FOSDEM'24

fedora

IPA-TUURA
FreeIPA connector for Keycloak

4 February 2024 | Brussels, Belgium

Francisco Triviño <**ftrivino@redhat.com**>

FreeIPA
Open Source Identity Management Solution

sssd

Background

Identity and Access Management (IAM) is an umbrella term

Identity and access management is an umbrella term, currently it defines multiple technologies and business processes to access the right assets at the right time for the right reasons while keeping an authorized access. Some examples of IAM products are:

- Microsoft Active Directory
- Red Hat Identity Management (FreeIPA)
- Keycloak
- Okta
- EntraID
- ……

Source:
Gartner Glossary Identity and Access Management (IAM)

Background

FreeIPA and Keycloak

FreeIPA

- Integrated identity management solution for POSIX-like environments (linux)
- Users and Groups consumed by the applications running in POSIX environment
- Ability to run application processes in presence of POSIX user and group IDs.

Keycloak

- IAM for Modern Applications
- Application level identities are not necessarily the same the system level ones.

Active Directory

- Users and groups relies on Security Identifiers (SIDs)
- Organizational Units (OUs)

Source:
FreeIPA.org
Keycloak.org
Active Directory

Background

Sometimes you need to integrate multiple IAM solutions

Sometimes you are happy having a standalone IAM solution… but that’s not the usual case… IAM defines:

- **SSO**: access multiple applications within the same organization or domain using a single set of credentials
- **Identity and User Federation**: It enables users to access applications or platforms across multiple enterprise domains that are part of the federated configuration

Source:
https://www.gartner.com/en/information-technology/glossary/sso-single-sign-on
https://www.gartner.com/en/information-technology/glossary/federated-identity-management

Background

Keycloak provides SSO and User Federation capabilities

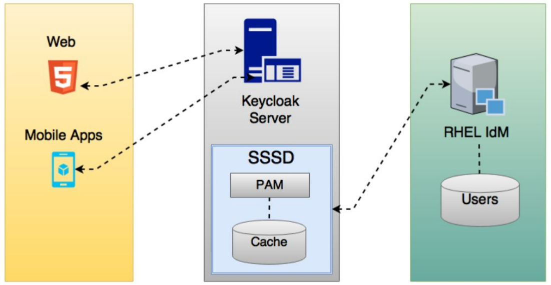
Keycloak User Federation Storage

- Keycloak first checks its internal user store when a user logs in and then looks through configured external User Storage providers if needed. Data from external stores is mapped into a common user model for runtime use.
- Keycloak already supports integration with FreeIPA as a backend to lookup and authenticate identities.

Source:
https://www.keycloak.org/docs/latest/server_admin/#_user-storage-federation

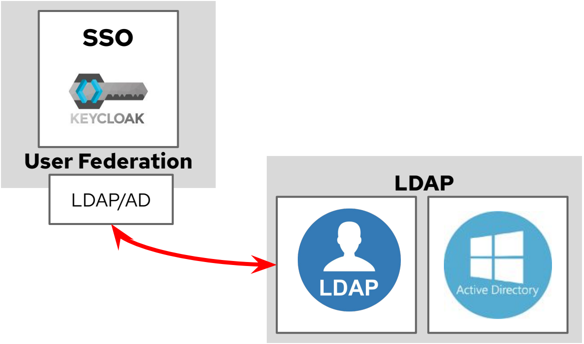
Background

Have a look to existing integration



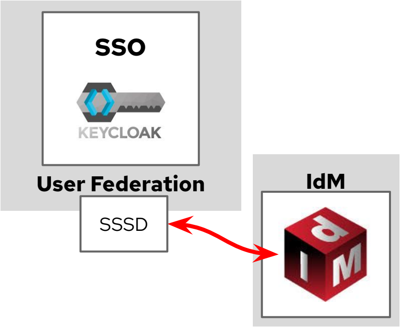
Keycloak and LDAP/AD

- Keycloak includes an LDAP/AD provider. You can federate multiple different LDAP servers in one Keycloak realm and map LDAP user attributes into the Keycloak common user model



Keycloak and SSSD/IdM

- Keycloak includes the System Security Services Daemon (SSSD) plugin. SSSD is part of the Fedora and Red Hat Enterprise Linux (RHEL), and it provides access to multiple identities and authentication providers. SSSD also provides benefits such as failover and offline support



Source:
https://www.keycloak.org/docs/latest/server_admin/#_ldap
https://www.keycloak.org/docs/latest/server_admin/#_sssd

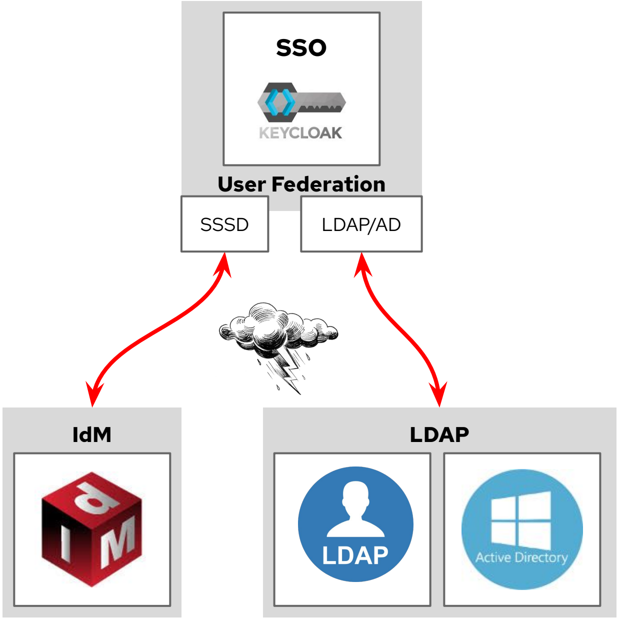
What's the problem then?

