

Secure Identity & Connected Workflow Automation

Identity and permission layer for connecting people, digital services, devices and operational actions through secure, auditable workflows.

What we offer

EBRE AI develops connected workflows where identity, permissions and operational rules determine what each user, service or device can do. The same layer can link digital access with APIs, physical touchpoints and existing operational systems.

A workflow can authenticate the actor, evaluate roles and context, route the request to the appropriate system, require approval when needed and keep a complete record of the resulting action.

This approach supports environments where access, automation and traceability need to work together across software and connected infrastructure.

Where it creates value

Identity and access

- Authentication, roles and groups
- Scoped permissions and service access
- User and credential lifecycle

Connected operations

- API integration with existing systems
- QR, NFC and connected touchpoints
- Rules and actions linked to user or device context

Governance

- Approvals for sensitive actions
- Auditable event and workflow history
- Controlled interaction between people, software and devices

Working foundations

Identity infrastructure: Keycloak-based authentication, realms, roles, groups, permissions and secure application access.

Connected workflow platform: NFC and QR touchpoints, secure credentials, readers, device channels, commands and audited reaction chains.

Role-scoped operations: Municipal and incident-management products where permissions, supervision and traceability govern operational actions.

Controlled agent actions: Agent workflows with typed tools, approvals, idempotent execution and audit for sensitive operations.

How a pilot can start

1. Choose one access or connected workflow with a clear user, system or device boundary.
2. Integrate the required identity source and the target API, controller or connector.
3. Define permissions, rules, approval points and the audit information required for each action.
4. Run a controlled pilot and validate the workflow before extending it to additional users, systems or locations.

What a pilot should prove

Access correctness

Are users and services consistently authorised according to the defined roles, permissions and context?

Integration reliability

Can identity and workflow rules trigger the intended actions reliably across the connected systems?

Traceability

Can each action be explained and audited from identity and decision through to the operational outcome?