D4.1 EU – Brazil Cooperation Workshop

Grant Agreement number:	**258655**
Project acronym:	**BIC**
Project title:	**Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services**
Funding Scheme:	**ICT Call 5 FP7**
Project co-ordinator:	**James Clarke** **Programme Manager** **Waterford Institute of Technology**
Tel:	**+353-71-9166628**
Fax:	**+ 353 51 341100**
E-mail:	**jclarke@tssg.org**
Project website address:	**http://www.bic-trust.eu**

Revision:

Revision [Final]

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	**Public**	

BUILDING International Cooperation for Trustworthy ICT

European Commission
Information Society and Media

EU-Brazil Cooperation Workshop held 3rd May 2011 co-located with International World of Telecommunications (IWT) Conference 2011

BIC Partners

TSSG

Waterford Institute of Technology

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM ParisTech

Atos

Rio de Janeiro, Brazil

3rd May 2011

Table of contents

1 Executive Summary 4
2 Introduction - Workshop objectives and goals 5
3 Panel A. Building a long term strategy for International cooperation in research related to Trustworthy ICT between EU and Brazil. 6
3.1 Building a long term strategy for International cooperation in Trustworthy ICT between EU and Brazil. 7
3.2 Digital Identity in Brazil 8
3.3 Trustworthiness in Cloud Computing. 9
4 Panel B. Future Internet initiatives in Europe and Brazil: an overview of related initiatives and ICT security challenges. 10
4.1 Future Internet in Europe: an overview of related initiatives and ICT security challenges 11
4.2 Research issues for security in the Future Internet – Brazil perspective 13
4.3 New models of communication and security for the Future Internet 15
4.4 Future Internet: New Network Architectures and Technologies 16
5 Discussions panel 18
6 Conclusions 21
Annex 1 Final Terms of Reference and Program 23
Annex 2. List of registered IWT attendees 24
Annex 3. Presentations made during the workshop 27

1 Executive Summary

Over the past four years, a sustained high-level international consultation activity, conducted through the FP7 INCO-TRUST project covering USA, Canada, Japan, Australia and South Korea, resulted in highly successful collaboration alignment with their various national program agencies and their researchers engaged within ICT Trust, Security and Privacy areas. Starting on 1st January 2011, funded within the project portfolio of the European Commission DG INFSO, Unit F5 ICT Trust and Security Research [1], the Coordination Action BIC project [2] – **B**uilding **I**nternational **C**ooperation for Trustworthy ICT*: Security, Privacy and Trust in Global Networks & Services* – will now expand the co-operation models of EU researchers and programme management with their peers in new ICT high-growth countries, specifically Brazil, India and South Africa, who represent emergent world-impacting information economies through the scale and sophistication of their growing ICT sectors. BIC will also continue to capture the experiences and engagement of the INCO-TRUST target countries into BIC via an International Advisory Group of the leading policy makers from the US and other countries.

The BIC project has four core objectives:

1. Charting the security and trust *landscape* of Brazil, India and South Africa and their initial and potential match to EU Trust, Security and Privacy themes.
2. Prioritisation of the EU-influenced vision and research directions including alignment of work programmes.
3. Global alignment, consensus and outreach of the European visions and challenges across all targeted countries.
4. Definition of Tangible International Activities including transnational partnerships with EU partners..

The EU – Brazil cooperation workshop of the BIC project was proposed and accepted by the organisation committee of the International World of Telecommunications (IWT) 2011 conference and workshop. The BIC workshop was held in Rio De Janeiro, Brazil on 3rd May along with IWT 2011. It was attended by over 60 delegates from around the world predominately from Brazil.

The aim of the BIC Brazil – EU workshop was to gain a shared understanding of critical issues, identifying promising trust and security research directions, and also to foster collaboration between EU and Brazil research teams. The organising committee were satisfied at the outcome of this workshop: that it had indeed met the objectives and that further collaborative work would ensure to facilitate international co-operation in Trust, Security and Dependability (TSD) research.

The organising committee of the workshop developed the programme around two panels: one covering research challenges for cooperation and one looking at initiatives and projects already underway in both countries. The workshop discussions led to identification of a number of research challenges, scoping research priorities and joint actions to address them.

The web site of the event can be found at is http://www.inatel.br/iwt/ and

http://www.inatel.br/iwt/slide-show/bic-workshop.

2 Introduction - Workshop objectives and goals

The BIC project, along with the tremendous assistance of the local organising committee of IWT 2011, hosted the Brazil – EU Workshop in Rio De Janeiro on 3rd May 2011 with over 60 attendees. The setup and preparation of the event took place over a number of months and the BIC partners relied heavily on local organisational support from CPqD, a major provider of Operations Support and Business Support systems, training and consulting services that employs over 1200 professionals, as well as INATEL, National Institute of Telecommunications, located in Santa Rita do Sapucaí in southern Minas Gerais.

The workshop was co-located with the International World of Telecommunications (IWT) annual event of 2011, whose main goal is to promote and discuss the latest innovations in the telecommunications area. The purpose of IWT is for the researchers to share ideas and learn more about the new developments and ongoing research. Therefore, it was considered highly appropriate for the BIC workshop proposal to be submitted in an open call for workshops and the proposal was accepted amongst fierce competition.

The overall theme of the BIC session was building a long term strategy in international research for Trustworthy ICT between Brazil and the EU.

The workshop had the following core objectives:

- to capitalise on the presence of a large group of research communities from Brazil and around the world present at IWT 2011;
- Understand the status and objectives of programs supported by EU and Brazil in all areas of Trustworthy ICT;
- Highlight potential collaboration subjects that are mutually beneficial and require further Brazil-EU collaboration for ensuring Trustworthy ICT, including security, privacy and trust against borderless cyber attacks;
- Share information about international projects and initiatives already underway in Brazil and Europe and begin to generate ideas for new ones;
- Decide next steps for the collaborations.

The Organising Committee structured the workshop around two panel sessions:

Panel A: Building a long term strategy for International cooperation in research related to Trustworthy ICT between EU and Brazil.

Panel B: Future Internet initiatives in Europe and Brazil: an overview of related initiatives and ICT security challenges.

The sessions were designed to identify a short list of key common-interest areas to pursue as proposals for the coming proposal calls and/or in defining future calls.

The sessions identified open research issues, cross-cutting links, and related infrastructural implications and input for road-mapping of possible research areas for a joint EU-Brazil collaboration.

