**Trust and Identity Breakout Sessions**
**9th December 2008 – 11:30 - 16:30**
**Venue: ETSIT, UPM Madrid**
**Session Report**

European Commission
Information Society and Media

Authors: Jim Clarke, Zeta Dooly, Kevin Quinn, Waterford Institute of Technology,
Volkmar Lotz, SAP, Nick Wainwright, HP, Michel Riguidel, ENST, Martin Potts,
Martel,…

# TABLE OF CONTENTS

# BACKGROUND

The Internet has become a crucial element of our economy and societies. Its evolution and how Internet has to respond to future challenges is at the core of the current discussions, with the need to strike the right balance between different and sometimes diverging interests between providers, users, communities, businesses. A Future Internet Assembly (FIA) was launched by the European Commission in April 2008 at Bled, Slovenia. This conference and technical workshop was the first European high-level event with the objective to raise awareness of European Member States on the need to dedicate resources to R&D efforts towards the Future Internet and reinforce the European Commission in its leading role.

The second Future Internet Assembly took place in Madrid on the 9th and 10th December 2008, this report details the discussions and outcomes from the Trust and Identity and Privacy break-out sessions. The overall objectives of the Madrid FIA The main aim of the Madrid technical workshop was to progress discussion on cross-cutting issues of common interest resulting in documenting through generation of position papers <u>the state of play, research orientations and possible integration paths towards the future internet, accompanied by a roadmap with milestones</u>, to be supported by the attendees.

An organizing committee (OC) for the FIA was established where a call for proposals of sessions was announced, 7 BO sessions were proposed by the EC and accepted by the OC as a result of the integration of the 23 received proposals, of which the Trust and Identity session was included. Each break-out session established a caretaker group which consisted of many of the initiators of the proposals.

Following a number of planning meetings the scope and format for each of the sub-sessions was devised within the caretaker group, a draft position paper was distributed to all 87 projects that have signed the 'Bled Declaration' and input was solicited from these projects, As contribution from the community was highlighted as one of the main objectives it was agreed that in order to ensure project contributions were included a questionnaire [Annex A] was sent to all projects and access given to the Trust and Identity wiki [1] for input to the position paper.

Once the scope of the sessions was identified a draft agenda was compiled with suggested panelists and keynote speakers, input was sought from other break-out session caretakers to ensure experts from other domains were included in the sessions so that the use cases discussed could generate some discussion /debate on challenges and solutions within a cross-domain perspective.

The presentation slides are available online at;
http://www.think-trust.eu/general/news-events/test.html

## INTRODUCTION

Two Breakout (BO) sessions were held on 9th December 2009 at the FIA conference in Madrid specifically identifying Trust, Identity and Privacy scenarios and consequent challenges faced within the Future Internet. Following the successful ICT Security BO session in Bled during April 2009, the FIA caretakers of the Trustworthy ICT areas decided to focus on the Trust, Identity & Privacy) areas for the FIA Madrid sessions.

The objectives of the two BO sessions were:

- explore how the common themes in Trust (morning session) and Identity & Privacy (afternoon session) will impact representative projects from each of the different domains;

- expose the 'gaps' in the programme as a whole, for example, in what the programme is covering, between expectations and reality, between theory and practice;

- identification of and how we can use experimental facilities to test and illuminate how it all fits together in practice;

- input to our research roadmap for trust and identity in the Future Internet.

As input to the BO sessions, the caretakers sent a draft version of the position paper and roadmap accompanied by a questionnaire to all relevant Bled Declaration signatory projects to contribute, and a subsequent version was then released prior to FIA Madrid (available at http://www.future-

internet.eu/home/future-internet-assembly/madrid-dec-2008.html). The position paper and roadmap specifically describes some R&D priorities identified within the Trustworthy ICT communities and attempts to establish cross-domain support in order to ensure that a comprehensive view of Trust and Identity requirements are considered within the FIA environment. Hence, the breakout sessions would provide an excellent opportunity to facilitate further refinement of this roadmap with stakeholders participating from across all domains.