What problems are we trying to solve

Keycloak and LDAP/SSSD/FreeIPA

Existing gaps of current Keycloak integration with IdM/SSSD/LDAP

- SSSD/IdM and LDAP/AD integrations offer different features - missing feature parity
- Existing SSSD federation plugin is read-only, requires java dbus libraries and UNIX sockets
- Limitations for deployment in containers
- Complicated setup steps required

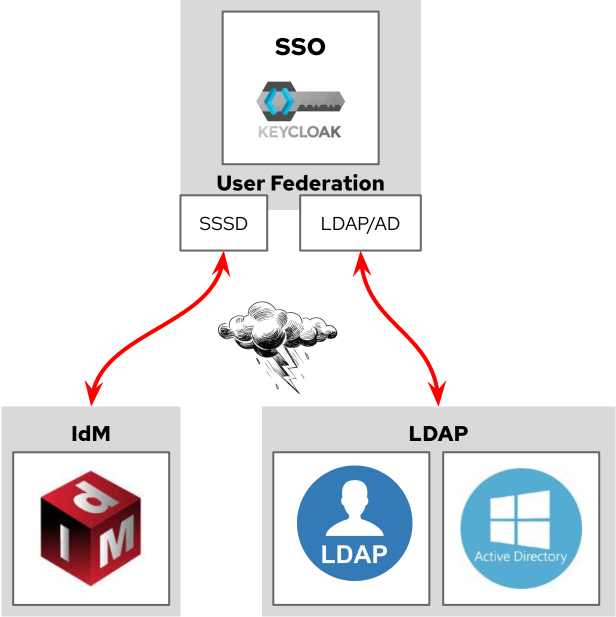


What problems are we trying to solve

Keycloak and LDAP/SSSD/FreeIPA

Existing gaps of current Keycloak integration with IdM/SSSD/LDAP

- SSSD/IdM and LDAP/AD integrations offer different features - missing feature parity
- Existing SSSD federation plugin is read-only, requires java dbus libraries and UNIX sockets
- Limitations for deployment in containers
- Complicated setup steps required



Re-design is needed

New ipa-tuura service comes into the play

What about to make a generic bridge?

Integration, automation, security, scalability….

We need a common API for managing identities, among other requirements:

- Able to read and write, authenticate users, from an Integration Domain
- Simplify integration. Replace existing plugins by just 1 plugin for FreeIPA/AD/LDAP
- Easy management of users/groups using the available lookup and import strategies
- Cloud-friendly maintainable solution
- No performance impact
- Do not reinvent the wheel, rely on existing open source projects

SCIM

System for Cross-domain Identity Management

SCIM

System for Cross-domain Identity Management

SCIM 2, the open API for managing identities is now complete and published under the IETF.

SCIM 2.0 is released as RFC7642, RFC7643 and RFC7644 under IETF

RFC7643 - SCIM: Core Schema

RFC7644 - SCIM: Protocol

RFC7642 - SCIM: Definitions

…… start from scratch?

- No need to…
  - There are multiple existing SCIM v2 open source projects we can rely on
- Let’s choose django-scim2,
  - written in Python, similar to FreeIPA.

