OPENNTF WEBINARS

November, 2022

Integrate Keycloak with Domino for Identity Management

Heiko Voigt, sIT GmbH

AGENDA

- Welcome
- Presentation – Heiko Voigt
- Q and A

THANKS TO THE OPENNTF SPONSORS

- HCL made a contribution to help our organization
  - Funds these webinars!
  - Contests like Hackathons
  - Running the organization
- Prominic donates all IT related services
  - Cloud Hosting for OpenNTF
  - Infrastructure management for HCL Domino and Atlassian Servers
  - System Administration for day-to-day operation

THIS IS OUR COMMUNITY

- Join us and get involved!
- We are all volunteers
- No effort is too small
- If your idea is bigger than you can do on your own, we can connect you to a team to work on it
- Test or help or modify an existing project
- Write guides or documentation
- Add reviews on projects / stars on Snippets

DECEMBER HAPPY HOUR

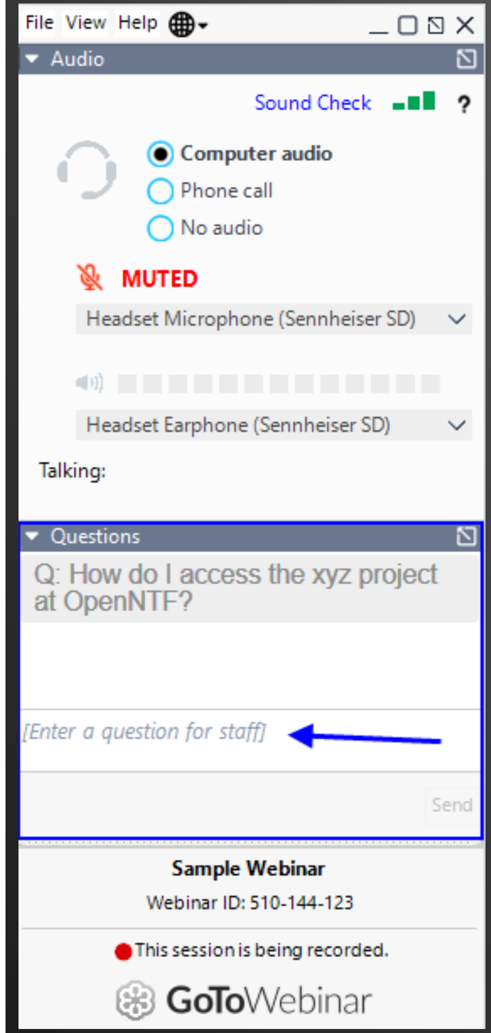
- Join us in December for a virtual Happy Hour!
  - Thursday 15th
  - APAC, Europe, North America
- Watch the web site for details

REPAIR CAFE

- Open chat room to bring your questions / problems / ideas
- Share your tips
- What topics do you want?
    - Use the Discord #suggestion-box

- January 12 – Development Topics
- January 25 – Admin Topics

ASKING QUESTIONS



● Computer audio
○ Phone call
○ No audio

MUTED

Headset Microphone (Sennheiser SD)

Headset Earphone (Sennheiser SD)

Q: How do I access the xyz project at OpenNTF?

[Enter a question for staff]

Sample Webinar
Webinar ID: 510-144-123

This session is being recorded.

GoToWebinar

- First Question – Will this be recorded?
  - Yes, view on YouTube!!!
  - https://www.youtube.com/user/OpenNTF
- Use the Questions Pane in GoToWebinar
- We will get to your questions at the end of the webinar
- The speakers will respond to your questions verbally
  - (not in the Questions pane)
- Please keep all questions related to the topics that our speakers are discussing!!!
- Unrelated Question => post at:
  - https://openntf.org/discord

PRESENTATION

Integrate Keycloak with Domino for identity management

Heiko Voigt

ABOUT HEIKO

- CEO of SIT GmbH in Germany and
  Harbour Light Software Development Ltd. in Canada
- Software Architect for 25+ years with N/D, Full-Stack Web Developer
- HCL Ambassador 2019-2022, IBM Champion 2019
- Core Team Member at C3UG and Board Member at OpenNTF
- Proud father of twins
- Sailor, Home brewer

HCL Ambassador

C3UG

Harbour Light Software Development Ltd.

SIT GmbH

https://www.harbour-light.com

https://www.sit.de

AGENDA

Few things to clear out:

OAUTH2 *!= Authentication*, only **Authorization**

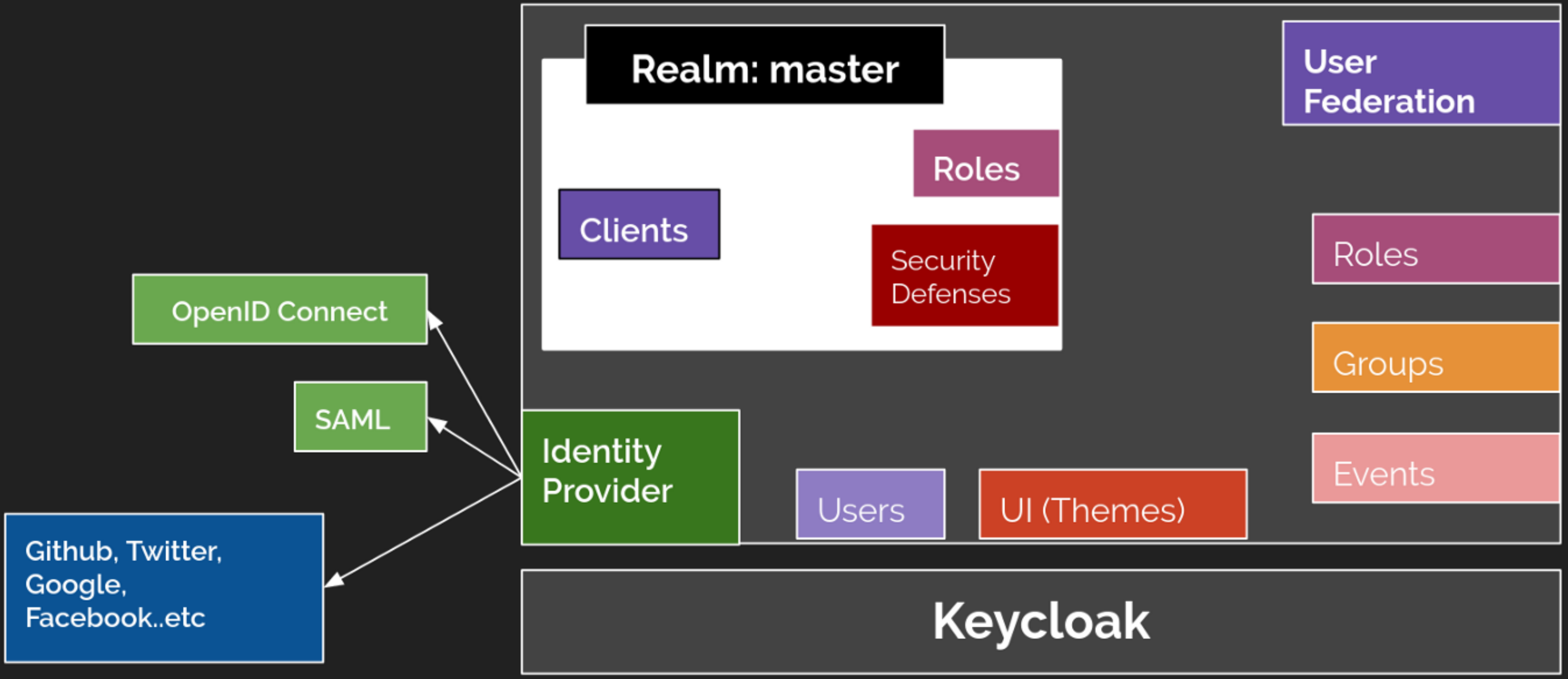
OpenID Connect = Identity + Authentication + Authorization

What we will cover:

- Keycloak and SAML/Web with Domino (Web + Notes SSO for DS <12.0.2 EA5)
- Keycloak and OIDC/OAUTH2 with AppDevPack and Domino REST APIs
- Keycloak and OIDC/OAUTH2 with Domino >= 12.0.2 EA3
- Keycloak and VERSE / Nomad Web /XPAges

WHAT IS KEYCLOAK?

Core Concepts



WHY IS KEYCLOAK A GREAT MATCH FOR DOMINO SHOPS?

- **Reliable Solution**
  “Red Hat running on Red Hat products (**Red Hat SSO**)”: the entire authentication/authorization system is based on Red Hat SSO, which is the downstream version of upstream product keycloak. It is designed following the standard security protocols to provide a dynamic single sign-on solution to small/large scale industry.

- **Open Source (3C’s) : Cost, Customizable / Contributions, Community**

  Apache License Version 2.0 with support of strong active open source community

- **Is it ready for production?**

  Yes, it can be used in production (Make sure to read documentation guide)

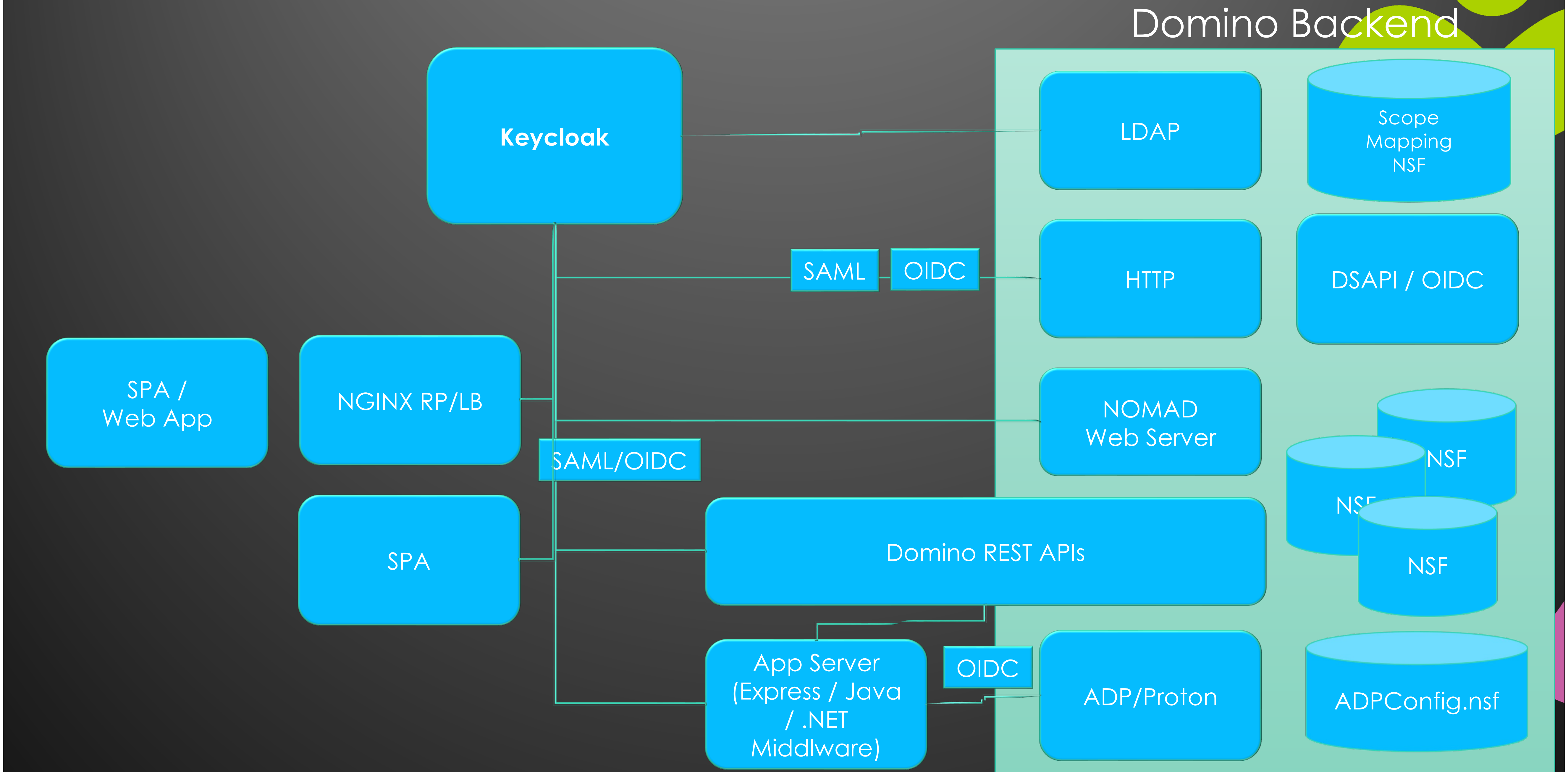
- **Standard Protocols (supported by keycloak)**

  - OpenID Connect
  - OAuth 2.0
  - SAML 2.0

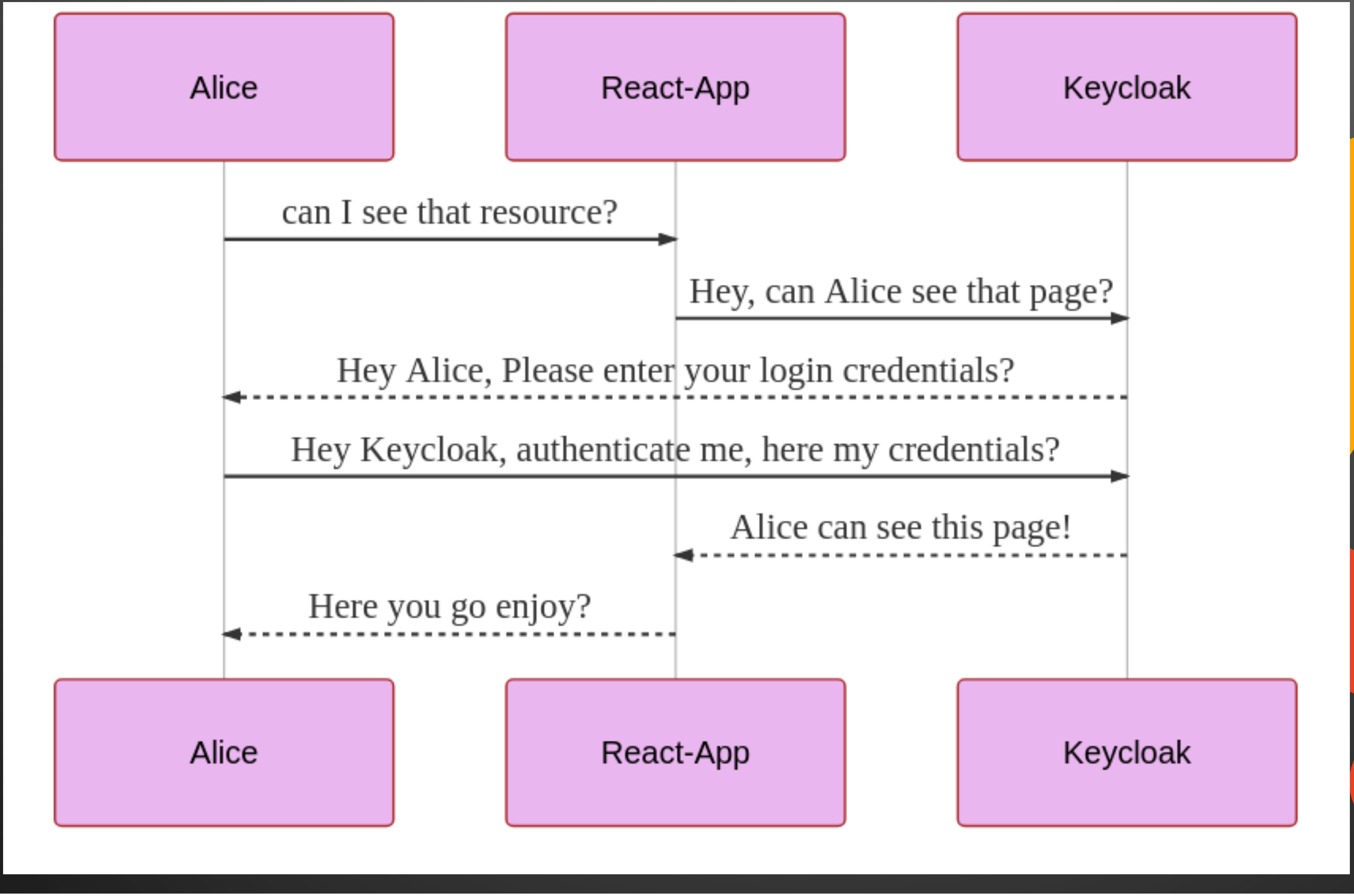
- **Applications/Tools** that support integration with the above protocols can be plugged with Keycloak.

