Trust & Identity in the Future Internet
FIA Madrid, 9th December, 2008
11:00-16:00

Overall session Chair – Jim Clarke, WIT
# FIA Madrid Agenda

## December 9, 2008

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 – 9:00</td>
<td>Registration</td>
</tr>
<tr>
<td>9:00 – 9:30</td>
<td>Plenary Introductory Session</td>
</tr>
<tr>
<td></td>
<td>- Introduction, Guillermo Cisneros, Director of ETSI Telecomunicación, UPM</td>
</tr>
<tr>
<td></td>
<td>- European Perspectives &amp; Orientations, Joao da Silva, Director, European Commission</td>
</tr>
<tr>
<td></td>
<td>- Welcome message, Javier Uceda, Rector - President of UPM</td>
</tr>
<tr>
<td></td>
<td>- Opening Remarks, Francisco Ros, Secretary of State - Viceminister for Telecom and Information Society</td>
</tr>
<tr>
<td>9:30 – 10:45</td>
<td>National Future Internet Initiatives</td>
</tr>
<tr>
<td></td>
<td>- Germany – Volkmar Dietz, BMBF, “G-Lab”</td>
</tr>
<tr>
<td></td>
<td>- France – Francois Jutand, Scientific Director, Telecom Institute</td>
</tr>
<tr>
<td></td>
<td>- Finland – Reijo Paajanen, CEO of TIVIT, “Future Internet in the ICT SHOK initiative”</td>
</tr>
<tr>
<td></td>
<td>- Spain – Fernando Fournón, Executive President of Telefónica I+D “Internet del Futuro”</td>
</tr>
<tr>
<td>11:00 – 13:00</td>
<td>Future Content Networks (1)</td>
</tr>
<tr>
<td></td>
<td>Management &amp; Service Aware Networking Architecture (1)</td>
</tr>
<tr>
<td></td>
<td>Trust and Identity in FI (1: Trust)</td>
</tr>
<tr>
<td>14:00 – 16:00</td>
<td>Future Content Networks (2)</td>
</tr>
<tr>
<td></td>
<td>Management &amp; Service Aware Networking Architecture (2)</td>
</tr>
<tr>
<td></td>
<td>Trust and Identity in FI (2: Identity)</td>
</tr>
<tr>
<td>16:30 – 18:30</td>
<td>Future Internet Service Offer (1)</td>
</tr>
<tr>
<td></td>
<td>Real World Internet (1)</td>
</tr>
<tr>
<td>11:00 – 13:00</td>
<td>Future Internet Service Offer (1)</td>
</tr>
<tr>
<td></td>
<td>Real World Internet (1)</td>
</tr>
<tr>
<td>11:30 – 13:00</td>
<td>Usage of Experimental Facilities based on Use Cases</td>
</tr>
</tbody>
</table>

## December 10, 2008

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 – 11:00</td>
<td>Future Internet Service Offer (2)</td>
</tr>
<tr>
<td></td>
<td>Real World Internet (2)</td>
</tr>
<tr>
<td></td>
<td>Usage of Experimental Facilities based on Use Cases</td>
</tr>
<tr>
<td>9:30 – 10:45</td>
<td>Closing Plenary Session</td>
</tr>
<tr>
<td></td>
<td>Cross ETP Vision, David Kennedy on behalf of the ETPs. (15 minutes)</td>
</tr>
<tr>
<td></td>
<td>Summary of Achievements, by the Breakout Session Rapporteurs (7 times 5 minutes, 3 slides)</td>
</tr>
<tr>
<td></td>
<td>Forthcoming FIA conference in Prague, Gabriela Krcmarova (10 minutes)</td>
</tr>
<tr>
<td></td>
<td>Closing message by Joao da Silva (10 minutes)</td>
</tr>
</tbody>
</table>
Opening of session, objectives & format

- explore how the common themes in Trust (morning session) and Identity (afternoon session) 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,

- Input to our research roadmap for trust and identity in the future internet

- what and how we can use experimental facilities to test and illuminate how it all fits together in practice.
Trust & Identity in FI-Session format

Trust session
11:00 - 14:00

Identity and Privacy session
14:00 – 16:00

Present position paper
Present input from projects

Keynotes

Panel session – walkthrough a number of scenarios/use cases

Experimental facilities

FIA Path to Prague
Trust & Identity in FI Strategy - background

- Position paper covers five ‘lanes’
  - Lane 1 – Trust
  - Lane 2 – Identity and Privacy
  - Lane 3 – Security
  - Lane 4 – Trustworthiness
  - Lane 5 – Non technology topics – governance, social, regulations, ..

