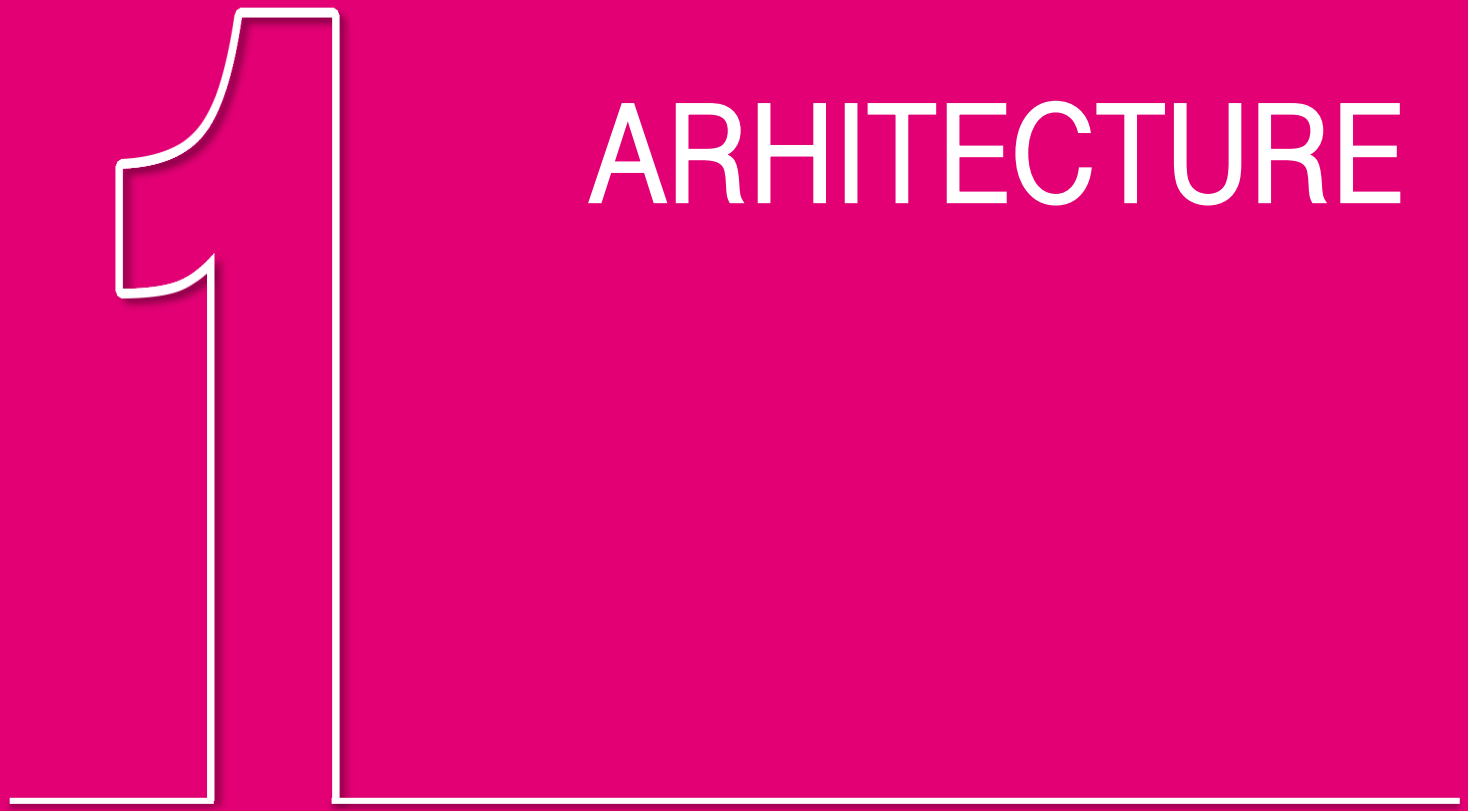
Keycloak in Croatia Telekom

Hands on experience in deployment and customization

T · ·

LIFE IS FOR SHARING.



