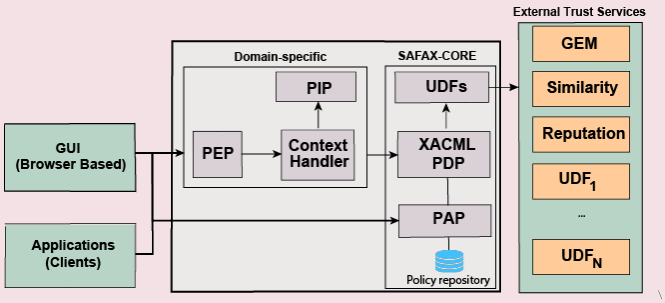
SAFAX A Flexible and Extensible Authorization Service

TU/e

SAFAX offers authorization as a flexible and extensible service. SAFAX is a novel XACML-based architectural framework tailored to the development of extensible authorization services for distributed and collaborative systems. The key design principle underlying SAFAX is that all components are loosely coupled services, thus providing the flexibility, extensibility and scalability needed to manage authorizations in complex environments.

Software Modularity and Service-Oriented Architecture

The SAFAX architecture adheres to the XACML reference architecture and implements it through a service-oriented approach. This ensures software modularity, a key paradigm in creating scalable, flexible, and maintainable software.



The architecture consists of three main blocks:

- domain-specific components (i.e., PEP, CH, and PIP)
- SAFAX-CORE represents the baseline of the authorization service
- external trust services are used to evaluate custom constraints in policies

Extensibility

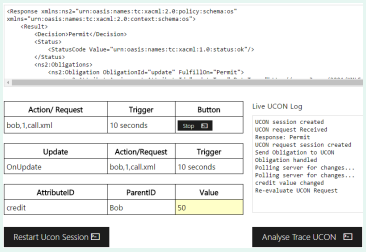
SAFAX architecture allows external service providers to easily plug-in their trust services. Trust services can be used for a range of purposes such as retrieving trust information from external sources and relocating the computation of complex functions relieving the burden on the PDP. As each SAFAX component is self-contained and does not depend on the context or states of other components, advanced features can be added to SAFAX framework while core functionalities are still maintained. Users can choose components and external trust services to be used for policy evaluation based on their needs.

External trust services

- Credential-based trust management
- Reputation-based trust management
- Policy interoperability with ontologies
- Geolocation (compatible with GeoXACML)

Advanced features

- **Usage control**: control sensitive information during the entire lifecycle of their usage.
- **Transparency**: make users engaged in a collaboration aware of policy conflicts and how these conflicts are resolved by the authorization service.

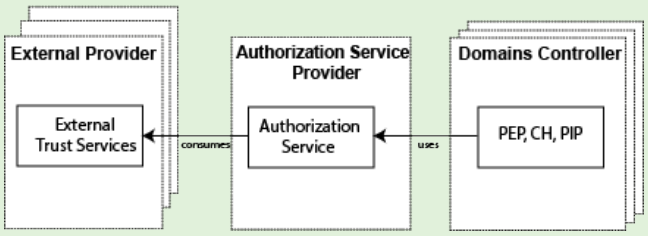


SAFAX A Flexible and Extensible Authorization Service

TU/e

Flexibility

SAFAX architecture allows great flexibility in terms of deployment, configuration, and integration. In particular, part of the authorization service can be outside control of an authority.



SAFAX allows three types of deployment models:

- Centralized
- Distributed
- Distributed and delegated trust model

Graphical User Interface

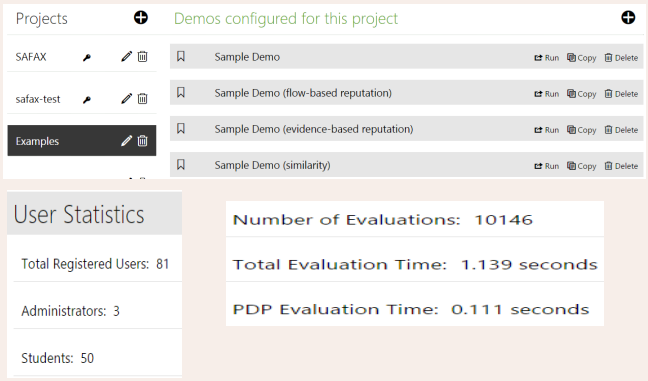
SAFAX provides a user friendly web interface that is easy to use and requires no installation. The web interface is compatible with all major web browsers such as Chrome, IE, and Firefox.

Features for End-Users

- Deployment of access control policies
- Policy engine configuration
- Access request evaluation

Features for Administrators

- Service registration
- Statistics view
- User account administration



Valorization and Exploitation

SAFAX has been used in education, research, and industry. Applications of SAFAX includes:

- Lab for bachelor course on security
- Research on access control for collaborative situation awareness
- Integration with Secure DPIF, collaboration with

D-CIS LAB THALES

Supported by

AU2EU

M2M Grids

FEDERATED SECURITY SHIELD

ACCUS Adaptive Cooperative Control in Urban (sub) Systems

IN-4-STARS 2.0

Contact Information

TU/e - Security Group

Duc Luu PDEng
Dr. Jerry den Hartog
Dr. Nicola Zannone

Email: safax.authservice@gmail.com
Website: http://security1.win.tue.nl/safax/