TRUST IN THE DIGITAL WORLD 2014

Enabling the economics of trust

Executive Summary

7-8 April 2014
Vienna, Austria

EEMA and Trust in the Digital World 2014
Enabling the Economics of Trust
7- 8 April 2014 in Vienna, Austria

Executive Summary

Speaker presentations available to download from www.eema.org

Opening Plenary
The Austrian Federal Economic Chambers (WKO) was the proud host of the second annual Trust In The Digital World. at its headquarters in Vienna, it was the privilege of the event organisers, Chairman of EEMA, David Goodman and Chairman of TDL, Amardeo Sarma, to be joined by Professor Hans-Jürgen Pollirer from the Chamber to welcome the large number of delegates to the city of Vienna.

David Goodman commented that: "It is important that Trust In The Digital World provides a forum to have this debate between industry, government, policy-makers and knowledge institutes operating throughout the EU."

In the first keynote address Dr. Zoran Stančič, Deputy Director-General in the European Commission, DG CONNECT, explained how the digital world will only flourish if citizens have trust. He commented how Vice President of the European Commission, Neelie Kroes, had commented on the Snowden revelations by stating "It is for us a wakeup call." Mr Stančič added that whilst the European Parliament voted on 13th March to adopt the Network & Information Security (NIS) Directive, progress was not happening fast enough and he encouraged delegates to get involved and help to shape EU policy.

Martin Sprengseis, the COO of Bluesource, used his keynote to give a perspective on behalf of small and medium sized businesses discussing the rise of smart devices and the challenges of building a safe framework that will enable the economics of trust.

Plenary Panel - The Economics of Trust: Track 1
Chair: Stefan Bumerl – Managing Director, Cryptas

Stefan Bumerl raised the challenge of establishing citizen trust. Konrad Walser, FH Bern, presented results of a survey (eGov Monitor D21 2013) which he suggested indicates a general lack of trust in public administration.

Josef **Weidenholzer,** MEP, added that lack of trust is also present in the private sector. He went on to explain the 2012 proposal for a move from EU directive to regulation for data protection and tabling the idea of fines (5% of annual company turnover) for organisations that are involved in a serious breach of data protection. This was dismissed by Markus Schuller of Panthera Solutions who suggested that if the gains were big enough for the business then they would factor in the fine as a cost and digest it. Mr Schuller said that independent regulation combined with strict anti-trust law and giving all involved 'skin in the game' would present a solution. Moving away from technology challenges, Kreshnik Musaraj from Thales talked about the human attitudes to trustworthiness needs to be considered, commenting that trust is invisible and that it needs to be earned and deserved.

Building Trust in the Cloud: Track 2
Panel Chair: Dr. Sheikh M. Habib, CASED

One of the fundamental bases for acceptance of cloud computing services is trust. When computations are carried out in the cloud one must ensure the correctness of results or verify service performance or security assurances as agreed with service providers. In recent years, academia and industry came up with innovative techniques to build trust on cloud computing services. Likewise, government and standard bodies came up with best practice guides to adopt trustworthy cloud services. This track brought experts from academia, industry, government agencies and standard bodies to share their perspective towards building trustworthy cloud computing ecosystem.

Dr. Sheikh M. Habib, a senior researcher of CASED/TU Darmstadt, started with questions for the panellists.

1. Can/do users trust cloud providers?
2. Can/do cloud providers trust users?
3. Can/do the cloud components trust each other?

Alfred Bach, a Solution Architect of CA Technologies presented a case study about successful cloud integration in the context of identity management. The case study demonstrated the usage of advanced security technologies to develop a trustworthy MoneySend service for MasterCard. Ronny Bjones, Director of Cloud Identity & Privacy services from Microsoft mentioned the protection of confidential data as well as tracking behavioural patterns of the users as major privacy threats towards trustworthy cloud environments.

Professor Udo Helmbrecht, Executive Director of ENISA, emphasised the adoption of open standards and interoperability among cloud providers towards building trustworthy cloud ecosystem. Dr. Tobias Höllwarth, Vice-Chairman of EuroCloud. Apart from standards, he further emphasized the importance of transparent security audits and certification of cloud services to establish trusted relationships between users and cloud providers. Professor Stefan Katzenbeisser, represented CASED/TU Darmstadt brought forward the urgency of deploying practical security solutions to preserve privacy during data processing in the cloud. He thinks these solutions will act as a trust enabler in cloud environments.