The roadmap considers a number of necessarily related and cross cutting concepts represented as five (5) distinct 'lanes' as shown in Figure 1 and their interconnections with the other domains. Within the position paper, each lane attempts to address three levels, respectively:

a) current state of the art (the "today" perspective),

b) emerging trends (the mid-term perspective)
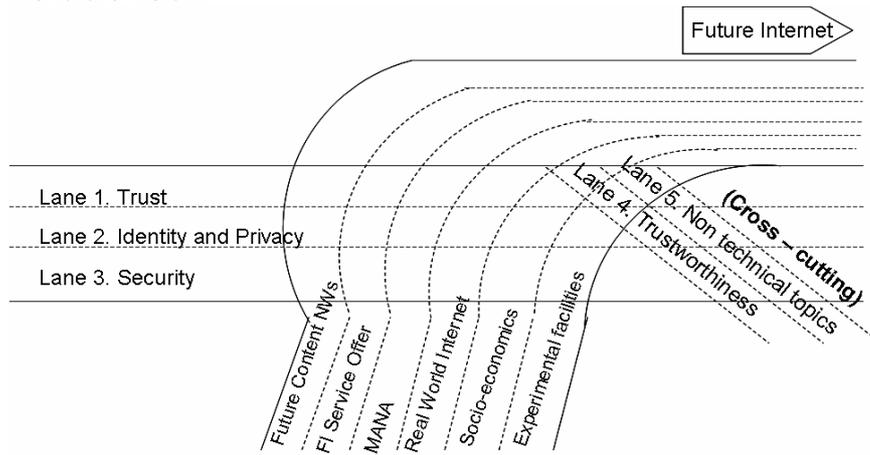
c) the future vision.



Figure 1. Trustworthy ICT Roadmap for Future Internet,

As already mentioned , the focus of the Second Future Internet Assembly (FIA) in Madrid was on lane 1, Trust and lane 2, Identity and Privacy. The intent of the caretakers is to now further develop this roadmap toward planning for the Third FIA in Prague, 11-13th May 2008. Therefore, it should be noted that these 'lanes' were not intended to limit but instead focus and frame the context for discussions in FIA Madrid and many overlaps in the discussions may emerge as concepts are often inter-connected and/or inter-dependent. The position paper and roadmap already contains some initial inputs from the other lanes and these will be further developed in the preparation activities and follow up to the FIA Prague event.

Each session used a format consisting of two inspirational keynote addresses in the relevant topics, a panel session from across the domains, with equal time for intensive discussions. The session also had a representative from FIRE Experimental facilities to present their offerings and generated useful discussions on how this offer could be taken up by the Trustworthy ICT and/or cross domain communities. In anticipation for this part of the session, all of the speakers in both sessions were instructed to use the position paper as inspiration and to explicitly include scenarios within Trust, identity and privacy areas with a view towards possible take up of the offer from experimental facilities. This proved quite useful as a number of scenarios were identified that could potentially be experimented within these facilities. Some examples highlighted during the sessions included the provisioning of identity management tools, a facility for security measurements and a network level service oriented security management system. The potential for collaboration between these communities will now continue as the available mechanisms become clearer and formalised. Finally, there was a final panel to discuss and agree the follow up activities necessary for the preparation of the third FIA event in Prague during 11-13th May 2009.


The Trust and Identity breakout sessions each had inspirational keynote speakers and panelists from the cross domain communities who were instructed by the caretakers to use the position paper in order to generate real scenarios that explicate the requirements for solutions within trust and identity areas for the Future Internet. The following sections of the report contain some content from the position paper and will not focus so much on the actual presentations, which are available for download at http://www.future-internet.eu/home/future-internet-assembly/madrid-dec-2008.html but instead will focus on the results of the two breakout sessions and the follow up activities towards FIA Prague.

# SESSION 1: TRUST (11:30 – 13:30)

## *Trust Scenarios*

A number of scenarios were presented at the Trust BO session. These are summarised below.

