Hyland™

Hyland

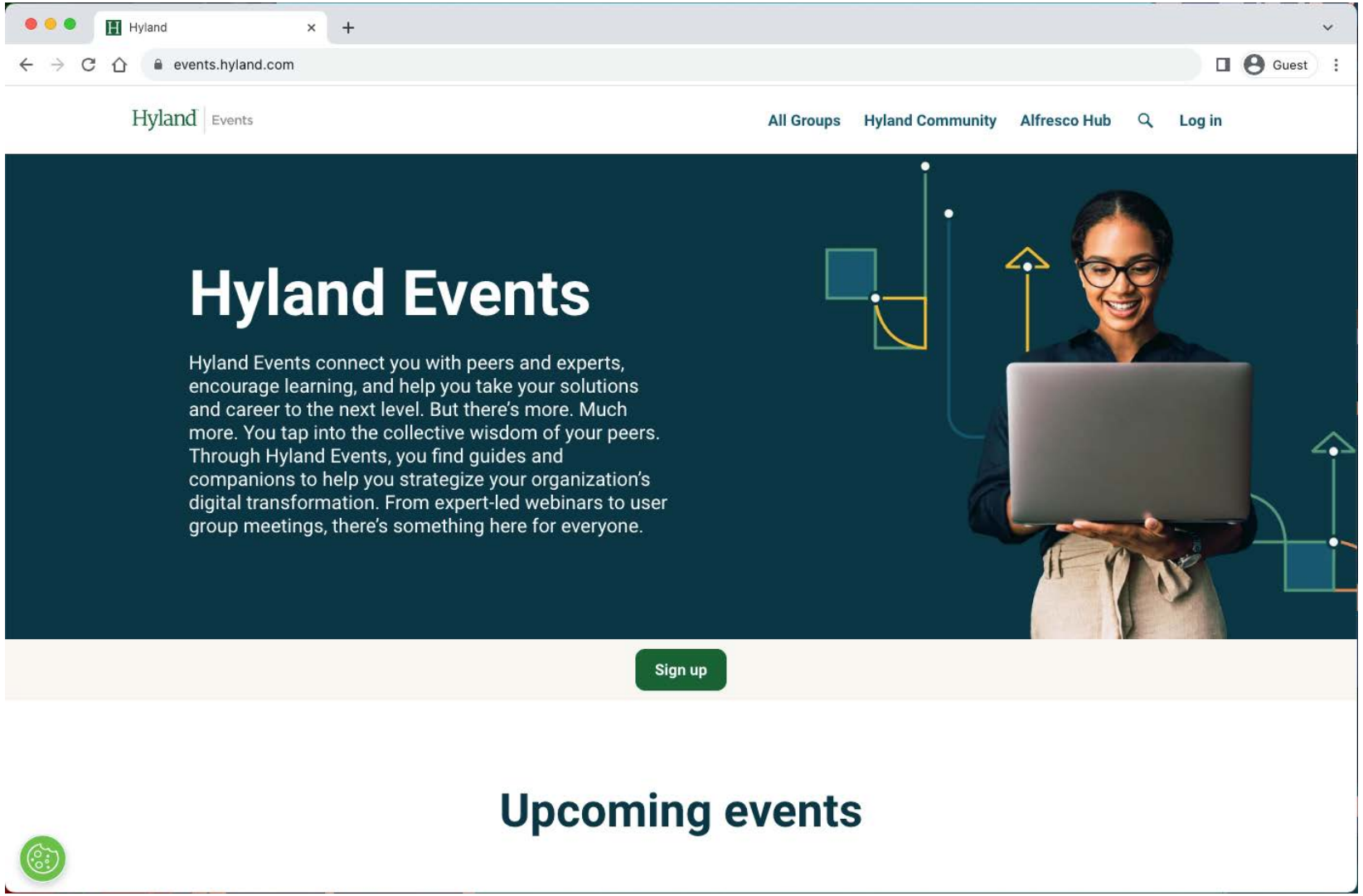
Alfresco
Tech Talk Live #152

December 21, 2023

Agenda

- Community news
- Alfresco Identity and Access Management: Then, Now & Next

Introducing events.hyland.com



Resources

Alfresco

- Hyland participation in DockerCon 2023 (Hub)
- Docker Init With Templates (GitHub)
- APS Action Share deployment (GitHub)
- Alfresco Content Store Selector (GitHub)

Resources to come

- Adapting your logging configuration to log4jv2
- Share to ADF migration guide (thanks Loftux for the feedback!)
- Using Spring Security with ACS 7.4

Collaboration

Blog posts

- Alfresco Repository performance tuning checklist by @abhinavmishra14

Contributions

- https://github.com/Alfresco/alfresco-docker-installer/issues/177 by @iohann95
- https://github.com/aborroy/alfresco-dockerx-builder/issues/9 by @MichaelMuller

Conferences

- https://www.data-community.ch/ - November 14th by our colleagues from dbi services
- https://hacktoberfest.com/ - Celebrate 10 years supporting Open Source
  - No Alfresco projects participating this year

TTL Speakers wanted!