  E.g. MFA components, FIDO2 plugins, HW-Token Handling and much much more.

OUR BASE ARCHITECTURE CHART…



DOMINO REST API/ADP OAUTH2/OIDC FLOW

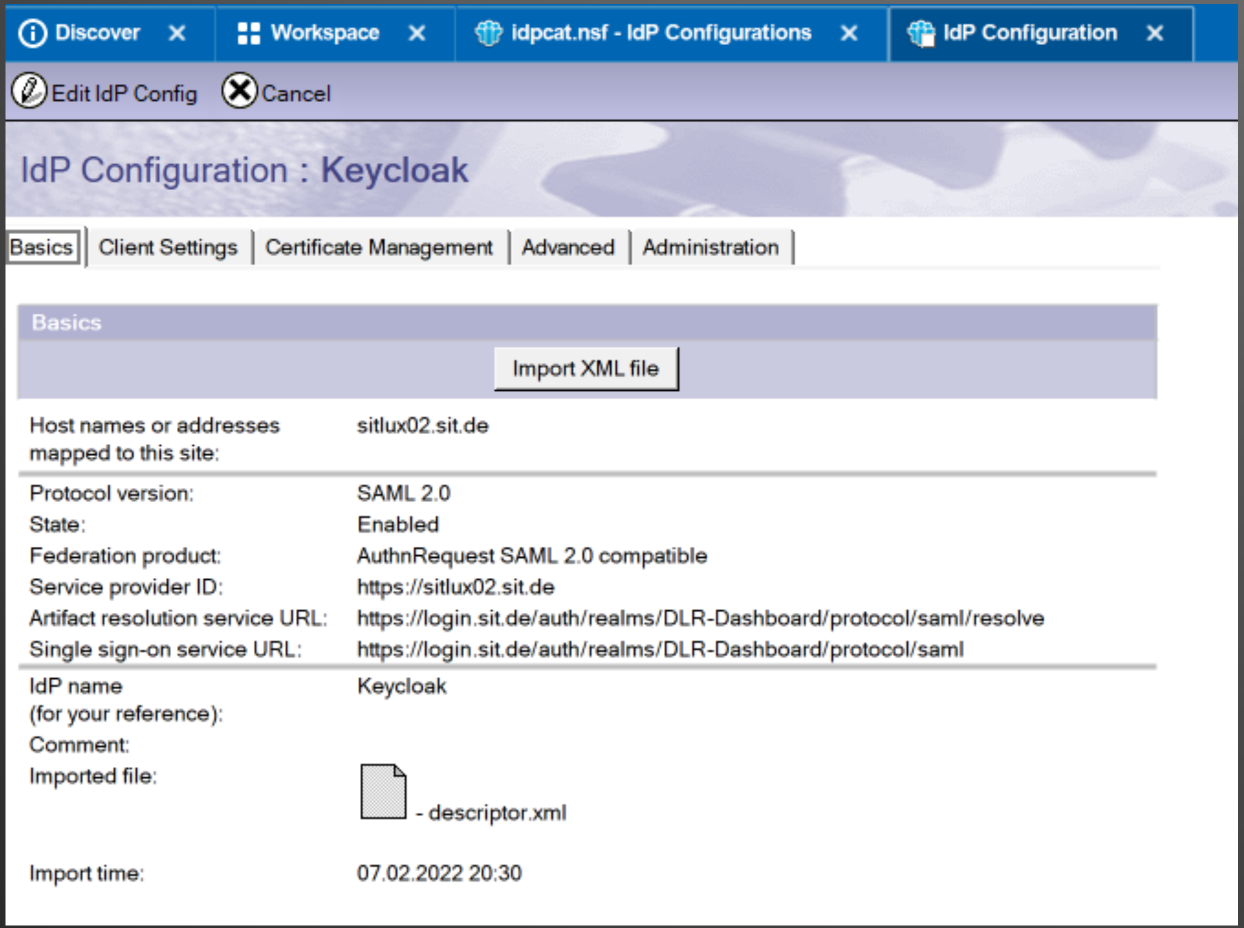


Alice
React-App
Keycloak
can I see that resource?
Hey, can Alice see that page?
Hey Alice, Please enter your login credentials?
Hey Keycloak, authenticate me, here my credentials?
Alice can see this page!
Here you go enjoy?
Alice
React-App
Keycloak

NOTES/DOMINO SAML CONFIGURATION

- Create and configure IDP Catalog (idpcat.nsf)
- Create trust configuration
- Configure Domino HTTP Settings
- Setup User Security Policy
- If needed: configure ID Vault for federated Login (Notes Client)
- Test!

1) DOMINO WEB ACCESS SAML CONFIG – IDPCAT.NSF

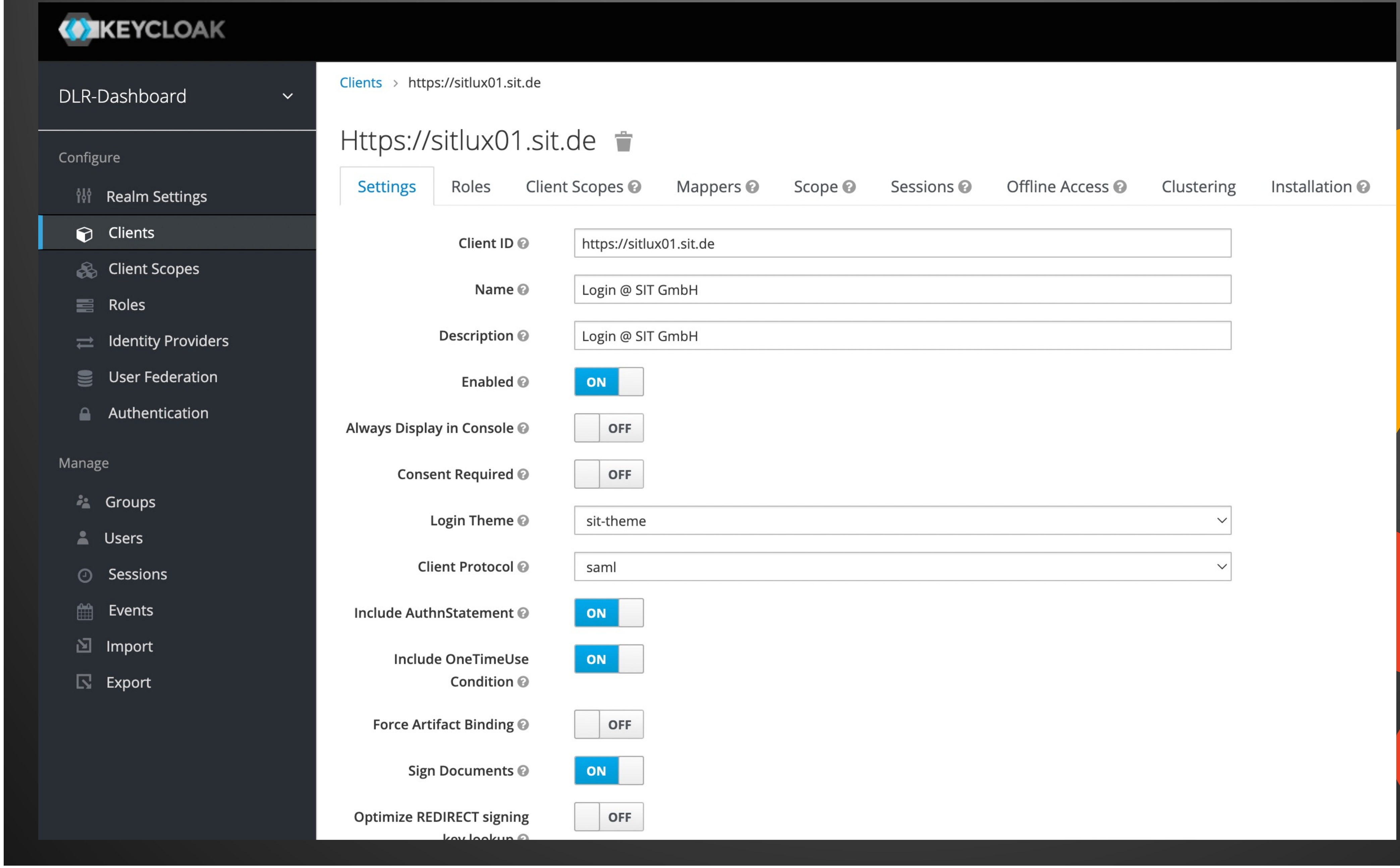


IdP Configuration : Keycloak

Basics

Host names or addresses mapped to this site:	sitlux02.sit.de
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://sitlux02.sit.de
Artifact resolution service URL:	https://login.sit.de/auth/realms/DLR-Dashboard/protocol/saml/resolve
Single sign-on service URL:	https://login.sit.de/auth/realms/DLR-Dashboard/protocol/saml
IdP name (for your reference):	Keycloak
Comment:	
Imported file:	- descriptor.xml
Import time:	07.02.2022 20:30

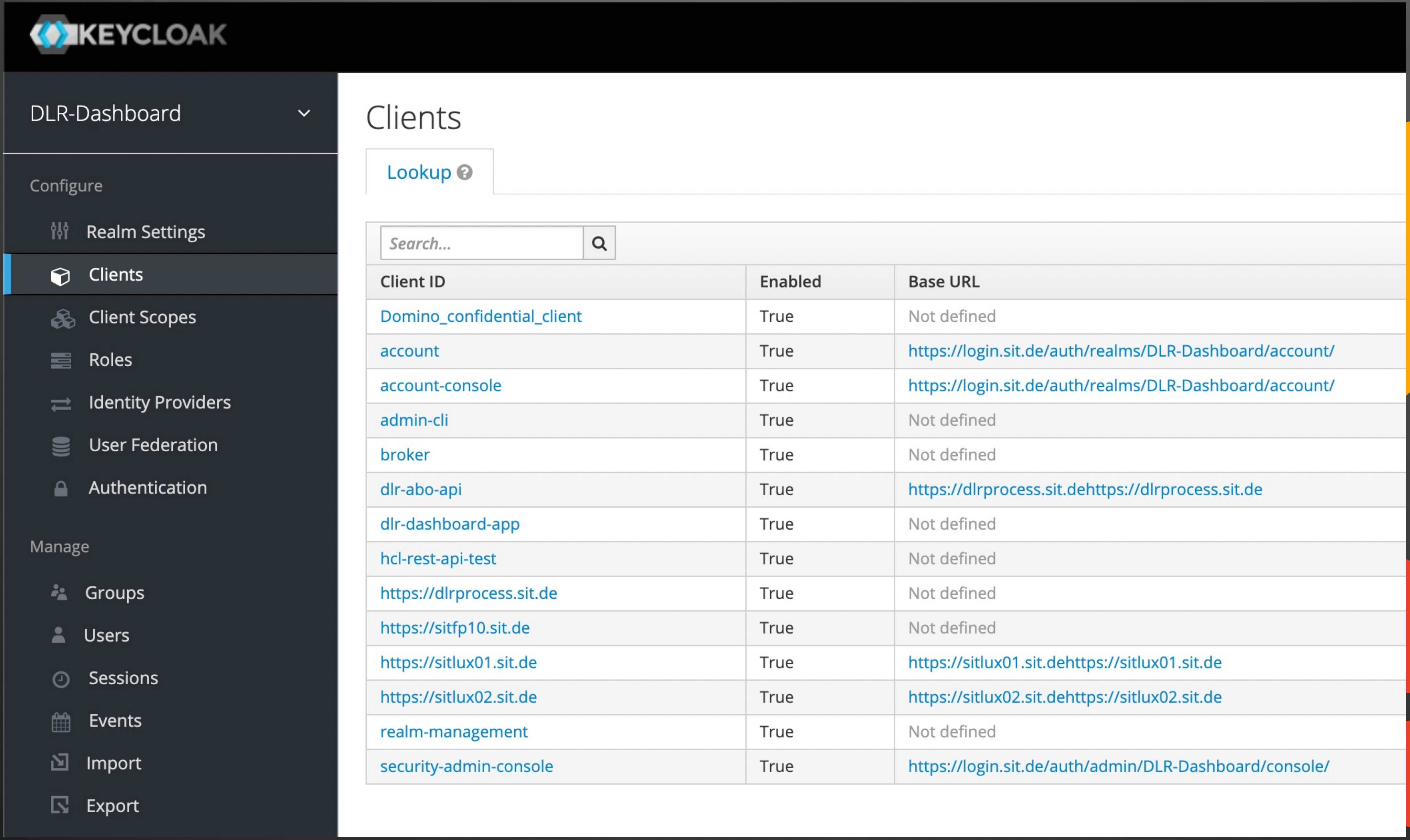
1) DOMINO WEB ACCESS SAML CONFIGURATION



Https://sitlux01.sit.de

Client ID	https://sitlux01.sit.de
Name	Login @ SIT GmbH
Description	Login @ SIT GmbH
Enabled	ON
Always Display in Console	OFF
Consent Required	OFF
Login Theme	sit-theme
Client Protocol	saml
Include AuthnStatement	ON
Include OneTimeUse Condition	ON
Force Artifact Binding	OFF
Sign Documents	ON
Optimize REDIRECT signing key lookup	OFF

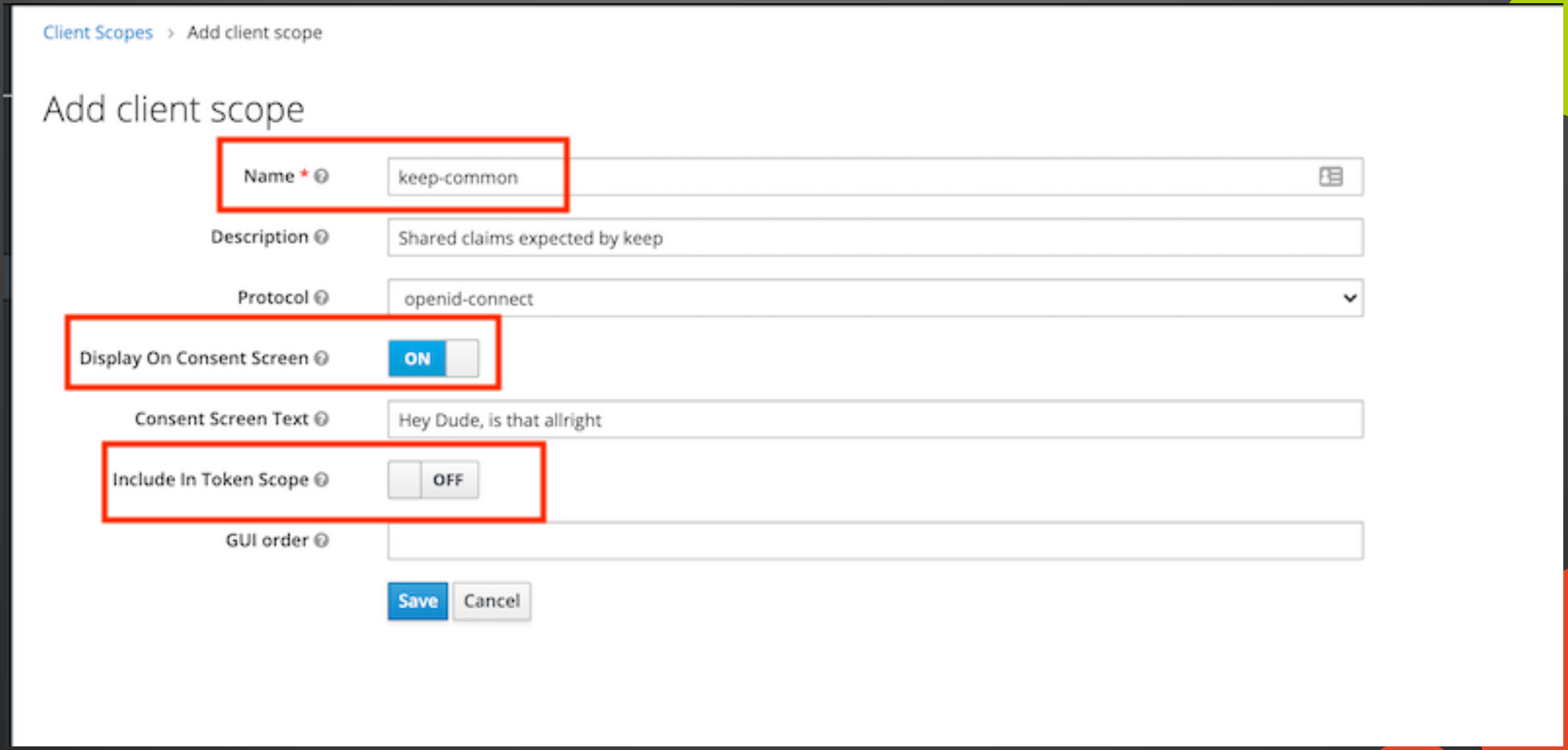
2) DOMINO REST API KEYCLOAK CONFIG



Clients

Client ID	Enabled	Base URL
Domino_confidential_client	True	Not defined
account	True	https://login.sit.de/auth/realms/DLR-Dashboard/account/
account-console	True	https://login.sit.de/auth/realms/DLR-Dashboard/account/
admin-cli	True	Not defined
broker	True	Not defined
dlr-abo-api	True	https://dlrprocess.sit.dehttps://dlrprocess.sit.de
dlr-dashboard-app	True	Not defined
hcl-rest-api-test	True	Not defined
https://dlrprocess.sit.de	True	Not defined
https://sitfp10.sit.de	True	Not defined
https://sitlux01.sit.de	True	https://sitlux01.sit.dehttps://sitlux01.sit.de
https://sitlux02.sit.de	True	https://sitlux02.sit.dehttps://sitlux02.sit.de
realm-management	True	Not defined
security-admin-console	True	https://login.sit.de/auth/admin/DLR-Dashboard/console/