REST API CRUD operations

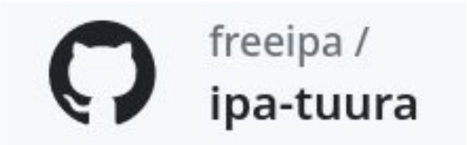
- POST
- PUT
- GET
- DELETE

django

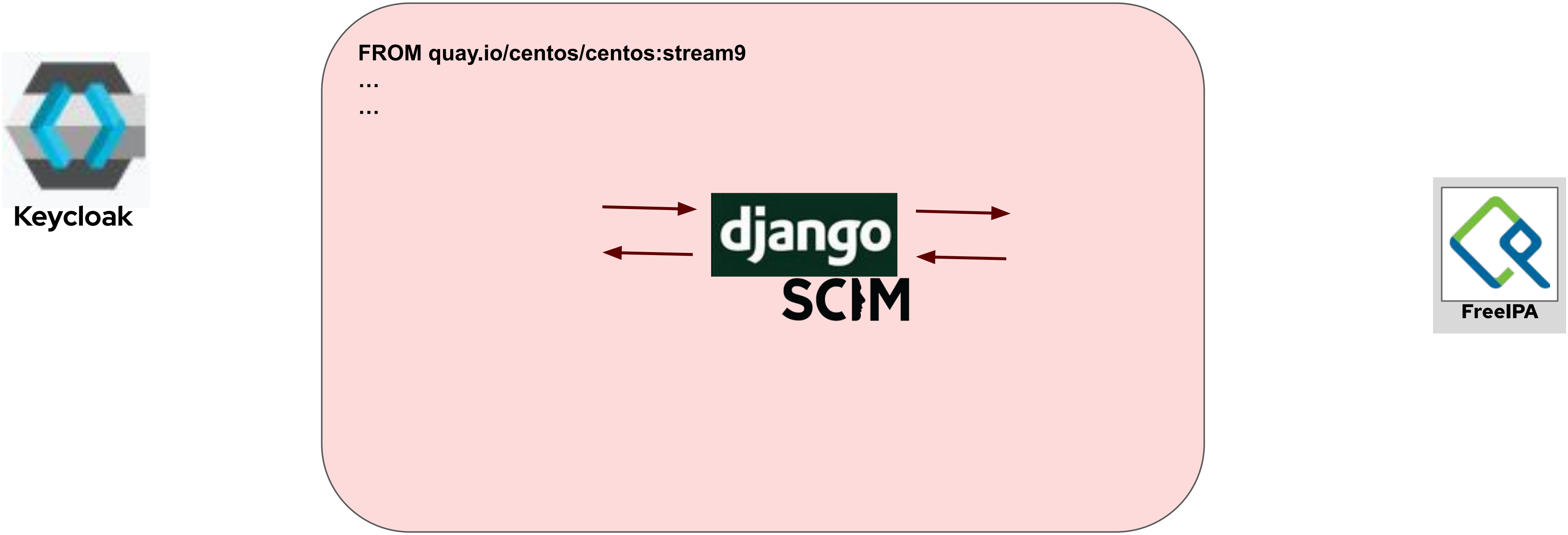
Source:
https://scim.cloud/

Ipa-tuura architecture

…… Cloud-friendly maintainable solution



freeipa /
ipa-tuura

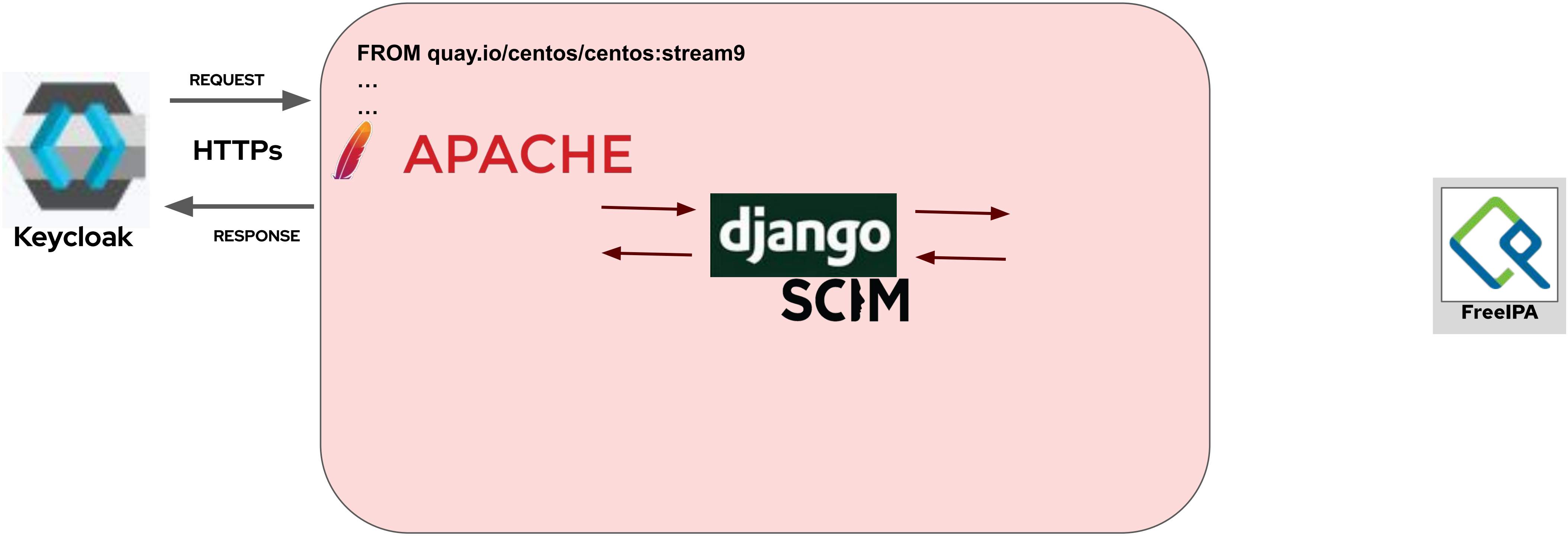


FROM quay.io/centos/centos:stream9
…
…

freeipa / **ipa-tuura**

Ipa-tuura architecture

...... Security

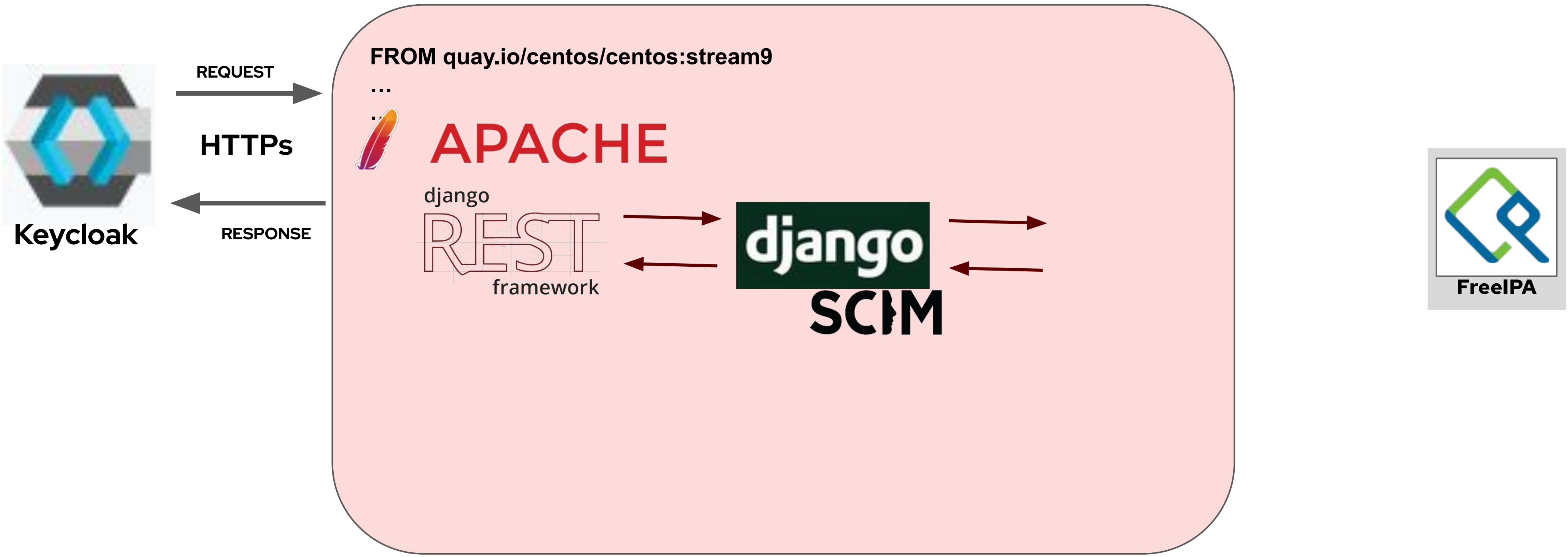


```
FROM quay.io/centos/centos:stream9
...
...
```

