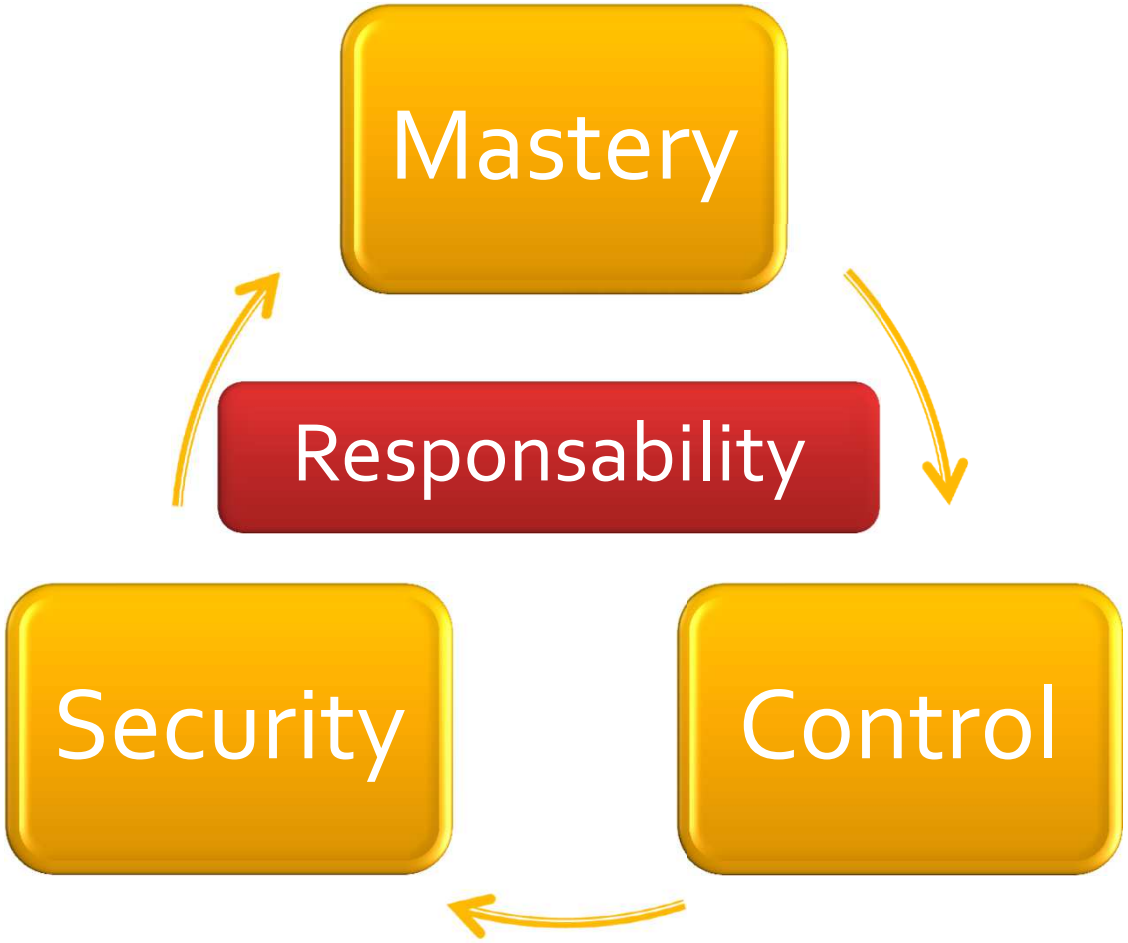
Access management Governance

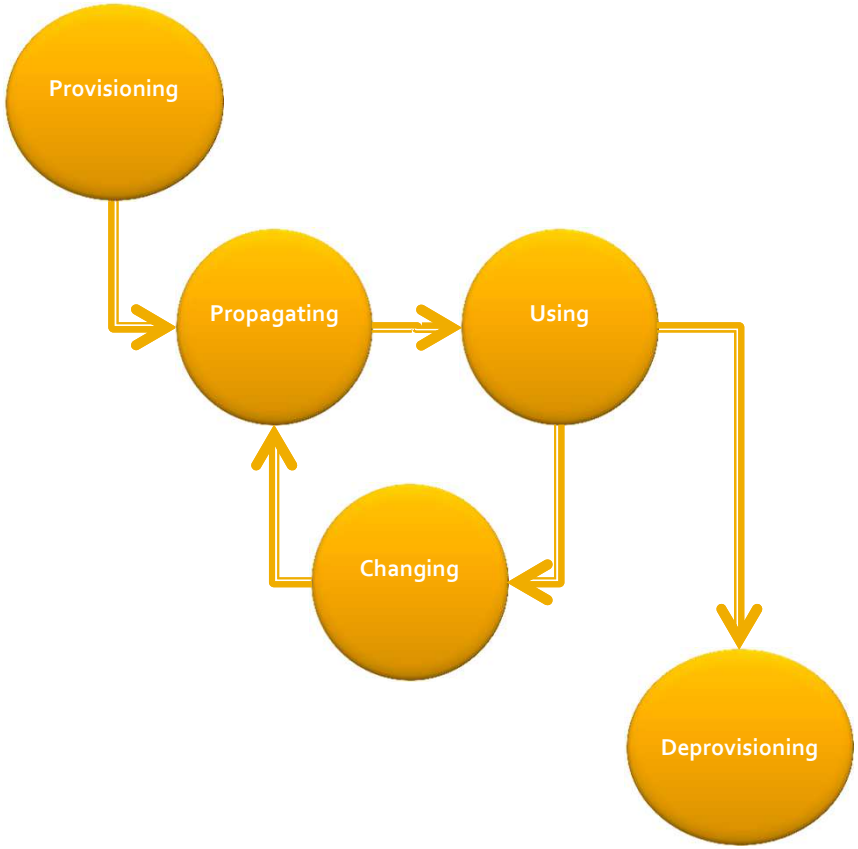
Roland Burgniard

Foreword



Management

IDENTITY MANAGEMENT



ACCESS RIGHTS MANAGEMENT

- DAC
- MAC
- RBAC
- TMAC
- ORBAC
- …

* authentication was voluntarily left out.

Today

In the enterprises, you often get this:

Which model?

Is it necessary to generalize a model for all needs?

- Each model has its advantages and inconveniences.
- **There is no ideal model**, but instead, a model **suited to a need**, to a **complexity**, to an **ORGANIZATION**.

ORFAG

A new model for access management governance

ORFAG - Definition

- **ORFAG** is the acronym for « **O**rganisation **R**oles based **F**or **A**ccess **G**overnance »