2) DOMINO REST API KEYCLOAK CONFIG

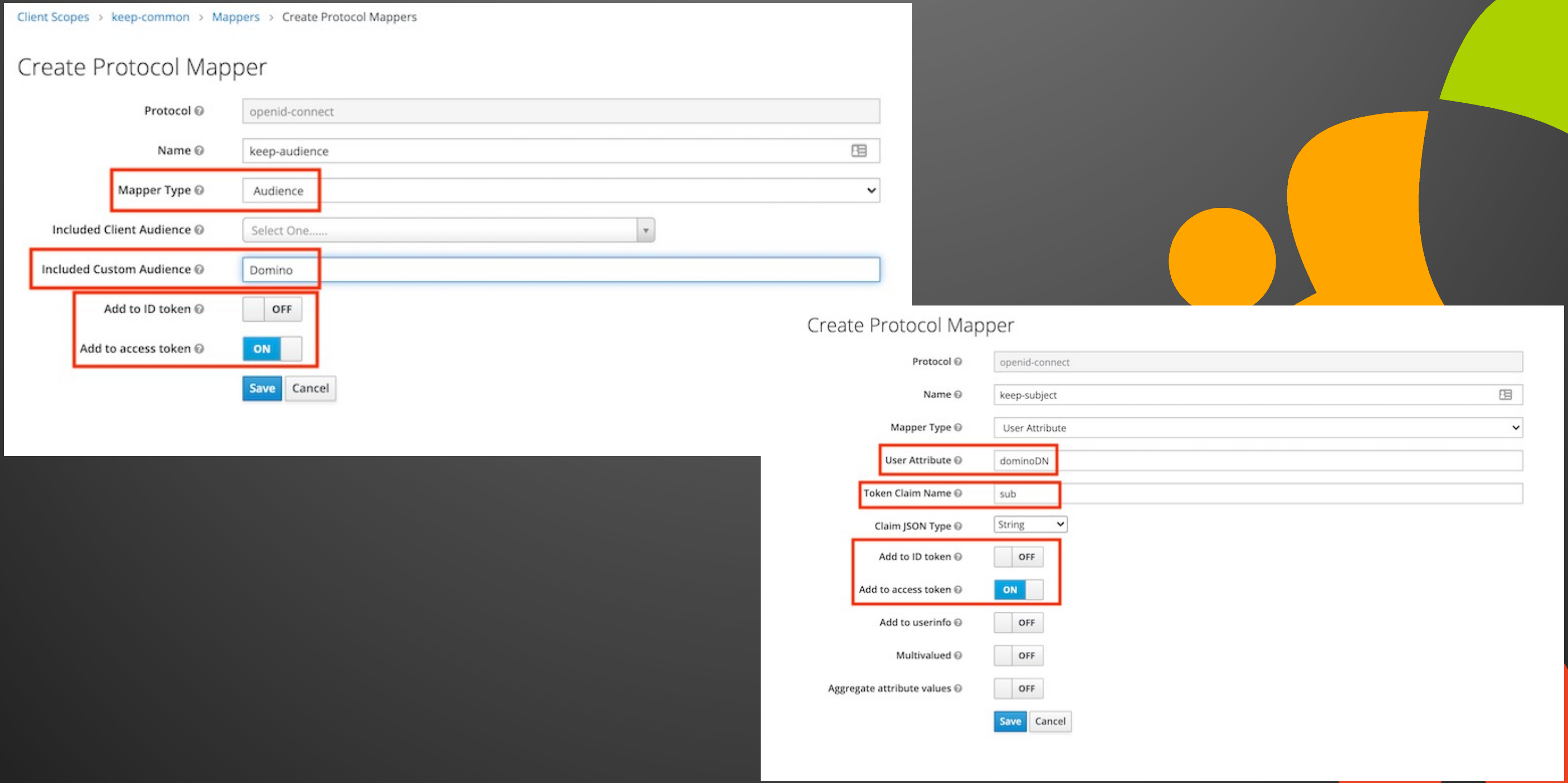


Client Scopes › Add client scope

Add client scope

Name *	keep-common
Description	Shared claims expected by keep
Protocol	openid-connect
Display On Consent Screen	ON
Consent Screen Text	Hey Dude, is that allright
Include In Token Scope	OFF
GUI order	

2) DOMINO REST API KEYCLOAK CONFIG



Client Scopes > keep-common > Mappers > Create Protocol Mappers

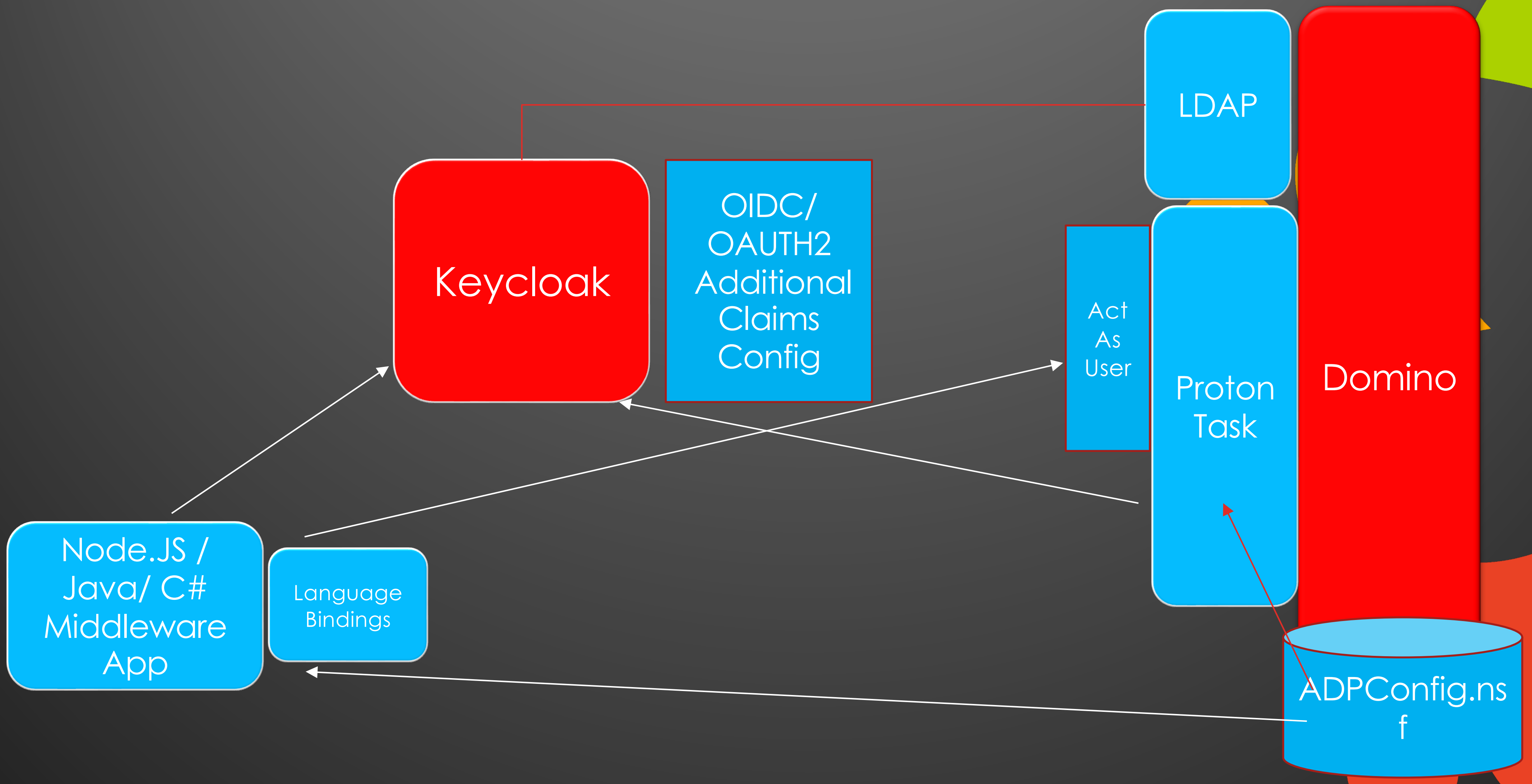
Create Protocol Mapper

Protocol	openid-connect
Name	keep-audience
Mapper Type	Audience
Included Client Audience	Select One......
Included Custom Audience	Domino
Add to ID token	OFF
Add to access token	ON

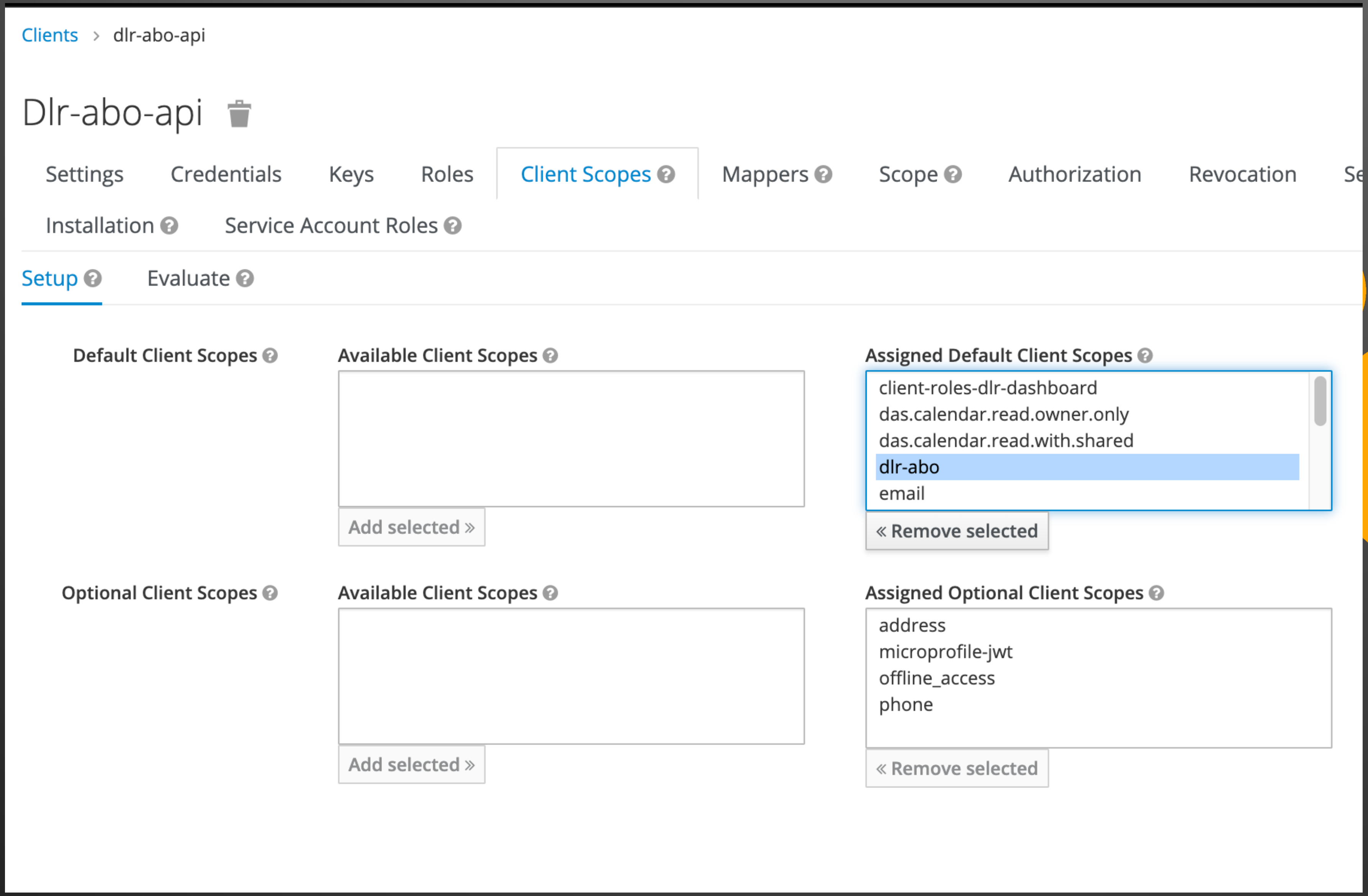
Create Protocol Mapper

Protocol	openid-connect
Name	keep-subject
Mapper Type	User Attribute
User Attribute	dominoDN
Token Claim Name	sub
Claim JSON Type	String
Add to ID token	OFF
Add to access token	ON
Add to userinfo	OFF
Multivalued	OFF
Aggregate attribute values	OFF

3) APPDEVPACK IAM REPLACEMENT


LDAP
Keycloak
OIDC/ OAUTH2 Additional Claims Config
Act As User
Proton Task
Domino
Node.JS / Java/ C# Middleware App
Language Bindings
ADPConfig.nsf

3)APPDEVPACK IAM REPLACEMENT - KEYCLOAK



Default Client Scopes

Available Client Scopes

Assigned Default Client Scopes

- client-roles-dlr-dashboard
- das.calendar.read.owner.only
- das.calendar.read.with.shared
- dlr-abo
- email

