ITALIAN IDENTITY FEDERATION UPDATES

eduGAIN and REFEDS Town Hall

October 2023

Mario Di Lorenzo
IDEM Federation Operator

mario.dilorenzo@garr.it

Topics

IDEM Dynamic Metadata Distribution Service (MDX)

- Requirements
- IDEM solution for EDS
- Implementation
- Requests vs Months

IdP in the Cloud 3.0: IDEM approach to IdP as a Service

- IdP in the cloud 2.0 vs 3.0
- Components
- Architecture
- Future work

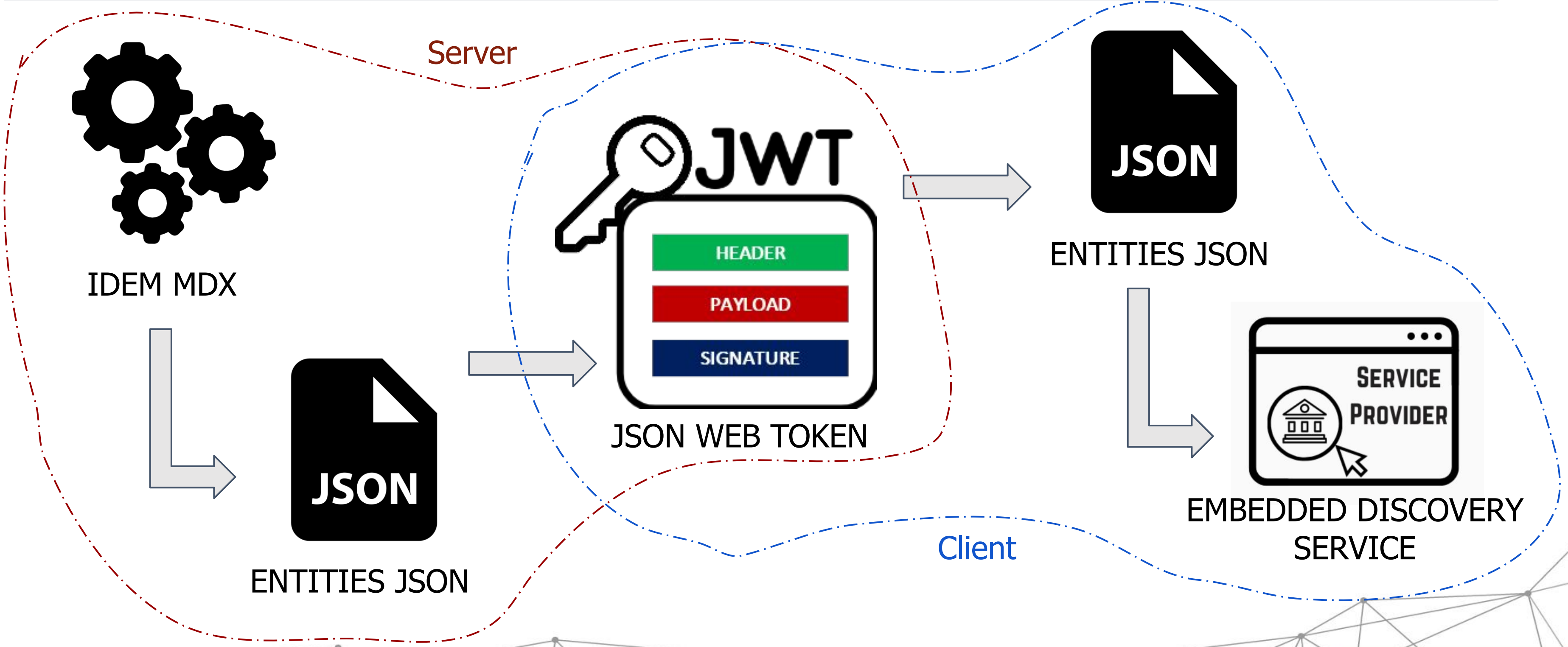
IDEM Dynamic Metadata Distribution Service (MDX)

Requirements

- A service back end, that will be used to parse the official IDEM metadata aggregates and it will create and sign one metadata file per entity
- A service front end, that will be able to serve all the files created by the service back end to the requesters
- Containerization of all the components
- Service in high-availability with load balancing
- Deployment with Ansible

IDEM Dynamic Metadata Distribution Service (MDX)

IDEM solution for EDS



IDEM Dynamic Metadata Distribution Service (MDX)