ARHITECTURE

LANDSCAPE – TODAY

HT libraries

Vendors libraries

Keycloak libraries

oAuth1.0a

SAML

Open ID Connect

Open ID 2.0

HT SSO

KEYCLOAK

ARCHITECTURE

Client APP

Redundant Load Balancers

Application server cluster

#1

Infinispan

KEYCLOAK

replication

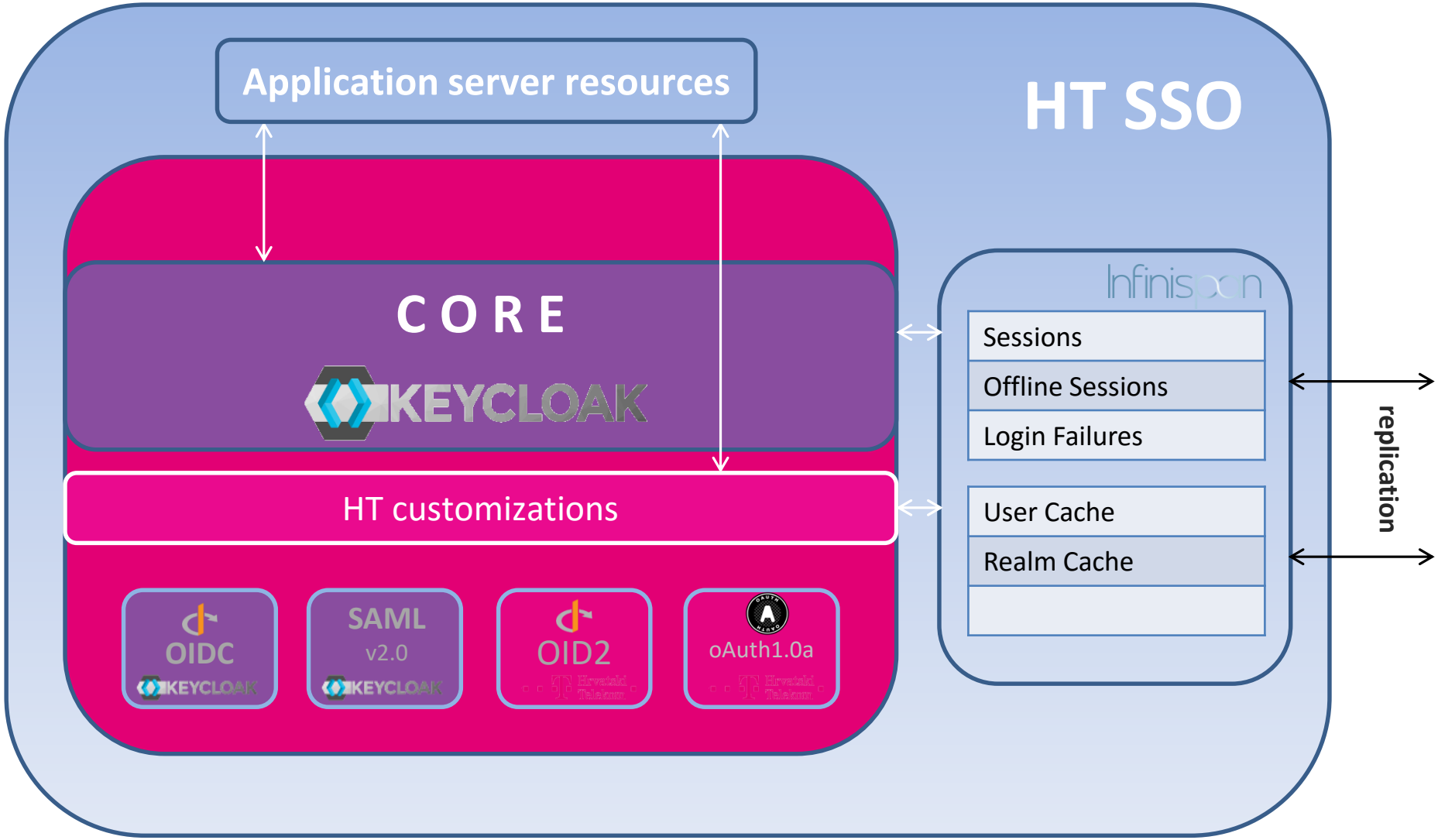
#N

Infinispan

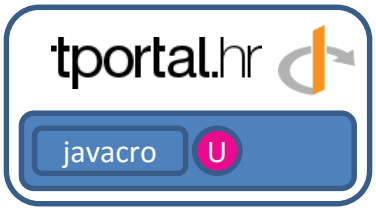
KEYCLOAK

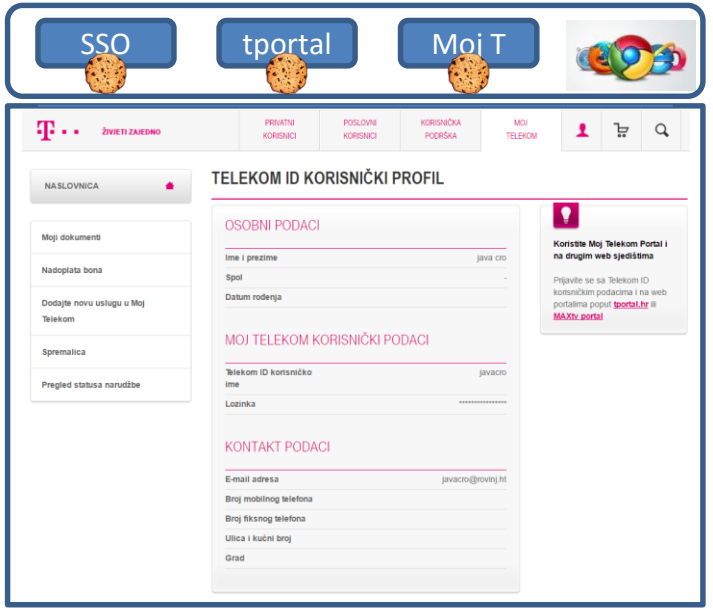
DB FARM

ARCHITECTURE (2)



REAL LIFE SCENARIO



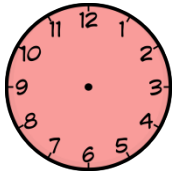


Infinispan

Sessions C U C U
Offline Sessions
Login Failures

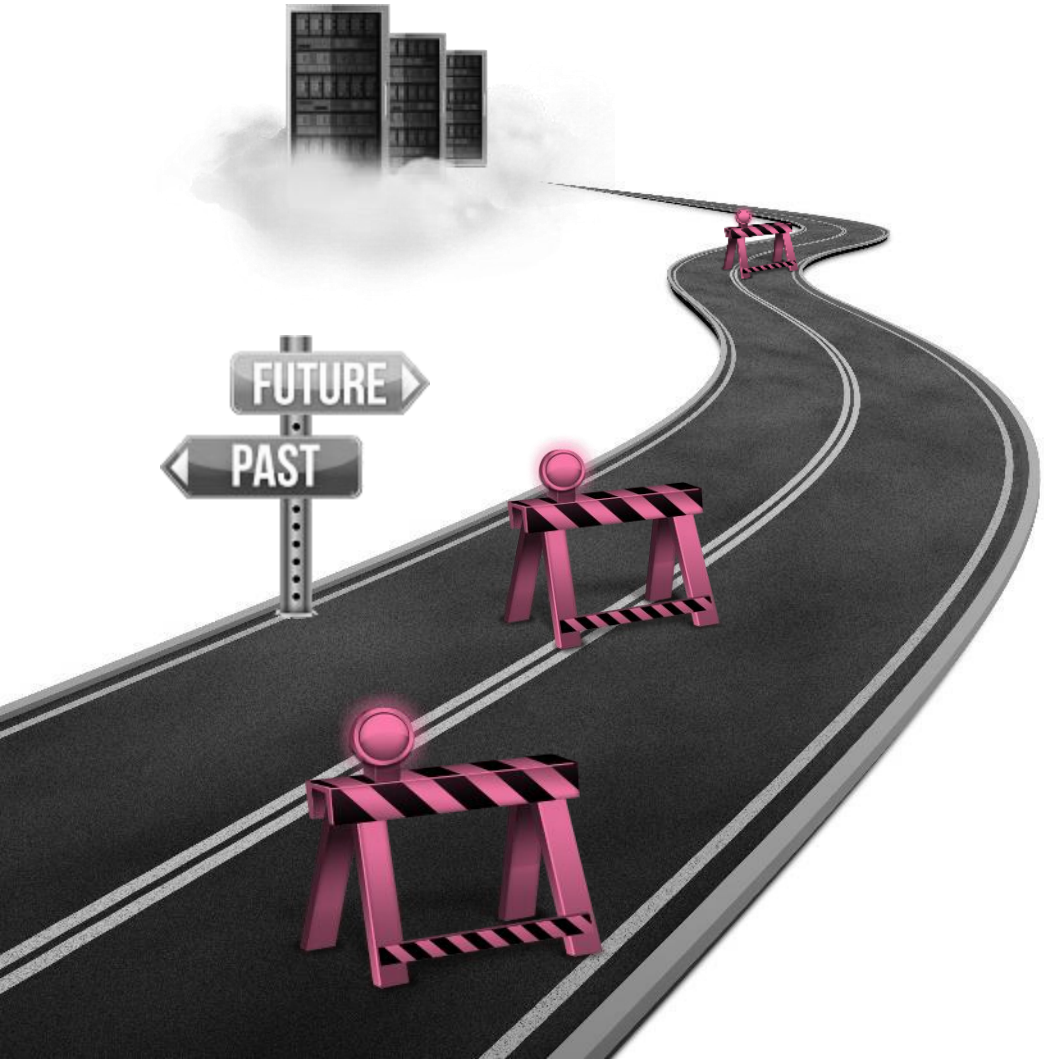
Infinispan

Sessions C U C U
Offline Sessions
Login Failures



MIGRATION

LONG WAY...



