



Future Internet Assembly, Stockholm, Nov 23/24 2009

Trust and Identity Track

FIA T&I Caretakers: Jim Clarke (WIT), Volkmar Lotz (SAP), Nick Wainwright (HP)

Executive Summary

Three Trust and Identity (T&I) sessions were organised within FIA Stockholm: Session I.2. *Approaches for e-Identity provisioning in the Future Internet*; Session II.2. *How to Measure Trust*; and session IV.3. *Trust and Identity* plenary session at which the T&I community working with the caretakers planned the programme for FIA Valencia and beyond. In addition, the FIA Caretakers contributed towards the FIRE and Smart Cities tracks. The FIA Trust and Identity sessions built on the [Preparation Workshop](#) FIA Trust and Identity workshop held in Brussels on 7th October 2009, which prepared the topics oriented tracks for FIA Stockholm.

Session I.2 Approaches for e-Identity Provisioning in the Future Internet.

Previous FIA events in Madrid (Dec 2008) and Prague (May 2009) addressed ID management for the Future Internet and Identity provisioning in the Future Internet (FI). FIA Stockholm (Nov 2009), building on the [Preparation Workshop](#), focussed on cross domain topics, recognising that all layers in the Future Internet stack – networks, services, applications, devices and terminals (sets of devices), and content – make use of identifiers and identifiable information.

The objective of the FIA Stockholm session was to provide an opportunity for the networks and the services/applications communities to lay out their motivation and challenges associated with their approaches to eID provisioning in the FI and to provide an opportunity for the communities to start discussing and debating their approaches with the aim of establishing a common ground for the evolution and broadening the scope of eID provisioning across the layers. The following challenges were identified:

- The need for embedded security and privacy at all network levels;
- Identity and entity based routing and symmetrical relations between users and providers;
- Future network architectures with communication setup and routing that are identity-data-aware only as necessary for the functions of the network without making the related users identifiable;
- A coherent and comprehensive framework for handling all aspects of usage and management of eID from the bottom to the top of the stacks;
- Close collaboration between researchers to maximise integration and consistency of approach;
- Global cooperation in line with the recommendations in the [RISEPTIS report](#).

It was recommended that the research communities continue to focus on achieving short, medium and longer term concrete results in these challenges / approaches highlighted above. The short term, in particular, should be a focus for ongoing work to be presented at FIA Valencia where the PPP on FI will be formally launched.

Session II.2 How to Measure Trust

While the question of how to measure security and trust related properties for networks systems and services, and how to build and adapt security and trust solutions based on risk considerations and economic aspects has frequently been touched in discussions at previous FIA events, this was the first time that a dedicated session had been set up to present expert views on the topic and to discuss it. Taking its truly cross-domain nature into account, the objective of the session was to explore the various dimensions of trust and security measurements and related metrics, in order to identify the scope, the relevant research challenges and the path towards meeting them. The importance of measurements arise from the fact that the Future Internet (FI) is unlikely to be a perfectly secure and trustworthy place everywhere and anytime, and that users will need to make trust decisions based on incomplete and uncertain information, including an assessment and prediction of current and future risks.

The session focussed on questions of what can and needs to be measured, how social- and economic-based models of trust will scale, and what can be the targets of measurement. The presentations showed promising results on various aspects of security and trust measurements in focused research efforts. This immediately raised the questions on how this research can be scaled to Future Internet dimensions in order to exploit the approaches for FI networks, services and applications. To do so, three essential points related to the

presented results were addressed in the discussions:

- Do results on trust experiments scale from the laboratory environment to the real worlds of the Future Internet?
- Can security predictions be generalised across different software components, programming languages, systems, environments?
- How to collect and share security-related data for experimental research in the line of the work presented?

Future work is needed to address the challenges related to publishing data in a transparent yet confidential and privacy preserving way to have solid grounds for building advanced theories. The discussions showed the interest in the topic as well consensus on measurements being the basis for an economically based approach to a trusted and trustworthy Future Internet, concluding that the major challenges that should be addressed by a Future Internet Research agenda are scalability and the provision of a sound database for experimental evaluation. It is suggested to continue the discussion along these lines, preferably with a stronger integration of the socio-economics and experimental facilities community.

Session IV.3 Trust and Identity plenary: Planning for FIA Valencia and beyond.

