



# IST 2006 Helsinki SecurIST Networking session

Nov 22<sup>nd</sup> 2006  
Room 203a



## Overview of the SecurIST Project

- European Security & Dependability Task Force (**STF**)
- Advisory Board (**AB**)
- **Today's networking session is split into**
  - Strand 1 – long term vision
  - Strand 2 –short-medium term vision
  - Open discussion (25 minutes)



## Agenda for networking session

### Strand 1: Reportage of medium – long term vision.

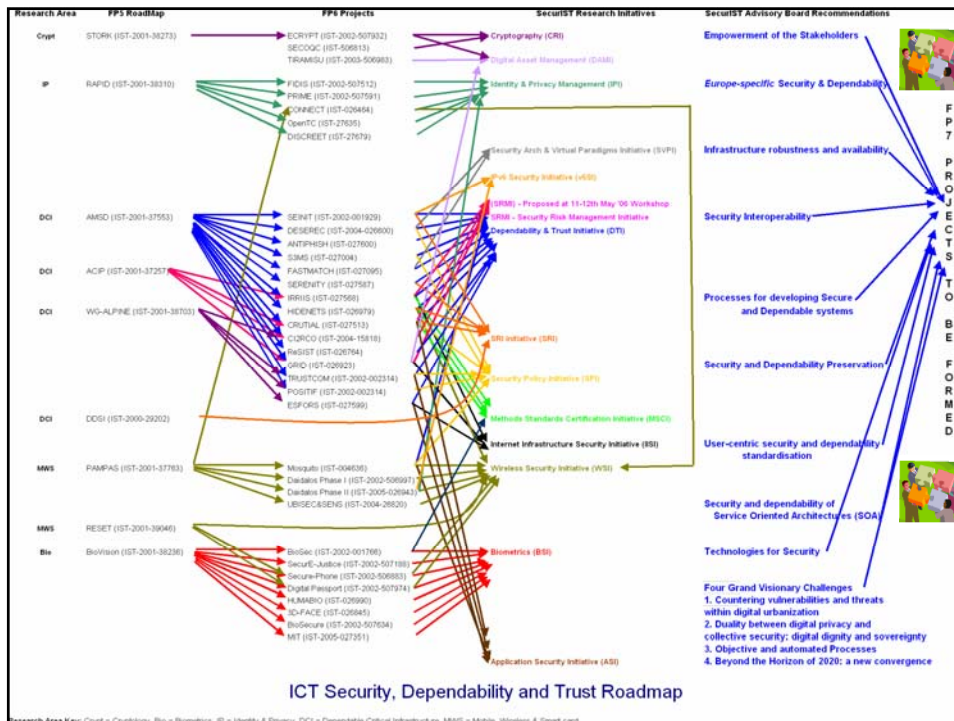
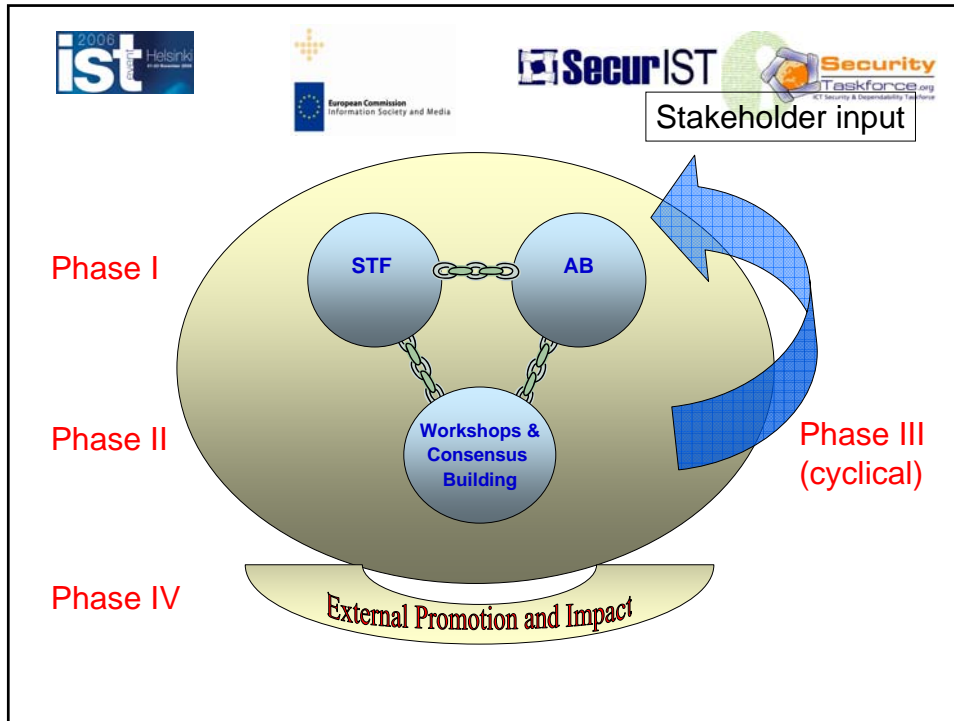
A panel or number of short presentations representing the SecurIST Advisory Board and prioritized recommendations for future research in Trust, Security and Dependability.

