★ Companies able to set up and operate secure, trustworthy virtual organisations can add real value to their business. **Phillippe Massonet** of the GridTrust project explains just why developing a vertical approach focused on improving trust, security and privacy is so important

Trust and security for next generation Grids

The commercial world is making ever more complex demands of its IT services. Global economic competition is intense, leading an increasing number of companies to look towards their IT services to provide them with a competitive advantage.

This is a situation which has served to stimulate ongoing IT research and development – into Grid services in particular – with a view to meeting the needs of global business. GridTrust, an FP6 European research project coordinated by CETIC in Belgium (Centre of Excellence in Information and Communication Technologies), is one of the prime movers in this area.

> Logistics is not a product, it is a service; a service that moves its customer's products from one place to another. Big haulage or courier companies may be chosen for their brand, but what ultimately makes the difference is the quality and price of the service.

The project's overall objective is to develop technology capable of managing trust and security for Next Generation Grids or service-based Grids, a task crucial to ensuring Europe's future economic prosperity.

CETIC proposes a vertical approach focussed on tackling the key issues of trust, security and privacy (TSP) from the requirement level right down to the application, middleware and foundation levels. CETIC's main emphasis is on developing models and tools which can assist in reasoning about trust and security properties within NGG architecture.

The GridTrust consortium is comprised of a large, diverse panel of industrial partners, end users, SME's and European research groups, an aspect of the project which makes it well placed to meet the complex demands of modern business. The industry sectors covered include (among others) requirement engineering, Grid technology and security. Meanwhile, the project's close links with Moviquity, HP and Interplay provide an important opportunity to test, refine and validate the GridTrust framework within a typical SME environment, including innovative applications such as "inter-enterprise knowledge management" and "distributed authoring".

Furthermore, Moviquity and De Agostini are committed to implementing and exploiting the project results at the foundation and middleware levels.

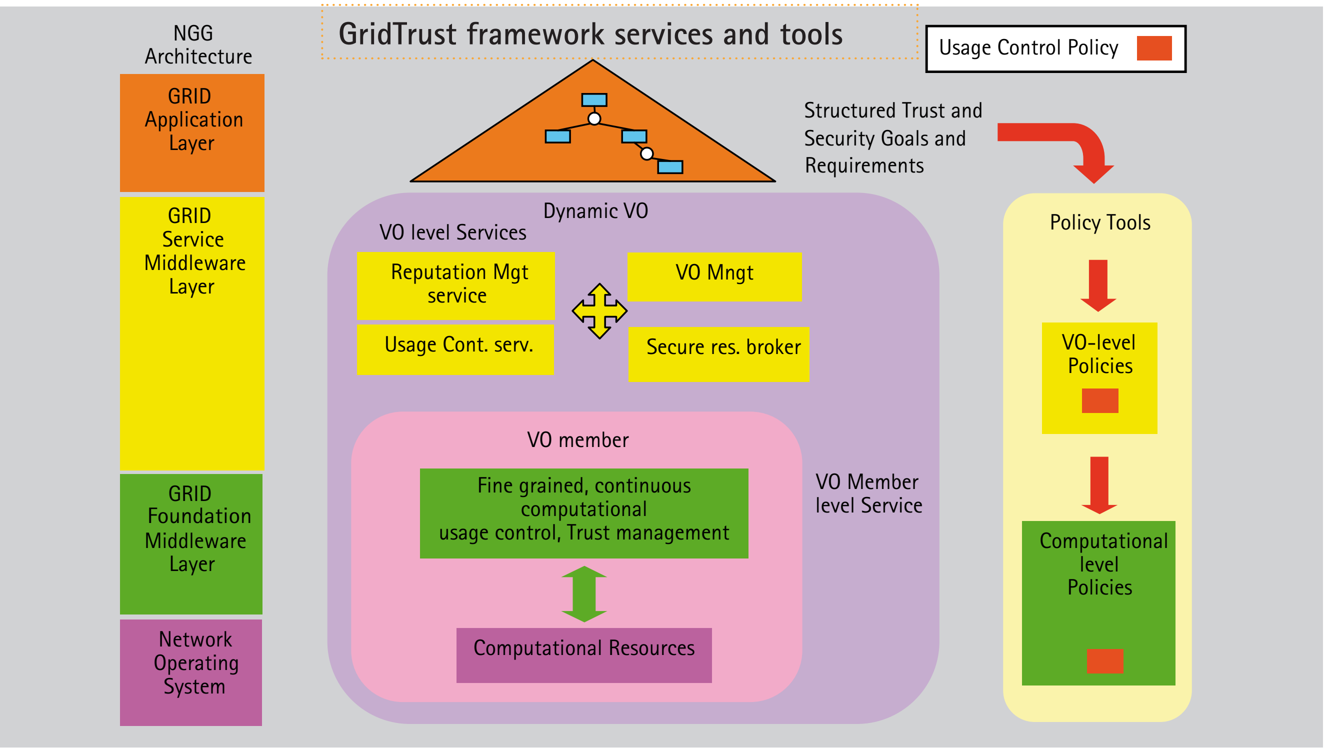
The main output of the GridTrust project will be a framework consisting of:

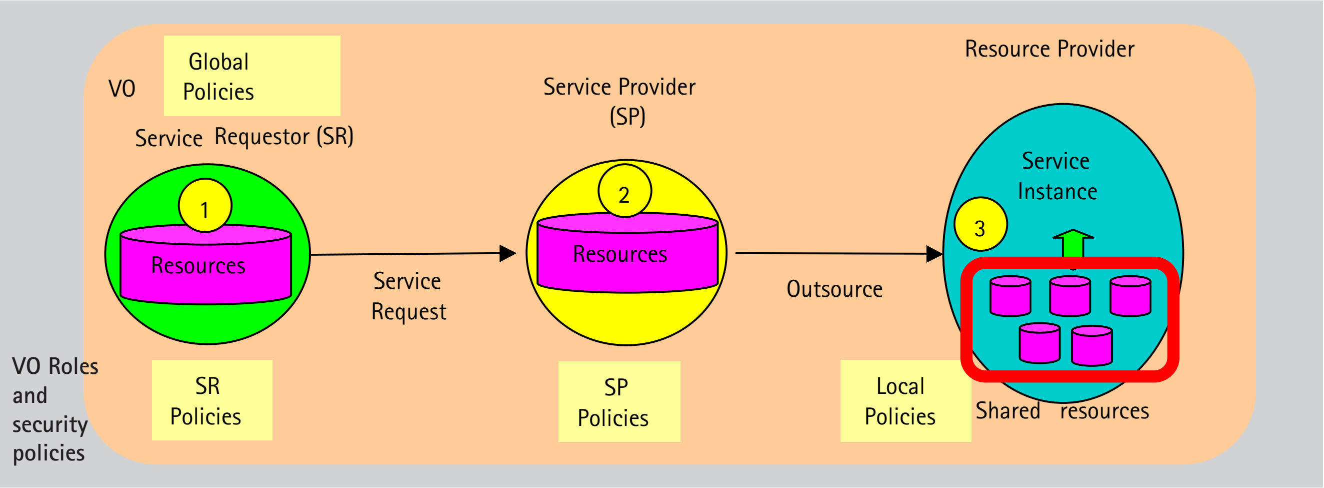
- A methodology and interactive execution environment that will help Grid service requestors and providers improve expression and reasoning on trust, security and privacy properties for different kinds of Virtual Organisation (VO) topologies. This will take different aspects such as self-organisation, self-management, self-adaptation and evolvability into account.
- A reference Grid Security Architecture, including an autonomous policy management for fine grained usage control of Grid resources.
- An open source reference implementation of trust and security management systems, validated by scenarios in the business domain. The resulting tools will be of a generic nature and will be validated by innovative applications from different application sectors. The tools will not be specific to the applications considered in the GridTrust project and will comply with Open Grid Services Architecture (OGSA).

The GridTrust framework

Figure 1 shows the GridTrust framework services and tools. The framework addresses three layers of the NGG architecture: the Grid application layer, the Grid service middleware layer, and the Grid foundation layer.

The framework is comprised of trust and security services and tools as indicated in the figure. The trust and





security services are provided by the service middleware and Grid foundation middleware layer. The services all-use usage control policies. The following services are included at the service middleware layer: a secure resource broker (Bertino et al. 2004), a reputation service (Arenas et al. 2007), (Resnick et al. 2000), and a service level usage control service. At the Grid foundation middleware layer fine grained continuous computational usage control (Baiardi et al. 2004), (Martinelli et al. 2005), (Martinelli et al. 2007) is provided.

The GridTrust framework policy tools aim to produce the security and trust policies needed by the different services. At the application level a requirements tool helps analysts define the goals and requirements in terms of security and trust, while it also produces high-level security and trust policies. A policy refinement tool takes the abstract security and trust policies as inputs and then refines them into both service and computational level usage control policies. These usage control policies are used by the different trust and security services.

