



CREATING A REUSABLE IAM TESTING ENVIRONMENT

INTERNSHIP

Contact:

Jeroen Hufkens

Company Information:

academy@identit.eu

IdentIT

Veldkant 35a

2550 Kontich

www.identit.eu

IDENTITY SECURITY, GUIDED BY EXPERTISE

IdentIT is an Identity Security Partner that helps organisations regain control over their digital identities. We combine independent advice with deep technical expertise in IAM, IGA and IVIP, and provide continuous guidance to help organisations build a sustainable identity landscape.

Our team currently consists of 40 IdentIT'ers who collectively manage 40 million digital identities. This makes us one of the largest dedicated Identity teams in the Benelux.

IdentIT is part of De Cronos Groep. This gives us access to the expertise, network and opportunities of a large technology group, while allowing us to retain our own focus, culture and way of working.

At IdentIT, you are given the freedom to take initiative, assume responsibility and shape your own growth. At the same time, you are never on your own: we bring together different strengths, help each other move forward and share our knowledge. New ideas and critical questions are always welcome, because learning works both ways. We approach complex challenges with focus and ambition, while valuing openness, humanity and spontaneity just as highly.

Assignment

During this internship, you will develop a local, reusable IAM Sandbox Factory for Curity. The focus is on DevOps, automation and Identity & Access Management. Using a single Git project, a colleague should be able to reproducibly install, configure, secure, test, reset and remove a complete sandbox on a Linux-based machine.

The sandbox is controlled through clearly defined parameters. Based on these parameters, various OAuth 2.0 and OpenID Connect clients, authentication scenarios, MFA methods, themes and a simple demo application are set up automatically. Ansible is the natural choice for the central orchestration layer, potentially combined with a local installation or containers.

What will you do?

- Design a local deployment strategy that works reliably on a Linux-based virtual machine, without depending on a public cloud or Kubernetes cluster.
- Build a Git-based project that installs and configures the sandbox using parameters.
- Automate prerequisites, installation, configuration, start-up, shutdown, validation, reset and removal.
- Provide multiple configurable OAuth 2.0 and OpenID Connect clients and connect them to a simple web application of your choice.
- Implement at least three scenarios: a basic sign-in with a username and password, a sign-in with MFA, and an advanced OAuth flow.
- Make authentication methods, client configuration and themes configurable so that colleagues can adapt the sandbox without major code changes.
- Provide HTTPS, proper certificate management and secure handling of secrets.
- Provide optional hardening that allows the default setup to be compared with a more production-oriented configuration.
- Document the complete solution, including prerequisites, configuration, scenarios, troubleshooting and day-to-day operation, for future internal users.

What technical skills will you learn?

- Applying DevOps principles to an IAM platform, with a focus on automation, reproducibility, idempotency and maintainability.
- Working with Infrastructure as Code and configuration as code using tools such as Git and Ansible.
- Evaluating and using a local runtime, such as a traditional Linux installation or Docker/Podman containers.
- Configuring Curity for OAuth 2.0, OpenID Connect, different clients, authentication flows and MFA.
- Properly managing TLS, local certificates, hostnames, secrets and security settings.
- Integrating a simple web application with Curity and demonstrating the selected scenarios end to end.
- Writing technical documentation that enables a colleague to install and use the tool independently.

What soft skills will you develop?

- Communication skills: reporting and documenting clearly and professionally, and collaborating with colleagues and stakeholders.
- Collaboration: working effectively within a multidisciplinary team in an agile environment.
- Problem-solving: analysing technical challenges and resolving them independently or in consultation with others.
- Self-organisation: taking responsibility for your tasks, planning and progress.
- Critical thinking: substantiating your choices and continuously improving based on feedback and evaluation.
- Customer focus: considering user needs and the business context when designing solutions.

Methodology

- The internship assignments follow the Scrum project methodology to provide a structured and efficient approach to tasks and subtasks.
- This reflects IdentiT's approach to projects.
- Scrum is a flexible framework that:
 - Promotes collaboration
 - Encourages adaptability
 - Ensures transparency.
- The work is organised into time-boxed iterations called sprints:
 - Each sprint lasts 2 to 3 weeks.
 - Each sprint has clear objectives and tasks.
- At the start of each sprint:
 - The intern(s) and supervisor(s) hold a sprint planning session.
 - The objectives are defined.
 - A sprint backlog is created.
- During the sprint:
 - Weekly stand-up meetings are held.
 - Progress is discussed.
 - Any obstacles are identified and addressed.
- At the end of each sprint:
 - A sprint review is held.
 - Where possible, a demo is given.
 - Feedback is collected.
- Scrum contributes to a collaborative and adaptable working environment.
- The aim is to achieve the best possible results within the given timeframe.

MVP

The minimum feature set we expect is:

- A locally executable Git project that installs a Curity sandbox locally based on parameters
- A web application that can integrate three authentication flows
- A choice of different UI themes
- Secure communication between the Curity server and the web application
- Comprehensive documentation covering prerequisites, a quick start, configuration reference, scenario guides, operations and troubleshooting.

Objectives

The following deliverables are expected at the end of the assignment:

- A technical analysis of the problem.
- The architecture of the required components.
- The MVP and any additional features.
- A demo of the end-to-end solution.
- Documentation of the entire process.