Domenico Presenza (Engineering)

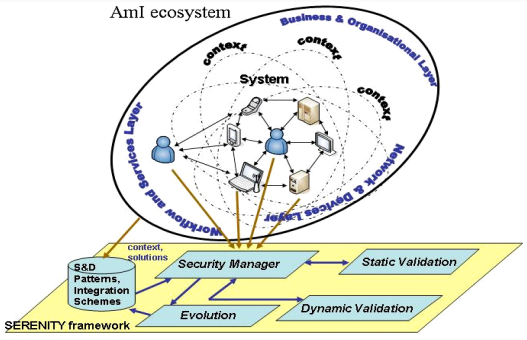
Resilient SERENITY

Using S&D Patterns to enhance resilience

Budapest - 22/03/07

The SERENITY Objective

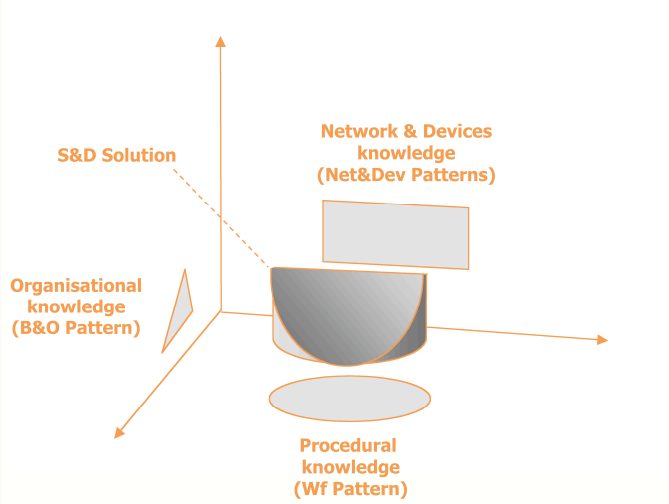
- To provide Security and Dependability (S&D) in Ambient Intelligence (AmI) scenarios.



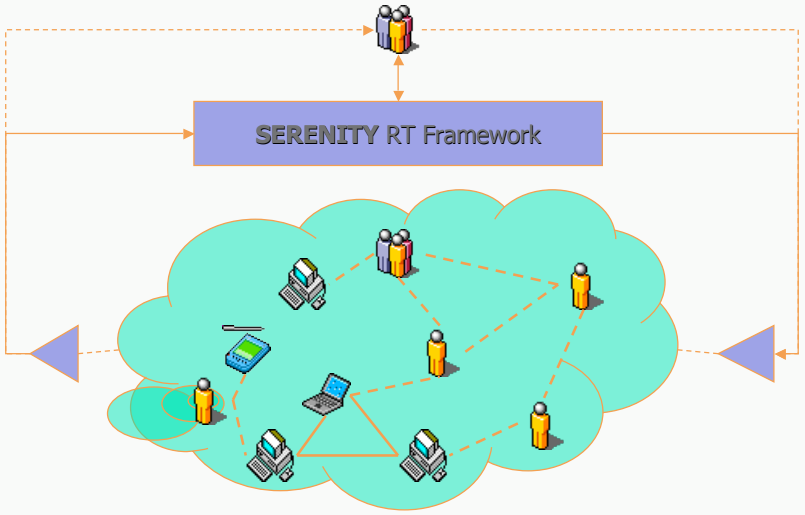
SERENITY Main Assumptions

- Security and Dependability knowledge can be coded (made explicit) through Security & Dependability Patterns (S&D Patterns);
- S&D Patterns can be integrated by means of Integration Schemes (IS);
- S&D Patterns can be monitored and, to some extent, enforced at run-time.

Aspects of S&D Solutions



SERENITY Run-time Framework



SERENITY about Resilience

- SERENITY is investigating whether S&D Patterns and Integration Schemes can be a tool to enhance the resilience of organisations by supporting run-time contextualisation of S&D management processes to the current situation.

S&D Patterns as RT Models

- An S&D Pattern/IS is used as an explicit representation of some portion of S&D Solution as perceived by Designers/Developers;
- Actors involved in S&D management interpret and adjust their behaviour to it;
- Prescribed part of the model are automatically interpreted and ambiguous/underspecified parts are left to the users for local adaptation, with tool support.

SERENITY Framework support

- The SERENITY RT framework will provide mechanisms for:
  - Monitoring integrity of S&D Patterns/IS and detecting deviations;
  - Monitoring status (QoS) of resources (services) available in the system;
  - Support coordination and communication of actors involved in the S&D management process;
  - Support on-line amendment of S&D Patterns/IS to reduce risks or cope with unexpected situations/threats.