Ipa-tuura architecture

...... generic API

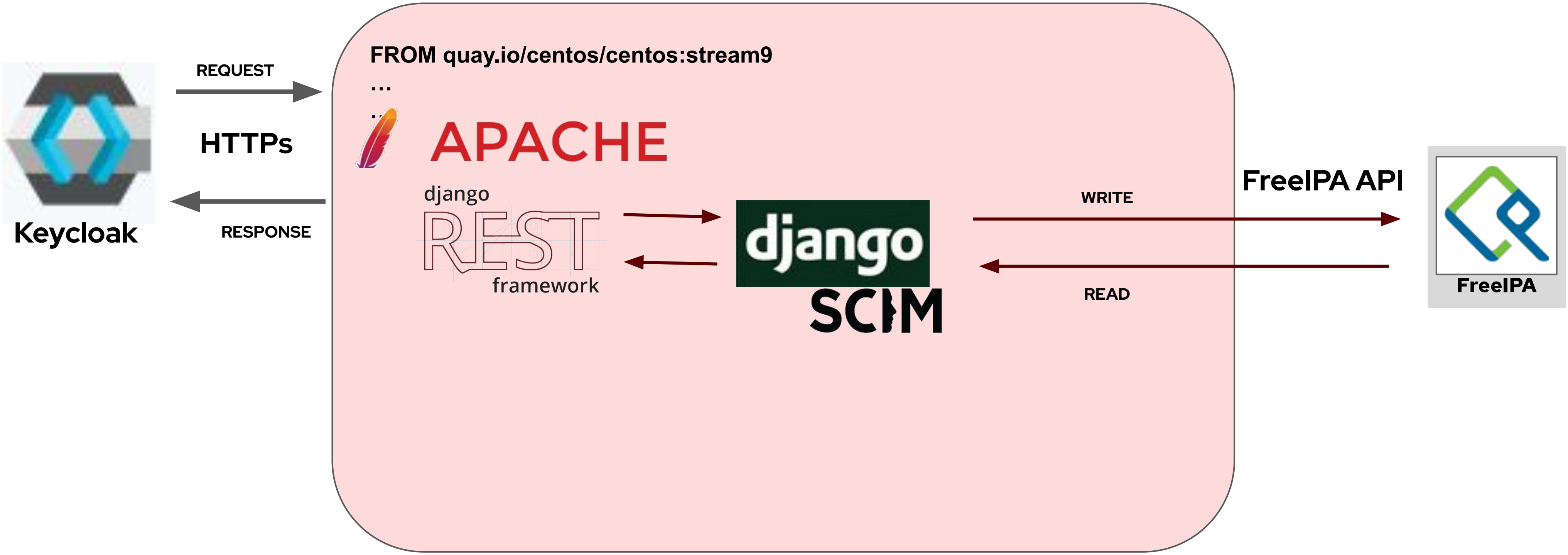
freeipa /
ipa-tuura


FROM quay.io/centos/centos:stream9
...
..

