

Secure Telecoms Infrastructure

Secure Telecoms Management / Service Platforms, Secure Back-End Integration

Telecoms Infrastructure needs Security

The telecommunications industry builds and operates large networks. For example, telecoms service platforms provide an open and standard interface to functions of an underlying network infrastructure, e.g. to a 3G mobile network. They can be used not only by the network operator, but also by 3rd party service providers, to implement telecommunications services. This raises several security issues for all involved parties. The network operator for example is concerned about the correct function of its network, and wants to open only a specific set of functions to others. The service provider e.g. wants to bill the customers, and the user demands a protection of privacy. Regulatory requirements, for example for data protection or legal access, also need to be considered. Robustness of the mission-critical IT infrastructure used to coordinate responses is vital. Information security plays a critical part in this.

Secure Telecoms Service Platforms

The complexity of IT security in such complex, interconnected environments is a major challenge. Many efforts are currently undertaken to design and build a common architectural standard for a joint-up, agile business-driven technology architecture. Service Oriented Architectures (SOAs), process-centric architectures (BPM), as well as data-centric architectures (e.g. DDS) are all being deployed alongside more traditional application integration platforms such as JavaEE, JMS, CORBA/CCM.

The vision of secure service platforms is not new. For example in the past there were some attempts to secure TINA and Parlay. Service platforms also contain a certain level of security functionality, for example for authentication. But this is mainly targeted at user management, which is only a subset of the challenge. Without the right tools, the management and enforcement of adequate security policies in service platforms is a challenge since the platforms themselves do not provide the necessary functionality. Secure services can be

implemented in very different ways, e.g. in the application itself. This is a very common approach, but has many practical disadvantages, from a greater burden to the application developer who now has to take care of the security functions, in addition to the business logic, to non standard management of security policies. A better solution is to build most of the core security functionality, authentication, protection, access control and auditing into an already secure service platform, and manage the security policies using ObjectSecurity's policy management solution.



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