-as-a-Service Securing PostNL's 100% Cloud Strategy** **Theo Punter**, PostNL PostNL deals in letters, parcels and everything related to letters and parcels. PostNL is with 60.000 employees and 3.4 billion of revenues the leader in The Netherlands and PostNL also works in Belgium, Luxembourg, the United Kingdom, Germany and Italy. Volumes in the letters business are declining and therefor cost cutting and having flexibility in cost both in Business and in IT are a key target for PostNL. For this reason, PostNL announced a 100% go to Cloud strategy where execution will be finished by the end of 2015 by migrating all on-premise hosted applications to the Cloud: "from on-premise/customized to cloud-based/standardized IT". Identity and Access Management is an essential part of the security domain within the PostNL Cloud Orchestration Kernel to facilitate the 100% Cloud Strategy and to comply to security standards and certifications for 'securing the cloud'. Through the IAM project Identity and Access Management is implemented for PostNL employees using the services of the IDaaS provider iWelcome – so a cloud service in itself. This full IDaaS service includes amongst others: availability of all employee identities, a login page including (two factor) user authentication, a portal (launch pad) for cloud application, user provisioning and authentication to relying parties, single sign-on/log-off and self service. Generally speaking there are five main areas in Identity Management being: (1) Identity Governance (business processes around so-called authoritative sources like SAP HR); (2) Identity Provisioning; (3) Identity Authentication and Access Management and (4) Application Authorization (business logic in the destination applications). Theo Punter will share his experiences with the audience about implementing IDAAS for the enterprise. Key Takeaways: • Current IAM solutions could not keep pace with developments in the cloud, mobile apps and federations; • With IDAAS PostNL is able to lower TCO significantly and thus serving improvements in PostNL's market position • Suppliers preferably to big to fail ... but partnership and flexibility is a key value as well • Stick to standards and enforce them • Define I&AM policies upfront to CSP's (as part of contract) • Over 90% use SAML2.0 for authentication but SCIM as a standard for provisioning is not there yet • Don't mix cloud with on-premise unless you design on-premise on cloud principles. • Release and transition management becomes even more important • Don't make critical IT plans on product roadmaps of suppliers.
15:30-16:30	**OASIS SAML & XACML for Consumer Identity** **Securing Sensitive Data While Enhancing Privacy** **Dr. Michael Garcia**, National Institute of Standards and Technology (NIST) **Gerry Gebel**, Axiomatics Americas **Karyn Higa-Smith**, U.S. Department of Homeland Security **Soren Peter Nielsen**, NineConsult **Daniel Raskin**, ForgeRock **John Tolbert**, Queralt This session will begin with an outline of the common technical elements of privacy regulations. The speakers will provide a high level overview of the OASIS SAML and XACML standards to elucidate how they're used to secure sensitive data, such as government data and intellectual property. The group will describe how standards-based technologies are solving privacy issues through current use cases. The audience will hear about the U.S. Department of Homeland Security's objectives to improve consumer privacy. And finally, the speakers will outline potential future versions and/or profiles of SAML and XACML that may enable them to better serve new privacy concerns. Audience participation will be encouraged.
16:30-17:30	Coffee & Networking **Room: EXPO AREA**

17:30-18:30	**Think Globally, Act Locally** **Understanding and Dealing with Macro-Level Risks that Affect your Institution's Risk Profile** **Ben Bildstein**, Department of Industry and Science (Australian Government) **Karyn Higa-Smith**, U.S. Department of Homeland Security **Dr. Roy Lindelauf**, Netherlands Defence Academy **Howard Mannella**, Alternative Resiliency Services Corp **Robin Wilton**, Internet Society The phrase "think globally, act locally" was initially invoked as a rallying cry of the environmental movement in an effort to help people connect their individual actions to global challenges, and increase their sense of efficacy to effect change by acting in concert to carry shared narratives of environmental risk mitigation into effect. The concept of "think globally, act locally" has new meaning in the context of business organization risk from IoT, the cloud and other networked information system functions. The local instances of information functions on which businesses increasingly rely are part of data and identity "supply chains" that are hybrids of technology and policy that are themselves increasingly part of vast global networks where individual businesses often perceive a loss of leverage and control and increased risk. In effect, federated and cloud based data and identity functions are enabling these functions to be outsourced, like shipping, payroll, accounting and other company functions that have previously been outsourced to global networks. There are myriad publicly and privately led initiatives (and many that are hybrids of public and private efforts), through which stakeholders from multiple organizations can work together to design, develop and deploy shared strategies where hybrids of technology and policy offer local solutions to new information and interaction challenges, increasing the sense of control from the cohesion of organizations acting in concert to carry their shared narratives of interaction risk mitigation into effect.
17:30-18:30	**Privilege Management** **Privilege Management Use Cases** **Christian Götz**, CyberArk **Serge Ingber**, ObserveIT **Amar Singh**, KuppingerCole **Edwin van der Wal**, Everett **Nathan Wenzler**, Thycotic In this session,we will walk through major use cases for Privilege Management. Which are the most common use cases, what to look at in particular and which specific features to stress-test in a PoC? **The Snowden Effect: Why seeing is believing** **Chris Pace**, Wallix **Wolfgang Roesch**, Tesis Sysware **Michael Yaffe**, BeyondTrust We pride ourselves on being proactive in dealing with external threats to our data. But why is our approach to the insider threat so much more reactive and forensic? Have we considered that being able to actively monitor and take action where privileged users behaviour is identified as risky might help us prevent this kind of data loss? Thinking beyond log management to identify behaviour. Key Takeaways: • Understanding the benefits of real-time monitoring. • Considering which parts of their organization are most and risk and might benefit from real-time monitoring.
17:30-18:30	**Business-Critical Infrastructure & Applications** **The Future of Directory Services: Data Models - Performance - Security** **Andrew Ferguson**, KuppingerCole Asia Pacific **Peter Gietz**, DAASI International GmbH **Thorsten Niebuhr**, WedaCon Informationstechnologien GmbH While there hasn't been much news around directory services in the last decade, we see new momentum in this area, driven by two challenges and both related to the "hyberconnected" enterprise that has to manage identities of consumer, things, devices etc. and their relationships. One challenge is performance. Managing some thousand employees or even tens of thousands or a few hundred thousand is fairly different from managing tens of millions of customers, billions of things, or all the related devices. There have been some large deployments particularly in the consumer space, but right now this is moving from a specialized use case in few industries towards a standardized requirement of virtually any industry. Vendors propose various answers to that challenge. HDAP (Hadoop + LDAP), Cloud Directory Services, or just larger deployments of their COTS products. But what does it really need? The other challenge are data models. LDAP, being derived from X.500 DAP, has its roots in phone directories. It has a rather inflexible data model. When looking at the broad variety of identities to manage, beyond humans, and theire complex relationships, the question arises whether the LDAP data model is good enough for the future. Some vendors already decided against LDAP as the core of their directory data model. But what does it really need? In this panel, both the challenge of performance and of data models will be discussed in depth. Is LDAP still the future or do we need something different? Will there be new REST-based standards or will we end up with proprietary approaches? **Business Critical Application Security** **Christian Patrascu**, Oracle Corp. **Gerhard Unger**, Onapsis Inc. Most transactions take place on business-critical applications and infrastructure, producing data and information with the highest possible value for attackers. Protecting these applications and infrastructure is a fundamental part of each corporate security strategy. In this session we will talk about the real security challenges facing your business critical infrastructure, i.e. your SAP system, how mitigate the risks involved and prevent against threats.

17:30-18:30	**Telcos & Innovation** **Identity Strategy for Innovation** **Chema Alonso**, Eleven Paths, Telefonica **Facing The Future: Identity Opportunities for Telco Operators** **Chema Alonso**, Eleven Paths, Telefonica **John Bradley**, OpenID Foundation, Kantara **Jörg Connotte**, Deutsche Telekom AG **Marco Dütsch**, Swisscom **Maarten Louman**, Qiy **Dr. Adriana Nugter**, Independant Senior Consultant **Arieh Shalem**, Orange **Nick Tuffs**, Vodafone With the advent of 4G/LTE, mobile operators are facing challenges and opportunities that will shape the future direction of communications for at least the next five to ten years. Faced with the erosion of revenues from the rapid encroachment of the so-called OTT (over the top) players, such as Apple, Google and many others, into their traditional market strongholds, operators are coming to the increasing realisation that data – 'big data' – represents their most significant asset in terms of being able to provide added value to their customers in the future. A key aspect of this transformation will be how operators are seen to astutely manage the wealth of user data at their disposal to good effect and position themselves as secure identity brokers and/or identity providers in what is already becoming a highly competitive market. This panel session will highlight the challenges facing operators in this brave new world and give examples of how some operators are already addressing the opportunities. Whilst focused on telco, other industry sectors, such as postal and general utilities, are facing similar challenges and opportunities and the session will also get an insight from these perspectives.
18:30-18:50	RISK is Not a @#$%&! Dirty Word! **Thom Langford**, Director Global Security Office, Sapient **Room: AUDITORIUM**
18:50-19:10	Connected Identity : Benefits, Risks & Challenges **Prabath Siriwardena**, Director, Security Architecture, WSO2 **Room: AUDITORIUM**
19:10-19:30	No Security without Identity **André Durand**, Founder & CEO, Ping Identity **Room: AUDITORIUM**
19:30-22:00	European Identity Awards Ceremony & Buffet Dinner **Room: AUDITORIUM**