- Concentration for FIA Madrid is on
  - Lane 1 – Trust
  - Lane 2 – Identity and Privacy
Trust & Identity in FI Strategy - roadmap

Lane 1. Trust
Lane 2. Identity and Privacy
Lane 3. Security
Lane 4. Trustworthiness (Cross-cutting)
Lane 5. Non technical topics

Future Internet Assembly

Future Content NWs, FI Service Offer, MANA, Real World Internet, Socio-economics, Experimental Facilities
Trust session 11:00 - 14:00
Chair Michel Riguidel, ENST

- Presentation of Position paper, Lane 1, Trust
  - Volkmar Lotz, SAP

Keynote
- ‘Trust in the Future Internet’, Sachar Paulus, Paulus.consult
Trust session 11:00 - 14:00

Chair Michel Riguidel, ENST

- **Trust** – Sachar Paulus, Paulus.consult, RISEPTIS

- **Management and Service-aware Networking Architectures for Future Internets** – Syed Naqvi, CETIC, RESERVOIR project

- **Future Content Networks** - Theodore Zahariadis, Synelixis, SEA, AWISSENET, projects

- **Real world internet** - Mirko Presser, University of Surrey, SENSEI project
Presentation of Position paper, Lane 1, Trust
Volkmar Lotz, SAP
A Simple View of the Future Internet...

Applications, Business Ecosystems, Communities, etc.
Service Delivery Platforms
Value-added / business services
Fundamental services
Network: Protocols and Devices

Internet of Services
Internet of Things
... and its characteristics

Layered, but augmented by a number of cross-cutting dependencies

Multitude in scale compared to the current Internet, billions of entities including things

Spontaneous and emerging behaviours and unanticipated new usages

Pervasive digital environment, heterogeneous infrastructures, terminals and technologies

User-centricity and usability is critical

Enablement of the “Internet of Services” and its new business models
Trust Challenges and Expectations

Trust spans all layers of the Future Internet

Scale of Future Internet and its impact on trust
- Persons, devices, things, services, organisation
- Billions of heterogeneous entities

Transparency, Accountability and Responsibility
- Balanced approach
- Compartmentalisation

How to build the desired trust
- The role of PKI --> EU-wide / Global Trust Centres?
- Reputation, observation, attestation
- Spontaneous behaviour, reacting to events
Trust in the Future Internet

Prof. Dr. Sachar Paulus
paulus.consult
My concept of Trust

- Trust = willingness to take risk in a given context
  - ex: rental car, bank account, being married
- Necessary prerequisite: „get back or blame“ option
  - either: damage recovery
  - or: damage extension
- Fact: if you can neither recover nor blame,
  - you don‘t trust (cannot have trust relationship)
  - you have faith (which may be good, but is something different)
How to realize Trust?

- By providing damage recovery options
  - mainly: contracts
  - prerequisites: legal entities, activity logs, defined and agreed transactions
    ‣ Accountability

- By providing damage extension options
  - mainly: reputation
  - prerequisites: openness, visibility, commonality
    ‣ Transparency
Trust into the Future Internet

● For businesses:
  - defined legal environment, allowing for an upfront risk assessment
    ‣ Measurability

● For individuals:
  - maintenance of societal rights, privacy, right to be „left alone“, right to „time“ and „memory loss“
  - but as consumers: defined legal environment
    ‣ Multi party security requirements
Trust in the Future Internet

- You cannot outsource trust
  - you can outsource trust management (the security folks can and will take care of that part)
- Trust is an intrinsic value of transactions, relationships, contexts
- Every entity in the future internet must decide about which level of trust to offer
- Technical requirements:
  - Transparency, Measurability & Accountability
Scenario: Cloud Computing

The players:
- LocService
- CRMAp
- PaymentApp
- OrderEngine
- Mobile
- SmartTag
- PoliceCase

The protocols:
- RF
- SMTP
- SMS
- WAP
- WAP

The scenario:

1. LocService interacts with CRMAp via RF and SMTP.
2. CRMAp interacts with PaymentApp via SMS.
3. PaymentApp interacts with OrderEngine via WAP.
4. OrderEngine interacts with Mobile via WAP.
5. Mobile interacts with SmartTag via WAP.
6. SmartTag interacts with PoliceCase via WAP.
7. PoliceCase interacts with CRMAp via WAP.

