

- » BOOST PERFORMANCE
- » REDUCE COST
- » INCREASE AGILITY
- » ENHANCE CRM
- » SHORTEN TIME TO MARKET
- » DRIVE INNOVATION
- » IMPROVE EFFICIENCY
- » INCREASE ADAPTIVITY
- » ENABLE BUSINESS TRANSPARENCY
- » FOSTER REGULATORY COMPLIANCE



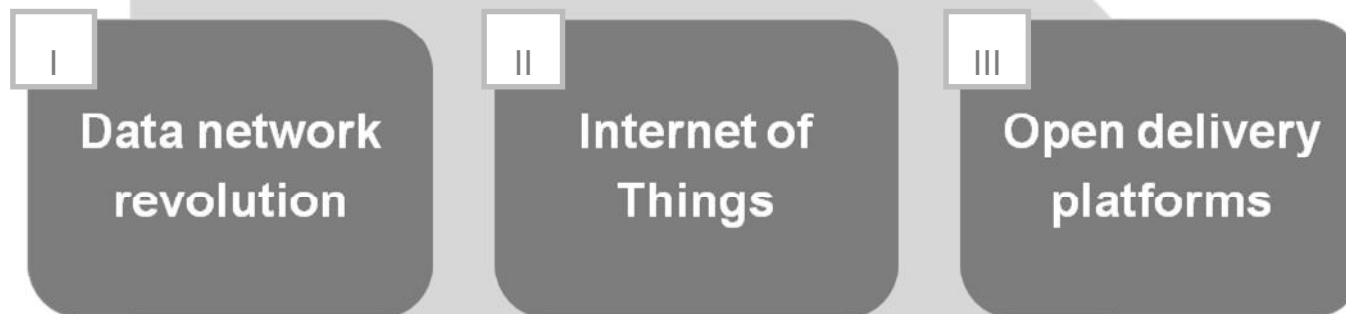
CONSULTING > SOLUTIONS > OUTSOURCING

Future Internet in Europe: An Overview of Related Initiatives and ICT Security Challenges

Aljosa Pasic
Johannesburg, August 16th, 2011

1. Problem Statement
2. EU Approach to Future Internet
3. FI Core Platform Architecture and Security Research
4. Other Initiatives in Europe
5. Few Open Challenges
6. Conclusions

The changes in ICT and business models



I
Data network revolution
New data networks, using LTE are being deployed. This means a huge data capacity increase for the customer and a technical challenge which will require a huge investment

II
Internet of Things
New intelligent devices and sensors offer new possibilities for information and analysis and open the door to new automation and control possibilities

III
Open delivery platforms
A new way of service deployment:

- Use only what you need and pay only what you use (Cloud)
- Open innovation ecosystems where apps from different parties may be combined and delivered multi-screen

Consumers: What people demand



General Challenges and Security Research

Manage explosion of data / info

- Data has growth 10-fold in last 5 years (from ~177 exabytes in 2006 up to ~ 1,700 exabytes in 2011): scale in prosumers and sensors will make data grow even at higher rates
- Need to filter and exploit what is relevant for me, now, here
- Need to preserve privacy, manage confidential data, multilevel security, data loss prevention...

Smart solutions for daily life situations

- People want to find and easily access applications that assist them in daily life situations: this would transform home and cities in better places to life
- Access should be provided anywhere, anytime, from any device
- Context-aware Security for “constraint-driven” environments (tiny devices, usability rules...)

Improved means for communication and collaboration

- People wish to share content/data and applications with others
- They wish to learn what has been useful/interesting to others, in real-time, on the go
- Reputation and trust become decision drivers

Internet as a critical infrastructure

- Internet is not longer an experimental tool: people expect it should secure by design
- People entrusted their life (e.g. lifelogging) and their business to internet so they want to govern access to their data and to have “user-centricity”
- People want internet to handle dynamicity just like physical world : dynamicity of privacy, trust and security solutions

Today



Vice-President of the European Commission, Neelie Kroes, launched the Future Internet PPP in Brussels on 3 May 2011

<http://www.future-internet.eu/>



FI-WARE Project Kick off at Telefonica I+D Offices in Madrid

<http://www.fi-ware.com>



FI-WARE project and partnership



Working together to make it possible:

- ✓ New services for everybody
- ✓ Smart applications
- ✓ Innovative business models

Providing the Technology Foundation

- Standard interfaces.
- Open to other actors (SMEs)
- Scalable and demand oriented (cloud)

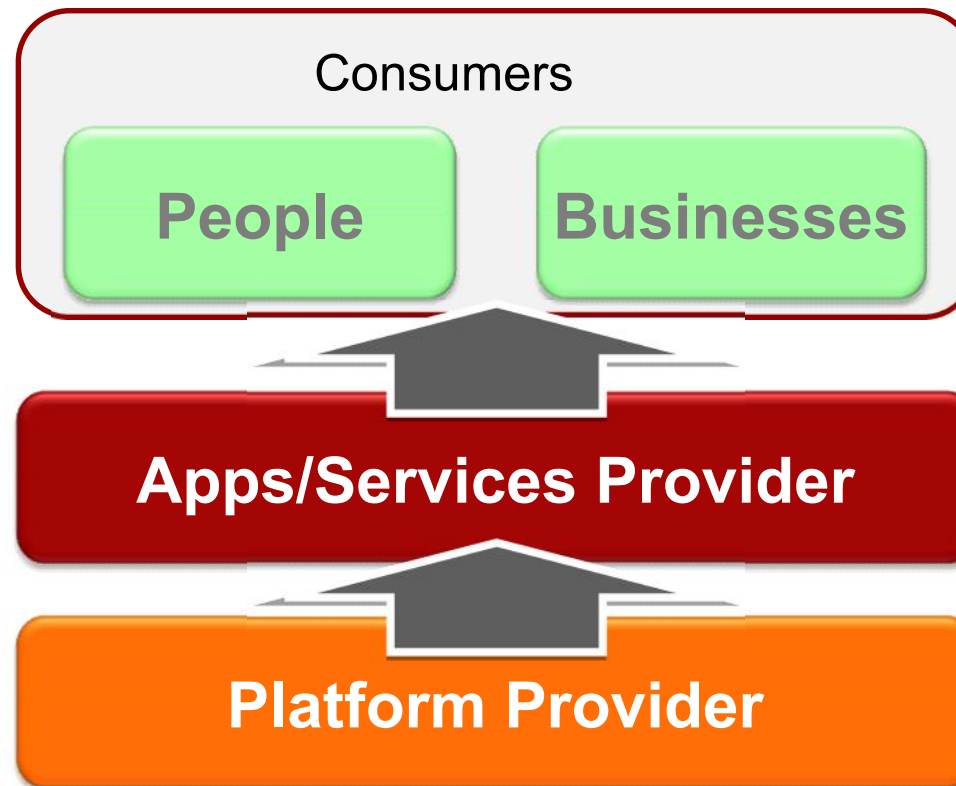
Our objective: create a solid basis for the Internet of the Future



The VISION



- *FI-WARE will be a technological foundation to satisfy the demands of application/services providers and consumers across various usage areas, stimulating and cultivating a sustainable FI service ecosystem*



