

ESFORS is a Coordination Action that aims at bringing together the European stakeholders for security and dependability Information and Communication Technologies (ICTs) to address the security and dependability requirements of emerging software service platforms.

ESFORS is positioned to support the emergence of a software and services platform architecture ensuring the incorporation of security and dependability best practice. This project will act as a bridge between the software and services application community and the security and dependability community.

KEY OBJECTIVES

- *Promoting networking of European stakeholders on security and dependability strategy*
- *Guide direction of Security and Dependability research in the Strategic Research Agenda on Software and Services for FP7 and the NESSI European Technology Platform*
- *Strengthen interplay between research and policy communities within soft & services arena*
- *Build industry awareness of the need for security in software-based services and systems*

First Project Outcomes

- The focus is a Service-centric view → Components out of different domains (different security and dependability qualities), different organizations (formal agreements required) and shared between many consumers (advanced confidentiality and isolation requirements).
- In future services and systems, trust will have to apply across the heterogeneous network infrastructure supporting the service oriented architectures.
- Research should involve a wider community than those traditionally involved in IT security (lawyers, social scientist, auditors and economists).
- The foundation for a trusted infrastructure lies in components that have security built-in.
- Society and Policy Considerations in ICT Security: Publicity of attacks lower the trust that society places on ICT-based services → need to investigate ways to promote society trust in the net.
- Security technologies must not introducing barriers to usability → Security technologies that deal with people must remain user-friendly while secure.

Partners



PROJECT CONTACT INFORMATION: <http://www.esfors.org>
esfors@esfors.org

ESFORS Position Statement

The service centric view (i.e. the notion that more IT will be delivered through the service lifecycle) is changing the way IT infrastructure and applications will be managed and delivered. The impact of this ICT innovation is evident as the most of the daily activities will be performed using the internet and the related web technologies. Ease of access and ability to share information is required along with the need to increase and improve the relationships among the different actors involved in this virtual world.

At a very high level of granularity, it is not difficult to claim that the main implication of this innovation will be at the following levels:

At the business level, as this will change the way the business is approached. The business context will change from closed doors, physical isolation environments where defending data and systems was the "must" and security was intended merely as a protection means to environments and contexts. The new paradigm will include openness, unbounded, dynamic, interconnected actors that need to share content and resources and where trust should become an enabler and not a disabler.

At the architectural level, to provide the support and the enablers to this new business and interaction environment. These architectures and infrastructures should be flexible enough to react to the dynamics of the environment and provide resiliency features.

Last but not least, at operation level: It is obvious that the services that will be offered to the users and stakeholders will be such that they should rely on their effectiveness and worthiness. These operations will be such they will have to be managed by interactions protocols that cannot be defined "a priori" but that will suffer the dynamics and the unpredictability of the operative context and environment.

Provided this background, the three levels where the ICT innovation is currently having impact is further detailed below; however, there are many unanswered trust questions which need to be addressed implying issues concerning security and dependability that will have a deep impact on the three identified levels above.

To better identify security and dependability challenges and issues that could arise within this new operative environment, it was decided to clarify the context further with the identification of three different scenarios within three operative domains: the large enterprises domain, the SMEs domain and the more generic user/citizens domain.

ESFORS Dissemination

- **Trust in the Net.** Vienna, Austria. February 2006
- **SecurIST workshop.** Brussels, Belgium. March 2006
- **ESFORS Presentation at NESSI Steering Committee.** Brussels, Belgium. April 2006
- **ISAS 2006: The 3rd International Service Availability Symposium.** Helsinki, Finland. May 2006
- **IST Africa.** Pretoria, South Africa. May 2006
- **IST mobile and wireless communications summit.** Mykonos, Greece. June 2006
- **EC IST FP6 Inter-Project Workshop on Security 2006.** St. Augustine, Germany. June 2006
- **WORKSHOP on Joint Software and Service Development, Security & Dependability.** Paris, France. September 2006
- **First NESSI Trust, Security & Dependability Working Group Meeting.** Paris, France. September 2006
- **International Carnahan Conference on Security Technology.** Lexington - Kentucky, USA. October 2006
- **eChallenges 2006.** Barcelona, Spain. October 2006
- **IST 2006.** Helsinki, Finland. November 2006



PROJECT CONTACT INFORMATION: <http://www.esfors.org>
esfors@esfors.org