- Take the opportunity to showcase your work with the community
- About Alfresco, Nuxeo, and associated technologies
- Best practices, integration, scaling, cloud, …

Today’s talk

Alfresco Identity and Access Management: Then, Now & Next

Valerio Provaggi
Product Manager at Hyland

Hyland™


Hyland™

Hyland

Then, Now & Next

Alfresco Identity and Access Management

Valerio Provaggi
Product Manager

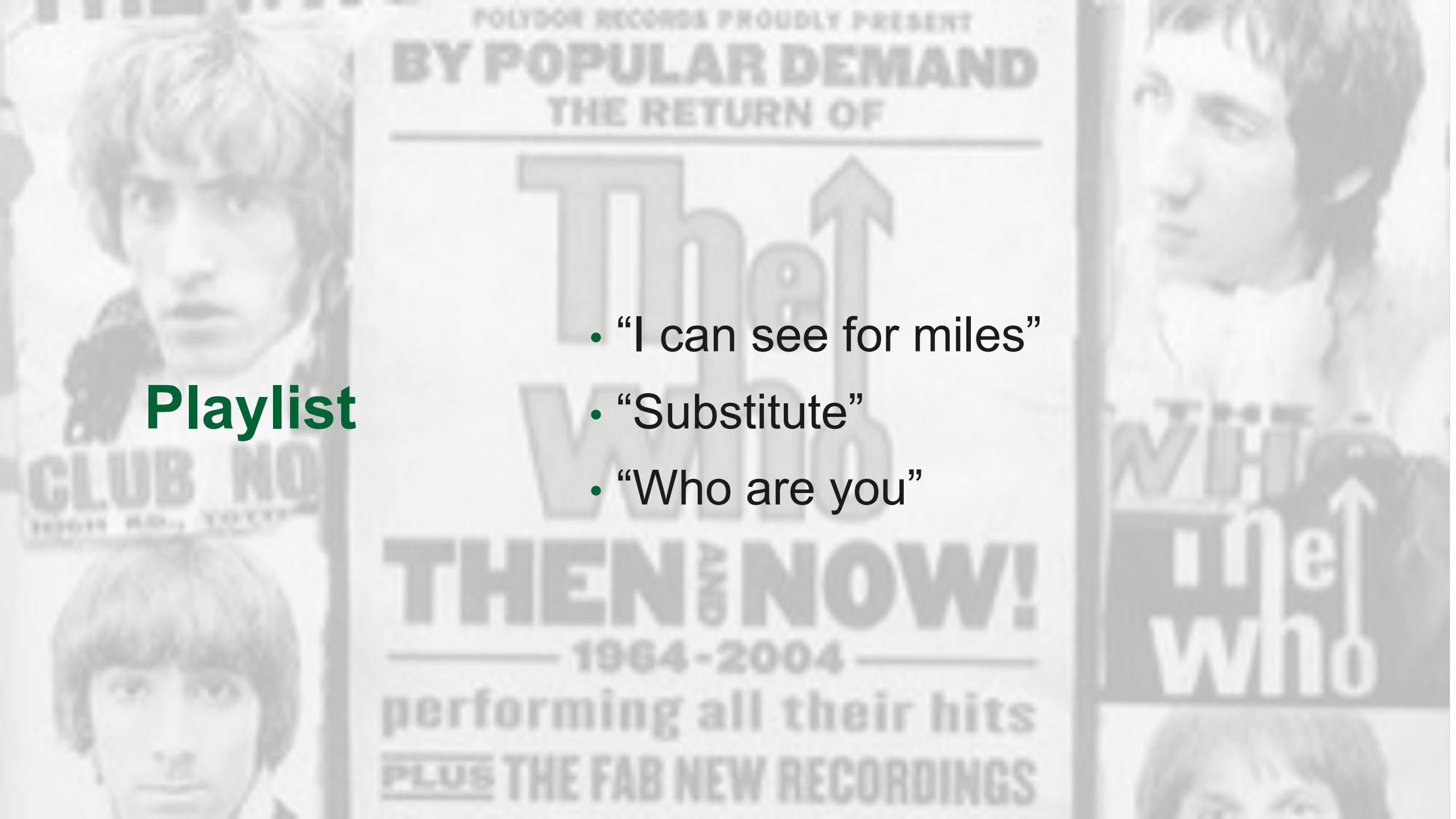
November 28, 2023

Hyland software - Safe harbor statement

All presentations, statements or demonstrations relating to Hyland's plans, directions, and intent are subject to change or withdrawal without notice at Hyland's sole discretion. Information regarding potential future products is intended to outline Hyland's general product direction and should not be relied on in making a purchasing decision.

This information is not a commitment, promise, or legal obligation to deliver any material, code or functionality and may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at Hyland's sole discretion.

All such information is confidential information of Hyland, and subject to the confidentiality obligations between you and Hyland. Customers who purchase Hyland products or services should make their purchase decisions upon services, features and functions that are currently available.



Playlist

- “I can see for miles”
- “Substitute”
- “Who are you”

“I Can See For Miles”