Further information is contained within the report and on the workshop web site at http://www.inatel.br/iwt/slide-show/bic-workshop.

3 Panel A. Building a long term strategy for International cooperation in research related to Trustworthy ICT between EU and Brazil.

Agenda

1. Building a long term strategy for International cooperation in Trustworthy ICT between EU and Brazil. Speaker: Jim Clarke, Waterford Institute of Technology

2. Digital Identity in Brazil Speaker: Noemi Rodriguez, PUC-Rio/RNP

3. Trustworthiness in Cloud Computing, Speaker: Neeraj Suri, TU Darmstadt

3.1 Building a long term strategy for International cooperation in Trustworthy ICT between EU and Brazil.

Speaker: James Clarke, Waterford Institute of Technology, TSSG, Ireland

Since January 2011, James Clarke is Project Coordinator of a European Framework Program 7 Co-ordination action entitled BIC, which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. BIC will engage the European Union trust and program management (funding organizations) and research communities with their peers in Brazil, India and South Africa and enable the collaboration with research communities in trust and security already established in the US, Australia, Japan, Korea and Canada established in the recently concluded INCO-Trust project that Mr. Clarke also coordinated from 2008 - 2010. In addition, Mr. Clarke is actively involved in the research community, having served in various international conference committees as organizing, technical and program committee member.

Mr. Clarke presented the activities related to international cooperation on Trustworthy ICT research between EU and Brazil, explaining that we are certainly not starting from scratch in this regard. Regarding the EU-Brazil research co-operation to date, two related workshops have already been held in 2009, one focused on Future Internet[1] and another one entitled EUBR2009[2] with more general focus on ICT research collaboration including a dedicated session on trustworthy ICT in the Future Internet. Multiple high level dialogues between the EU and Brazil about collaboration resulted in the signing of a formal scientific collaboration agreement and as European Commission Director-General of DG-INFSO Fabio Colasanti stated in one interview "The European Commission is very interested in establishing a long and prosperous partner with Brazil in the ICT domain, so we can work together in the development of the information and knowledge societies, so both societies and economies can have benefits from it."

On this basis, a joint call between EU and Brazil was established in the recent FP7 7th Call in 2010 and Mr. Clarke presented this joint call's mechanisms. Mr. Clarke explained that the BIC project intends to provide further evidence that the joint call mechanisms must not only be continued but expanded in scope and size to enable larger size and numbers of RTD projects between the countries. Details of the awarded projects from this call were not available before the workshop so these projects were not presented. More information will become available at http://cordis.europa.eu/fp7/ict/

Mr. Clarke explained the role of the BIC project in more depth, explaining that the project would coordinate the research communities to highlight problems/technologies of common interest where synergy could meaningfully add "local" (technological, societal) depth and explore together problems from the interconnected trans-national world of "things" (& attacks, impact, enforcement) where synergy would be very beneficial to jointly influence and leverage issues for all concerned. The project is looking for assistance in the following: scoping the landscape in Brazil research on ICT Trust and Security including: Who are the funding bodies? And Who are the technical/research communities? The project is putting together an International Advisory Group (IAG) and would like nominations for this and would like to receive topics of interest from the Brazil community for and Annual Forum.

Mr. Clarke concluded by stressing the importance of reading the open call and provided a tutorial of the current FP7 call 8. ref. ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2011-12_en.pdf

[1] http://www.cpqd.com.br/futurodainternet/
[2] http://www.cce.usp.br/servicos/eubr2009/

3.2 Digital Identity in Brazil.

Speaker: Noemi Rodriguez, PUC-Rio/RNP, Brazil

Noemi Rodriguez is associate professor at the Computer Science Department of the Catholic University of Rio de Janeiro (PUC-Rio). She also acts as a consultant for RNP in the area of Middleware, and more specifically has been involved, for the past years, in the establishment of CAFe, RNP's e-identity federation.

In this talk, a survey of the activities undertaken by RNP (Rede Nacional de Ensino e Pesquisa) in the area of identity management was presented. RNP is a non-profit, non-government organization that acts as Brazil's NREN (National Research and Education Network). Besides being responsible for Internet access of more than 300 organizations, RNP maintains a portfolio of services for the academic community.

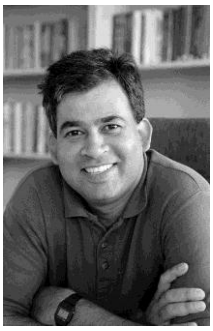
The model that is adopted for the development of new services is to have part of RNP's research and development team maintain a working group program. This program, which was formally launched in 2002, issues an open call once a year. The selected groups have one year to develop a prototype of the proposed service. After this, some of the resulting prototypes are selected for a second phase, in which the group develops a pilot of the service. If the pilot is successful, it becomes an experimental service, and finally, after one more year, goes into production. Over the 10 years of the program, several services have successfully reached production. Examples are video streaming and distribution, voice over IP, distance-learning tools, and services related to authentication and authorization.

In the area of authentication and authorization, two independent groups led efforts related, respectively, to public key infrastructures and to federated authentication and authorization. The first of these efforts resulted in ICPEDU, a PKI for the academic community. Prof. Ricardo Custodio, from UFSC (Universidade Federal de Santa Catarina), led the PKI efforts, and currently the root CA is maintained by his institution. The efforts of the second group led to the creation of CAFe, a federation for access to web-based services in which authentication is provided by the users' home organizations, known as their Identity Providers. Service Providers receive information about authentication and other attributes necessary for access control from these Identity Providers, creating a trust network.

RNP has now created a Technical Committee for Identity Management (CT- GId), with members from RNP itself and from the academic community, with the goal of overseeing the evolution and integration of identity-related services. One of the first activities of this Committee was to recommend the implementation of a pilot *eduroam* federation, for access to wifi networks. This is being demonstrated in the end of May 2011 at RNP's annual workshop (WRNP). Other foreseen activities include proposals for the integration of the Brazilian PKI and Federation with their international counterparts and the fostering of the use of these technologies in different scenarios.

The presentation and subsequent discussions concluded with a more in depth explanation of how to become involved in Working groups. A pointer was made to the annual Brazilian Symposium on Security, which may be an interesting opportunity to interact with the Brazilian research community: http://www.ppgee.unb.br/sbseg2011/sbseg2011.html.

