INSTITUTE OF INFORMATICS
SLOVAK ACADEMY OF SCIENCES

Usage of Federated Clouds in secure environments

Viet Tran
Institute of Informatics SAS
Slovakia

AI4 | eosc

eosc | SIESTA

iBERGRID | fct Fundação para a Ciência e a Tecnologia | Gobierno de España Ministerio de Ciencia, Innovación y Universidades | LIP Laboratório de Instrumentação e Física Experimental de Partículas | INCD Infraestrutura Nacional de Computação Distribuída | CSIC | European Commission | FM UP | HPC Now!

Outlines

- Retrieve and use access tokens without exposing them in plaintext
- Manage computing resources within the Federated Cloud
- Leverage cloud-native tools in a federated ecosystem
- Deliver secrets to applications and services securely
- Configure TLS access to services using Dynamic DNS

Motivations

- Services/jobs are typically deployed via CI/CD workflows
- The workflows may run on external machines
- The workflows need a variety of sensitive credentials:
  - User credentials for Cloud access
  - Application passwords, encryption keys, certificates, etc.
- How to manage the secrets securely?

Access tokens in FedCloud

- Usage of access tokens
  - Commonly used for AuthN/AuthZ in FedCloud via CLI and API.
  - Have short lifetimes and require frequent refreshing.
- Security risk
  - Exposing access tokens in plaintext poses a significant security risk.
  - Attackers could impersonate users, gaining access to all services.

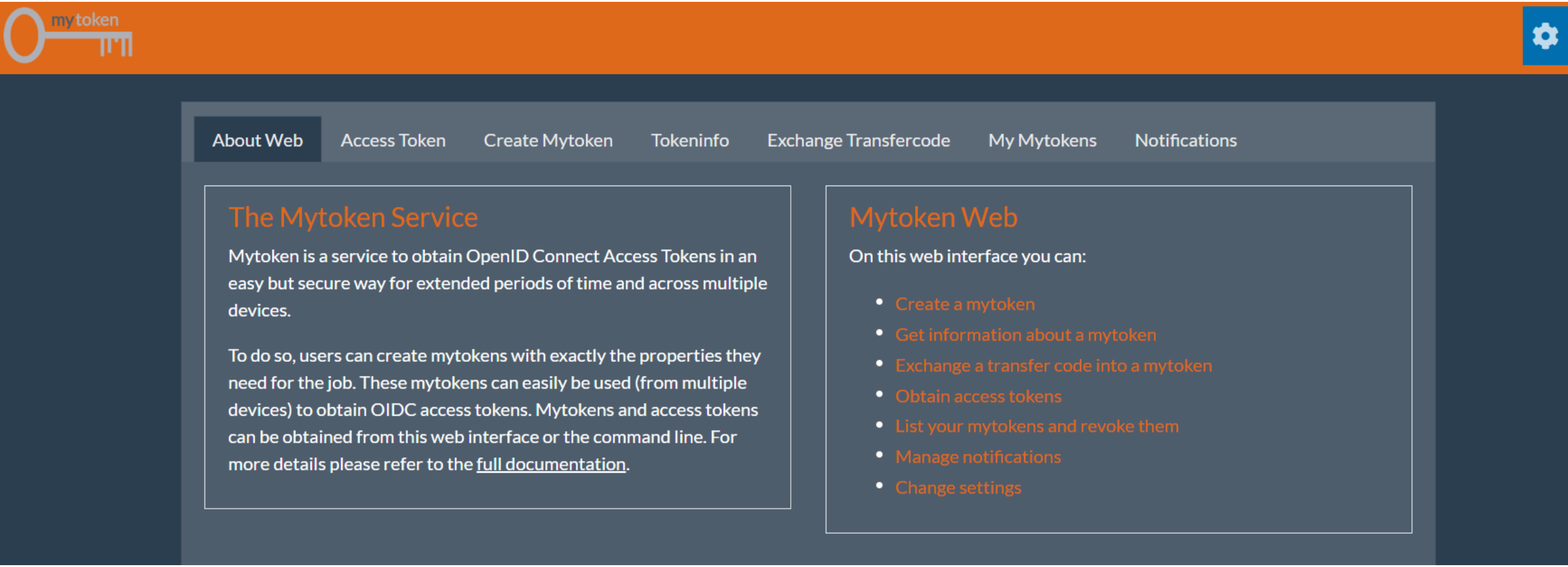
Managing access tokens

- Oidc-agent
  - Running as a daemon on client computer
  - Issues access tokens locally on requests
- Mytoken
  - Running as an external service
  - Issues access token based on “mytoken”
- FedCloud client can use both services