- The journey
- Design principles
- Two configurations

The journey - IAM

Connected

Full reliance on OIDC/OAuth2
SCIM as alternative to LDAP sync

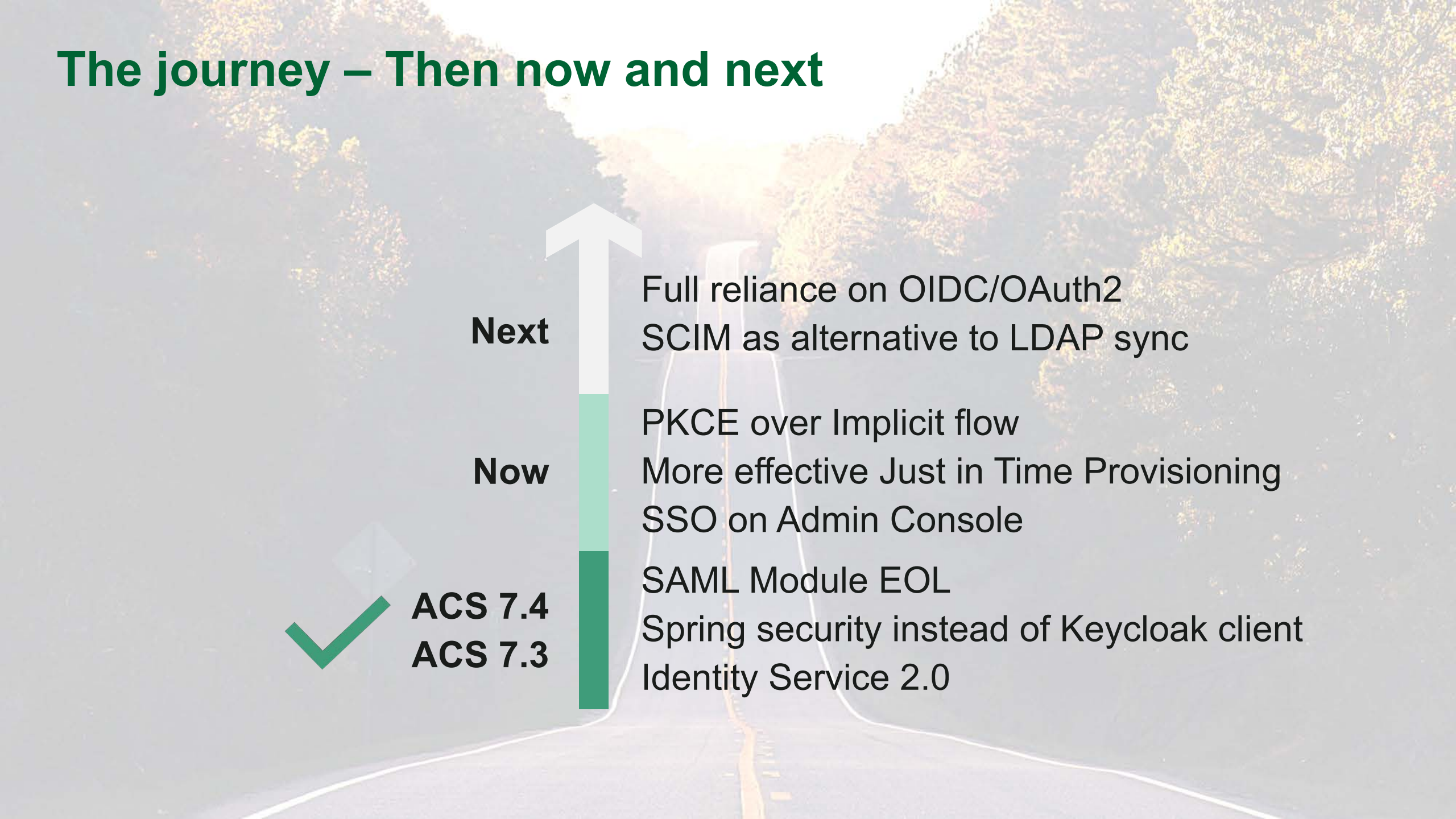
Consistent

More effective Just in Time Provisioning
SSO on Admin Console
PKCE over Implicit flow