3.3 Trustworthiness in Cloud Computing.



Speaker: Neeraj Suri, TU Darmstadt

Neeraj Suri received his Ph.D. from the University of Massachusetts at Amherst. He currently holds the Chair Professorship in "Dependable Embedded Systems and Software" at TU Darmstadt, Germany. His earlier appointments include the Saab Endowed Chair Professorship, faculty at Boston University and multiple sabbaticals at Microsoft Research. His research interests focus on design, analysis and assessment of trustworthy (dependable & secure) distributed systems and software. The emphasis is on composite issues of dependability and security for web-scale SW/OS, verification/validation of distributed protocols and especially "trusted/secure systems by design". Additional professional details are available at: http://www.deeds.informatik.tu-darmstadt.de/suri/activities/activities.html

This talk highlighted the trustworthiness challenges introduced by the cloud model as addressed in the EU, and specifically the opportunities for international collaboration in this space. The *Cloud* paradigm offers a communication and computation fabric to link geographically disparate resources. While the user benefits from transparent access to an anytime-anywhere global computing platform, this global resource pool and resource accessibility also implies a global scale attack surface for its trustworthiness (i.e., dependability, security and privacy).

The largest challenge from the trust perspective is the cloud provider needs to be able to control and ensure the protection including routing of data in their cloud doesn't go offshore and be able to prove this to the customer. Additionally, it raises a range of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others. The storing and processing of personal and professional user data on servers that are not within direct user control not only raises questions on the confidentiality of the data but also a variety of privacy and trust concerns that need to be address both legally and technically. New information security approaches have to be developed, when the components of the ICT system are no longer stably identified and in-depth defence principles are challenged. The cloud environment consisting of virtualisation machines, mechanisms, policies and levels of abstraction involved could cause a situation where we are not comprehensively attacking all of the real security issues if not careful. Hence, it is only a matter of time before trust falls apart if not addressed comprehensively and coherently.

In addition, we need robust operating systems for the *cloud*. There were some discussions in the session where hardware support for advanced security systems is needed while some providers in the audience were saying they already had or knew of potential systems for this. In any case, there is a need for rigorous virtual environment hygiene and there is an need for robust dedicated operating systems that cover the whole life cycle: create, operate and delete the virtual environments when they are no longer needed.

The international research community must develop together four complementary actions:

(a) Identify appropriate provisions to better approximate cloud computing specificity and the European legal framework on security and privacy;

(b) Adjust/develop standards and certification schemes to better control security and privacy aspects of cloud computing;

(c) Propose a Service Level Agreement template accounting for (a) and (b) to strengthen users trust and confidence;

(d) Prepare awareness raising campaigns encouraging users to take the opportunity of cloud computing offer to deepen their ICT risk analysis knowledge.

4 Panel B. Future Internet initiatives in Europe and Brazil: an overview of related initiatives and ICT security challenges.

Agenda

1. Future Internet in Europe: an overview of related initiatives and ICT security challenges. Speaker: Aljosa Pasic, Atos Origin, Spain

2. Research issues for security in Future Internet. Speaker: Celia Ghedini Ralha, University of Brasilia

3. New models of communication and security for the Future Internet. Speaker: Michel Riguidel, ENST , Paris

4. Future Internet: New Network Architectures and Technologies Speaker: Christian Esteve Rothenberg, Fundação Centro de Pesquisa e Desenvolvimento (CPqD), Campinas, Brazil.

4.1 Future Internet in Europe: an overview of related initiatives and ICT security challenges

Speaker: Aljosa Pasic, Atos Origin, Spain

ALJOSA PASIC current position is Public Sector Director of Atos Research & Innovation (ARI), which is a department within Atos Origin Spain. He graduated Information technology at Electro technical Faculty of Technical University Eindhoven, The Netherlands, and has been working for Cap Gemini (Utrecht, The Netherlands) until the end of 1998. In 1999 he moved to Sema Group (now part of Atos Origin) based in Madrid, Spain, where he occupied different managerial positions. During this period he was participating in many international research or consulting projects, always related to the areas of information security or e-government. He is also member of Board of Directors of EOS (European Organisation for Security) and has been involved in the work of many other international organisations such as ENISA, ERCIM, NESSI, EFIA, IARIA or IFIP. His current interests include Secure Software Engineering (e.g. the chairman of NESSOS industry advisory group), electronic identity (e.g. involvement in thematic network SSEDIC) and trust management (e.g. member of the advisory board of Trust in Digital Life initiative).

The presentation covered the EU approach to Future Internet, initially focusing on the project FI-WARE that aims to develop the core platform for Future Internet. The presentation furthermore covered an overview of other relevant initiatives as well as open challenges when it comes to trust, security and dependability.

The introductory part explained trends such as data network revolution, internet of things or open delivery platforms. Data has growth 10-fold in last 5 years (from ~177 exabytes in 2006 up to ~ 1,700 exabytes in 2011) and scale in prosumers and sensors will make data grow even at higher rates. There is a need to filter and exploit what is relevant for me, now, here. There is also a need to preserve privacy, manage confidential data, multilevel security, data loss prevention… In parallel, people want to find and easily access applications that assist them in daily life situations: this would transform home and cities in better places to life. This means that access should be provided anywhere, anytime, from any device which stresses importance of research in context-aware Security for “constraint-driven” environments (tiny devices, usability rules…). People wish to share content/data and applications with others and they wish to learn what has been useful/interesting to others, in real-time, on the go. This challenge also implies research need for security, although more related to reputation and trust which become important decision drivers. Internet is not longer an experimental tool: people expect that it should secure by design. People entrusted their life (e.g. lifelogging) and their business to internet so they want to govern access to their data and to have “user-centricity”. Finally, people want internet to handle dynamicity just like physical world: dynamicity of privacy, trust and security solutions.

All these challenges associate security research for Future Internet with the real demand from society. FI-WARE project, that held its kick off meeting practically at the same time like BIC workshop in Brazil, is also following this people-oriented approach. FI-WARE will be a technological foundation to satisfy the demands of application/services providers and consumers across various usage areas, stimulating and cultivating a sustainable FI service ecosystem.

The FI Core Platform comprises a set of technological “Generic Enablers” which are considered general purpose and common to several current and future “usage areas”. Generic Enablers (therefore, the FI Core Platform) will provide open interfaces for development of Applications Future Internet Applications run on top of “FI Core Platform Instances” built upon selection and assembly of “Platform Products” implementing “Generic Enablers” of the “FI Core Platform”. Use Case trials will consist on application scenarios running on top of FI Core Platform Instances, involving real users.