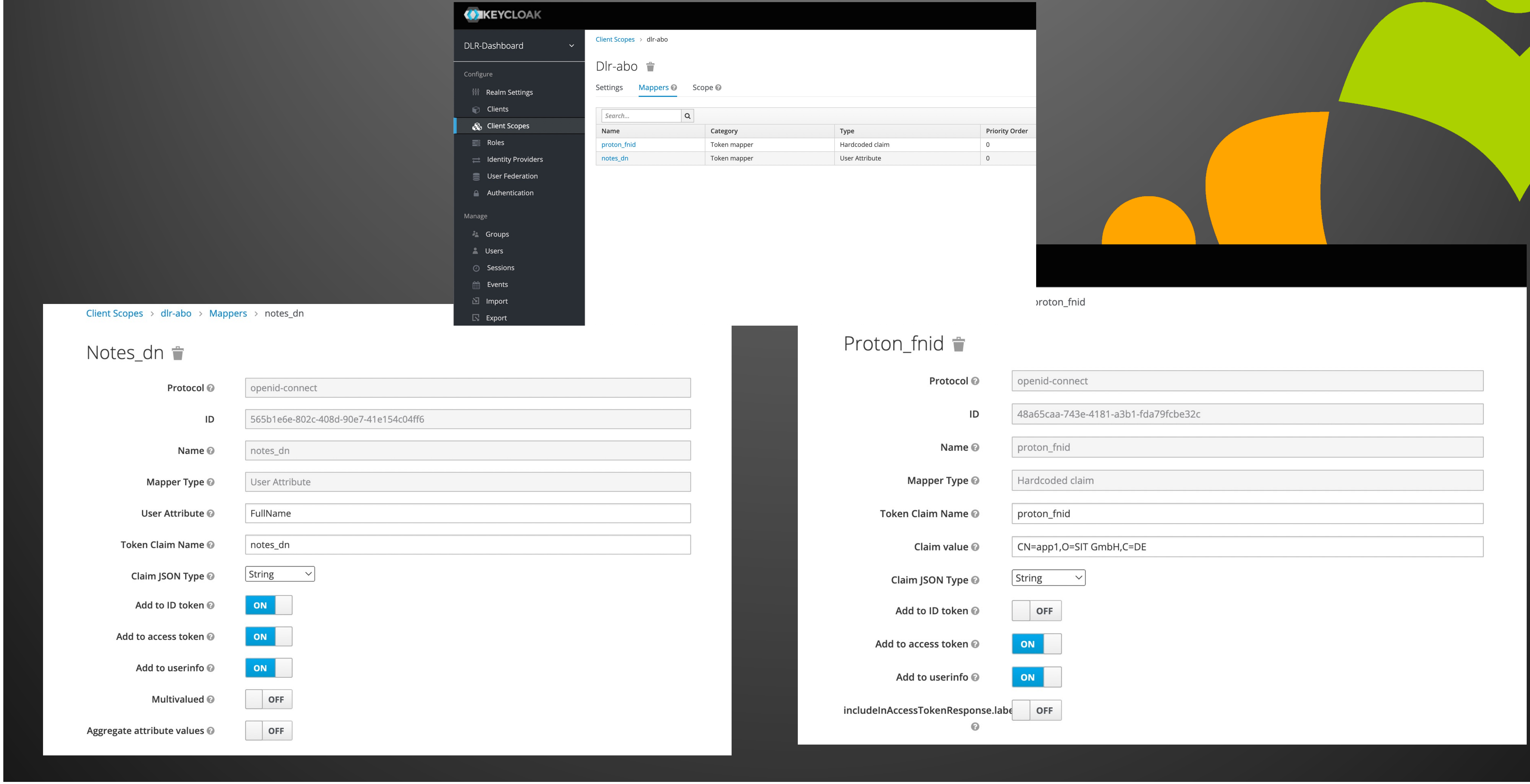
Optional Client Scopes

Available Client Scopes

Assigned Optional Client Scopes

- address
- microprofile-jwt
- offline_access
- phone

3)APPDEVPACK IAM REPLACEMENT - SCOPES



Client Scopes › dlr-abo

Dlr-abo

Name	Category	Type	Priority Order
proton_fnid	Token mapper	Hardcoded claim	0
notes_dn	Token mapper	User Attribute	0

Client Scopes › dlr-abo › Mappers › notes_dn

Notes_dn

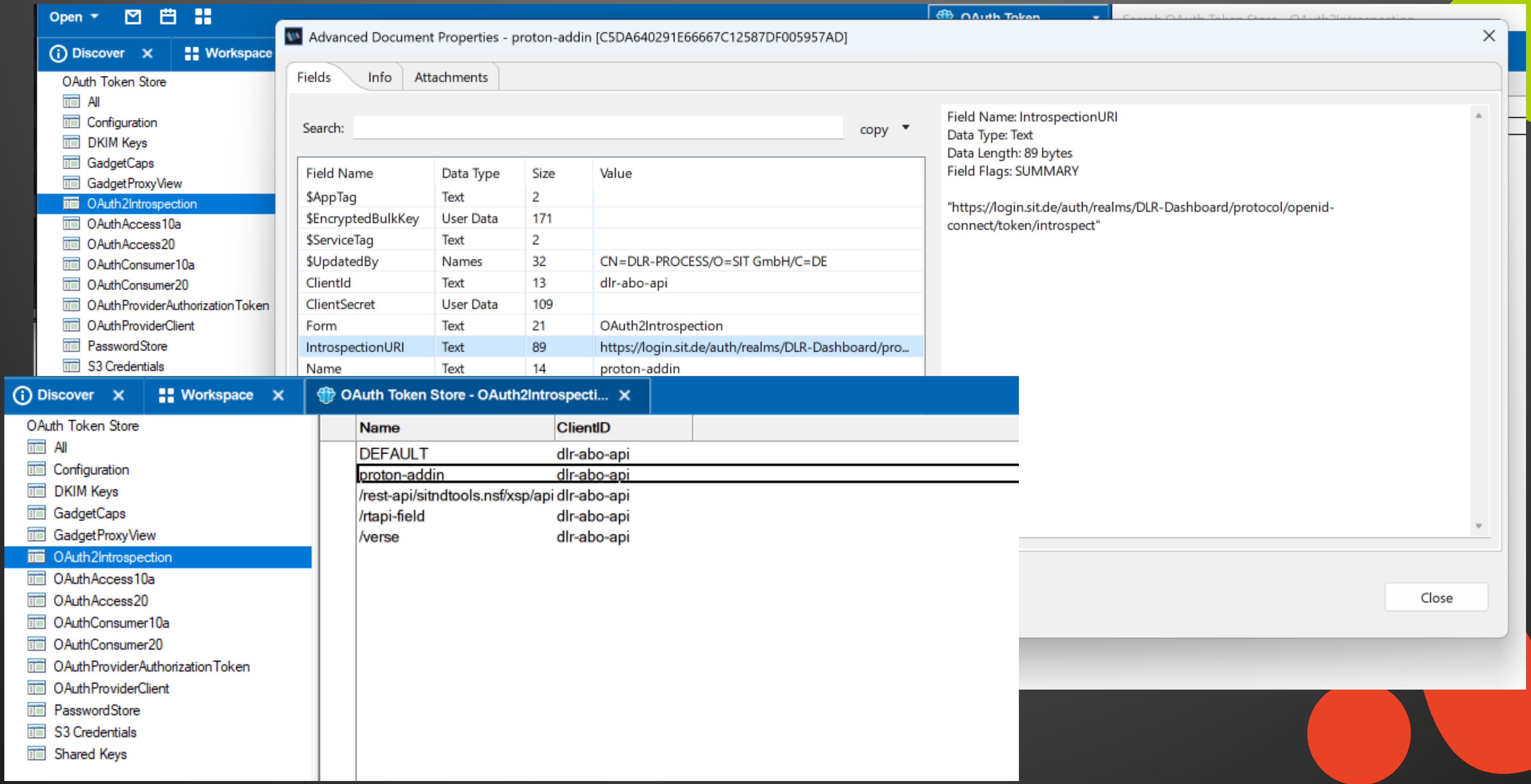
Protocol	openid-connect
ID	565b1e6e-802c-408d-90e7-41e154c04ff6
Name	notes_dn
Mapper Type	User Attribute
User Attribute	FullName
Token Claim Name	notes_dn
Claim JSON Type	String
Add to ID token	ON
Add to access token	ON
Add to userinfo	ON
Multivalued	OFF
Aggregate attribute values	OFF

roton_fnid

Proton_fnid

Protocol	openid-connect
ID	48a65caa-743e-4181-a3b1-fda79fcbe32c
Name	proton_fnid
Mapper Type	Hardcoded claim
Token Claim Name	proton_fnid
Claim value	CN=app1,O=SIT GmbH,C=DE
Claim JSON Type	String
Add to ID token	OFF
Add to access token	ON
Add to userinfo	ON
includeInAccessTokenResponse.labe	OFF

3)APPDEVPACK IAM REPLACEMENT - INTROSPECTION



Advanced Document Properties - proton-addin [C5DA640291E66667C12587DF005957AD]

OAuth Token Store
- All
- Configuration
- DKIM Keys
- GadgetCaps
- GadgetProxyView
- OAuth2Introspection
- OAuthAccess10a
- OAuthAccess20
- OAuthConsumer10a
- OAuthConsumer20
- OAuthProviderAuthorizationToken
- OAuthProviderClient
- PasswordStore
- S3 Credentials
- Shared Keys

Search:

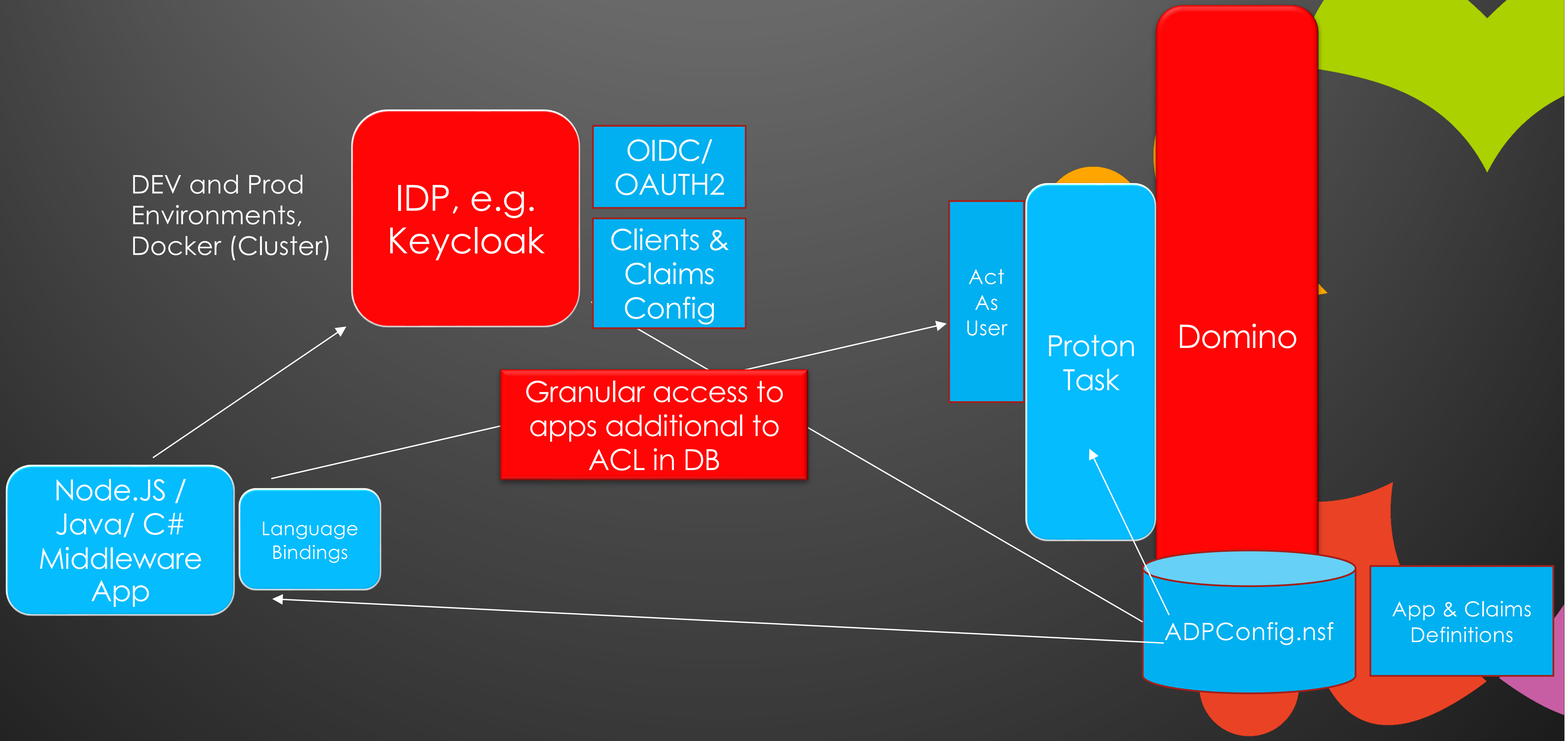
Field Name	Data Type	Size	Value
$AppTag	Text	2	
$EncryptedBulkKey	User Data	171	
$ServiceTag	Text	2	
$UpdatedBy	Names	32	CN=DLR-PROCESS/O=SIT GmbH/C=DE
ClientId	Text	13	dlr-abo-api
ClientSecret	User Data	109	
Form	Text	21	OAuth2Introspection
IntrospectionURI	Text	89	https://login.sit.de/auth/realms/DLR-Dashboard/pro...
Name	Text	14	proton-addin

Field Name: IntrospectionURI
Data Type: Text
Data Length: 89 bytes
Field Flags: SUMMARY

"https://login.sit.de/auth/realms/DLR-Dashboard/protocol/openid-connect/token/introspect"

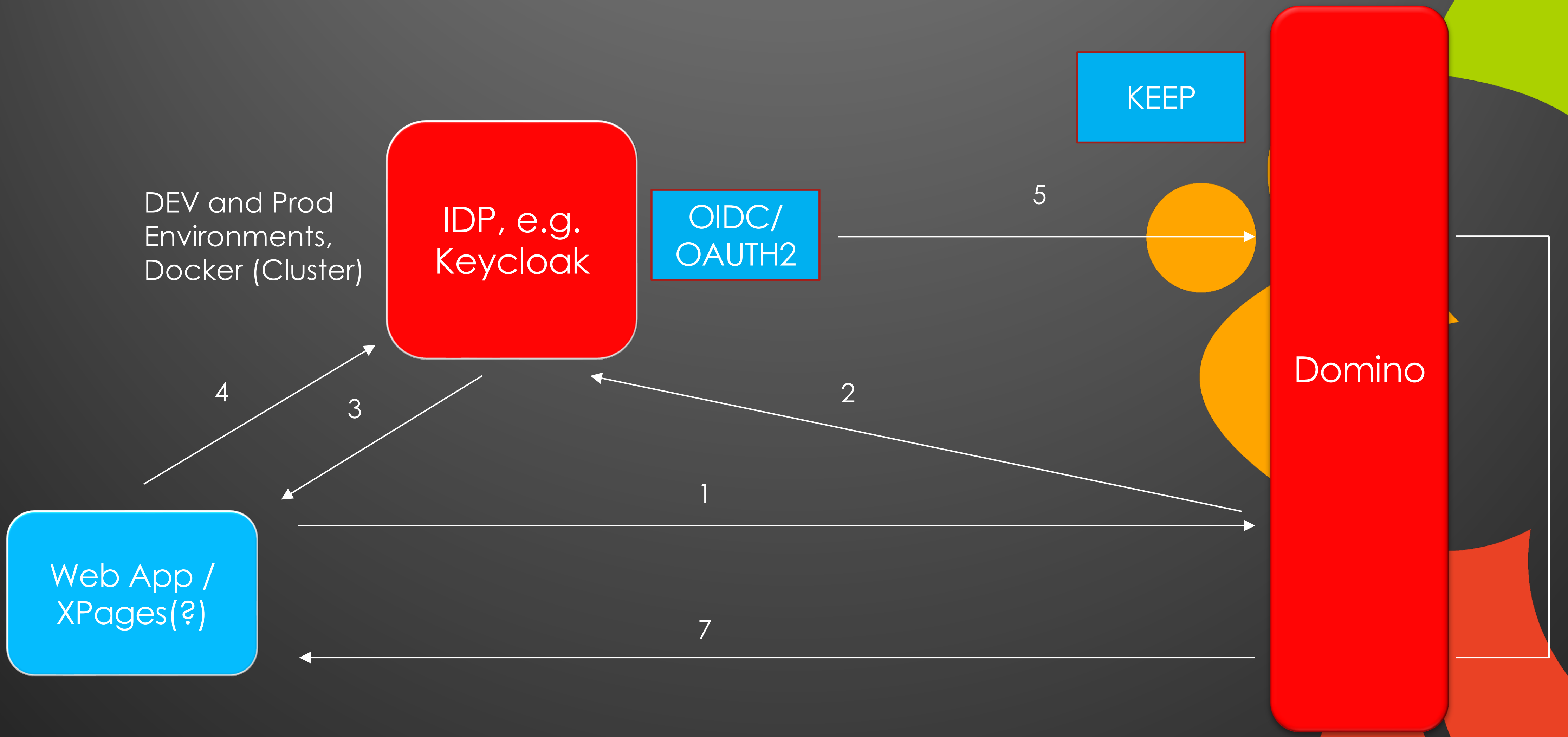
Name	ClientID
DEFAULT	dlr-abo-api
proton-addin	dlr-abo-api
/rest-api/sitndtools.nsf/xsp/api	dlr-abo-api
/rtapi-field	dlr-abo-api
/verse	dlr-abo-api