The Trust and Identity 'plenary' brought together the T&I research community to discuss and review the FIA T&I tracks that we have been participating in, to review the FIA processes and consider what actions and steps should be taken to further improve the effectiveness of participation in FIA, and to consider what activities should be scheduled for upcoming FIA event in Valencia and beyond.

The opportunity to have less formal working sessions in between the FIA events has contributed to ensuring that the T&I research community works well together. The T&I caretakers held a preparatory workshop on 7 Oct. 09, which had helped considerably to plan for and create worthwhile sessions and real progress at FIA Stockholm. It was agreed to hold another interim preparation event between FIA Stockholm and FIA Valencia (during February 2010) to address these topics, and that planning for this event will start right away.

In general, it was felt that the cross domain interactions were valuable, and that this should be emphasized with more opportunity for this kind of interaction. The session structure created by the caretakers for the Trust and Identity sessions for FIA Stockholm enabled a wide range of researchers from both within the T&I field and across the other research domains to contribute and interact. It was noted that to maintain momentum would require follow-up after the FIA events; For example, through collaboration on position papers (even if controversial!) and that the opportunity to submit papers to FIA would be valuable. It was felt that there is a need for more information about FIA, the expectations of the Commission for FIA, and goals that they have for FIA to be communicated to the FIA signatory project communities and also to communities outside FIA.

Finally, discussion of the upcoming topics for FIA Valencia concluded by identifying three topics that are priorities for the Future Internet and which would benefit from cross-domain attention through the Future Internet Assembly:

- 1) There should be continued work on e-Identity provisioning, focussing on Privacy and ID provisioning across the layers, and looking at the short, medium and long term issues, including considering how network infrastructure evolves and their impacts on the topics;
- 2) In the Future Internet, it is important to consider what new threats will emerge that will demand new and different security approaches. Therefore, Security for the Future Internet is a topic that should be addressed through a cross domain approach in FIA;
- 3) The perspective of the user and how to engender Trust for the Future Internet in the user of the systems and services of the Future Internet was considered to be the third important topic for Valencia, building on the work in FIA Stockholm.

Authors: Jim Clarke, Volkmar Lotz, Nick Wainwright. December 2009.

The next sections provide the detailed reports for the individual sessions.



Session I.2. Approaches for e-Identity provisioning in the Future Internet (23 November 2009, 11:15 – 12:45)

Objectives for the session

Overall Chair - Jim Clarke, Waterford Institute of Technology, IRELAND, FIA Trust and Identity Caretaker, co-author of the [Problem statement on Identity Provisioning](#)

Background to the session

FIA Madrid (December 2008) – session concentrated on *ID management for the FI*.

FIA Prague (May 2009) – session concentrated on *Identity provisioning for the Future Internet* including Identity and claim frameworks and platforms plus interesting applications and trials in the pipeline.

Caretaker's preparations for FIA Stockholm – new approach taken for dividing up sessions: enable more cross domain interactions; split sessions along topics rather than the FIA domains/clusters; volunteers to write **problem statements** for topics to be addressed in the identified sessions.

"Identity" topic originally *ID Management, including routing and addressing in the Future Internet*; **problem statements**: good mix of cross domain approaches towards broadening scope of eID management and provisioning in FI across the multiple levels/stacks – networks, services, applications, device and terminals (set of devices) and content; also minimum requirements for identifying user(s) when accessing a resource. Included also privacy and usability aspects of eID.

Preparation Workshop (for Stockholm), Brussels 07-OCT-2009, set up by Trust and Identity caretakers: to progress and clarify topics. There was productive debate between networks and services/applications communities on approaches for eID, and agreement that the FIA Stockholm session should be renamed **I.2 - Approaches for e-Identity provisioning in the Future Internet** focussing on the following **objectives**:

- Provide opportunity for the networks and services/applications communities to lay out their motivation and challenges associated with their approaches to eID provisioning in the FI;
- Provide an opportunity for the communities to start discussing and debating their approaches;
- Identify the key personnel, projects and initiatives in the fields;
- Enable the focus on whether there are synergies or consistencies to the points of view;
- Identify any gaps between the approaches and best way to fill these together;
- Look at the feasibility of establishing a common ground for the evolution and broadening the scope of eID provisioning across the layers;

Key points from presentations

Panel Chair - Marcus Brunner, NEC Labs Europe, GERMANY (FIA MANA Caretaker, co-author of [Problem statement for Identity Provisioning](#))

Question to the panellists about whether we must look at this topic as a cross cutting one: all layers require identification of some sort, perhaps with different 'security properties'; all layers require some sort of routing, finding and discovery; therefore, implies answer is YES.

