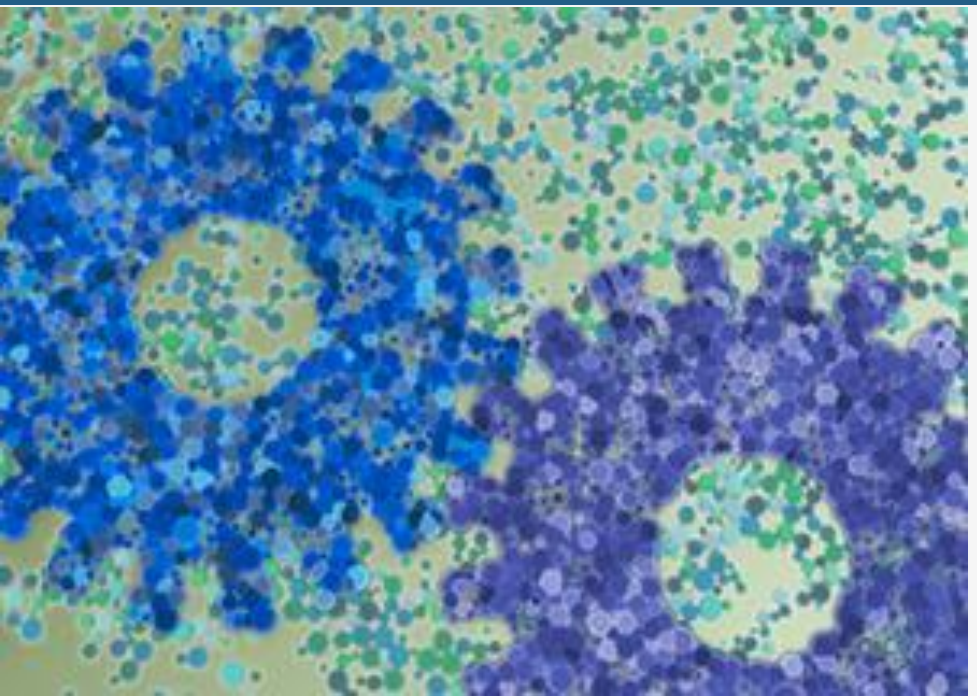
Ecosystem for Collaborative Manufacturing Processes – Intra- and Interfactory Integration and Automation



Security Framework

Nacho González

Atos Research & Innovation

Co-funded by the European Union

COMPOSITION

Outline

- COMPOSITION Security Framework architecture
- Components
- Authentication service (Keycloak)
- Authorization service (EPICA)
- RAAS
- XL-SIEM
- Reverse proxy (Nginx)
- Integrity and trust of information