The next part of presentation focused on security research within FI-WARE project.

Security Monitoring is one of the main areas of research and research in FI-WARE especially addresses challenges of scalability for monitoring of things, services, systems and applications which run in a Future Internet and generate events which are kept in event logs or elsewhere. There is a need to have a consistent interface to these events, parsers significance etc, alerts, notifications detection of events which occur on multiple systems and many other issues. One of the main EU projects in this area is MASSIF (http://www.massif-project.eu/). When it comes to FI-WARE, research on this topic include collection of heterogeneous information and standardisation, risk analysis and correlation, decision making support and simulations, visualisation and reporting and forensics.

The second security research task group is considering so called Generic Enablers for security, such as Identity and privacy, Authorisation and Usage Control Policies, Auditing, Context-based security and Compliance, Security properties and service descriptions and Selection and deployment of reconfigurable solutions. Finally, the third security research task group is focusing on optional security enablers (e.g. protected data etc) for the core platform.

For example, access control policies are used to manage the access of end users to services and resources offered by an organisation in the current internet. However, as the number of users increases, and new organisations join to the same federation or the relationships among them change, the management of these policies becomes more and more complex. This is due mainly to the great amount of policies to manage, either access control policies, privacy policies or validation policies based on Levels of Assurance (LoA), among others. Therefore, there is a need to re-assess these generic enablers for their feasibility in the Future Internet.

In addition, to achieve end-to-end assurance and trustworthiness in complex Future Internet environments, we need to look holistically at how to provide evidence gathering and aggregation across different “slices” (e.g. internet of things, clouds etc). While widely used Service-level agreements (SLAs), that specify the exact types of information that will be shared are essential for future internet delivery model, Protection-Level Agreements (PLAs) might represent an additional option for expressing protection objectives and related indicators for a business process that is run partially in a different trust domain. PLAs provided by Future Internet core platform should include external points of reference and provide “boilerplate” text that can be customized. Compliance checking and auditing services can be provided “on-demand” by specialised provider only if evidences are created and delivered by core platform. In regard to dynamic binding with other security assurance and assessment services it is important to notice that these operations might be implicitly contained in WSDL description(e.g. getcompliancecapability (service) in order to obtain information about events or traces that provider might deliver).

The final part of this presentation focused on a specific topic of privacy. It has been mentioned that privacy is highly contextual, subjective, dynamic...while regulations are described in a pretty “descriptive “ and generic terms (for instance, the “Proportionality Principle”). This makes it subject to different interpretations and additional problems rise from the fact that the national guidelines and regulations are sometimes incompatible with each other. Evaluation of privacy compliance is a lengthy and costly process, especially if service provider works around the globe. Therefore, there is a need for a Context-aware and Agile Privacy Solutions in Future Internet.

Finally, the presentation covered other relevant EU initiatives in the area of security, such as EP3R or EOS, have been briefly presented.

4.2 Research issues for security in the Future Internet – Brazil perspective

Speaker: Celia Ghedini Ralha, University of Brasilia

Célia Ghedini Ralha is an Associate Professor at the Department of Computer Science, University of Brasília, Brazil. She received her Ph.D. degree in Computer Science from Leeds University, England, UK in 1996. Her M.Sc. in 1990 was received at the Aeronautics Institute of Technology (ITA), São José dos Campos, São Paulo, Brazil. She has a BASc in Administration from the Catholic University of Brasília, Brazil. She has experience in Computer Science, focusing on Intelligent Information Systems, with research interest on the treatment of information and knowledge using Multi-Agent Systems approach, focusing the intelligent agent interaction protocol and the association to other technologies, such as SOA, Web Intelligence, Web Semantic, Business Process Management and Knowledge Management.

The speaker first presented a short overview of Brazil´s Research and Developments (R&D) priorities according to the Ministry of Science and Technology (MCT) - 2007-2010 plan, which includes the following areas of research:

- ICT
- Nanotechnology
- Biotechnology
- Technological Development of Enterprises
- Nuclear Policy
- Space Program
- Management of Ecosystems
- Energy and Mineral Resources
- Climate Changes
- Meteorology, Climatology & Hydrology
- Biodiesel
- Hydrogen and Fuel Cells
- Biodiversity
- Antarctica

According to the cited R&D scenario, the speaker presented the ICT priorities for the European and Brazil (EU-BR) coordinated call:

- Future Internet - Experimental Facilities
- Future Internet - Trust and Security
- e-infrastructures
- Networked Systems and Control
- Microelectronics/Microsystems

The area of Future Internet - Trust and Security was justified according to the 2010-2014 National Plan for Broadband Access in Brazil, where the government intends to reduce the actual regional and social disparities to information broadband access: South-East 23,81%, South 21,33%, Center-West 20,45%, North 13,45%, and North-East 4%. For this the government has investments in the order of R$ 49 billions (EUR 18 billions) to fixed single access type (urban and rural) to guarantee in 2014 around 30 millions of broadband access. Considering the Communitary Fixed Access the goals are:

- 100% broadband access for government institutions
- 100% Federal Administration
- 100% Public schools
- 100% health centers (more than 177.000)
- 100% public libraries (more than 10.000)

- 100% public security institutions (more than 14.000)
- Create 100.000 federal telecenters.

Considering the mobile access the goal for 2014 is 60 millions of broadband mobile access in the country.

Many challenges are introduced according to the necessary scenario transformation for Future Internet – Trust and Security priority area in Brazil. For digital inclusion, citizens must trust the environments. This cannot be based solely on technology, a trusted system should incorporate technological, social and legal guarantees. Solutions that are globally relevant will have the greatest impact and hence the longer benefit, and consequently international cooperation is mandatory. Some trust and security goals and mechanisms were cited.

The EU-BR coordinated call was presented, citing that in September 2010, the CNPq and DG INFSO launched a coordinated call for binational projects in ICT with the total amount of R$ 11 million/4 million Euro, with up to R$ 3 million/1.5 million Euro per project. Five areas were included in the call (Edital CNPq No. 066/2010): Future Internet - Experimental Facilities, Future Internet – Security, Networked Systems and Control, e-Infrastructures and Microelectronics/Microsystems. But only one project per area will receive the budget!