**Scenario 1. Cloud Computing.**

As per the slide below which generated a number of questions for discussion such as where is the data located? Who runs the services? who runs the servers?. It was generally accepted that Accountability is key but without clear legislation it is often to decipher where the accountability lies.
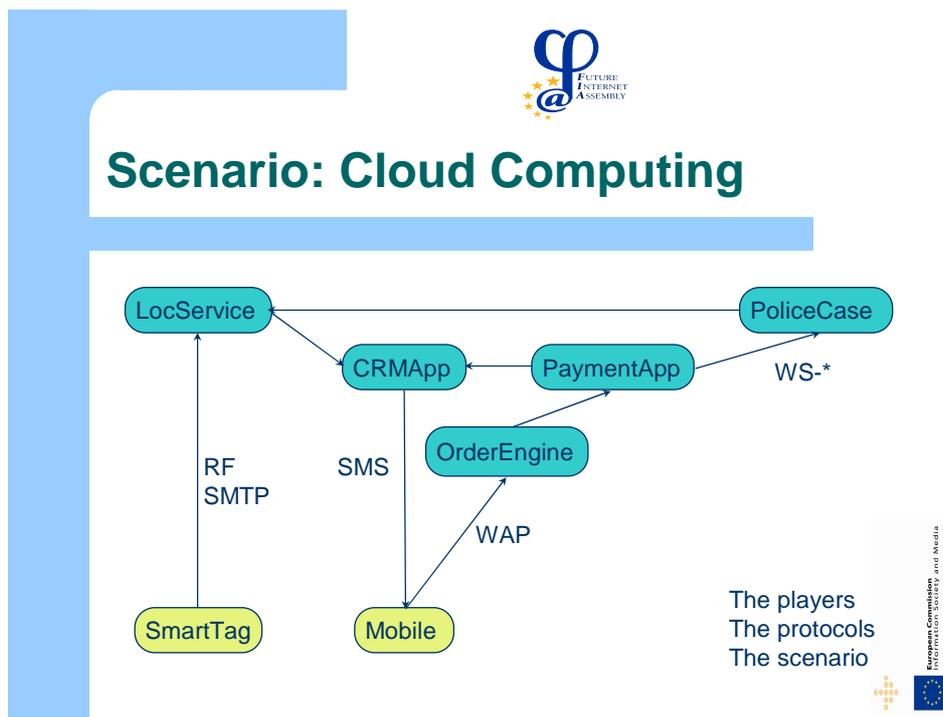


It was stressed that Accountability, Transparency & Measurability are technical pre-requisites but that they should be treated (mainly) as non-functional requirements.

**Scenario 2. Trust in the FI Services domains**

A scenario was presented by the RESERVOIR project related to establishing trust in the services domains. In order to define trust, they consider the mapping of the ITU definition of trust to the future internet environment. Namely, *An entity **A** is considered to trust another entity **B** when entity **A** believes that entity **B** will behave exactly as expected and required.*[1]
They are investigating whether services can be modeled as generic entities whilst remaining resilient (and hence trustworthy) taking into account the convergence needs of the many interrelated concepts.

The security requirements of the Reservoir scenario include:

- separation of services running in the same virtual environment;

- trust: inter-operation of service vendors;

- protection of the management interfaces;

- policies upon migration: only allow migration to domains with same policy.

---

[1]        International Telecommunications Union

**Scenario 3. Content provision in the Future Internet**

The next scenario involved the accelerating phenomenon whereas the consumers can be regarded both as a consumer and a producer of content (sometimes referred to as "prosumers"). Within the trust areas, these "prosumers" have to be satisfied in relation to identity management including authentication, privacy, usage and business aspects (e-payments), social context (e.g. protection mechanisms for children), and scalability issues with networks.

**Scenario 4. Complexity scenario (no single representative scenario)**

A final scenario was presented, which could be considered a concatenation of many scenarios in a Future Internet environment. As envisaged, there is no single representative scenario considering there are billions of nodes meet billions of consumers coupled with behavioural changes in real-time. A number of approaches for this were discussed including how trust could start at the elementary point, i.e., the node. The following attributes would also have to be addressed accordingly: authentication, authorisation, payment, accuracy, quality of service, amongst others. An example of this scenario was given an led to multiple discussions.
Alice was described as a consumer of sensing and actuation services. She wants to get information from a WS&AN island that she does not yet know which has highlighted some trust issues as per below:

- Trust of the WS&AN island that its communication partner is in fact Alice (related to authentication)
- Trust of the WS&AN island that Alice is authorized to use the service
- Trust of the WS&AN island provider that someone will pay for Alice's service usage
- Alice's trust that she is, in fact, communicating with the "right" WS&AN island (related to authentication)
- Alice's trust that the information received from the island is accurate
- Alice's trust in quality of services provided by third parties based on WS&AN information

Possible technical solutions to these challenged include classical certification mechanisms, reputation systems, and possibly more approaches.

Addition details on the trust scenarios can be found in the session slide sets.