Security Research in FI-WARE

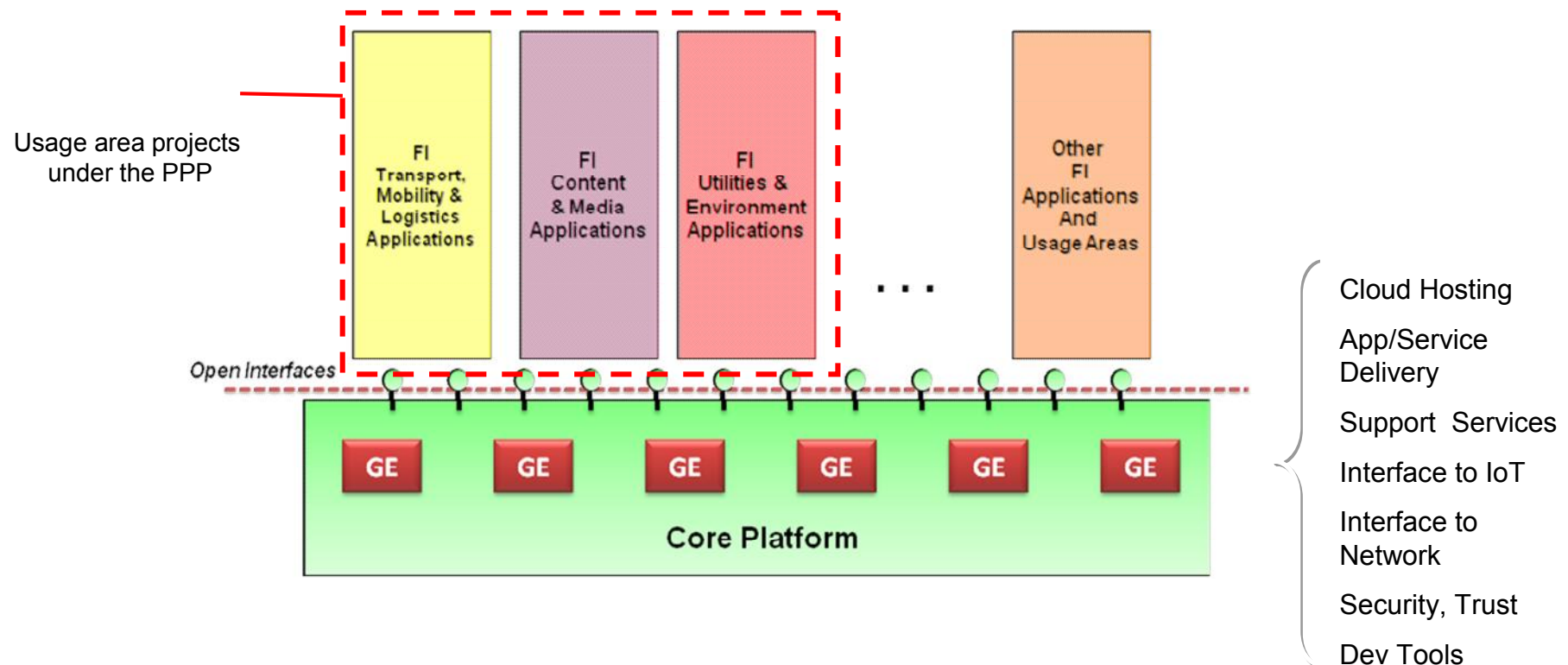


- Security Monitoring
 - Collection of heterogeneous information and standardisation
 - Risk analysis and correlation
 - Decision making support and simulations
 - Visualisation and reporting
 - Forensics
- Generic Enablers
 - Identity and privacy
 - Authorisation and Usage Control Policies
 - Auditing
- Context-based security and Compliance
 - Security properties and service descriptions
 - Selection and deployment of reconfigurable solutions
 - Monitoring aspects
- Optional security enablers (e.g. protected data etc)