Implementation

Backend

pyFF

A SAML Metadata Appliance

- Creates metadata
- Performs signing
- Creates JSON files for Embedded Discovery Service

- Automatic rsync between nodes
- Create JWT from JSON files

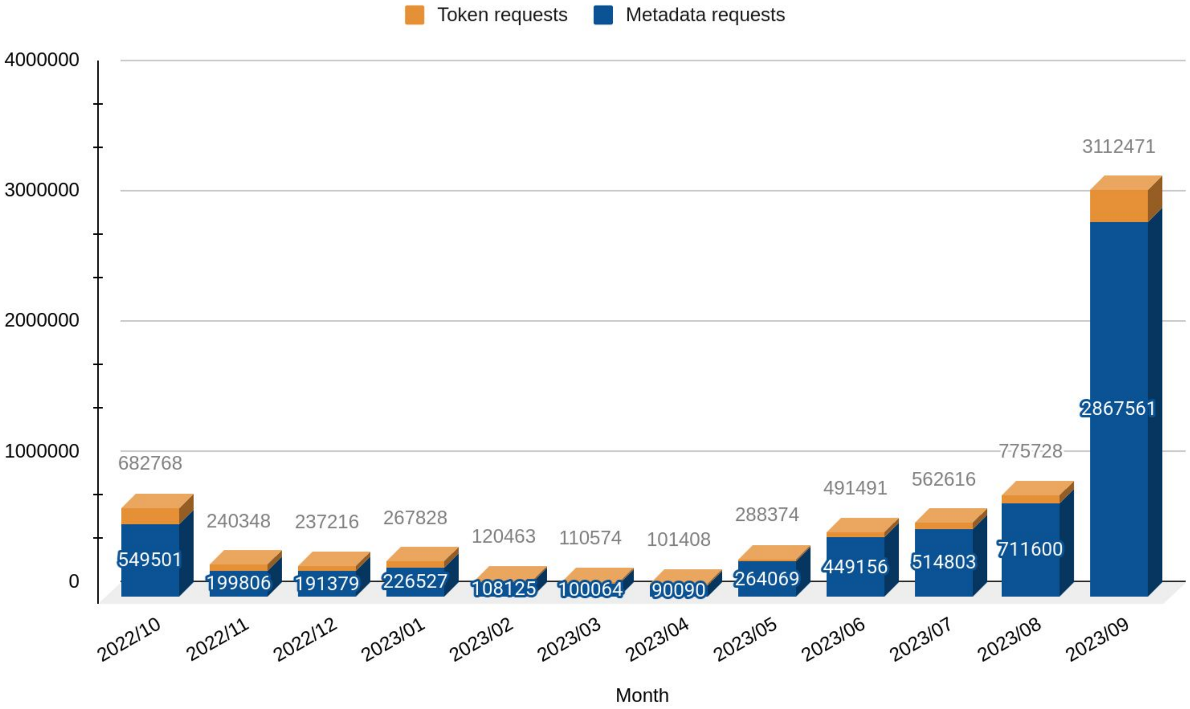
Frontend

- Web server serving:
  - Metadata
  - JWT for EDS

- High availability
- Load Balancer

IDEM Dynamic Metadata Distribution Service (MDX)

Requests vs Months



IDEM Dynamic Metadata Distribution Service (MDX)

The service is available at:
https://mdx.idem.garr.it

You can find the code on GitHub:
https://github.com/ConsortiumGARR/idem-mdx

IdP in the Cloud 3.0: IDEM approach to IdP as a Service

IdP in the Cloud 2.0 vs 3.0

- Idp in the Cloud Service 2.0
  - Over 40 VMs (one for each IdP)
  - Complicated and non-intuitive Identity Management System
  - No Multi Factor Authentication

- IdP in the Cloud 3.0 - *Requirements*
  - Multi-Tenant Identity Provider
  - Multi Factor Authentication (Time Based OTP via App + OTP via Email)
  - A completely new Identity Management System
  - Containerization of all the components
  - High availability and Load Balancing