Ipa-tuura architecture

…… generic API

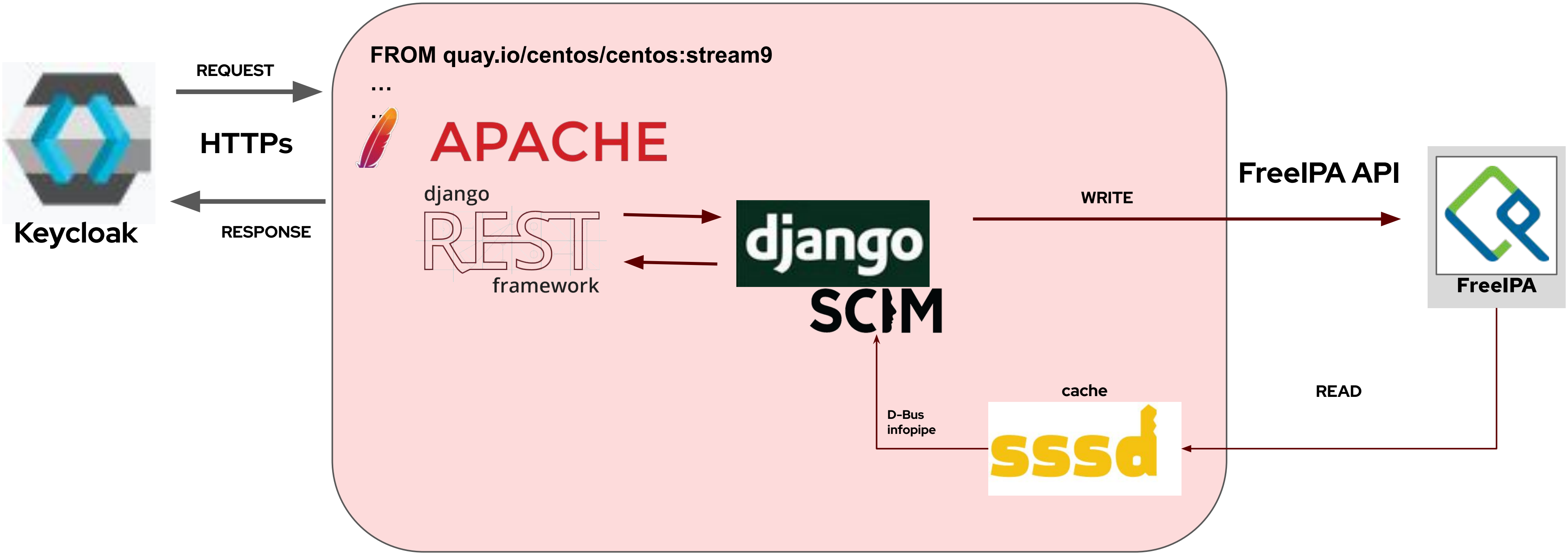
freeipa /
ipa-tuura



freeipa / ipa-tuura

Ipa-tuura architecture

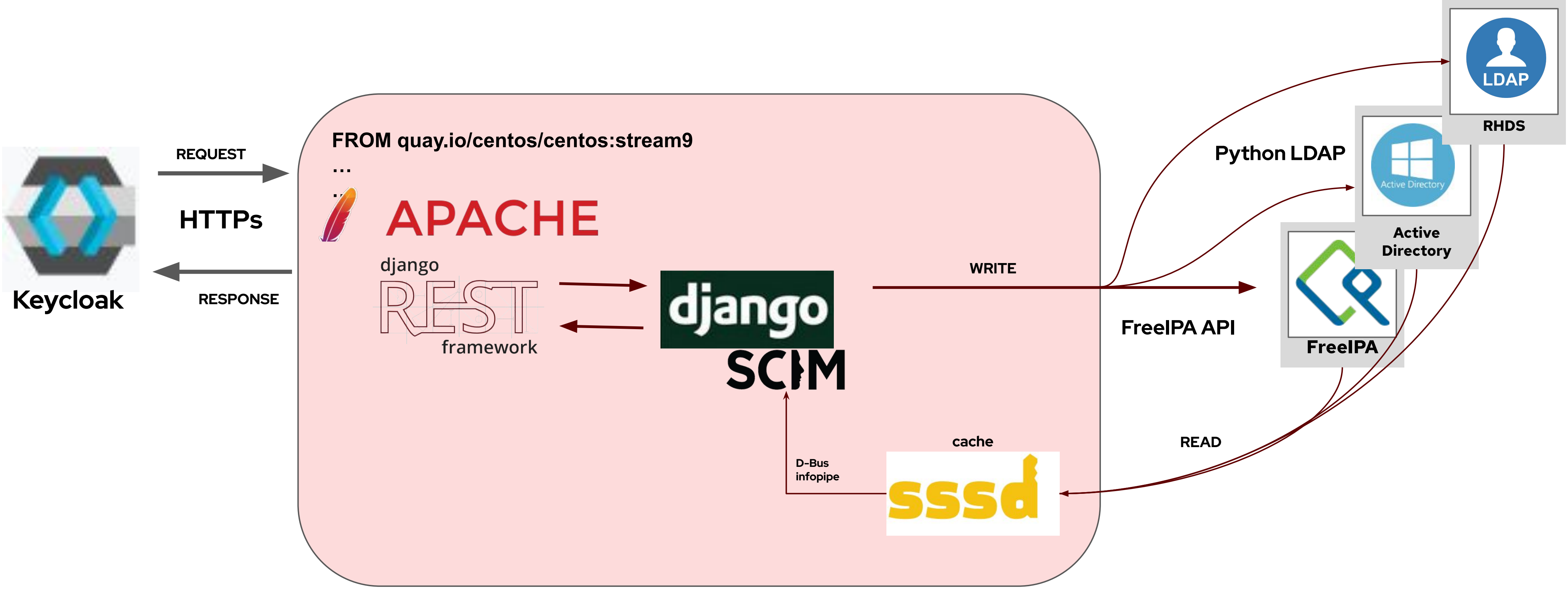
... no performance impact



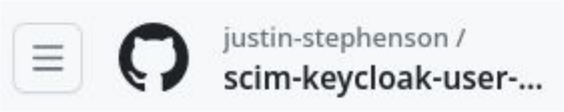
Ipa-tuura architecture

... unify

freeipa /
ipa-tuura



What about Keycloak, does it support SCIM calls?



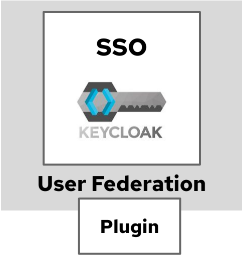
justin-stephenson /
scim-keycloak-user-...

What about Keycloak?