2017 +

More consolidated landscape

New features implementation, more integrated applications

Keycloak upgrade

2016-now

- **Keycloak** in production
- **OpenID Connect** as standard for new applications

- Support for **legacy protocols** and **Delegated Login Forms**
- Many **custom legacy features** implemented on Keycloak
- **Migration** of >20 applications
- **Retirement** of old SSO systems

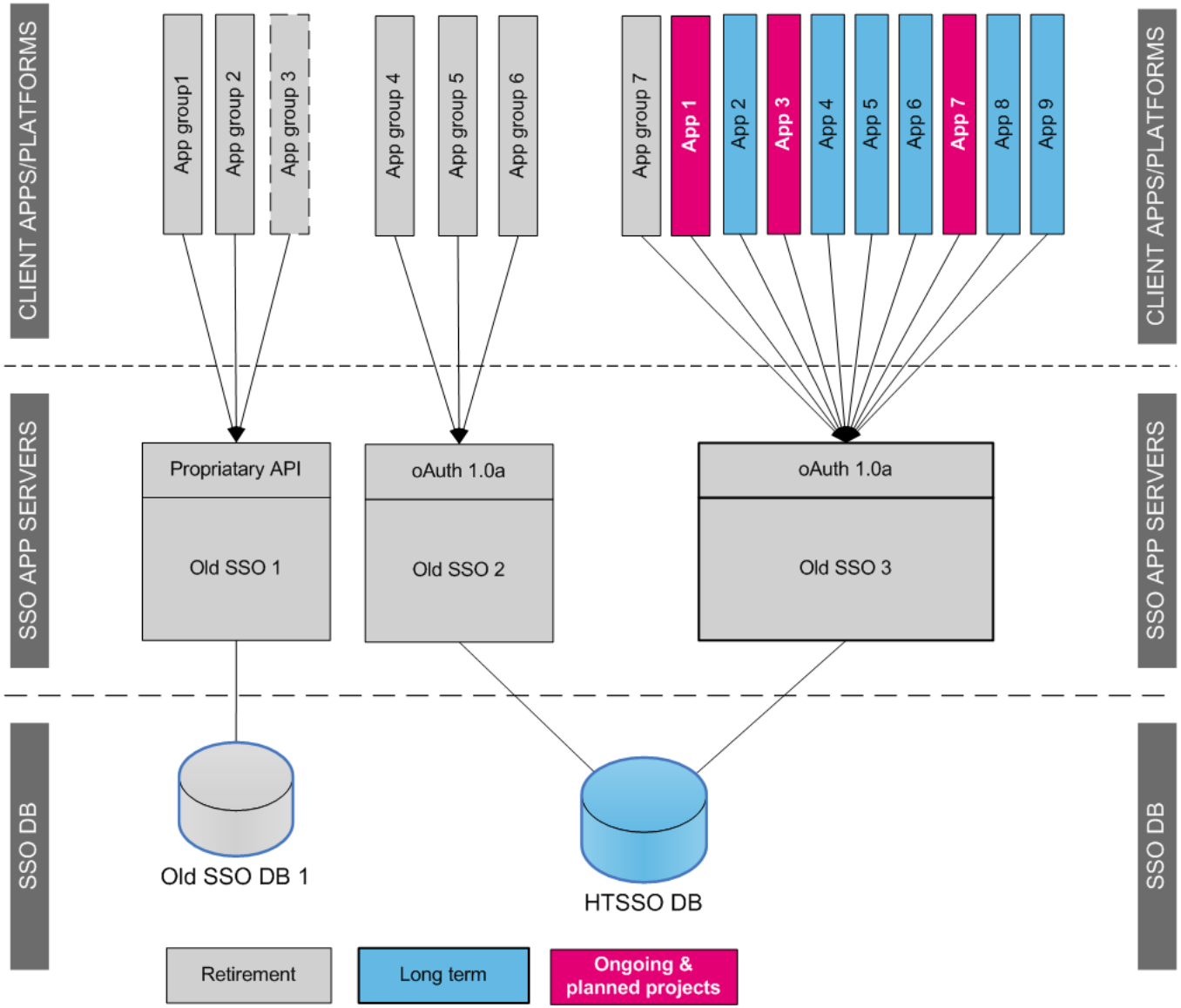
- Launched new application on Keycloak (Tportal)
- **'Test Lab'** implementation
- Open Stack readiness
- Full virtualization

2013- 2015

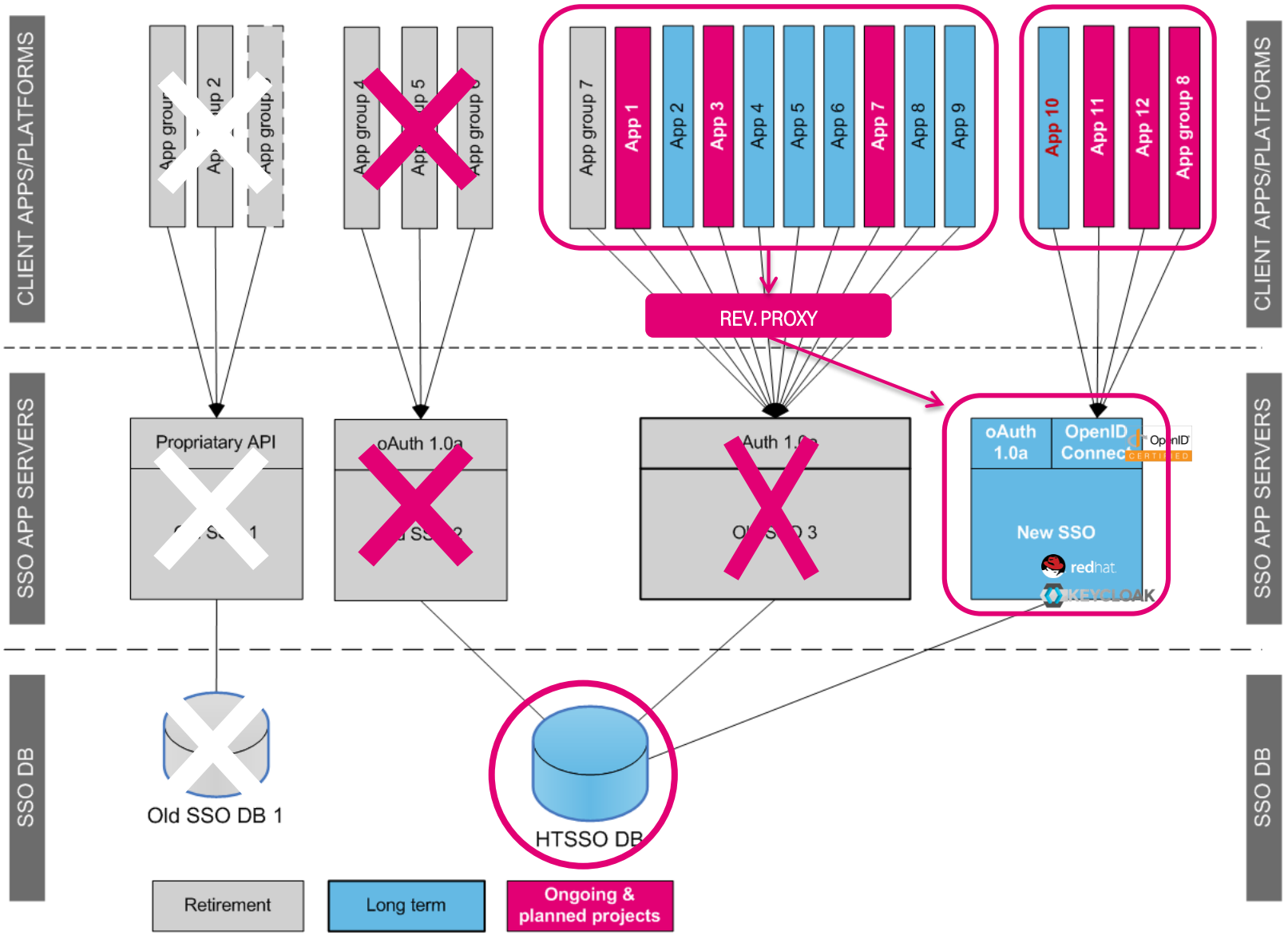
Idea & Conceptualization of Target Picture

Proof of Concept for Keycloak

...WHERE WE STARTED...