More secure

SAML Module EOL
Spring security instead of Keycloak client
Identity Service 2.0

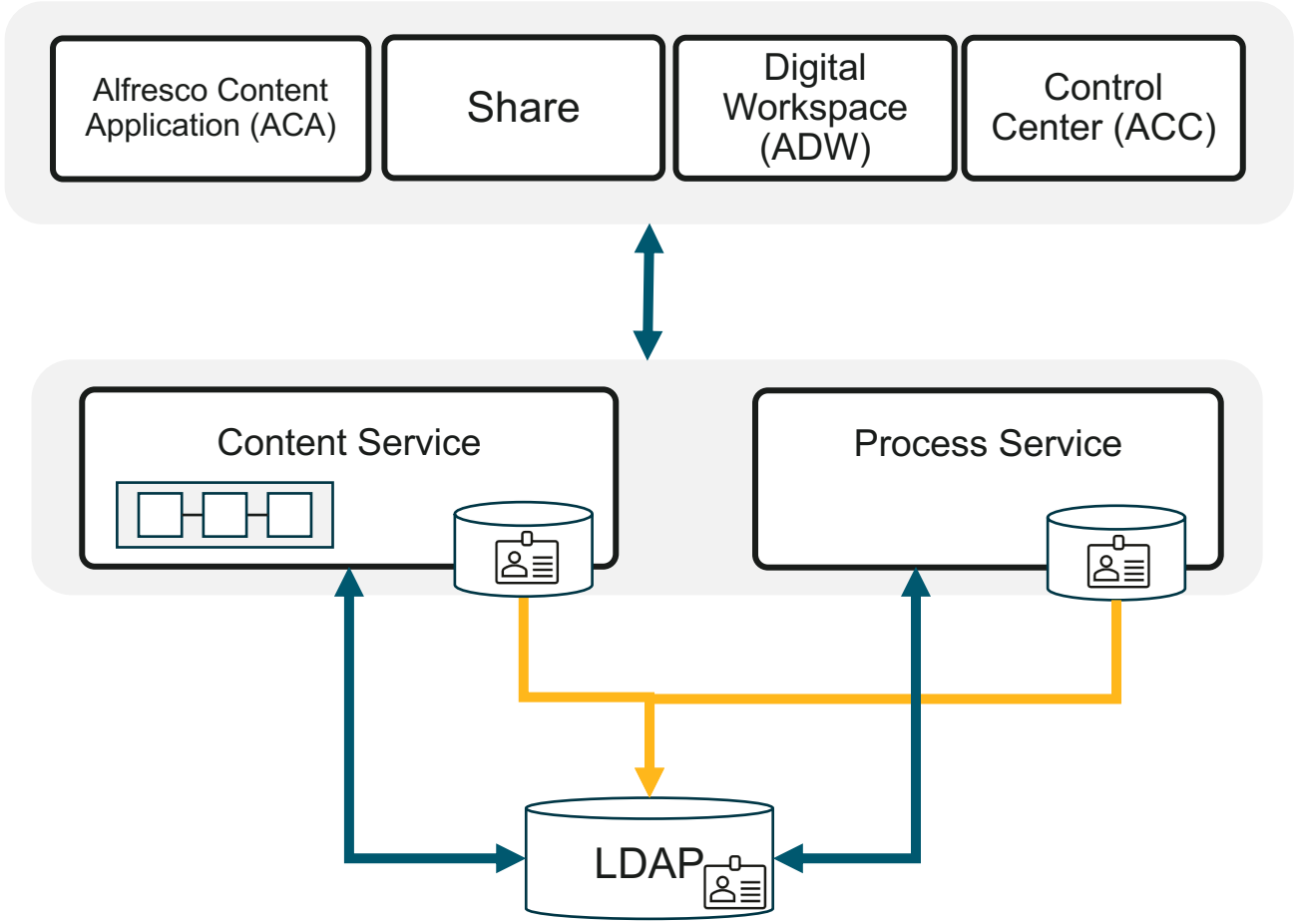
The journey – Then now and next



Design Principles

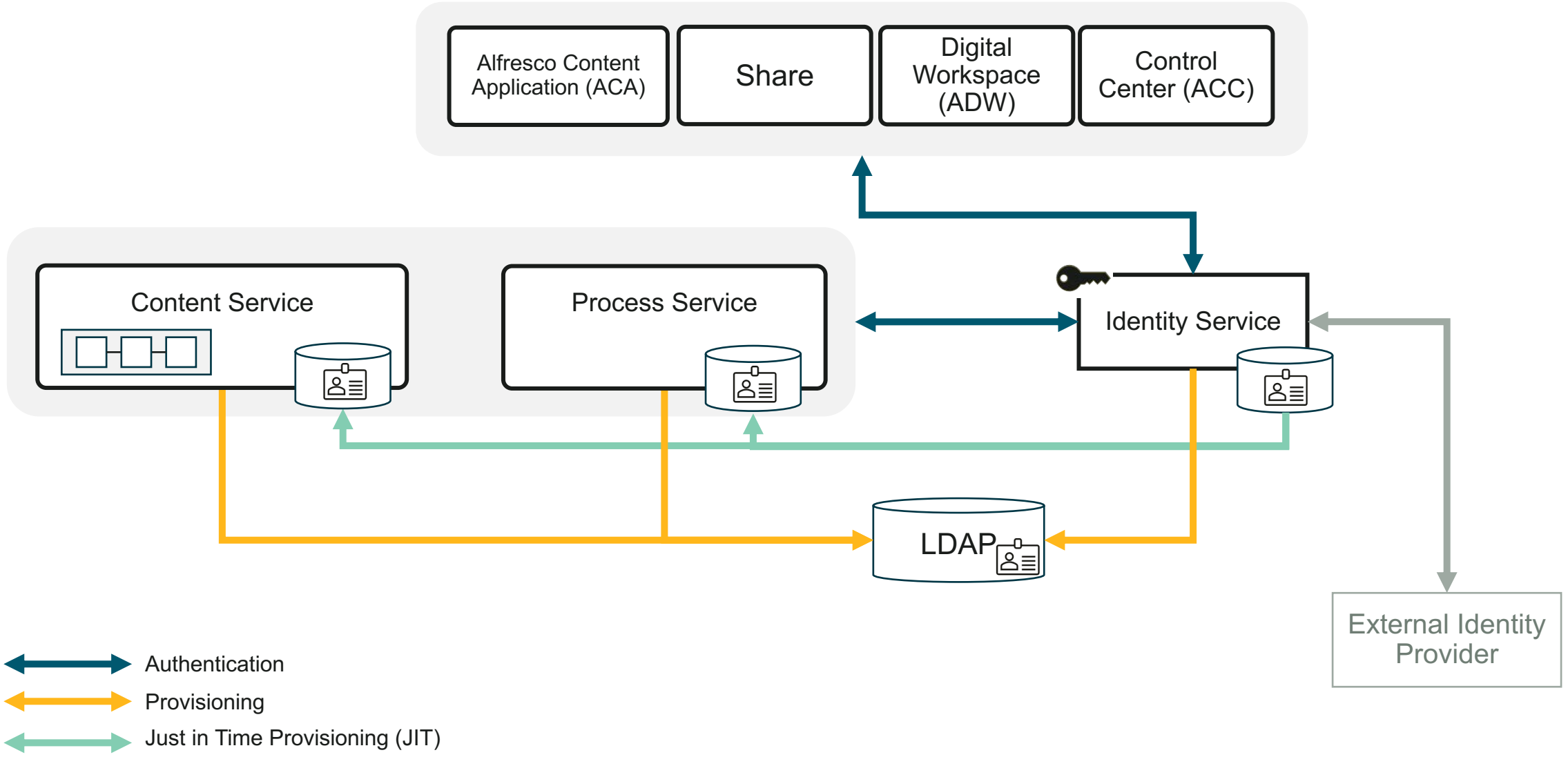
- Rely on standards
- Single source of truth