Dr. Claire Vishik, Trust & Security Technology & Policy Manager of Intel Corporation pointed out the gaps in the current trust implementations and discussed future research priorities towards a trustworthy cloud ecosystem.

Identity Management: Track 3
Chair: Ahmad Sabouri, Scientific Researcher, Goethe University Frankfurt

The ABC4Trust Project offered a panel featuring a variety of current applications of Privacy-ABC. The panel demonstrated that usable and trustworthy identity management systems are technically possible and in several cases already a working reality. Presentations covered were:

- General technology presentation of ABCs in ABC4Trust (Dr. Gregory Neven, IBM)
- Privacy respecting ICT innovations in education: electronic course evaluations in higher education and beyond (Prof. Yannis Stamatiou, Computer Technology Institute and Press)
- Restrictive download of documents from cloud storage in FI-Ware (Robert Seidl, Nokia Solutions and Networks)
- Performance of privacy-enhancing cryptography on smartphones (Dr. Jan Hajny, Brno University of Technology)
- Information security supporting data protection (Dr. Rodica Tirtea, ENISA)

Major questions and discussions in the panel:

- What would be some interesting examples of Privacy-ABCs applications?
  Apart from the pilots of ABC4Trust that deal with privacy-friendly online course evaluation and privacy-friendly school community platform, one could consider e-government polls, age verification and public transportation ticketing to be very relevant problems that can be addressed using Privacy-ABCs.
- There are so many cryptographic solutions to deal with privacy problems. Why use ABC4Trust framework and not any other one?
  ABC4Trust framework is defined in a generic way based on the identified features that are required from Privacy-ABCs. Therefore, it gives the opportunity to any crypto provider to implement the specified interfaces and therefore be pluggable to the framework. ABC4Trust is not limited to any specific technology and it also helps to avoid a lock-in situation.
- One of the major blocking factors in front of adoption of Privacy-ABCs concerns the application developers not being familiar with the crypto. What can be done in this regard?
  The ABC4Trust project has provided a crypto-agnostic API set to Privacy-ACBs, which relieves the burden of complicated crypto. The reference implementation of ABC4Trust is publicly available on Github along with documentations and integration examples for the developers.

Cyber Security Standardisation Session: Track 4
Panel Chair: Demosthenes Ikonomou, Head-Information Security & Data Protection, ENISA Cybersecurity

The objective of the session on 'Cyber Security Standardisation' was to discuss the current situation and future of standardisation in the area of Network and Information Security. The session composed of initiatives in the research community, industry and public sector. Over the last 2 years a number of initiatives have taken place at the level of International Standardisation Organisations (ISO) with the main aim of putting forward proposals concerning the

future of standardisation initiatives in NIS. The most notable example of such an initiative is the ETSI CEN CENELEC Cyber Security Coordination Group (CSCG) www.cencenelec.eu
http://docbox.etsi.org

At the same time, a number of similar initiatives promoting the creation of cyber security standardisation initiatives in the EU aimed at the introduction and adoption of standardised technological solutions in the market place: - ETSI has recently announced the launch of a new technical committee on Cybersecurity to address the growing demands for standards in this field
http://www.etsi.org/

The EP is setting standardisation of NIS products among the priorities at EU level (for example http://www.europarl.europa.eu/)
- Similar initiatives are called upon by the European Commission in its proposal for a Cyber Security Strategy for the EU (http://ec.europa.eu).

Against this background, this session discussed the possible future of NIS standardisation and the actions required in order to materialise such high level policy objectives that can be taken by the various sector actors including the EU funded R&D programs (e.g. H2020), the private and public sector (for example public sector procurements are mentioned as a possible instrument to promote standardised technology solutions) as well as other instruments such as certification.

Building up an Eco-system: Tack 5
Chair: **Stefan Bumerl** - *Chairman Austrian Identity Federation Authority*
Ecosystems are complex constructions and require lots of players to drive competition. How can you start one for eID?

