SUPERTOKENS VS KEYCLOAK

Table of Contents

- If you want to add a password strength meter to registration, how does it work?
- If a session expires is there a pop-up? Does the user have to handle it?
- RBAC, check properly, how to get the role of the user within the API for custom logic for both frontend and backend.
- Implementation with ssr
- Is there a mechanism for protecting routes (similar to the supertokens auth wrapper). How easy is it to protect multiple pages and what does the code look like?
- Email is not verified but password reset is done, does that verify email?
- How well do they support various platforms and SDKs?
- How to disallow sign up and only have sign in?
- Changing Email for social provider, how it works?

01 Describe the dev setup experience (how many steps and what are they + time overall)

Keycloak

- Setting up the keycloak server through the getting started guide is quick.
- The next parts of the guide go into granular detail of server installation which is very overwhelming. It mentions multiple ways to startup the server, mentioning multiple “operating modes” to run it, clustering, database and network setup and downloading additional tools for more configuration…
- It is easier to google for a third party tutorial showing how to set it up for your particular tech stack which in this case was node and react.
- You could then log into the keycloak dashboard and started configuring my app
- Total time taken for configuration was about 10 mins. This includes setting up the realm, with signin/sign up, email verification.
- There are alot of customizations available and it was alot to take in and go through...
- Setting up an email for email verification and password reset requires you to set up smtp mail. No in-built or out-of-the-box solution.
- Setting up Social Providers seems simple, for setting up google, had to put the clientid and client secret, some configuration so it could work on my local setup but no other issues with social login.
- Setup keycloak in the react app according to the tutorial. Seems easy with minimum configs as the most configuration is done in the dashboard.

SuperTokens

- See video here

- **FRONTEND**
  - Install frontend SDK
  - Call the init function
  - Add routing handler
  - Add session interceptor (if using axios)

- **BACKEND**
  - Install backend SDK
  - Call the init function
  - Add middleware and error handler

- **CORE**
  - If managed service
    1. Sign up
    2. Select region
    3. Use instance
  - If self hosted
    1. Download docker image / zip binary
    2. Install binary (if used that)

02 Can you easily add a custom social provider?

Keycloak

Flow for setting up Google and Facebook:

- Generate the client secret and client id from you google app
- Add google as a provider from the Identity provider tab on the dashboard
- Add the generated client secret and client id

The dashboard has extensive customization options(setting a custom login flow, setting scopes etc..)

- By default keycloak supports most social providers. Additional custom Identity providers can be added from the dashboard if they fall under the SAML or Open ID connect protocols. There seem to be incompatibility issues with login with apple though, sign in with apple uses some params of the OIDC spec which is not commonly used and keycloak's built in OIDC implementation does not support it yet. Keycloak also has Service Provider Interfaces, this allows users to add custom code to support custom identity providers.

Ease of implementation: 4/5

SuperTokens

Yes. We support any OAuth 2.0 provider: See docs. All the code required to add a custom provider + extract profile info from their payload is within your own backend SDK, as a simple callback function.

03 How to go about sending emails yourself if you want to?

Keycloak

Keycloak is not able to send emails by default but requires you to use a smtp mail server.

Flow for setup using zoho mail:

- Got the smtp URL from zoho
- Add the correct port
- Added my zoho mail credentials

Ease of implementation 5/5

SuperTokens

We have callback functions for sending email, which you can use to send custom designed emails using whichever method you want.

04 How to implement sign out functionality?

Keycloak

- The keycloak object on your frontend has a logout function

Ease of implementation: 5/5

SuperTokens

The API for sign out is automatically exposed via our backend SDK. You have to use the signOut function exposed by the frontend SDK and you are done.

