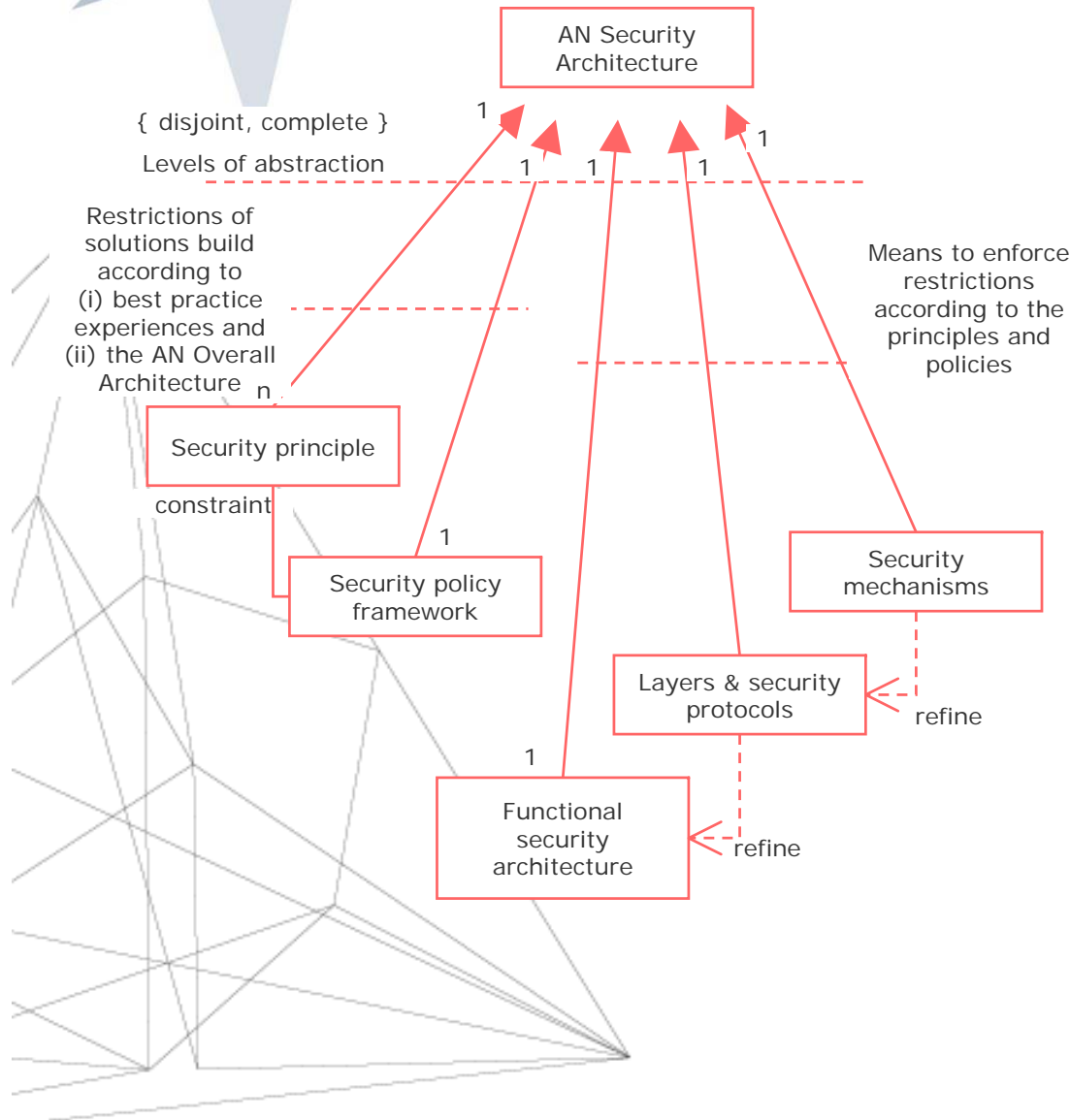


- Work in Progress: **IST Project Ambient Networks** (www.ambient-networks.org)
- Technology scope:
 - existing heterogeneous network technology
 - BANs, PANs, ad hoc networks, WLAN, 2.5G, 3G networks, and amenable for 4G
- Main **Security and Privacy Requirements** addressed
 - Ambient Networks shall provide a seamless, comprehensive and flexible security scheme (AN Security) that operates consistently across a dynamically shifting environment of constituent heterogeneous networks and component entities and services. AN Security shall cover a multiple network-operator/service-provider environment that is characterised by:
 - user friendliness and helpfulness, while remaining as far as possible invisible to the user;
 - smooth transition between different bearers and services;
 - trustworthy operation;
 - robustness and resilience under attack and mishap;
 - ease of management;
 - protection and privacy of user and network information and assets;
 - protection and privacy of identity and location;
 - accountability.

AN Security shall take into account regulatory and law-enforcement requirements. AN Security shall contribute to the overall availability and dependability of networks and services.

Mobile Adventure

Concept of the Main Elements of the Ambient Network Security Architecture



- **Levelled definition**, where the level indicates the degree of abstraction
- Higher levels **restrict / define** what is **allowed / possible** on the lower levels
- **Requirements and constraints are deduced by the models** (scenarios, business, trust, etc) for which we intend to build Ambient Networks

This work is conducted in "Ambient Networks" project.

This presentation has been produced in the context of the Ambient Networks Project. The Ambient Networks Project is part of the European Community's Sixth Framework Program for research and is as such funded by the European Commission.

All information in this presentation is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

For the avoidance of all doubts, the European Commission has no liability in respect of this presentation, which is merely representing the authors view.

Partners of the consortium are:

- Ericsson AB (project co-ordinator), Sweden
- Alcatel SEL AG, Germany
- British Telecommunications plc, UK
- Budapest University Of Technology And Economics, Hungary
- Concordia University, Canada
- Consorzio Ferrara Ricercha, Italy
- Critical Software S.A., Portugal
- DaimlerChrysler AG, Germany
- DoCoMo Communications Laboratories Europe GmbH, Germany
- Elisa Corporation, Finland
- Ericsson Eurolab Deutschland GmbH, Germany
- Ericsson Magyarorszag Kommunikacios Renszerek K.F.T., Hungary
- France Telecom SA, France
- Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung e. V., Germany
- Instituto De Engenharia De Sistemas E Computadores Do Porto, Portugal
- Kungliga Tekniska Hogskolan, Sweden
- Lucent Technologies Network Systems GmbH, Germany
- Lucent Technologies Network Systems UK Limited, UK
- Motorola Japan, Japan
- National ICT Australia (University Of New South Wales), Australia
- NEC Europe Ltd, UK
- Nokia Corporation, Finland
- Oy LM Ericsson AB, Finland
- Panasonic European Laboratories GmbH, Germany
- Rheinisch-Westfaelische Technische Hochschule Aachen, Germany
- Siemens AG, Germany
- Siemens AG Oesterreich, Austria
- Siemens Mobile Communications SPA, Italy
- Swedish Institute Of Computer Science AB, Sweden
- Technical Research Centre Of Finland, Finland
- Technische Universitaet Berlin, Germany
- Telecom Italia SPA, Italy
- Telefonica Investigacion Y Desarrollo SA Unipersonal, Spain
- Telenor Communication AS, Norway
- TeliaSonera AB, Sweden
- TNO - Netherlands Organisation For Applied Scientific Research, Netherlands
- University Of Surrey, UK
- Universidad De Cantabria, Spain
- University College London, UK
- University Of Ottawa, Canada
- Vodafone Group Services Limited, UK