Elements & Functions of FI Core Platform



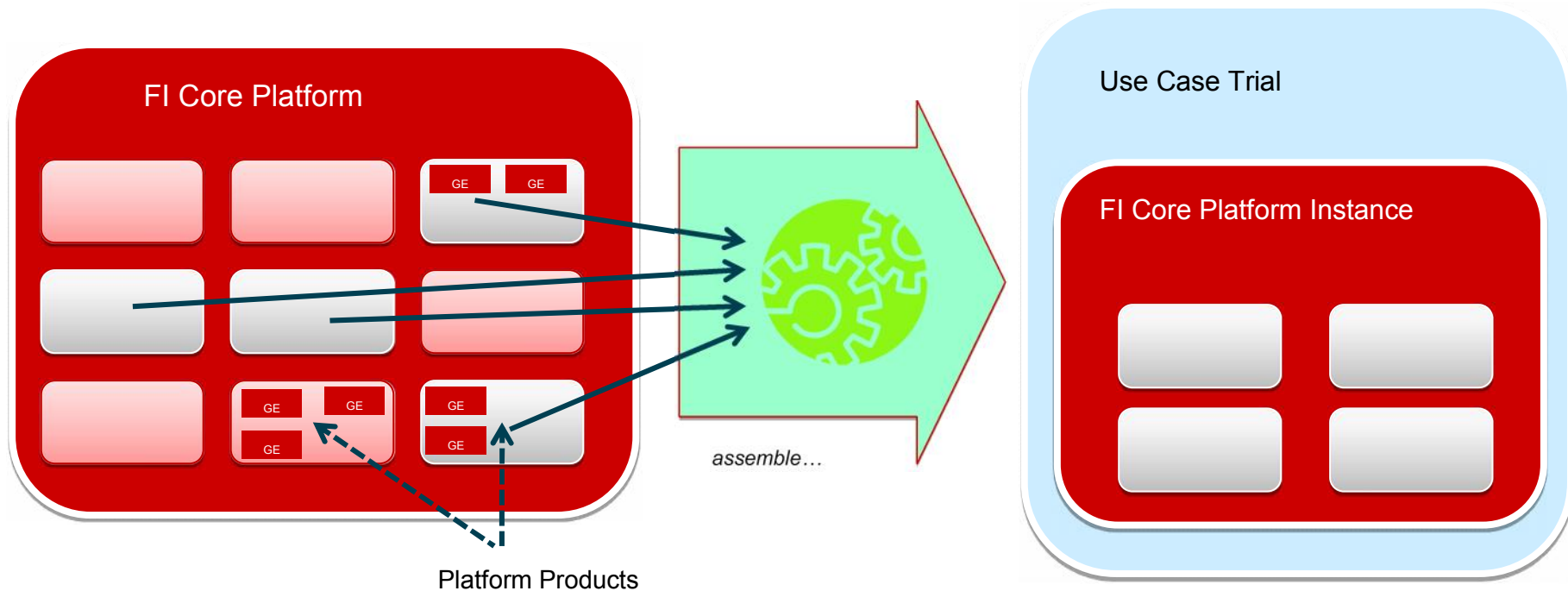
- The FI Core Platform comprises a set of technological “Generic Enablers” which are considered general purpose and common to several current and future “usage areas”
- Generic Enablers (therefore, the FI Core Platform) will provide open interfaces for development of Applications



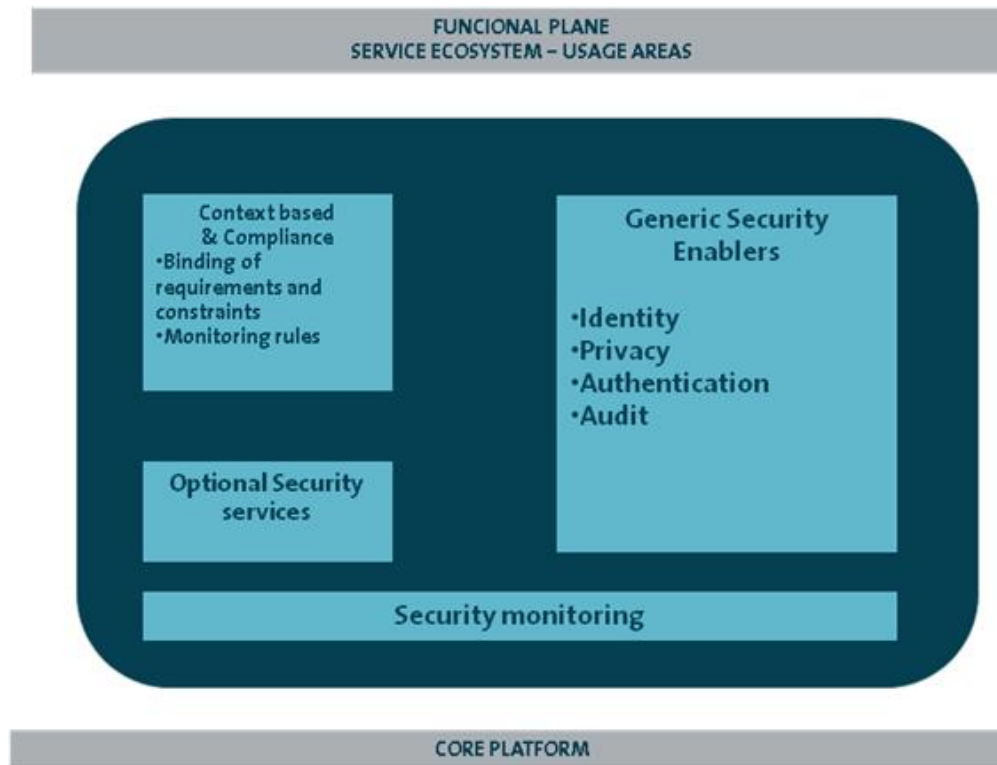
Core Platform Instances and Use Case Trials