The concept of eID as a Cross Stack or Intra-Stack solution was defined: Cross-stack identification solutions are working across stacks where Identity Management is a modular piece (service); functionality is not duplicated (cross-layer optimization); but binding between stacks has privacy implications. This solution also would not fit as well with the onion principles use in many security solutions.

The Intra-Stack solution keeps eID very near to the service/application itself with targeted mechanisms and protocols. eID information would be isolated from other stacks where possible e.g., determine time when an individual is at home by analysing energy consumption via smart meters, sensing information content or their Internet usage pattern, etc..

Clearly, there are privacy and usability issues that need to be addressed, and users need to be educated as there is a lack of knowledge at present.

Ricardo Azevedo Pereira, Portugal Telecom, PORTUGAL presented the motivation for a networks-based or converged approach to eID for the Future Internet. The trends for the *Future Internet* are towards larger, more heterogeneous and diversely, dynamically federated environments, with eID operation and management across all the whole space. eID use and management functions are currently spread across all layers of the

Internet. This is unworkable as there is no common understanding of eID at the different layers, services, applications, devices, etc. Present Internet protocols were not designed for current rich and complex service environments. The identity-related operations at different layers cannot be combined or associated except by the applications that use them. The same problem applies across multiple applications that are part of the same complex *task*. This fragmentation prevents optimization in terms of resources, security, session mobility and even presentation to the user. A further problem is multiple identities in the same terminal – who is doing what? Regarding addressing and identification, a digital entity is tightly coupled to its delivery channel and device so that reach-ability is not independent of devices. This does not support dynamically compounded identities/identifiers and will lead to identifier/locator overload, resulting in interdependency between the identity of an end-host and its location. A number of challenges were identified that address these points: addressing accountability, the need for a privacy-friendly, trustworthy, device independent, network-independent connectivity; enabling *ad hoc* collaboration without neglecting privacy and trust – Federation; Identity based routing and symmetrical relations between users and providers enabling entities to communicate across different domains using locator-independent identifiers, without being subject to limitations of IP, and ensuring a proper treatment of mobility, multi-homing, and multi-domain policy negotiation. Communications should take into account the intended task, and not the layers involved.

Amardeo Sarma, NEC Labs Europe, GERMANY presented research challenges associated with the networks approach to eID in the Future Internet. Mr. Sarma stressed the need for functions and operations ‘with the user in mind’, especially when dealing with objects (things), multiple identities/roles and multiple devices. Privacy and data protection must be addressed enabling OECD guidelines on privacy across the layers. Mr. Sarma stressed that the research communities must carry out work to enhance both functionality and privacy at the levels of network and service enablers. There is already pioneering work in these areas of privacy across the layers in EU research projects SWIFT, iNEM4U and DISCREET projects.

Identity-related data exists in the network today, e.g., IP and MAC addresses that can be associated (possibly wrongly) with individuals or locations. The question is how to use identity information in the network while maintaining a maximum of privacy – more than today!

We need to arrive at a solution that gives the better of two worlds!

1. Make it impossible (difficult) to link partial ID to entity → privacy;
2. Maximize ability of partial ID to support functions & operations → functionality.

In order to accomplish this, digital identities should be part of the future network architecture such that the communication setup and routing should be identity-aware *for the needed functions of the network* without making the related *users* identifiable. This should ensure better privacy and security than available today. Mobility is required to maximise the capabilities of the network by providing it with enough information, for example, having identities representing entities and not only devices and identities across terminals considering security and other capabilities enabling use of arbitrary (public) devices. It is also necessary to maximize the capabilities and scalability of the network by providing it with (personally non-identifiable) locally relevant data about intended use.

Mr. Sarma concluded with suggestions on how to carry out R&D in order to “tame the beast” of Identity with possibly personally identifiable data rather than ignoring it or putting our heads into the sand. This would require investigation of the scope of using Identity data in the network in such a way that there is an increase in functionality and associated usability while increasing privacy and security, in particular, managing identification across the layers. Some approaches to discuss and compare as starting points could be an evolution of the Host Identity Protocol and/or creation of Communication Sessions in the network amongst others.

