

Secure Air Transportation

Air Traffic Control, Airport, Airlines (CDM & SWIM)

Challenges of Air Transportation: CDM & SWIM

Air transportation today is increasingly faced with inefficient use of infrastructure, limited throughput (airport / aircraft etc.), poor slot compliance, frequent late stand & gate changes, flight delays etc. These problems affect many stakeholders, including air traffic control (ATC), airports, and airlines. Inadequate flow of information is often the cause, complicated by independently built information systems, lack of information access by stakeholders and a reluctance to share sensitive information

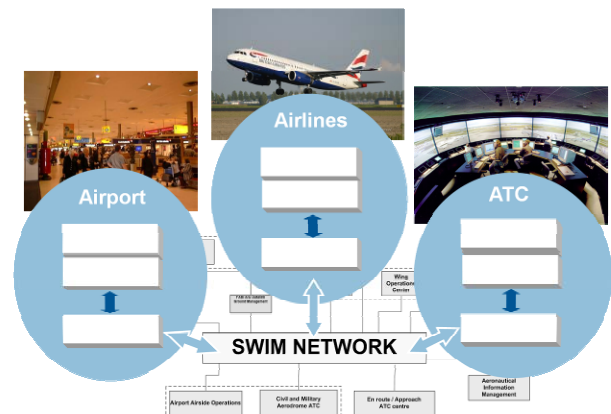
Collaborative Decision Making (CDM) proposes to replace the current central planning paradigm with a collaborative process where information owned by individual partners is shared in a system-wide representation providing shared situational awareness. CDM is being advocated by Eurocontrol for airports (A-CDM) and for air traffic management. System Wide Information Management (SWIM) facilitates such general information accessibility across all involved stakeholders. In short, SWIM provides the mechanisms which support the partners in managing information sharing. Specifically, a CDM/SWIM system should control which information is shared and all details of how the information will be shared such as when, how, in what form and so on..

Security & Compliance: Critical Enablers

Information security policy management, in addition to appropriate security mechanisms is a critical enabler for CDM/SWIM. Without manageable security, partners will refuse to share commercially sensitive information. Moreover, information consumers will not be able to fully trust the information provided. Air transportation CDM/SWIM systems will most likely be cross-platform, cross-technology architectures, e.g. including Web services, DDS, CORBA, JMS and others, creating significant complexity. One of the hardest problems of such a complex, dynamically changing IT landscape is security policy management.

A comprehensive security policy management system should: enable the business person to specify their own

security-related requirements without involving IT security administrators; demonstrate compliance with policies in real-time; and support business and IT environments like air transportation which change frequently. This is what we have built with OpenPMF.



ObjectSecurity OpenPMF lets you intuitively select business-centric security & compliance policies, which are then automatically enforced across your IT landscape (using a "model-driven security" approach). You can conveniently manage your policies at run-time, and even change your software applications and workflows without extra administration. OpenPMF reduces costs, improves security, and enables agility. Available as a packaged product and as an integrated turn-key solution.

Products & Services

- OpenPMF (packaged product & turn-key solution)
- SimulateWorld 4D synthetic environment toolkit
- SecureMiddleware: secure open source middleware
- Services: security policy management, Web 2.0 / SOA / Cloud / SaaS Security, middleware security, training workshop, tech. support, R&D
- Studies: in-depth documents about hot topics in security, e.g. model-driven security & SOA

www.objectsecurity.com