SMART CITIES: Track 6
Panel Chair: Prof Dr. Max Muhlhauser, Technische Universitat Darmstadt

Prof Dr. Max Muhlhauser discussed the challenges and opportunities of ICT-related trust that are – or may be – specific to the upcoming smart cities initiatives.
ICT was clarified to refer to two different aspects: **"Trusted ICT"** i.e. dependable/secure/resilient/fault-tolerant/tamper-proof ICT, is often defined as "ICT that works as expected"; it was clarified that this term is misleading in the sense that 100% is an illusion: ICT systems that are said to deliver 24/7 availability still have a small residual failure probability.

"Computational trust", on the contrary, refers to ICT-based means (models, software) for assessing and conveying trust in people, organizations, (digital and physical) products and services, etc. Computational trust emphasizes the probabilistic nature of trust that is insufficiently reflected in the "trusted ICT" realm.

Smart Cities were defined according to three characteristics:
1. Cyber physical systems (CPS) are established and leveraged that link the 'cyber world' of software that models & controls a city in real time to the 'physical world' of the city's
2. This leverage provides improvements. economy, environment, and/or quality-of-life
3. Corresponding services, (cyber physical) social networks, processes, and data are provided to the stakeholders – from municipal authorities and personnel to utility companies, citizens, and the private sector.

Issues were identified at the "seam" of trust-in-digital-life and smart cities: Trust in data quality: Trust in operation resilience: Trust in service liability: 4.Trust in community reputation

Prof. Dr. A Min Tjoa, Vienna University of Technology, emphasized smart cities as cities that entail both
a) the application of existing technologies in new ways and
b) the development and application of new technologies, including sensor, communication and analytical technologies and design solutions to urban infrastructure such as energy, water and transport systems.

Prof Tjoa identified only six top level categories: Information, Water Cycle, Energy, Matter Cycle, Mobility, and Nature (Streets, Gardening, Parks, Agriculture, Forest).

Prof. Spiekermann, Vienna University of Economics and Business, asserted that trust is a phenomenon of reliance on the good intentions and/or adequate competences of others in situations characterized by dependence, vulnerability and risk. Her view was that trust is an important element of an ethical view on ICT in a humane world, which should abandon the "dumbest assumable user " view of customers and users, and the trend towards a "cyborg" view.

Dr. Volkmar Lotz, Senior Researcher at SAP, presented the TDL consortium, discussing a paradigm shift from trust as an impediment (cost factor, hindrance) to trust as an asset (value, business case). He explained the ICT price levels, preparedness-to-pay (for trustworthy ICT), net user value for trustworthy ICT, all under the influence of the incidents becoming transparent to the stakeholders.

Dr. Lotz related these issues to the panel topic in two ways. Major relationships between trust and smart cities: Pervasive and ubiquitous ICT (CPS, sensors, …)

- Interconnected domains and critical infrastructures
- Smart Cities domain impacts personal environment and life
- Extended attack surface with high exposure
- Complexity, both technical and organisational
- Multiple stakeholders with different intentions
- Strong privacy impact (surveillance, profiling, correlating information, …)
- High risk (and, more important, risk perception) requires high level of trust

Secondly, he put up corresponding enablers for a paradigm shift (items 2, 3, and 4)

1. Awareness and transparency of incidents, business models and behaviour
2. Perceived user's need for trustworthy ICT
3. Realise security and privacy as business enabler
4. Willingness to pay for trustworthy ICT solutions
5. Regulations enforcing privacy and security by design

Mr Jurgen Imhoff, Senior Business Architect at Microsoft, stated the megatrends drive the smart cities movements: (mega) cities will represent 70% of the world's population by 2050, 80% of the global GDP, and up to 80% of the world's energy consumption.

Mr Hugo Kerschot reported on an ongoing project called ECIM: European cloud marketplace for intelligent mobility, *trust factor in a smart cities service environment.* By this, he perfectly responded to the quest for foci on vertical markets and applications brought forward by Mr Imhoff. He also backed the hope for a 'competitive' federation of different vendors, even for applications that make heavy use of customer data – one of the most valuable vendor assets. He showed the ECIM architecture and four-step user level process applied for a unified access to all integrated mobility services. Mr Kerschot put up the quest for The Smart City as a secure and trusted innovation PLATFORM with the ability to create and use a range of services.

eAuthentication: Track 7
Chair: **Milan Petkovic,** *Philips*
Provided insights into how to address the problems associated with eAuthentication

eIdentity Session: Track 8
Panel Chair: Robert Garskamp, Identity .Next

Robert Garskamp gave an insight into the important role of digital identity in the world of security and trust, with a special focus on the central role government within Europe. Governments would like to be in control and provide public and private digital identities. Some governments choose to seize identity, others to radically defer it to the

market, while any scenario has to deal with the citizen's own demand for control, usability and interoperability within ONE Europe.