### *Session results*
It is easy to see why trust has emerged as a common theme across many domains in FIA Bled and thus toward FIA Madrid. It has many implications for networks, citizens, businesses, security, privacy, identity and others. The major challenge perceived is that of **scale**: while trust in the current networked systems is to a large extent a relation between a small number of parties (or even bilateral), the FI asks for schemes that include millions or even **billions of highly heterogeneous entities**. This leap is a consequence of the fact that trusted interactions may occur on the level of individual services (Services stream), things (Real World Internet stream), and information (Content stream). Given this, trust **spans all layers of the FI**, including the layers of personal users and their connection to the FI. Dynamics of trust becomes important: for instance, if changes in a service choreography occur, how do they affect the overall trust evaluation, in particular, since some of these changes might not be visible on some layers or for some entities?
The trust considerations, and how to embed them in the FI, should be informed by first developing and agreeing models for attaining mass confidence in participation in the FI-based society and economy by

- delivering security,
- attaining trustworthiness by means of rigour, integrity, transparency and openness in, and the ease of obtaining restitution from, the control processes and accountability chains

There is a broad consensus among the stakeholders that transparency and accountability are essential principles of the FI. This is an immediate consequence of the multitude of stakeholders in the FI contributing to its trust with distributed ownership and potentially conflicting interests.
The following solutions may be applicable to trust challenges relative to the three aforementioned timescales::

Today: reputation systems, PKI-based trust schemes, trust management for small groups of virtual entities, …

**Mid-term**: EU-wide or global trust center(s), privacy-preserving access to empirical data, mechanisms to ascertain minimal disclosure.. privacy-preserving data mining, trust based on attestation of properties, …

**Long-term**: real-time response trust schemes coping with spontaneous behavior or reacting to events, transparency, accountability, privacy-preserving utilization of PII in business processes (this allows for similar business models as today while retaining the privacy of citizens)

At Madrid it was agreed that trust spans all layers of the Future Internet in particular, the following areas were highlighted:

1. Scale of Future Internet and its impact on trust
   a. Persons, devices, things, services, organisation
   b. Billions of heterogeneous entities
2. Transparency, Accountability and Responsibility
   a. Balanced approach
   b. Compartmentalisation
3. How to build the desired trust
   a. The role of PKI --> EU-wide / Global Trust Centres?
   b. Reputation, observation, attestation
   c. Spontaneous behaviour, reacting to events

In summary, the following topics were presented as the consolidated results from the Trust Session.

- Real-time establishment of trust:
  – recommendations
  – history data (and their impact on privacy)
- Compartmentalisation
  – different means and technologies in place,
  – multiple levels of responsibility
- Trust is multi-lateral:
  – parties,
  – layers and structures
  – Accountability
  – Non-transitivity of trust
  – liability
- Usability of trust mechanisms
  – trust can't be outsourced
  – but trust management can
- The proper level of regulation
  – adapt ideas of consumer protection law
- Trust feasibility and assessment
  – visibility, measurements
  – but it will be impossible to provide complete transparency.

# SESSION 2: IDENTITY & PRIVACY (14:30 – 16:00)

## *Identity & Privacy Scenarios*

The panelists presented a number of scenarios in order to stimulate the discussions:

**Scenario 1. Virtual IDs across domains.**

This involved the separation of one person's different IDs (for example, an ID from work and a non traceable ID from home. Reference – work in the FP6 IP DAIDALOS project.

**Scenario 2. Privacy Protection Cycle.**

This involved a scenario to demonstrate the concept for a systemic privacy protection cycle for users moving into and out of Peer-to-Peer based smart spaces with enhanced security backed-up with the infrastructure defined in the FP7 PERSIST project.

**Scenario 3. Real World scenario.**

The basis of this scenario is work carried out in the ASPIRE project. The scenario included a number of different 'real world' activities and then explored a number of questions from the perspective of Identity.

One of them was the safe tracking of your children. A number of questions were raised for this scenario: Who else can see? How to validate the correct user?

Another was the safe tracking of the food we eat with the consequent questions: Where does it come from? How long did it take to get to me? Am I paying my bill to the right person?

For both of these scenarios, the question was posed - What does identity really mean?

Addition details on the trust scenarios can be found in the session slide sets.

## *Session results*

Identity is a fundamental concept for a trusted and trustworthy Future Internet. In the FI, Identity management no longer applies to individuals only, but **extends to services, devices, objects, and virtual entities**. However, adequate schemes need to understand the difference in nature and role of the entities involved. Since an individual's interaction with the FI spans a lifetime and involves many different roles, the need for an independent ID provisioning and management system that smoothly interacts with the different contexts and respects a user's privacy becomes evident.

The relation between identity and trust is complex: Identity requires trust in a plethora of entities: systems and platforms that are involved in transactions for provisioning identities; software being used; protocols for identity federation; parties that vouch for identities. Then identity is again used to establish trust into parties, devices, organizations etc. As identity is a component of building trust, perhaps we need to consider an identity layer or indeed utilize frameworks [ref: Kim Cameron's Laws of Identity]. In addition, an "unlinkability layer" might need to be considered – otherwise the frequently stated demand on 'privacy-friendly identity service provision' could turn out to be unachievable.

