



Subject: Agenda and breakout sessions of the next Future Internet Assembly in Stockholm

1. DRAFT AGENDA

During the caretakers meeting of 26 June in Brussels it was decided that the next FIA workshop in Stockholm would address topics on which the different FIA groups wanted to discuss with other groups. At the same time, 9 possible topics were proposed by the caretakers. These topics were confirmed after consultation with the different groups, and are now scheduled as follows in the draft agenda.

FIA Stockholm

November 23, 2009			
7.30 – 8.30	Registration		
8.30 – 10.30	Plenary introductory session Welcome message, Gunnar Landgren, Rector – Vice Rector of KTH (15') European Perspectives & Orientations, Mario Campolargo, Director, EC (30') Industry preparations for a FI PPP, David Kennedy on behalf of ETP's (15') Socio-economic viewpoint on FI (30') Questions (30')		
10.30 – 11.00	Coffee break with Posters (poster also available at www.future-internet.eu)		
11.00-13.00	Different architectures for different business models?	ID Management, including routing and addressing in the Future Internet	What does it mean to conduct experimentally driven research?
14.00-16.00	Orchestration across things, services and content	How to measure trust?	What does Future Internet mean for smart cities?
16.00-16.30	Coffee break with Posters		

FIA Stockholm

November 23, 2009 – cont.							
16.30-18.30	The question of 'Discovery & Search' in the future Internet		What does Future Internet mean for enterprise?		Deploying on "Future Internet Research & Experimentation" (FIRE)		
November 24, 2009							
9.00-11.00	FI Socio-economics	Management & Service aware NA	Trust and Identity	Usage of facilities	FI Service Offer	Real-world Internet	Future Content Networks
11.00-11.30	Coffee break and Posters						
11.30-13.30	Future Internet as seen by Ericsson - Hakan Eriksson (30') National Future Internet initiative (10') ?? (Which country ??? UK???) Summary of Achievements, by the Breakout Session Rapporteurs (60') The Future Internet conference in Valencia - Host Introduction (10') Closing message by Mario Campolargo (5')						

2. INPUT RECEIVED FOR TOPICS FOR BREAK OUT SESSIONS

(1) *Different architectures for different business models?*

The Mana group produced a first input for the discussion topics during the session. See annex 1. This draft now needs to be revised based on the input of the other people that said to be interested in this topic. For email addresses of the interested people see the file Stockholm - Topics for breakout sessions - 13 August 2009.

Actions: Send comments to current draft to Henrik Abramowics before September 4.

(2) *ID Management, including routing and addressing in the Future Internet*

This topic has received input from both Mana and Trust & Identity. As can be seen from the annex, both groups changed slightly the title and have a different view on the topic. Markus Brunner and Jim Clarke are currently reconciling their contributions to one.

Actions: New draft circulated to the people interested in this topic by September 4.

Send feedback about that new draft to Jim Clarke and Markus Brunner by September 11.

(3) *What does it mean to conduct experimentally-driven research?*

No input received so far.

Actions: FIRE to provide first draft and circulate it to the people interested and ask for their feedback by September 4.

(4) *Deploying on “Future Internet Research & Experimentation” (FIRE)*

The Trust & Identity group has provided initial input. Needs to be extended by the other people interested in the topic.

Actions: Send comments to current draft to Ruben Montero before September 4.

(5) *Orchestration across things, services and content*

MANA has provided a first draft. Needs to be extended by the other people interested in the topic.

Actions: Send comments to current draft to Alex Galis before September 4.

(6) *The question of ‘Discovery & Search’ in the future Internet*

No input received so far.

Actions: FISO to provide first draft and circulate it to the people interested and ask for their feedback by September 4.

(7) *What does Future Internet mean for smart-cities?*

Input received from Nick Wainwright of Trust and Identity. Needs to be extended by the other people interested in the topic.

Actions: Send comments to current draft to Nick Wainwright before September 4.

(8) *How to measure trust?*

Input received from Volkmar Lotz of Trust and Identity. Needs to be extended by the other people interested in the topic.

Actions: Send comments to current draft to Volkmar Lotz before September 4.

(9) *What does Future Internet mean for enterprise?*

Input received from Man-Sze Li from FISO. Needs to be extended by the other people interested in the topic.

Actions: Send comments to current draft to Man-Sze Li before September 4.

2.1. General remarks

For email addresses of the interested people see the file Stockholm - Topics for breakout sessions - 13 August 2009.

2.2. Plans of Socio-Economics group

The Socio-Economics group will have a plenary session of 30 minutes and will contribute to the different topics. The caretakers are now:

- Mike Boniface (University of Southampton IT Innovation/IRMOS)
- Burkhard Stiller (University of Zurich/SmoothIT) replacing David Hausheer
- Sergios Soursos (Intracom/SmoothIT) replacing Spiros Spirou

The Socio-economics group has agreed to organise a 30 minute plenary slot for socio-economics

- 2x 10 minute presentations + 10 minute Q&A
- Chaired by Burkhard Stiller
- Presenters to be confirmed

The socio-economics group will contribute to topics 9, 7, 1, 8 (in order of priority) and will have a representative at each session. They will create a position statement on each topic as input to the session. This work will start next week via the FISE list.