As a result to this call, different research groups in Brazil and EU had the common objective to promote interaction and cooperation, but for many research groups in Brazil it was the first experience submitting project with FP7 requirements and format. Nevertheless, several consortiums were formed, but not so many achieved the coordinated project submission.

To conclude the talk, some of the learned lessons with the coordinated project submissions were cited, mainly considering that the coordinated call is fundamental to have a formal means to promote cooperation between researches from European and Brazilian communities. The group also considers that it is a good idea to have more specific calls to Future Internet and related topics, in order to stimulate more projects, more consortiums to improve the quality and experience of the partners.

4.3 New models of communication and security for the Future Internet

Speaker: Michel Riguidel, ENST , Paris
Michel Riguidel is now Professor Emeritus (since May 2010), previously the Head of the Department of Computer Science and Networks, at Telecom ParisTech (Ecole Nationale Supérieure des Télécommunications, www.telecom-paristech.fr) in Paris, where he lectures in security and advanced networks. His research is oriented towards security of large Information Systems and Networks and architecture of communication systems (Security of the Future Internet, Trust, Privacy and Advanced Networks, Critical Infrastructure Protection). He is contributing to the Coordinated Action of the FP7 ThinkTrust, IncoTrust (2008-2010) and BIC (2011-2013) for coordinating research on security at the international level (EU, USA, Japan, Australia, South Korea, Brazil, India, South Africa). He is involved in FIA (Future Internet Assembly) as FIA caretaker.

The talk consisted of a visionary approach for communications and security for the Future Internet. The speaker first set the scene whereby a future pervasive ICT will consist of billions of networked devices, leading us to self-organising, self-healing and self-protection systems. Such a paradigm could benefit from bio-living world inspiration where such organised communities/populations exist and evolve. In particular, we shall have to develop self-healing and self-organising capabilities into the ambient computing space. This will involve a proper understanding of the ecology of these interactions and interconnections. More generally, we have to look to maintaining the resulting heterogeneous systems in a cohesive unit. This route leads us towards the vision of incremental development and deployment – systems are never finished, evolution is incessant, upgrades, changes in functionality, new features are being added at a continuous pace; systems are expected to be able to respond to the changing circumstances of the ambient where they are embedded.

Another important area to address is the need to change the current asymmetry between users and suppliers/publishers/service providers. These users, whether private individuals or professionals, must take back control (at least in part) of their personal, digital space. Even so, currently confidentiality is fragile, both in respect of commercial service providers and in terms of risks of intrusion and interception by private and public players. This represents a manifest risk of the growing trend towards a massive dissemination of digital traces representing behavioural, personal and even biological information (such as DNA, fingerprints, etc…). Similarly, the choice of configuration of tools present in this personal space partially eludes the control and even the knowledge of these users.

It is essential to return to them the driving role, by seeking subsidiarity and independence, arriving at developing methods for user-oriented risk assessment; developing methods, tools, and repositories to help developers analyse security implications of their code, and more generally to develop verifiably secure software; developing tools and infrastructure that will guarantee to end users that software to be installed on the systems they use is secure through verifiable evidence.

This vision of a future user-centric system will need to offer features such as personalisation and smooth interaction with users, who will also expect that these systems will offer an individual or community “sphere” providing protection and privacy. It will also offer a series of features such as authentication or anonymity, secure data storage, data matching or exchange, and trusted execution. The result should be able to combine privacy protection with personalisation. In a similar fashion, we need mechanisms and tools for assessing and proving the trust and security of a complex system. These tracks are not exhaustive and could be extended with other suggestions that touch on the emergence of new types of terminals, biometry and questions of nomadism and mobility.

4.4 Future Internet: New Network Architectures and Technologies

Speaker: Christian Esteve Rothenberg, CPqD, Campinas, Brazil.
His current research interests span Internet routing and packet forwarding, data center networks, NGN/IMS, OpenFlow, and named data networking. He received his Ph.D. in Electrical and Computer Engineering from University of Campinas (UNICAMP) in 2010. In his doctoral studies he worked on probabilistic data structures applied to packet forwarding in content-oriented networks. He was a visiting researcher at Ericsson Research Nomadiclab, Helsinki, Finland, and contributed to the EU FP7 Publish/Subscribe Internet Routing Paradigm (PSIRP) project. He holds the Telecommunication Engineering degree from the Technical University of Madrid (ETSIT - UPM), Spain, and the M.Sc. (Dipl. Ing.) degree in Electrical Engineering and Information Technology from the Darmstadt University of Technology (TUD), Germany, 2006. During his master thesis at Deutsche Telekom he worked on IMS-based fixed mobile convergence and mobility management, and was engaged in R&D activities on converged access networks (ScaleNet) and self-optimizing radio access networks.

The talk covered how the application and user demands on the Internet are increasing with mobile technologies and media content in a situation where the Internet today is a complex agglomerate of protocols that inherits the grown legacies of decades of patchwork solutions.

There is a common consensus that the Internet needs improvement. Nevertheless, there is not yet a shared vision on how this may happen. As a direct consequence research programs have started worldwide to re-think traditional Internet design principles and to come up with new architectural concepts for the so-called Future Internet (FI).

The talk provided an overview of Future Internet research directions and trends, in particular with a focus on Future Internet architectures that are currently under discussion and related technologies. It presents the Future Internet research initiatives around the world and the efforts to establish experimental facilities for FI research. Among the approaches discussed are addressing and routing concepts, adaptability, autonomicity, self-*, *-aware and manageability, virtualization, neutrality, openness, diversity, extendibility, flexibility and evolvability. The talk also presents some interdisciplinary aspects related to artificial general intelligence and bio-inspired ICT.

Along the proposed approaches and (visionary) ideas, there are a series of remarkable shifts common to many FI projects. For instance, the basic issue of resource multiplexing is moving towards integrated management of packets and circuits (aggregates) in addition to the support of virtualization of all network resources (routers and links) to allow multiple slices coexist in isolation. The issue of connection establishment was traditionally concerned with minimizing the round trips. New ideas consider including a phase for exchange of identity, the need to diffuse attack, and the support of the DTN paradigm. The old view on addressing focused on a node numbering scheme designed for efficient packet forwarding.

The new view is to take into account security issues (accountability, privacy, deterrence, hiding), management issues (re-numbering), multi-homing, and even the fundamental entity to be addressed, questioning whether addressing physical nodes should be less the focus in favour of addressing services, information and content. The latter approach leads to the approach of introducing an information-layer that may become the new Internet waist. While the old view was to consider naming of content/information as an application issue, the new approach is to have a framework around naming and identity of information, independent of how you get it, improving availability of information by pushing it into the network. The emergence of the Cloud puts in evidence the problems around communications being end-point focused and not data focused.