Simone Fischer-Hübner, Karlstad University, SWEDEN presented the motivation for Services/Applications approaches for eID. The challenges associated with privacy and security were highlighted especially in terms of global networks issues related to cookies, spyware, location-based services, ambient intelligence, RFID, and especially social networks. The approach taken by the PRIME project was presented i.e., privacy-enhancing identity management – partial identities based on audience segregation where users reveal different (partial) identities based on their current roles/relationships. It is an integrated approach taking into account data-minimisation, assurance and life cycle management and transparency.

Prof. Fischer-Hübner concluded with an introduction to the PrimeLife project, which is looking at Sustainable Privacy and Identity Management to Future Networks and Services. This relates to the understanding of privacy-enhancing identity management ‘for life’, bringing Privacy to the future web/social networks and research on Policies, HCI, and Infrastructures. The project is also addressing “Beyond data minimization” by addressing data-intensive scenarios and user-generated content (Web 2.0, virtual communities such as Friendster, SecondLife) and has a goal of making privacy-enhancing identity management widely available.

This involves looking at the required infrastructures, Open Source, and Standards, cooperation with other Projects (Master, TAS3, SWIFT,...), and emphasis on education (summer schools, ...).

Kai Rannenberg, Goethe University Frankfurt, GERMANY made a presentation on behalf of himself and **Jan Camenisch, IBM Zurich, SWITZERLAND**, who sent apologies due to not being able to travel. The presentation centred on PETs – privacy enhancing technology from both the approaches of the PrimeLife and PICOS project perspectives. Regarding the network layers, Professor Rannenberg questioned whether anonymous routing should be the default for the Future Internet? It was discussed how we need some ‘cultural discussions’ about this. On whether there is a need for an ‘identity plane’ that spans the layers, there was a question about whether this is instead based more on business model needs (to expand business role between the layers) rather than a technology issue. Prof. Rannenberg asserted that perhaps it is not the technology that is in conflict with privacy but more the business model motivations and efforts that are in conflict with privacy aims. The PICOS project has a particular focus on user centric concepts and has found that within particular communities (angling and transport), people like to share certain information in certain contexts. In a ‘mobile’ community, you might meet someone you only expected to know in a virtual community. There is a need for partial identities and a further limited set of information for each partial identity to cope with these scenarios.

Discussion

There was a lively discussion session and the following summarises the points raised.

The need for more focussed research on Accountability: we need to look at the underlying assumption that ‘whatever is stored, or can be stored, needs to be provided to law enforcement’ as a social issue. Another issue now is that there is a significant change in the costs paradigms of capture/store/use of information; in the past, it was hard to capture and retain information. Conversely, nowadays, it is hard to discard information.

Point raised about the ID being addressed across the layers due to the thrust from business interests rather than technology reasons. The response was that there are real problems and issues in the network today that need to be addressed by the research communities. For example, it is possible to link data across layers (Mac, IP, application). The idea of drawing up a linkages matrix for identity/identifiers/attributes spread across the layers was discussed and it was agreed the networking and services/applications research communities could come together and look at each and every element and discuss what is needed and why. There is already a cluster group called PrimCluster made up of a number of projects working together on some of these related issues.

What is meant by “Maximum of privacy or appropriate amount of privacy”: The response was that it means the minimum amount of information flowing to the network layers to achieve what is required. This also depends on certain things eg. context of the situation and the desired applications. It refers to the data of overall intention and only pieces needed to set up a services and connection. It has to be noted that there are also costs involved – how far are we prepared to re-engineer the Internet to provide more privacy? For example, it will cost to have ‘anonymous routers’ and new overlays, underlays, etc will be needed. At the application layer, the extra costs will depend on what the application and the context is.

Closing remarks of panellists. The session participants were asked to give their closing remarks on what they felt was a good approach going forward. In summary, the responses were:

- Need to branch out further than Europe and take account of global perspectives;
- Look at the more complicated environments also and pay attention to usability issues eg. Cloud computing environments;
- More coordination needed between network and services/applications researchers;
- Let’s just do it (have communities identify and discuss the cross layers issues related to identities/identifiers/attributes).

Conclusions and Next Steps towards Valencia

In conclusion, the session generated a lot of interest and was very well attended with over 100 participants.