The preliminary agenda for the final FISE wrap up session is:

- Introduction (10 minutes) - Mike
- Panel summary of sessions (1, 7, 8, 9) from a FISE perspective (4 x 5 mins = 20 mins) FISE session representatives
- Brainstorm key socio-economic questions (15 mins) - Burkard
- Focused discussion around the questions (1 hour) - Mike
- Summary and next steps (15 mins) - Sergios

2.3. General comments given by FISO

We also received some general comments from the Service Offer group. These were as follows: the topic of the European Citizen is not strongly highlighted – although this may be related to 7. Smart Cities.

The topic of software engineering of future service-based systems is also missing.

A topic on HCI and the Future Internet would be interesting

Future Internet for specific communities e.g. elderly citizens.

2.4. New white paper written by EIFFEL

We believe that the preparation of some of the topics can benefit by the reflections given in the new white paper written by EIFFEL. It is available from http://www.future-internet.eu/fileadmin/documents/reports/Report_TT2008.pdf.

3. PROPOSED CALENDAR

- 4 September:
 - First draft of topic description decided
 - preliminary assignment of topic leaders, see separate excel file
- topics are put online for everyone's input 18th September (FIA-caretakers meeting in Brussels)
 - sessions are assigned to time slots
 - final arbitrage (if any) is made on the content of each topic
 - rapporteurs are assigned to each topic
 - opening of registrations for Stockholm; participants are asked which session they intend to participate and are [invited to apply/added] to the distribution lists of each topic
 - Draft of each of the session's agenda's available
- Until Stockholm
 - pre-agree on as much content as possible for each topic (*'what do we agree in advance?'*)
 - clearly identify points for discussion (*'let's understand our disagreements'*)
 - decide the detailed program of each session (format, speakers, keynotes, etc).
- Final preparation meeting for Stockholm 16 October, Brussels (to be confirmed)
 - If necessary, finetune the detailed program of each session
- In Stockholm
 - hold the sessions with a view towards dispelling as many disagreements as possible (remember: audience should be aware of the issue well in advance)
 - if questions remain (and are of importance enough), narrow them and propose a follow-up topic for Valencia
- After Stockholm
 - finalise reports
 - decide immediately of topics for Valencia

Annex - Input received for topics.

1. *Different architectures for different business models?*

Received from Mana – Henrik Abramowics

Problem Statement:

We are currently in a transformation mode where different business segments are merging continuously and rapidly into something new. Traditionally we have been looking at Cellular communication, Internet, Media and Service distribution separately each having their own business drivers, model and corresponding architectures. We have a growing number of applications, devices and recourse based platforms that are multi modal and interconnected and working cross-domains.

A motivating meeting point is in the systems enabling faster mergers of the most ICT business segments, impacting the roles of the actors and stakeholders.

So what will happen when these diverse business segments are increasingly being merged? Will the different business segments try to sustain their current models?

Are we going from vertical oriented business models and architectures towards horizontal? What impacts do we see on an overarching architecture? Revenue and value sharing between different actors to be considered? Advertisement based?

On the other hand there are more specialized applications segments e.g. home securities and surveillance, health services being established- that is really vertical segments. How will these emerging (?) segments and their business models impact architecture?

Key Topics for presentations, discussions and agreements:

- New architectures and system interfaces for diverse business models integrating:
 1. Polymorphic facets of the Internet (e.g. communication-centric, information-centric, context-centric, resource-centric, content –centric, service/computation-centric, device-centric, object-centric and management-centric Future Internet);
 2. Organisational & federated domains;
 3. Diverse user/consumer-facing functionality
- How to change; programmatic changes and system life cycle costs of change for these architectures
- Migration towards new architectures
- Mapping of existing architectures into new forms

Expected Results:

- Agreement and initial description of the system interfaces and architectures enabling integration of polymorphic faces of the Internet
- Initial description of the milestones and roadmap of research results

Caretakers: Henrik Abramowicz (MANA)

Participants: Alex Galis (MANA), John Domingue (FISO), Markus Brunner (MANA), Norbert Niebert (FCN), Pierre-Yves Danet (FCN), Stefano De Panifilis (FISO), Theodore Zahariadis (FCN)

Points of agreement:

These are the starting points:

- The different ICT segments are merging
- We are going more and more from vertical business models towards horizontal and hourglass types and consequently the architectures need to follow suit. We need to mirror the business interfaces that are defined according to business models to technical interfaces
- The management of the new architectures reflecting dynamic relationships between actors and stakeholders
- New forms of the infrastructures enabling change

Points of discussion:

See scope above.

Follow up actions: <List of agreed actions to do after Stockholm and before Valencia.