The diagram illustrates the interactions and communication protocols between the players in the scenario.
Questions: Cloud Computing

Q1: Where is the data located?
Q2: Who runs the services?
Q3: Who runs the servers?

==> Accountability is key!
Trust issues: Cloud Computing

I1: privacy
I2: roll-back option / memory loss effect
I3: public security demand

==> Transparency is key!
One word to privacy

- Privacy = Anonymity (of action) against specific parties for a defined time span
- Services must respect the right of the user
  - need technical design capabilities to address multi-party (security, accountability, privacy) requirements:
    - Local Accountability
      - example: undeniable signatures
- Services must realize „memory-loss effect“
  - example: „data older than X must be made invisible to specified parties“
Now ... how?

- Security, Privacy, Trust are non-functional design properties
  - there are necessary functional parts, but that is not the issue
- Strong need to fire them in
  - there is no way to outsource, add them later or simply wait for a miracle
- Treat them as CORE design requirements when developing concepts and ideas
Summary

- Trust = willingness to take (understood) risk
- Technical prerequisites:
  - Accountability, Transparency & Measurability
- Treat them (mainly) as non-functional requirements
- Process approach necessary
- Get from an art to science!

- End of keynote………..
Trust session 11:00 - 14:00  
Chair Michel Riguidel, ENST

- **Trust** – Sachar Paulus, Paulus.consult, RISEPTIS

- **Management and Service-aware Networking Architectures for Future Internets** – Syed Naqvi, CETIC, RESERVOIR project

- **Future Content Networks** - Theodore Zahariadis, Synelixis, SEA, AWISSENET, projects

- **Real world internet** - Mirko Presser, University of Surrey, SENSEI project
An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required.

*International Telecommunication Union*

Can future internet services be modeled as a generic entity?
Future Internet Services

- Bunch of high-level services
- Security comes first
- Broader scope, outreach, ...
- Higher flexibility
- User-centric Service Frontend
- Support for Vertical Handover
FIS – from Google search …

Active services  Reactive services  Proactive services  Federated services
Software as a service  Resource as a service  Communication as a service
Process as a service  System as a service  Information as a service
Loosely-coupled services  Service utilities  Guaranteed quality of service
Open services  Highly available services  Interoperable services
Universality of services  Accessibility of services  Software-based services
Data services  Information services  Knowledge services  Virtual services
Virtualization of services  Value added services  Semantically rich services
Autonomic services  Personalized services  Localized services
Network-aware services running over the service-aware networks
Collaborative services  Intelligent services  Business-oriented services
Secured services  User-centric services
FIS – Convergence Areas for Trust

- Scalable set of services
- Federation of services
- Universal discovery of services
- Interoperable services
- Resilient services
- Dependable services
- Interactive user-centric services
RESERVOIR Security Challenges

- Guarantee the security of applications and associated data, allowing end users to specify requirements for service tasks
  - Protecting a service from other services running in the same virtual environment
  - Protect confidentiality of stored service data
    - Need to protect service data relating to amount of resources consumed, accrued billing...
  - Handle requirements induced by multi-tenancy
    - The Service Definition will need to support special requirements/restrictions due to multi-tenancy
      - Example: I don’t want my data residing on the same physical storage as my competitor
  - Protecting a VEE from other VEEs running in the same compute node
RESERVOIR Trust Challenges

- Guarantee the ability of SOI vendors to interoperate in a secure way, building mutual trust and defending themselves from misbehaving vendors or end users.
  - Ensure the authenticity and integrity of management entities, compute nodes and VEEs.
  - Secure communication of sensitive end user and vendor data over local and wide area networks (message integrity and confidentiality)
  - Protecting the access to the management interfaces

- Security policies for a site must be securely discoverable in order for cross-domain migration
  - i.e. only allow migration to sites with the same security policy
Trust & Identity in the Future Internet

Future Content Networks

Theodore Zahariadis
Synelixis Ltd
Prosumer’s Internet

Future Internet will enable seamless, personalised, trusted and PQoS-optimised multimedia content delivery, across heterogeneous broadband networks