4) APPDEVPACK DSAPI FILTER – OIDC/OAUTH



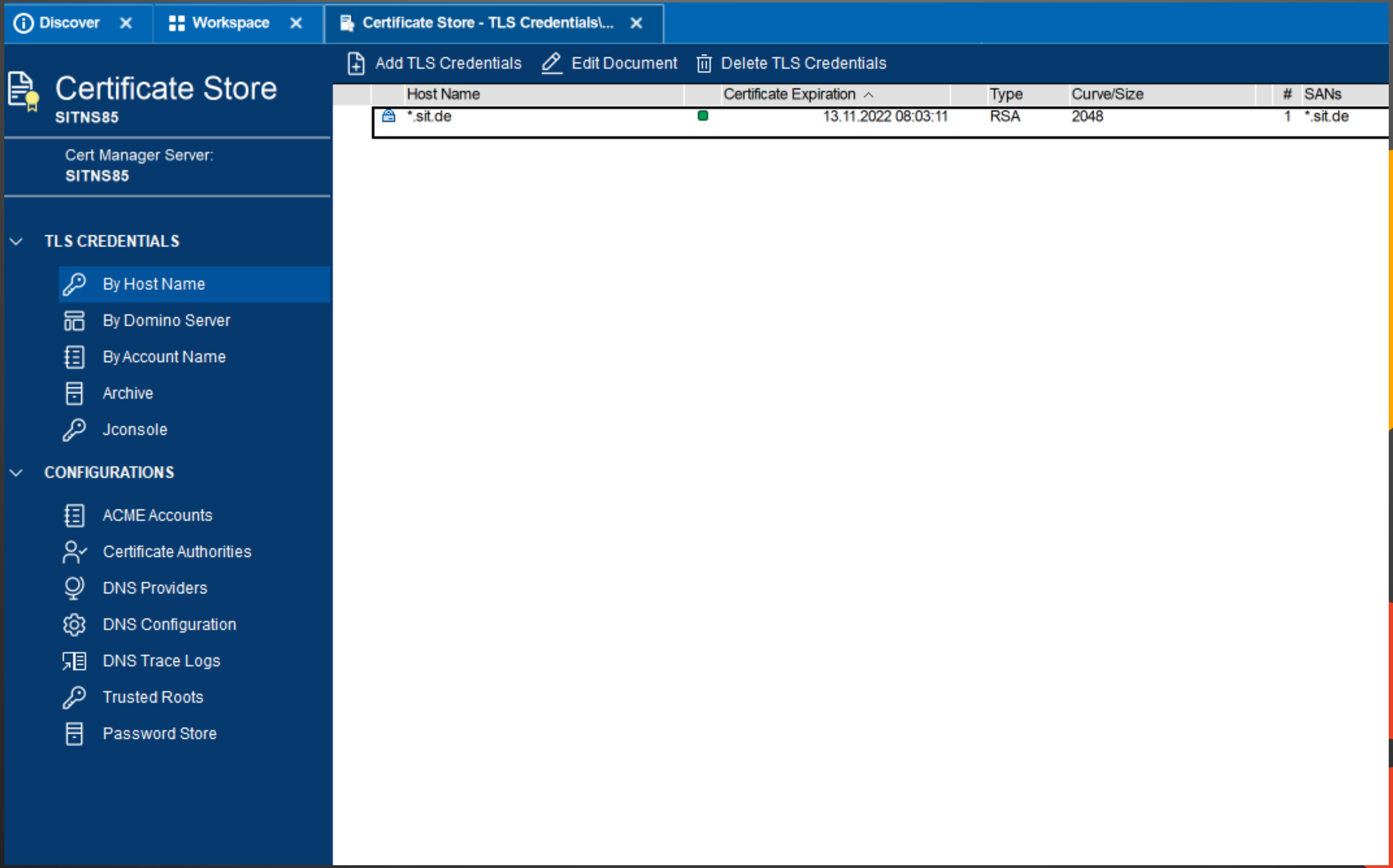
DEV and Prod Environments, Docker (Cluster)

5) DOMINO 12.0.2 – "DANUBE" & OAUTH/OIDC



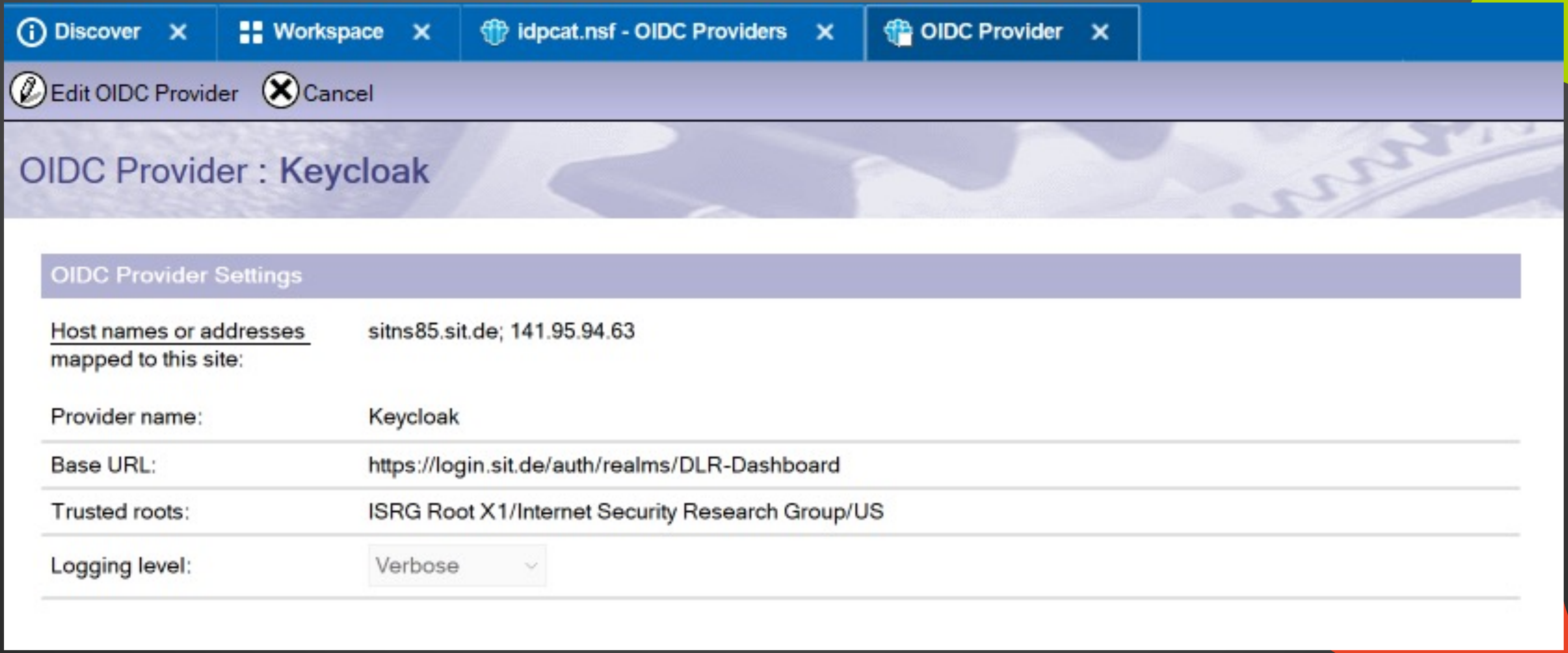
DEV and Prod Environments, Docker (Cluster)

5) DOMINO 12.0.2 – "DANUBE" TLS IN CERTMGR



Host Name		Certificate Expiration	Type	Curve/Size	#	SANs
*.sit.de	🟩	13.11.2022 08:03:11	RSA	2048	1	*.sit.de

5) DOMINO 12.0.2 – "DANUBE" OIDC PROVIDER CONFIG

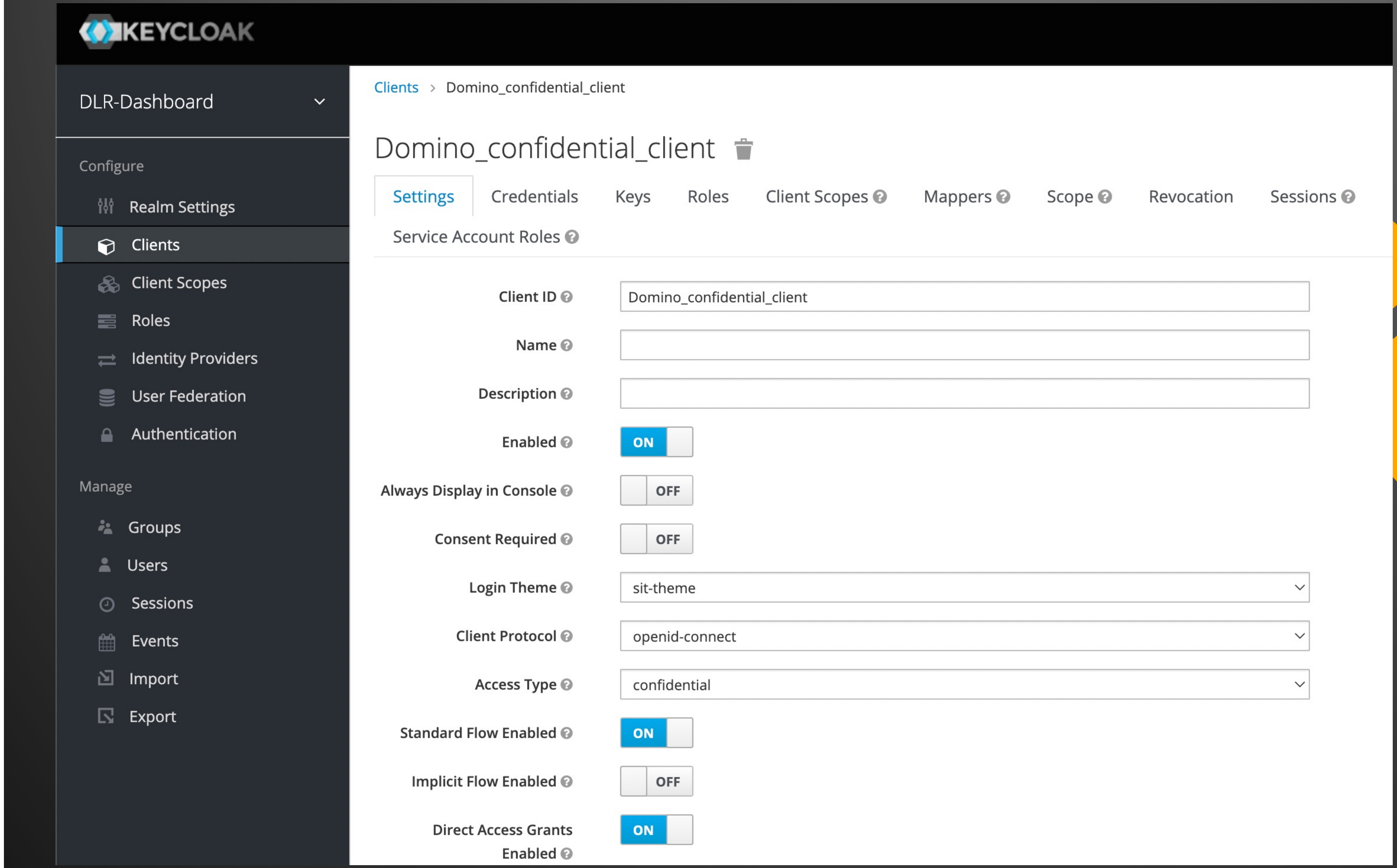


OIDC Provider : Keycloak

OIDC Provider Settings

Host names or addresses mapped to this site:	sitns85.sit.de; 141.95.94.63
Provider name:	Keycloak
Base URL:	https://login.sit.de/auth/realms/DLR-Dashboard
Trusted roots:	ISRG Root X1/Internet Security Research Group/US
Logging level:	Verbose

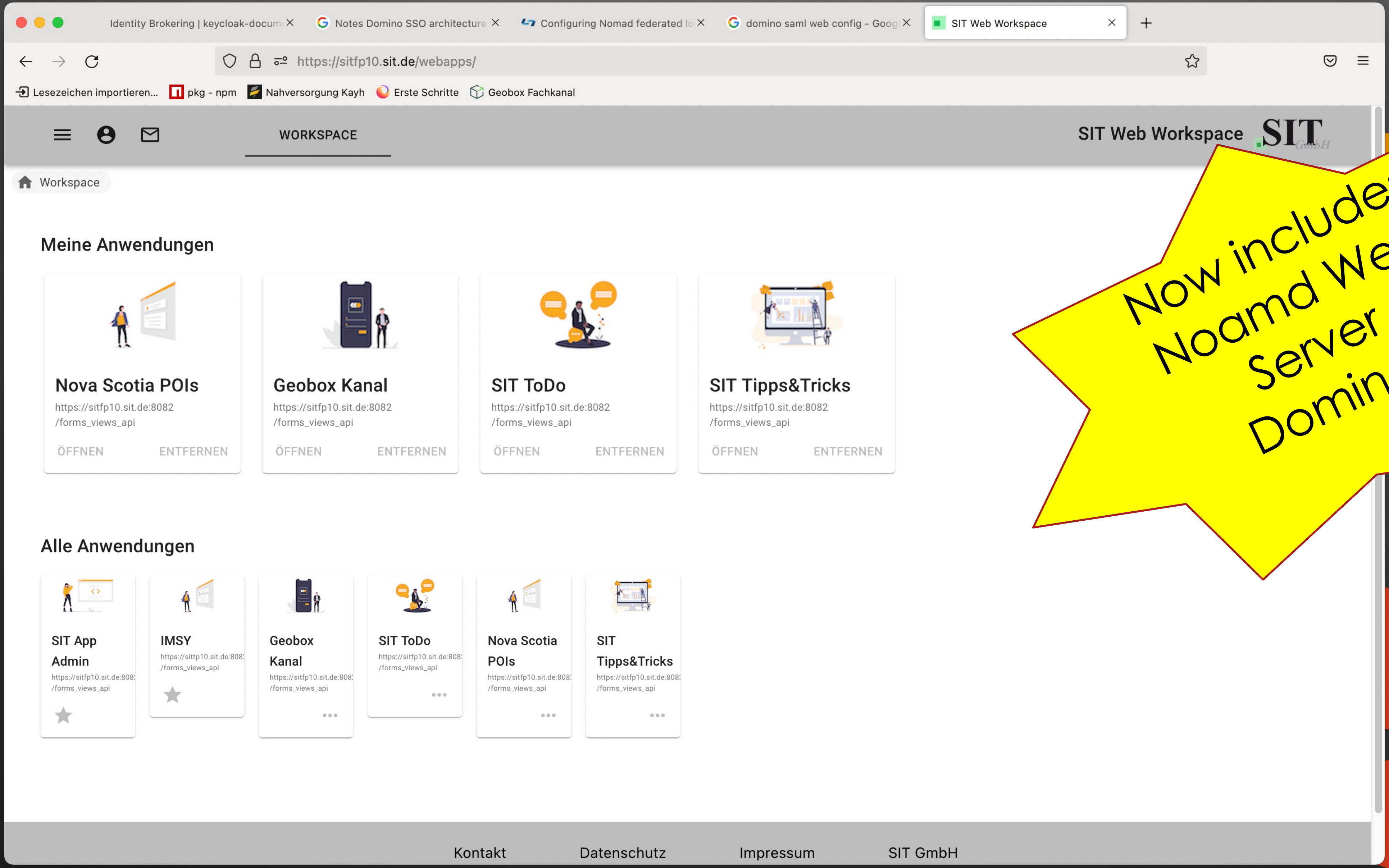
DOMINO 12.0.2 “DANUBE” KEYCLOAK CONFIG



Domino_confidential_client

Client ID	Domino_confidential_client
Name	
Description	
Enabled	ON
Always Display in Console	OFF
Consent Required	OFF
Login Theme	sit-theme
Client Protocol	openid-connect
Access Type	confidential
Standard Flow Enabled	ON
Implicit Flow Enabled	OFF
Direct Access Grants Enabled	ON

