MidPoint Integrations: Partner Series

Keycloak as an Access Layer

Ján Marcin

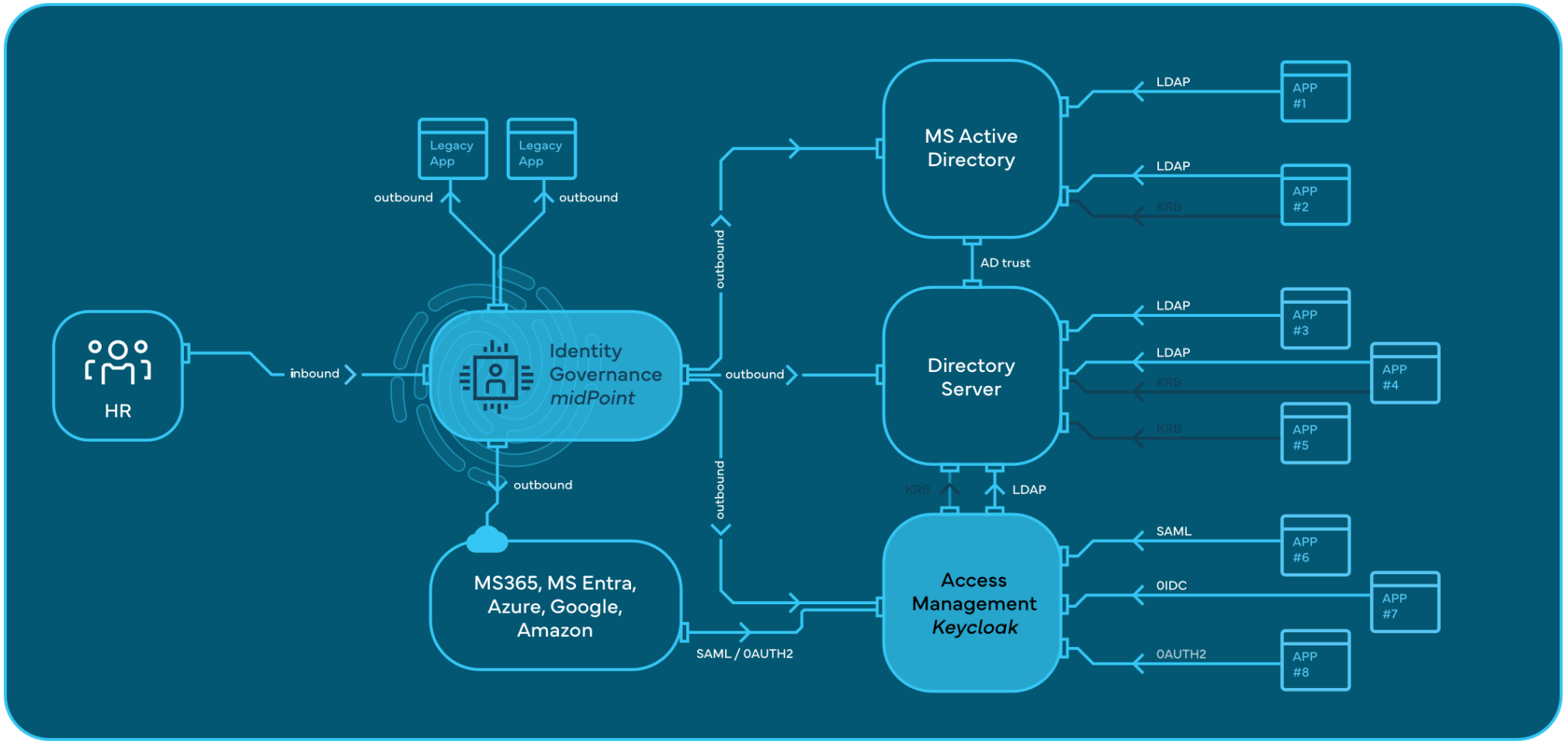
COO at Inalogy a.s.

IAM, IDM, IGA, AM

- IDM - Identity Management is focusing on identity lifecycle management and data orchestration.
  - Identity lifecycle management
  - Password management
  - Management policies
  - Requesting access
  - Data synchronization
- IGA - Identity Governance and Administration expands on IDM by adding governance and compliance features.
  - Identity analysis
  - Recertification
  - Role governance
  - Segregation of duties
  - Audit and Compliance
- AM - Access Management specifically about controlling access, rather than managing identities.
  - Central authentication
  - Single Sign-On (SSO)
  - Clients and services management
  - Multifactor authentication (MFA)
  - Identity federation
- IAM - Identity and Access Management is an overarching concept that includes aspects of all the others.
  - IDM
  - IGA
  - AM