In Future Internet everyone may be:
- Content Producer/Provider
- Content Mediator
- Content Consumer

Move from Client-Server to P2P and subscribe/push models
Identity vs Content Groups
Content Issues

- Who is asking for my content?
- Who is at the other side of the peer? Is he trusted?
- What is he allowed to do with my content? Watch? Edit? Forward?
- Will he pay for privileged access? What business can I make?
- Is buying content over the Internet safe?
- Is my privacy protected?
- Is my content protected in the network?
- Is my email/communications protected?
- Are my children protected from being exposed?
- Is my PC/network protected while allowing my edge device/RG to be exposed as a (streaming/service) peer?
- Is my access guaranteed/protected? (network/service robustness)
(Ad-hoc/Sensor) Networks Issues

- Is the (sensor) node the one that it appears to be?
- Is the sink node the one that it appears to be?
- Which is the most trusted path between two nodes (or between two domains)?
  vs.
- Which is the most energy efficient path between two nodes (or between two domains)?
- Are data protected in the network?
- Is my privacy protected in a sensor network?
- How can I achieve maximum security with minimal energy consumption?
- Is the service provision node trusted (and has it the energy to provide the service in a robust way)?
- How can I detect intrusion and isolate intruders? What traffic patterns should I identify?
- How can my network recover based on distributed trust?
Identity requirements

a) Authorization
b) Authentication
c) Trust/trustworthiness
d) Privacy
e) Integrity
f) Security/encryption/cryptography
g) DRM
h) Robustness
i) Parental control
j) Software Viruses
k) Spam/Advertisements
l) Denial of service
Real world internet

Mirko Presser,
University of Surrey,
SENSEI
Trust in SENSEI

- Vision of the future internet (RWI part)
  - Billions of WS&AN will provide sensing and actuation services
  - Billions of consumers will use these services

- Alice is one of these consumers
  - She wants to get information from a WS&AN island that she does not yet know → trust issues
    - 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

- Instruments to address these issues include classical certification mechanisms, reputation systems, and possibly more approaches…
Identity and Privacy session 14:00 – 16:00
Chair Nick Wainwright, HP

Presentation of Position paper, Lane 2, Identity & Privacy
– Volkmar Lotz, SAP

Keynotes

- ‘State-of-art, mid-term perspectives of identity management’ – Caspar Bowden, Microsoft

- ‘How to provide privacy in the cloud, privacy-friendly identity, minimization of data through claim frameworks’ - Phil Janson, IBM
Identity and Privacy session 14:00 – 16:00
Chair Nick Wainwright, HP

- **Network** - Joao Girao, NEC, DAIDALOS
- **Future Internet Services** - Kajetan Dolinar, SETCCE, PERSIST Project
- **Real world internet** – Neeli Prasaad, Aalborg University ASPIRE Project
- **Identity** - Caspar Bowden, Microsoft
- **Privacy** – Phil Janson, IBM
What is an identity in the Future Internet?
- Persons, devices, objects, services, organisation
- Billions of heterogeneous entities

The need for independent privacy-preserving identity schemes

Privacy-friendly service provision
- Claims-based

Usability and Flexibility

Usage control enforcement
- TC, “virtual” TC
An example of a strategic privacy technology and implications for policy

Caspar Bowden
Chief Privacy Adviser, Microsoft EMEA
9th December 2008
Future of the Internet - Madrid
Privacy vs. Security?

“Everybody knows”:

- to get authorized to access a system a person must disclose their identity?
  - …but suppose that’s not true

- the accepted principles of privacy protection are technology-neutral
  - …but perhaps some technologies are intrinsically better for privacy than others

- cyber-security and privacy is a tradeoff
  - …but perhaps both can be improved together
The trouble with PKI ("public-key infrastructure")

- "certificate" contains identity attributes
  - verifiable by a digital signature
- must disclose entire certificate in order for verification mechanism to work
  - ....results in disclosure of "excessive" data for any particular transaction
- Cert ID is inescapable persistent identifier
  - "Too bad!" - just the way the maths works
- Well, no...can do (much) better
  - 20 years of research into "multi-party" security and privacy techniques
Minimal disclosure tokens

Name: Alice Smith
Address: 1234 Crypto, Seattle, WA
Status: gold customer
DOB: 03-25-1976
Reputation: high
Gender: female
Prove that you are from WA and over 21