Christian Rupp shared his story about the use of an easy, secure and free eID in Austria and cross border. As spokesperson for the Federal Platform "Digital: Austria", which coordinates the ICT and eGovernment activities for the Austrian Government, within and outside the Republic of Austria, he stated that the usage of eID will become more important and that would improve cross border access of citizens and businesses to public services in Europe Europe by provision of interoperable IT solutions.

Rainer Hoerbe (independent federated identity management consultant and contributor of Kantara initiative and OASIS) explained that a high level of interoperability is required between governments within ONE Europe to embrace federated identity management. Based on policy framework it is possible to deliver 4 levels of assurance for every citizen. The claim is to standardise on the level of controls, and allow particular federations to customise policies while maintaining a high level of interoperability.

Founder and CEO of Miicard, James Varge, gave his insight about the value of digital identity from a commercial perspective. James sees the digital identity as information that uniquely describes a person or even a thing and contains information about the subject's relationships, where it is evident that the consumer/citizen must be empowered and not the business. He also states that the higher the assurance, the higher the value of the identity will be because when there is more value for the business, there is more reason for the market to adopt this. Christian closed the panel discussion with the fact that eGovernment is a journey and not a destination. And the government should support the European citizen by creating the ecosystem that fulfils the needs. Something that was fully agreed by the attendees of this session.

Regulation & Legal Aspects: Track 9
Chair: Dr. Jörg Hladjk, *Hunton & Williams*
This panel looked at the developing EU legal frameworks for cyber security, data protection and cloud computing and shared their views on the challenges these new frameworks bring and focused on the business impact

Governance, Trust and Security: Track 10
Panel Chair: Martin Muhleck , Trust & Security Unit, European Commission

Following the Snowden revelations, there are occasional reports in the specialist press that as a result business opportunities for ICT security and privacy enterprises in Europe are on the rise, in particular for start-ups and SMEs, to develop new innovative products and to have stronger business cases than previously.

The panel discussed the current gap between scientific excellence and innovative & competitive products on the market and what needs to be done to support enterprises to bridge this gap.
Professor Bart Preneel from University Leuven said that while there are some security companies based in Europe, the majority are in the US and Governments often fall behind. In particular the long time frame of European projects does not contribute to address the current research and innovation challenges.

Christian Polster, chief strategy officer at Radar-Services and James Vargas from MiiCard presented their experiences from an SME/Start-up point of view. Ronny Bjornes from Microsoft Trusted Cloud Computing underlined the innovation opportunities offered by the cloud for SMEs. Professor Reinhardt Posch, CIO for the Austrian federal government, highlighted the main seven challenges for fostering innovation in Europe.

TDL Sprint Winners Presentation

TDL announced Trustseed SAS France as the winner of its prestigious SPRINT award, which validates new, innovative and trustworthy ICT in very short project cycles of three months. The company received €25,0000 for its work in the field of legal digital signatures and the implementation of the SPRINT. By linking its online e-signature solution with

the Microsoft e-authentication platform, Trustseed creates a connection between e-authentication, e-signature and e-validation.

Towards Defining Priorities for Cybersecurity Research in Horizon 2020s Work Programme 2016-17
Panel Chair: Raúl Riesco Granadino, INTECO: Track 11

The Chair introduced the cybersecurity research framework, including the EU Cybersecurity strategy, the NIS Directive and the creation of the NIS public private platform with 3 different work groups for risk management, information sharing and especially the WG3 for Secure ICT Research & Innovation.
Martin Mueleck (European Commission) described the H2020 approach and the relationship with NIS results for 2016-2017. He explained the key pillars and what has changed in cybersecurity research and the differences and objectives of Societal Challenges, LEIT and Excellence approaches and emphasised industry, business cases and stakeholder involvement.