INALOGY

Inalogy IAM concept



INALOGY

midPoint

Why there is a need for access layer

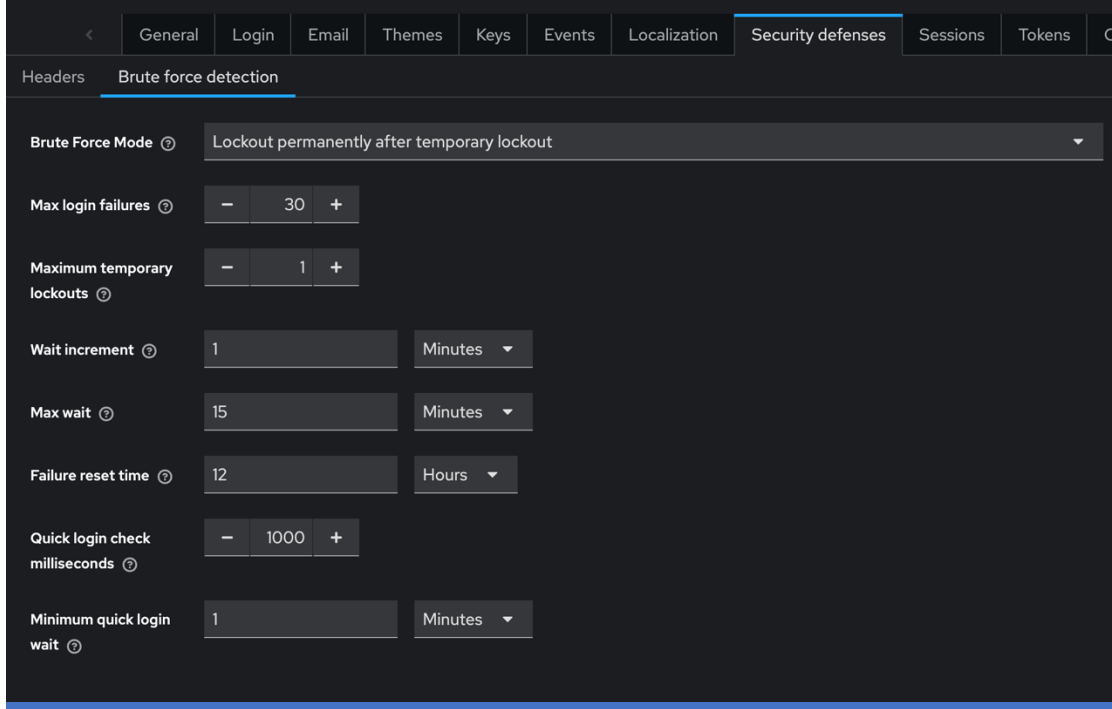
- To isolate the authentication layer
- Advanced safety mechanism
  - Brute force prevention
  - MFA
- Single Sign-On
- Delegated authentication
- Multiple options on the market
  - Keycloak
  - Microsoft Entra
  - Okta
  - CAS
  - Etc…