Summary of challenges identified in this session:

- The need for **embedded security and privacy** at all network levels, and in every operation – discovery, identity validation, session setup and management, routing, network transport, signalling.
- **Identity and entity based routing** and **symmetrical relations between users and providers** enabling entities to communicate across different domains using locator-independent identifiers, without

being subject to limitations of IP, and ensuring a proper treatment of mobility, multi-homing, and multi-domain policy negotiation. This would require trustworthy identity discovery and validation mechanisms that use the identity of the entity, and not the machine and/or network point-of-attachment/interface, to address as the communication endpoint.

- **Future network architectures** with communication setup and routing that are **identity-data-aware only as necessary for the functions of the network without making the related users identifiable**, coping with “Identity” data in the network in such a way that there is an increase in functionality and associated usability while increasing privacy and security, in particular, managing identification across the layers. Some approaches to discuss and compare as starting points could be an evolution of the Host Identity Protocol and/or creation of Communication Sessions in the network, amongst others.
- **A coherent and comprehensive framework** for handling all aspects of usage and management of eID from the bottom to the top of the stacks. This should include administrative aspects (creation, provision/registration, revocation of identities, and the management of attributes); operational aspects (how eIDs and their attributes are used, controlled, protected, and monitored - including accountabilities – paying particular attention to the need for interoperability on the widest scale; the supporting abstract services to provide interoperability; and the access controls by (productive) networked services based on eID.
- **Close collaboration between researchers to maximise integration and consistency of approach.** The panellists recommended working together to develop a matrix of identity, identifiers, attributes and linkages information at each level, and identify what is needed (and not).
- **Global cooperation** is needed especially in this topic, which is very much in line with the recommendations in the [RISEPTIS report](#).

After the discussions, the session went on to consider the headline “problem statement” to carry forward to FIA Valencia. It was recommended that the research communities continue to focus on achieving short, medium and longer term concrete results (short term in particular to be presented at FIA Valencia where the PPP on Future Internet will be launched). To do this, it was agreed that the participants would work together on answers to the important questions posed in the challenges above.

Can we identify:

- convergence of the approaches?
- consistency/synergies of the approaches?
- gaps between the approaches?
- issues associated with the approaches?
- (Joint) solutions associated with the approaches?

In addition, have we achieved enough cross-domain interactions on the topic? (*Answer: probably not, but a good start with T&I and MANA but should now incorporate Content, RWI, IoT. ... in the next phase*)

It was agreed to hold another interim preparation event between FIA Stockholm and FIA Valencia (during February 2010) to address these topics, and that planning for this event start right away.



Session II.2. How to Measure Trust (23 November 2009, 14:15 – 15:45)

Objectives for the session

Overall Chair – Volkmar Lotz, SAP Research, FRANCE, FIA Trust and Identity Caretaker, co-author of the [Problem Statement on Trust Measurement](#)

While the question of how to measure security and trust related properties for networks systems and services, and how to build and adapt security and trust solutions based on risk considerations and economic aspects has frequently been touched in discussions at previous FIA events, this was the first time that a dedicated session had been set up to present expert views on the topic and discuss it. Taking its truly cross-domain nature into account, the objective of the session was to investigate in the various dimensions of trust and security measurements and related metrics, in order to identify the scope, the relevant research challenges and the path towards meeting them. The importance of measurements arise from the fact that the Future Internet (FI) is unlikely to be a perfectly secure and trustworthy place everywhere and anytime, and that users need to make trust decisions based on incomplete and uncertain information, including an assessment and prediction of current and future risks. Following the key points of the problem statement:

- FI business and social opportunities will only be realised if the FI can be trusted,
- Trust is a subjective decision related to the specific context, thus, individuals and entities need to capture (i.e., measure) all relevant parameters for this decision,
- These parameters include the value of a transaction, the associated risk, the trustworthiness of a service / infrastructure, and others,
- The complexity, flexibility and dynamics of the FI increase the difficulty of trust evaluation
 - in terms of capturing the relevant context information,
 - in terms of defining and applying the adequate metrics,
 - in terms of probing a system in order to execute measurements,
- Trust decisions are made by end users,

The session was designed to focus on questions of what can be and need to be measured, how social and economic models of trust scale, and what can be the targets of measurement.

Key points from presentations

The format of the session was chosen to provide a deeper dive into two quite different types of measurements and their evaluations, aiming to facilitate the discussion of types and targets of measurements and the current state of the art.

