

## PROJECT INFORMATION:

ANIKETOS is a collaborative project funded under the EU 7th Research Framework Programme. It is aligned to the strategic objective 1.4. Secure, dependable and trusted infrastructures defined by the European Commission in the FP7 ICT Work Programme 2009-2010.

- Start Date: 01 August 2010
- Duration: 42 months
- Total Cost: 14 M€



Contact: Dr. Richard Sanders  
[Richard.Sanders@sintef.no](mailto:Richard.Sanders@sintef.no)

Project Website:  
[www.aniketos.eu](http://www.aniketos.eu)

## CONSORTIUM:



# ANIKETOS

## Ensuring Trustworthiness and Security in Service Composition



The research is partly funded by the European Community's Seventh Framework Programme under grant agreement no. 257930

## Rationale

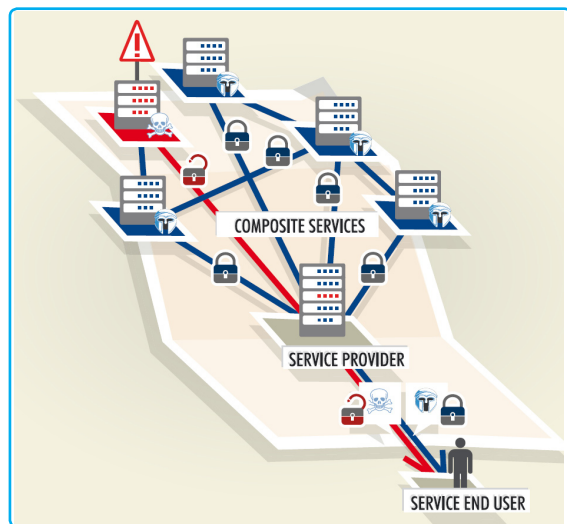
In an environment where services are offered by range of suppliers, users are likely to unknowingly invoke underlying services in a dynamic and ad hoc manner. Thus, the applications that end users experience may be composed of multiple services from many different providers, and in this setting the end user may have insufficient guarantee that a particular service or service supplier will offer the security claimed.

Aniketos will align existing and develop new technology, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composite services, addressing service developers, service providers and service consumers.

## Objectives

Aniketos establishes and maintains trustworthiness and secure behaviour in a constantly changing service environment through:

- **The development of an integral platform**, which provides methods and facilitates tool support for secure interoperable service implementation, composition, adaptation and management.
- The definition on how to efficiently analyze, solve and share information on how new **threats and vulnerabilities can be mitigated** or how services can adapt to them.
- The promotion and contribution to best practices, standards and **own certification work related to security and trust**.



- **The demonstration and evaluation of the practical use of security techniques**, platforms, patterns and tools in ordinary development of software and service with end-user-trials.

## Key Challenges

In order to achieve these objectives, a multi-disciplinary effort involving research and industrial/technology partners and business end-users addresses the following key challenges:

- **Design-time support:** Future Internet services cannot be created the same way as we traditionally have been doing. We need to be able to define safe and secure behaviour (offered/required).
- **Runtime composition:** We need improved mechanisms for establishing trust and verification of safe and secure service behaviour between multiple service providers.
- **Service adaptation:** Run-time security adaptation to an evolving environment of threats and operating conditions.
- **Evaluation and testing** in a realistic setting with services critical to the future European infrastructure.

## Project Results

Aniketos platform for creating and maintaining secure and trusted composite services.

## Project Impact

- Critical services/systems of **Future Internet achievement of the security requirements**.
- **Future Internet service infrastructure management and trustworthiness assurance**.
- New secure **system certification and standards**.