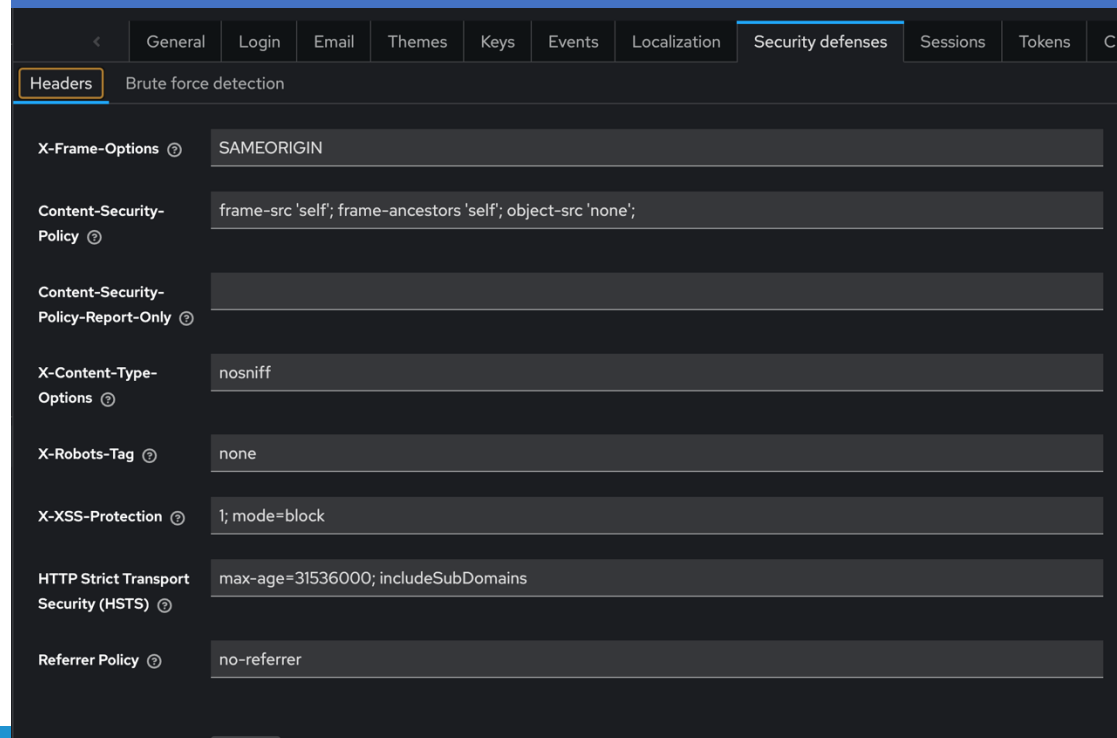
Why Keycloak

- Open-Source backed by CNCF
- Highly customizable UI
  - Themes
  - Localizations
- Supports customization of flows, processes, and screens via extension modules without impacting core code
- All standardized protocols
  - OAuth, OpenID Connect, SAML2.0
- Identity brokering via 3rd party IDPs
  - Microsoft, Google, Apple…
  - Custom IDPs supporting standard protocols
- MFA
  - OTP
  - Webauth
  - Certificates
  - Physical keys (Yubikey)
  - Passkeys
  - Push-notifications*

Mitigating security threats

- Defense mechanisms
  - Brute force detection
    - Lockout permanently
    - Lockout Temporarily
    - Lockout permanently after temporary lockout
  - Security Headers