Replace existing SSSD plugin by a generic SCIM Client

Replace existing plugin with SCIM plugin for IdM/AD/LDAP:

- New Keycloak plugin acts as SCIM client, uses Apache HTTPs client to make calls to scim v2 endpoints
- Requests for user information and user authentication in keycloak will be forwarded to the plugin and proxied to backend
  - Users SSO login and password authentication
  - Supports
  - -- Looking up users
  - -- Adding users
  - -- Deleting users
  - -- User modifications (Email, first name, last name)

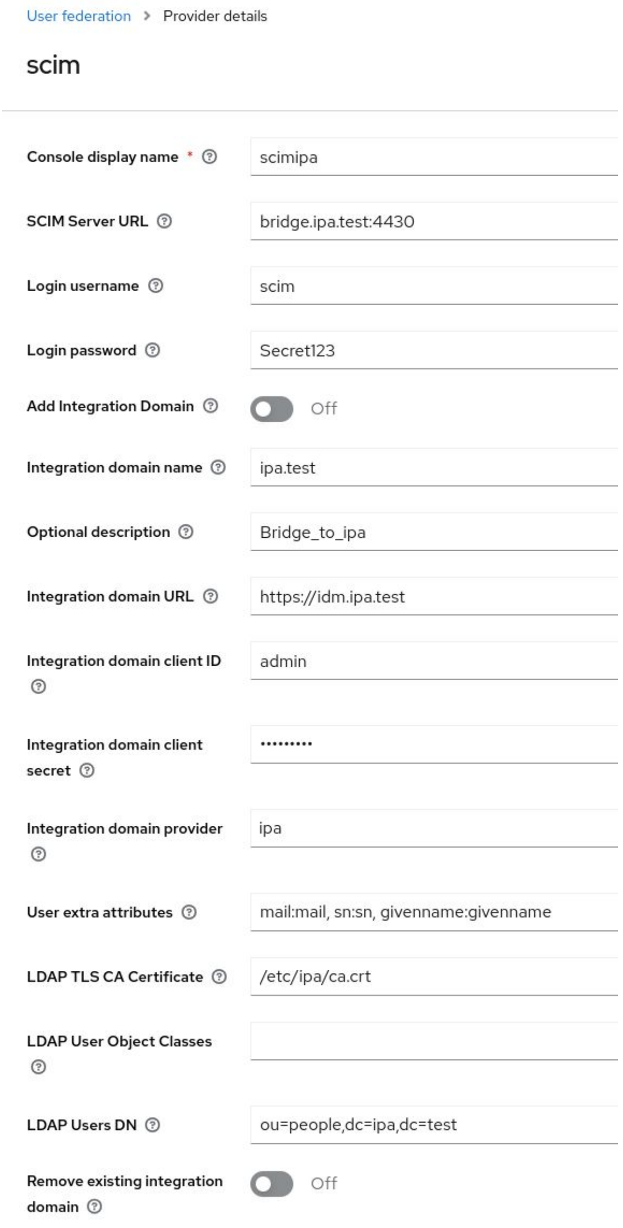


Source:
https://github.com/justin-stephenson/scim-keycloak-user-storage-spi/

What about Keycloak?

Replace existing SSSD plugin by a generic SCIM Client

Ipa-tuura: FreeIPA connector for Keycloak



User federation > Provider details

scim

Console display name *	scimipa
SCIM Server URL	bridge.ipa.test:4430
Login username	scim
Login password	Secret123
Add Integration Domain	Off
Integration domain name	ipa.test
Optional description	Bridge_to_ipa
Integration domain URL	https://idm.ipa.test
Integration domain client ID	admin
Integration domain client secret	•••••••••
Integration domain provider	ipa
User extra attributes	mail:mail, sn:sn, givenname:givenname
LDAP TLS CA Certificate	/etc/ipa/ca.crt
LDAP User Object Classes	
LDAP Users DN	ou=people,dc=ipa,dc=test
Remove existing integration domain	Off

SCIMv2 Bridge connection

Integration Domain enrollment

SCIMv2 Bridge options

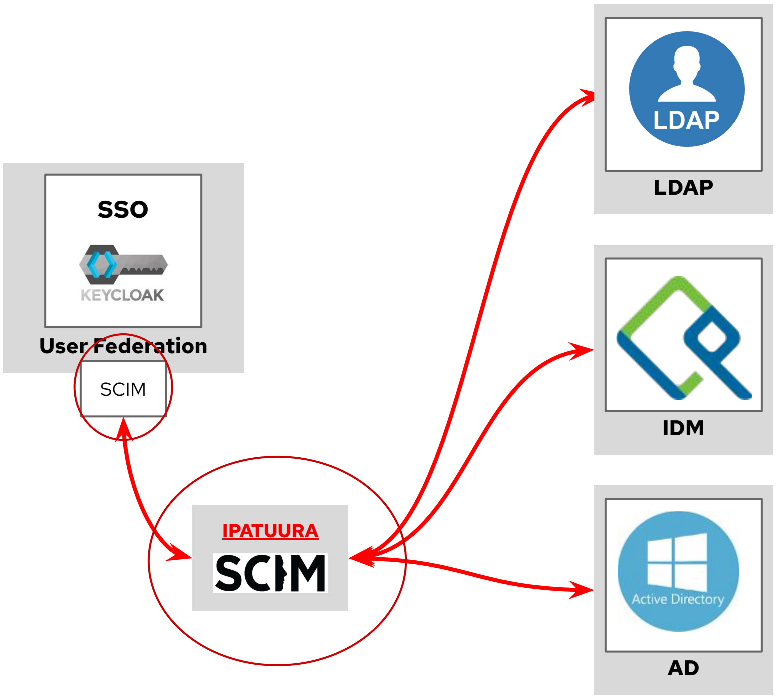
(configures SSSD)