Thursday, 07.05.2015

08:00-18:00	Check-in & Registration **Room: COUNTER EXPO AREA**
08:30-08:50	Finding the Balance Between Secrecy and Operational Efficiency **Dr. Roy Lindelauf**, Military Operations Research, Netherlands Defence Academy **Room: AUDITORIUM**
08:50-09:10	Identity & Access Process Automation: Improving Business Alignment & Reducing Digital Risk **Dirk Venzke**, Director, Commerzbank AG **Room: AUDITORIUM**
09:10-09:30	tba **Ravi Srinivasan**, Director, IBM Security Systems **Room: AUDITORIUM**
09:30-09:50	CISO in the Cloud with Diamonds **Arieh Shalem**, CISO, Orange **Room: AUDITORIUM**
10:00-11:00	Coffee & Networking **Room: EXPO AREA**

11:00-12:00	**EU Privacy Regulation** **The Proposed New European Union Data Protection Regulation - Status and Implications** **Rhiannon Davies**, DAC Beachcroft LLP **Kuan Hon**, Queen Mary University of London **Dr. Karsten Kinast LL.M.**, KuppingerCole The proposed new data protection regulation aims at European data protection standards which are better harmonized than the current legislation and also suit the technical standards in times of transformation. A unified data protection Regulation that is directly applicable as part of the EU's Digital Single Market shall make it easier for all parties to understand what their rights and obligations are and what compliance risks they need to manage. One of the main changes foresees that EU data protection law is valid whenever the European market is targeted – whether from within or outside of the EU. Amongst other regulatory novelties, strict enforcement and data protection by design will mean a truly new data protection environment. Take-aways: • What is the proposed New European Data Protection Regulation all about? • Data Protection Compliance issues to come • Risk Implications for companies and groups **The Role of Privacy by Design in the New EU Data Protection Regulation** **Dr. Karsten Kinast LL.M.**, KuppingerCole **André Lutermann**, Dell Software The upcoming EU privacy legislation demands for implementation of a "privacy by design" approach for organizational IT-systems and processes. To showcase technology embracing this principle for Identity, access and secure authentication EU funded the attribute-based Credentials for Trust project (ABC4Trust). ABC4Trust is an EU-funded research and development project advancing the federation and interchangeability of technologies supporting trustworthy and at the same time privacy-preserving Attribute-based Credentials (Privacy-ABCs). • What is ABC4Trust all about, what are benefits and shortcomings? • How can actual technology help to meet privacy and security requirements
11:00-12:00	**Access Governance Best Practice** **One-Click Insight, Lean Recertification, Improved Compliance: Redefining Access Governance for the Digital Business** **Matthias Reinwarth**, KuppingerCole Improve your level of compliance, gain up-to-date insight and reduce recertification workload. Add business risk scoring to your Access Governance Architecture, focus attention on high-risk access and extend your existing infrastructure to provide real-time access risk information. Re-think your existing Access Governance processes and understand upcoming IAM challenges and their impact on your infrastructure. In his opening notes for the Access Governance Track, Matthias Reinwarth will share with you his experience from a decade of Identity & Access projects in various industries and describe, why KuppingerCole propose to redefine Access Governance so that it fits to the needs of the Digital Business. **Externalized Access Management (ABAC, RBAC) at Talanx Systeme AG for Bancassurance** **Frank Wittlich**, Talanx Systeme AG Beginning from the architectural impact of authorisation as a cross-sectional function in the system environment of an insurance service stack, role based access control (RBAC) and attribute based access control (ABAC) will be introduced. After these preliminary considerations it will be shown by means of the case study of the Talanx Bancassurance that both models co-exist efficiently and seamlessly by using a standard authorization tool. **IAM Processes and their Communication Loops** **Stephanie Jaecks**, Bayer BBS Need of basic business demands – providing IAM solution - establish fundamental operation – guidance, support and communication. To ensure the implementation of these chain within an global organization and to fulfill or exceed the expectations of our customers, regarding quality, service level and usability is a challenging and fascinating job. In this session the principles based on examples will be presented how IAM processes and their communication loops are established successfully at Bayer

11:00-12:00	**The Future of Collaboration** **Digital Rights Management – UBS Case Study** **Marek Pietrzyk**, UBS As a global operating financial institution UBS provides investment banking, asset management, and wealth management services for private, corporate, and institutional clients worldwide. UBS is the biggest bank in Switzerland, operating in more than 50 countries with about 60,000 employees around the world. As a leading financial services provider, UBS defines information security as the backbone of our business. Our clients, as well as employees trust us to keep their information safe and secure, so it is critical that we prevent any accidental or unauthorized access to them. The session will present UBS' experience in defining and executing an enterprise-wide data classification and protection project to ensure the safety and integrity of the firm's sensitive client data. The presentation will focus on UBS´ experience on: • Classification and protection of reports generated from applications containing CID (Client Identifying Data). • Methods for automatic protection of downloaded or user generated files. • Measures for effective controls of internal and external transmissions of emails with sensitive content. • Keeping all activities logged, reported and monitored enterprise-wide. • And how to successfully deploy such a major security infrastructure release – avoiding number of security traps. **Coutts Bank Case Study** **Andrew Church**, Coutts **Secure Information Sharing - The User Experience** **Andrew Church**, Coutts **Marek Pietrzyk**, UBS **Amol Sawarkar**, International Federation of Red Cross and Red Crescent Societies (IFRC) As a result of the number of high profile, headline-grabbing revelations about security breaches and the consequent, well-publicised legal and financial implications, many enterprises, already worried about the free-and-easy transmission of sensitive company material have been impelled to take action to ensure that in the future their digital assets are far better protected from falling into the wrong hands than previously. This session will show the experience and lessons learned from some of the early adopters of rights management
11:00-12:00	**Life Management Best Practice** **Life Management in Finance & Insurance Industry** **Frank Cooler**, Intrasurance **Marcel van Galen**, Qiy Foundation **Ad van Loon**, X-media Strategies **Dr. Adriana Nugter**, Independant Senior Consultant European Union legislation like PSD2 and the proposed new Data Protection Regulation have a serious impact on financial business. Should we pretend business as usual or change the way the finance & insurance industry interacts with their customers. The "privacy by design" approach of Trust Frameworks might be a solution. • Simplicity; reducing complexity • User-friendliness • Bring the customer 'in control'
12:00-13:00	**Cloud Contracting Risks** **Reaching Compliance Across Jurisdictions: Fundamental Considerations Before Signing a Cloud Services Contract** **John Hermans**, KPMG **Dr. Karsten Kinast LL.M.**, KuppingerCole **SaaS Contracting: From Risk to Complaince** **Edwin Sturrus**, KPMG Advisory N.V. Although SaaS adoption is rapidly increasing, many organisations struggle to establish a sustainable process for SaaS contracting. The one-size-fits-all aspect of cloud computing is often reflected in the limited flexibility of cloud service providers during contract negotiations. More and more organizations are left with the choice of signing standard terms and conditions. This strongly increases the need for organizations to define their contract requirements prior to selecting a SaaS solution. The specific types of data (e.g. confidential data, privacy sensitive data) to be stored in the future SaaS solution, the related risks and applicable legal domains (e.g. data privacy, trade controls) should determine the contract requirements. These requirements have to be taken into account in order to ensure compliance with laws and regulations after accepting any terms and conditions. During this presentation the basics of data classification for SaaS, determining applicable legal domains and verifying the resulting contract requirements against the terms and conditions are discussed. Key Takeaways: • Understanding how to define contracting requirements • Ability to determine applicable legal domains • Understanding and comparing terms and conditions

