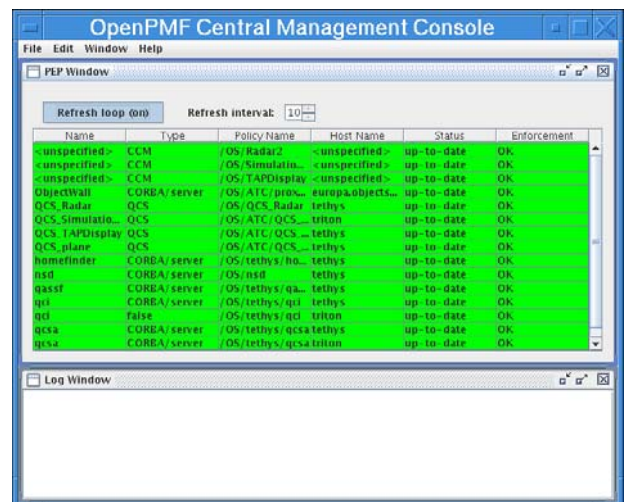


## Press Release – ObjectSecurity is deploying their secure middleware platform for air traffic control across the Internet

(Cambridge/UK – 24 April 2006) – ObjectSecurity, the leading solutions provider for middleware security in mission-critical industries such as air traffic control, announced today that it has tested a full pilot deployment of their secure middleware platform across the internet. It is now being officially deployed as part of the AD4 project.

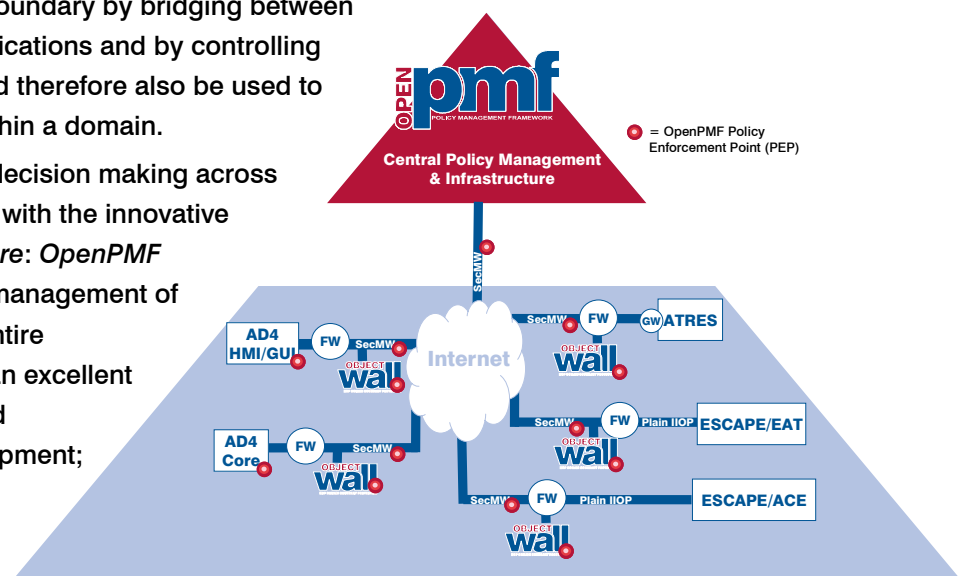
The secure ATC simulation environment prototype demonstrates that secure, large scale collaborative decision making systems over domain boundaries are easy to implement with the *ObjectSecurity Framework Architecture (OpenPMF, SecureMiddleware, ObjectWall)*.

The pilot scenario integrates a number of existing, large simulation systems (Escape ACE, Escape EAT and Vitrociset ATRES) and a newly developed system for the 4d visualisation of airspace (AD4). The security of the simulation platform is centrally managed and monitored by ObjectSecurity (organisations could also manage their security policies themselves if required).