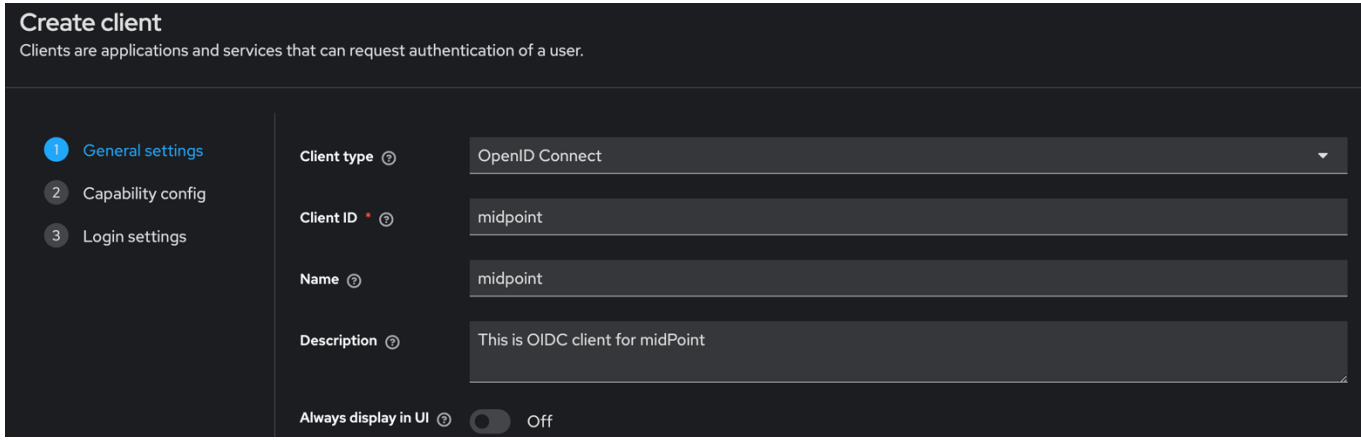


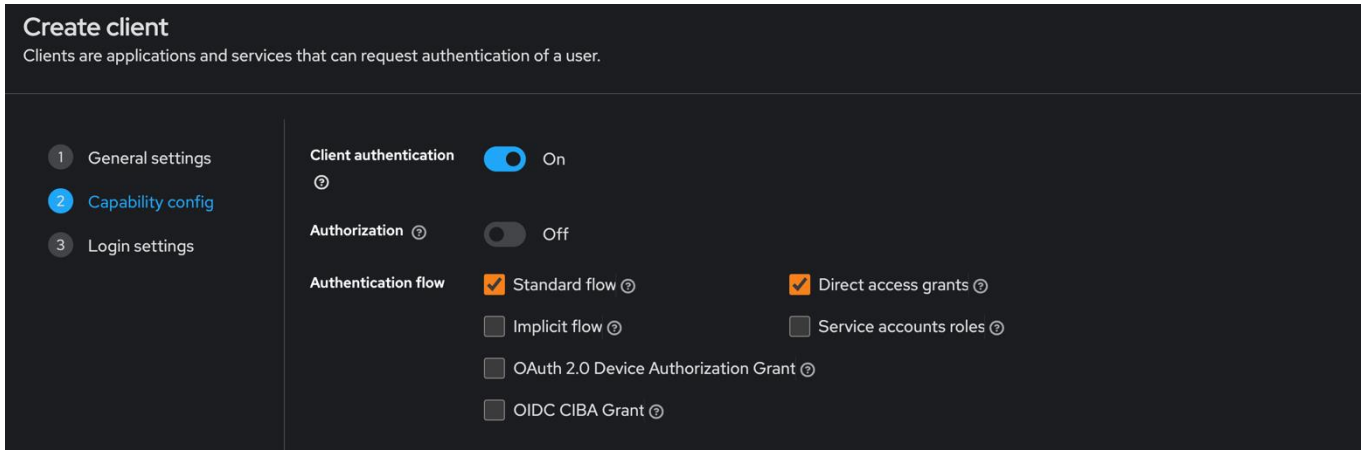
INALOGY

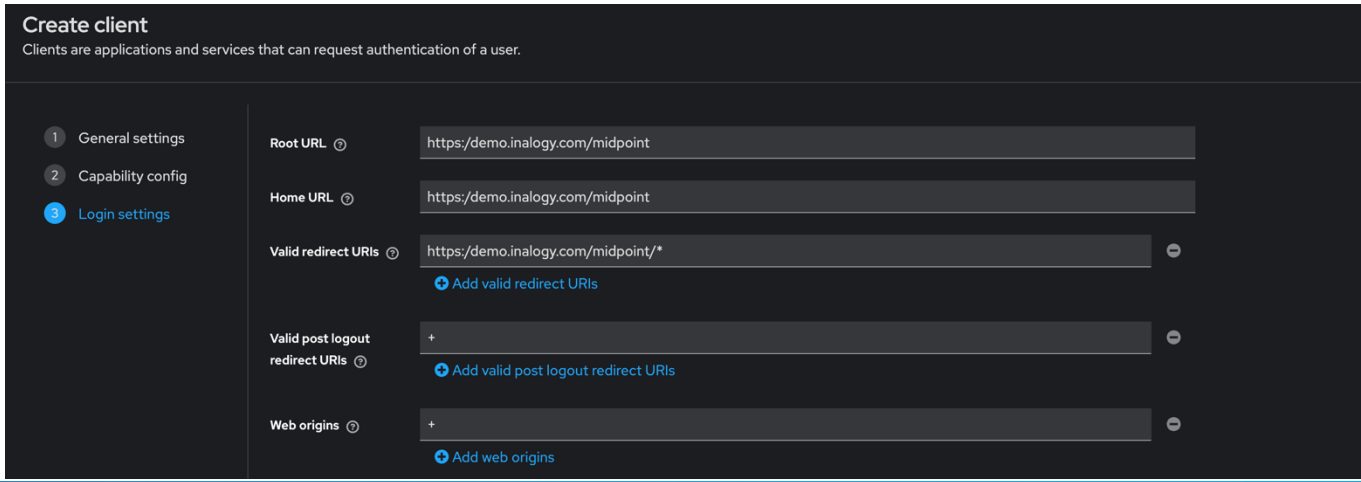
midPoint OIDC configuration

Keycloak side

- Create midPoint client in Keycloak
  - General settings
  - Capability configuration
  - Login settings
- Secret is generated after client creation
- Documentation link







INALOGY

midPoint OIDC configuration

midPoint side

- Security policy
- Flexible authentication
- OIDC module
- Authentication via ClientID and Secret
- Documentation link

1. To allow logging in for users that have no accounts in Keycloak (e.g., default midPoint `administrator`). Not strictly necessary.
2. OpenID Connect login for ordinary users.
3. Technical information that may be basically anything legal for inclusion into URI.
4. ID of the client as registered in Keycloak.
5. Secret of the client as generated by Keycloak (or provided manually).
6. URL at which Keycloak runs.

INALOGY

```
<securityPolicy>
    <authentication>
        <modules>
            ...
            <loginForm> (1)
                <identifier>loginForm</identifier>
            </loginForm>
            ...
            <oidc> (2)
                <identifier>gui-oidc</identifier>
                <client>
                    <registrationId>oidc-registration</registrationId> (3)
                    <clientId>midpoint</clientId> (4)
                    <clientSecret>
                        <t:clearValue>RwdBxRhOggkDCr321SzyGwkEVvRHd7g1</t:clearValue> (5)
                    </clientSecret>
                    <clientAuthenticationMethod>clientSecretBasic</clientAuthenticationMethod>
                    <nameOfUsernameAttribute>preferred_username</nameOfUsernameAttribute>
                    <openIdProvider>
                        <issuerUri>http://192.168.4.100:8080/realms/master</issuerUri> (6)
                    </openIdProvider>
                </client>
            </oidc>
            ...
        </modules>
        ...
        <sequence> (2)
            <identifier>gui-oidc</identifier>
            <channel>
                <channelId>http://midpoint.evolveum.com/xml/ns/public/common/channels-3#user</channelId>
                <default>true</default>
                <urlSuffix>gui-oidc</urlSuffix>
            </channel>
            <module>
                <identifier>gui-oidc</identifier>
            </module>
        </sequence>
        ...
        <sequence> (1)
            <identifier>gui-login-form</identifier>
            <channel>
                <channelId>http://midpoint.evolveum.com/xml/ns/public/common/channels-3#user</channelId>
                <urlSuffix>gui-login-form</urlSuffix>
            </channel>
            <module>
                <identifier>loginForm</identifier>
            </module>
        </sequence>
        ...
    </authentication>
</securityPolicy>
```