Two configurations - Basic Authentication



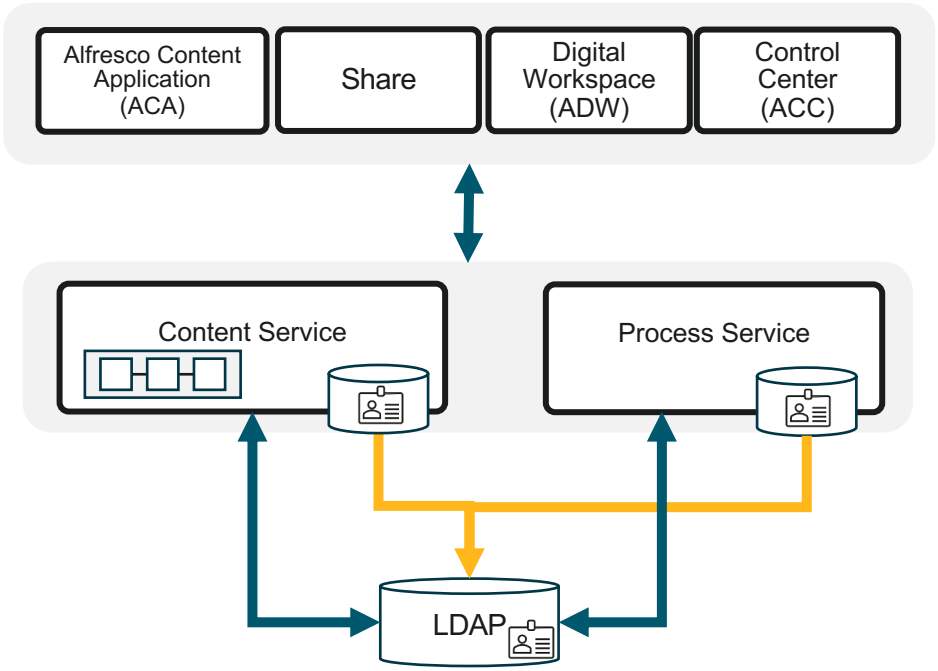
https://docs.alfresco.com/content-services/7.4/admin/auth-sync/