COMPOSITION overview

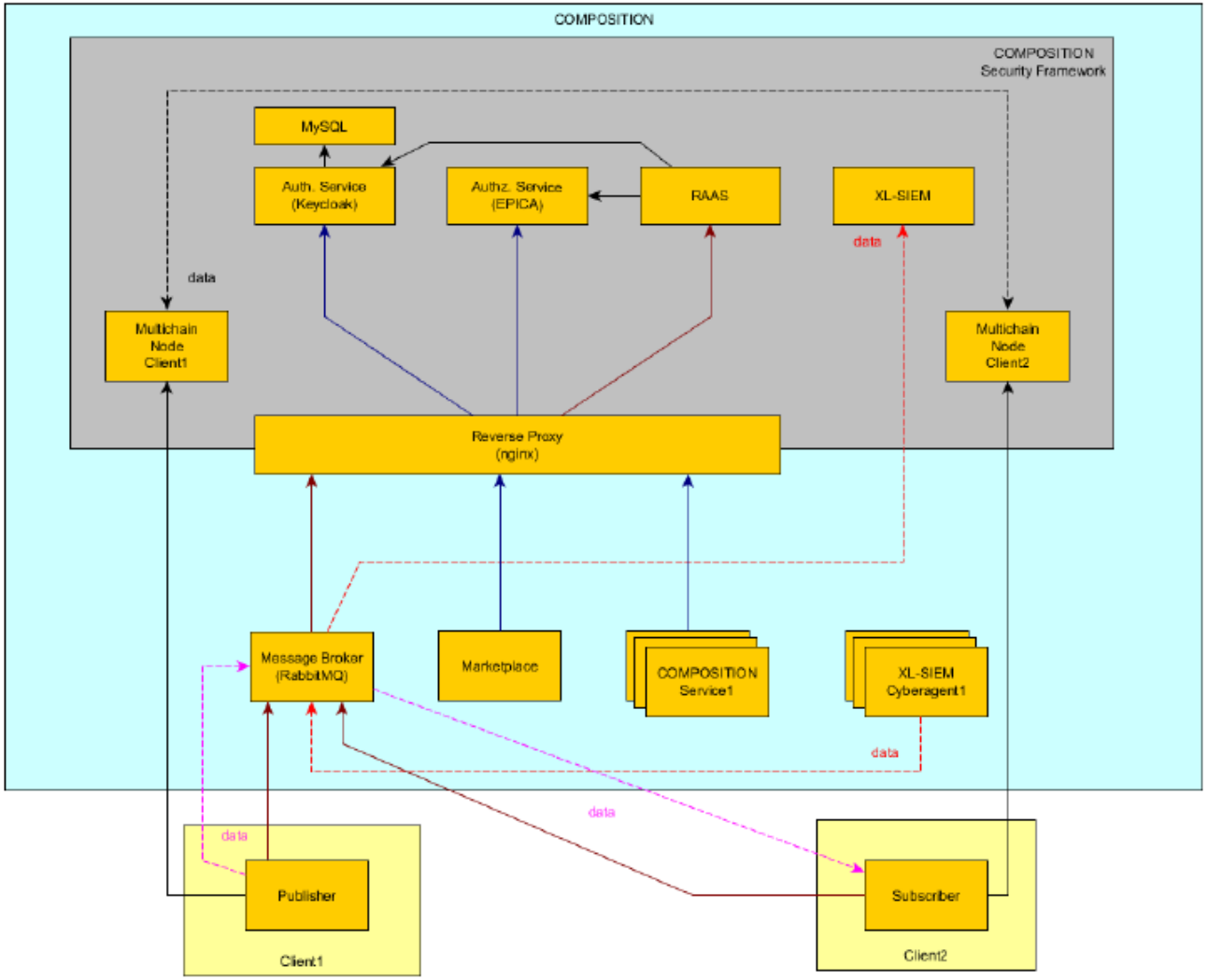
- Objectives
  - Integrate data along the value chain inside a factory into one integrated information management system (IIMS) combining physical world, simulation, planning and forecasting data to enhance reconfigurability, scalability and optimisation of resources and processes inside the factory
  - Create a (semi-)automatic ecosystem, which extends the local IIMS concept to a holistic and collaborative system incorporating and interlinking both the *Supply* and the *Value Chains*.
- https://www.composition-project.eu/

COMPOSITION

Security Framework architecture

- Objective
  - Guarantee security, confidentiality, integrity and availability of managed information
  - All authorized stakeholders within COMPOSITION platform

Security Framework architecture



Security Framework components

- Components to cover Inter-Factory and Intra-Factory scenarios
  - One authentication service (Keycloak)
  - One authorization service (EPICA)
  - Two RAAS services (intra and inter Factory)
  - A set of cyber-agents

Authentication service (Keycloak)

- Provide authentication mechanisms for users, applications and devices
- Standard authentication protocols
  - Oauth 2.0
  - Open ID Connect (OIDC)
  - SAML 2.0
- Custom mapper in development
  - Possibility to add custom external information to keycloak tokens

Authorization service (EPICA)

- Provides authorization mechanisms
- Based on XACML 3.0
  - Attribute-based Access control mechanism
  - Definition of authorization policies
- Component developed under the umbrela of Atos Research & Innovation

RAAS

- RabbitMQ authentication and authorization service
- HTTP service
- Enables the use of the authentication (Keycloak) and authorization (EPICA) services using a message bróker (RabbitMQ)