DEMO – REST APIS, XPAGES, OIDC/SAML, SPA



Identity Brokering | keycloak-docum
Notes Domino SSO architecture
Configuring Nomad federated lo
domino saml web config - Goog
SIT Web Workspace

https://sitfp10.sit.de/webapps/

Lesezeichen importieren... pkg - npm Nahversorgung Kayh Erste Schritte Geobox Fachkanal

WORKSPACE

SIT Web Workspace SIT GmbH

Workspace

Meine Anwendungen

Anwendung	URL		
Nova Scotia POIs	https://sitfp10.sit.de:8082 /forms_views_api	ÖFFNEN	ENTFERNEN
Geobox Kanal	https://sitfp10.sit.de:8082 /forms_views_api	ÖFFNEN	ENTFERNEN
SIT ToDo	https://sitfp10.sit.de:8082 /forms_views_api	ÖFFNEN	ENTFERNEN
SIT Tipps&Tricks	https://sitfp10.sit.de:8082 /forms_views_api	ÖFFNEN	ENTFERNEN

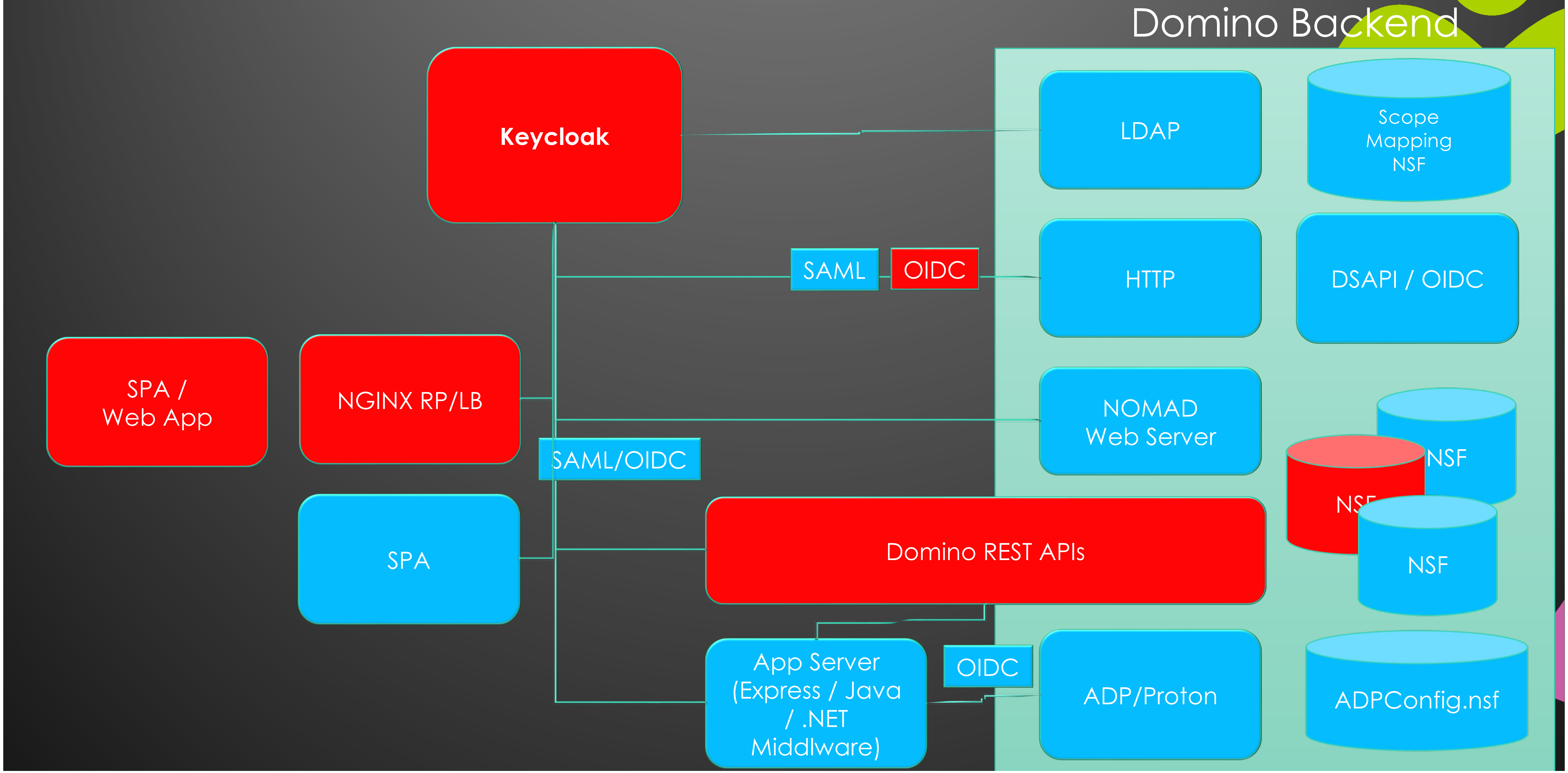
Alle Anwendungen

Anwendung	URL
SIT App Admin	https://sitfp10.sit.de:808 /forms_views_api
IMSY	https://sitfp10.sit.de:808 /forms_views_api
Geobox Kanal	https://sitfp10.sit.de:808 /forms_views_api
SIT ToDo	https://sitfp10.sit.de:808 /forms_views_api
Nova Scotia POIs	https://sitfp10.sit.de:808 /forms_views_api
SIT Tipps&Tricks	https://sitfp10.sit.de:808 /forms_views_api

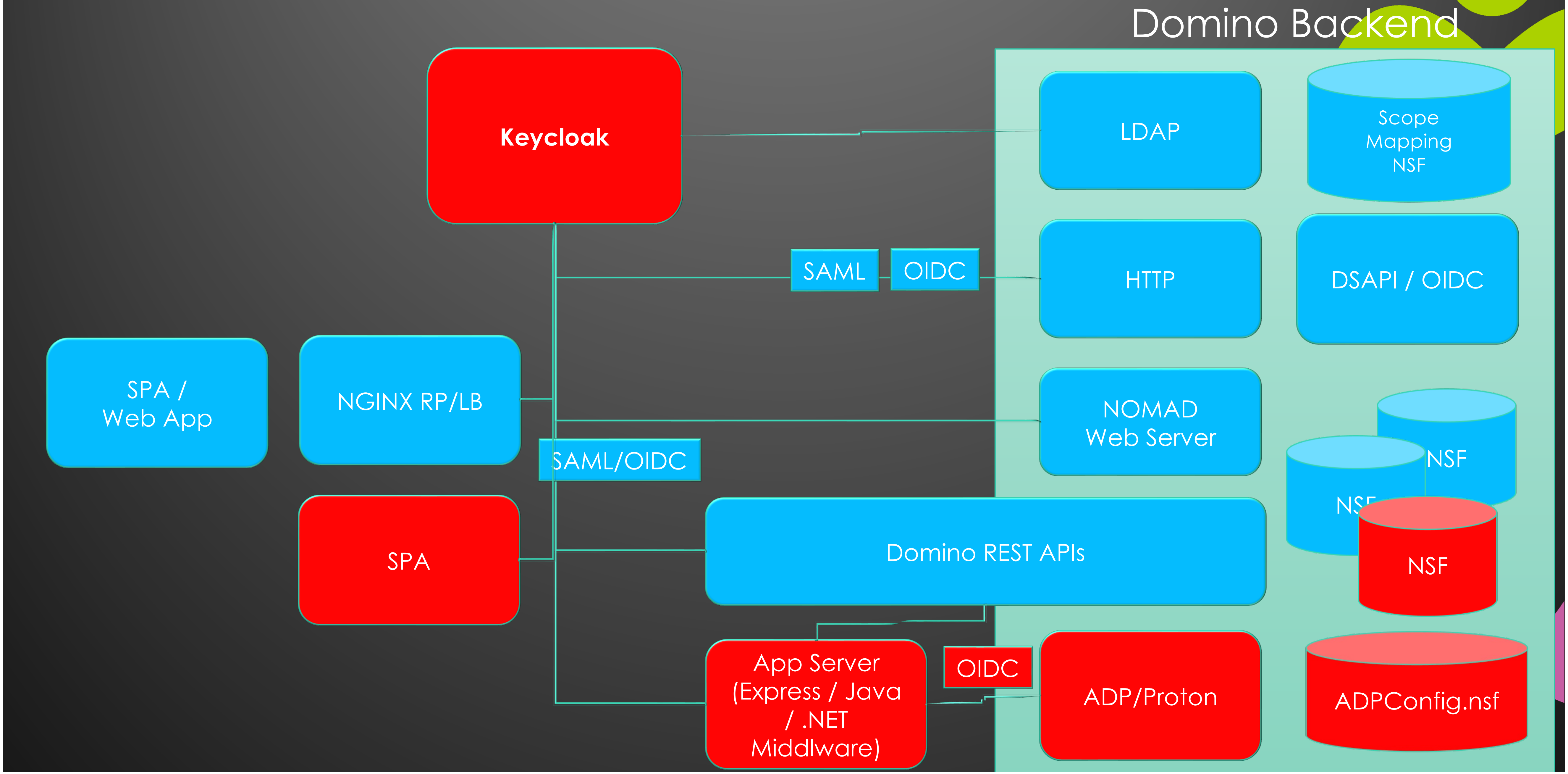
Kontakt Datenschutz Impressum SIT GmbH

Now includes Noamd Web Server Domino!

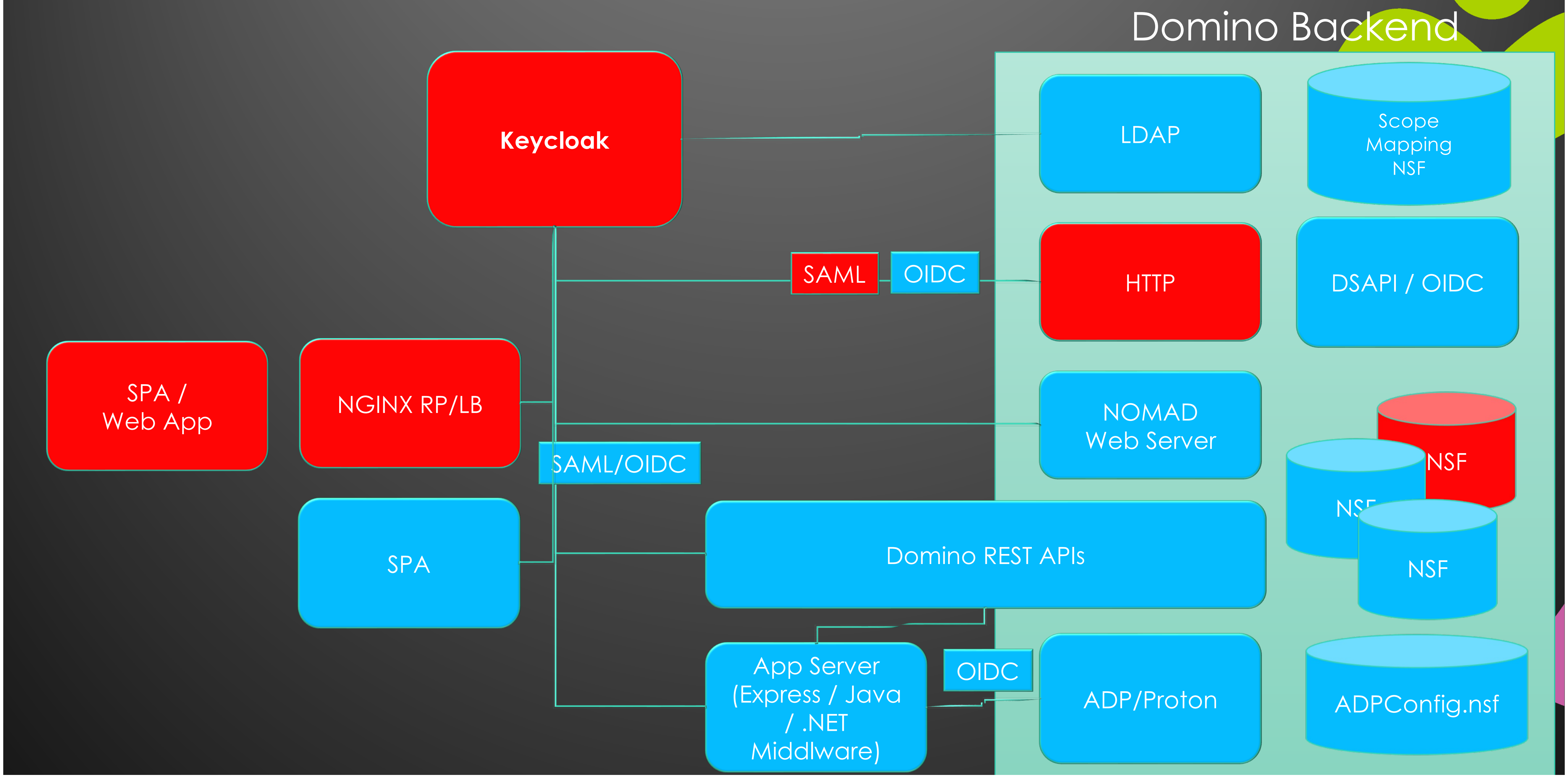
1ST APP…


Domino Backend
Keycloak
LDAP
Scope Mapping NSF
SAML
OIDC
HTTP
DSAPI / OIDC
SPA / Web App
NGINX RP/LB
NOMAD Web Server
SAML/OIDC
NSF
NSF
NSF
SPA
Domino REST APIs
App Server (Express / Java / .NET Middlware)
OIDC
ADP/Proton
ADPConfig.nsf