...AND WHAT WE DID...

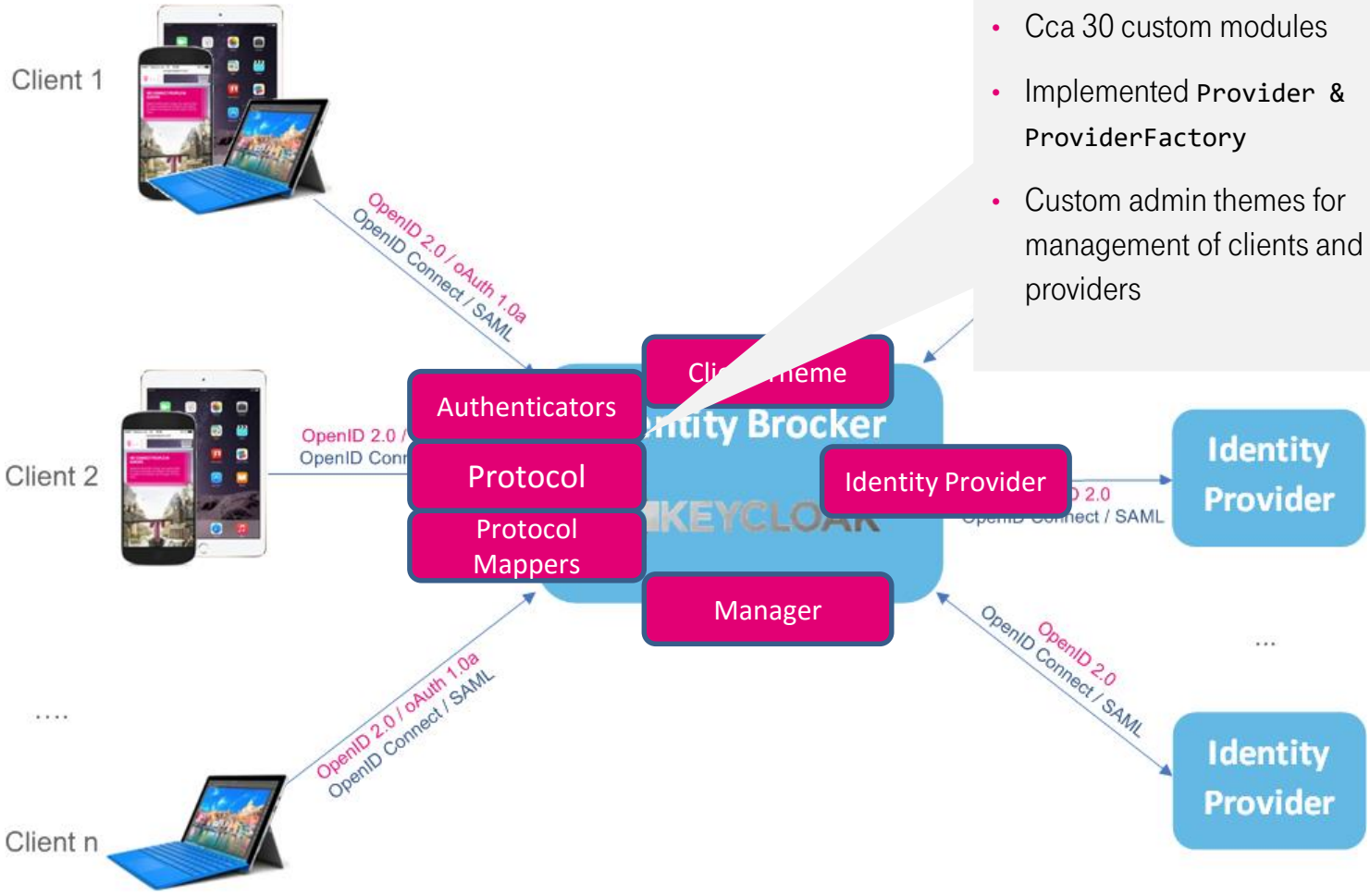


CUSTOMIZING KEYCLOAK

CUSTOMISATIONS

Keycloak as Identity Provider	Keycloak as Identity Broker	OpenId 2.0 support	oAuth 1.0a support	Custom client views
HA architecture	Manager SPI	Authenticators	Keycloak data model extensions	Personalized themes
Keycloak/Wildfly configuration	Protocol SPI	Identity Provider SPI	Zero Touch Authentication	Delegated Login Forms

CUSTOMISATIONS (2)

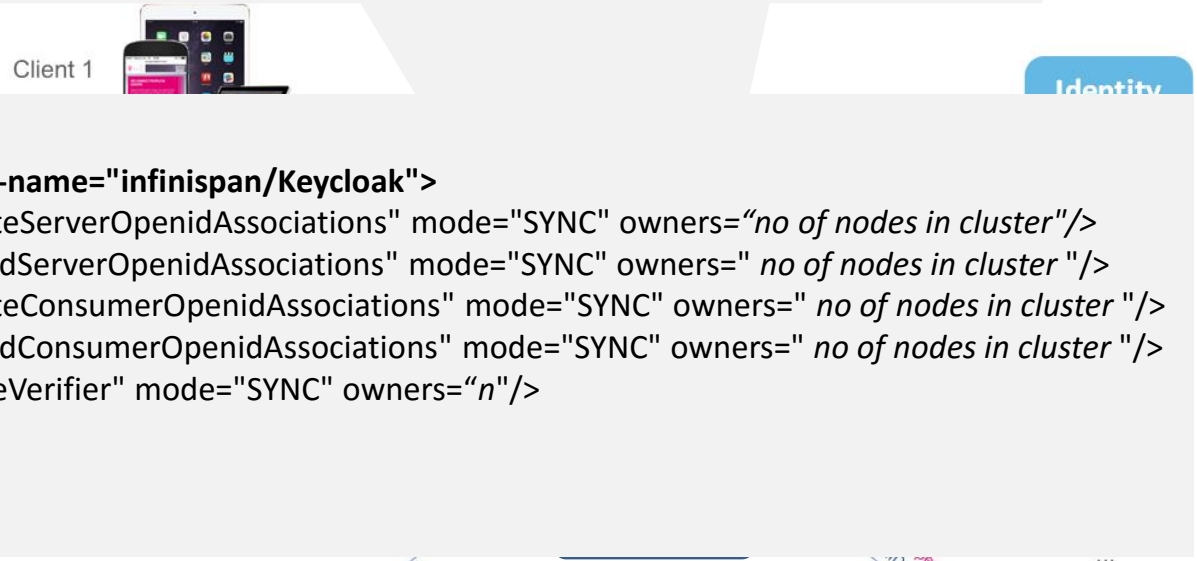


PLUGGABLE MODULES

- Cca 30 custom modules
- Implemented `Provider & ProviderFactory`
- Custom admin themes for management of clients and identity providers