Name: Alice Smith
Address: 1234 Crypto, Seattle, WA
Status: gold customer
DOB: 03-25-1976
Reputation: high
Gender: female

Which adult from WA is this?
Authentication ≠ Identification

Prove that you are a gold customer

Name: [Blurred]
Address: [Blurred]
Status: gold customer

U-Prove
Prove that you are a gold customer.
Applications

- Avoid unnecessary ("excessive") data trails in transactional systems
  - Access services based on proof-of-age-limits, or class of entitlement
  - reduce liabilities, exposure to breaches / insider-attacks
  - safe private-sector use of data in national eID systems

- Verifiable audit trails
  - can show different parts of trail to different parties according to need-to-know

- Apply different policies to different risks
  - revocable tokens which preserve privacy

- These capabilities are counter-intuitive!
Evolution of law and technology

- **1970s – 1st Data Protection laws, Fair Information Practices**
  - ...invention of asymmetric cryptography
- **1980s – Council of Europe 108, OECD principles**
  - ...invention of concept of cryptographic “blinding”
  - PKI standards, Digital Signature laws
  - ...refinement of “blinding”, fraud-control techniques
- **2000s – APEC, security breach notification laws**
  - federated identity system architecture
  - ...rich family of “multi-party” security/privacy techniques
- **2010s - is the law still technology-neutral ?**
  - What does personal information mean ?
  - What does data minimisation mean ?
  - What does identifiable mean ?
A dialogue between policy and technology

- “de-identification” doesn’t really work
- Advances in re-identification algorithms are undermining distinctions between personal and non-personal data
  - (e.g. Shmatikov – PETS Award winner 2008)
- Profiles based on “anonymous” data result in people being treated differently – but with no transparency?
- What to do....
  - continue legal fiction of effective remedies and tech neutrality
  - ...or perhaps can reinterpret privacy principles?
- Three ideas:
  1. Regulate the application of re-identification and profiling
  2. Consider the specific legal grounds when justifiable for a system to “recognize” a person without their consent
  3. Build systems around concept of individual access
Fundamental legal and policy issue

- Systems increasingly collect transactional data identifiably – and disproportionately (various Art.29 WP Opinions)
  - “side-effect” is that a database of all transactions is retained (e.g. for retrospective fraud tracing), but can the database be used for surveillance purposes as a “free by-product”?
    - (also remember CoE R.87 requires specific law authorizing blanket collection....)

- Art.8 of ECHR:
  - state should limit intrusions into privacy to that which is necessary, if possible case-by-case according to the circumstances of the individual (and according to law, foreseeability etc.)

- Use of certain strategic PET techniques is mandatory under ECHR (subject to reasonable feasibility), because it infringes privacy only to an extent that is individually proportionate.
  - “balancing” with positive obligations of ECHR Art.2 (“right to life”)?
  - Osman vs. UK 1998: “real and immediate risk to life of an identified individual or individuals from the criminal acts of third parties.” => there is no “free pass” for surveillance systems
“Strategic” PETs in a legal framework

- **Strategic PETs**
  - improve both privacy and cyber-security
  - have to designed into the whole system
  - are “conceptually generic” – only realistic option

- Others:
  - ? “Differential Privacy” in statistical databases
  - ? Transport-layer identifiability (e.g. ToR)

- **Consider phase-in timelines**
  - public-sector lead by example ?
    - EU Commission Communication 20.9.03
    - Procurement guidelines referencing strong data minimization, unlinkability as basic capability ?
Privacy Challenges in the Future Internet

Phil Janson (pj@zurich.ibm.com)
Manager, Security & Cryptography
IBM Zurich Research Laboratory
IBM Academy of Technology
Problem Statement

- The physical world is forgetful - The digital world is not
  - No train conductor or bar tender remembers all the ID cards they see in a day
  - But every visited service provider is eager to log as much as it can about users
    – allegedly to serve them better, usually to pester them with more marketing junk

- Content accumulates ever faster
  - Much collected behind our backs by sensing devices (e.g. surveillance cameras)
  - Much also volunteered by unsuspecting users themselves (e.g. social networking sites)

- Data mining capabilities continue to increase exponentially
  - incl. open crawling over the web and public info records