12:00-13:00	**IAM Standard Processes** **Roles or no Roles, that's the Question. Two Different Approaches for Compliant IAM Processes.** **Matthias Reinwarth**, KuppingerCole **Dr. Horst Walther**, KuppingerCole In this session, Matthias Reinwarth and Horst Walther will present the KuppingerCole standard IAM process models in two variants. One uses roles for implementing a consistent, comprehensive approach. However, there are various situations where deployment of complete role models is not feasible. For these situations, KuppingerCole has developed a lean model that works without roles, but allows organizations streamlining and standardizing their IAM processes anyway and meeting essential compliance requirements. **RBAC & ABAC Hybrid Approaches** **Frank Böhm**, FSP **Thorsten Niebuhr**, WedaCon Informationstechnologien GmbH **Patrick Parker**, EmpowerID **Frank Wittlich**, Talanx Systeme AG Over the past several years, there have been a lot of discussions around terms such as RBAC (Role Based Access Control), ABAC (Attribute Based Access Control), Dynamic Authorization Management (DAM) and standards such as XACML. Other terms such as RiskBAC (Risk Based Access Control) have been introduced more recently. Quite frequently, there has been a debate between RBAC and ABAC, as to whether attributes should or must replace roles. However, most RBAC approaches in practice rely on more than purely role (i.e. on other attributes), while roles are a common attribute in ABAC. In practice, it is not RBAC vs. ABAC, but rather a sort of continuum. However, the main issue in trying to position ABAC as the antipode to RBAC is that attributes vs. roles is not what the discussion should be about. The difference is in how access is granted. This panel will be not be about RBAC vs. ABAC. It will be about RBAC & ABAC & more. What are the essential elements for moving towards an adaptive, policy-based access management (or APAM)? What do we need for a better access management that we can implement today and extend subsequently, moving from static to dynamic controls and from ACLs to policies? How to make this work with and without application integration? This panel is a must-attend panel for all people involved in defining and redefining their Access Management approaches.
12:00-13:00	**Market Maturity** **Protecting and Tracking Sensitive Data** **Dr. David Goodman**, KuppingerCole **Dan Plastina**, Microsoft Modern organizations routinely share sensitive data both internally and externally. This session will present a solution capable of letting data owners protect, control, and track their sensitive data regardless of where it is used (or abused). We'll specifically present solutions for both front office and industrial use cases. **Information Centric Security; the Way to Go?** **Rui Melo Biscaia**, Watchful Software **John Grillos**, Seclore **Henk Van der Heijden**, TecHarbor **Eyal Manor**, Secure Islands **Scott Masson**, TITUS **Dan Plastina**, Microsoft **Jose Manuel Rodriguez**, Prot-On In the current world of fast-moving organizations with high demands of new services and supporting IT-systems we can no longer deal with the "old" perimeterized way of protecting the organizations assets. We are in need of a much more focussed and efficient approach that will allow us to protect our assets on their needs. Classification of information and protecting at it it's source is the way forward. Solutions have evolved that can make this happen without the major downsides of previous technologies that had business users adjust their behaviour and think about the needed protection at the end-user level. Nowadays technologies can be implemented that are transparent and easy-to-use while protecting the organizations assets against abuse and misplacement. The presentation will describe the changing landscape, the methodology to such an approach and a description of technologies that can assist in moving forward protecting your information. Key Takeaways: • Alternative view on protecting your organizations assets • Methodological approach to such a process • Key technologies that can assist
12:00-13:00	**Bring Your Own Privacy** **Life Management Use Cases & Business Models** **Katryna Dow**, Meeco Enabling individuals, citizens, consumers to take control of their data with the opportunity to "exchange" it for shared value, will be one of the most significant shifts in business models in the decade ahead. What are the opportunities for individuals, government, business, health, education and consumer brands? What does disruption look like? What opportunities are there for new business models? **Empowering the Consumer for Digital Business and the Identity Economy** **Prof. Dr. Sachar Paulus**, KuppingerCole The transformation of business models into digital and the creation of new, natively digital business models, is requiring a new quality of interaction between individuals, businesses, governments and other institutions. Digital Business needs personal information of the consumer and therefore only can be successfull, if the consumer is able to have full control over what to share with whom. In this session, we will have a look at the market readiness for "privacy-by-design" approaches and user empowerment and give an outlook on how the markets will develop.

13:00-14:30	Lunch & Networking **Room: EXPO AREA**
14:30-15:30	**Software Defined Everything** **The Role of Policy Management in the Software-Defined Era** **Tim Grance**, NIST **Andy Land**, IBM **Anthony Nadalin**, Microsoft **Ken Owens**, Cisco Systems **Hemma Prafullchandra**, HyTrust The morning sessions explored policy-based solutions to IoT, cloud and other online-based risks. This session explores the connection of technology and people through the growing role of standards in policy management in an era where the reliability of software-based organization and operations are increasingly depended upon by organizations. This session will seek to help businesses to identify what elements of risks are mitigated, and what new risks arise, with these changes. “Software-defined” is an emerging technology trend that is getting rapid traction, allowing for amazing management, security and compliance innovations. But ‘software-defined’ also makes the application of policy more critical – and more complicated. For example, new servers and networks can be provisioned anytime, anywhere. Assets can connect with other resources, and be used for any purpose by anyone, all based on policy. A policy is a principle or protocol to guide decisions and achieve rational outcomes. How do we rationalize regulations requirements with software-defined, context-aware security policies? The panel is comprised of industry experts from NIST NCCoE, Microsoft, Intel, Cisco and HyTrust, who will discuss the role of policy management in the software-defined era. Speakers will present commonly used policy definitions and usage, and debate the emerging need for policy-based resource lifecycle management, including how to secure these resources and demonstrate compliance, leveraging concrete use cases: 1) Software Defined Networking, 2) Software Defined Data Center/Orchestration, and 3) NCCoE Building Blocks – ABAC and Trusted Geo-Location.
14:30-15:30	**Dynamic Authorization** **Adaptive Policy-Based Access Management: Beyond ABAC and RBAC** **Martin Kuppinger**, KuppingerCole Over the past several years, there have been a lot of discussions around terms such as RBAC (Role Based Access Control), ABAC (Attribute Based Access Control), Dynamic Authorization Management (DAM) and standards such as XACML. Other terms such as RiskBAC (Risk Based Access Control) have been introduced more recently. In particular, a frequent discussion has been going on between RBAC and ABAC enthusiasts, as to whether attributes should or must replace roles. However, most RBAC approaches in practice rely on more than purely role (i.e. on other attributes), while roles are a common attribute in ABAC. In practice, it is not RBAC vs. ABAC, but rather a continuum. During this session, Martin Kuppinger will open the discussion on the different ways how access is granted - in a static, ACL-like approach or more dynamically, based policies and contextual information - and what the challenges are when moving to a more dynamic approach. **The Future of Authorization** **Gerry Gebel**, Axiomatics Americas **Martin Kuppinger**, KuppingerCole **Darran Rolls**, SailPoint **Markus Weber**, ForgeRock **Frank Wittlich**, Talanx Systeme AG
14:30-15:30	**New Security Solutions for the Enterprise** **What If the Future of Security Means Not Knowing It’s There?** **Kim Cameron**, Microsoft **Nishant Kaushik**, CA **Christian Patrascu**, Oracle Corp. **Jackson Shaw**, Dell For the modern enterprise, agility is the name of the game. What does that mean for enterprise security? How can security practices and policies evolve at the same rate as the business, while simultaneously adapting to an anywhere, anytime, any device IT environment that faces an increasing number of increasingly complex security threats? As the real world becomes more real-time, security will need to adjust by transitioning from a highly structured, policy-based, block-and-interrupt model to an identity based, adaptive architecture that relies on an information rich environment, advanced analytical capabilities and more automation to become a ubiquitous, passive presence. In this panel discussion, a group of identity and security thought leaders will examine how identity, cloud and emerging tech are enabling new and innovative security solutions for the borderless enterprise, and the adjustments, challenges and opportunities that these solutions will create for businesses. **User Discovery: Changing Best Practices and Protocol Convergence** **Pamela Dingle**, Ping Identity The simple question of "who are you" is a problem with changing importance in the identity industry. Reigning best practice in authentication has favored a stateless model, where all users are treated as strangers when a session is not detected, regardless of high likelihoods of recurring usage by a single person on a given browser or device. This best practice is now under challenge, as multifactor authentication more tightly binds user identity to devices, and as security context, identity context, device context, geographical location and user consent become common and important parts of authentication ceremonies. Pamela Dingle will discuss how identity protocols are combining to attempt to correctly identify the user in advance of the authentication moment, and the advantages of this guessing game for identity and security architects.

14:30-15:30	**IoT/OT Privacy & Security** **Security and the Internet of Everything and Everyone** **Mike Small**, KuppingerCole The vision for an Internet of Everything and Everyone (IoEE) is for more than just an Internet of Things. It provides opportunities for organizations to get closer to their customers and to provide products and services that are more closely aligned to their needs. It provides the potential to enhance the quality of life for individuals, through better access to information and more control over their environment. It makes possible more efficient use of infrastructure by more precise control based on detailed and up to data information. It will change the way goods are manufactured by integrating manufacturing machinery, customers and partners allowing greater product customization as well as optimizing costs, processes and logistics. However the IoEE comes with risks, and organizations adopting this technology need to be aware of and manage these risks. The realization of the vision is based on existing systems and infrastructure which contain known weaknesses. This is leading to risks to individual privacy and the organizations using the technologies risk using tainted data. After attending this session you will be able to: • Describe the 4 major challenges from the IoT • Describe the 5 major steps and organization needs to take to securely exploit the IoEE **IoT Privacy Risks, Legislation and Solutions** **Kuan Hon**, Queen Mary University of London **Yariv Lenchner**, Cyber-Ark Software **Peter Niblett**, IBM **John Sabo**, OASIS Idtrust **Erik Sucksdorff**, GlobalSign In this session the panel will look at how the IoT is changing the privacy landscape. People are using devices without being aware of the amount of data that these devices are collecting or the potential uses to which this data will be put. At the same time the legislation around privacy is being strengthened and how will this impact on the processing of this data. How will the OASIS Privacy Management Reference Model and Methodology (PMRM) help to implement the policies controls and functionalities to mitigate these risks.
15:30-16:30	**Risk Metrics** **What Gets Measured Gets Done – Identifying New Metrics for Distributed Digital System Performance to Evaluate and Mitigate Risk.** **Dr. Roy Lindelauf**, Netherlands Defence Academy **Nathan Wenzler**, Thycotic Data is the lifeblood of organizations and managers of organizations have access to increasing volumes of data; but what does data really mean in a given context? How can effective and dynamic risk evaluation and mitigation processes be cultivated from better measurement practices in an organization, and a more nuanced understanding of how different sources of risk will reveal themselves through different sorts of metrics. **How to Measure the Real Access Risk?** **Niels von der Hude**, Beta Systems Software **Wolfgang Roesch**, Tesis Sysware There are many factors that make up the access risk of users. Access to privileged accounts, but also elevated privileges in certain applications sum up to a complete picture of access risks. Users with uncommon combinations, user that have fairly different access than their peers, users with many direct assignments of entitlements: All these indicators might be related to higher access risk – or not. Aside of that: Not only the assigned entitlements are risk indicators, but also the use of access rights. Someone might access only the records of customers he is currently working with – or the ones of all customers he potentially has access to. The first one is just normal, the other an indicator of fraud. However, organizations need to understand the real risks for being able to mitigate these. In this session, the participants will discuss various approaches on measuring risk, looking at that from various angles.