05 How to go about customising the email design and or the sender's domain?

Keycloak

- Keycloak allows for full customization of the UI but this customization is not user-friendly. There is no method of customizing the ui from keycloaks dashboard, you can only set what theme you would like to apply. If you want to customize a theme you need to create a custom theme as according to the documentation you should not make any changes to the default themes. To create a custom theme you need to navigate to the keycloak/theme directory and create your custom theme file there. Most tutorials recommend copying the contents of one the base themes into your custom theme directory and then start making changes. Each theme has an individual directory responsible for a certain category, for example, there is a login directory that contains all the properties for the login, otp, registration, forgot password UI, an email directory containing all the content (messages/subject) which would be sent for emails. I started checking out the customization for the login screen, there is a css file I can change which allows me to change all the properties of the elements shown on the login screen.
- The senders domain can be customized from the keycloak dashboard

Ease of implementation: 1/5

SuperTokens

We have callback functions for sending email, which you can use to send custom designed emails using whichever method you want.

06 How would adding custom sign up fields work?

Keycloak

- Adding custom fields to the registration form also has to be done through a custom theme. The base theme which all other themes extend contains a configuration for what fields are shown on the registration form. We can add additional fields to this configuration. The theme configuration for the account management page in the keycloak dashboard has to be updated so it can now display the new fields. Detailed info about the additional configuration can be found here

Ease of implementation: 1/5

SuperTokens

- See docs
- They would need to handle those custom fields themselves post sign up

07 How would adding custom sign up validators work?

Keycloak

- Keycloak has a set of authentication flows defined. Ex. Registration is an authentication flow which consists of a series of actions(Registration User Creation, Password Validation etc...). To create custom signup validators, i would have to create a new Authentication flow which would be a copy of the original Registration flow(Can be easily done through the dashboard) and add a custom action to the new flow. To create the custom action requires you to write Java code that implments some keycloak interfaces where you define you custom validation. You need to then build this into a JAR file and add it to a specific directory in your keycloak installation.

Ease of implementation: 1/5

SuperTokens

- See docs
- They would need to handle those custom fields themselves post sign up

08 Changing password validation(or some similar feature) for sign up does this get propagated to other places(-Signin, password reset)

Keycloak

Changing the password validation in one flow will not affect another flow. If one wants these changes to propagate to other custom flows we would need to create the custom action(password validation in this case) and use it in place of the default action in all Authentication flows

SuperTokens

Yes

09 How do we do things like handle sign up success?

Keycloak

It's possible to do so but this would involve similar steps to adding custom validation. In keycloak Registration flow is comprised of a series of actions as mentioned above. You can create a copy of actions in the base registration flow, modify the User Creation action and apply the action to the Registration flow. Similarly an additional action can be created to take place after user registration.

Ease of implementation: 1/5

SuperTokens

- We have a frontend event that's fired that providers them details of the new user
- We allow users to easily override the backend (their backend) APIs that our SDK adds to handle post sign up like functionality. Within that override, they can call the original implementation so as to not have to implement everything within that API.

10 How to implement revoking a user's session functionality?

Keycloak

- The user's session can be revoked by calling the keycloak logout menthod on the frontend. This will clear the auth cookies on the browser and invalidate the refresh token. On the backend a all user sessions can be revoked using the user id, a single user session can be revoked using a session id can be revoked or all users can be logged out.

Ease of implementation: 5/5

SuperTokens

The backend SDK has `revokeSession` function which takes various inputs...

11 What if you want to embed the sign up / in page into your website UI (As opposed to opening a new tab..). Is that possible?

Keycloak

Haven't found information about people embedding keycloak into their webpage. What some people have suggested is using their own project login ui and calling keycloak's authorization/authentication apis as mentioned in this comment. This method has difficulties in implementing the OTP and social login features though.

SuperTokens

Yes. It is possible. See this as an example.

12 If one needs to do something like paginating across all users in the app in their API, how can they do that?

Keycloak

- Keycloaks backend admin client for node allows you to query information about users. Information can be retrieved with multiple filters including realm, email, first(id of the user), max (number of users to return), etc.. The issue is the lack of documentation regarding the library. There is in-depth information/ descriptions about the API spec so it's annoying to figure out the what are the inputs to the attribues.

Keycloak allows for pagination and has an api that you can use to query for paginated user data. It takes to query parameters, first and max. first is the element id and max is the number of elements to return. More info can be found here

SuperTokens

- Our SDK has functions for that.
- We also allow devs to export all users as CSV from our dashboard

13 Will their solution work with serverless env like in nextjs or netlify?

Keycloak

Keycloak has no native support for react and ssr, there is a third party library which uses the javascript client adapter and allows for ssr. Used the third party library, There is almost no documentation, had to set it up using the example provided in the github repo.