MidPoint Keycloak integration

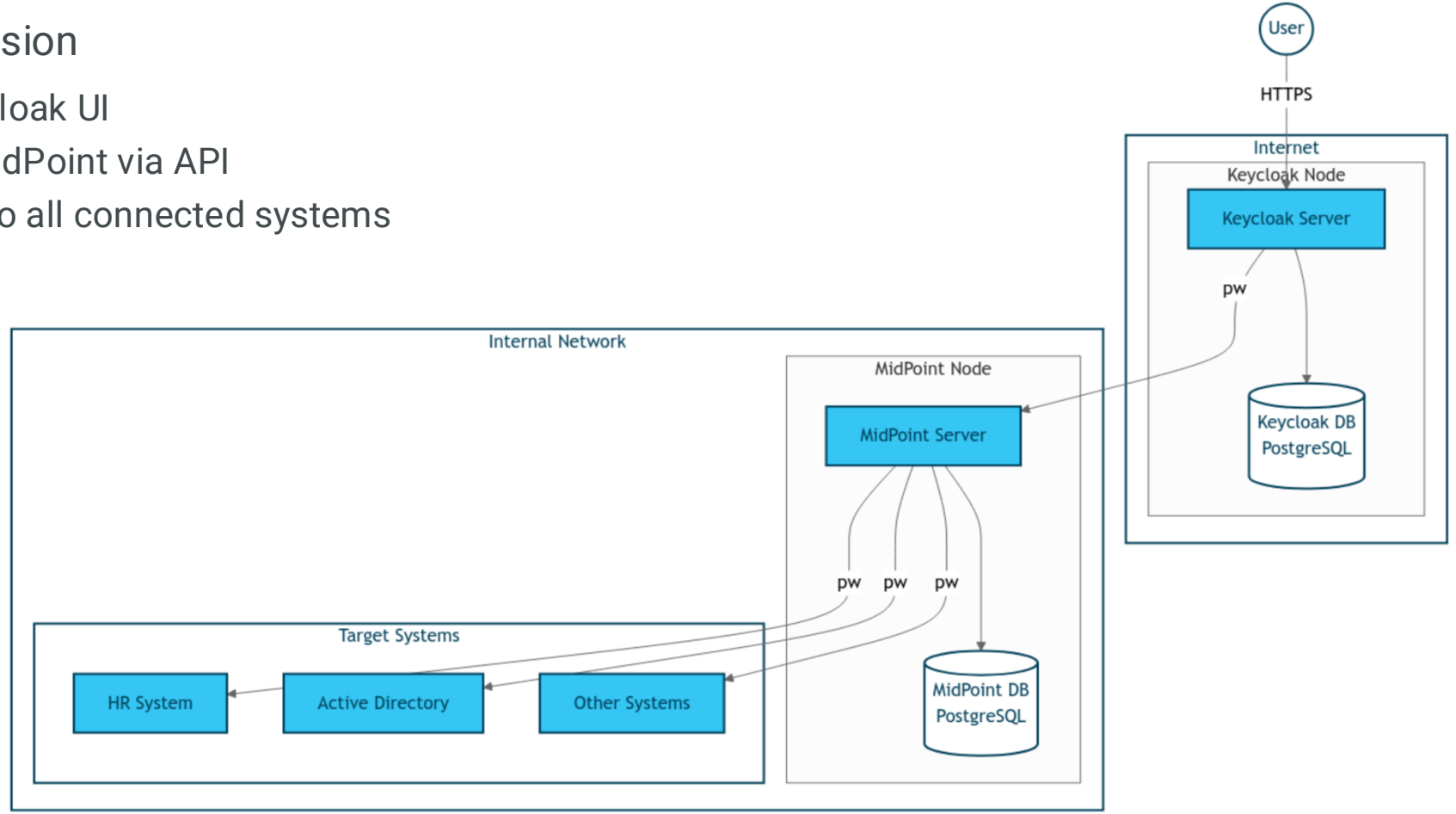
Outbound

- Keycloak connector by NRI
  - https://docs.evolveum.com/connectors/connectors/jp.openstandia.connector.keycloak.KeycloakConnector/
  - Assigning KC roles directly
- Native LDAP federation
  - Assigning KC roles via LDAP groups
- 3rd Party Identity providers like EntraID
  - Assigning KC roles via AD groups