Evangelos Markatos (Crete University) described the first deliverable of WG3 which is Secure ICT landscape. He described the expected results by using an example on IDS (Intrusion detection systems) and showed a presentation describing what is considered the most relevant section of the deliverable, the research challenges.

Aljosa Pasic (ATOS) described the deliverable of WG3 named Business Cases and Innovation Paths. He used examples of a specific case (Secure SW) based on NESSOS initiative. He helped the audience to understand that the NIS platform is willing to help the adoption of research into business cases for profit.

Gisela Meister (G&D) described the first of the areas of interest - individual layer, part of the SRA deliverable (Strategic Research Agenda). She described the vision, as well as the enablers/inhibitors standard approach that all AoI's are following for a posterior cross revision for priorization. She showed that apart from technological aspects, Economical, Societal and Education, are all important for success.

Volkmar Lotz (SAP) described the second AoI - collective layer perspective, part of SRA. He clarified the vision and why it is so important to analyze the future through this layer as lots of efficiencies or security services would be possible under a collective approach. He also clarified with real examples, different enablers and inhibitors, where again, other areas other than technical, are so important, like education.

Steffen Wendzel (Fraunhofer) described the last layer, the Trustworthly (hyper connected) Infrastructures layer. He used some examples and made a special effort to be more visionary. He also explained specific challenges identified in terms of adaptive & resilience infrastructures and the need to link with FP7 results.

Q. How can we help SMEs to engage in cybersecurity research engagement?
A. Panel members discussed options like Services API ecosystem availability, also SMEs can re-use infrastructure for new services, H2020 simplification approach ready for a better engagement, etc.

Q. How to promote the transfer of technology for the creation of new products/services and companies/start-ups.
A. Different options were discussed like ICT clusters (eg. Germany), Private investments and also seed capital.

Chair commented on the hard job behind being done on the business model behind the research, the cross analysis phase that could help to define priorities inside the SRA, the several types of enablers & inhibitors, different from technological point of view, as well as the challenge WG3, which has to be more visionary.

Trusted Personal Data Management: Track 12
Chair: Jacques Bus (Digital Enlightenment Forum)

- Personal Data Management - State of Affairs *Jacques Bus (DEF, BE)*
- Ethical Personal Data Management - *Luk Vervenne (Synergetics, BE)*
- Electronic Identification, Privacy and Trust in eGovernment Services: the e-SENS Project - *Lefteris Leontaridis*
- Privacy laws and pervasive sensing /big data: forever incommensurate? *Prof Max Mühlhaüser, Un Darmstadt, DE*

Jacques Bus gave a short introduction to Digital Enlightenment Forum (see www.digitalenlightenment.org **)** which is associated with TDL. Then he introduced the subject with some descriptions of his use of relevant concepts: (1) *Identity*: total of "body and soul", behavior, presentation, knowledge, … of an individual (more than data); (2) *Privacy:* being free from unreasonable constraints on the construction of the own identity in the Digital Society; (3) *(Context-dependent) PDM:* enables individual to control access and use of her PD in a way that preserves privacy, (and depends on the context of the transaction). He emphasised the distinction between actively and passively collected data and the latter with or without knowledge of the subject or data inferred from big data analysis.
He ended with explaining the principle of Trust Networks (TN) as part of an infrastructure for PDM which allow the subject to control use of PD in transactions with trusted services in a certain context (e.g. health, loyalty cards use).

Luk Vervenne (Synergetics) further detailed how his company offers TN infrastructure that gives the user of services reasonable certainty about how his PD is being used. Compliance of SPs with the rules of the TN, as well as additional rules set by the user is assured by technology random tests, audits and trusted governance. Services can use all types of data and policy are partly agreed at TN level, and can partly be set by the user.
The infrastructure includes interoperable interfaces with external TTPs (eg for authentication, storage provision, reputation) as well as the various networked services (SPs) through an API portal, which allows for building a broad ecosystem of community-based TNs, TTPs and SPs.

Lefteris Leontarides (e-SENS) presented the e-SENS project which focuses on developing an interoperable infrastructure for public administration services. It builds upon the projects: STORK (cross-border identification), e-CODEX (support of the Justice process), PEPPOL (e- procurement), EPSOS (Healthcare data and services) and SPOCS (support of government administrations to the business life cycle). Important challenges for public administration are related to minimal data use and purpose binding when collecting data and trust building in various areas, including the handling and linking of sensitive data. Interoperability at the European scale creates many challenges for identification (attribute-based?), dynamic (context-dependent) consent, and delivery of sensitive data. In addition the changing scene raises problems of stakeholder-driven government, trust and awareness.