In addition to the risks of availability due to network outages, security is a main concern due to poor endpoint authentication or policy issues (HIPAA) due to restrictions not being expressible with existing routing protocols. The network should assist with content retrieval in addition to enabling host-to-host communication. The question is "can we create a network architecture based on naming data instead of naming hosts?"

These and any Future Internet architectural question should not only be validated on paper and simulation work but tested at scale on real network equipment. Beyond the lessons learned from an experimental-driven research, the enabling experimental infrastructures federated to reach scale are in a unique position to show the way to allow an (incremental) deployment path of any new global scale architecture.

In summary, the topics covered in the presentation include:

- · Motivation for Future Internet Research
- · Review of Principles of Internet Architecture
- · Evolution of Internet architecture
  - IPv6, MPLS, IP Mobility and Multi-Homing, etc.
- · Scenarios of Evolution for a Future Internet Architecture
- · Overview of Future Internet Recent and Ongoing Projects
  - Overview of selected projects from the EU Framework Programs, US FIND, AKARI (Japan), etc.
  - Experimental Facilities for Future Internet research
  - PlanetLab, FIRE, GENI, G-Lab, etc.
- · Future Network Architectures: Technological Challenges and Trends
  - Capacity, Ubiquity, Scalability and Virtualization
  - Information-centrism, Semantic, Context, Identification, Mobility, Naming, Indirection Resolution and Routing
  - Adaptability, Autonomicity, Self-*, *-Aware and Manageability
  - Security, Privacy, Trust, Transparency and Anonymity
  - Service-centrism, Neutrality, Openness, Diversity, Extendibility, Flexibility and Usability
  - Simplicity, Sustainability and Evolvability
  - Artificial General Intelligence and Bio-inspired ICT

A main reference for the talk can be found here - New Network Architectures: The Path to the Future Internet, Springer, Series: Studies in Computational Intelligence, Vol. 297, Tronco, Tania (Ed.), 1st Edition, 2010, 250 p., ISBN: 978-3-642-13246-9.

5 Discussions panel

After the workshop presentations concluded, there was a panel session to discuss and identify research topics as possible candidates for initial research collaborations that could also lead to potential joint proposals. While the preceding sections detail the technical issues of mutual interest, the intent of this section is to highlight and summarize key joint-interest priority areas as:

- **Cloud Computing & Cloud Storage** is increasingly "the" international conduit for data and knowledge sharing along with the corresponding international impact implications if its trustworthiness gets compromised across the internationally diverse physical, human and functional elements.
    - While there are a multitude of technical activities of mutual interest, the issues of **data governance and liability** are key themes that need to be addressed from both a policy and technology viewpoint.
    - As the Internet of Things also relates to the cloud model, the nature of legally and globally consistent identifiers of both people and "things" required international harmonization.
- **Infrastructures Integrity** is a dedicated international association issue for infrastructures spanning the telecommunication SLA's behind the cloud and the Future Internet, or for the financial and services sector (data centres, service and support centres etc). Similar to the cloud issues, the policy issues of governance and liability are critical.
- **International Data exchange capabilities and dataset sharing:** The interconnections across computing systems and data on an international scale requires coordination as countermeasures across globally penetrative security attacks. A repository of globally accessibly attacks and countermeasures repository would form a high international interest activity.
- **Security Compliance Management and Information Security Assurance** is a key international policy element that needs to be developed to link the above technical issues, and very much needs to be detailed from a multi-national and multi-cultural viewpoint. A necessary element to develop is the economics of security from an international compliance, governance and provenance aspect.
- **Future Internet data and information provenance (trusted source)** especially during times of disaster and large events is a topic that was highlighted at the session, for mutual cooperation between Brazil and the EU. Recent examples (eg. Japan earthquake and subsequent tsunami) were discussed at length in which the reliability of information becomes extremely questionable for long periods due to the vicious cycle of feeding untrustworthy or incorrect information between conduits via the 'new media'. For a more trustworthy Future Internet, the user must be able to categorically trust the source and integrity of the data and information they are receiving. There are complimentary skills in Europe and Brazil on these research topics and they can be leveraged well together on this topic.

The panel also discussed each country's funding agencies and their available mechanisms for funding research in RTD involving trustworthy ICT. A summary of these is contained here.

Brazil

Within Brazil, there are a number of funding agencies for ICT related research in Brazil:

- CNPq (National Research Council) and FINEP (financiadora de estudos e projetos) have public calls for funding. These are national foundations linked to the Ministry of Science and Technology. More information at http://www.cnpq.br/english/cnpq/index.htm and http://www.finep.gov.br/english/FINEP_folder_ingles.pdf.

- FUNTEL, which is a fund for technological development of Telecommunications. FUNTEL is linked to the Ministry of Communications of Brazil. http://www.funtel.com.br

- State Research Foundations - Each State has its own foundation with its own budget and they have freedom to establish their own calls, but it is not only specific to ICT.

EU – Framework Programme 7 (FP7)

The overall focus of ICT trust and security research in the seventh Framework Programme is on developing knowledge and technologies for building an open, secure and trustworthy information society in Europe, where citizens and organizations can fully reap the benefits from the new technologies. Central to the research is enabling users to manage and protect their digital assets, identities and personal data when they interact in the digital world.

Closely interrelated thematic areas are promoted as target outcomes inside of topic "trustworthy ICT", including:
a) Heterogeneous networked service and computing environments, including Architectures and protocols; Future Internet; Virtualisation and other techniques for protection, assurance; Metrics and tools for quantitative security; and Enabling technologies (languages, biometry, crypto, ..).
b) Trust, eID and Privacy management Infrastructures, including Trust assurance; Privacy infrastructures; and Management of ID claims (usability, privacy, control).
c) Data policy, governance and socio-economic ecosystems, including Management and governance frameworks for trust and security policies; Technology supported socio-economics frameworks; Multi-polar security governance; and Tools for trust measurement.
d) Networking and Coordination Activities, regarding Stimulating and organising interplay technology-law-society-economy; Promoting standards, certification, best practices; and Coordination national RTD activities.

The current open call is number 8 (deadline January 2012) and information for this call can be found at ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2011-12_en.pdf.