- Pragmatic development during several years
  - Beginning of thinking IA² : 2001
  - Based on GINA, operational with more than 300 applicative services.

ORFAG

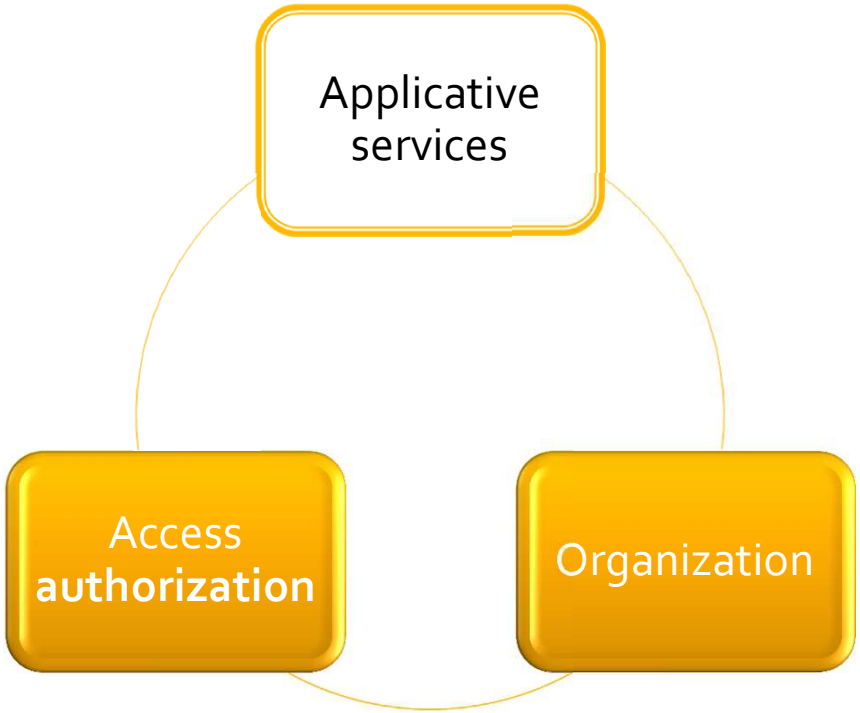
- The model is meant to be **unique** within a large company.
- It interoperates with other role-based models
- It takes into account a **dual dynamic of evolution**:
  - the dynamic of an applicative service, with its lifecycle and its vision of the theoretical organization.,
  - the dynamic of the organisation itself.
- Two Responsibilities = Intervention of **two** actors for the granting of an access right:
  - The owner of the applicative service,
  - The person in charge of the organization that is using it.