Two configurations - SSO

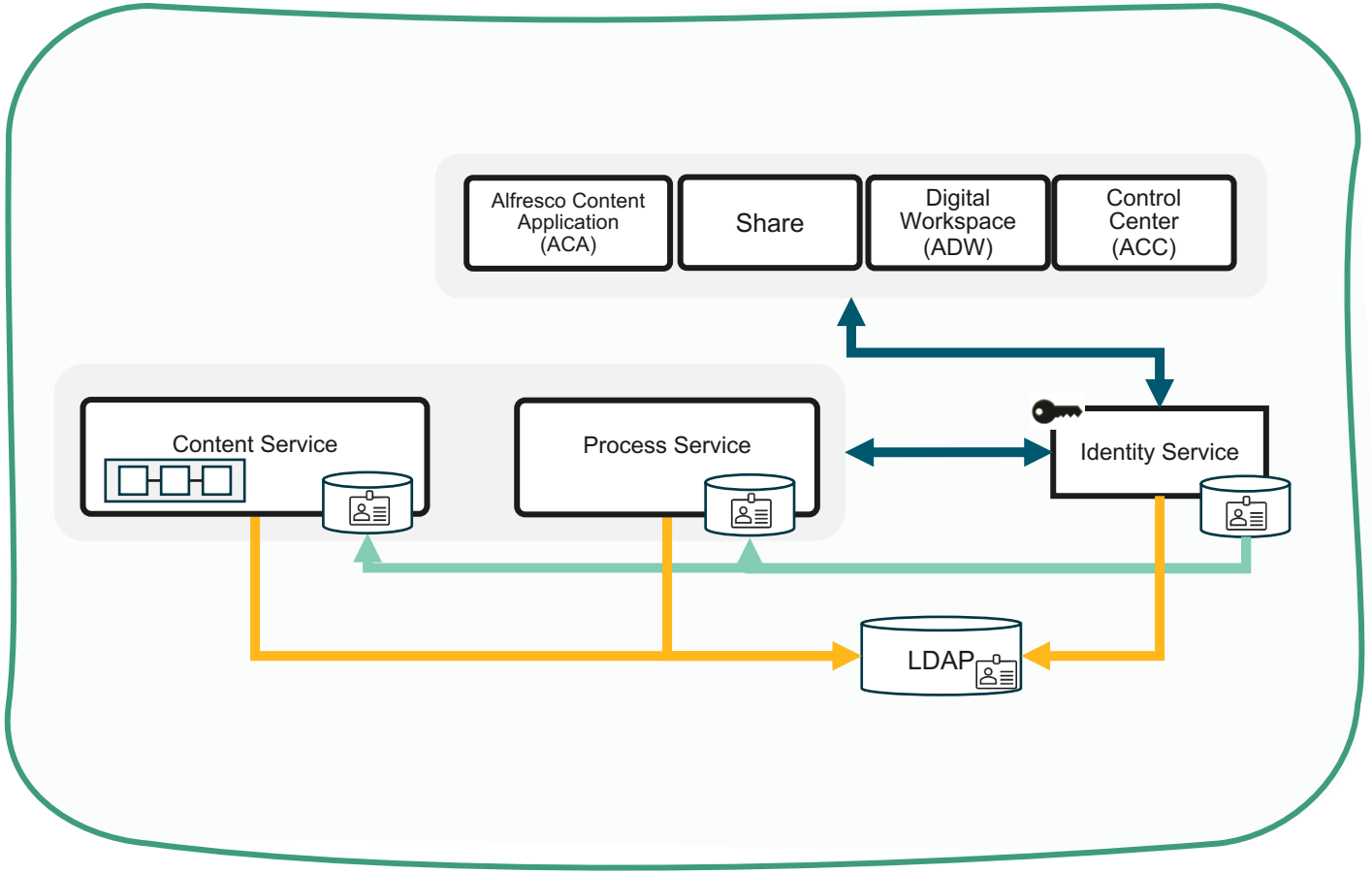


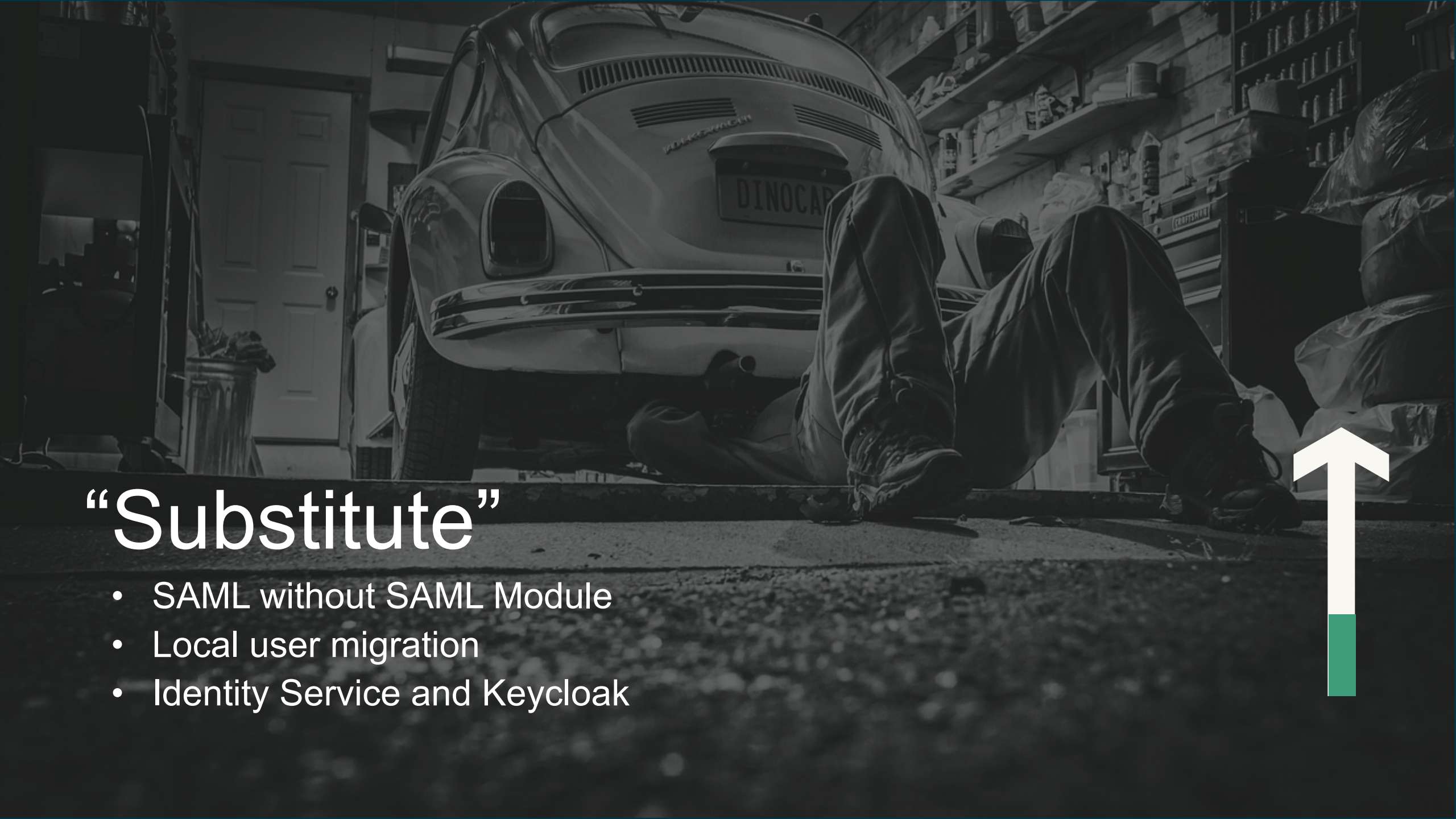
https://docs.alfresco.com/identity-service/latest/tutorial/sso/