EU – Brazil Coordinated Call (FP7 Call 7)

In September 2010 (deadline early 2011), there was a Coordinated EU – Brazil call released between the European Commission and CNPq. The call covered five topics, including:

- Future Internet Experimental Facilities
- Future Internet Trust and Security

- e-infrastructures
- Networked Systems and Control
- Microelectronics

Within this coordinated call, the maximum budget per topic available was listed as 1.5M€ EU contribution (although if all five were accepted, this would result in c. 1M€ EU maximum contribution each). The submitted Part B of the proposal describes the overall project in one coherent document with both the EU and the Brazil elements and clearly defining each roles. When submitted, the proposal document (Part B) was submitted to both authorities on the same day, with the European version being submitted in English and the Brazil version being submitted in Portuguese respectively. The Part A's (financial and administrative parts) of the proposals were submitted individually in the EU and Brazil. This submission process made it quite easy for the participants.

Although this call is now completed, if you would like further information on it, the documents can be found here:

The Coordinated Call between European Union and Brazil http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=377

The call was also released in Brazil under a call for proposals issued by CNPq http://www.cnpq.br/editais/ct/2010/066.htm (in Portuguese)

6 Conclusions

In recent years, there have been a number of productive joint activities held already between the EU and Brazil in looking at joint collaborations between the countries, such as:

- In September 2009, there were two international workshops held in Brazil examining EU-Brazil cooperation on new architectures for the FI[3].
- A coordinated call was already held in EU FP7 call 7 between the EU and Brazil including one topic on Future Internet Trust and Security.

One of the goals of the BIC project is to follow the considerable Brazil – EU joint efforts already done and to increase productive joint activities and collaboration between the EU and Brazil research communities. This very interactive and lively cooperation among both research communities has contributed to the success of this Brazil – EU Workshop.

During the workshop, a number of potential technical areas and initiatives for further mutual collaboration were identified between Brazilian and EU researchers in ICT Trust and security. These are summarised here.

- **Security metrics and assurance:** both European and Brazilian participants shared a joint vision that there is a need to have internationally recognised criteria for security metrics and assurance and that further collaboration on user acceptance and confidence in solutions such as service compositions or cloud computing, should be fostered.

- **Security and privacy:** in collection of data from heterogeneous sources, design, composition, discovery and delivery of context-aware secure services are pinpointed as objectives for many participants. Technologies such as the Near Field Communication (NFC), for example, eases the collection of contextual data and link a service such as payment to an actual physical location. Other proximity sensor technologies such as Bluetooth, Wi-Fi or barcodes pose similar problems and the setting of associated privacy rules seems not to be sufficient since the preferences can be very dynamic while users trust varies from location to location.

- **Privacy by design principles:** closely related to a specific service business model should help the user in the management of this location information. The integration of sensor networks with social networks is another example of applications that can sense the context, provide new services, but also extend the notion of “identifiable” data. Context can be also observed on micro-blogging services such as Twitter.

- **Future Internet**: environments that combine sensors (Internet of Things), social networks (Internet of People) and service provision (Internet of Services) involve event-related security information that must be understandable independently of language, age, physical condition, social status, or education of the recipient. This is an important aspect where Brazil has a great deal of experience and track record in the past, such as in the design of their installed Automated Teller Machines (ATM) machines in the 1970’s in which a rigorous design process involving customers was followed in the user interface design resulting in extremely user friendly interfaces. In

[3] http://www.cce.usp.br/servicos/eubr2009/ ; http://www.cpqd.com.br/futurodainternet/programacao.html

the Future Internet (FI), context-aware services and devices with localization systems will be offering attractive new functionality. People who travel and need access in mobile international environment, such as, for example, tourists or business people, will use not only contents but likely other services such as on-line collaboration, context-aware social networking or trusted local services such as emergency related or mobile payment services. The challenge for a "roaming" user will be to discover and use only 100% trusted and secure services where origin and data provenance can be verified. There is work ongoing in Brazil on this topic and the participants exhibited a willingness to work together with Europe on this.

- **Universality of trust and privacy:** Concerns about trust and privacy are universal. Citizens on the move are especially sensitive and vulnerable targets given that different platforms, service providers, organizations, business processes, policies and technologies may be involved within international service-chain provision. Therefore, user-centric security, trust and privacy configuration sets are needed. As a user typically uses the same device in multiple contexts, assistance or even automation of adaptation of configuration to a specific context is needed. It is important, therefore, to provide adaptable and context-aware privacy protection mechanisms and tools for automatic customization and personalization of security services.

- **Standardisation:** Privacy is one of the research issues that is highly subjective and contextual and there is a need for the agreement and publications of standards for WS-Agreement, and similar web service protocols, while the Semantic Web technologies for Secure Web Services may be yet further investigated while the community reaches consensus on the appropriate approach. Europe is ahead in the research on this topic.

- **International cooperation in Cyber-security:** The need of a comprehensive research towards international Intelligence, Surveillance, and Reconnaissance (ISR) in the cyberspace domain was highlighted by some participants, as the interdependent network of IT infrastructures is considered to be one global domain within the information environment, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Furthermore, the ability to conduct comprehensive intelligence collection on any threatening of our cyberspace activity followed by near-simultaneous processing, exploiting and disseminating of the information depends on international collaboration, data and knowledge exchange and sharing between all countries.

In conclusion, the BIC project will contribute to coordinating the research communities addressing common Brazil – EU interest where synergy could meaningfully add "local" (technological, societal) depth and explore together problems from the interconnected trans-national world of "things" (& attacks, impact, enforcement) where synergy would be very beneficial to jointly influence and leverage issues for all concerned. An International Advisory Group (IAG) is being set up within BIC in order to maintain and strengthen the EU's international collaboration links with participant countries, Brazil included.

The audience at the workshop was very enthusiastic and interested to collaborate together on future networking opportunities in Trustworthy ICT, for example in call 8 of FP7, as in other topics, i.e. the bilateral coordination for the enhancement of S&T Partnerships (FP7-INCO-2012-2, BILAT).

Annex 1 Final Terms of Reference and Program

Workshop on **Building a long term International strategy in Trustworthy ICT**

BIC Project – more details can be found here http://www.inatel.br/iwt/slide-show/bic-workshop

Main Themes:

The BIC workshop will focus on the need for an international approach to deal with Research and Technological Developments (RTD) to deal with research challenges and open issues related to all areas related to Trustworthy ICT.