ORFAG - Constitution

- The ORFAG model handles a theoretical **"What"**: the roles defined for the applicative services,
- And associates the "**Who**" to roles in an organization managed in a unique and decentralised manner for the whole set of applicative services.

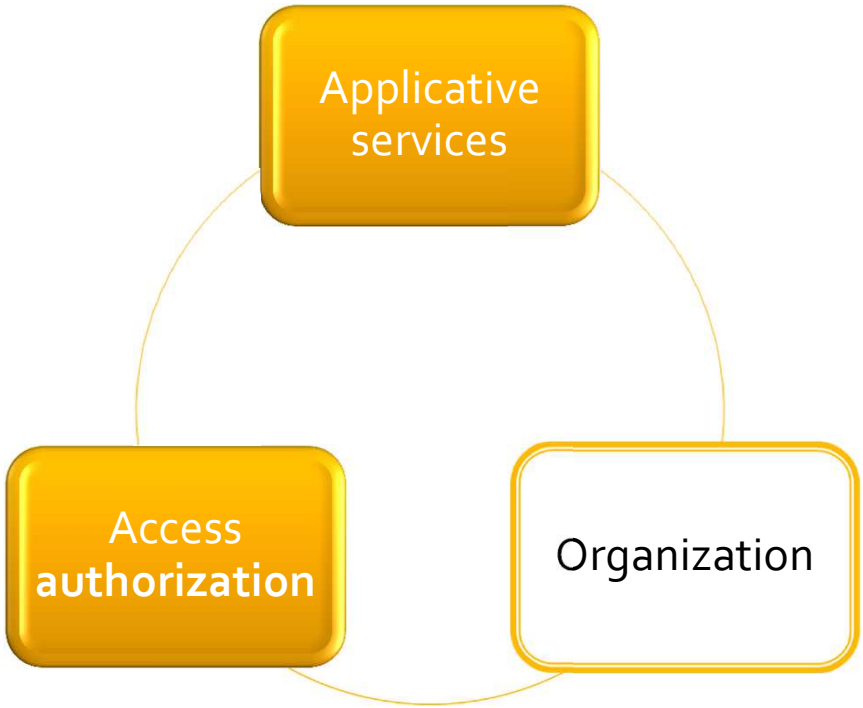
* The environment (as a security domain) could be seen as a fourth component

ORFAG – Applicative Services



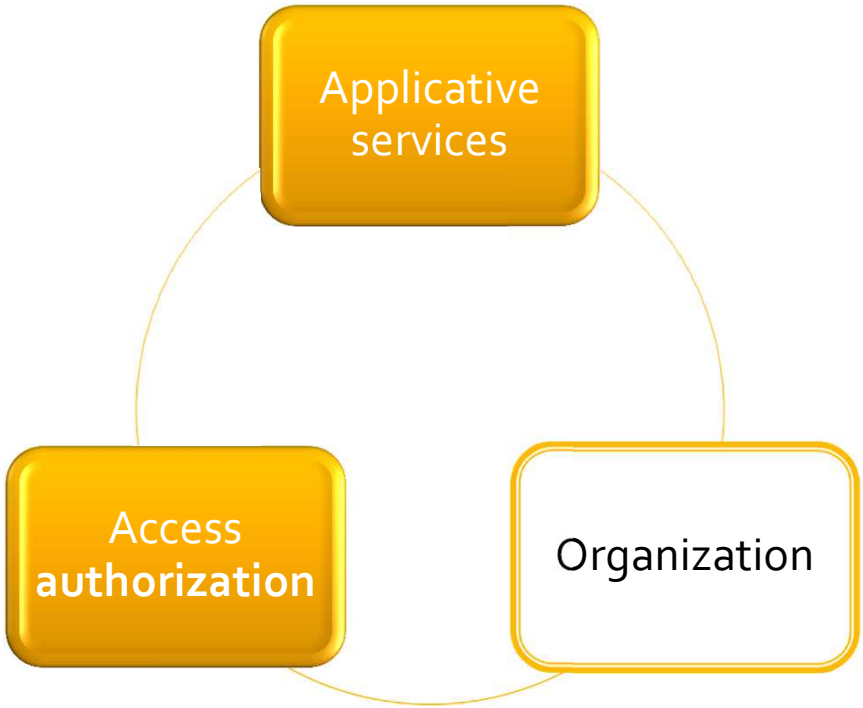
- We call **applicative service** any instance of a solution or a software bringing a set of services to a group of users.
- We need to establish an **inventory** of the applicative services of the company.
- A **governance** of the accesses is only **possible** if we **control** that **inventory** and the **responsibilities** associated with it