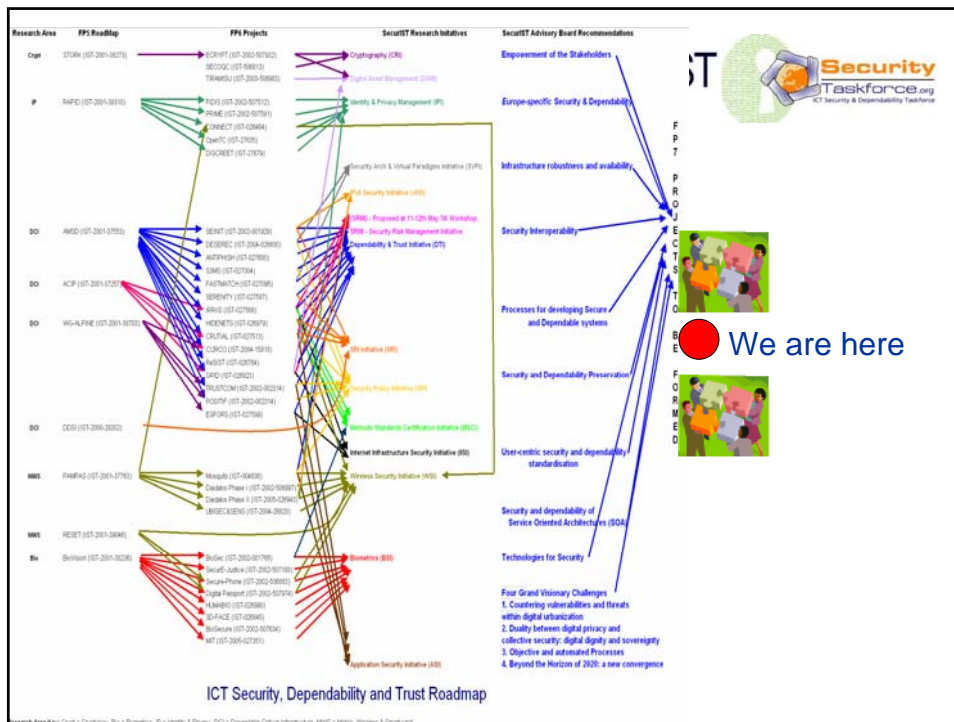
09:00 – 09:05	Opening welcome, objectives and format. Introduction to SecurIST Advisory Board Recommendations	Willie Donnelly SecurIST Project Co-ordinator, Waterford Institute of Technology, Ireland
09:05 - 09:15	Countering vulnerabilities and threats within digital urbanization.	Bart Preneel, Katholieke University Leuven, Belgium
09:15 -09:25	Duality between digital privacy and collective security: digital dignity and sovereignty.	Kai Rannenber, Goethe University, Germany
09:25– 09:35	Objective and automated Processes.	Tobias Christen, Zurich Financial Services, Switzerland



**Strand 2: Consortia building: Short – Medium term vision.** A panel/number of short presentations from current researchers in the Security, Trust and Dependability area that have requested a slot and already identified project proposals for Call 1 of FP7 and gaps in current research in Europe. WIT/TSSG will facilitate this co-ordination group as we continue preparation for FP7.

09:35 – 09:40	Security Challenges in FP7	Gwendal le Grand, ENST, France
09:40–09:45	Security Risk Management Research Challenges	Eyal Adar, Cyber White Knight, Israel
09:45 – 09:50	Global TSD Assurance in Systems of Systems	Ruben Alonso,ESI - Tecnalía
09:45 – 09:50	Multilayer Approach for Dependability and Security System	Antonio Gomez-Skarmeta, Universidad de Murcia, Spain
09:50 – 09:55	Secure Usability	Sebastian Hoen, Albert-Ludwig University, Freiburg, Germany
09:55 – 10:00	European Microsoft Innovation Center’s FP7 Security & Privacy research interests	Joris Claessens, Microsoft, Germany
10:00 – 10:05	Virtualisation for attack mitigation algorithm contextability of learning	Atta Badi, University of Reading, UK





- 
- AB Recommendations**
1. Empowerment of the Stakeholder:
  2. European Security and Dependability:
  3. Infrastructure robustness and availability:
  4. Security Interoperability
  5. Process for Secure and Dependable Systems Development:
  6. Security and Dependability Preservation
  7. End user centric security and dependability standardization:
  8. Security and Dependability of Service Oriented Architectures:
  9. Technologies for Security



The report also contains four Visionary Grand Challenges where possible (r)evolution might be anticipated.

**1. Countering vulnerabilities and threats within digital urbanization**

The security and dependability improvement for the expansion and globalization of digital convergence by 2010-2015 :

- *how to move from “clastro-security” (closed and ciphered world) to an “agora-security” (open and clear world)?*
- *how to move from static and standalone activities to a collaborative, network centric architecture vision with full mobility and full interactivity with people and reality?*
- *how to make the actors’ chain proportionally responsible and accountable for malevolent or erroneous actions?*



The report also contains four Visionary Grand Challenges where possible (r)evolution might be anticipated.

**2. Duality between digital privacy and collective security: digital dignity and sovereignty**

The second grand challenge concerns privacy issues of all the players – citizens, groups, enterprises, and states.

- *how to override the “big Brother” syndrome and the dark security?*



### **3. Objective and automated Processes**

*The third grand challenge is the obligation to attain a controllable and manageable world of complex digital artefacts by 2015 toward a provable security (predictability of faults, anticipation of threats).*

- *how to inject regular, quantitative techniques and engineering to make the field truly scientific?*



### **4. Beyond the Horizon: a new convergence**

*The fourth grand challenge is the preparation of a new convergence at a horizon of 2020 and beyond, which is the bio-nano-info-quantum "galaxy".*

The big question will then be:

- *how to protect the interfaces and to attain and maintain a security continuum?*



## Wrap Up



- **STF roadmap FP5 -> FP6 -> FP7**
- **Align within current WG Initiatives of STF or highlight missing elements**
- **As part of STF, continue to refine research priorities and challenges and be included to WP**
- **Focus on key areas for medium (2007 – 2010) and long term (2010 – 2013)**
- **Provide comments to Advisory Board Recommendations**
- **Develop consortiums to target results in these areas.**
- **Beyond SecurIST, STF will continue and we want you to be a part of this...**