Capabilities of the FedCloud Client

- Resource management: Allows management of resources across all OpenStack sites within the federation.
- Easy to use: simple syntax with site and VO
- Compatibility and integration: Support integration with cloud-native tools like Terraform or rclone

Live demo with mytoken + FedCloud client

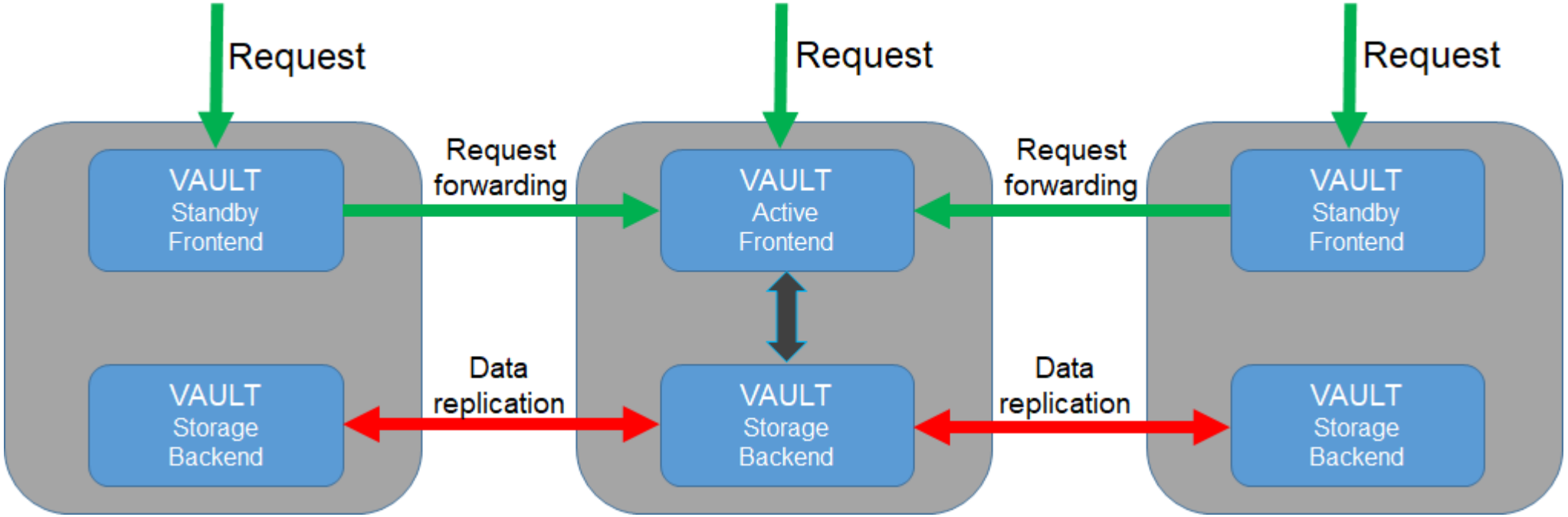


Secret Management for Applications

- Examples of required secrets:
  - Database passwords
  - Certificates
  - Data encryption keys
  - (and more)
- Requirements for secret management:
  - Securely managed: Creation, rotation, sharing, and auditing of secrets.
  - Secure delivery: Ensure secrets are delivered securely to target VMs in CI/CD workflows.

Secret management service

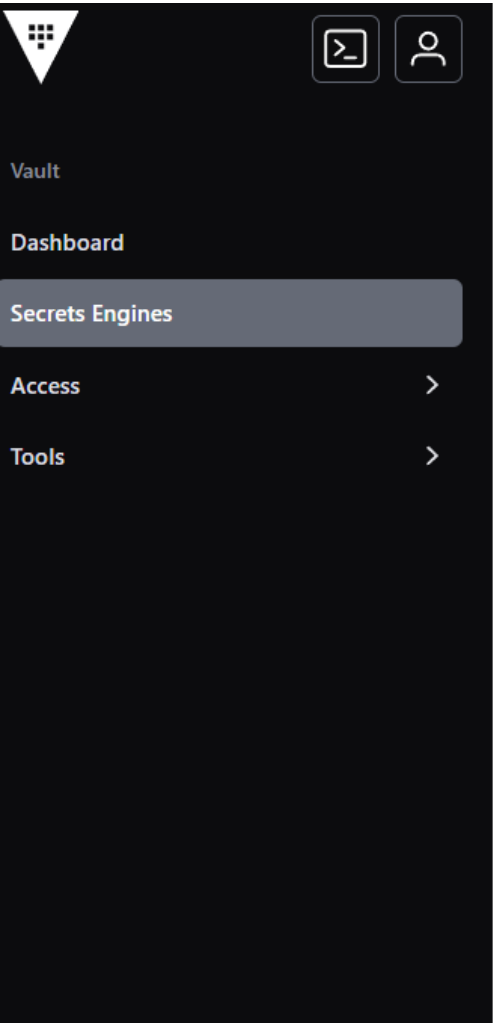
- Based on HashiCorp Vault
- High availability cluster at IISAS, IFCA and INFN
- Security improvements via FedCloud client