MidPoint Keycloak integration

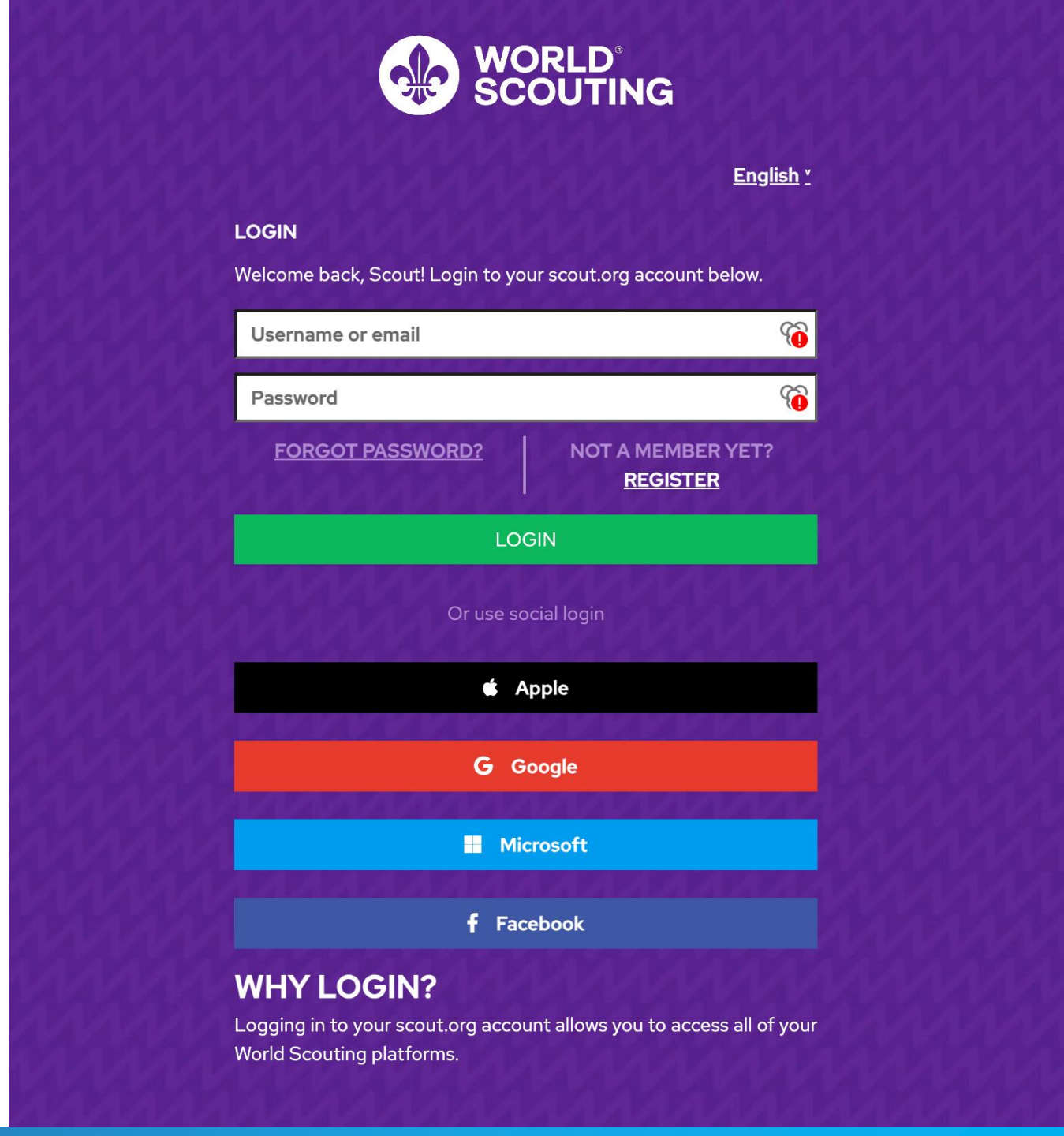
Inbound

- Password provisioning extension
  - Manage password via Keycloak UI
  - Send a new password to midPoint via API
  - Distribute new passwords to all connected systems
- Use cases
  - Password change
  - Forgotten password
  - Account recovery