Max Mühlhäuser (Techn Univ Darmstadt) presented the legal Privacy protection rights – i.p. the right to fair processing for specified purposes and based on consent. He showed how the principles of Big Data collection – collect more data and don't throw any data away – is fully incompatible with these rights. The two main concepts used to implement privacy protection are anonymization and data thrift. However, anonymized storage is essentially impossible in a fool proof way. The collection of ubiquitous sensor data which is considered generally not PII and for which consent is often impossible makes anonymisation a myth. The challenge is a shift from data protection in storage to data protection in use. One (debatable) solution would be a trusted data store with a well-controlled interface including contextual rules.

The discussion focussed on how such trusted data storage could be organised in a way that could address the upcoming liability under the new DPR operational, and proper data management, linking and exchange, in particular in government administrations could be organised.

Privacy: Track 13
Panel Chair: Bart Preneel, Professor, KU Leuven

Claudia Diaz (COSIC, KU Leuven) started by discussing transparency tools that expose privacy-related practice on the Internet. She discussed device/browser fingerprinting; unlike cookies, these techniques are hard to detect and block by users and described the TOR system for anonymous routing (in contrast to many other security and privacy systems, TOR seems to be hard to break in a large scale even for NSA); she presented an overview of the research challenges related to anonymous routing. Finally, she discussed the relation between different privacy concepts and

technology; privacy is a broadly used umbrella term that covers mass surveillance, social privacy (undesirable leakage of information through on-line social networks), and data protection.

Reza Shokri (Dept. of Computer Science, ETHZ) discussed fundamental problems in computational location privacy. From the Snowden data we know that NSA has location tracking problems such as Co-Traveler and HappyFoot that can deliver a large amount of contextual information. The speaker discussed computational aspects to privacy, this involves two aspects: quantifying privacy and means to protect privacy. One approach is to deliver location-based services in a privacy-friendly way using cryptographic techniques (e.g. PIR or Private Information Retrieval); however, it seems unlikely that service providers would switch to this approach.

An alternative is user centric: a user could try to cover her tracks: removing identifiable data or obfuscating a trace (e.g. by increasing the granularity). One can then consider the questions how location privacy can be quantified and which information can be obtained from an inference attack; this problem can be studied using statistical inference. A natural question is how to define the optimal obfuscation strategy for a user for a fixed utility level. This is a complex problem as the adversary is adaptive, a game-theoretic approach is necessary, resulting in an interactive mechanism.

Ronny Bjones pointed out that these methods do not protect against the mobile network operator and mentioned that his research focuses on the app ecosystem that builds on location information; mobile network operators know the user's location but they are bound by contractual agreement. In principle one could build a mobile network in which the operator does not know where its users are, but this would be highly inefficient.

Ronny Bjones (Director of Cloud Identity & Privacy Services, Microsoft) gave a presentation on building privacy in the cloud. He discussed the threat of privacy from profiling through correlation, e.g. by the Facebook Like button. Next he presented the role of a broker in an identity federation protocol and looked at the question on how privacy could be provided; most of those brokers use persistent session identifiers; web servers also need to keep state across a transaction through a session identifier in the browser as the web itself is stateless . The proposed approach is to pass assertions through on orchestrator that separates the domain of identity provider and service provider. However, this approach does not protect against colluding identity and service provider. For this case privacy attribute-based credentials (PKI on steroids) can be used. The content of his talk can be found at http://blog.beejones.net/the-identity-fideration-do-not-track-pattern, http://blog.beejones.net/privacy-attribute-based-credentials, and the ABC4Trust project website.

Quick wins can be made in user awareness, although there was some reservation to which extent users can be convinced to take action – perhaps regulation is required. A second element is broader use of existing tools such as secure network connections, secure email and TOR.