OPEN ID MANAGER

- CONSUMER - Serves as Identity Federation Provider
- SERVER - Serves as Identity Provider; required to store private and shared associations according to protocol, implements nonce verifier, uses Infinispan to work in a cluster:
- Manager is taking care of time expiration of associations

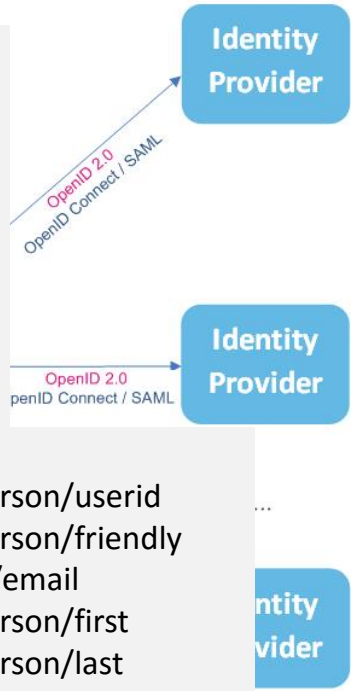



```
<cache-container name="keycloak" jndi-name="infinispan/Keycloak">
        <distributed-cache name="privateServerOpenidAssociations" mode="SYNC" owners="no of nodes in cluster"/>
        <distributed-cache name="sharedServerOpenidAssociations" mode="SYNC" owners=" no of nodes in cluster "/>
        <distributed-cache name="privateConsumerOpenidAssociations" mode="SYNC" owners=" no of nodes in cluster "/>
        <distributed-cache name="sharedConsumerOpenidAssociations" mode="SYNC" owners=" no of nodes in cluster "/>
        <distributed-cache name="nonceVerifier" mode="SYNC" owners="n"/>
        ...
</cache-container>
```

PROTOCOL & PROTOCOL MAPPERS

- Protocol
  - Discovery endpoint
  - Authorization / Logout endpoint
  - Installation -> module.xml
- Protocol mappers
  - Attribute exchange with client

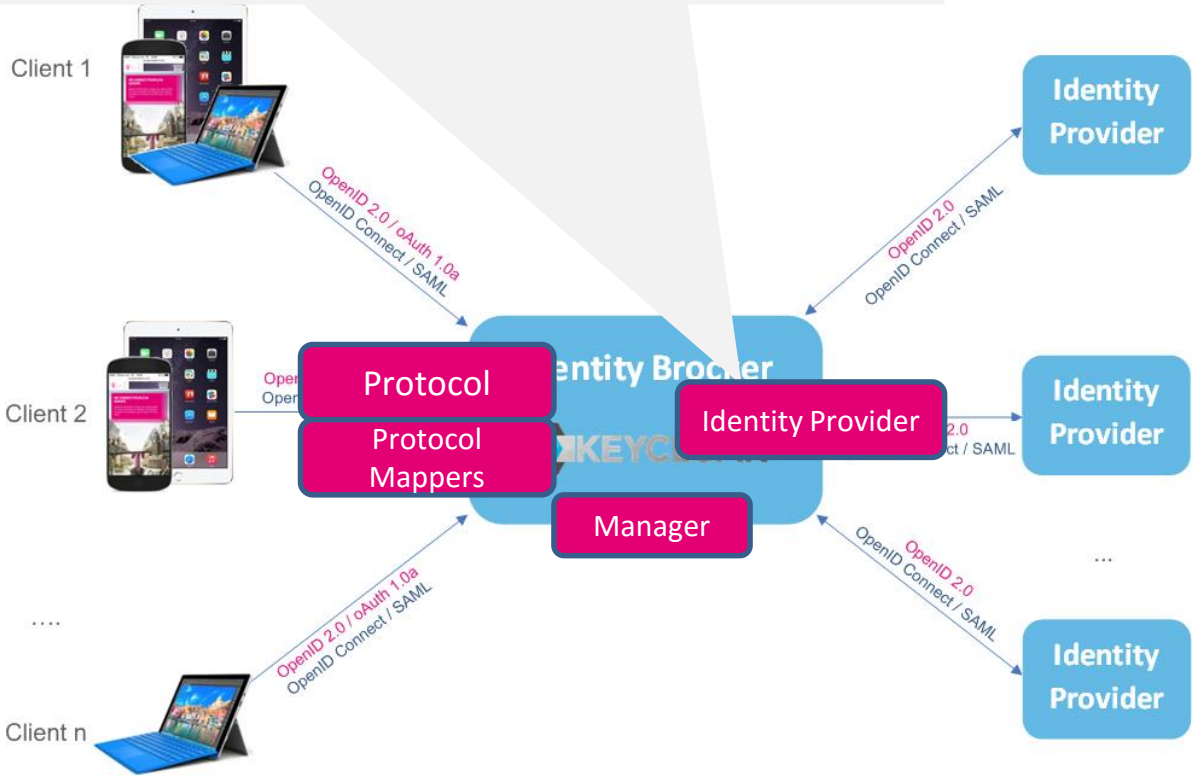
```
<?xml version="1.0" encoding="UTF-8"?>

<module xmlns="urn:jboss:module:1.3" name="org.keycloak.keycloak-ht-services-oid2">
        <resources>
                <resource-root path="keycloak-custom-oid2-1.0.0.Final.jar"/>
        </resources>
        <dependencies>
        <module name="org.keycloak.keycloak-core" services="import"/>
        ...
        <module name="org.openid4java"/>
        <module name="org.jdom"/>
        ...
        </dependencies>
</module>
```



http://axschema.org/namePerson/userid
http://axschema.org/namePerson/friendly
http://axschema.org/contact/email
http://axschema.org/namePerson/first
http://axschema.org/namePerson/last