SuperTokens

Yes

14 Sharing session across sub domains

Keycloak

Test sharing across subdomains:

- Set `a.example.com` and `b.example.com` to point to localhost in /etc/hosts
- Logged into `a.example.com`
- Changed URL to `b.example.com`
- There is a redirect to the keycloak auth server but the user is automatically logged in.

SuperTokens

Possible by setting the cookieDomain to be .example.com via our frontend and backend configs.

15 Documentation review

Keycloak

The Keycloak quickstart is quick and easy to follow but that just involves setting up and configuring the keycloak server, for actually configuring keycloak in your app you will have to follow the main documentation. The main documentation really overwhelming to go through with a lot of configuration options mentioned, also the documentation for client adapters is minimal, for example, the nodejs admin client adapter has no documentation on the official documentation page and the readme for the library on github gives minimum information

SuperTokens

- It is split into recipes.
- Each recipe doc has all the steps needed to use it from getting started to customisations, to overrides, to integrations with other frameworks like NextJS or AWS lambda or Hasura

16 Email verification with Social providers, how does it work

Keycloak

- When email verification is enabled in the dashboard, when a user signs in/registers with a social provider they get redirected to a page that prompts the user to check their mail and clink on the link.
- I set up google as a social provider and tested the flow, on signing in it sent an email to my gmail account with a verification link.

SuperTokens

- If the provider gives us that the email is verified already, we mark it as verified in our db
- Else we show the email verification screen to the end user (if it is switched on by the dev).
- If the email changes on the social provider's side, it is marked as unverified again.

17 User has multiple sessions, only want to revoke a couple of them, how does that work

Keycloak

On the backend the admin library can revoke sessions using a session id, you can retrieve all the session information belonging to a user and revoke the required session

SuperTokens

Each session has a unique ID (that we call `sessionHandle`). You can call `revoke_session` with a specific `sessionHandle` in your backend.

18 If you want to add a password strength meter to registration, how does it work?

Keycloak

No such implementation of changing GUI in the login screen seen by us, the only things we've seen people do is write hooks that would display a custom message when input was given to a form field.

SuperTokens

You can override the specific component that show the password field, and add the password strength meter to it.

19 If a session expires is there a pop-up? Does the user have to handle it?

Keycloak

There is no session expires pop up when the frontend access token expires the frontend has to refresh the session.

SuperTokens

As of now, the user has to handle it. But we have open issues for this.

20 RBAC, check properly, how to get the role of the user within the API for custom logic for both frontend and backend.

Keycloak

- Create roles and assign them to users(easily done through the dashboard)

Frontend

- On your front end after authentication happens store(up to the user to decide where to store it) the access token retrieved from the keycloak object.
- Create an axios interceptor to add the access token to the Authorization header for requests to the backend.

Backend

- Initialize keycloak on the backend(one of the recommended methods for setup was not working at all, had to manually setup the config)
- You can protect your routes by adding keycloak.protect("role") as a middleware to the route

SuperTokens

- Devs can add a role to a session on creation (based on the userID).
- This role can be fetched on the backend (post session verification) and on the frontend.
- Roles can be edited in the session on the backend (post session verification).

21 Implementation with ssr

Keycloak

Using the @react-keycloak/ssr to setup a nextjs app with keycloak.

