# FIA session 1.4 on Building a Trust Framework for Future Internet Services and Infrastructures

*Rapporteurs: Laurent Ciavaglia (Alcatel-Lucent, FP7-IP UNIVERSELF)*
*Other contributors: Amardeo Sarma (NEC, TDL consortium), Aljosa Pasic (Atos, FP7-NoE NESSOS), Henning Arendt (@BC)*

## Session summary

Amardeo Sarma introduced the session with a comprehensive overview outlining the multi-facet nature of trust and stressing the need to ensure end-to-end trust across applications, services, systems or devices. Trust frameworks need to go beyond trusted systems and include those that use, operate, or access it in order to enable multiple Levels of Assurance (LoA) for different end-to-end environments and application scenarios towards a continuum and total trust management. The three dimensions addressed in the session are: 1) *network-centric trust*, dealing with autonomic networks and their behavioural models, in terms of compliance/conformance to operator and service strategies; 2) *component-centric trust*, dealing with software components, services and their respective security aspects; and 3) *user-centric trust*, dealing with authentications, identity management, operational issues, socio-economic and psychological factors, vendors, end-user, etc. assuming a growing number of stakeholders.

Amardeo presented the Trust Framework Provider developed within the Trust in Digital Life consortium [1] focusing on the novel attributes provider role. In his presentation, Aljosa Pasic argued about the path from assurance to assumptions management as proposed by the NESSOS project [2] based on devising mechanisms to validate or manage assumptions including secure services architecting and engineering; design- and run-time validation; simulations; ability to monitor, measure, test and predict the security status of a system; reputation and similar mechanisms and not forgetting to link the physical/real world. Laurent Ciavaglia supported the network-centric point of view dealing with trust in decentralized and autonomously controlled systems. Five requirements and the UniverSelf project [3] approach to meet them have been detailed: 1. Trust must be measurable, 2. Trust must be domain-specific, 3. Trust must be model-driven, 4. Trust must be propagated end-to-end, 5. Trust must be certified. The UniverSelf project has developed a model based on trust predicates that are defined at the design phase as abstract behaviours, and verified at run-time as fully qualified ones, and prove to have the power of policies – check them once and re-use many times; rewrite them to cater for new behaviours. Finally, Henning Arendt highlighted the user perspective based on the use of protection goals together with “Privacy by Design” and “Privacy by Default” paradigms. Privacy by Design needs to be explicitly included as a general binding principle into the existing data protection legal framework. This would compel its implementation by data controllers and ICT designers and manufacturers while offering more legitimacy to enforcement authorities to require its effective application in practice. A panel debate concentrating on the 5 motivating questions concluded the session: What needs to be protected? What is the end-to-end trust model? What are the metrics? How to enable end-to-end trust? Is trust an element to consider only at the design-time or run-time? What actions should be taken towards research and standardization? What is changed by the introduction of software and autonomic systems? A sequel of the session as part of the next FIA meeting in Aalborg, Denmark (10-11 May 2012) is envisaged based on the feedback received.

## Links and info

FIA program: http://www.event.fi-poznan.eu/online/?view=session&session_id=145

[1] Trust in Digital Life http://www.trustindigitallife.eu/

[2] NESSOS FP7 NoE http://www.nessos-project.eu/

[3] UniverSelf FP7 Project www.univerself-project.eu/

Presentation No.1: Introduction by Amardeo Sarma, NEC

Read more: http://www.event.fi-poznan.eu/online/?view=session&session_id=146

Presentation No.2: Large Scale Authentication Architecture by Amardeo Sarma, NEC

Read more: http://www.event.fi-poznan.eu/online/?view=session&session_id=146

Presentation No.3: Trust Assumptions Trustworthiness Assurance by Aljosa Pasic, Atos

Read more: http://www.event.fi-poznan.eu/online/?view=session&session_id=146

Presentation No.4: A view on trust in autonomic networks by Laurent Ciavaglia, Alcatel-Lucent

Read more: http://www.event.fi-poznan.eu/online/?view=session&session_id=146

Presentation No.5: Trustworthiness by integration of informational self-determination and privacy requirements by Henning Arendt, @BC

Read more: http://www.event.fi-poznan.eu/online/?view=session&session_id=146