15:30-16:30	**Best Practice** **IAM/IAG @ Continental AG: Clearing Process as a Basis for Identity Management** **Theodor Heindl**, Continental Corporate Infrastructure The history of Continental consists of many mergers and aquisitions which lead to a very heterogeneous environment concerning accounts and account processes. Continental designed a special clearing process to securely map the HR data and account data of each employee and create the digital identity. As a next step the identity lifecycle processes will be defined and implemented. **Identity Relationship and Access Management and Dynamic Authorisation Management as a Driver for New Business Opportunities** **Laura Lätti**, DNA Finland If you can externalise authorisation management away from the application you will simplify online application development considerably. If you can externalise authorisation and identity management to your customer you can achieve considerable cost savings through self-service functions. If you put your customer in control of their identity data, and link your Identity Relationship and Access Management (IRAM) solution to your CRM, you can automate registration processes and invite customers directly from the CRM to your online services. As the customer has control over their identities and authorisations using the IRAM solution, you will improve the quality of the customer data within your CRM and you'll be able to increase the efficiency of your sales and marketing by 30%, or as much as your CRM currently holds out-dated, corrupt or incorrect data. With 3 million customers DNA Ltd. is Finland's largest cable operator, a leading pay TV provider in both the cable and terrestrial networks the and third largest mobile operator. At the end of 2013 DNA adopted an Identity Relationship and Access Management solution to help them better manage their corporate customers. Dynamic Authorisation Management has proven to be the biggest benefit of the IRAM deployment facilitating considerable cost savings. In 2014 DNA started to offer selected cloud services to their customers. The cloud brokerage service is utilising the IRAM solution extensively. New B2B services will be integrated to the IRAM solution in the Spring of 2015. With the help of Identity Relationship and Access Management DNA was able to generate new business and achieve considerable cost savings. Come and see how this was possible. Key takeaways: • How to generate new business opportunities with Identity Relationship and Access Management solutions • How did dynamic authorisation management help DNA • How can you effectively manage a corporate customer base of tens of thousands with an Identity Relationship and Access Management solution • What's the bottom line? Was it worth it?
15:30-16:30	**IAM as a Managed Service** **IAM as a Service Best Practice: B.Braun Melsungen AG** **Martin Oberlies**, B.Braun Melsungen AG **Experiences with IAM as a Service and/or IAM Managed Service** **Martin Oberlies**, B.Braun Melsungen AG **Theo Punter**, PostNL **Darran Rolls**, SailPoint **Maarten Stultjens**, iWelcome **Yso Vonk**, NXP Semiconductors **Peter Weierich**, iC Consult GmbH Many organizations today raise the question whether they could and should move their IAM infrastructure to the cloud (IAM as a service) or run it as a managed service. However, many IAM infrastructures still primarily support on-premise applications, thus this would be about connecting back to the on-premise IT infrastructure. So, does IAM in the cloud or as managed service only work well for organizations that run most of their IT in the cloud anyway? And what about customizations? IAM deployments commonly are heavily customized – will this work in such environments as well? Or is it anyway the better approach to rely more on standards for IAM processes etc.? And what about the risks of running IAM, which deals with the sensitive areas of identity and access, outside of the enterprise? Is it too much of a risk? The panelists will discuss these and other questions around when and why to move IAM to the cloud and when to better leave it on-premises.

15:30-16:30	**Identity of Things** **Putting Identity at the Center of IoT- Kantara IDoT Strategic Review** **Victor Ake**, ForgeRock **Andre Boysen**, SecureKey Technologies **Ingo Friese**, Deutsche Telekom AG **Hannes Tschofenig**, ARM The whole world is talking about the business opportunities that the Internet of Things (IoT) will enable. Industry analysts predict that IoT product and service suppliers will generate growing revenue exceeding $300 billion in 2020. While others forecasts that the worldwide market for IoT solutions will grow to $7.1 trillion in 2020. With numbers in the billions and trillions it's no surprise that the enterprise is paying more and more attention. This landscape of promise also brings mountains of strategic questions for the Identity and Security experts to ponder. There are many standards that can be applied in the IoT space. However broad cross vertical interoperability remains as a challenge in the IoT. This session will review the current landscape for Identity considerations in the IoT space. It will discuss existing standards as well as the gaps to address to work toward broad market interoperability. The discussion will provide real world examples of challenges and opportunities for Identity in both the industrial and personal real of pervasive IoT. We invite you to join this interactive discussion of experts. Your takeaways from this session: • What are current challenges and opportunities for identity in the IoT? • What are the existing standards and existing gaps industry needs to address? • Is my organization ready for the digital identity IoT transformation? • What do I need to know today to take action? **Process Control, Production IT and Operational Technology - No Go Areas for IDM?** **Eleni Richter**, EnBW IDM usually covers classical office IT. IDM controls who is allowed to do things, who is responsible, who is inside and who stays outside. In areas of operational technologies (OT) and process control we find similar questions. This presentation will take a closer look at typical usecases and practical patterns in OT-Areas. • Motivation and starting point: Why should IDM cope with OT? When is the right time to get involved? • Decoupling, robustness and decentralization: Some considerations on aspects beyond office IT working hours. • Some organizational aspects: What are the main differences? • Some thoughts on future prospects and widely divergent aims: Office IT, Cloud, IoT, OT.
16:30-17:00	Coffee & Networking **Room: EXPO AREA**
17:00-18:00	**Adopting the New Thinking on Digital Risk** **Bringing it All Together – Distributed Strategy Solutions for Distributed Risk** **Dr. Karsten Kinast LL.M.**, KuppingerCole **Dr. Scott David, LL.M.**, KuppingerCole In evaluating distributed systems risk, the attention to data is misdirected. Rather it is the distributed nature of data management systems (and the increase in interaction volume) that increase the perception and actuality of risk. Distributed problems need distributed solutions. Applying the community of interest approach – how can your organization more effectively reduce and manage risk?
17:00-18:00	**Access Intelligence** **Access Intelligence, User Activity Monitoring, Recertification: What do we Really Need?** **Ramses Gallego**, Dell **Dr. Michael B. Jones**, Microsoft **Rainer Knorpp**, Devoteam **Thierry Winter**, Evidian Improve your level of compliance, gain up-to-date insight and reduce recertification workload. Add business risk scoring to your Access Governance Architecture, focus attention on high-risk access and extend your existing infrastructure to provide real-time access risk information. Re-think your existing Access Governance processes and understand upcoming IAM challenges and their impact on your infrastructure. This panel will discuss which approaches on redefining and extending existing approaches on Access Governance suit today's need best.
17:00-18:00	**Behavioral Analytics** **The Anthem Breach and how it could have been Avoided** **Dave Kearns**, KuppingerCole In January, Anthem Healthcare, the US's second-largest health insurer, reported that the personal records of as many as 80 million individuals were compromised. Many so-called "security gurus" quickly called out the company for two flaws that were felt to be the major causes of the breach. The gurus were wrong. Kuppinger-Cole analyst Dave Kearns will guide you through the most likely vector for the attack, why the gurus' recommendations wouldn't have stopped the attack and also tell you the two things that could have prevented this breach **Risk Based Realtime Security Through Behavioral Intelligence: Concepts and Market Maturity** **Martin Kuppinger**, KuppingerCole Behavioral Intelligence is simply taking the actions someone is performing and comparing them to previous actions. For example, keystroke biometrics - monitoring the way people enter data on a keyboard (such as a username/password combination) - is one example of Behavioral Intelligence used in a risk-based security system. This session will explore different methods of risk-based security using Behavioral Intelligence, where the market is today and what could be coming in the near future.