Flow

- Click on the login button, redirects you the keycloak login page
- Enter account credentials
- On redirection, the ssr library will set the access token cookies in the browser
- Refresh tokens seem to automatically refreshed
- kcToken decoded payload:


```
{ “exp”: 1617188790, “iat”: 1617188490, “auth_time”: 1617187986,
“jti”: “fedd20ef-ce34-43bc-bea2-e3ab005e149a”, “iss”: “http://
localhost:8080/auth/realms/Keycloak-Demo”, “aud”: “account”,
“sub”: “f78d9978-8f96-40f3-9e48-57e481ca64ae”, “typ”: “Bear-
er”, “azp”: “nextjs-frontend”, “nonce”: “ffadcd8a-27bd-4ba2-
8d62-14eea49981de”, “session_state”: “eabd12a8-7529-4a66-
b908-4eaddae71658”, “acr”: “0”, “allowed-origins”: [ “*” ],
“realm_access”: { “roles”: [ “offline_access”, “admin”, “uma_au-
thorization”, “user” ] }, “resource_access”: { “account”: {
“roles”: [ “manage-account”, “manage-account-links”, “view-pro-
file” ] } }, “scope”: “openid profile email”, “email_verified”:
false, “name”: “johndoe”, “preferred_username”: “johndoe@gmail.
com”, “given_name”: “john”, “family_name”: “Doe”, “email”:
“johnDoe@gmail.com” }
```


- kcIdToken decoded payload:


```
{ “exp”: 1617188790, “iat”: 1617188490, “auth_time”: 1617187986,
“jti”: “42e254cc-f7ea-4572-87d3-20b11f42c2c7”, “iss”: “http://
localhost:8080/auth/realms/Keycloak-Demo”, “aud”: “nextjs-fron-
tend”, “sub”: “f78d9978-8f96-40f3-9e48-57e481ca64ae”, “typ”:
“ID”, “azp”: “nextjs-frontend”, “nonce”: “ffadcd8a-27bd-4ba2-
8d62-14eea49981de”, “session_state”: “eabd12a8-7529-4a66-b908-
4eaddae71658”, “at_hash”: “uxVNHLsPyX-8Zem6_s7OAg”, “acr”: “0”,
“email_verified”: false, “name”: “johnDoe”, “preferred_username”:
“johnDoe@gmail.com”, “given_name”: “john”, “family_name”: “Doe”,
“email”: “johnDoe@gmail.com” }
```

SuperTokens

- Yes.
- With NextJS we have dedicated docs for this here

22 Is there a mechanism for protecting routes (similar to the supertokens auth wrapper). How easy is it to protect multiple pages and what does the code look like?

Keycloak

- Keycloaks javascript adapter is genric and is to be used with any javascript framework(react, angular, pure javascript...) so there is no native support or react built in, like no react components. I followed along a tutorial that used the javascript adapter to make components to secure routes, automatically refresh sessions, and redirect to the auth page on session expiry. The tutorial isnt very hard to follow, the only issue is that there is no other of this method and no documentation mentions how to do it this way.
- Ease of implementation: 2/5

SuperTokens

Yes

23 Email is not verified but password reset is done, does that verify email?

Keycloak

When email verification is turned off resetting your password does not verify the email. When email verification is turned on and you click on the password reset link, it redirects you to the email verification screen. On clicking the email verification link you continue with the password reset flow and are able to reset your password.

SuperTokens

No. But this is an open issue at the moment.

24 How well do they support various platforms and SDKs?

Keycloak

- Good support(Complete Documentation, examples, active community)
- Java: JBoss EAP, WildFly, Fuse, Tomcat, Jetty 9, Servlet Filter, Spring Boot, Spring Security
- JavaScript (client-side): JavaScript
- Node.js (server-side): node adapter

No keycloak sdks(used as a generic OIDC provider)

- C#: OWIN (community)
- Python: oidc (generic)
- Android: AppAuth (generic)
- iOS: AppAuth (generic)
- Apache HTTP Server: mod_auth_openidc

SuperTokens

As of this writing, we have support for NodeJS and react + vanilla JS sessions. One can build their own UI + backend using our APIs (a few days of work), as long as we support sessions for their frontend (as that is really complex for them to build out).

25 How to disallow sign up and only have sign in?

Keycloak

The Dashboard provides an option to disable sign ups.

SuperTokens

- Can override the backend API to disallow sign up (by throwing an error in that case)
- Can override the frontend component that lets users switch to the sign up view

26 Changing Email for social provider, how it works?

Keycloak

- Keycloak doesn't provide a flow for changing emails. They do provide an end-point for updating emails in their management API.
- The users in this forum post mention issues implementing an email update flow

SuperTokens

- Each login will update the email used by the end user in our db. So if the social provider has changed the email, ours will change too.