ORFAG – Organization



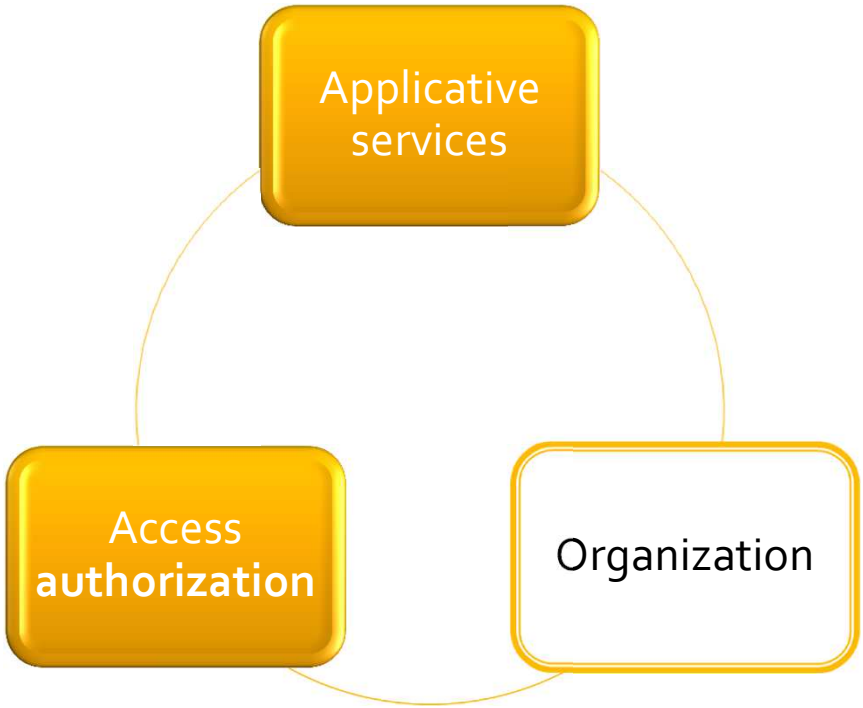
- The ORFAG distinguishes two types of organization :
  - the **internal** organization of the enterprise
  - the **external** organizations

ORFAG – Roles



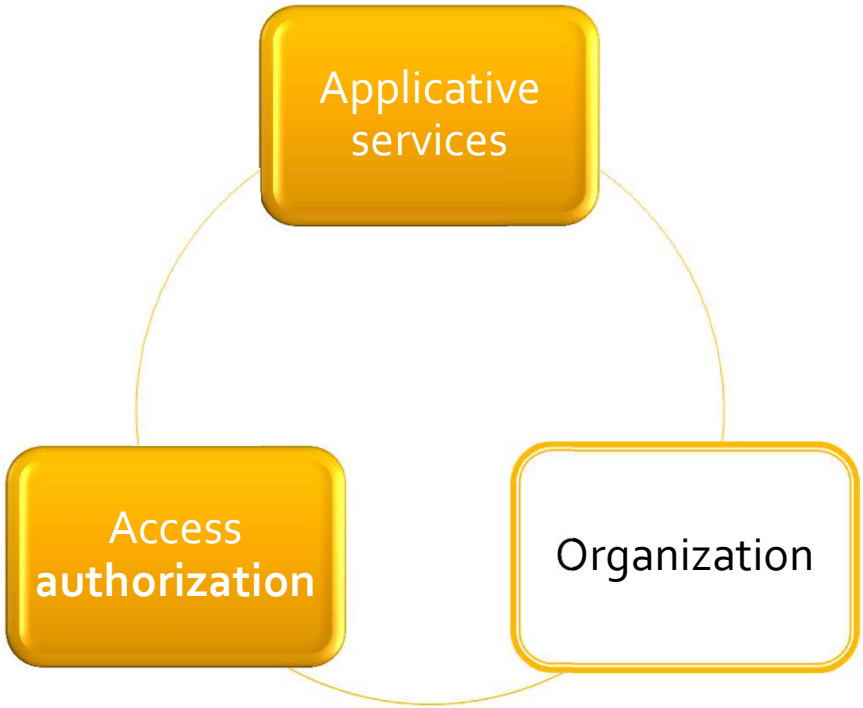
- Introduction of the notion of a **role** played par an individual in an organization.
  - **Managed** roles
    - roles that are specific to an organizational unit,
    - project roles, related to a specific activity,
    - roles that are imposed by the model.
  - **Transversal** roles
    - These roles allow us to ameliorate the system's efficiency.