The different nodes are geographically dispersed across Europe (see diagram) and illustrate two types of simulation systems: (1) CORBA based ESCAPE, directly integrated over ObjectSecurity’s robust *ObjectWall* IIOIP firewall, and (2) proprietary ATRES, wrapped into the framework architecture by *SecureMiddleware*, a CORBA Components (CCM) implementation with strong security support and a full model-based (MDA) development tool chain. The newly developed innovative 4d AD4 components are fully built using *SecureMiddleware*, which reduces development and deployment time and increases software re-use (through quickly-built legacy wrappers and a high degree of componentisation). *ObjectWall* supports painless, secure, and complete traversal of existing company firewalls (even with NAT) based on the central *OpenPMF* policy. It protects the organisational domain boundary by bridging between encrypted and unencrypted communications and by controlling access at a fine granularity, and could therefore also be used to protect security unaware systems within a domain.

To summarise, secure collaborative decision making across organisational boundaries is feasible with the innovative *ObjectSecurity Framework Architecture: OpenPMF* allows the centralised, unified, easy management of expressive security policies for the entire infrastructure; *SecureMiddleware* is an excellent platform for rapid legacy wrapper and component based application development; *ObjectWall* supports secure traversal across domain boundaries (also for protecting legacy applications).



The complete distributed system is protected directly by using ObjectSecurity *OpenPMF*, a central policy management framework that allows expressive security and QoS policies to be specified in a unified representation from within a central management console. *OpenPMF's* local policy enforcement points (PEPs) automatically enforce the policies on the underlying systems.

*OpenPMF* reduces the complexity of security administration and improves security effectiveness. Through its innovative modular plug-in model, practically any networked IT system to be protected (e.g. applications, middleware, operating systems, databases, firewalls). *OpenPMF* also protects against insider attacks because security can be controlled down to a very fine granularity and down to very small software entities (e.g. components) both at domain boundaries and directly at the applications.

The *ObjectSecurity Framework Architecture* allows the secure exchange of information across domain boundaries, thus enabling distributed air traffic control across co-operating agencies. In the deployment scenario, ATC tracks data from the ESCAPE ATC simulation platform is securely distributed to several organisations. One of the immediate benefits of this pilot project is that the data from the ESCAPE ATC simulation platform is now available for authorised partner organisations across the internet. The applications of this platform are numerous. For example, various data feeds with tracks from other control centres, weather data or airline data can easily be made available in a secure manner.

#### **Background: Benefits of the ObjectSecurity Framework Architecture**

There is a strong trend towards network centric and collaborative decision making in air traffic control and defence today. The driver is that better, faster, and more accurate decisions are required, based on more information combined from many different sources. Both newly developed systems and legacy systems need to be integrated. A particularly important aspect of such collaborative environments is that information is integrated across different organisations, such as air traffic control agencies, weather agencies, airports etc.

And information security is the critical enabler – without strong security, organisations will not open up their data systems to the outside. According to most national and international air traffic control organisations, airports, and defence agencies, information security plays the most critical role. This includes the protection of the core systems (especially from denial of service attacks and insider attacks) and of the communications. Collaborative information sharing between different organisations means that different security policies, different security levels, different existing security and middleware infrastructures, and different networks (intranet LANs, extranet backbones, closed WANs, and open WANs/Internet) need to be integrated. Efficient and secure communications are critical.

Other requirements are near real-time availability, high data rate, and – especially in air traffic control – closely coupled IT systems. XML web services, a middleware increasingly used in the commercial world, are not very well suited for such environments. This is because (1) of their poor performance, (2) their lack of quality of service (QoS) support, (3) because ATC legacy systems are typically object-oriented, (4) because communications channels between applications are long-term, and (5) because typically application integration is required instead of simple data integration.

The *ObjectSecurity Framework Architecture* together with *OpenPMF*, *ObjectWall*, and *SecureMiddleware*, have been specifically designed to meet all those needs.

To learn more and get started, we invite you to talk with us about the solution that works for your needs and environment.

Please contact us at: [info@objectsecurity.com](mailto:info@objectsecurity.com).

[www.objectsecurity.com](http://www.objectsecurity.com)