Keycloak customization

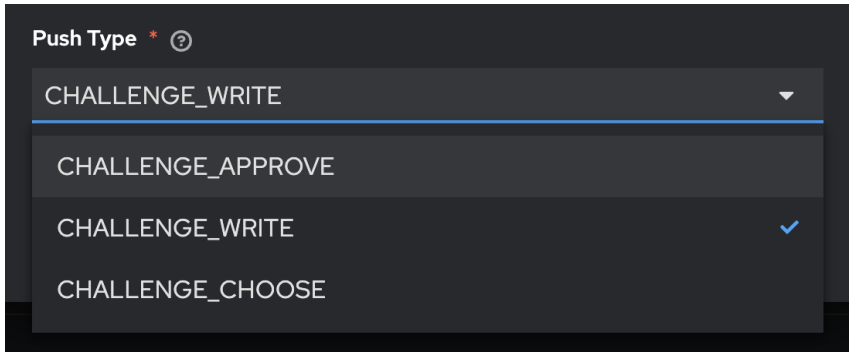
- Authentication flows
  - Login
  - Register
  - Password reset
- Themes
  - Templates (Apache FreeMarker)
  - Custom CSS
  - Custom e-mail templates
- Extensions



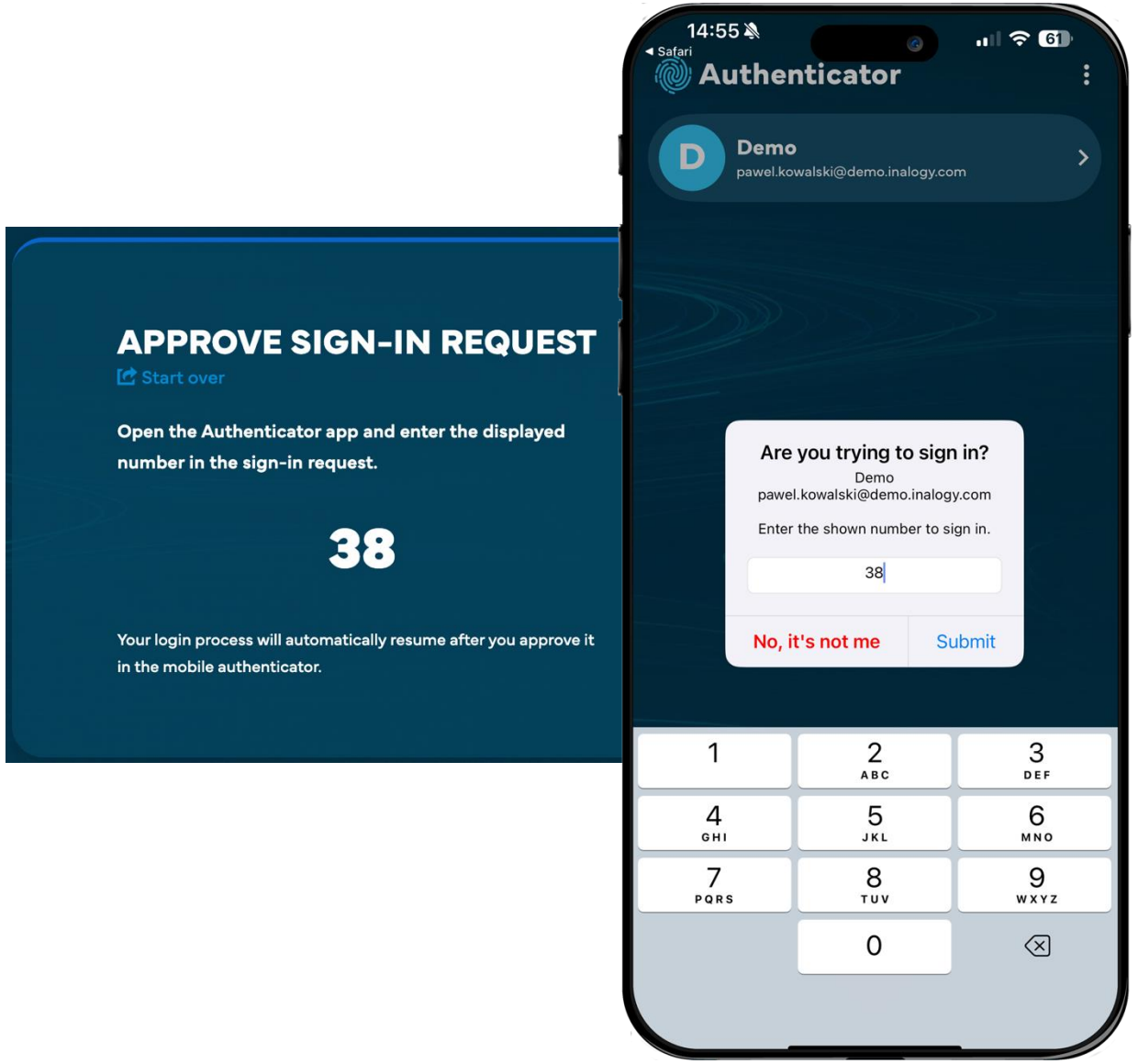
INALOGY

Push Notifications for on-prem AM

- Push notifications for on-prem AM
- Multiple security options



- Inalogy Authenticator available for free

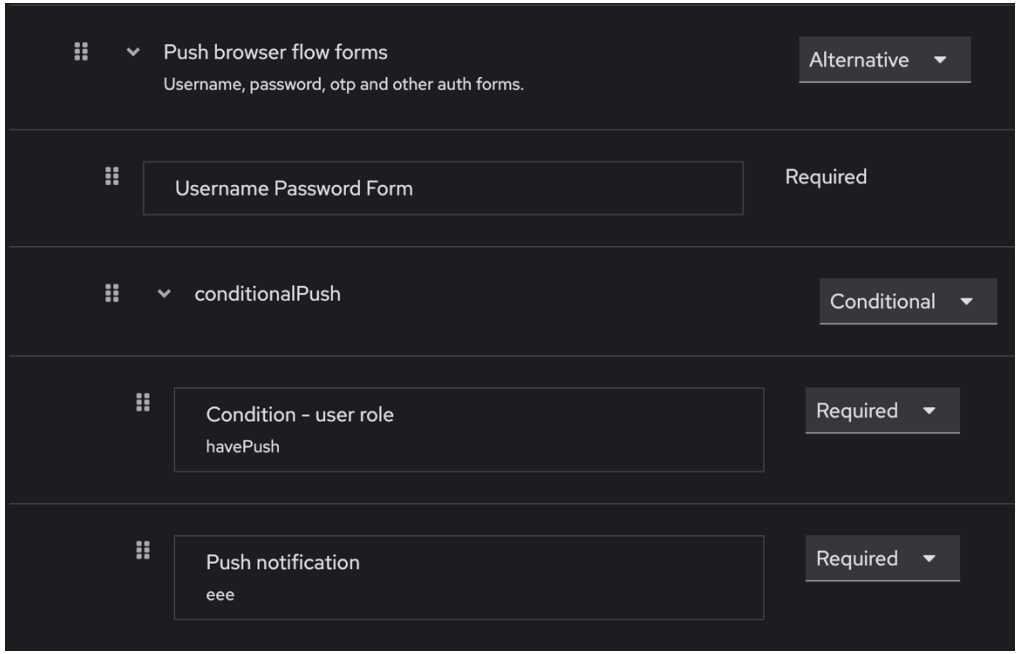


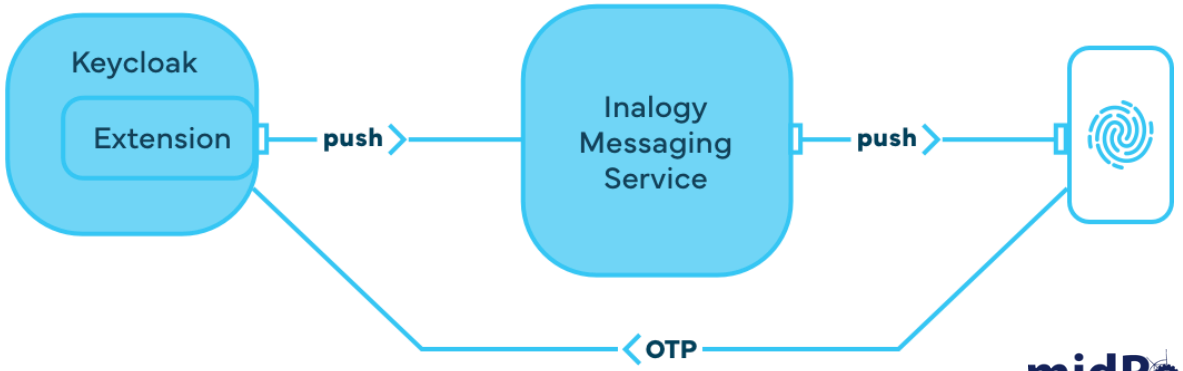
INALOGY

midPoint

Under the hood

- Keycloak extension
  - Configurable directly in Keycloak auth flow wizard
- IMS
  - Cloud messaging service providing a bridge between Keycloak instances and Mobile Authenticators
  - Communicates with Keycloak non-admin API
- Inalogy authenticator
  - Native iOS application
  - Native Android application





INALOGY

midPoint

Demo

- Live Demo
  - Password change
  - Role driven MFA
  - MFA via push notification

INALOGY

Thank you for your attention

Inalogy Authenticator

Follow me on LinkedIn for IAM info
https://www.linkedin.com/in/jan-marcin/

midPoint
MidPoint Integrations: Partner Series
2024