The FI will have much larger impact on individuals', businesses' and authorities' interaction among each other, both due to the increasing number and size of such interactions, as well as their traceability over a long time span. Increased surveillance and profiling capabilities, sensing of actions, exchange of information and availability of information to an increased number of parties ask for enforcement of usage control, with an impact on SW architecture and network as well as hardware structures (Trusted Computing, privacy-preserving computing, SW attestation, …)

There is much attention being placed on **privacy-friendly identity service provision** (systems based on claims whereby instead of performing identification you claim your entitlement to a service and you give the proof of it without disclaiming further identity attributes[2].

Identity

>   ***Today***: advanced identity schemes for individuals (e.g., supporting federation), attribute certificates, …
>   ***Mid-term***: advanced identity schemes (including openID, Cardspace, Liberty) deployed for restricted scenarios (e.g., specific businesses), protocol support in products, privacy-friendly identity service provision, eID functionality integrated in passports / ID cards (suited for qualified digital signature), user provisioning from legacy systems, interoperable schemes…
>   Delegation schemes, e.g., to allow children or elderly in a legal way to interact in the information society, will become increasingly relevant once identity infrastructures will

---

[2]     Such systems include: uprove, ident-x of IBM, credentica recently acquired by Microsoft, etc.

emerge and major parts of governmental processes will move towards electronic processes. This is related again to accountability as the delegation complicates matters.

Life-time aspects of identity management

**Long-term**: Unified identity provision and management for users, services, things; user control over identity, , …Allowing for anonymity while retaining accountability; otherwise, it will be hard to get adoption in many environments; advanced hardware tokens; ontology-based reasoning over trust properties of Identity Providers; fully-user-centric schemes; key management issues solved; recovery from credential loss

Privacy

**Today**: Policy languages expressing users' requirements, privacy-preserving computation schemes for selected scenarios and functions, trusted computing modules available (but not largely used), …

**Mid-term**: policy enforcement / usage control (based on trusted computing), privacy-aware privacy policy agreement;

**Long-term**: "virtual trusted computing" based on cryptographic schemes (supporting platform-independent usage control), generalized usage control concepts (applying to individuals and businesses), on-line policy negotiation and adaptation (of both policies and technology),

Additional challenges come from cloud computing when the service provider runs their services on virtual machines (VMs) on physical machines in the cloud owned by other parties in different legal domains, and when the virtual machines may be migrated between computation services providers or just physical machines seamlessly. Challenges: protection requirements for PII must be (provably) enforced by the computation environment the VM is running in. This is related to the Security Lane.

Another long-term aspect is real-time compliance monitoring, both within or across service boundaries which can ensure detection of policy violations. Major challenges here are architecture (e.g., a monitoring interface for services) and security challenges on how to prevent attackers (e.g., insiders) from tampering with events and logs. This strongly relates to security also.

The challenges presented included the following:

- Security is about controlling <u>access</u> (to info)
  - Privacy is about controlling <u>accuracy and usage</u> (of personal info)
  - It is about controlling access to PII at info custodians / by 3rd parties
  - It implies sticking policies to PII as it moves around
  - and enforcing these policies + auditing usage over time
- Security and IDM have traditionally been driven by provider requirements
  - Privacy now requires putting users at the center – <u>user-centric</u> IDM
- Privacy clashes with accountability, anonymity with traceability
- Privacy requires the ability to conduct transactions under pseudonyms or even anonymously at all levels with some potential safeguards
  - Network (e.g. onion routing)
  - Application (e.g. attribute-based identification)
- Scenarios
  - Voting, blind decision-making, opinion survey
  - E-Service provision to restricted classes of users (e.g. members, children, adults, seniors, residents, nationals, gender, etc.)

In summary, the following topics were presented as the consolidated results from the Identity and Privacy Session.

- FI amplifies privacy challenges
    - The digital world is not forgetful
    - People are going to leave lifelong traces in the FI
- Reconciling privacy with accountability, anonymity with traceability
- Technologies that allow for privacy-preserving identity management start to be available
    - minimal disclosure tokens
    - to be further explored
- User Awareness
    - Privacy doesn't seem to be a priority of people yet
    - privacy loss in and  of itself is not yet a risk. It is a pre-condition to a risk
- Challenges: Deployment and regulation
    - harmonisation of technologies: standardisation, interoperability
    - legal landscape has gotten very cluttered
    - Regulation moving slower and behind technology
    - Public procurement in the lead?