These actions are to be undertaken by the 7 groups>

- Consolidation of the description of the system/infrastructure interfaces and architectures
- Consolidation of the description of the milestones and roadmap of research results

Reference:

To be completed

<References to external documents should be included here with a view to keep the overall text not longer than 2-4 pages. Include as well the presentations made during the conference>

Does this topic require a follow-up discussion in Valencia? **Yes**

Title: Consolidated and Integrated architectures and infrastructures for diverse business model

ID Management, including routing and addressing in the Future Internet

2 inputs received, 1 from Mana – Markus Brunner and 1 from Trust&Identity – Jim Clarke

Title: Identification, Finding of Elements, and Routing in the Future Internet (ID management including routing and addressing)

Input received from Markus Brunner

Problem Statement:

In the today's Internet the commonly used identifications are the IP address (i.e. identifying the location in the IP topology and identifying the interface of a host or router), then there are the DNS names identifying a host or server, and the URL identifying some resources on a node typically.

In a Future Internet the question is what the elements to be identified are there? What the security properties of such identifications are? How the relationships between different elements living in a FI are expressed and maintained? How to govern the increasing number of FI object-identifiers? How to use the object's identifications as enablers for development and management of independent federated network, services and applications. Finally, the question is, whether it is still possible to scale up the searching, finding, negotiation, monitoring and routing towards the elements in a Future Internet.

Key Topics for presentations, discussions and agreements:

- Different types of identifiers: IP addresses (structured addresses), context-identifiers, information object-identifiers, resource (i.e. network, computation, storage) – identifiers, content-identifiers, device identifier, computational objects identifiers, service identifiers, virtual objects identifiers, virtual resource–identifiers, artifacts–identifiers, interface-identifiers; multihoming identifiers;
- Identification and issues in federations and multi-domains environments.
- Adequate addressing schemes where identity/identifiers and location are not embedded in the same address.
- Mechanisms for publish/subscribe, aiming for a balance of incentives and roles between the sender and the receiver. E.g. information based publish / subscribe routing protocols.
- New and integrating naming frameworks, including both channel/session identifier and location, endpoints (source & destination points)-to-location resolution, identifier/location splits, and support for addressing and observability of information, context objects and services at all relevant FI levels
- Security properties of names and identifiers.
- Governance schemes for FI identifiers

Expected Results:

- Agreement and initial description of the
 1. FI identifiers,
 2. Naming and addressing mechanisms
 - a. e.g. publish/subscribe schemes for FI
 - b. novel structured approaches
 - c. others
 3. Governance for FI identifiers
- Initial description of the milestones and roadmap of research results

Caretakers: Marcus Brunner (MANA)

Participants:

Alex Gluhak (FISO) Jim Clarke (FISO), Michel Riguidel (FISE), Norbert Niebert (FCN), Tasos Gavras (FIRE), Theodore Zahariadis (FCN), Alex Galis (MANA), Henrik Abramowicz (MANA)

Points of agreement: <List here the points of agreement and a brief explanation of why/how a consensus has been reached. Include as well significant options that have been left behind.>

- list of elements to be identified
- problems to scale up
- adequate naming frameworks
- governance schemes

Points of discussion:

See scope above.

Follow up actions: <List of agreed actions to do after Stockholm and before Valencia. These actions are to be undertaken by the 7 groups>

- Consolidation of the description of the FI systems and objects identifiers and architectures
- Consolidation of the description of the milestones and roadmap of research results

Reference: <References to external documents should be included here with a view to keep the overall text not longer than 2-4 pages. Include as well the presentations made during the conference>

Does this topic require a follow-up discussion in Valencia? **Yes**

If yes, specify draft title: **Future Internet Routing**

Title: *Electronic ID (eID) management and provisioning in the Future Internet services, content and network infrastructures*

Input received from Jim Clarke – Trust & Identity

Problem Statement(s):

Design and development of a coherent and comprehensive *framework* for handling all aspects of usage and management of eID. The scope of eID in this document encompasses the virtual identities which services, content or network objects can take on, as well as the minimum requirements for identifying persons when accessing a resource. This should include:

- administrative aspects: the 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;
- the access controls by (productive) networked services based on eID;
- considerations of supportive legal measures covering possible rights, responsibilities and liabilities, as below.

Work already carried out, as above, can provide a valuable initial basis for further investigations.

Contextual usage of multiple Identities and user aspects: Investigate naming and multiple attributes covering aspects of identity required in different contexts (eg. if it is a virtual entity such as a web service or a network resource, or in the case of natural or legal person whether you are a parent, a citizen, an adult, a patient, consumer, etc.). Behind this, it is necessary to take into account the accountability and authentication aspects within specific contexts and situations. This introduces more complexity with (human) usability becoming an increased challenge.

At the Prague FIA event, the predominant approach discussed for tackling the issue was to involve the users within the design processes of the systems. It is essential that research is carried out on how to balance the sophistication required for all these attributes and the usability required. If the systems are too cumbersome to use, it will disable the usage and confidence levels. In Stockholm, this approach can be further explored on how to integrate the user/usage aspects with a view towards implementation within the research communities;

Links to "service description frameworks" and languages, in particular from a naming and a semantic perspective: For the service-oriented-architecture aspects, it is necessary to think in terms of the knowledge and semantics of the attributes, and the necessary interoperability for a wider use across heterogeneous platforms. This must be extended to attribute definition of the services themselves. For example, characterizing the "state" of an individual service and the functions it offers [including its security state]. Other aspects include discoverability, availability, and composability for more sophisticated services.