IdP in the Cloud 3.0: IDEM approach to IdP as a Service

Components

LDAP Server — OpenLDAP

SAML Identity Provider — simpleSAMLphp

High-availability Database cluster — MariaDB Galera Cluster

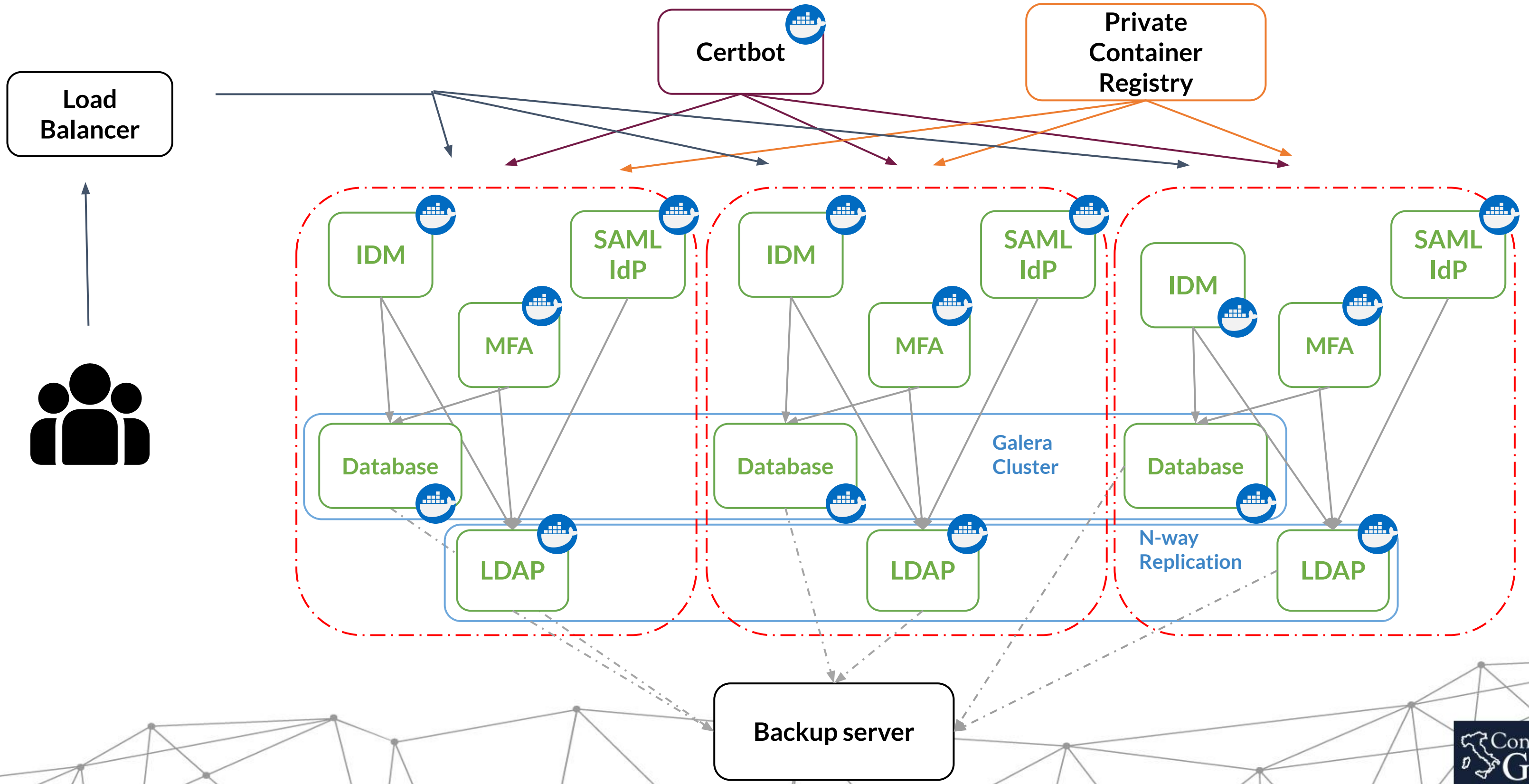
Multi Factor Authentication (MFA) — privacyIDEA AUTHENTICATION SYSTEM

Identity Management System (IDM) — django

Load Balancer — HAPROXY

IdP in the Cloud 3.0: IDEM approach to IdP as a Service

Architecture



IdP in the Cloud 3.0: IDEM approach to IdP as a Service

Future work

- Moving to Kubernetes Cluster
- Implementing Assurance (IDEM Assurance Profiles)
- Expand the Multi Factor Authentication
    - WebAuthn
- Publish our work on GitHub!

Thank you for your attention!

Questions?

Icons: https://www.flaticon.com