Summing up

New integration

freeipa /
ipa-tuura

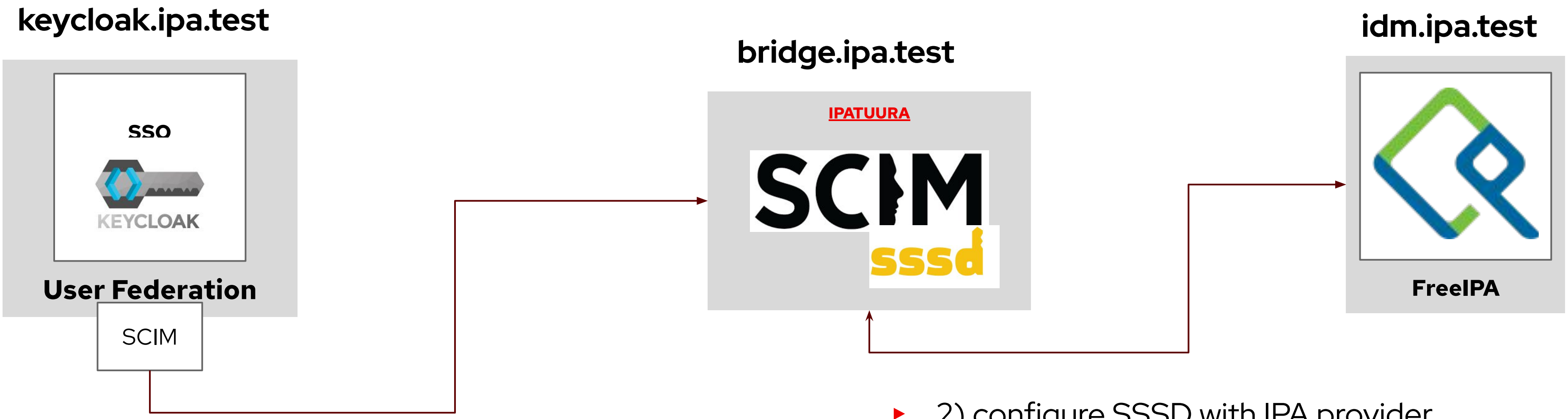
- Keycloak plugin sends with ipa-tuura (Bridge service) over HTTPS to ***/domains/v1/domain*** endpoint to add and remove Integration domains.
- Keycloak plugin communicates with ipa-tuura (Bridge service) over HTTPS to ***/scim/v2*** specification endpoints.
- **ipa-tuura** provides REST API, translates SCIM endpoint requests into identity provider operations on the backend.
- Keycloak Plugin does **not** communicate directly with backend servers (IDM, AD, LDAP).



Source:
https://github.com/freeipa/ipa-tuura

DEMO

Add FreeIPA Integration Domain

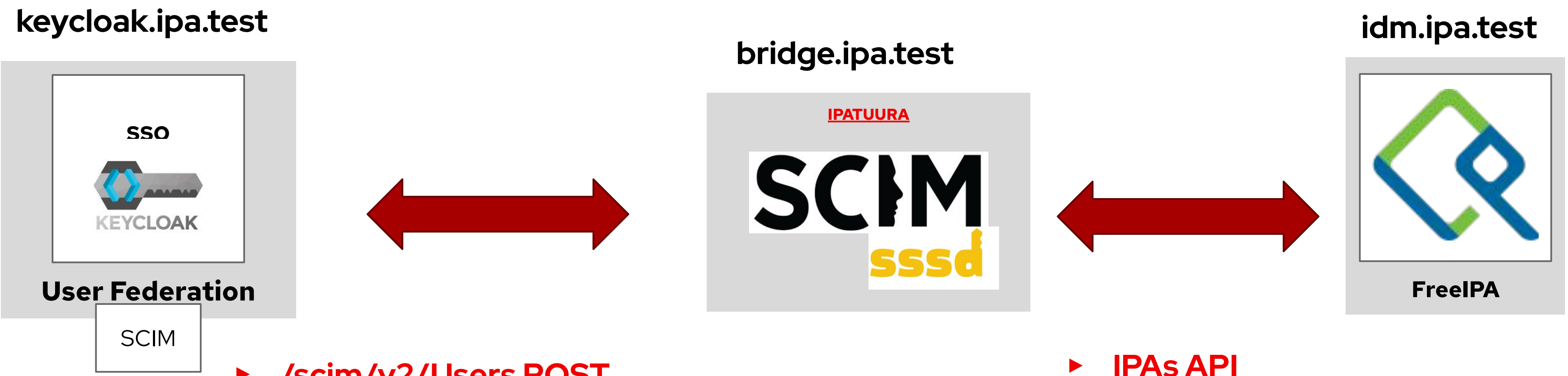


- 1) HTTPs POST request to ***/domains/v1/Domain***
  - *bridge.ipa.test:4430*
  - *ou=people,dc=ipa,dc=test*
  - ….

- 2) configure SSSD with IPA provider
- 3) add ipa-tuura **service** using IPAs API
- 4) add ipa-tuura **role** using IPAs API
- 5) add ipa-tuura **privilege** using IPAs API
- 6) generate a **keytab** for the writable interface