For example, a service is named and described according to a given operating context, and it is being used within another context. The semantics could, in the longer term, support the portability of identity attributes across national states, e.g. you are on holiday

and you want to access health care, but you need to prove your health insurability from your home country.¹

Consideration of Legal, Regulatory and governance policies: Another challenge related to Identity management and provisioning in the Future Internet that must be addressed is the links with legal, regulatory and governance policies.

It was also clear in the FIA session in Prague that establishing who/what is in control of the data/information and customer awareness is a critical aspect that must be addressed.

There are clear links here with the work of RISEPTIS Advisory Board², which should be exploited.

Security and Privacy aspects: although this may be considered as a full topic itself, if not addressed elsewhere, it could be addressed here as the role/contribution of good eID to privacy aspects:

- directly in minimum disclosure
- protecting user's 'application' data from falling into the wrong hands via digital dustbins
- other aspects of anonymity?
- better granularity of accountability
- assist better/finer access control
 - (i) users accessing and controlling of data - putting the user in control of her/his information;
 - (ii) others accessing users data - ensuring that 'private' information cannot be interfered with (networks and addresses, packet inspection, etc.) legitimate / non-legitimate access, etc.

Caretakers that volunteered for this topic: <Jim Clarke, (TI - author of this draft, alignment with other caretakers pending), Alex Gluhak (RWI), Michel Riguidel (TI), Norbert Niebert (FCN), Pierre-Yves Danet (FCN), Tasos Gavras (FIRE), Theodore Zahariadis (FCN)>

Participants: same as listed in caretakers plus research community people invited to workshop in October 7 2009.

Points of agreement:

- Need to have less formal event(s) to explore greater synergies between research communities;
- Difficulties with parallel panel sessions during the FI Technical days (eg. T&I and Content or Networks);
- Between official FIA events, caretakers spend disproportionate amounts of their time dealing with administrative aspects eg. locating / inviting speakers and topics, instead of more pro-active and productive technical discussions amongst the members in the other FIA domains areas.

Points of Discussion:

¹ Note: there is also some good work being done in the STORK project that can be included here. F5 has already held a workshop with them. See <http://www.think-trust.eu/general/news-events/2008-10-14-workshop-on-id-management-in-the-future-digital-society-takes-place-in-brussels.html> for report on event.

² "Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society" <http://www.think-trust.eu/riseptis.html>

Holding workshop on 7th October 2009 to prepare for FIA Stockholm with the following objectives:

1. To bring together FIA domain members (in a less formal setting than the FIA events) from the **Trust and Identity FIA community** with the members of the other FIA domains: **Future Content Networks, Management and Service-aware Networking Architectures, Future Internet Service offer, Real World Internet, Socio-Economics, Future Internet Research and Experimentation Software and Services,**
2. To provide an opportunity to review **cross domain Trust and Identity issues,** building on the achievements so far (in annex, list of documents from FIA Bled, Madrid, Prague, ..)
3. Allow for open and frank discussions on what the important **multi-disciplinary requirements and challenges** are for a Trustworthy Future Internet, especially in relation to privacy and identity, trust platforms and experimental facilities

Follow up actions: Amongst the TI caretakers only, we have discussed sequencing of topics in FIA Stockholm and have come to a recommendation of a possible sequence.

2. ID Management, including routing and addressing in the Future Internet	1. Different architectures for different business models?	5. Orchestration across things, services and content
8. How to measure trust?	3. What does it mean to conduct experimentally-driven research?	6. The question of 'Discovery & Search' in the future Internet
4. Deploying on FIRE	7. What does Future Internet mean for smart-cities?	9. What does Future Internet mean for enterprise?
Wrap up where all Domains group individually	Wrap up where all Domains group individually	Wrap up where all Domains group individually

Reference: In Madrid (Dec. 08) and Prague (May 2009), the Future Internet Assembly workshops held initial dedicated sessions on these topics, organised by the Trust and Identity caretakers.

A clear need was established for a coherent approach to careful handling, usage, and management of identities and identity-related information (eIDs) in the Future Internet. This must cover both future requirements for global interoperability and the current legacy. Principles set out in the *Laws of Identity*³ provide guidance.

A common identity framework addressing these principles has been outlined⁴. In the digital society, *Identities* will be multi-faceted and identity-provisioning and usage must take account of fundamental differences between physical identity and our digital identities. The Future Internet must move on from the flat or unique protocols for identity to more flexible ways of expressing and using identity appropriate to specific contexts and supporting interoperability.