RAAS

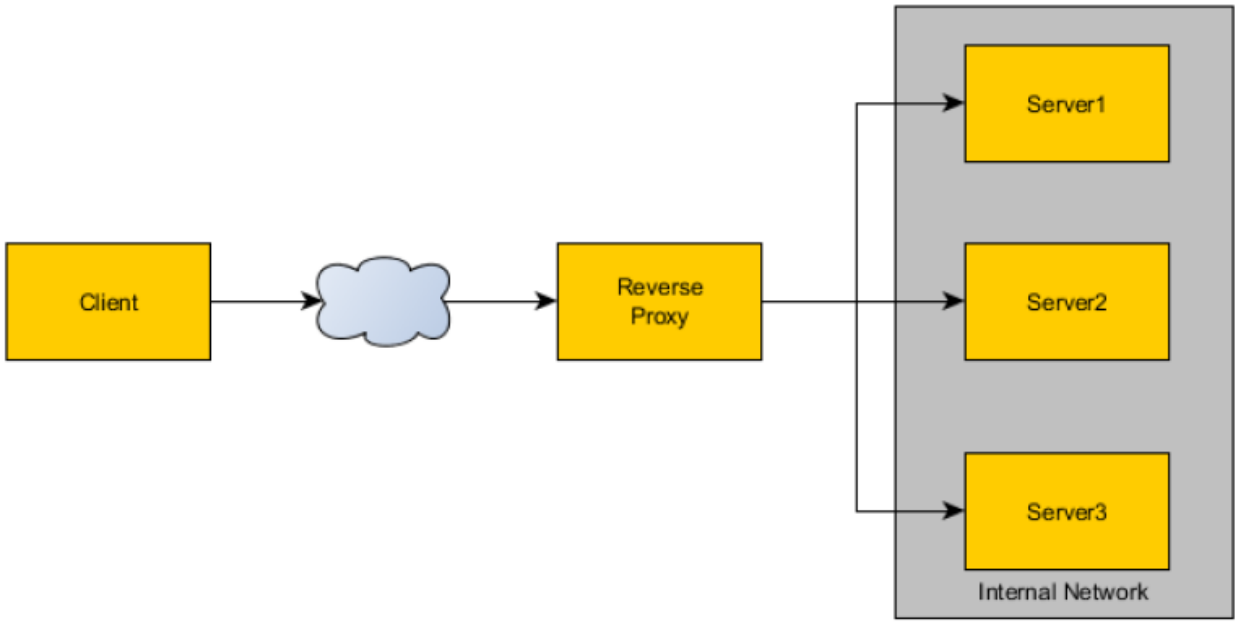
- Two working modes
  - RAAS will be the responsible to request and manage tokens from Authentication service (Keycloak) and perform authorization request to Authorization service (EPICA) with the obtained tokens. The clients make login in the message broker with username and password.
  - RAAS will be only responsible to verify the validity of tokens from Authentication service (Keycloak) and perform authorization request to Authorization service (EPICA) with the provided tokens. The clients are responsible to obtain and manage the authentication tokens and provide them to RAAS. The clients make login in the message broker with the token from Authentication service, no password involved in this mode.

XL-SIEM

- Inputs provided by SIEM agents
  - Responsibles of data collection
  - Deployed within the monitored structure
- Handles large volumes of data
- Raise security alerts from a business perspective
  - Analysis and event processing in Storm cluster
- Real time collection and analysis of security events
- Prioritization, filtering and normalization of the data gathered from different sources
- Consolidation and correlation of security events to carry out a risk assessment and generation of alarms and reports

Reverse proxy (Nginx)

- Directs client requests to the appropriate backend server
- Secures communication by enabling the use of TLS (Transport Layer Security) cryptographic protocol



Integrity and trust of information

- Reputation model
  - Each agent of the marketplace must be able to provide a rating related to each single transaction, when they act as the requestor (trustor): these ratings could be integer values within a predefined interval, for expressing different level of “satisfaction”
- Digital signature
  - One of the cornerstones to increase trust in the content of the messages flowing in COMPOSITION is the inclusion of the digital signature on all messages.
  - Messages are designed to be digitally signed using JWS27 (JSON Web Signature) which is an IETF28 proposed standard for signing arbitrary data

Thanks for your attention

Ignacio.gonzalezf@atos.net

COMPOSITION has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under Grant Agreement No 723145.

Please see us here: www.composition-project.eu