

# Unified MFA with PrivacyIDEA

*FreeIPA + Keycloak + PrivacyIDEA*

Scientific Data and Computing Center

Brookhaven National Laboratory

Masood Zaran

20 May 2021



BROOKHAVEN SCIENCE ASSOCIATES

# Background:

- With more applications and services being deployed at BNL SDCC the adoption of Multi-factor Authentication (MFA) became inevitable.
- While web applications can be protected by Keycloak (SSO) with its MFA feature, other service components within the facility rely on FreeIPA (LDAP) for MFA authentication.
- This technically satisfies cyber security requirements; but it also creates a situation where users need to manage multiple tokens under the BNL SDCC services umbrella.

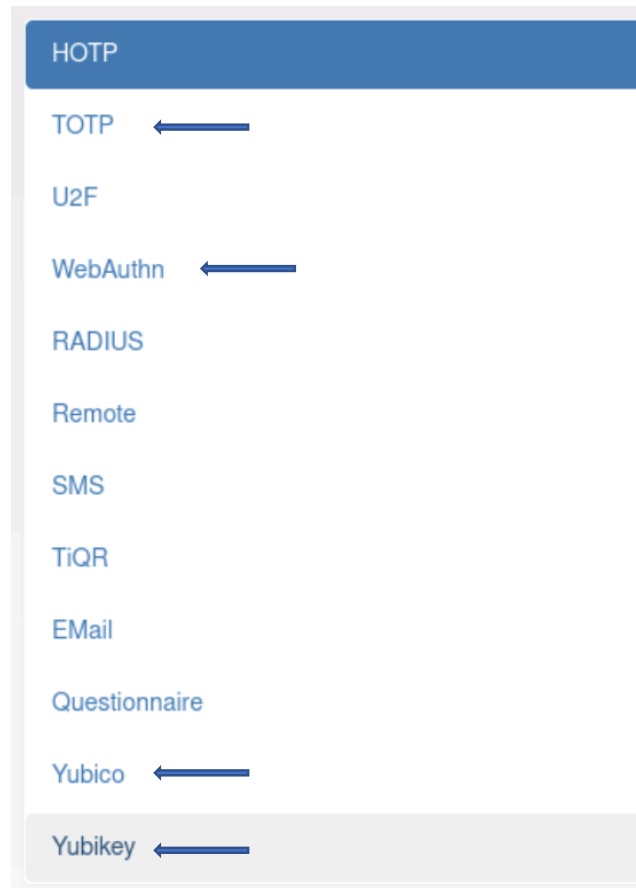
# Current OTP challenges

- Keycloak unable to consume FreeIPA based OTP tokens due to a design limitation.
  - (RFE Case #02592998)
- As a result, Keycloak & FreeIPA stores user OTP tokens separately, tokens are not interchangeable.
  - Ex. Keycloak uses 20-digit base32 encoded secret Vs IPA uses 32-digit base64 encoded secret for OTP.
- End users consume multiple OTP tokens.
  - Ex. web applications like Jupyterhub consumes Keycloak-based OTP token vs IPA client like NX consumes IPA-based OTP token. Confusing to users.
- Keycloak's OTP tokens are unique per "Realm".
- Need to provide users a single OTP which can be used everywhere including other services like mail or future new services.

# PrivacyIDEA

- Enterprise ready opensource modular authentication system.
- Comes with a variety of MFA tokens and features built-in.
- Easy to integrate to other systems with the use of plug-ins.
  - Ex. PAM, OTRS, Apache2, FreeRADIUS, ownCloud, simpleSAMLphp and Keycloak.
- Customization using REST API, policies and event handlers.
- Policies allow modification of system level attributes.
  - Ex.auth, webui, max tokens etc.
- Ability to map single realm to multiple external realms in Keycloak.