³ <http://www.identityblog.com/stories/2004/12/09/thelaws.html>

⁴ Posch, R., Rannenber, K., Cameron, K., "Proposal for a common identity framework: A User-Centric Identity Metasystem";

Does this topic require a follow-up discussion in Valencia? Yes

If yes, specify draft title: ... ***Electronic ID (eID) management and provisioning in the Future Internet services, content and network infrastructures***

Deploying on “Future Internet Research & Experimentation” (FIRE)

Problem Statement: Testing and experimenting with Trust and Identity in FIRE

[This is an incomplete draft, requires more discussion amongst the group]

Contribution received from Trust&Identity

The FIRE experimental facilities let us explore whether Future Internet systems operating at scale exhibit the properties and behaviours that we intended when we designed them and tested in the lab, whether systems constructed independently can be integrated together and whether they function as we expect when they are integrated. If we are able to make facilities available for others to use we can also look for emergent properties and emergent usage of systems (e.g. creative use of facilities by users who discover different ways. A fuller treatment of the role of experimental facilities has been explored by the working group on modular federation of FIRE facilities in [1].

At the Prague FIA meeting we explored some of the experimental approaches to Trust in Future Internet. These can be broadly characterised as

- Observing and monitoring attacks on systems in the public internet (e.g. ‘Honeynets)
- Experimental work with ‘real’ end users (e.g. living labs)
- Provision of ‘trust services’ e.g. eID on which more trustworthy services can be constructed
- Experimental identification of technical vulnerabilities in systems

Provide quarantine areas of the testbed. There will be vulnerabilities at all levels in the systems and components of the future internet. Can we create isolated (quarantined) experimental facilities in which one could run explore robustness of systems and components against attack? For example, can we launch a distributed denial of service attacks on services without bringing down the whole FIRE facility or even worse impacting the entire internet?

Provide eIdentity facilities? Can we provide a comprehensive electronic ID facility in FIRE that is used by all experimental activities using FIRE? How do FIRE users access and use such systems?

Caretakers: Alex Gluhak, John Domingue, Nick Wainwright, Piere-Yves Danet, Tasos Gavras, Theodore Zahariadis

Participants:

Points of Agreement

Points of Discussion:

Follow up actions:

Reference: Towards a collaboration and high level federation structure for the FIRE facility, 20th July 2009, Working Group on Modular Federation of FIRE facilities

Orchestration across things, services and content

Input received from Alex Galis - MANA

Problem Statement:

In the today's Internet there some orchestration embedded capabilities for enabling *network-of-networks* to grow organically, to operate and interwork.

In a Future Internet the question is what are the orchestration capabilities needed to integrate and govern the complete behavior and operations of the *system-of-systems* (i.e. communication-centric systems, information-centric systems, context-centric systems, resource-centric systems, content –centric systems, service/computation- centric systems, device-centric systems, object-centric systems, things-centric systems and management-centric systems)? What are the capabilities needed to dynamically grow, adapt and optimize infrastructure (network, computation, storage, content) resources in response to changing context and in accordance with applicable business goals and governance policies? What are the supervisory and interworking capabilities that integrate all other system behaviour insuring integrity of the FI operations? What are the capabilities supporting the simple and fast merging different Internet business segments into new forms?

Key Topics for presentations, discussions and agreements:

- Mechanisms and capabilities for controlling workflow for all systems of all FI system-of-systems, ensuring bootstrapping, initialisation, dynamic reconfiguration, federation, adaptation and contextualisation, optimisation, organisation, and closing down of system components, which represents one facet of the FI Orchestration Plane
- Mechanisms and capabilities for allowing heterogeneous systems to interwork (i.e. communication-centric systems, information-centric systems, context-centric systems, resource-centric systems, content –centric systems, service/computation- centric systems, device-centric systems, object-centric systems, things-centric systems and management-centric systems), which represents on other facet the FI Orchestration Plane
- Orchestration Plane architectures and its interfaces to the Infrastructure (network, computation, storage, content) resources, to the Self-Management functionality and to the Service functions
- Mechanisms and capabilities for controlling co-existence of multiple and parallel FI(s) based on multiple socio-economies matrices and measures.
- Mechanisms for distributed governance.
- Mechanisms and capabilities for controlling the sequence and conditions in which one service component invokes other service components in order to realize some useful function.
- Mechanisms and capabilities for negotiation in order to solve conflicts among FI systems. Negotiation can also occur between different domain systems.
- Mechanisms for allowing conflicting interests (the so called “tussle networking” introduced by D. Clark) such as conflicting policies, different compensation approaches and different operations.
- Mechanisms and capabilities for the dissemination of knowledge regarding the Orchestration Plane.
- Mechanisms and capabilities for FI federation: these control the union/separation of network and service resources having different autonomic management domains. They identify the

steps necessary to compose/decompose different federated domains, triggering actions to change the networks and services.