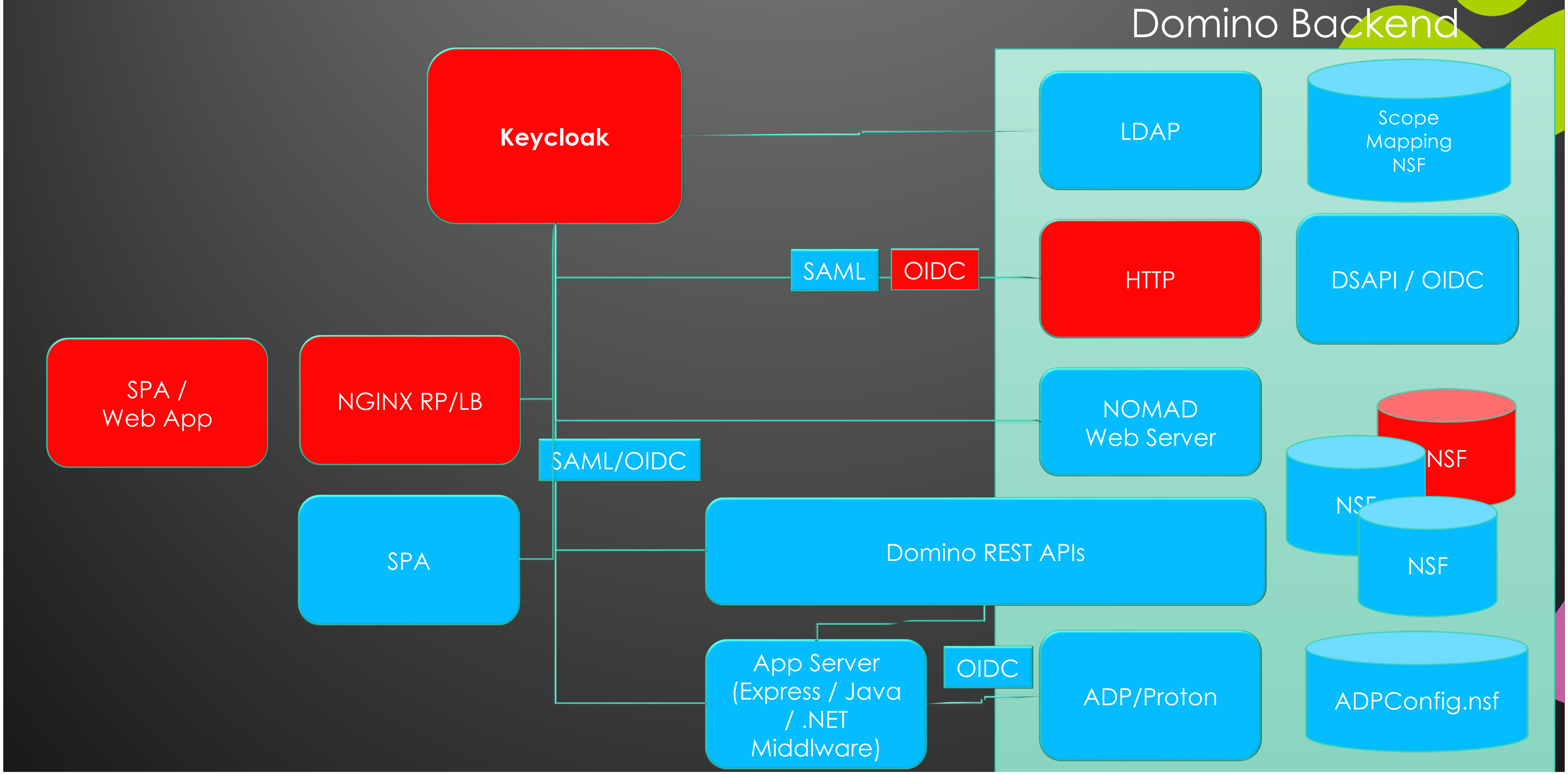
2ND APP…


Domino Backend
Keycloak
LDAP
Scope Mapping NSF
SAML
OIDC
HTTP
DSAPI / OIDC
SPA / Web App
NGINX RP/LB
NOMAD Web Server
SAML/OIDC
NSF
NSF
NSF
SPA
Domino REST APIs
App Server (Express / Java / .NET Middlware)
OIDC
ADP/Proton
ADPConfig.nsf