ORFAG – Users



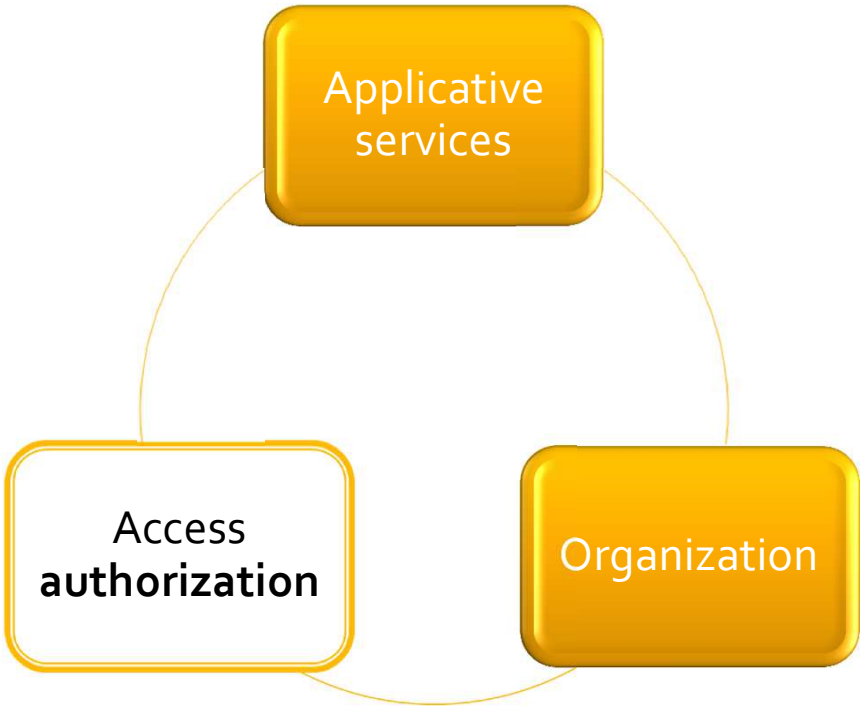
- The ORFAG model distinguishes two types of user :
  - The users **internal** to the enterprise:
    - Physical persons
    - Generic accounts
  - The users **external** to the enterprise:
    - Manually managed identities
    - Federated identities
    - Self-managed identities

ORFAG – External users



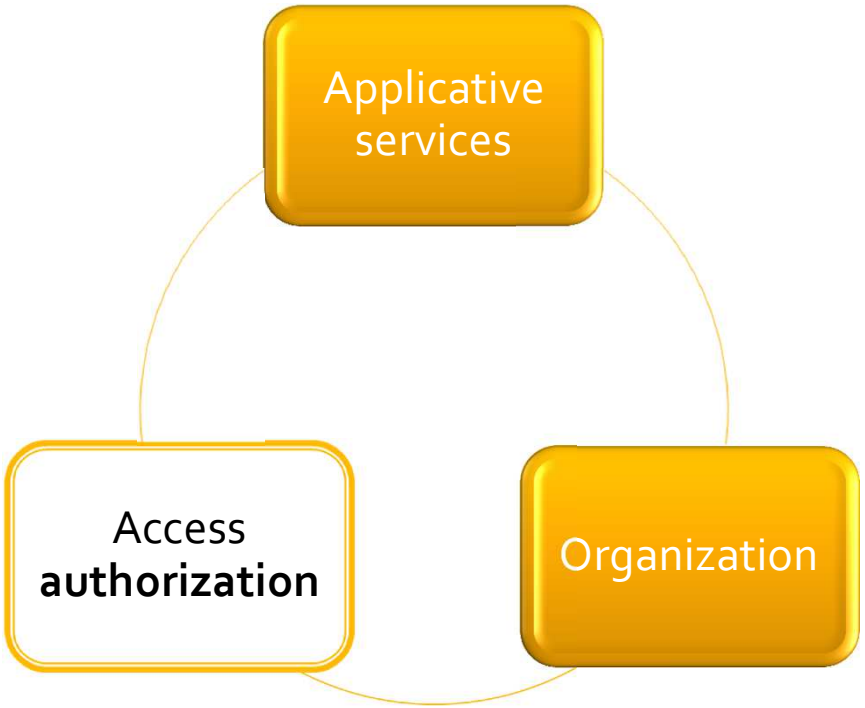
- The ORFAG model distinguishes two types of external user :
  - Physical persons
  - Legal persons
- Supervision
  - An internal authority is responsible for the relationship with the external organization?
  - Definition of rules of enrolment