- Mechanisms and capabilities for controlling the information flow. They define the “What, When and Where” of the information: What information to collect, when to collect, and from whom (where). They supervise the storage of information.
- Mechanisms for cognitive control. They define system data collection, management and decision making, which enable the Internet infrastructure to learn about its own behaviour, to tune its operation, and to enforce its decisions on data manageability.
- Mechanisms for bootstrapping and initialisation systems under supervision.
- Mechanisms for dynamically reconfiguring and adapting of other systems under supervision.
- Mechanisms for dynamically optimising and organising other systems under supervision.
- Mechanisms for dynamically closing down of other systems under supervision.
- Mechanisms for supervision of QoS controllers, triggering an instantaneous modification of the configuration. For example, when following a failure, an instantaneous reconfiguration of the virtual systems is necessary.
- Mechanisms for supervision of resource allocation in several virtual systems. For example, this capability would trigger a change in resource allocations following changes in the context.
- Mechanisms and ontologies that describe the functionalities and enable dynamic discovery, understanding and interaction with the respective offered capabilities.
- Mechanisms to create holistic network view from separate views of the elements in all system level and in all virtualization levels.
- Mechanisms and capabilities for allowing nesting of different control loops with respects to the same objective or the same set of resources.

Expected Results:

- Agreement and initial description of the
 4. FI Orchestration Plane (OP) capabilities and reference configuration
 5. Explicit OP interfaces
 6. Explicit Governance for the OP
 7. Business value enabled by the OP
- Initial description of the milestones and roadmap of research results

Caretakers: Alex Galis (MANA)

Participants: Alex Gluhak (FISO), John Domingue (FISE), Stefano De Panfilis (FISE), Theodore Zahariadis (FCN), Marcus Brunner (MANA), Henrik Abramowicz (MANA), Jon Mikel Rubina (FISE), Stephan Haller (RWI), Alessandro Bassi (RWI), John Serrat (MANA), Stuart Clyman (MANA), Joe Butler (FISE), Martin Vigoureux (MANA), Nancy Alonistioti (MANA)

Points of agreement: <List here the points of agreement and a brief explanation of why/how a consensus has been reached. Include as well significant options that have been left behind. >

- Orchestration Plane (OP) capabilities and reference configuration
- Orchestration Plane (OP) interfaces
- OP Integration in Future Internet architectures

Points of discussion: <List here the sub-points, which are still under discussion as well as a brief explanation of the open options for each>

See scope above.

Follow up actions: *<List of agreed actions to do after Stockholm and before Valencia. These actions are to be undertaken by the 7 groups>*

- Consolidation of the description of the FI OP capabilities, architectures and interfaces
- Consolidation of the description of the milestones and roadmap of research results

Reference: *<References to external documents should be included here with a view to keep the overall text not longer than 2-4 pages. Include as well the presentations made during the conference>* **TBD**

Does this topic require a follow-up discussion in Valencia? **Yes**

If yes, specify draft title: **Orchestration in Future Internet**

What does Future Internet mean for smart-cities?

Input received from Nick Wainwright – Trust & Identity

Problem Statement: Building the Internet Infrastructure for Smart City

70% of the world's population live in cities. This proportion is increasing. Urban environments are dense, complex spaces. Reducing the carbon footprint of cities is a pressing issue, necessitating sophisticated control and management of energy use on both the supply and demand side across all aspects of city life. Much of the current focus on smart cities focuses on this aspect.

However, Smart Cities are not just about carbon footprint; maintaining and increasing quality of life in large dense urban environments necessitates smart security, transportation, healthcare, and work and leisure activities. Efficient operation of urban environments requires the means to monitor and control complex services, each comprising many different services and countless components.

A Future Internet in a smart urban environment must provide the infrastructure for public services, enterprise, and citizens to manage, control, optimise, and improve all these aspects of their lives at both the micro- and the macro- level. Our interpretation of 'smart' is the ability to model, measure, optimise, control, and monitor complex interdependent systems of dense urban life. A Future Internet must provide the means for a multiplicity of services, working independently and together, to interact with and manage all aspects of urban life.

Clearly many if not all of the research challenges associated with the development of the Future Internet are significant enablers for a smart city (pervasive, trusted, reliable, secure networks and service platforms in particular). Rather than repeat what is already covered in FIA initiatives, we attempt to identify challenges that are cross cutting and integrative of many different technologies and needs.

- 1. Creating a pervasive connection between the physical and the digital worlds:** We will need to dramatically reduce the cost and power needs of network endpoints so that we can embed them in physical devices to link sensors and actuators so that we can manage and control the physical world. The cost of ubiquitous, trustworthy, low cost and energy efficient network connectivity must be vanishingly small. Power needs of network endpoints must be commensurate with the environment in which they are situated. The network must scale – perhaps thousands of nodes in a home, millions in a factory, and billions in a transport network. The network must exhibit security and reliability properties appropriate for the services and systems that rely on them.
- 2. Creating an active digital analogue of the physical world.** To create a truly smart city, we must be able to construct an open digital analogue of that physical world, a model that mirrors the state of the physical world and on which we can develop and deploy new services to manage and control our smart city. Just as geographic maps have enabled us to plan and build the urban environment, an active digital analogue of the state of the physical world will give us the means to control and manage it. The

digital analogue of a city must identify all the objects in it, their state, and their interfaces. Its users must be able to understand and trust it. It must take an appropriate approach to centralisation for high level perspective and management, and decentralisation that scales and reflects the boundaries between social and legal constructs. An active digital analogue of the physical world can be a foundation for creating and delivering services that will make a city truly ‘smart’.