Claudia Keser, University of Goettingen, GERMANY, demonstrated how game-theory based economic experimentation can be effectively used to measure how reputation systems influence trust decisions and trustworthiness of people conducting transactions over a network. Based on classical trust experiments (Berg, Dickhaut, McCabe, Games & Economic Behavior 1995), where trust is defined as initial investment of a buyer, and trustworthiness as a seller's return, she reported on the design and execution of extended experiments that were able to show that the presence of a reputation system measurably increases both trust (i.e., increase investments of buyers in the game) and trustworthiness (i.e., increases return by the sellers in the game). This demonstrates that people are sensitive to reputation-based social control mechanisms, with similar effects on interaction with unknown people in short-term relations as can be observed for interactions with established partners. The results also help to design reputation systems in an effective way by providing a means to compare different reputation system instances. Future work will investigate different control mechanisms and are likely to provide the grounds for decision support on mechanism selection in different risk contexts, taking economical considerations into account. The understanding of how users perceive trust and trustworthiness of online interactions and adapt their behavior depending on the security and trust features is considered an essential contribution to the understanding of how a trusted Future Internet can be built in an economically feasible way.

Stephan Neuhaus, University of Trento, ITALY, emphasized the importance of security and vulnerability predictions. In the complex scenarios of the Future Internet, it is important to be able to estimate those areas and components where security vulnerabilities are likely to occur and provide pointers to where scarce and

precious resources for security analysis and hardening the environment should be spent most effectively. Investigations in Mozilla Firefox, RedHat Linux and CVE vulnerabilities showed that empirical security data, and analytical data on component dependencies and inclusion relations fed into machine learning algorithms allow identification of potentially vulnerable components with a significantly larger probability than random choice:

- “Tell me what you include and I’ll tell you how vulnerable you are.”
- “Tell me your dependencies and I’ll tell you how vulnerable you are.”

The success of these investigations gives rise to the vision of a “security weather forecast”, where empirical data and measurements can be used for robust predictions and forecasts of security critical events and components. Nevertheless, it is important to choose the right metrics and to present them in their context.

Discussions

The presentations showed promising results on various aspects of security and trust measurements in focused research efforts. This immediately raised the questions on how this research can be scaled to Future Internet dimensions in order to exploit the approaches for FI networks, services and applications. In order to do so, three essential points related to the presented results were addressed in the discussions:

- Do results on trust experiments scale from the laboratory environment to the real worlds of the Future Internet?
- Can security predictions be generalised across different software components, programming languages, systems, environments?
- How to collect and share security related data for experimental research in the line of the work presented?

Future work is needed to address the challenges related to publishing data in a transparent yet confidentiality and privacy preserving way to have solid grounds for building advanced theories.

Conclusions and Next Steps towards Valencia

In conclusion, the session was well received and generated a lively discussion. Feedback received expressed appreciation for the approach to focus on few deep-dives on diverse aspects of the broad topic for the first inter-disciplinary session. The discussions showed the interest in the topic as well consensus on measurements being the basis for an economically based approach to a trusted and trustworthy Future Internet.

The discussions concluded that the major challenges that should be addressed by a Future Internet Research agenda are scalability and the provision of a sound database for experimental evaluation. It is suggested to continue the discussion along these lines, preferably with a stronger integration of the socio-economics and experimental facilities community.



Session IV.3. Trust and Identity Session (24 November 2009, 09:00 – 11:00)

Objectives for the session

Session IV.3 was the Trust and Identity 'plenary' which brought together the T&I research community to discuss and review the FIA T&I tracks that we have been participating, to review the FIA processes and consider what actions and steps should be taken to further improve the effectiveness of participation in FIA, and to consider what activities should be scheduled for upcoming FIA event in Valencia and beyond.

Summaries of FIA Stockholm activities

Jim Clarke gave a recap of the e-Identity provisioning session and Volkmar Lotz gave a summary of the 'Measuring Trust' session, both covered earlier in this report.

Nick Wainwright presented a summary of the FIRE session at which the use of experimental facilities for Trust and Security were explored, and of the Smart Cities track which he co-organised.