Terms of Reference:

- To capitalise on the presence of a large group of research communities from Brazil and around the world present at IWT 2011, the BIC session is held the day before on 3rd May 2011;
- Understand the status and objectives of programs supported by EU and Brazil in all areas of Trustworthy ICT;
- Highlight potential collaboration subjects that are mutually beneficial and require further Brazil-EU collaboration for ensuring Trustworthy ICT, including security, privacy and trust against borderless cyber attacks;
- Share information about international projects and initiatives already underway in Brazil and Europe and begin to generate ideas for new ones;
- Decide next steps for the collaborations.

Session A

1. Building a long term strategy for International cooperation in Trustworthy ICT between EU and Brazil, Speaker: Jim Clarke, Waterford Institute of Technology

2. Digital Identity in Brazil, Speaker: Noemi Rodriguez, PUC-Rio/RNP

3. Trustworthiness in Cloud Computing, Speaker: Neeraj Suri, TU Darmstadt

4. Data protection and Privacy issues and challenges: A Brazilian perspective, Speaker: Danilo Doneda, CTS-Fundação Getúio Vargas

5. Questions and answers

Session B

1. Future Internet in Europe: an overview of related initiatives and ICT security challenges, Speaker: Aljosa Pasic, Atos Origin, Spain

2. Research issues for security in Future Internet, Speaker: Celia Ghedini Ralha, University of Brasilia

3. New models of communication and security for the Future Internet, Speaker: Michel Riguidel, ENST , Paris

4. Future Internet: New Network Architectures and Technologies Speaker: Christian Esteve Rothenberg, Fundação Centro de Pesquisa e Desenvolvimento (CPqD), Campinas, Brazil.

4. Open discussion, questions and answers

5. Wrap-up and closing

Annex 2. List of registered IWT attendees

Name	Surname
Marcelo	Alencar
Mathieu	Boutin
Roger Fredy	Larico Chavez
Ahmed	Barnawi
Reuben	Shar
Fernando	Pinotti
Raul	de Lacerda
Warley	Junior
Ronaldo	Aparecido de Abreu
Joao	Mendes Filho
Miguel	Arjona Ramirez
Rodolfo	Vertamatti
Luis Henrique	Gibeli
Gina	Quelal
Joao	Alves
Kira	Kastell
Thiago William	Capucin
Max	Costa
Djeisson	Thomas
Ozgur Koray	Sahingoz
Luiz	da Silva Mello
Luis Fernando	Abanto Leon
Charles	Despins
Dr. Karoly	Farkas
Jeferson	Stenico
Fernando	Andrade
Marcio	Dantas
Aldebaro	Klautau
Jose Candido	Silveira Santos Filho
Andrei	Legg
Carlos Daniel	Altamirano
Luis Otavio	Mataveli
Jose Alexandre	Nalon
Clauirton	Siebra
Ana Gloria	Mamani Chipana
Tiago	Cariolano de Souza Xavier
Anderson	Lima
Nilson Maciel	de Paiva Junior
Marcelo Portela	Sousa
Catia	Valdman
Rodrigo	Lima
Ewerton	Castro
Valderez	Donzelli
Anderson	Nunes
Victor Andre	Pinho de Oliveira
Yuzo	Iano
Bernardo	David

Gustavo	Nozella Rocha
Nelson	Neto
Luiz	Caldeira
Marcos	Mokarzel
Juraci	Galdino
Geraldo Gil	Ramundo Gomes
Carlos	Ynoguti
Estevan Marcelo	Lopes
Carlos Augusto	Rocha
Andre	Abbade
Antonio Marcos	Alberti
Luciano Leonel	Mendes
Carlos Nazareth	Marins
Marcelo	Carneiro de Paiva
Rausley	Adriano Amaral de Souza
Firmiano	Perlingeiro
Marcello	Costa
Carlos Vinicio	Rodriguez Ron
Karine	Carbonaro
Dayan Adionel	Guimaraes
James	Clarke
Neeraj	Suri
Jorge	Souza
Michel	Riguidel
Jose Marcos	Camara Brito
Eduardo	Rosa
Robson	Prado
Lesley Beethoven	Rodrigues Mendes de Jesus
Weldisson	Ferreira Ruas
Bruno	Magalhaes
Vinicius Lourenco	Dias Ferro
Thales Antonio	Fernandes Valerio
Tiago	Marins
Sandro	Gatti
Wania Danielle	C. Konageski
Wagner Anilton	Almeida
João Alfredo	Cal Braz
Marcela	Murad
Ana Cristina	Gomes Ribeiro
Aline	Lima Monteiro Machado
Carlos	Santos
Renato	Baldini Filho
Tania Regina	Tronco
Christian Esteve	Rothenberg
Shu	Lin
Hiroaki	Harai
Otto	Strobel
Cassiano	Pizzolato Rosa
Luciano Ferraz	Jurioli
Agostinho	Vaz
Aljosa	Pasic
Célia	Ghedini

Noemi	Rodriguez
Danilo	Doneda
Eduardo	Tavares Leite
Ricardo	Marques Ribeiro
Hrvoje	Bosnjak
Ulku	Arga
Luisa	Silva Costa
Lee	Ling
Antônio	Amorim
Edson	Ferreira Suisso
Luiz Eduardo	da Costa Martins
Telma Lúcia	Alcântara da Costa Silva
Fabiano	Rego Pereira

Annex 3. Presentations made during the workshop

Available from http://www.bic-trust.eu/events/eu-brazil-cooperation-workshop/

1. Building a long term strategy for International cooperation in Trustworthy ICT between EU and Brazil. Jim Clarke, Waterford Institute of Technology, Ireland

2. Digital Identity in Brazil. Noemi Rodriguez, PUC-Rio/RNP

3. Trustworthiness in Cloud Computing. Neeraj Suri, TU Darmstadt

4. Future Internet in Europe: an overview of related initiatives and ICT security challenges. Aljosa Pasic, Atos Origin, Spain

5. Research issues for security in Future Internet. Celia Ghedini Ralha, University of Brasilia

6. New models of communication and security for the Future Internet. Michel Riguidel, Telecom-ParisTech, Paris, France

7. Future Internet: New Network Architectures and Technologies Speaker: Christian Esteve Rothenberg, Fundação Centro de Pesquisa e Desenvolvimento (CPqD), Campinas, Brazil.