Scenarios

Although not a project objctive, logistics makes a useful case study – it is not a product, it is a service; a service that moves its customer's products from one place to another. Big haulage or courier companies may be chosen for their brand, but what ultimately makes the difference is the quality and price of the service, while trust and security also need to be addressed.

Assuming that every transportation task is completed successfully and that the right product is delivered in good condition to the right destination, competition in the transport sector is driven by two main factors - delivery time and price.

To ensure low delivery times a courier company usually charges high costs. This is largely because if speed is the priority then there is no time to wait and load other goods, thus meaning the fleet is not utilised to its maximum. Indeed, many vehicles probably circulate half-empty.

Another characteristic of logistic systems is that only a few big players make use of global optimisation techniques to find the best routes for each transportation task with a view to improving fleet utilisation. Improving the efficiency of couriers' fleet utilisation has the potential to significantly lower the number of trucks circulating, something which will bring clear environmental benefits. However, small companies relative lack of customers or cash reserves means they often don't have the resources to invest in operating research techniques, they just execute their tasks in a first-come first-served way.

But how can a small courier company improve its operations to compete with the big players? How can a courier find enough transportation tasks to improve its own fleet utilisation? And how can a customer find the best courier for each given transportation task? The system proposed by the GridTrust project tries to answer these questions with a solution based on two fundamental ideas:

Firstly, as a case study, we plan to use an auctioning system that exploits competition between couriers and allows customers to find the best provider for each task. Only part of this scenario will be used to validate the GridTrust security and trust services. The second idea is to have a common routing computing service that allows even small couriers to optimise their routing. Both the auctioning system and the routing service will be hosted on couriers' VO resources using a Grid. The GridTrust usage control service will monitor the use of the Grid resources and enforce VO and local trust and security policies. The GridTrust framework provides a secured VO to the different stakeholders.

The main benefits offered by our proposed solution are that:

- The auctioning system allows clients to propose requests for quotation for transportation tasks (such as "move N units of P from A to B")
- Each courier (Cx) wanting to make a competitive offer must recalculate its routing with the added transportation task;
- Routing recalculation is performed on VO resources using the common routing service;
- After recalculation each individual courier (Cx) can make its offer;
- Choice of the best offer may be based on price, planned delivery time and courier's reputation;
- The chosen offer makes up the SLA (Service Level Agreement) between courier and customer;

This SLA is monitored by the shipping VO system and upon delivery the courier's record (on which their reputation is based) is updated according to whether they have met the SLA stipulations.

What is expressed for the big companies by their brand (a promise of quality, respect for values, care for each customer, etc.) will be summarised for the small courier companies by the reputation measure provided by a component part of the GridTrust Framework, the reputation service.

The trust index of a courier is based on its record of previous accomplishments and is tracked at Transporter VO level. Trust increases with successful shipments and lowers with product rejections, but it can also be lowered if the courier doesn't fully comply with the terms agreed in the SLA or if the courier's behaviour in its own VO is not in line with VO security policies.

Added value for businesses

The GridTrust project is focussed on providing tools to design security and trust for virtual organisation, thus ensuring they are sufficiently robust to meet the diverse needs of modern business.

Indeed, the project's work will allow companies to set up and operate secure, trusted virtual organisations, something that we believe will be enormously beneficial to the overall European economy. Virtual organisations will allow companies to both provide Grid resources and gain access to those of their partners in order to achieve their common goals.

Virtual organisations are also valuable in the wider context of Service Oriented Architectures aimed at setting up 'virtual' markets, thus ensuring that businesses will be able to adapt to changing market conditions, both today and well into the future. ★

At a glance

Trust and Security for Next Generation Grids

Objectives:

To develop the technology to manage trust and security for service based Grids. We propose to have a vertical approach tackling issues of trust, security and privacy (TSP) from the requirement level down to the application, middleware and foundation levels.

Project partners:

CETIC, Belgium; STFC, United Kingdom; CNR, Italy; VUA, Netherlands; Interplay, Italy; Hewlett-Packard European Innovation Centre, HP, Italy; IGDA, Italy; Moviquity and De Agostino, Spain

Project duration:

Three years

Contact:

e: phm@cetic.be
t: +32 472 569 831
www.Gridtrust.eu

Philippe Massonet

Coordinator

Philippe Massonet is scientific coordinator of CETIC. His research experience is in the areas of software, requirements, security and service engineering, and distributed systems, especially service-oriented Grids. He has experience in innovation and technical transfer from research to industry and government from several years in consultancy.