ORFAG – Access



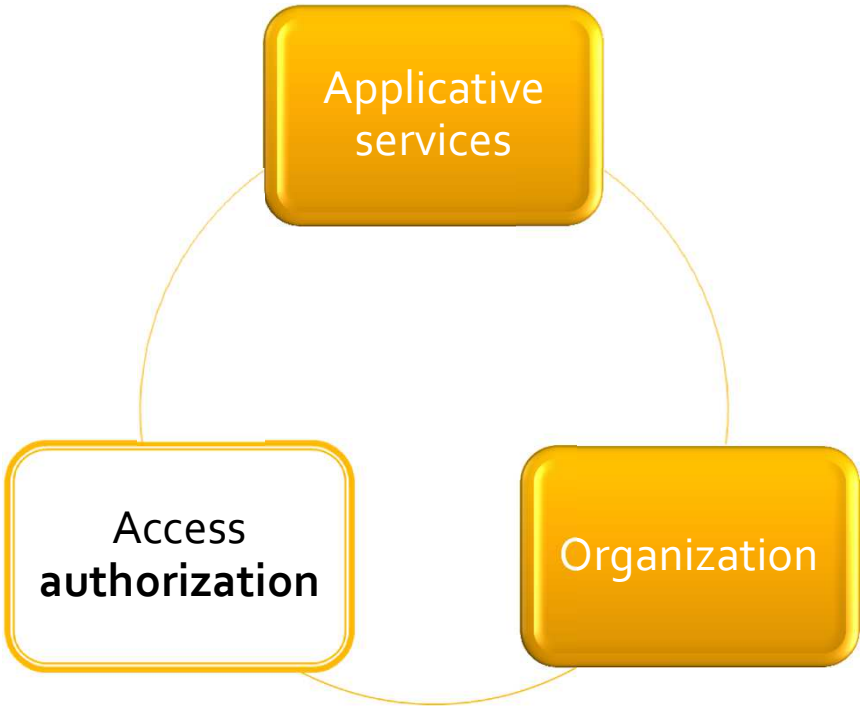
- The ORFAG model imposes the intervention of **two actors** for a double goal:
  - Acknowledgement of the two dynamics of evolution, under different responsibilities
  - Decentralized nominative access control