# EXPERIMENTAL FACILITIES (16:00 – 16:15)

The caretakers of the session(s) invited the FIRE area to present how these projects offerings could assist the Trust and Identity areas with testing facilities as shown in Figure 2.
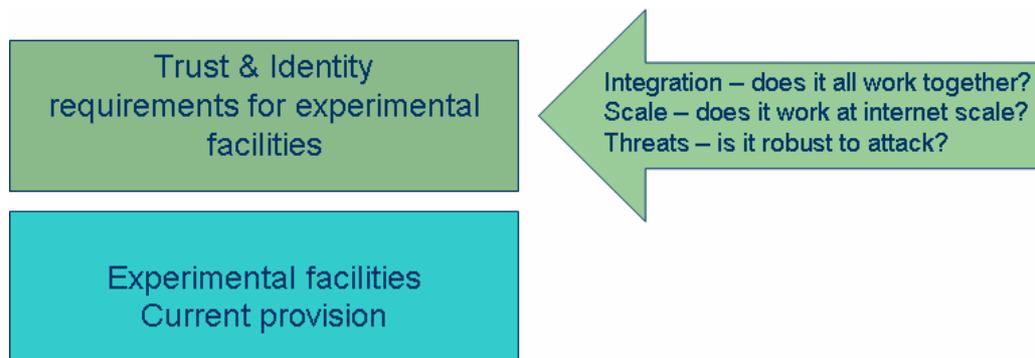


Figure 2. Experimental facilities provisioning

Martin Potts of Martel presented the FEDERICA[3] (**F**ederated **E**-infrastructure **D**edicated to **E**uropean **R**esearchers **I**nnovating in **C**omputing network **A**rchitectures) project, whose goal is the provision of an e-Infrastructure for researchers on Future Internet. The project operates on a concept in which researchers would be allowed access to "slice", which is defined as "a set of (virtual) network and computing resources which are independent (so can be used for different roles/identities)". In addition, "slices" may communicate with the General Internet.

There is a core infrastructure in place, which is also being extended, and the project is in the process of putting together a user information pack in which the perspective projects could apply for access to a "slice". The pack will be available on the project web site and will contain the following:
- Simple Memorandum of Understanding
- Acceptable User Policy, Access Rules
- Guide for proposals, Brief Introduction to FEDERICA
- Technical template, Feedback template

Requests for using FEDERICA should be sent to: fed-upb (at) fp7-federica.eu. Further information can be requested from: info (at) fp7-federica.eu

The floor was then opened to the participants for questions and in order to scope out the possibility of mapping some of the trust and identity scenarios. A question was raised about "who pays" and it was told that the projects themselves would be responsible for costs outside of the "slice" (for example, to connect physically to a FEDERICA Node) but that the resources within the slice would be available free of charge. If an experiment can be performed by hosting a user's software on FEDERICA´s Virtual Nodes (i.e. without needing external physical access), this is also free of charge.

A number of potential scenarios were raised and discussed as good potentials for using the experimental facilities. Although the facilities seemed to lend themselves to the network level, there were discussions about the potential of implementing some identity management and/or privacy enhancing technologies for testing purposes. A scenario of setting up a service oriented virtual execution environment management infrastructure for trustworthy, secure, scalable, federated, resilient services. Another scenario for setting up a security test-bed environment to simulate attacks was suggested and this may be very relevant for the FIA Prague event and after when the Security lane will be in more focus.

These trust and identity scenarios were re-iterated again in the FIRE BO session and in the FIA closing plenary session by the Experimental facilities representative.