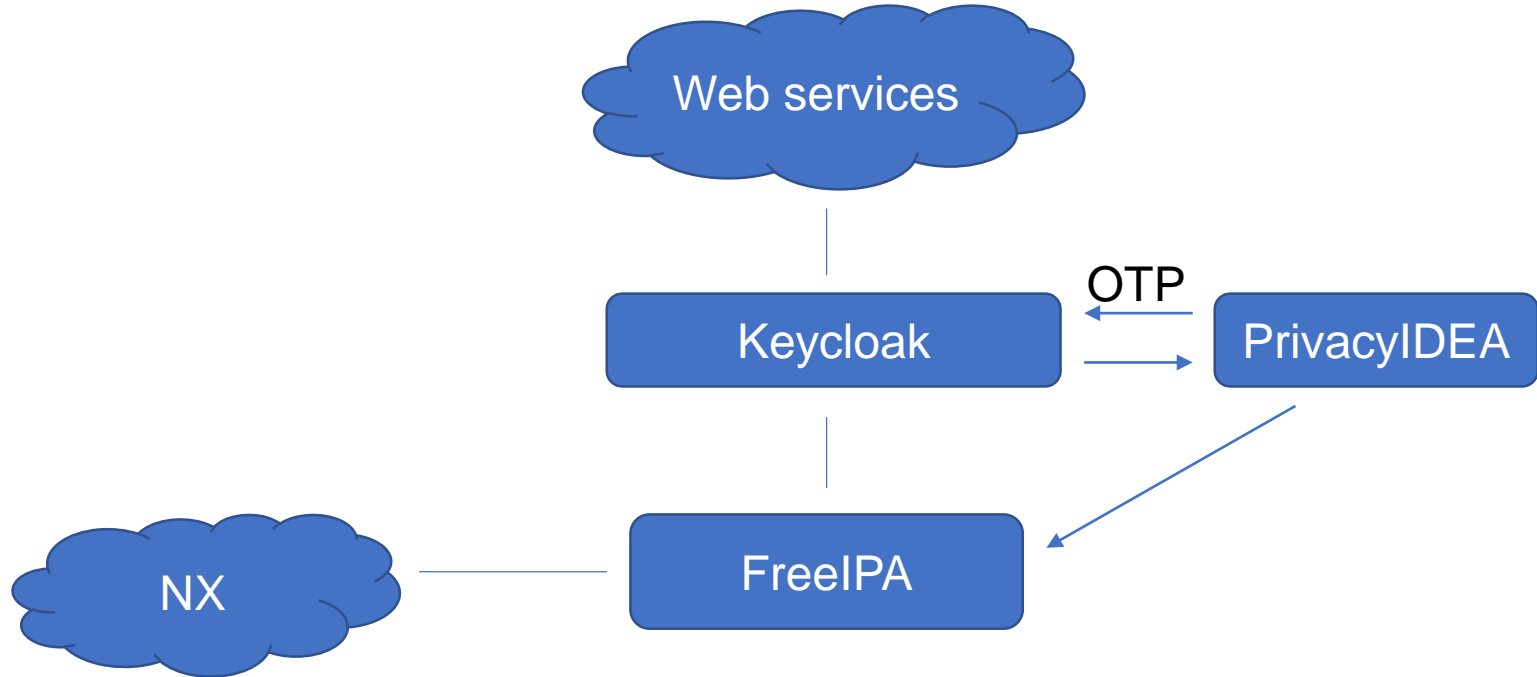
# PrivacyIDEA current MFA offerings



## + More

- Push Token
- Four Eyes
- Certificate Token
- Indexed Secret
- mOTP
- OCRA
- SSH Keys
- TAN Token
- TiQR

# Overview



# Keycloak enrollment using PrivacyIDEA

**BROOKHAVEN** | Scientific Data and  
NATIONAL LABORATORY | Computing Center

## SDCC\_MFA\_TEST

Username


Password


**Log In**



nl.gov/auth/realms/SDCC\_MFA\_TEST/login-actions/authenticate?execution=afc93e88-e62a-4f2a-bb7c

## SDCC\_MFA\_TEST

 You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
  - FreeOTP
  - Google Authenticator
2. Open the application and scan the barcode:  

3. Enter the one-time code provided by the application and click Submit to finish the setup.

One-time code \*

**Submit**



# Keycloak login using PrivacyIDEA

**BROOKHAVEN**  
NATIONAL LABORATORY | Scientific Data and  
Computing Center

**SDCC\_MFA\_TEST**

Username

Password

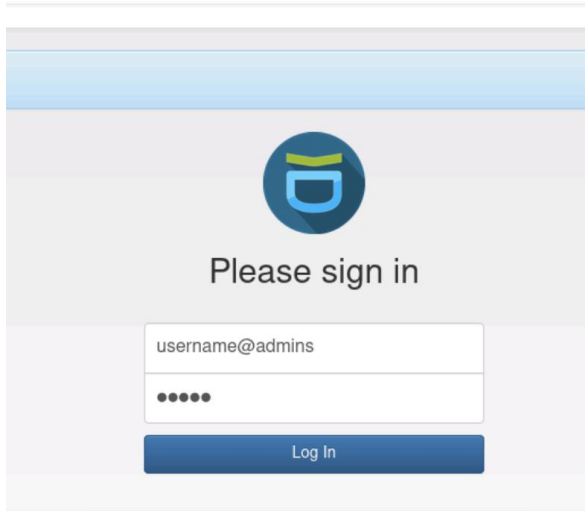


masood  
[Restart login](#)