Basic Auth still supported



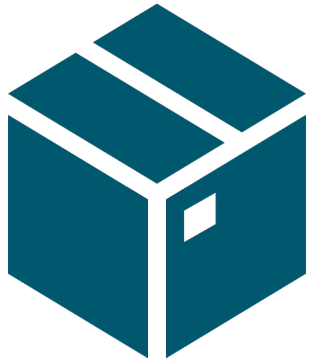
Focus on SSO





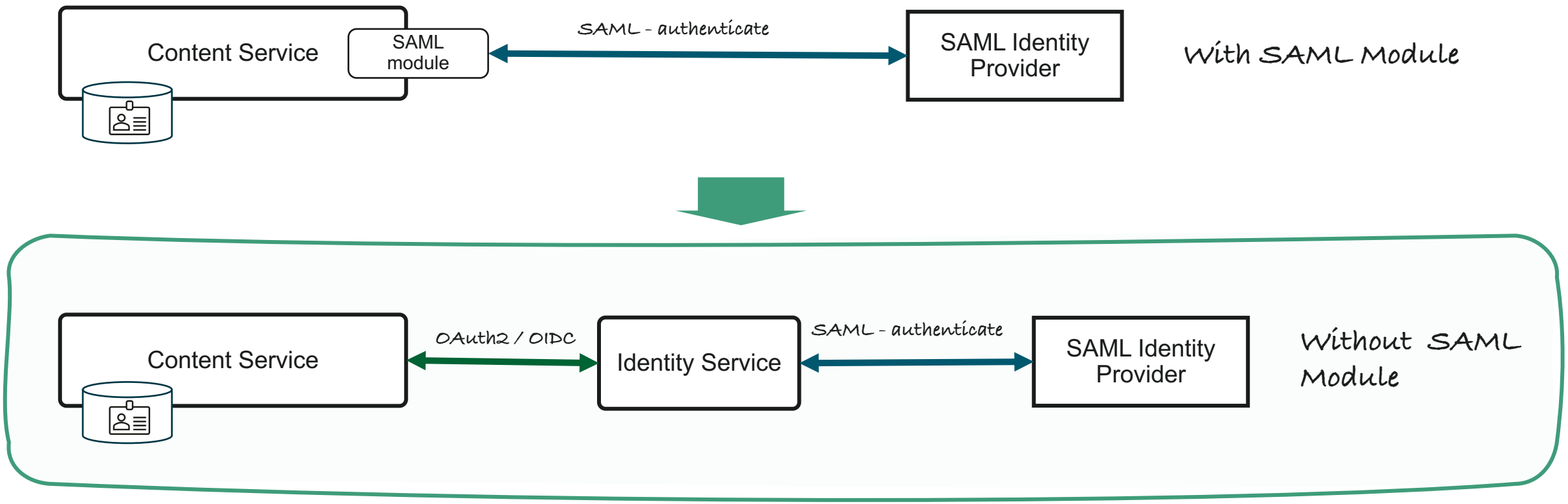
“Substitute”

- SAML without SAML Module
- Local user migration
- Identity Service and Keycloak