---

[3]     **www.fp7-federica.eu**

# FOLLOW UP ACTIVITIES IN PREPARATION FOR FIA PRAGUE (16:15 – 16:30)

In the final session, a panel made up of the overall chair and caretakers presented the envisaged follow up activities and preparations to continue refinement of the position paper and roadmap between FIA Madrid and FIA Prague. A summary is shown in Figure 3.
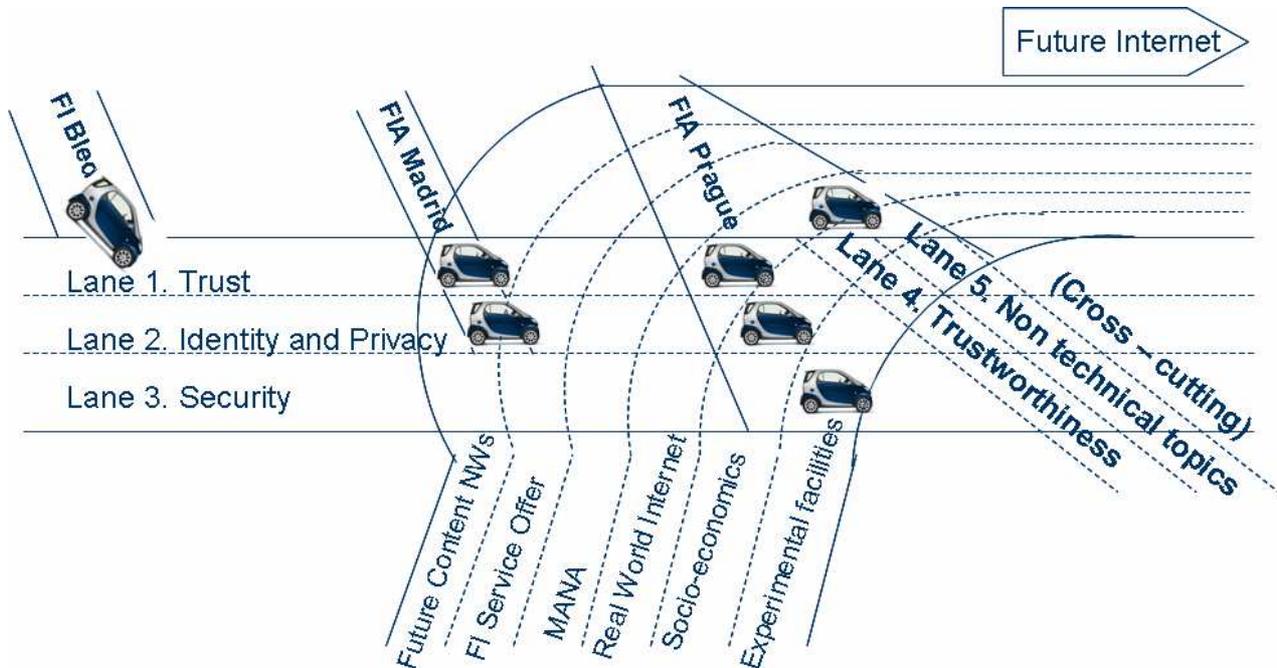


Figure 3. Roadmap between FIA Madrid and FIA Prague.

In addition to progressing the work in the first two lanes Trust and Identity, for FIA Prague, there will be a renewed focus on the refinement of the other lanes of the Trustworthy ICT roadmap, including:
- Lane 3. Security
- Lane 4. Trustworthiness
- Lane 5. Non-technical aspects

It was also agreed that we would consolidate scenarios towards reference scenarios that could be used towards the implementation of the reference scenarios within other cross domain areas, in particular, for example within service platforms, and/or through experimental facilities, and/or others TBD…

In conclusion, there was a feeling that we were probably at a point where further collaboration could be carried out across the domains to progress the roadmap and/or talk about project ideas and it might be a good opportunity to meet in smaller groups (via workshops, on line, etc.). Mechanisms for these kinds of activities would be further explored by the caretakers and the relevant communities to occur between the FIA events or within the umbrella of the FIA Prague event in May 2009.

Further information on the future activities can be found at http://security.future-internet.eu/index.php/FIA_Caretakers. Please contact the caretakers to become a member of the Wiki.

# AGENDA

| Time | Description | Chair/Speaker |
|---|---|---|
| **11:00- 11:10** | Opening of **Trust & Identity Session**<br>Overview of objectives & structure of session | Jacques Bus, EC<br>Overall Chair<br>Jim Clarke/ WIT |
| **11:10 -11:20** | Opening of **Trust session**<br><br>Presentation of position paper (Trust section)- Volkmar Lotz, SAP | Chair - Michel Riguidel/ ENST |
| **11:30 – 11:40** | **Keynote**<br><br>Beyond the construction blocks that makes trust possible – lessons learnt and way forward | Sachar Paulus, Paulus.consult |
| **11:40 – 12:30** | Presentation by Chair of Trust issues from project contributions<br><br>Panelists to use position paper to walk through examples of trust scenarios<br><br>**Panel Session**<br>**Trust** – Sachar Paulus, RISEPTIS<br><br>**Future Internet Services** – Syed Naqvi RESERVOIR<br><br>**Future Content Networks** - Theodore Zahariadis, SEA, AWISSENET<br><br>**Real world internet -** Mirko Presser, SENSEI | Chair - Michel Riguidel/ ENST |
| **12:30 – 13:00** | Open house discussion & Q & A Session | |
| **14:00 – 14:05** | Opening of **Identity & Privacy session**<br>Presentation of position paper (Identity & Privacy section)- Volkmar Lotz, SAP | Chair,<br>Nick Wainwright, HP |
| **14:05 – 14:35** | **Keynote**<br>State-of-art, mid-term perspectives of identity management (both identity card projects but as well infocard, windows 7, openid, etc.)<br>**Keynote**<br>How to provide privacy in the cloud, privacy-friendly identity, minimization of data through claim frameworks, etc. | Caspar Bowden, Microsoft<br><br><br>Phil Janson, IBM |
| **14:35 – 15:00** | Presentation by Chair of Identity issues from projects contribution<br><br>Panelists to use position paper to walk through examples of trust scenarios<br><br><br>**Panel session**<br>**Future Internet Services** - Kajetan Dolinar, PERSIST<br>**Real world internet (IoT etc.) –** Neeli Prasad, ASPIRE<br>**Network** - Joao Girao, DAIDALOS<br>**Identity -** Caspar Bowden, Microsoft<br><br>**Privacy** – Phil Janson, IBM | Chair - Nick Wainwright |
| **15:00 – 15:30** | Open house discussion & Q & A Session | |
| **15:30 – 15:45** | **Contribution to experimental facilities** | Martin Potts, Martel |
| **15: 45- 16:00** | **Follow-up activities in prep for Prague FIA & End of session** | Caretakers Panel |