In the **FIRE Session**, Nick Wainwright, HP Labs, UK, [presented a perspective](#) commenting on the range of areas where experimental facilities might be of value in experimental research in trust and security concluding that whilst much trust research required experimentation with end users, there was scope for using large scale experimental facilities to explore behaviour and response of systems to attack, and that where 'risky' experiments were being conducted, such as large scale attacks on systems or release of malware these would need to be conducted within an isolated facility. Mauro Campanell, GARR, Italy, gave a presentation on '[Deploying Isolated Testbeds on Federica](#)'. It is clear that these kinds of experimental facilities can provide a safe place for testing attack scenarios at network and service levels, and that Federica does provide a way to create isolated environments, and that it could be used to conduct experimental research that explored the resilience of systems and protocols under attack.

Nick Wainwright observed that the Smart Cities session speakers who were engaged in creating 'smart cities' uniformly emphasised that digital technologies should be deployed to solve real problems and were wary of 'technology push'. Nevertheless there was a hint that horizontal platforms had potential benefits in smart cities environments as many sectors addressed have some common needs. Applications spanned community building, transportation, digital industries, energy, buildings, and urban planning. Fiona Williams, Ericsson, presented a perspective on infrastructure for smart cities that would be a platform for connectivity and interoperability. Nick observed that will be much need for trustworthiness to be considered at the heart of smart city infrastructure and services and that this could provide valuable use cases and scenarios to explore in the future.

Review of FIA processes

The group reviewed the FIA processes with the following observations.

Working sessions between FIA events: The opportunity to have less formal working sessions between the FIA events would be helpful to ensure that the T&I community works well together. The T&I caretakers had held a preparatory workshop on 7 Oct. 09 prep workshop which they believed had helped considerably to create worthwhile sessions and real progress at FIA. It certainly made the caretakers feel less stressed in the period just before the FIA Stockholm event as there was a considerable amount of early preparations.

In general, it was felt that the **cross domain interactions were valuable**, and that this should be emphasized with more opportunity for cross domain interactions. It was also suggested that more people should be able to contribute and to 'have their say', not just the FIA caretakers; a comment which the FIA caretakers wholeheartedly supported!

It was noted that to maintain momentum would require **follow up after the FIA events**, e.g. to collaborate on position papers even if controversial and that the opportunity to submit papers to FIA would be valuable.

It was felt that it is important that **more information about FIA**, and the expectations and goals of the Commission for FIA be communicated to the FIA signatory projects, but also outside that immediate community.

Topics for FIA Valencia

Finally, discussion of the upcoming topics for FIA Valencia concluded with selecting

- 1) **eIDentity provisioning** should focus on Privacy and ID provisioning across the layers, and looking at the short, medium and long term issues, including considering how network infrastructure evolves;
- 2) **Security for the Future Internet.** The group felt strongly that in the Future Internet, it is important to consider what new threats will emerge that will demand new and different security approaches. Topics to be considered included secure SW engineering, systematic approaches, security by design, and that we should also address social and economic aspects, user interface and usability issues and consider legal connection with privacy and ID provisioning (responsibility, due processes, etc.);
- 3) **Trust for the Future Internet.** The perspective of the user and how to engender trust by the user of the systems and services of the future internet were considered to be the third important topic for Valencia. Involving the user in the process, reasonable expectation management, helping the user make informed decisions based on awareness, tools allowing users to monitor what happens, and tools to deal with outcomes, transparency of procedures and undoing transactions, user interface issues such as how to display warnings and how to enable users to take appropriate actions were all discussed as topics to be considered.

It was agreed that an interim meeting to prepare these topics would be of value and should be actively considered on the schedule.

Session Notes compiled by the Trust and Identity Caretakers: Jim Clarke, Waterford Institute of Technology; Volkmar Lotz, SAP Research; Nick Wainwright, HP Labs.

Acknowledgements: *In addition to all of the speakers and attendees, the T&I caretakers would like to especially thank all those who helped with the problem statements and the organisation of the FIA Stockholm sessions and the [preparatory workshop](#) especially Keith Howker (WIT-TSSG), Kieran Sullivan (WIT-TSSG), Brian Foley (WIT-TSSG), Michel Riguidel (ENST), Philippe Laurier (ENST), Artur Hecker (ENST), Dieter Sommer (IBM Zurich), Marcus Brunner (NEC Labs Europe) and Syed Naqvi (CETIC). Also the European Commission Trust and Security and Software and Service Architectures and Infrastructures Units for their continued support.*