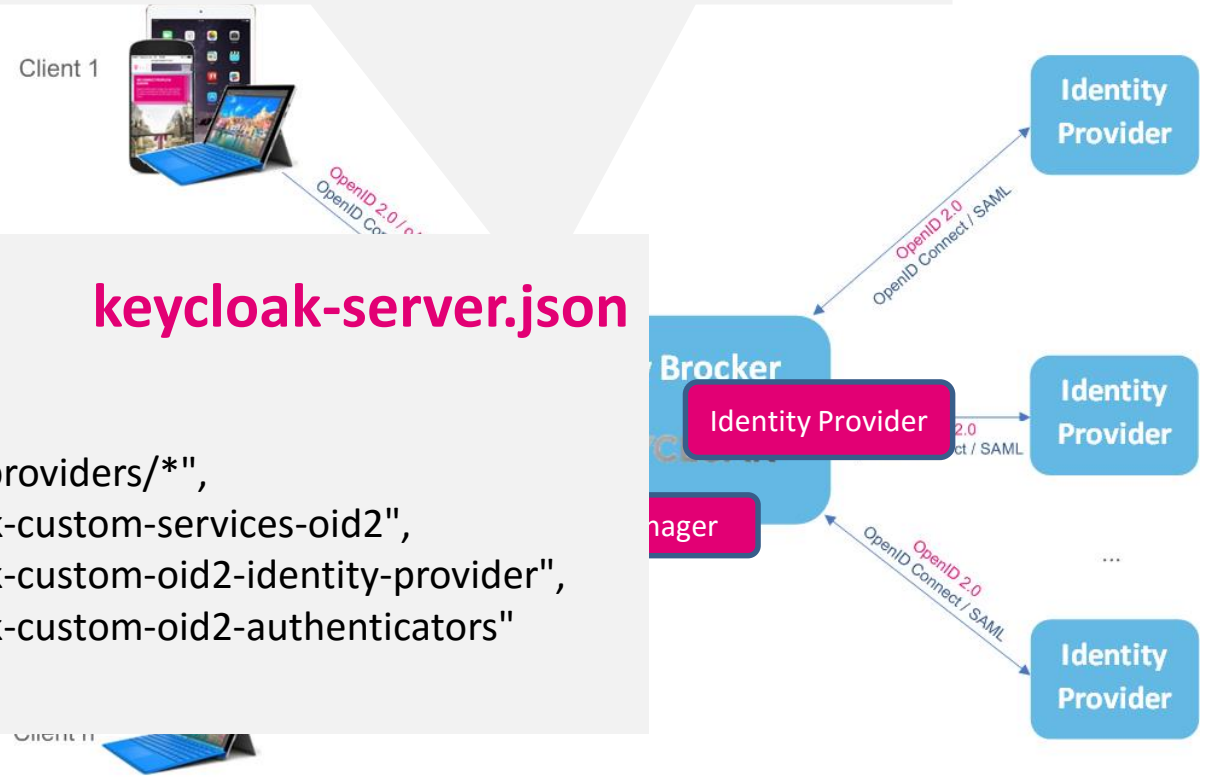
FEDERATED IDENTITY PROVIDERS

- logout endpoint / callback endpoint that parses federated IDP attribute exchange values (supports logout action initiated from the federated IdP)
- choose from dropdown or pass providerid hint (support for multiple federated IdPs)



AUTHENTICATORS

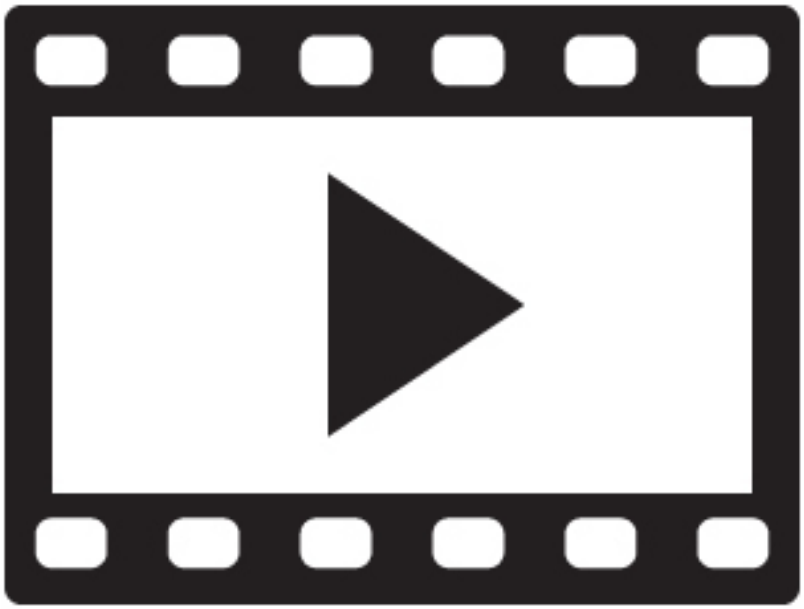
- cookie check
- if openID is present:; recognize user by claimed _id identifier
  http://specs.openid.net/auth/2.0/identifier_select



keycloak-server.json

```
"providers": [
   "classpath:${jboss.home.dir}/providers/*",
   "module:org.keycloak.keycloak-custom-services-oid2",
   "module:org.keycloak.keycloak-custom-oid2-identity-provider",
   "module:org.keycloak.keycloak-custom-oid2-authenticators"
],
```