# REFERENCES

[1] http://security.future-internet.eu/index.php/Future_Internet_Assembly_Trust_%26_Identity_session

# ANNEX A – PROJECT CONTRIBUTION QUESTIONNAIRE

**Instructions for completing this questionnaire**

The caretakers of the Future Internet Assembly ([fiacaretakers@think-trust.eu](mailto:fiacaretakers@think-trust.eu)) Trust and Identity break-out session, and the European Commission would appreciate if you on behalf of your project which has signed up to the Bled declaration can complete the following questionnaire to ensure cross-domain challenges and solutions are considered during this break-out session:

**Contact details:**

| | |
|---|---|
| **Project Name:** | Project XX |
| **Contact name:** | If you have a work package with a security theme a member may be best position to answer this questionnaire |
| **Email address:** | zzz@ |
| **Phone number:** | +code etc |

Our session is divided into 2 sub-sessions – Identity and Trust
**Which of these sessions is your research interest/project particularly interested in and describe the area of your contribution/input.**

| | | |
|---|---|---|
| ☐ | **Identity** | |
| ☐ | **Trust** | |
| ☐ | **Other security-related** | |

## 1. Managing Trust

How do you manage trust in your area?

How do you ensure that the expectations that your users have are met?

How do you ensure that third party components are 'trusted'?

Have you generated any metrics for trust?

## 2. Users & expectations

For Future Internet research to be successful we need to understand the **expectations of users** of
in the future internet, users approach the internet with a set of expectations about trust and privacy.

**What are the expectations that users have about the security and trustworthiness of your area?**

**What do you say to users about how their privacy is handled by your area?**

**Are you aware of any redress measures that users can take if commitments on privacy and trust aren't met?**

## 3. Managing privacy

- How do you manage privacy in your area?

- What mechanisms do you use to ensure that you can meet the expectations that are set and the commitments you make?

- Have you generated metrics or levels of privacy and how is this measured and monitored

## 4. Managing Identity

**What identity provisioning mechanism does your project /area currently adopt?**

**Does this fit your current requirements, please elaborate**

**We believe that identity will be an enabling technology do you believe your chosen identity provisioning mechanism will meet broad Future Internet requirements?**

**Do you have a view on emerging identity services such as Liberty, alliance, OpenID and eID services and their appropriateness for the Future Internet?**

**Please describe the top 4 trust/identity/privacy/security issues or possible solutions that can be addressed to add further value to your project?**

| 1 | |
|---|---|
| 2 | |
| 3 | |
| 4 | |

## 5. Gaps and problems

**Where do see the gaps between expectations and implementation?**

**Are there hidden 'network effects' that compromise or facilitate trust or privacy?**

**Are there dependencies on other systems that might mean you can't meet the trust and privacy commitments?**

**Can you propose any use case(s) from your project that could be implemented and explored using experimental test facilities?**

**Yes** ☐
**No** ☐

**If yes please describe, if it has specific security, trust, identity dimensions please include.**

**Are you available to discuss aspects of this questionnaire in more detail if required?**
**Yes** ☐
**No** ☐

**Please return this questionnaire to:**
fiacaretakers@think-trust.eu

We look forward to your contribution and active participation in Madrid
**Include attachments as appropriate.**