Achieving the Trust Paradigm Shift : Track 14
Chair: **Milan Petkovic**, *Philips*
An EU project to contribute to trustworthy ICT solutions. The project approach, the design of a test bed architecture with its building blocks and a concrete case was presented and discussed.

eHealth Session: Track 16
Panel Chair: Georg Aumayr, Head of R & D, Johanniter

Georg Aumayr was talking about identity construction and destruction in eHealth environment. This produced a socio-theoretical foundation for Mario Drobics presentation about eHealth and its trustworthiness. Mario Drobics specified eHealth applications in the cloud and the worth of IHE as a framework is a way to provide a trusted system. One of the great challenges within this topic is how to bring an understanding of the system to the user to make real trust possible.

Kerstin Zimmermann presented the special use case of Ambient Assisted Living (AAL) as a model for trusted eHealth Systems from a research perspective. The idea of innovation with an ethical perspective as a foundation for eHealth solutions was stated as a necessary factor for funding actions. Within AAL, ethics has become a primary aspect for funding decisions. Also the end user involvement has to be part of each design and development. By talking about end user driven innovation, a major spin has come to the normal, technical approach.

Marianna Rissetto presented the benefits of strong identification instruments for trusted Systems. Especially the idea of using handscan systems. By using infrared sensors an image of vessels in the palm of the user is identified and grants access to data or features of the distinct system.
Finally, Georg Aumayr demonstrated the user perspective of eID and personal data to the audience with a short experiment. After each participant wrote his or her telephone number on a piece of paper, he gathered them all and picked by chance one of these numbers to call. So the depersonalized number becomes personal data again. Actually he didn't call the number but stopped there to ask the audience how they feel now and how they would feel if this was a setting outside this conference and with business options involved.

The New Attacker Model: Track 17
Panel Chair: Ghassan Karame, Senior Researcher, NEC

2013 witnessed the introduction of a novel, and extremely powerful attacker model. Notably, the world became aware of one of the biggest attacks on data privacy and confidentiality when news claimed details of a massive surveillance program which mined data from social networks, and Internet Service Providers (ISPs). This surveillance program was apparently not hindered by the various security countermeasures deployed within the targeted services.

The new attacker model was discussed and the panel explored possible avenues to enhance user privacy in the presence of such a powerful attacker. This panel was chaired by Dr. Ghassan Karame from NEC Laboratories in Europe, and comprised of the following members: Prof. Dr. Srdjan Capkun (Associate Professor, ETH Zurich), Dr. Kazue Sako (Innovation Producer, NEC), Stefan Roehrich (IT Security Specialist, Rhode & Schwarz), and Dr. Jorge-Lopez Hernandez-Ardieta (Head of Cybersecurity Research at Indra).

Prof. Dr. Capkun presented a number of threats against existing wireless technology, such as GPS spoofing attacks, cellular network eavesdropping, and attacks on medical implants. Prof. Dr. Capkun remarked that these systems can be easily attacked using available off-the-shelf low cost technology. Dr. Kazue discussed how the Japanese society perceives global surveillance programs and motivated for the notion of "personal clouds" as an effective solution to create a safer cloud which empowers users with the rights to decide on their privacy and data sharing policies. Mr. Roehrich discussed insights into the new attacker model and argued for the need of serious evaluation of the security products and cryptographic measures that we are using nowadays. Dr. Hernandez-Ardieta concluded with a discussion on possible ways to counter global surveillance. These included the reliance on European-only products and infrastructures, the establishment of large-scale international cooperation to share threats, and the need for staff training to be aware of such threats.

The panel chair asked all panel members to comment on whether our societies are equipped to counter such a global and powerful attacker model. Most panel members were reserved and pessimistic about the existence of a technology which can thwart such global attacks. The panel however, concluded on a positive note, urging all researchers and industrial partners to consider deploying existing security technology and conforming at all times with current security practices in order at least to harden, if countering is not possible, attacks on user privacy.

SSEDIC 2020: Track 18
Discussions on the future format and funding of SSEDIC 2020
Chair: **Jon Shamah,** *Vice-chair EEMA* **& Christian Schunck,** *Senior Research, Nestor*
With over 200 experts from more than 60 partner organizations from the EU and beyond SSEDIC has become the broadest resource of eID expertise in Europe. SSEDIC.2020 will build on the SSEDIC success. For further information please contact Jon Shamah at jon.shamah@eid-ssedic.eu

Executive Summary:
Lorraine Spector - EEMA Member