- Our privacy shrinks as we grow up
  - The whole life of millennium children will be on the web for all to see
    by the time they start applying for jobs (or looking for spouses ;-)

- The digital world will not only record but increasingly control the physical one
  - Location-based services are only a harmless basis to start from
  - Spontaneous behavior will emerge

- Accountability is hard in a global world for lack of global regulations
Challenges

- Security is about controlling **access** (to info)
  Privacy is about controlling **accuracy and usage** (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 – **user-centric** 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.)
Federated, user-centric, privacy-enhanced identity management

User

Identity Provider

Transactions unlinkable

Relying Party

Transactions unlinkable

SwissPassport
UserId = ay6789bx42
SNo = 4534653324
Firstname = “Jane”
Lastname = “Doe”
Bdate = 1970/03/12

SwissPassport[Bdate] < 1989/03/28
Enc1 = SwissPassport[Sno]

Enc1

4534653324

Decryption Authority
Privacy-enhanced (Hippocratic) Database technology

This solution consists of –

a) **Active Enforcement Component**
   - Fine-grained
   - Database-agnostic
   - Application transparent

b) **Compliance Auditing Component**
   - Supports compliance
   - and accountability
Research Directions

1. Policy languages for policy description, composition, evaluation, matching, translation, etc.
2. User interfaces to manage and deal with policies as needed/desired
3. Cryptographic support for additional functional requirements
   - Delegation, escrowing, revocation, restrictions
   - Dynamic cross-domain service composition
   - New scenarios and applications
   - Built-in support requirements
4. Leveraging eID, e-passport, e-banking, SIM and other cards
   - Putting the technologies on identity provider chip cards
5. Key/credential management, esp. recovery through events of life
6. Sticky policy enforcement through Trusted Computing infrastructure
7. Compliance monitoring tools
8. Privacy in computing clouds
9. Standards, infrastructures, open source packages, education, regulations, legislation
Joao Girao, NEC, SWIFT, DAIDALOS project
Cross-layer use of Identity
Identity in the Future Internet

- Goal is to bring Identity Management to the network
  - Enable access and reachability across domains
  - Make Identities of people, services, things, software modules a part of the future Internet architecture
- The Future Internet could (should?) be … the identiNET
  - **Identity** as the future *end point* of communication
    - whether user, service, thing, device or software module
  - Support access, (non-) reachability, ubiquity
  - Privacy can be dealt with vertically thus reducing the danger of conflicting policies and mechanisms
  - non-walled garden business is enabled
Privacy Protection Cycle
(A concept for a systemic privacy protection)

Kajetan Dolinar

FIA Madrid, 9th December, 2008, 11:00-16:00
Digital Community

- Actors collaborating in electronic transactions
- Mostly peer-to-peer backed up with infrastructure
- Trust, privacy and security play integral role
- Only a systemic and systematic approach can assure for a sustained protection
PERSIST Privacy Protection Cycle

At first data are held private. Protection before disclosure:
1. Write privacy policy
2. Check peer reputation
3. Negotiate privacy policy
   - regard privacy preferences
   - yields a privacy agreement
4. Produce suitable identity
5. Make up direct protection
   - conservation: archive to preserve integrity, time
   - confidentiality: encrypt, obfuscate
   - configure access control
   - insure data against abuse

The data are disclosed. Protection after disclosure:
1. Sticky policy
   - defines actions allowed on the data attached
2. Entertain access control
   - by credentials, ACLs
   - by purpose (should match allowed from sticky policy)
3. Record all actions on data
   - type of action, purpose, time
data and sticky policy
4. If suspicion of abuse
   - authority does audit of privacy audit trail
5. If abuse
   - insurance compensates the curtailed person
   - insurance penalizes the perpetrator
6. If severe abuse
   - police and court take over
Real World Internet (IoT, etc.): Identity Management

● Neeli Prasad, Aalborg University ASPIRE Project
scenario...

National and International zones

Macrocells:
- Suburban
- Regional
- National

Microcells:
- City-centers
- Highways

Picocells:
- In-house

Personal Area Network (PAN)

Megacommunications (1 Tb/s)

Ramjee Prasad - 2008
IoT: My World

Source: Dr. Shingo Ohmori, 2006
Identity implications

What does ‘identity’ really mean? Refining the elusive definitions of identity in the Real World Internet

Identity or credential?