DEMO

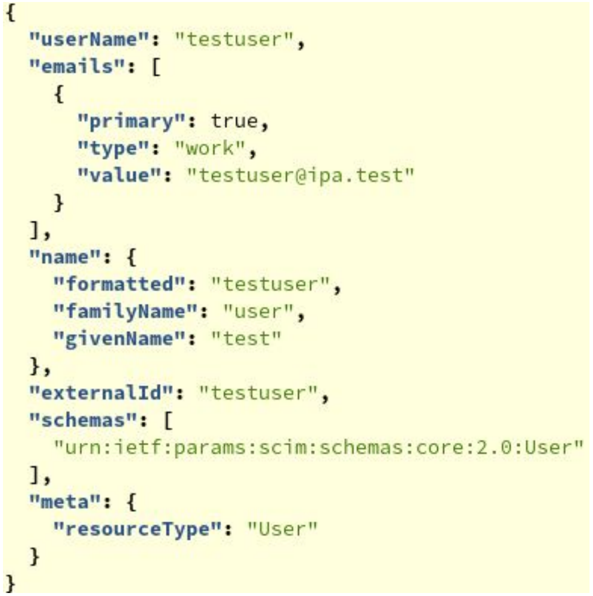
Ready to manipulate users


keycloak.ipa.test

bridge.ipa.test

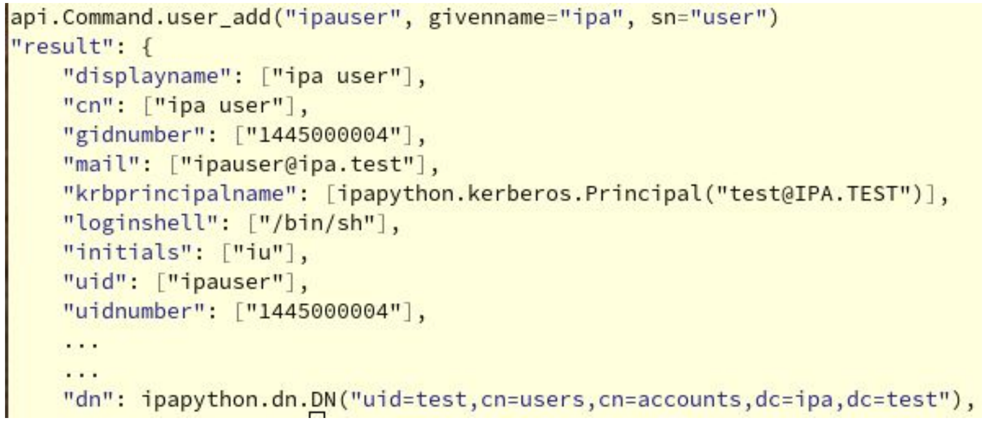
idm.ipa.test

- **/scim/v2/Users POST**



```
{
  "userName": "testuser",
  "emails": [
    {
      "primary": true,
      "type": "work",
      "value": "testuser@ipa.test"
    }
  ],
  "name": {
    "formatted": "testuser",
    "familyName": "user",
    "givenName": "test"
  },
  "externalId": "testuser",
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "meta": {
    "resourceType": "User"
  }
}
```

- **IPAs API**

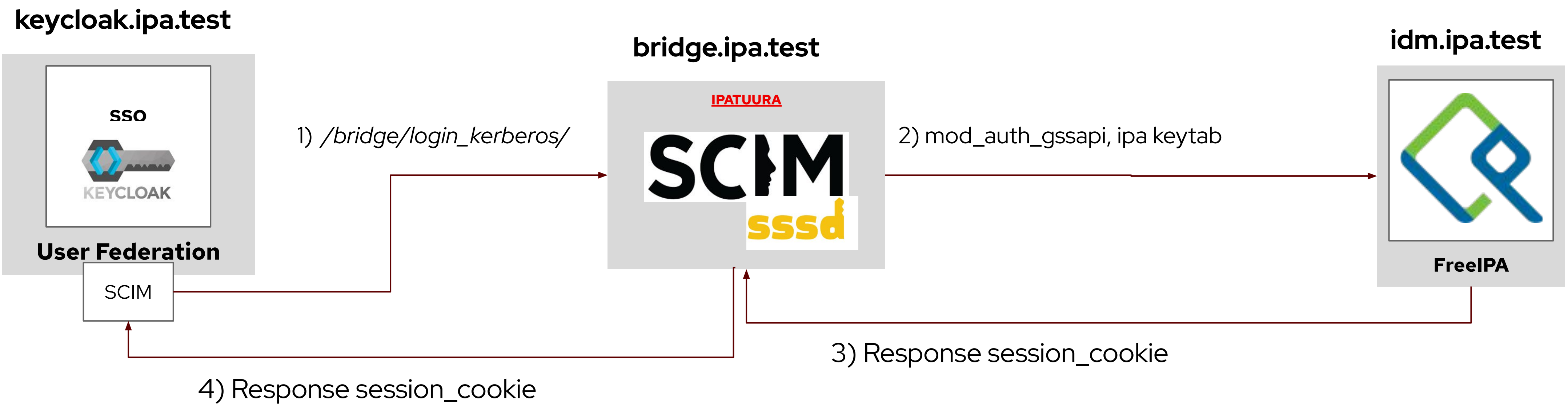


```
api.Command.user_add("ipauser", givenname="ipa", sn="user")
"result": {
    "displayname": ["ipa user"],
    "cn": ["ipa user"],
    "gidnumber": ["1445000004"],
    "mail": ["ipauser@ipa.test"],
    "krbprincipalname": [ipapython.kerberos.Principal("test@IPA.TEST")],
    "loginshell": ["/bin/sh"],
    "initials": ["iu"],
    "uid": ["ipauser"],
    "uidnumber": ["1445000004"],
    ...
    ...
    "dn": ipapython.dn.DN("uid=test,cn=users,cn=accounts,dc=ipa,dc=test"),
```

Ipa-tuura: FreeIPA connector for Keycloak

Work In Progress

Kerberos GSSAPI Authentication


keycloak.ipa.test
SSO
KEYCLOAK
User Federation
SCIM
1) /bridge/login_kerberos/
bridge.ipa.test
IPATUURA
SCIM
sssd
2) mod_auth_gssapi, ipa keytab
idm.ipa.test
FreeIPA
3) Response session_cookie
4) Response session_cookie

Potential usages

Ipa-tuura: FreeIPA connector for Keycloak

The bridge can also be used in a variety of different scenarios:

- Synchronization of identities across different providers
- Migration of identities across different providers
- Provide a SCIM server for other IAMs such as Okta, EntraID...

https://github.com/freeipa/ipa-tuura

https://github.com/justin-stephenson/scim-keycloak-user-storage-spi/

Q&A

Tech Stack

django REST framework

SCIM

Red Hat Developer

django

KEYCLOAK

podman

FreeIPA
Open Source Identity Management Solution

APACHE
HTTP SERVER PROJEC

sssd

Thank you