17:00-18:00	**Integration** **Mastering IoT Privacy and Security Risks Without Losing the Benefits of IoT** **Gershon Janssen**, OASIS Open Standards Group **Peter Niblett**, IBM **Jeff Stollman**, Secure Identity Consulting **Dirk Wahlefeld**, ITConcepts **Souheil Ben Yacoub**, Verisign Organizations, both commercial and non-commercial, are eager to explore the new opportunities afforded by the Internet of Things. Applications range from the apparently trivial, such as Internet-connected toothbrushes, all the way through to critical infrastructure such as power grids. The designers and operators of such solutions may not be aware of the risks that they are exposing themselves to, and lack the tools and processes to protect them properly. In this panel we will discuss: • the steps that an organization should take to identify risks, protect their assets and safeguard data, and then to detect, respond to and recover from attacks, and how cloud implementations can mitigate some of the risk inherent in operating an IoT solution. We will also also try to review the role that standards have to play and look at some of the security challenges that still remain. • Concrete IoT devices/research initiatives under development that illustrate the innovation and benefits expected with IoT technologies, and the challenges being addressed. • The challenges that follow from trying to securely integrate these devices together with each other and together with existing IT systems. • Concrete IoT devices/research initiatives under development that illustrate the innovation and benefits expected with IoT technologies, and the challenges being addressed.
18:00-18:30	Closing Keynote **Prof. Dr. Sachar Paulus**, Scientific Advisor, KuppingerCole **Room: AUDITORIUM**

Friday, 08.05.2015

08:30-10:00	Check-in & Registration **Room: COUNTER HOTEL**

09:00-12:30

Roles, Recertification, Access Governance: The Lean Approach

Matthias Reinwarth, KuppingerCole

Identity Management, Access Management and Access Governance are vital elements of an IT strategy laying the administrative foundation layer for achieving strategic goals. These goals include:

- The efficient management of user access to corporate resources and
- Evidence of compliance to legal and regulatory requirements, such as the Sarbanes-Oxley act or national data protection legislations.

Experience shows that currently implemented solutions and architectures for the management of corporate identities and their access to resources tend to be overly complex, require substantial manual efforts and lack flexibility.

But flexibility is key when organisations of all types face fundamental changes. And it is key especially for both of the above given goals when the only constant factor is change. This includes changing requirements resulting from changing markets, changing business models and product strategies, from changing legal and regulatory requirements and organisational changes from restructuring to mergers and acquisitions.

In this workshop we will look at changing and increasing requirements, diverse and sometimes contradicting strategies for shaping and assigning access rights while maintaining compliance to regulatory and legal requirements.

Swiftly assigning the right access to the right people gets more and more important, and empowering the users' expertise might be the decisive factor for agile companies succeeding against competitors. Next generation access management and access governance will most definitely look different from today's existing complex role designs with scheduled access recertification campaigns and provisioning cycles that taken days instead of instantaneous access when required and approved.

This workshop will illustrate that the role of access management and access government is currently shifting from being an "internal IT and administration thing" to becoming a vital component of an overall technology strategy providing an important operational foundation layer for modern businesses, while ensuring security and governance far beyond the requirements by regulators and legislation.

Attendees will learn about:

- Lean role design principles
- Attribute-based access control
- Complementing role design with access risk assessments
- The deployment of a sureccess automation and access analytics
- Strategies for leveraging organisational knowledge by empowering the user

To achieve this, the workshop will discuss current trends of developments in access management and governance while providing valuable information for deciding whether to transition towards leaner strategies.

Agenda

9:00 - 10:30

- **Access management, role design and Access Governance: Where we are and where to go**
  - Access Governance: Status Quo in different sectors (Financial Industry, Telcos and others
  - Requirements for a next generation access governance
    - Change as the new normal
    - From extended enterprise to the new ABC
    - Changing legal requirements
    - changing business requirements
    - changing markets
    - changing organizations
    - changing business models
    - Flexibility and agility

10:30-11:00 Coffee Break

11:00 - 12:30

  - **Understanding different role design approaches**
    - Complex, but comprehensive enterprise models
    - Or lean, pragmatic approaches
    - Risk and access criticality
    - Flexibility and agility vs. regulatory compliance
    - Full coverage vs. 80%
      - Access risk assessment as part of the role design process
      - Roles tend to be volatile,
        - Agile role lifecycle managmement
        - Reassess risk

13:30 - 14:30

    - **Context, risk and user empowerment**
      - Risk based access and dynamic authorization
      - Context based authorisation and authentication
      - Empowering the user
        - Self service access request
        - Re-Approval instead of Re-Certification

- Ask the expert: Approval by
  - Line Managers
  - System Owners
  - Risk management
- Attribute-based role assignments
- Automation and Analytics

14:30 - 15:00 Coffee Break

15:00 - 16:00

- **Best of all worlds: Getting „lean“, „pragmatic“ & „compliant“**
  - Gradual transitions
  - Hybrid designs
  - Quick wins
    - Improved security
    - Simplified compliance processes
    - Easy adjustment to changed requirements
    - Direct support for business requirements

09:00-12:30

Cloud Risk Assessment

Mike Small, KuppingerCole

When moving to the use of cloud service it is most important to take a risk based approach. However the process involved is often manual and time consuming; a tool is needed to enable a more rapid and consistent assessment of the risks involved.

This session describes why a risk based approach is needed. It provides detailed information on the KuppingerCole Cloud Rapid Risk Assessment Tool developed by KuppingerCole to help organizations assess the risks around their use of cloud services together in a rapid and repeatable manner.

After attending this session you will be able to:

- Explain why a risk based approach to the use of cloud services is needed.
- Explain the inherent risks that the KuppingerCole Cloud Rapid Risk Assessment Tool covers.
- Collect the information needed to use the tool.
- Describe the KuppingerCole Cloud Rapid Risk Assessment Tool.

Completion of this workshop qualifies for up to 3 Group Learning based CPEs

Who should attend?

This workshop is intended for the people in an organization that are concerned with procuring and assuring cloud services including:

- IT Governance/Compliance/Audit managers
- IT service managers
- IT risk/security managers
- Procurement and Legal managers
- Line of business managers considering cloud services

Detailed Workshop Program

Time	Content
09:00-10:30	**Introduction to KuppingerCole Cloud Rapid Risk Assessment Tool** • The different service and deployment models • The real risks of cloud computing • The best practices and controls that can make a difference
10:30-1100	**Break**
11:00-12:30	**Using the KuppingerCole Cloud Rapid Risk Assessment Tool** • Identifying the assets at risk • Collecting the information that you need • Identifying the risks that apply and their importance • Demonstration of the use of the tool

The KuppingerCole Cloud Rapid Risk Assessment Tool is intended to help organizations assess the risks around their use of cloud services and choose the controls that could mitigate these risks. The tool has a built in database which includes the most important risks in the use of a cloud service, together with their impact and probability. This provides a starting point that makes it easier for organizations to assess risk by building upon what exists rather than starting from scratch.

This tool uses information collected by the user to determine the relative risk of a specific cloud use case and deployment. The specified use case is evaluated through the use of a questionnaire which leads the user through the risks. Each risk can be included or excluded from consideration or given a priority. For the risks that are included the tool considers the assurances that are provided by the CSP and/or actions taken by the customer to mitigate each risk. These assurances are used to modify the impact or the probability of the inherent risk.

This workshop uses real life scenarios to demonstrate the use of the KuppingerCole Cloud Rapid Risk Assessment Tool to understand the risks of using a specific cloud service and to ensure that these risks are managed to meet the organization’s risk appetite while obtaining the required business benefits.