Trust, Security and Privacy Challenges

- If the operation of a city is heavily reliant on sophisticated and pervasive communications infrastructure and service platforms it must be robust against system and component failure, unanticipated demand and usage patterns, and malicious attack to the network and service platforms.
- Vulnerabilities of technical solutions will not vanish in the Future Internet, yet it is the glue that ties together systems managing vital infrastructure and services at both macro- and micro- levels. Therefore explicit notions of ‘trust’ and methods to assess trustworthiness must be built into the FI infrastructure along the lines outlined in other contributions to FIA (see ‘Measuring Trust ...’)
- Comprehensive capabilities for ‘privacy preserving’ identity management must be explicitly built into the future Smart City infrastructure to give citizens confidence to interact with smart services (see eID management and provisioning)

Caretakers: Alex Gluhak, John Domingue, Nick Wainwright (author of this draft), Stefano De Panfilis, Tasos Gavras

Participants: A Future Internet for Smart Cities cuts across every area in the FIA remit, and goes beyond that. We highlight specific network technologies (Networks, physical layer), pervasive networking (Internet of Things), and an open platform (Internet of Services). It might also be fruitful to make a direct link to other areas, e.g. SmartGrids, or Smart Transport to bring a user perspective into the discussion.

Points of agreement:

To be identified during the discussion.

Points of discussion:

- What’s our vision for ‘smart cities’
- How do we use ‘smart cities’ scenarios to drive challenging cross cutting Future Internet research challenges?
- What are the Future Internet challenges inspired by ‘smart cities’ that go beyond our current thinking, or are integrative across disciplines?

Follow up actions

- Teleconference and review contributions before Stockholm

Reference: TBD

How to measure trust?

Contribution received from Volkmar Lotz – Trust & Identity

Title: *How to Measure Trust?*

Problem Statement: From the discussions at the previous FIA conferences, there can be no doubt that there is a broad consensus that trust in the Future Internet is essential. Without trust, FI opportunities will not materialise in new business platforms and models strengthening the European economy or novel applications increasing quality of life. The reason lies in the value of interactions over the FI for the stakeholders involved and its distributed ownership / federation, demanding entities to behave as expected in order to not put the values at risk.

A trusted FI, however, does not mean that nothing can go wrong: vulnerabilities of technical solutions are a fact of life (and there is no evidence that they will vanish with the advent of the FI), and they are likely to be exploited by malicious entities. The key to a trusted FI, thus, lies in the ability to assess the risk associated with these vulnerabilities and the likelihood of malicious behaviour as well as having means at hand to mitigate those risks by adequate controls. This allows a user, for instance, when consuming a service, to make informed decisions about the risk upon engaging in a transaction and to mitigate the risk if necessary (or withdraw from the interaction, if either the risk or the mitigation costs are too high).

If trust is considered to be the outcome of such a decision process, there is a need to capture the parameters influencing the decision:

- The value of an interaction – this requires to define what a particular interaction consists of and which assets are affected by it in which way. Interactions can be computations, accesses to resources, transactions, long-term relations, persistent storage, delegation of business processes, service calls and many other types
- The risk associated with the execution of the interaction – this expresses the likelihood and potential damage of misbehaviour of participating entities
- The available means for mitigating the risks, the necessary investments to deploy them (e.g., the cost of invoking a control service) and their impact on the likelihood and potential damage of misbehaviour

It is important to notice that this decision has to take into account the distributed nature of trust in the FI. Due to its lack of central control and the multitude of stakeholders in different roles, there are multiple anchors of trust, including applications, services, service delivery platforms, infrastructure, and devices.

The challenge for the measurement of trust lies in describing the nature of the related parameters (are they to be expressed in terms of values, properties, behaviours or others in order to allow informed decisions) and in actually capturing them in a given interaction context. When talking in terms of values, the challenge lies in finding sufficiently expressive metrics. A property based assessment of trust is likely to be sufficiently expressive and would allow to distinguish between guaranteed properties (capturing the notion of trustworthiness) and desired properties (required by a service consumer, say, from a consumed service for the consumer be willing to engage with the service, i.e., accept the remaining risk or trusting the service), but asks for capturing the deviation between two (sets of) properties.

The measurement of trust needs to be integrated in the architecture of the FI, spanning its layers and components. Thus, in addition to investigate into the nature of trust

measurements, there is a need for defining and integrating methods, components and services that support the user in assessing trust in a given context:

- management methodologies and tools, ready to be used by the service consumer (services and users) and taking lifecycle and aggregation aspects into account (→ dynamic risk evaluation)
- a trust and security “toolbox” that can be flexibly adapted to the given business / risk context and allows to mitigate risks / increase trust
- methods and tools for assessing the effectiveness of a given selection and composition of controls
- their integration in FI architecture

We also need to investigate in the automation of the decision and mitigation process. The final decision is with the user, but it is infeasible to ask for user input each time, for instance, a service is consumed (these services are to a large extent consumed on lower layers of the technology stack). The establishment and management of user-friendly trust policies are required.