ORFAG – Responsibilities



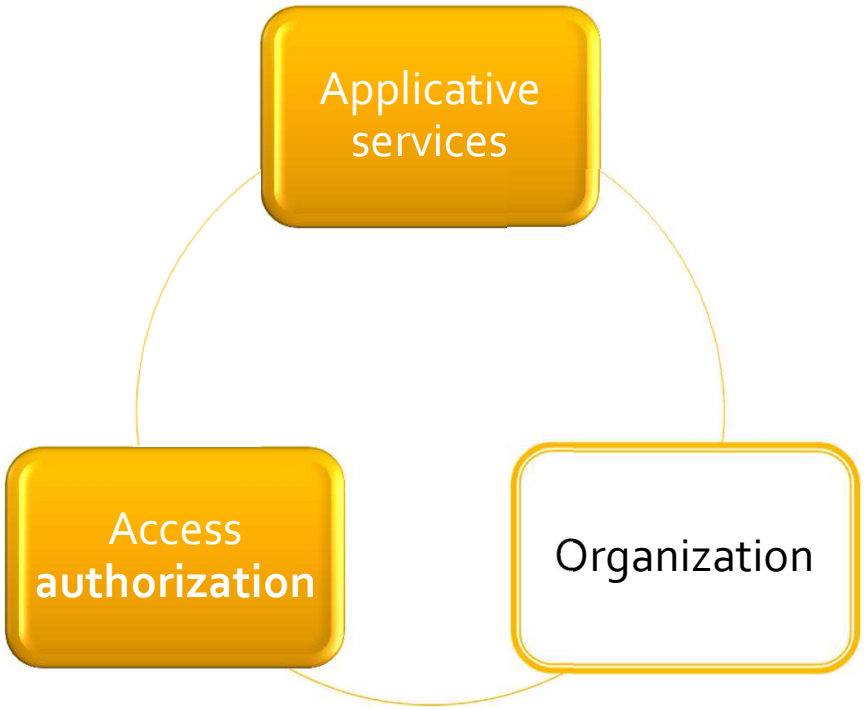
- **On the applicative service side**, the owner of the service can grant an authorization of one out of three forms:
  - Role inheritance
  - delegation of management to an organizational role
  - delegation induced by interoperability.
- The model imposes a **double validation of the authorization** for each delegation of responsibility.

ORFAG – Responsibilities



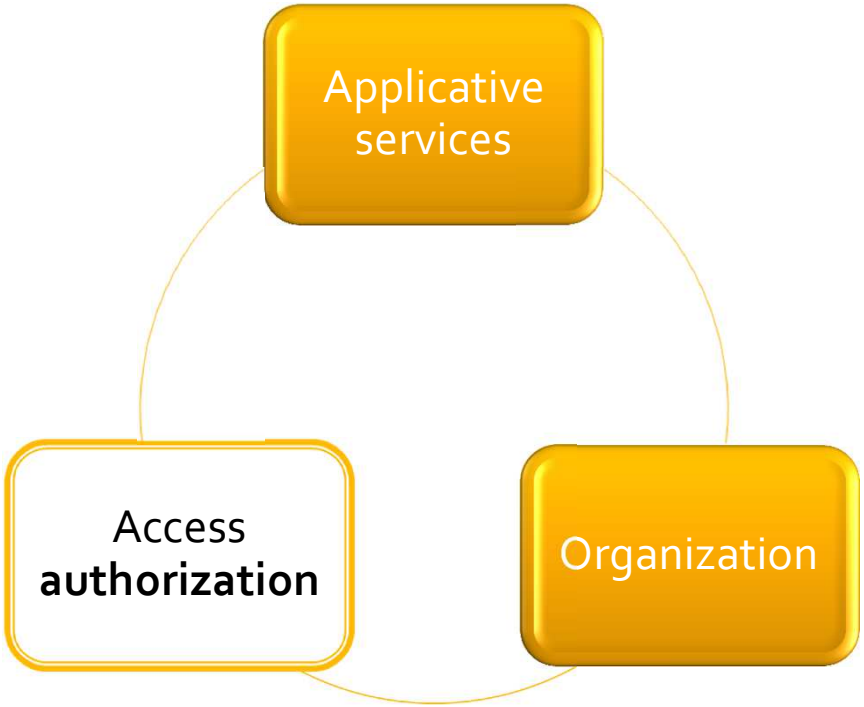
- **On the organizational unit responsible side**
  - No nominative authorization granting is possible
  - True separation of power
    - Intervention of **two** actors to grant an access.

ORFAG – Delegations



- The ORFAG model distinguishes two categories of delegation:
  - Within a same organizational unit
  - To another organization

ORFAG – Delegations



- **Attribution process of Business role**
- **Numerical identity <> registry**

ORFAG – Summary I

- This governance model allow a **centralized monitoring of access management** for the whole set of security realms of the enterprise.
- At any moment, it is **capable to identify the person(s) responsible** for a **decision** of an access authorization.
- The **nominative management** so **factorized** regarding the different applicative services **provides a de facto improvement in efficiency** of the access rights management.

ORFAG – Summary II

- It provides an **inventory** of the **applicative services related to internal and external organizations** of the enterprise.
- It takes into account **system interoperability**.
- It **handles the notion of project** .
- It **imposes** for all possible authorization cases' **the intervention of two actors**.
- It is **monitorable**.

Answers

Questions

contact@orfag.com