User centric identity management?
Identity requirements

- In order to access a device or service, the user needs to provide an identity that can be authenticated and authorised by the RWI components.
- The provision of such an identity needs to be user friendly.
- In addition it should be possible to exchange the identity without affecting the privacy of the user.
- Concepts of anonymity and pseudonymity should be adapted to develop a coherent Identity Management solution, which is interoperable with the existing addressing, naming and Identity management systems.
- Scalable and efficient methods for protection of user identity will be defined.
Martin Potts - Martel
On behalf of the FEDERICA project

Future Internet Assembly
Madrid, December 9th, 2008
FEDERICA Goals

Current Status

Next Steps
FEDERICA Goals

Current Status

Next Steps
FEDERICA Goals

- Create an e-Infrastructure for researchers on Future Internet. Allow researchers a complete control of set of resources in a “slice”, enabling disruptive experiments. “Slices” are a set of (virtual) network and computing resources which are independent (so can be used for different roles/identities). “Slices” may communicate with the General Internet.

- Support research in virtualization of e-Infrastructures integrating network resources and nodes capable of virtualization (V-Nodes). Topics might include multi-(virtual)-domain control, management and monitoring, security, virtualization services and user-oriented control.

- Strive/engineer for reproducibility of experiments.

- Open to interconnect / federate with other e-Infrastructures worldwide.

- Gain experience of what may represent the next generation of European Research and Education Networks.
FEDERICA Goals

Current Status

Next Steps
Core Infrastructure

MILANO
ITALY
GARR

GERLANGEN
GERMANY
DFN

POZNAN
POLAND
PSNC

MILANO
ITALY
GARR

PRAGUE
CZECH REPUBLIC
CESNET

Now operational.

1 Gbps Ethernet
Work plan outline

Slices

Layers available to the User

Layers NOT available to the User

FEDERICA Substrate centrally managed

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
FEDERICA Network Layer substrate
FEDERICA Data Link layer substrate
FEDERICA Physical Layer substrate

Month 1 (Jan 2008)
Month 10
Month 21
Month 30

Time availability
The user requests an Infrastructure made of L2 circuits, un-configured virtual nodes, to test a new BGP version.

1. Create user credentials and authentication, create entity “Slice”
2. Create Virtual Gateway (in red) to bridge the user from outside into the slice
3. Create resources and connect them as specified by the user
FEDERICA Goals
Current Status
Next Steps
Each new PoP will be equipped with a smaller switch/router (Juniper EX family) and one (or two) V-Nodes.

1 Gbps Ethernet
Federating FEDERICA

- Data plane is IP based (packet switched Ethernet)
- External physical connectivity can be accepted
- Access is currently regulated by humans, but is intended to be automated (trust and security is needed)
- Resources representation schemas are not yet available (needed to describe the available services)
FEDERICA - Onelab

A Onelab node can be hosted in a FEDERICA slice. That specific node has full control of its network interface and circuits up to the egress from FEDERICA into General Internet.
How To Request Access

- A user information pack is almost ready and will be available in the web site, containing:
  - Simple Memorandum of Understanding
  - Acceptable User Policy, Access Rules
  - Guide for proposals, Brief Introduction to FEDERICA
  - Technical template, Feedback template

Send requests for using FEDERICA to:
- fed-upb (at) fp7-federica.eu

Information can be requested from:
- info (at) fp7-federica.eu
Thank you for your attention
Contribution to experimental facilities

- Trust & Identity requirements for experimental facilities
- Experimental facilities Current provision

Integration – does it all work together? Scale – does it work at internet scale? Threats – is it robust to attack?
Contribution to experimental facilities

- Experimental Faculties – current provision
  - Someone from experimental facilities
- Trust and Identity – requirements from experimental facilities
  - Some one presenting aggregated scenarios??
Follow up activities for preparation for FIA Prague

Lane 1. Trust
Lane 2. Identity and Privacy
Lane 3. Security
Lane 4. Trustworthiness
Lane 5. Non technical topics

Future Content NWs
FI Service Offer
MANA
Real World Internet
Socio-economics
Experimental facilities

Future Internet
End of Session

- To become part of the Trust and Identity community, please contact Zeta Dooly zdooly@tssg.org
- Michel Riguidel, ENST
- Volkmar Lotz, SAP,
- Nick Wainwright, HP
- ............