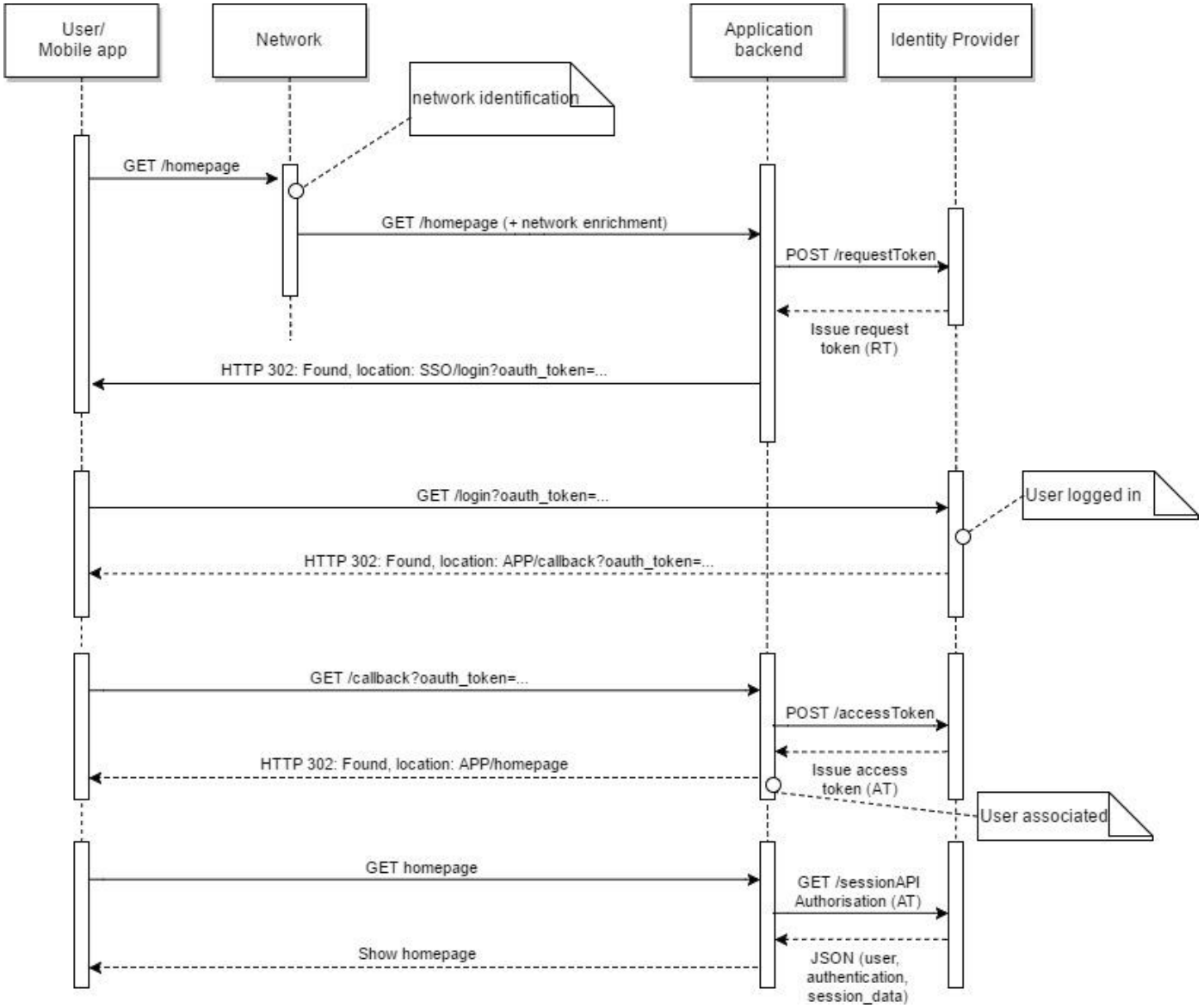
DEMO



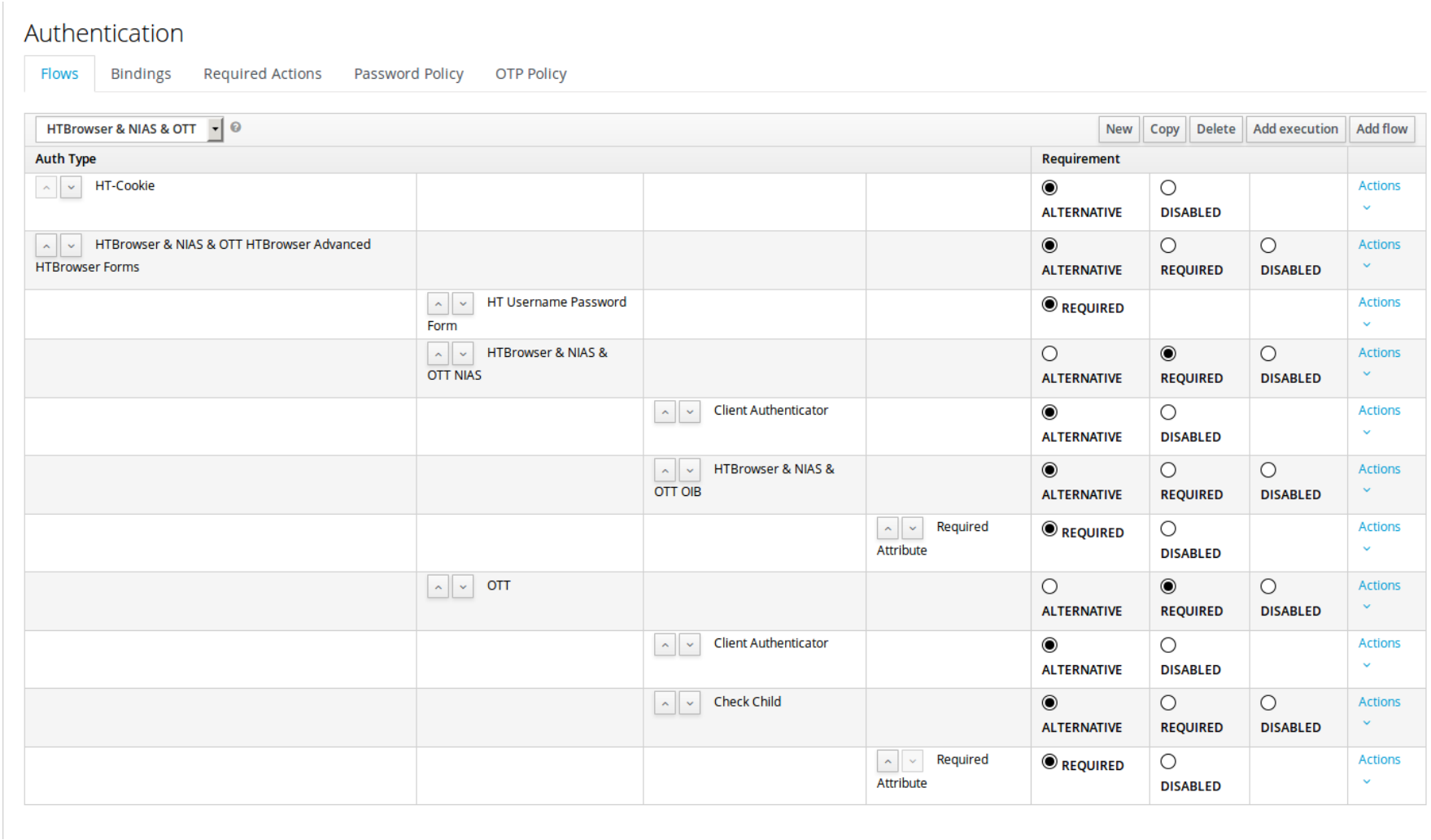
ZERO TOUCH AUTHENTICATION

- User is automaticly authenticated in its account – TelekomID – associated with his mobile phone number (MSISDN)
- Mobile network is used as an enabler for this feature)
- Customizations:
  - Keycloak data model extension
  - Custom ZTA authenticator
  - Keycloak REST interface extension for integration with BSS systems