09:00-12:30	**Industry Focus Workshop: Insurance & Financial Services** **Prepare your Organization for the Digital Transformation: Enable the Agile, Connected Business** **Martin Kuppinger**, KuppingerCole **Wolfgang Rupprath**, FSP **Finding the balance between new business requirements and compliance & information security challenges** This workshop will focus on the fundamental changes organizations are facing these days. On one hand, there is business demand for connecting with business partners, customers, and mobile workforces in a far more flexible way than ever before. Cloud Computing is increasingly becoming a reality. The IoT will massively affect business models, with health information of customers or data from connected vehicles becoming available, leading to entirely new types of contracts. On the other hand, ever-tightening compliance regulations and the need for information security in a connected world are threatening. Finding the right balance and preparing your IT for being able to serve to the business requirements while meeting the compliance & information security challenges of this agile, connected business is key to success. While this workshop puts emphasis on the financial services and in particular insurance companies, the discussion will be valuable for attendees from other industries as well – all industries are facing the same challenges in the digital transformation of businesses. During this workshop, Wolfgang Rupprath from FSP will introduce the delegates into the "Bipro" called initiative for process standardization between companies in the Insurance sector. TGIC (Trusted German Insurance Cloud) is the technical business enabler. Together they build the backbone for an insurance industry wide process optimization possibility. As an example, for the “Bipro Authentication and Authorization” standard, the TGIC can serve as a Trust Center. The TGIC infrastructure can also be the means for a lot of new trusted (secure) (shared) cloud services. After attending this workshop you will be able to • Regoccnize and define the challenges of the digital transformation of businesses • Know Future-proof blueprints for Information Security • Define Processes and guidelines for Information Security in agile, connected businesses • Understand and measure the risk of cloud and on-premise IT services This workshop qualifies for 3 Group Learning based CPEs.
12:30-13:30	Lunch Break **Room: RESTAURANT**
13:30-16:00	**Roles, Recertification, Access Governance: The Lean Approach** **Matthias Reinwarth**, KuppingerCole
13:30-16:00	**Beyond your On-Premise IT: Privilege Management for Cloud, Virtualization, SDE, OT, and IoT** **Dave Kearns**, KuppingerCole **Edwin van der Wal**, Everett **Nathan Wenzler**, Thycotic Privilege Management for now has been primarily focused on the core IT infrastructure running on-premises. This is changing. While supporting the servers, applications, and client systems in your on-premise environment still is a major requirement, there is increasing demand for extended coverage. Managing privileged users in Cloud services on both the tenant and the service provider side is one challenge. Getting a grip at all layers of virtualized environments, from the host over the hypervisor to the guests is another. Managing the software-managed components in the upcoming Software-defined Environments (SDE) also creates new challenges for Privilege Management. OT (Operational Technology) with many types of specific systems that need to become better protected is a both interesting and challenging field for innovation in Privilege Management. And there also will be a need for managing privileged access to things in the IoT, for instance for managing patches and updates – here we are talking about massive scalability. This not only means that vendors have to drive innovation, but customers need to think about their future strategy for Privilege Management. In this workshop, the specific requirements imposed by these new challenges will be discussed, looking at feature areas such as scalability, support for new (and, in the case of OT, old) protocols and interfaces, etc. Based on this, the workshop will cover whether and how to extend the reach of on-premise, IT focused Privilege Management – or whether different solutions are the better choice. After attending this workshop you will be able to • Explain the difference between Simplified SignOn (SSO) and Privileged User Management • Identify the common cyber security Privileged Password mistakes • Implement individual audit tracking for shared accounts • Understand Privileged Password Management in the Cloud and how to build access barriers Completion of this workshop qualifies for up to 2 Group Learning based CPEs.

13:30-16:00	**Identity Mixer, uProve, Qiy Trust Framework, UMA: Providing Control to the Individual** **Ronny Bjones**, Microsoft **Joni Brennan**, Kantara Initiative **Dr. Maria Dubovitskaya**, IBM Research **Marcel van Galen**, Qiy Foundation **Bram Neuteboom**, Qiy Foundation **Daniel Raskin**, ForgeRock Securing access to personally identifiable information in a way that the individual that information is pointing to has full control, is one of the challenges in the era of digital transformation. In this workshop, we will do a deep-dive into the available and forthcoming standards, technologies and their implementation for what we call Life Management Platforms (LMPs), which combine personal data stores, personal cloud-based computing environments, and trust frameworks. LMPs allow individuals managing their daily life in a secure, privacy-aware, and device-independent way. In contrast to pure personal data stores, they support concepts, which allow interacting with other parties in a meaningful way without unveiling more data than necessary to lead the intended interaction to a success. Think about comparing offers for insurance contracts or think about pulling articles from various sites for the 'personalised newspaper' without unveiling the full list of current interests. After attending this workshop you will be able to • Give an Overview on existing standards and projects (Kantara UMA, Microsoft uProve, Qiy Trust Framework), their maturity and potentials • Describe Life Management Business Models and current implementations • Estimate Market Development in the coming 5 years This workshop qualifies for 2 Group Learning based CPEs.

Workshops

FIDO Alliance Update

04.05.2015 14:00-18:00
The FIDO Alliance Update Seminar will provide an understanding of where the FIDO Alliance stands in its effort to address online authentication problems — problems best exemplified by the weakness of passwords! Recent announcements by companies including Google and Microsoft have demonstrated that the FIDO Standards are becoming the way to address authentication.

At the Seminar we will explain the UAF 1.0 and U2F 1.0 FIDO Standards which were released in December. You will learn how they work and what they can do for you. We will also discuss how companies are approaching the deployment of FIDO-based authentication solutions. Questions answered will include:

- What will I have to do to deploy FIDO in my business?
- What will the effort be?
- How do I get started?

There will be demonstrations of FIDO Ready™ products. Come talk with the people who built them.

This seminar is designed to answer your questions about the FIDO Alliance. Come join us!

Agenda

Monday, 04.05.2015	
14:00-14:15	Welcome **Donal O'Shea**, FIDO Alliance
14:15-14:45	Catching up on the FIDO Alliance **Donal O'Shea**, FIDO Alliance
14:45-15:30	A UAF Primer **Rolf Lindemann**, Senior Director Products & Technology, Nok Nok Labs
15:30-16:00	Coffee and demonstrations
16:00-16:45	A U2F Primer **Alexei Czeskis**, Software Engineer, Google
16:45-17:30	Case Study: Experience in FIDO Deployment
17:30-17:45	Q & A
17:45-18:00	Closing remarks **Donal O'Shea**, FIDO Alliance

Speakers

Alexei Czeskis
Software Engineer
Google

Rolf Lindemann
Senior Director Products & Technology
Nok Nok Labs

Rolf Lindemann brings more than 15 years of experience in product management, R&D and operations from the IT security industry. He works for Nok Nok Labs, Inc. as Senior Director Products & Technology. Prior to Nok Nok Labs Rolf Lindemann worked as Senior Director Product Management in the user authentication group at Symantec where he was responsible for research and product strategy on device authentication in smart grids and mobile networks. Before Symantec's acquisition of TC...

Continuing Education Credits

Prerequisites: None
Advance Preparation: None
Learning Level: Intermediate
Field: Computer Science

After attending this seminar you will be able to:

- Understand the problem associated with passwords on the Internet
- Describe the objectives of the FIDO Alliance
- Understand where the FIDO Alliance is in the process of addressing the password problem
- Explain the benefits and risks arising from the new approach to authentication
- Describe the approaches needed to successfully deploy the FIDO solutions
- Describe how organizations have successfully and securely implemented these technologies

This block qualifies for up to 4 Group Learning based CPEs.

KuppingerCole is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing education on the National Registry of CPE Sponsors. State Boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry through its website: www.learningmarket.org

For more information regarding administrative policies such as complaint and refund, please contact Mr. Levent Kara at our office's telephone +49 211 23707710, email: lk@kuppingercole.com

OpenID Foundation Workshop

05.05.2015 09:00-13:00
This OpenID Foundation Workshop provides early insight and influence on important new online identity standards like the EIC Award-winning OpenID Connect. We will provide updates on the OpenID Connect Self Certification Test Suite and Mobile Profile Working Groups of OpenID Connect as well as other protocols in the pipeline like Account Chooser and Native Applications. Leading technology experts from Microsoft, Google, Ping Identity and others will update developments with these key protocols, review work group progress and discuss how they help meet enterprise business challenges.

- **OpenID Connect Self Certification and Registration** by Don Thibeau of the OpenID Foundation
- **OpenID Connect Conformance Testing** by Roland Hedberg of the Umea University of Sweden
- **OpenID Connect** by Co Chairs Mike Jones and Nat Sakimura of the NRI
- **Mobile Profile for OpenID Connect** by Chair Torsten Lodderstedt of Deutsche Telekom
- **Account Chooser** by TBD Google Identity Team and/or Pam Dingle of Ping Identity
- **"HEART" Health Relationship Trust Profiles of OpenID Connect and Related Specifications by Co-Chair Eve Maler of ForgeRock**
- **Native Applications Work Group** by Co Chair John Bradley of Ping Identity

Speakers

John Bradley
OpenID Foundation, Kantara

John Bradley is an Identity Management subject matter expert and IT professional with a diverse background. Mr. Bradley has over 15 years experience in the information technology and identity management field. Mr. Bradley advises Government Agencies and commercial organizations on the policy and technical requirements of Identity Management, Federated Identity, PKI and smart card solutions. He is also Chair of the Leadership council and a Member of the Board at Kantara. He is treasurer of...

Jörg Connotte
Project Manager
Deutsche Telekom AG

Jörg Connotte has been working in identity management at Deutsche Telekom for the last 5 years. As a technical expert he contributes Deutsche Telekom's experiences and ideas to cross operator initiatives like Mobile Connect. He is one of the editors in the OpenID Mobile Profile Working Group. At Deutsche Telekom he helps partners to integrate digitals services into the SSO infrastructure of Deutsche Telekom.

Pamela Dingle
Senior Technical Architect
Ping Identity

Pamela Dingle is a Senior Technical Architect within the Office of the CTO at Ping Identity. Pamela has a long history with Identity Management, working as an implementer and moving into architecture and strategy over 10 years of evolution of systems such as directories, application servers, web access management systems, provisioning, and now federation. Pamela is also on the board of directors of both the Information Card Foundation and the OpenID Foundation and runs the Pamela Project, an...

Roland Hedberg
Senior Researcher
ICT Services and System Development (ITS), Umeå University

Roland Hedberg has received one Master degree in Biology and Chemistry from Umeå University, Sweden and another in Mechanical Engineering from Luleå Technical University, Sweden. He is senior researcher at ICT Services and System Development (ITS), Umeå University, Sweden. His main research areas includes distribute authorisation and authentication service infrastructure and identity management. He is involved in three different subtasks within the GEANT3 project (Moonshot,...

