Securing Service Oriented and Event Driven Architectures
Results of an Evaluation of Enterprise Security Frameworks

- Security threats
- Counter-measures
- Principle approaches
- Results of the evaluation
- Future research work
Security threats in a SOA

Scoring Company

Unauthorized
- access to information
- modification of information
- modification of functionality
Measures against the threats in SOAs

- Authentication
- Authorization
- Digital signing
- Encryption
- Auditing
Interception of communication between services and enforcing security policies at the point of interception.

**Interceptor:**
Contains a kind of policy enforcement unit, which receives policies defined by the administration server and is responsible for enforcing the distributed policies.

Diagram:
- Network
- Interceptor
- Administration server
- Policy distribution
AquaLogic Enterprise Security

Enables
- Authentication
- Authorization
- Role-/Credential-Mapping
- Auditing
due to local interceptor plugins (SSM) for every server
Enables
- Non-Repudiation + Integrity
- Confidentiality
- End-to-End-Security
  - Service ATN + AZN

Due to local interceptors working as a proxy server for every server.
The whole Security Scenario

secured by AquaLogic Enterprise Security

**Presentation Layer**

secured by Business Security Framework

**Service Layer**

secured by Business Security Framework

**Process Layer**

**ALES**
- + extensible due to open APIs
- + full support of delegated administration
- + allows securing of conventional java apps
- - no real end-to-end security, therefore need for additional ESB (data- and connection security)
- - kind of vendor dependency due to SSM plugins for servers

**BSF**
- + connection and data security out-of-the-box
- + no vendor dependency
- - still no replacement for ESB (Service locator, QoS etc.)
Future research work on

- Pattern-based security modeling
- Model-driven security policies
- …

in the scope of the work on doctoral thesis