ZERO TOUCH AUTHENTICATION - FLOW

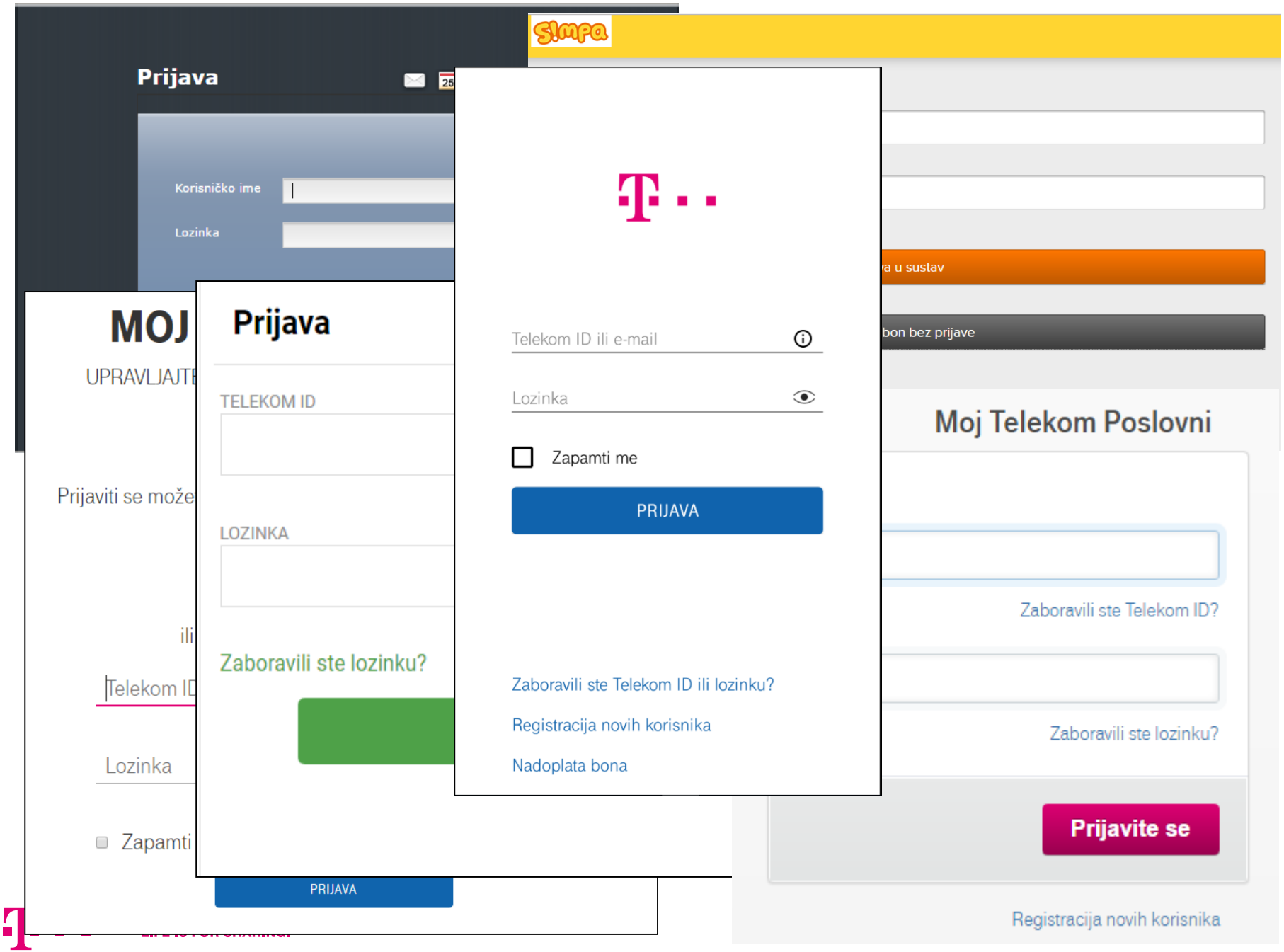


COMPLEX AUTHENTICATION FLOW EXAMPLE



OAUTH 1.0A AND DELEGATED FORMS CUSTOMISATION

- oAuth 1.0a – in order to support seamless migration of applications (>20) using legacy protocol
- Most of the customizations is the same as for the OpenId 2.0
- Legacy applications also used Delegated Login Forms (DLF); the mechanism that also needed to be supported in order to have seamless migration
- DLF also enabled to keep the existing look and feel of all applications
- Specifics:
  - Keycloak REST interface extension for (legacy) session i user management
  - Introduction of request token and login token (for DLF)


Prijava
Korisničko ime
Lozinka
Simpa
MOJ
UPRAVLJAJTE
Prijaviti se može
ili
Telekom ID
Lozinka
Zapamti
Prijava
TELEKOM ID
LOZINKA
Zaboravili ste lozinku?
PRIJAVA
Telekom ID ili e-mail
Lozinka
Zapamti me
PRIJAVA
Zaboravili ste Telekom ID ili lozinku?
Registracija novih korisnika
Nadoplata bona
a u sustav
bon bez prijave
Moj Telekom Poslovni
Zaboravili ste Telekom ID?
Zaboravili ste lozinku?
Prijavite se
Registracija novih korisnika

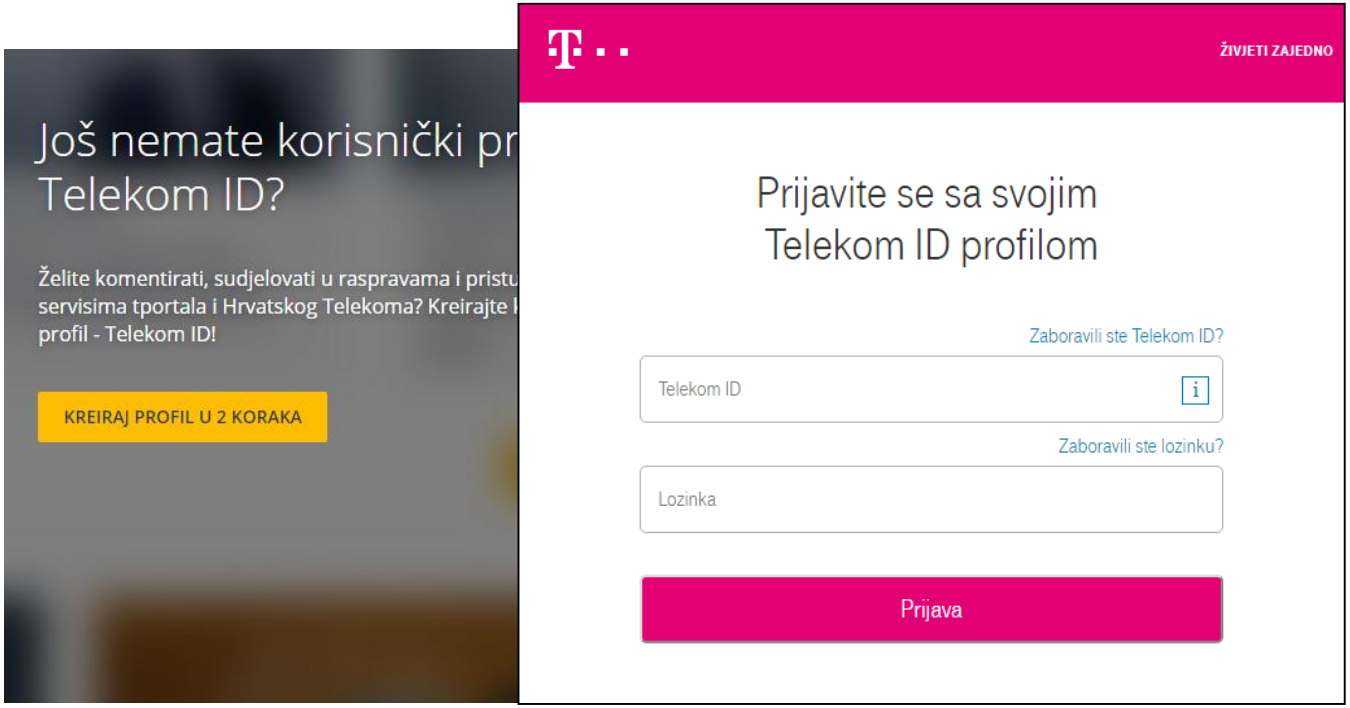
OPEN ID CONNECT AND PERSONALISED THEMES

- During the OpenId Connect session creation, Keycloak is aware of the client application the user is using to establish the session
- Extending *Login Forms Provider* and *Email Template Provider* we are able to easily implement personalisad themes for each client/application (login page, reset password page, email notifications, ...)

Client theme novi-tportal

Client theme nias

Client theme ott_mobile



TOP - *!?@#!!

- Infrastructure: Offline tokens loading problem after node restart (Infinispan)
- Infrastructure: Replication challenges in huge number of active sessions scenario

- Core: Extended Brute Force Protection
- Core: Data structure adjustments (old SSO -> Keycloak)
- Core: Required action adjustments to fit all four protocols, old custom delegated login forms and functional business demands

- OAuth 1.0a: promoting anonymous to non-anonymous session
-

THANK YOU FOR YOUR ATTENTION!

QUESTIONS?