- Future Internet Applications run on top of “FI Core Platform Instances” built upon selection and assembly of “Platform Products” implementing “Generic Enablers” of the “FI Core Platform”
- Use Case trials will consist on application scenarios running on top of FI Core Platform Instances, involving real users



Security and trust in Pilots



Trust and Security:

- Spanning from infrastructure and “things” all up to the application layer
- Common enablers for identity, authentication and authorization
- User privacy management
- Protection against any malicious action damaging its services and reputation

Operations

- Lifecycle Management Support
- End user usage accounting
- Platform usage accounting
- Support for Analytics

<http://www.fi-ppp.eu/projects>



European Future Internet Portal



ENVIROFI

OUTSMART



INFINITY
INfrastructures for the
Future Internet commuNITY



ADVANCE YOUR BUSINESS >>

- EP3R Partnership focuses on Internet Resilience and Internet as a Critical Infrastructure
 - Area 1: Key assets/ resources/ functions for the continuous and secure provisioning of electronic communications across countries
 - Area 2: Baseline requirements for security and resilience of electronic communications
 - Area 3: Coordination and cooperation needs and mechanisms to prevent and respond to large scale disruptions affecting electronic communications

Other EU Initiatives (II)



- EOS working group on ICT security focuses mainly on cybersecurity and privacy in Homeland security and Defence sectors
- Transversal issue: Architecture & procedures for secure exchange of data
- Transversal issue: Standardisation, validation & certification of solutions & services
- Specific issue: Pilot MS / local competence & capabilities to face cyber attacks
- Specific issue: EU Information Sharing and Alert Systems
- Specific issue: EU cyber crime center/platform
- Specific issue: Pilot & validation cyber resilience of C.Is
- Specific issue: Cloud security
- Specific issue: EC CERT / network

Other EU Initiatives (III)



- Trust in Digital Life focuses more on “consumers” and societal aspects of ICT security:
 - Technology and Requirements,
 - Use cases,
 - Law and Technology
- SSEDIC thematic Network focuses more on digital identity and e-ID
 - use of e-ID in leisure, government, transport
 - Technical issues & architecture for e-ID
 - Legal & others