Eve Maler
VP Innovation & Emerging Technology
ForgeRock

Eve Maler is a renowned strategist, innovator, and communicator on digital identity, access, security, and privacy, with particular focus on creating successful wide-scale ecosystems and fostering individual empowerment. Eve drives Identity Relationship Management innovation for the ForgeRock Open Identity Stack; she also directs ForgeRock's involvement in related industry standards, particularly for access control and privacy, to which end she leads the User-Managed...

Nat Sakimura
Senior Researcher
Nomura Research Institute

Nat Sakimura is the research lead on Digital Identity at Nomura Research Institute (NRI). He has been working on digital identity and privacy for the past decade. His main theme cosinstently has been to empower the people with the digital identity so that they can live happily and peacefully in the cyber space transacting and connecting whenever and wherever they want. To that end, he has been active in standardization sapces such as OASIS Open, OpenID Foundation, Kantara Initiative, and...

Don Thibeau
Executive Director

OpenID Foundation

Don is President and Chairman of the Open Identity Exchange (OIX) a non-profit organization of leaders from competing sectors, including enterprise, data services, telecommunications, consulting services, SaaS, banking, retail and government. OIX is helping to build solutions to roadblocks for online transactions and serving as a test bed for business, legal and governance policies in the emerging identity ecosystem. Don is also the Executive Director of the OpenID Foundation, where he...

Continuing Education Credits

Prerequisites: None
Advance Preparation: None
Learning Level: Intermediate
Field: Computer Science

After attending this session you will be able to:

- Describe the benefits of using the OpenID Connect technical test suite and technical components of the OpenID Connect Standard
- Explain the benefits arising from the self-certification and registration of the legal assurance of technical conformance to the OpenID Connect Standard
- Describe the general status of the OpenID Foundation standards development process and technical focus of active and chartered OpenID Foundation Work Groups
- Describe how organizations like Microsoft, Google, Paypal and others have implemented OpenID
- Connect and are working on future profiles and extensions

Completion of the workshop qualifies for 4 Group Learning based CPEs

KuppingerCole is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing education on the National Registry of CPE Sponsors. State Boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry through its website: www.learningmarket.org

For more information regarding administrative policies such as complaint and refund, please contact Mr. Levent Kara at our office's telephone +49 211 23707710, email: lk@kuppingercole.com

The Foundations of API Security and API Gateway Technology

05.05.2015 09:00-13:00
This workshop will explore API gateway technology. What it is, how it's applied today, the benefits of API gateway technology, and implementation examples.

As enterprise architectures become increasingly complex, organizations are challenged with creating a modern and secure infrastructure. In this workshop, you will learn how API gateway technology is a fundamental component to achieving business agility and information security.

Additional topics covered:

- How to modernize legacy and existing services
- Centralizing identity enforcement, including SAML and OAuth
- Modern access control strategies and best practices

Presentations will include sessions from industry leaders as well as an implementation showcase where attendees have the opportunity to participate in hands-on exercises.

This workshop is supported by Forum Systems.

Agenda

Tuesday, 05.05.2015	
09:00-10:00	How to Implement Multifactor Single Sign-On (SSO) **Dr. Dirk Krafzig**, CEO, SOAPARK
10:00-11:00	Foundations of API Security **Jason Macy**, CTO, Forum Systems
11:00-11:30	Coffee Break
11:30-12:30	Implementation Showcase **Jason Macy**, CTO, Forum Systems **Mamoon Yunus**, CEO, Forum Systems
12:30-13:00	Technical Round Table Discussion **Alexei Balaganski**, Senior Analyst, KuppingerCole **Dr. Dirk Krafzig**, CEO, SOAPARK **Jason Macy**, CTO, Forum Systems **Mamoon Yunus**, CEO, Forum Systems

Speakers

Alexei Balaganski
Senior Analyst
KuppingerCole

Alexei is an analyst with specific focus on cybersecurity. His deep technical understanding allows him to support customers even with complex architectural and security challenges. Previously he has served as KuppingerCole's CTO. After graduating with an MSc degree in Mathematics and Computer science he has worked in the IT industry for over 15 years. His experience includes software development, network administration and information security. Before joining KuppingerCole in 2007, he...

Dr. Dirk Krafzig
CEO
SOAPARK

Dr. Dirk Krafzig has over 20 years of experience in the IT industry and specializes in enterprise architecture management. As the CEO of SOAPARK and author of Enterprise SOA, Dr. Krafzig is considered a pioneer in the field of service oriented architecture (SOA).

Jason Macy
CTO
Forum Systems

Jason Macy is the Chief Technical Officer responsible for innovation and product strategy for global operations. Jason has been a leading visionary for enterprise architecture design and successful deployment API identity and security technology. With hundreds of deployments worldwide, Jason's unique ability to pragmatically solve complex, industry use cases and provide sustained engineering initiatives continues to forge the leadership role of Forum Systems product technology. Drawing...

Mamoon Yunus
CEO
Forum Systems

Mamoon Yunus is an industry-honored CEO and visionary in API, Cloud and XML-based technologies. As the founder of Forum Systems, Mamoon Yunus pioneered XML Security Gateways & Firewalls with the only granted patent for XML network appliances. He has spearheaded Forum's direction and strategy for eight generations of award-winning API, SOA and XML security products.

Continuing Education Credits

Prerequisites: None
Advance Preparation: None
Learning Level: Intermediate
Field: Computer Science

After attending this workshop, you will be able to:

- Describe the critical importance of APIs for business agility and information security
- Describe the foundations of API security and identity enforcement, including standards like SAML and OAuth
- Implement and publish APIs in compliance with modern access control strategies and best practices
- Draft a strategy for modernizing legacy and existing enterprise services

Completion of the workshop qualifies for 4 Group Learning based CPEs

KuppingerCole is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing education on the National Registry of CPE Sponsors. State Boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry through its website: www.learningmarket.org

For more information regarding administrative policies such as complaint and refund, please contact Mr. Levent Kara at our office's telephone +49 211 23707710, email: lk@kuppingercole.com

Kantara Workshop

05.05.2015 09:00-13:00
The Kantara Initiative annual EIC workshop will focus on the Kantara Initiative strategy for Connected Life & Access Management 2.0. Organizations of all types are faced with permanent change - in technology, markets, business models, and regulation. This continuously changing environment applies for organizations big and small, as well as local and global. Services that leverage identity and personal data are becoming pervasive and the identity data of people, organisations, applications and devices represents a user's digital DNA.

Kantara Initiative workshop presentations and panels will feature industry leaders discussing Identity Solutions that innovate around the context, consent, and access management across the world. This workshop will explore how Identity Relationship Management (IRM) concepts are transforming digital identity with a focus on innovations that enable high levels of user engagement with in both private and public sector.

Agenda

Tuesday, 05.05.2015	
09:00-09:15	Welcome **Robin Wilton**, Technical Outreach Director, Identity & Privacy, Internet Society
09:15-09:45	Kantara Overview - Bridge to Global Identity Market **Joni Brennan**, Executive Director, Kantara Initiative
09:45-10:15	The Laws of Relationships - Captuing Relationship Context in the Age of People, Entities, and Things **Andre Boysen**, Chief Identity Officer, SecureKey Technologies **Ian Glazer**, Senior Director, Identity, Salesforce **Mark Lizar**, Founder, SmartSpecies **Robin Wilton**, Technical Outreach Director, Identity & Privacy, Internet Society
10:15-10:45	Consent and Information Sharing - Minimum Viable Consent Receipt **Mark Lizar**, Founder, SmartSpecies
10:45-11:00	Coffee Break
11:00-11:30	User Managed Access Demo and Status Update **Dr. Maciej Machulak**, CEO, Cloud Identity Limited **Eve Maler**, VP Innovation & Emerging Technology, ForgeRock
11:30-12:10	eIDAS Progress on the Road to EU Identity Services Interoperability - An Update from the European Commission **Andrea Servida**, Head of Task Force "Legislation Team", European Commission
12:10-12:55	Identity Relationship Management - The Transformation of Identity Services **Victor Ake**, VP of Customer Innovation, ForgeRock **Andre Boysen**, Chief Identity Officer, SecureKey Technologies **Ingo Friese**, Project Manager, Deutsche Telekom AG **Michelle Waugh**, VP, CA Technologies **Robin Wilton**, Technical Outreach Director, Identity & Privacy, Internet Society
12:55-13:00	Closing Remarks **Robin Wilton**, Technical Outreach Director, Identity & Privacy, Internet Society

Speakers

Victor Ake
VP of Customer Innovation
ForgeRock

Victor is an Information Technology veteran with more than 27 years of experience in areas of Software Development, Security, Networking, Identity Management and Identity Relationship Management. He is one of the Co-Founders of ForgeRock and the VP of Customer Innovation at the CTO Office. In his role, Victor is in charge of promoting innovative solutions based on the ForgeRock Open Identity Platform. He has worked with several Fortune 100 companies around the globe, such as IBM, 3Com and...