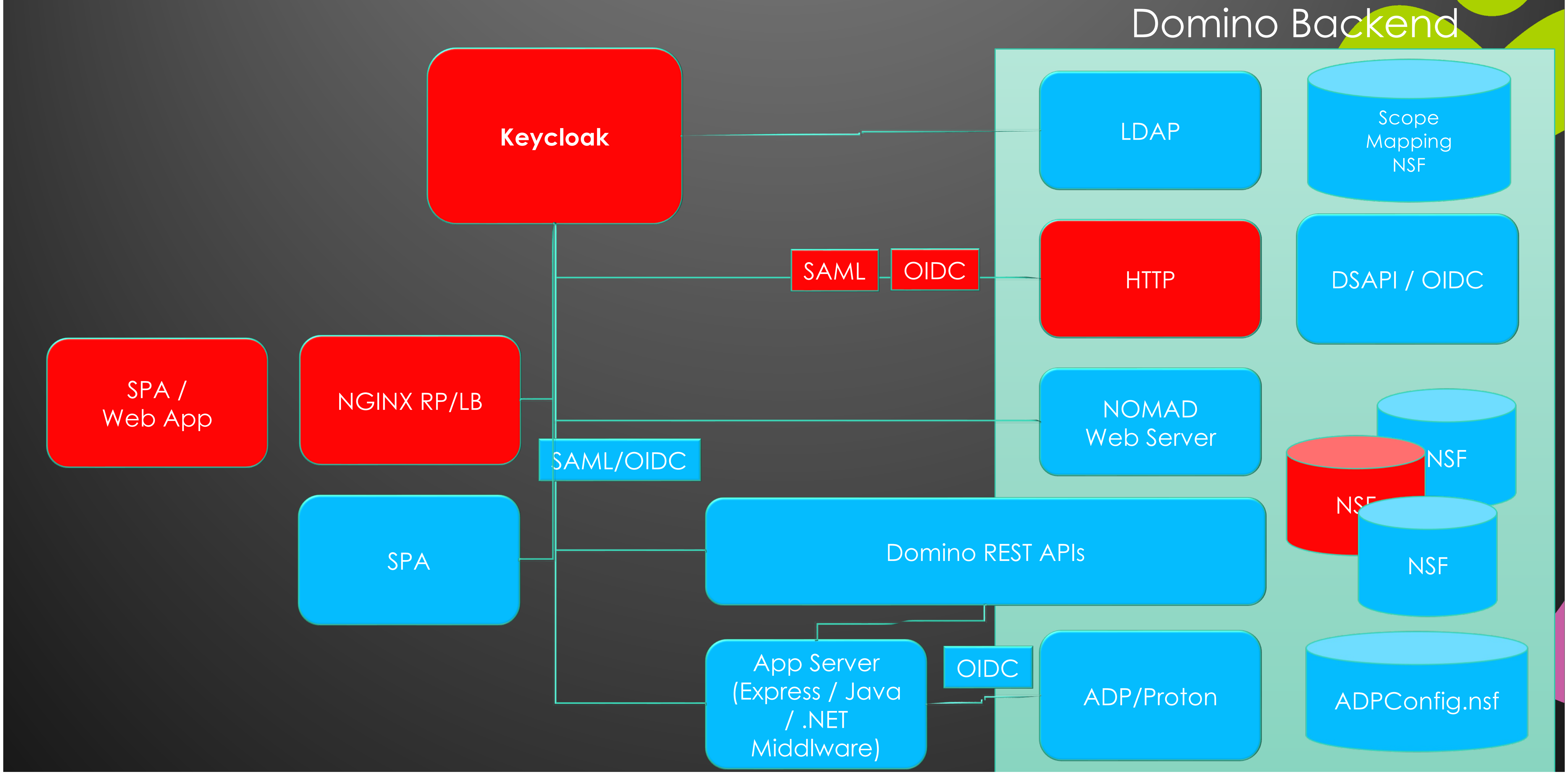
3RD APP… VERSE



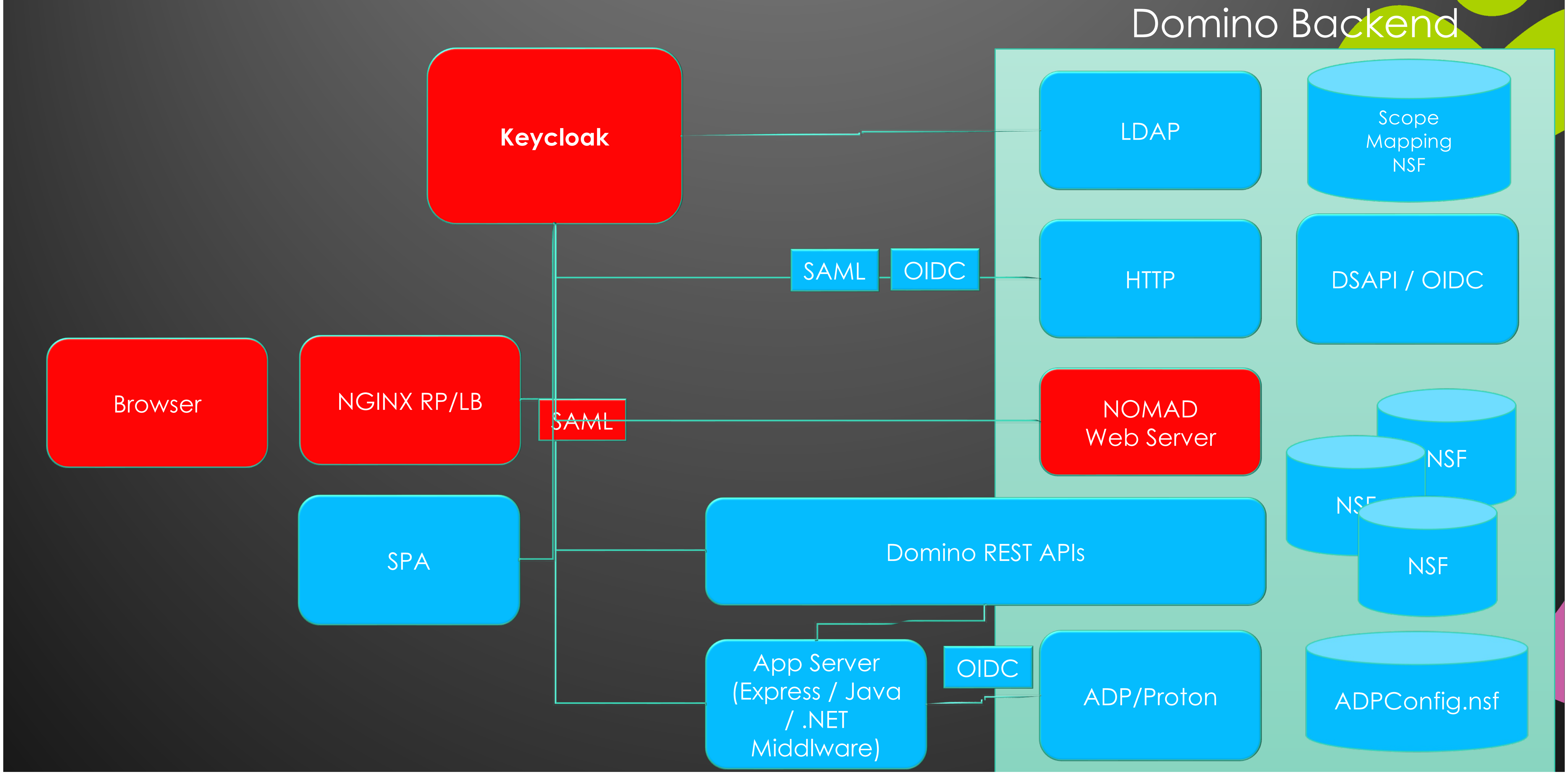
4TH APP – DOMINO 12.0.2 OIDC



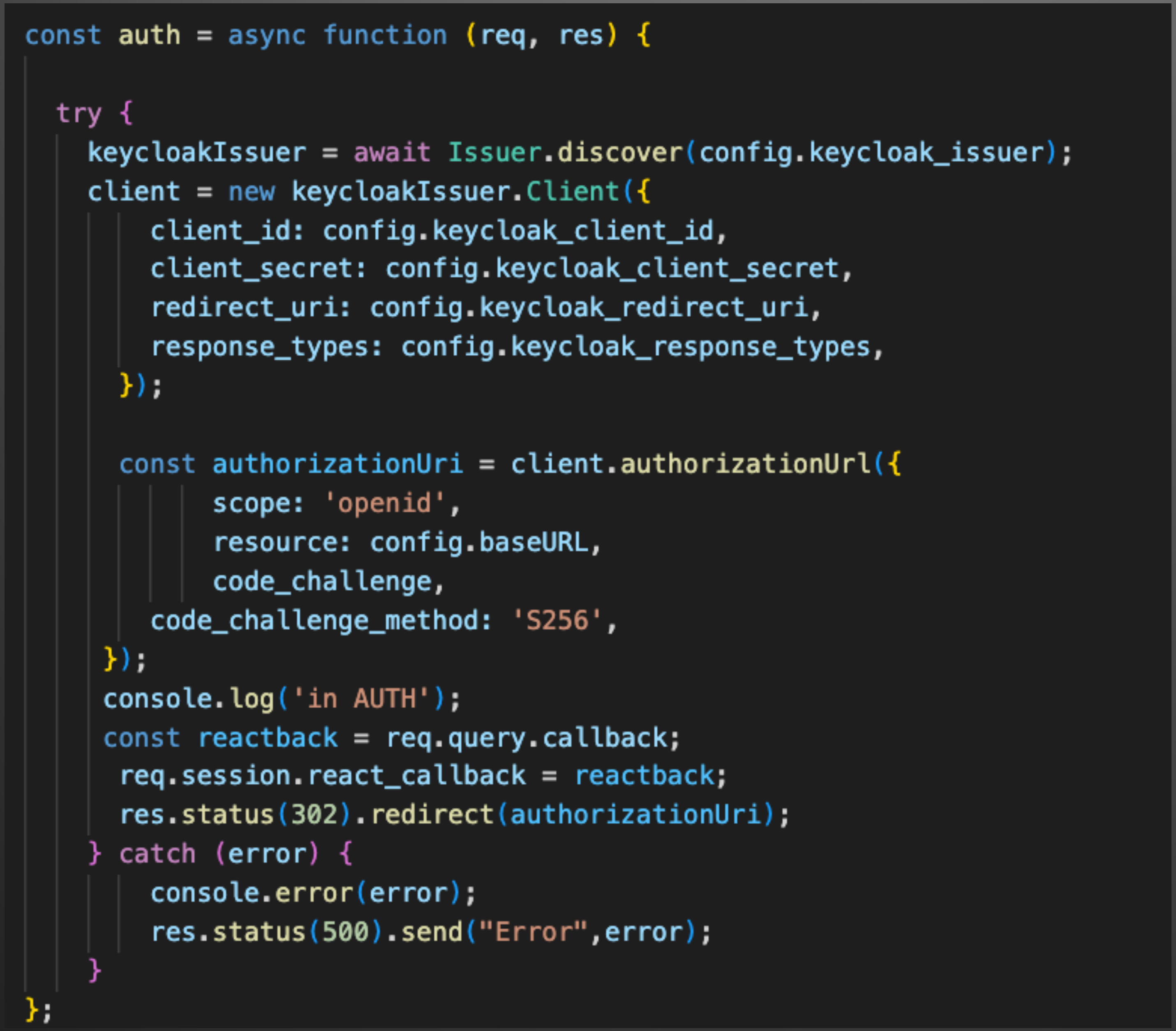
5TH APP - XPAGES



6TH APP – NOMAD WEB FOR DOMINO



NODE.JS SAMPLE CODE OIDC CLIENT (KEEP & ADP) - AUTH

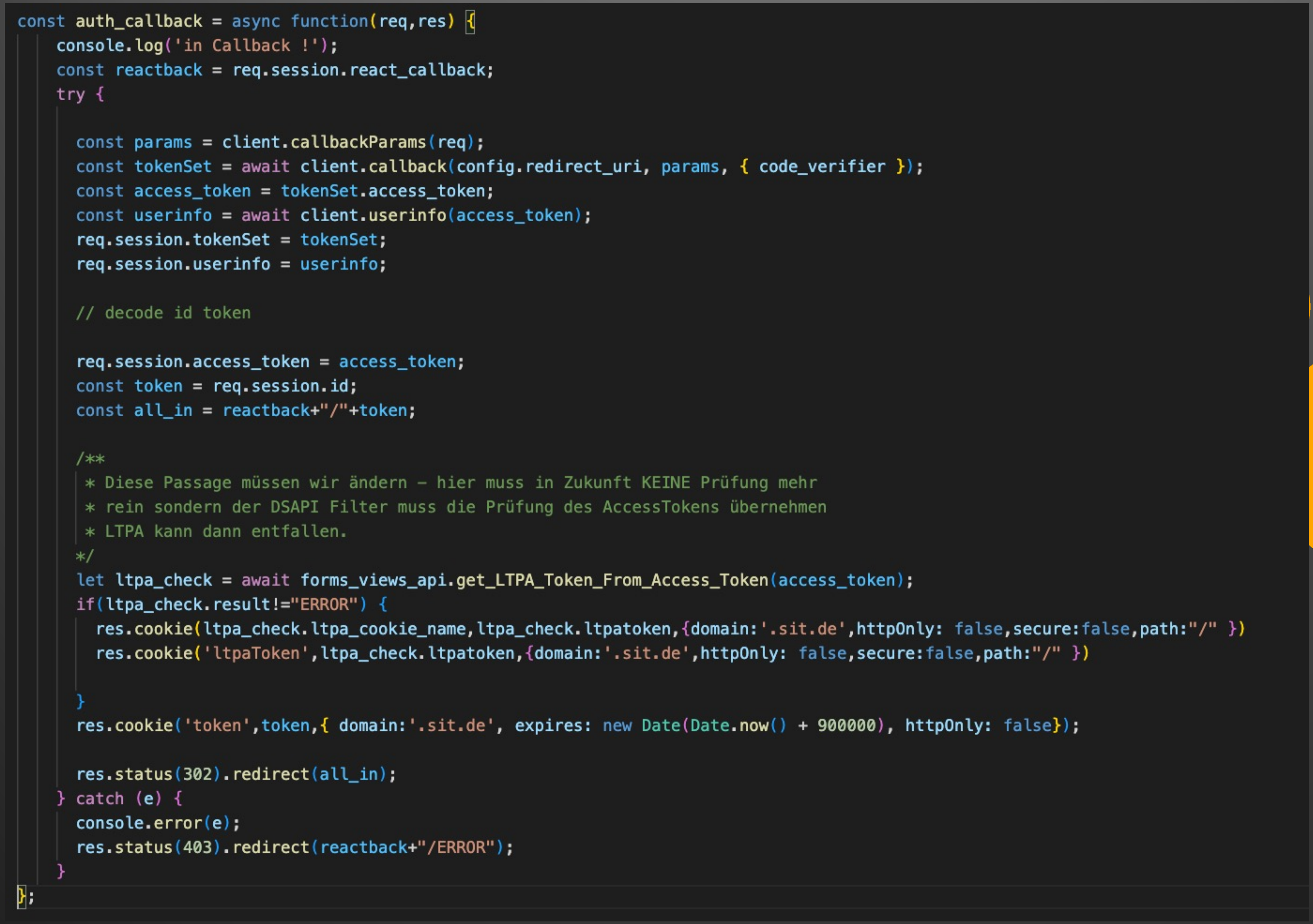


```
const auth = async function (req, res) {

  try {
    keycloakIssuer = await Issuer.discover(config.keycloak_issuer);
    client = new keycloakIssuer.Client({
        client_id: config.keycloak_client_id,
        client_secret: config.keycloak_client_secret,
        redirect_uri: config.keycloak_redirect_uri,
        response_types: config.keycloak_response_types,
      });

      const authorizationUri = client.authorizationUrl({
            scope: 'openid',
            resource: config.baseURL,
            code_challenge,
        code_challenge_method: 'S256',
     });
     console.log('in AUTH');
     const reactback = req.query.callback;
      req.session.react_callback = reactback;
      res.status(302).redirect(authorizationUri);
    } catch (error) {
        console.error(error);
        res.status(500).send("Error",error);
    }
};
```

**Standard OIDC Clients vs.
Vendor Specific Packages!**

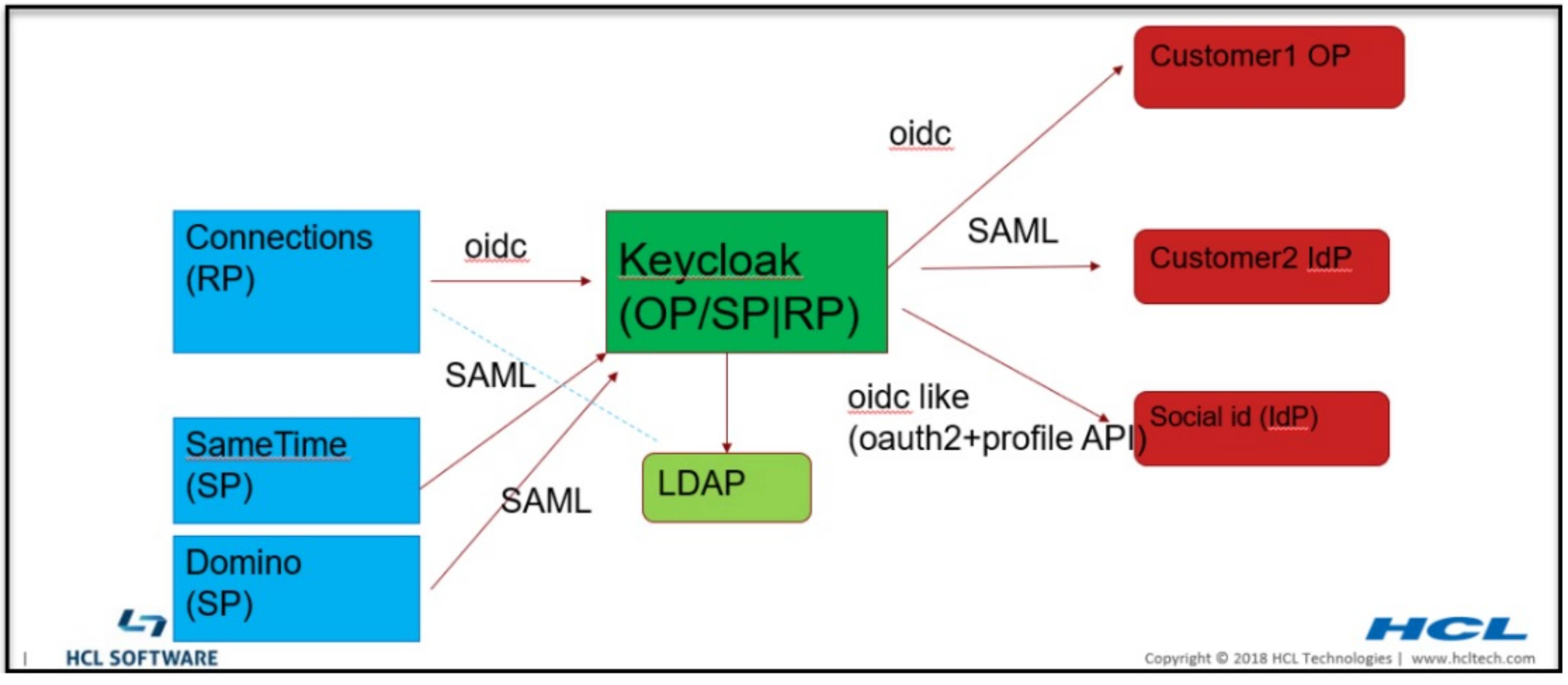
Same Code for different APIs

NODE.JS SAMPLE CODE OIDC CLIENT (KEEP & ADP) - CALLBACK



```
const auth_callback = async function(req,res) {
    console.log('in Callback !');
    const reactback = req.session.react_callback;
    try {

      const params = client.callbackParams(req);
      const tokenSet = await client.callback(config.redirect_uri, params, { code_verifier });
      const access_token = tokenSet.access_token;
      const userinfo = await client.userinfo(access_token);
      req.session.tokenSet = tokenSet;
      req.session.userinfo = userinfo;

      // decode id token

      req.session.access_token = access_token;
      const token = req.session.id;
      const all_in = reactback+"/"+token;

      /**
       * Diese Passage müssen wir ändern - hier muss in Zukunft KEINE Prüfung mehr
       * rein sondern der DSAPI Filter muss die Prüfung des AccessTokens übernehmen
       * LTPA kann dann entfallen.
      */
      let ltpa_check = await forms_views_api.get_LTPA_Token_From_Access_Token(access_token);
      if(ltpa_check.result!="ERROR") {
        res.cookie(ltpa_check.ltpa_cookie_name,ltpa_check.ltpatoken,{domain:'.sit.de',httpOnly: false,secure:false,path:"/" })
        res.cookie('ltpaToken',ltpa_check.ltpatoken,{domain:'.sit.de',httpOnly: false,secure:false,path:"/" })

      }
      res.cookie('token',token,{ domain:'.sit.de', expires: new Date(Date.now() + 900000), httpOnly: false});

      res.status(302).redirect(all_in);
    } catch (e) {
      console.error(e);
      res.status(403).redirect(reactback+"/ERROR");
    }
};
```

KEYCLOAK & THE REST OF THE (HCL-) PACK....

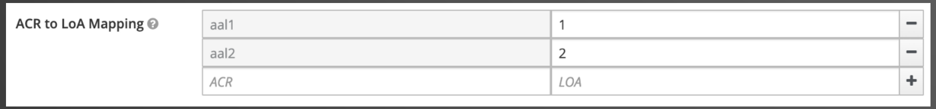


SSO between Connections, SameTime and Domino can be done via Keycloak. We can also include DX and even Commerce.

https://help.hcltechsw.com/connectionscloud/_012_Keycloak+Authentication+and+SSO/download/Keycloak+Authentication+and+SSO.pdf

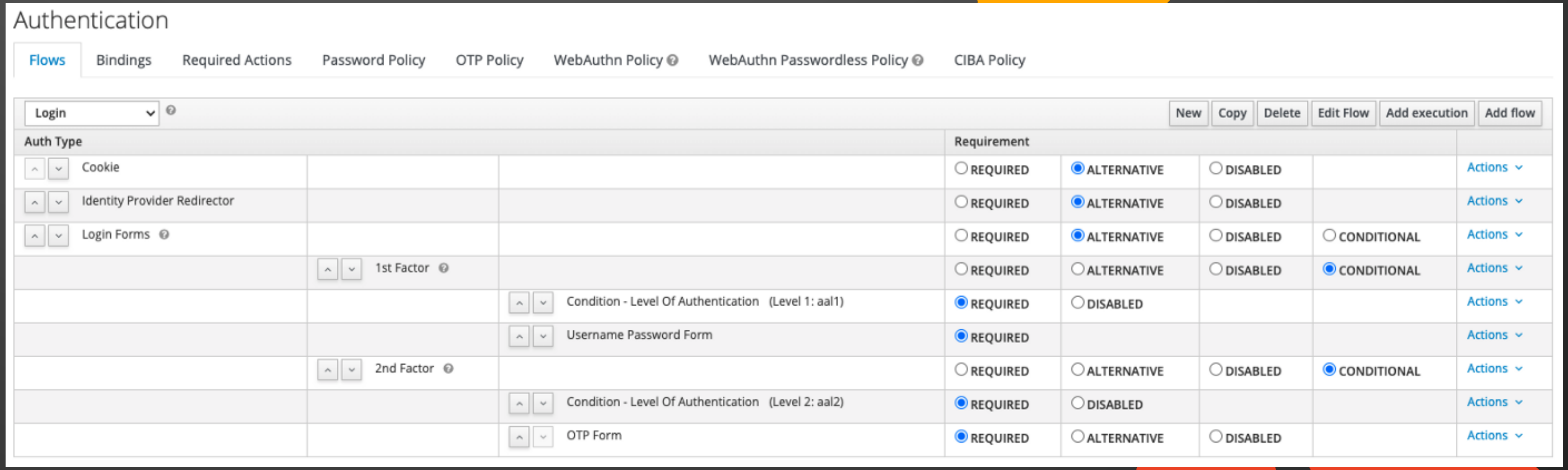
MFA & STEP-UP AUTHENTICATION IN KEYCLOAK

- Keycloak supports step up authentication
- TOTP Config per REALM & Users
- Supports Google Authenticator and FreeOTP



ACR to LoA Mapping			
	aal1	1	−
	aal2	2	−
	ACR	LOA	+

- Business Rules for Step Up Config
- Apps request the step up flow by sending ACR levels



Authentication

Flows | Bindings | Required Actions | Password Policy | OTP Policy | WebAuthn Policy | WebAuthn Passwordless Policy | CIBA Policy

Login

New | Copy | Delete | Edit Flow | Add execution | Add flow

Auth Type			Requirement				
Cookie			○ REQUIRED	● ALTERNATIVE	○ DISABLED		Actions
Identity Provider Redirector			○ REQUIRED	● ALTERNATIVE	○ DISABLED		Actions
Login Forms			○ REQUIRED	● ALTERNATIVE	○ DISABLED	○ CONDITIONAL	Actions
	1st Factor		○ REQUIRED	○ ALTERNATIVE	○ DISABLED	● CONDITIONAL	Actions
		Condition - Level Of Authentication (Level 1: aal1)	● REQUIRED	○ DISABLED			Actions
		Username Password Form	● REQUIRED				Actions
	2nd Factor		○ REQUIRED	○ ALTERNATIVE	○ DISABLED	● CONDITIONAL	Actions
		Condition - Level Of Authentication (Level 2: aal2)	● REQUIRED	○ DISABLED			Actions
		OTP Form	● REQUIRED	○ ALTERNATIVE	○ DISABLED		Actions

- For APIs as well!

With step-up authentication, Web Applications or APIs that allow access to different types of resources can require users to authenticate with a stronger authentication mechanism to access sensitive resources.

WHAT IS IDENTITY BROKERING?

Identity Brokering

An Identity Broker is an intermediary service that connects multiple service providers with different identity providers. As an intermediary service, the identity broker is responsible for creating a trust relationship with an external identity provider in order to use its identities to access internal services exposed by service providers.

From a user perspective, an identity broker provides a user-centric and centralized way to manage identities across different security domains or realms. An existing account can be linked with one or more identities from different identity providers or even created based on the identity information obtained from them.

An identity provider is usually based on a specific protocol that is used to authenticate and communicate authentication and authorization information to their users. It can be a social provider such as Facebook, Google or Twitter. It can be a business partner whose users need to access your services. Or it an be a cloud-based identity service that you want to integrate with.

WHAT'S THE TAKE ?

- Keycloak covers all SSO angles for the HCL Digital Solutions portfolio.
- Keycloak offers Identity Brokering capabilities for free
- Token mapping between SAML and OIDC is brilliant
- Open Source and Extensibility
- Cloud Hosting, SaaS and on-premises
- High availability scenarios available (on-prem and SaaS)
- Keycloak brings even more that we did not cover (WebAuthn, MFA …)

Keycloak & HCL Domino -

The perfect match for all things SSO.

QUESTIONS

Thank you !

Heiko Voigt

- heiko.voigt@harbour-light.com
- @HarbourLightcom
- https://github.com/heikovoigt

https://www.c3ug.ca/

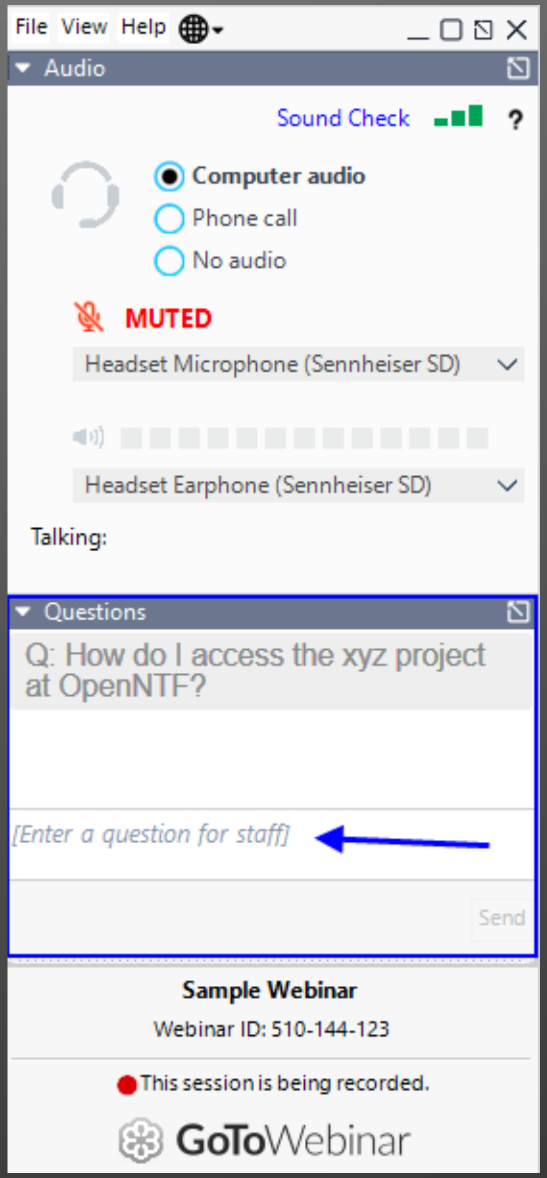
QUESTIONS?

Use the GoToWebinar Questions Pane

Please keep all questions related to the topics that our speakers are discussing!!!

Unrelated Question => post at:

https://openntf.org/discord



Q: How do I access the xyz project at OpenNTF?

[Enter a question for staff]

Sample Webinar

Webinar ID: 510-144-123

This session is being recorded.