Digital agenda and security



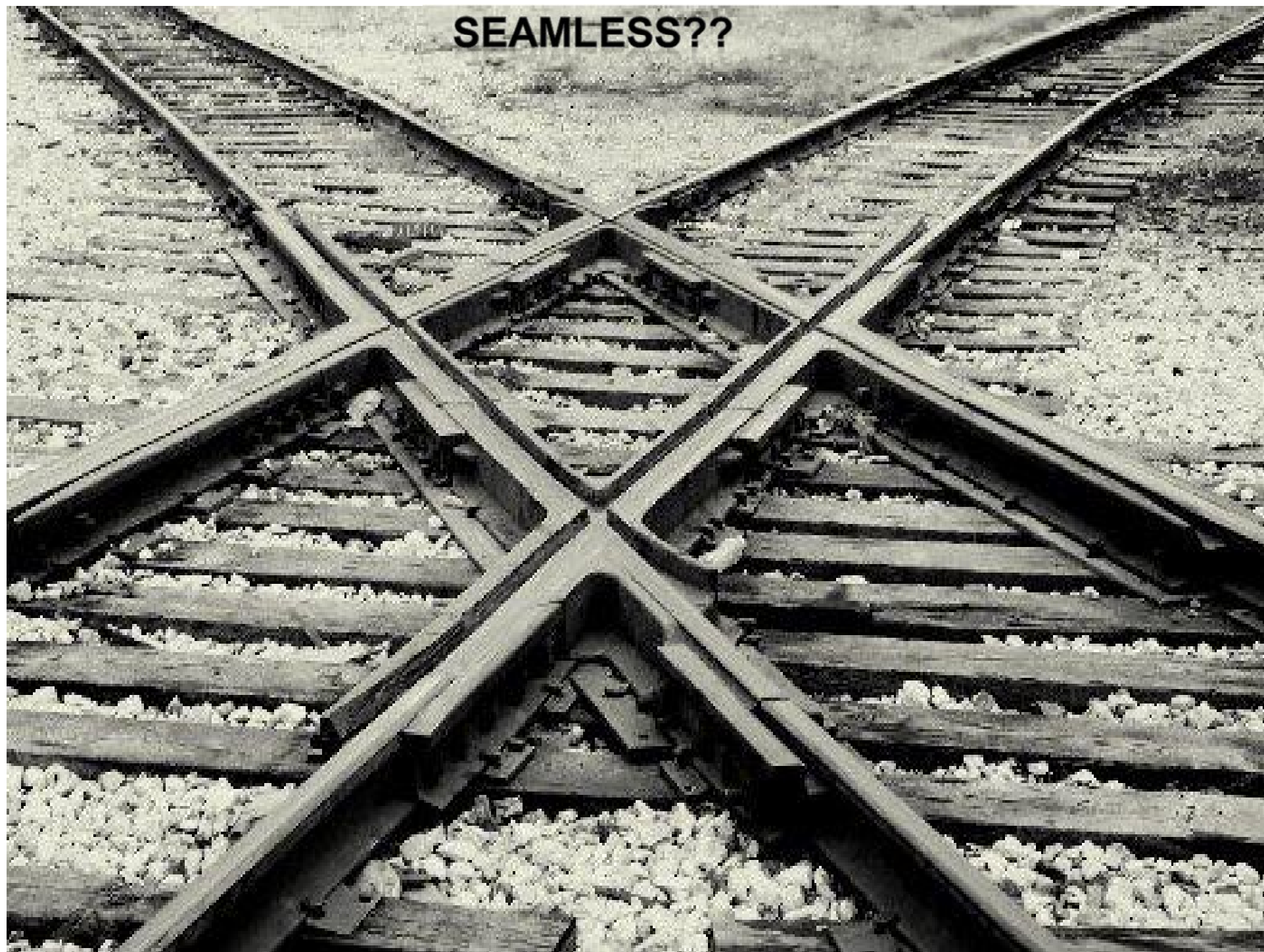
- [Action 38: Member States to establish pan-European Computer Emergency Response Teams](#)
- [Action 39: Member States to carry out cyber attack simulations](#)
- [Action 41: Member States to set up national alert platforms](#)
- [Action 56: Member States to Engage in large-scale pilots financed by the Competitiveness and Innovation Programme](#)

Digital agenda and Security (II)



- [Action 33: Support EU-wide cyber-security preparedness](#)
- [Action 35: Guidance on implementation of Telecoms rules on privacy](#)
- [Action 32: Strengthen the fight against cybercrime at international level](#)
- [Action 33: Support EU-wide cyber-security preparedness](#)
- [Action 30: Establish a European cybercrime platform](#)
- [Action 41: Member States to set up national alert platforms](#)

SEAMLESS??



Issue 1: Seamless security management



- The more context sources leads to better solution, but it has to be manageable
- Automation of physical & virtual security context information gathering and processing should be a must
- Automated processing (e.g. correlation) needs also some reasoning on security info (weight, priority etc)

ADAPTIVE??



Issue 2: Dynamic security management



- The existence of appropriate infrastructure (smartmeters, sensors, services etc) is pre-requisite, but security agents should be able to configure sec mechanisms ad-hoc
- We need adaptation (e.g. of secure service delivery), personalization, dynamic reconfiguration...



Internet
Future is not
what it used
to be

Paul Valéry

French critic & poet
(1871 - 1945)

Conclusions (II)



International collaboration in Future Internet research
is ESSENTIAL in order to avoid mistakes from the
past !!!!

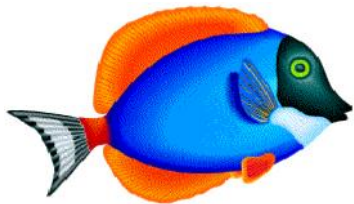


Aljosa Pasic

1969-xxx



Thank you



FACING TECHNOLOGICAL CHALLENGES TOGETHER
Aljosa Pasic (Atos Origin)
aljosa.pasic@atosorigin.com