Security improvements

- Lockers
  - Isolated secret storages, accessible only via locker tokens
  - Limited lifetimes and usage counts
  - No access tokens required on VMs
- Why using locker tokens instead of access tokens on VM:
  - Lifetime could be set up to 30 days
  - Limited damage if stolen
  - Possible to create single-use locker
  - Auto-clean when expired

Live demo of secret management



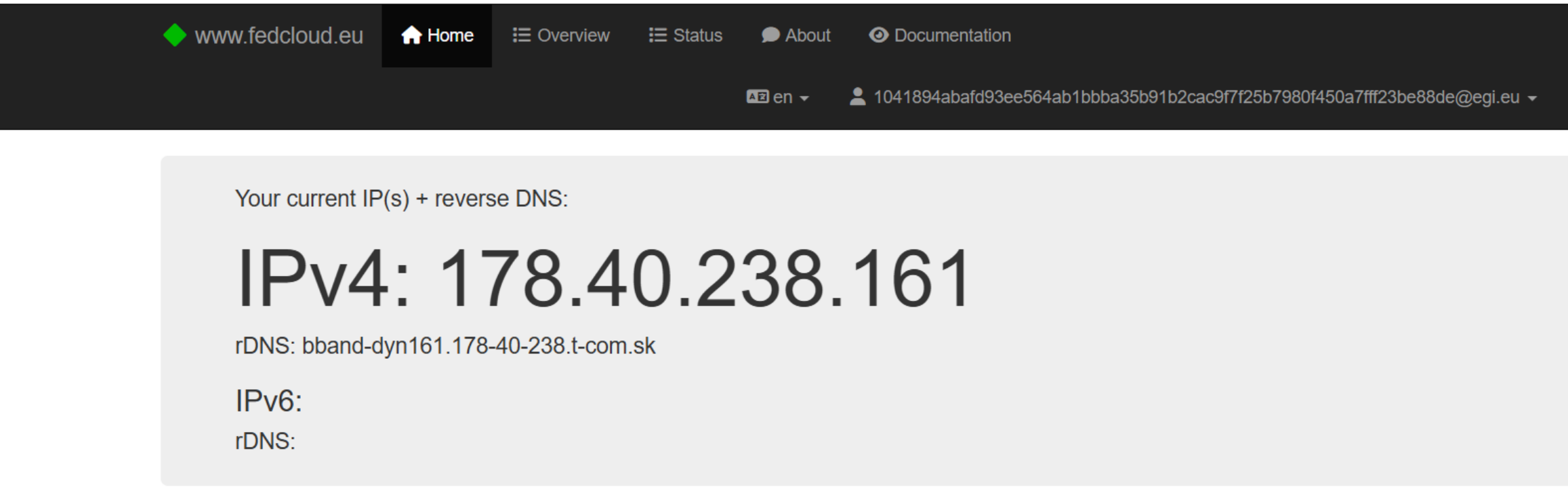
Dynamic DNS for Cloud Services

- Domain requirements:
  - Memorable, user-friendly URLs for easy access
  - SSL certificates for secure connection
- Challenges with dynamic deployment:
  - IPs are unknown in advance for dynamically deployed services.
  - Traditional DNS registration is slow and requires admin intervention.
- Solution: Dynamic DNS Service
  - Self-Service: Full self-service registration for users.
  - Quick Updates: IPs update within 1 minute, fully automated.
  - No Credentials Required: Operates without needing user credentials.

Demo Dynamic DNS

IBERGRID 2024
better software for better science

INSTITUTE OF INFORMATICS
SLOVAK ACADEMY OF SCIENCES



www.fedcloud.eu — the Dynamic DNS service for EGI Federated cloud

Summary

- Security is critical when the applications become large and require automation
- The offered tools and services can significantly improve the security of FedCloud:
  - Oidc-agent and Mytoken for token management
  - FedCloud client for resource management and support for cloud-native tools
  - Secret management service for storing app secrets
  - Dynamic DNS for user-friendly URLs and certificates

Thank you for your attentions

Support: viet.tran@savba.sk