One-time code \*



# PrivacyIDEA login / roles

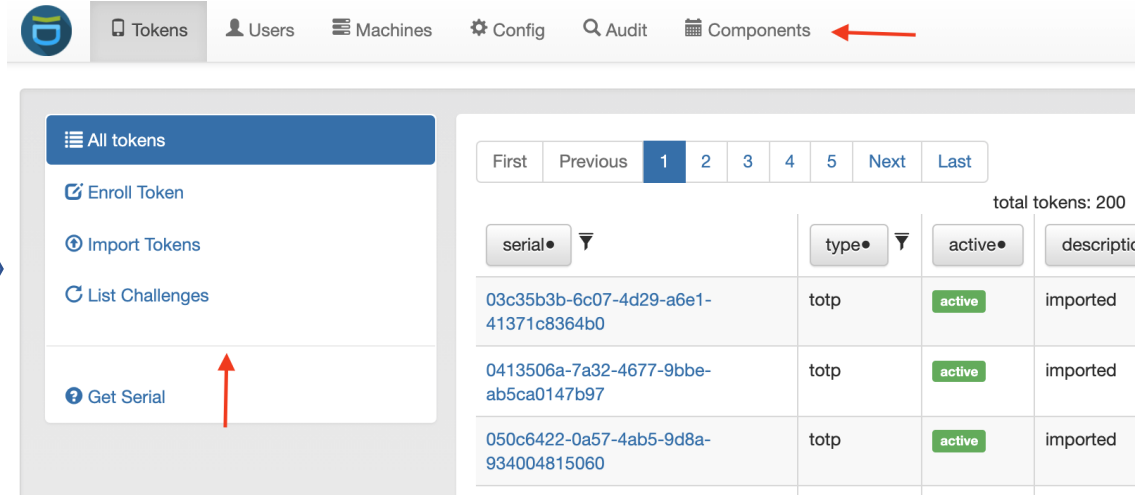


Please sign in

username@admins

.....

Log In



Tokens Users Machines Config Audit Components

All tokens

- Enroll Token
- Import Tokens
- List Challenges
- Get Serial

First Previous 1 2 3 4 5 Next Last

total tokens: 200

serial	type	active	descriptio
03c35b3b-6c07-4d29-a6e1-41371c8364b0	totp	active	imported
0413506a-7a32-4677-9bbe-ab5ca0147b97	totp	active	imported
050c6422-0a57-4ab5-9d8a-934004815060	totp	active	imported

# PrivacyIDEA login / roles

The diagram illustrates the PrivacyIDEA login process and the Tokens management interface. On the left, a login screen shows a 'Please sign in' prompt with a username field containing 'testuser@helpdesk' and a password field with masked characters. A 'Log In' button is at the bottom. A blue arrow points from the login screen to the Tokens management interface on the right. The Tokens interface has a top navigation bar with 'Tokens', 'Users', and 'Audit' tabs. A red arrow points to the 'Audit' tab. Below the navigation bar, there is a section for 'All tokens' with an 'Enroll Token' button. A red arrow points to the 'Enroll Token' button. To the right of the 'All tokens' section is a table of tokens. The table has columns for 'serial', 'type', 'active', and 'de'. The 'active' column contains green 'active' buttons. The 'de' column contains 'imp' buttons. The table lists four tokens with their serial numbers, types (all 'totp'), and active status.

serial	type	active	de
03c35b3b-6c07-4d29-a6e1-41371c8364b0	totp	active	imp
0413506a-7a32-4677-9bbe-ab5ca0147b97	totp	active	imp
050c6422-0a57-4ab5-9d8a-934004815060	totp	active	imp
067bc342-0d4a-43e6-b5c2-ff9230c0fb89	totp	active	imp

- Customized policies used to restrict authorization.
- Customization of Web UI access (timeout, pop up message, UI buttons).
- Restrict specific set of users from logging in all together.

# Questions?