Caretakers: Markus Brunner, Michel Riguidel, Norbert Niebert, Pierre-Yves Danet, Theodore Zahariadis, Volkmar Lotz (author of this draft, alignment with other caretakers pending)

Participants: : same as listed in caretakers plus research community people invited to workshop in October 7 2009.

Points of agreement:

- Need to have less formal event(s) to explore greater synergies between research communities;
- Difficulties with parallel panel sessions during the FI Technical days (eg. T&I and Content or Networks);
- Between official FIA events, caretakers spend disproportionate amounts of their time dealing with administrative aspects eg. locating / inviting speakers and topics, instead of more pro-active and productive technical discussions amongst the members in the other FIA domains areas.

Points of Discussion:

Holding workshop on 7th October 2009 to prepare for FIA Stockholm with the following objectives:

4. To bring together FIA domain members (in a less formal setting than the FIA events) from the **Trust and Identity FIA community** with the members of the other FIA domains: **Future Content Networks, Management and Service-aware Networking Architectures, Future Internet Service offer, Real World Internet, Socio-Economics, Future Internet Research and Experimentation Software and Services,**
5. To provide an opportunity to review **cross domain Trust and Identity issues**, building on the achievements so far (in annex, list of documents from FIA Bled, Madrid, Prague, ..)
6. Allow for open and frank discussions on what the important **multi-disciplinary requirements and challenges** are for a Trustworthy Future Internet, especially in relation to privacy and identity, trust platforms and experimental facilities

Follow up actions:

Reference: In Madrid (Dec. 08) and Prague (May 2009), the Future Internet Assembly workshops held initial dedicated sessions on these topics, organised by the Trust and Identity caretakers.

Does this topic require a follow-up discussion in Valencia? Yes

If yes, specify draft title:

What does Future Internet mean for enterprise?

Contribution received from Man-Sze Li – FISO

Problem Statement: What will the Future Internet deliver for Enterprises?

How to ensure that the full potential of the Future Internet is accessible to, relevant for, and put to use by European enterprises including SMEs?

The vast majority of enterprises are going through hard times. This is expected to have a knock-on effect on enterprises' adoption of ICT. In its mid-term review of i2010, the European Commission reported that many parts of the EU still lagged behind in adopting ICTs⁵. In particular, the use of ICTs for transactions with business partners was still limited to a small subset of enterprises; only 15% of all enterprises were selling online and slightly fewer had established automatic links with their business partners⁶. This picture is expected to further deteriorate for the present period.

However, the present crisis may also present a unique opportunity to embrace change and usher in a new era for enterprise innovation. In this regard, the Internet of the future may be considered as *a universal business system* on which new values can be created by competing as well as collaborating enterprises, incumbent as well as new. Tomorrow's ICT may need to sustain a new kind of infrastructure as an open and level playing field, which is stable with an initial fixed set of services, in order to enable enterprises to build their (business) infrastructure at low cost. Individual enterprise systems of the future are likely to be leaner, more adaptive, flexible and portable; they also need to deliver value beyond economic value and drive innovation that meets a set of business objectives and sustainability concerns that are much broader than those of today.

Caretakers:

- Man-Sze Li, FISO, FISE, MANA

FInES Cluster Co-Chair, FInES Cluster Position Paper Chief Editor
http://cordis.europa.eu/fp7/ict/enet/ei_en.html

- Sergio Gusmeroli, FISO, RWI
FP7 COIN IP Technical Coordinator

<http://www.coin-ip.eu/>

- Michele Missikoff
FInES Research Roadmap Task Force Rapporteur

⁵ "Preparing Europe's digital future - i2010 Mid-Term Review", COM(2008) 199 final, 17.04.2008

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0199:EN:NOT>

⁶ "i2010 Annual Information Society Report 2008 - Benchmarking i2010: progress and fragmentation in Europe's information society" (EC Staff Working Document Vol. 1), SEC(2008) 470, 17.04.2008
http://ec.europa.eu/information_society/europe/i2010/docs/annual_report/2008/sec_2008_470_Vol_1.pdf

http://cordis.europa.eu/fp7/ict/enet/ei_en.html

Participants: tbc

<Names of the people who indicated interest at registration>

Points of agreement: tbc

<List here the points of agreement and a brief explanation of why/how a consensus has been reached. Include as well significant options that have been left behind.>

Points of discussion: tbc

<List here the sub-points which are still under discussion as well as a brief explanation of the open options for each>

Follow up actions: tbc

<List of agreed actions to do after Stockholm and before Valencia. These actions are to be undertaken by the 7 groups>

Reference:

- FInES Cluster Position Paper (Version 2), 8 July 2009
http://cordis.europa.eu/fp7/ict/enet/fines-positionpaper_en.html

Note: Final Version due for publication in early September 2009

- FInES Research Roadmap, First Public Draft planned for publication in October 2009

[Does this topic require a follow-up discussion in Valencia? Yes/No

If yes, specify draft title: ...]