Andre Boysen
Chief Identity Officer
SecureKey Technologies

Andre is responsible for positioning SecureKey's growth strategy, cultivating opportunities in new and existing markets, and promoting demand for the company's solutions globally. He serves as SecureKey's digital identity evangelist. Prior to joining SecureKey, Andre co-founded and served as chief technology officer of 724 Solutions Inc. Previously, he served as chief technology officer for Footprint Software and as chief executive officer for the company's Asia...

Joni Brennan
Executive Director
Kantara Initiative

Joni builds diplomatic and collaborative relationships within and across communities of interest. She participates in international organizations and industry standards committees including: OECD ITAC, ISOC, IEEE, OASIS SSTC, ISO SC27 WG5, and ITU-T SG17 Q6. She has served as the NSTIC / IDESG Trust Framework WG Chair. She has provided testimony regarding Trusted Identity and Access Management systems for the US ONC HITSP as well. Joni has helped drive and formalize strategic partnerships...

Ingo Friese
Project Manager
Deutsche Telekom AG

Ingo Friese is a research engineer and project manager at Deutsche Telekom AG . He has more than 10 years' experience in the field of in Identity Management, Next Generation Networks and IMS. Ingo has been engaged in several research- and strategic projects for Telekom Innovation Laboratories the central innovation unit of DT AG. Currently he is in charge for architecture and standardization in a machine-to-machine communication project with various pan-European partners. Ingo is...

Dr. Michael Garcia
Deputy Director
National Institute of Standards and Technology (NIST)

Mike is a PhD economist and Federal 100 award winning cybersecurity expert. He's currently serves at the National Institute of Standards and Technology implementing the National Strategy for Trusted Identities in Cyberspace, working to catalyze a marketplace of innovative online identity solutions through pilot programs, a private sector-led organization developing the Identity Ecosystem Framework, and early federal adoption of innovative technologies. Mike has...

Ian Glazer
Senior Director, Identity
Salesforce

Ian Glazer is the Senior Director for Identity, at Salesforce. His responsibilities include product strategy and identity standards work. Prior to that, he was a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner where he oversaw the entire team's research. Mr. Glazer is an industry veteran having worked in the identity space for over a decade. He is a member of the Management Council and Board of Directors for the US Identity Ecosystem...

Mark Lizar
Founder
SmartSpecies

Mark is the chief architect of the consent receipt specification, the Founder of Open Notice and the Co-Chair of the Consent & Information Sharing Work Group. Mark's focus is on engineering personal data transparency and control through consent management through his SmartSpecies.com consultancy firm in Canada as well as R&D in conjunction with an experiential technology firm called Drive Technologies in London.

Dr. Maciej Machulak
CEO
Cloud Identity Limited

Dr Maciej Machulak specializes in security, privacy and trust in the Cloud as well as in personal data management. He is the founder and CEO of Cloud Identity Limited where he works with his team on research and development of innovative identity management and privacy solutions that allow individuals to have better control over their personal information in the Cloud. As the lead architect and developer, he also advises companies during all stages of their projects and helps them adopt...

Eve Maler
VP Innovation & Emerging Technology
ForgeRock

Eve Maler is a renowned strategist, innovator, and communicator on digital identity, access, security, and privacy, with particular focus on creating successful wide-scale ecosystems and fostering individual empowerment. Eve drives Identity Relationship Management innovation for the ForgeRock Open Identity Stack; she also directs ForgeRock's involvement in related industry standards, particularly for access control and privacy, to which end she leads the User-Managed...

Andrea Servida
Head of Task Force "Legislation Team"
European Commission

He is Head of the Task Force "Legislation Team (eIDAS) in Directorate General 'Communication networks, content and technology' (DG CONNECT) of the European Commission. From 2006 to 2012, he was Deputy Head of the Unit "Internet; Network and Information Security" in DG INFSO where he co-managed the Unit and was in charge of defining and implementing the strategies and policies on network and information security, critical information infrastructure protection, electronic signature and...

Michelle Waugh
VP
CA Technologies

As Vice President of Security Solutions for CA Technologies, Michelle Waugh is responsible for go to market strategy, messaging and positioning, and marketing execution for CA's Identity and Access Management (IAM) security solutions, including on premise and SaaS offerings. In her leadership role, Michelle also represents CA on the Board of Trustees for Kantara Institute, and as a corporate member of the Cloud Security Alliance. She holds CISSP certification, and a Masters in...

Robin Wilton
Technical Outreach Director, Identity & Privacy
Internet Society

Robin Wilton brings 28 years of industry experience to the role of Technical Outreach Director for Identity and Privacy, in the Internet Society's Trust and Identity Initiatives group. Since 2001 he has specialised in digital identity, privacy and public policy, building a reputation as a thought leader, communicator and translator between different stakeholder


groups. Before joining the Internet Society Robin spent two years as a research analyst in Gartner's Identity and Privacy...

Continuing Education Credits

Prerequisites: None
Advance Preparation: None
Learning Level: Intermediate
Field: Computer Science

After attending this session you will be able to:

- Describe the key concepts of Identity Access Management services that leverage user- centric tools, context, and consent.
- Describe the strategic concepts of digital identity with in the Internet of Things for
- Operational Technology and Policy Development.
- Explain why Access Control is critical for the evolution of identity risk management
- Describe the approaches needed to successfully manage these risks
- Describe how organizations have successfully and securely implemented these technologies
- Explain how Access Control innovation enables user-engagement and market growth leveraging identity services

Completion of this workshop qualifies for 4 Group Learning based CPEs.

KuppingerCole is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing education on the National Registry of CPE Sponsors. State Boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry through its website: www.learningmarket.org

For more information regarding administrative policies such as complaint and refund, please contact Mr. Levent Kara at our office's telephone +49 211 23707710, email: lk@kuppingercole.com

Contextual Security Intelligence

05.05.2015 09:00-13:00
Behaviour-based approaches to detecting intrusions have recently gained importance and momentum as a complementary model to the purely knowledge based approach. Behavioural intrusion detection is based on the assumption, that intrusions regularly create deviations from the normal behaviour, which is defined by reference models. In permanently comparing network activity with the reference model, such deviations can be detected and used to create an alarm.

Using the behavioural context to detect intrusions is proposing an exciting side-effect: In permanently comparing network activity with reference models, it is possible to discover and learn previously unknown attack patterns and provide "intrusion intelligence".

In this workshop, KuppingerCole's Principal Analyst Martin Kuppinger will introduce you to the concept of Contextual Security Intelligence and describe the challenges you will have to master, like

- keeping false alarms low
- extending behavioural approaches beyond vulnerability-attacks to the area of privilege misuse
- keeping your reference model up-to-date with changing behaviours
- avoiding privacy concerns

and then will hand over to Dr. Csaba Krasznay and Péter Gyöngyösi from BalaBit, who will give you a deep and intense overview on state-of-the-art Contextual Security Intelligence, divided into the core areas of

- Privileged Activity Monitoring and
- User Behavioural Analysis

Agenda

Tuesday, 05.05.2015	
09:00-09:15	Welcome **Martin Kuppinger**, Principal Analyst, KuppingerCole
09:15-10:45	Introduction to Contextual Security Intelligence **Martin Kuppinger**, Principal Analyst, KuppingerCole
10:45-11:00	Coffee Break
11:00-13:00	Deep dive into Contextual Security Intelligence **Péter Gyöngyösi**, Product Manager, BalaBit **Dr. Csaba Krasznay**, Product Manager, BalaBit

Speakers

Péter Gyöngyösi
Product Manager
BalaBit

Péter Gyöngyösi is the product manager of Blindspotter, a user behavior analytics solution developed by BalaBit, the creators of syslog-ng. His main duty is to create a vision and strategy and making sure it is followed. He is responsible for coordinating marketing, sales, support and development efforts and act as a product owner towards the teams in the development. Before switching to Blindspotter, he was responsible for the syslog-ng product line of BalaBit for over two...

Dr. Csaba Krasznay
Product Manager
BalaBit

Dr. Csaba Krasznay received his MSc in 2003 in electrical engineering at Budapest University of Technology and Economics. He works for BalaBit as a Product Manager. He is responsible for the vision and product strategy of BalaBit's Shell Control Box (SCB). He is the member of board at Magyary E-government Association and Voluntary Cyberdefence Coalition. He received his PhD at National University of Public Service, where he’s assistant professor, and his research topic is the security...

Continuing Education Credits

Prerequisites: None
Advance Preparation: None
Learning Level: Intermediate
Field: Computer Science

After attending this workshop you will be able to:

- Describe the concept of contextual security intelligence
- Explain how behavior-based approaches can detect intrusions
- Describe reference models for behavior and how to identify deviations
- Explain how to calibrate a reference model to your organization

This block qualifies for up to 4 Group Learning based CPEs.

KuppingerCole is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing education on the National Registry of CPE Sponsors. State Boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry

through its website: www.learningmarket.org

For more information regarding administrative policies such as complaint and refund, please contact Mr. Levent Kara at our office's telephone +49 211 23707710, email: lk@kuppingercole.com