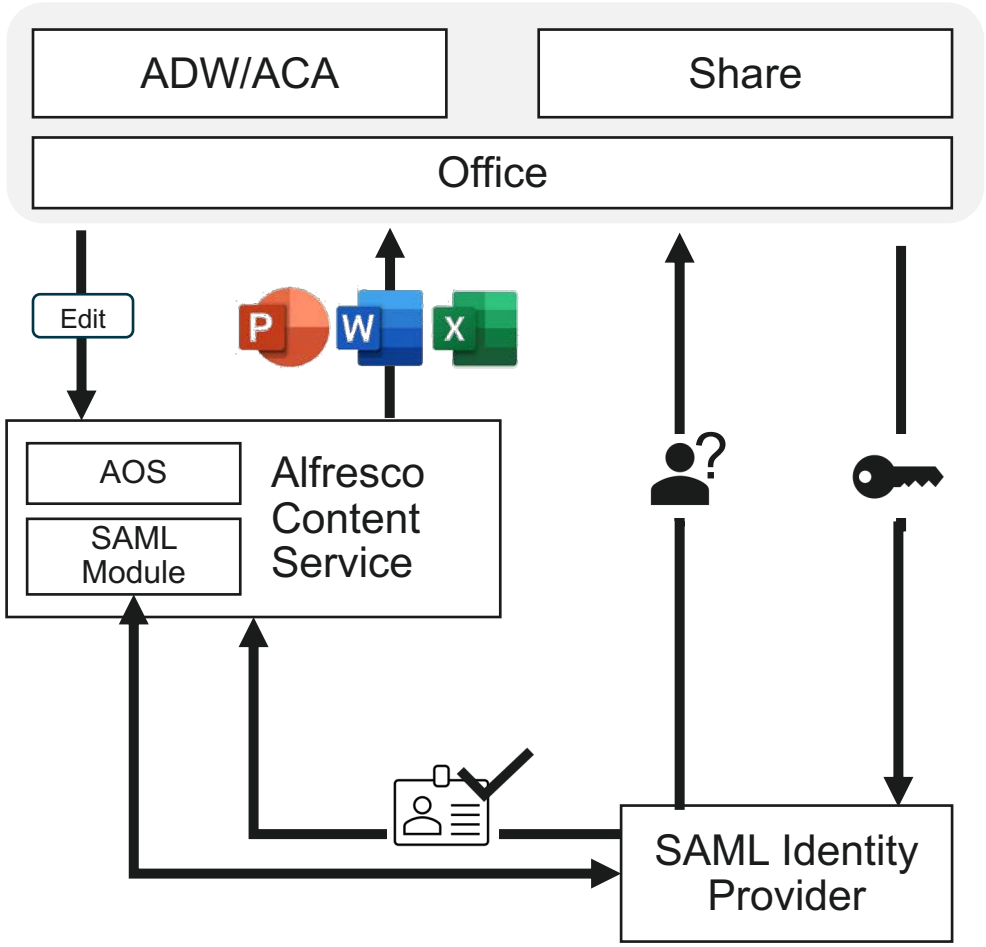


ACS 7.3
SAML Module Removal

SAML SSO Without SAML Module

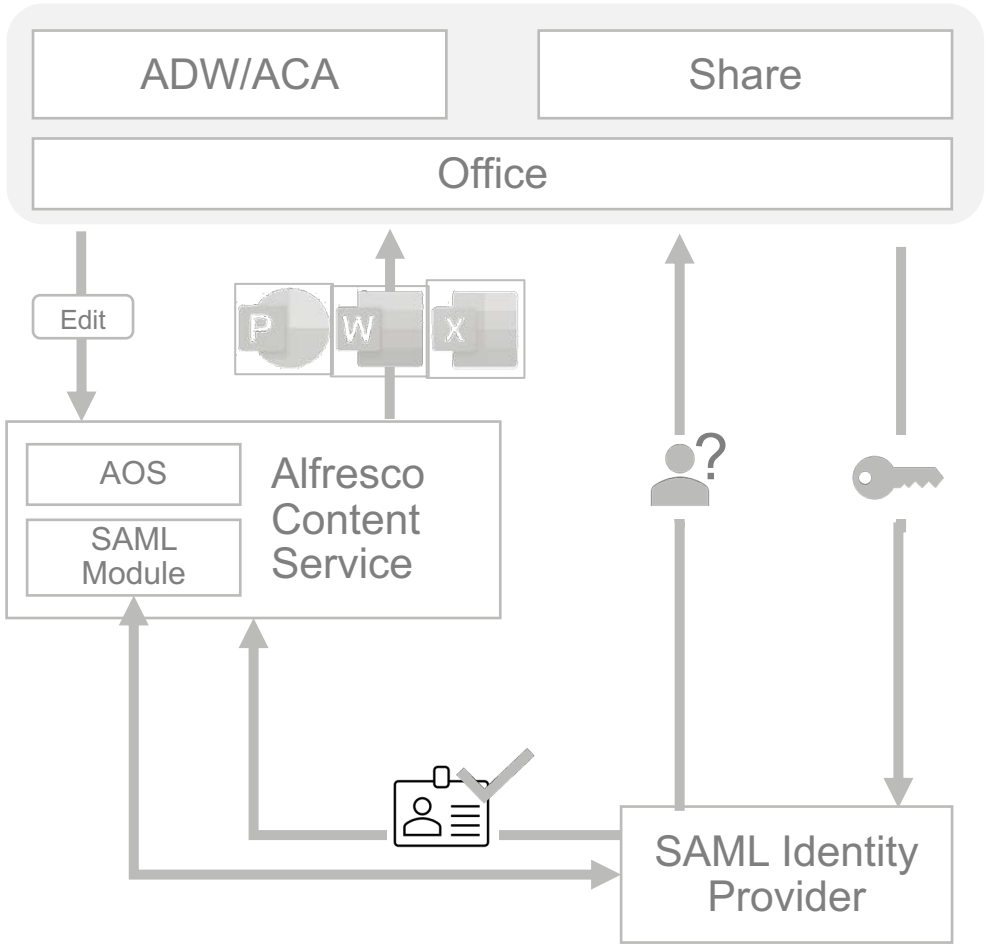


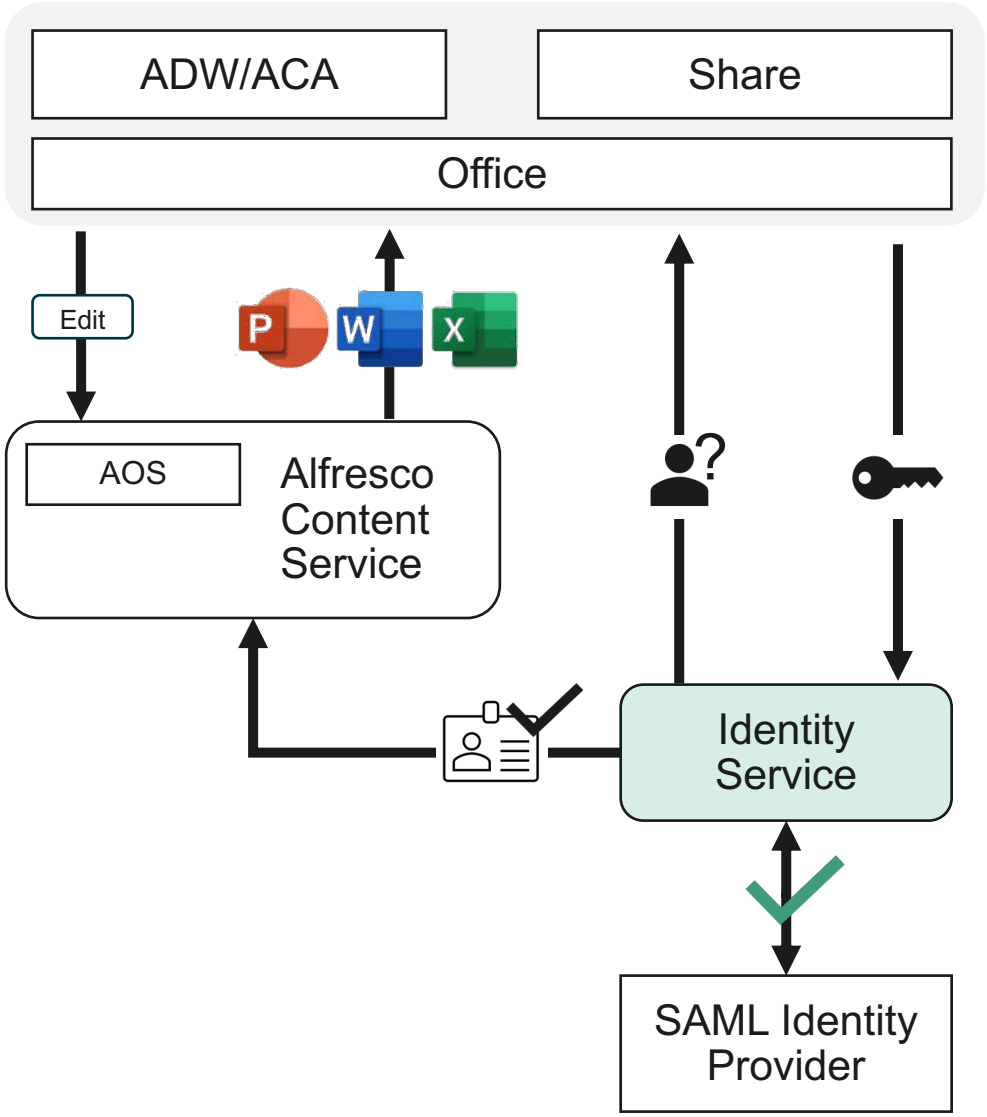
7.2 SAML SSO with SAML Module



- Choose to edit in MSOffice
- Add a Sharepoint Location

7.3+ SAML SSO with SAML Module





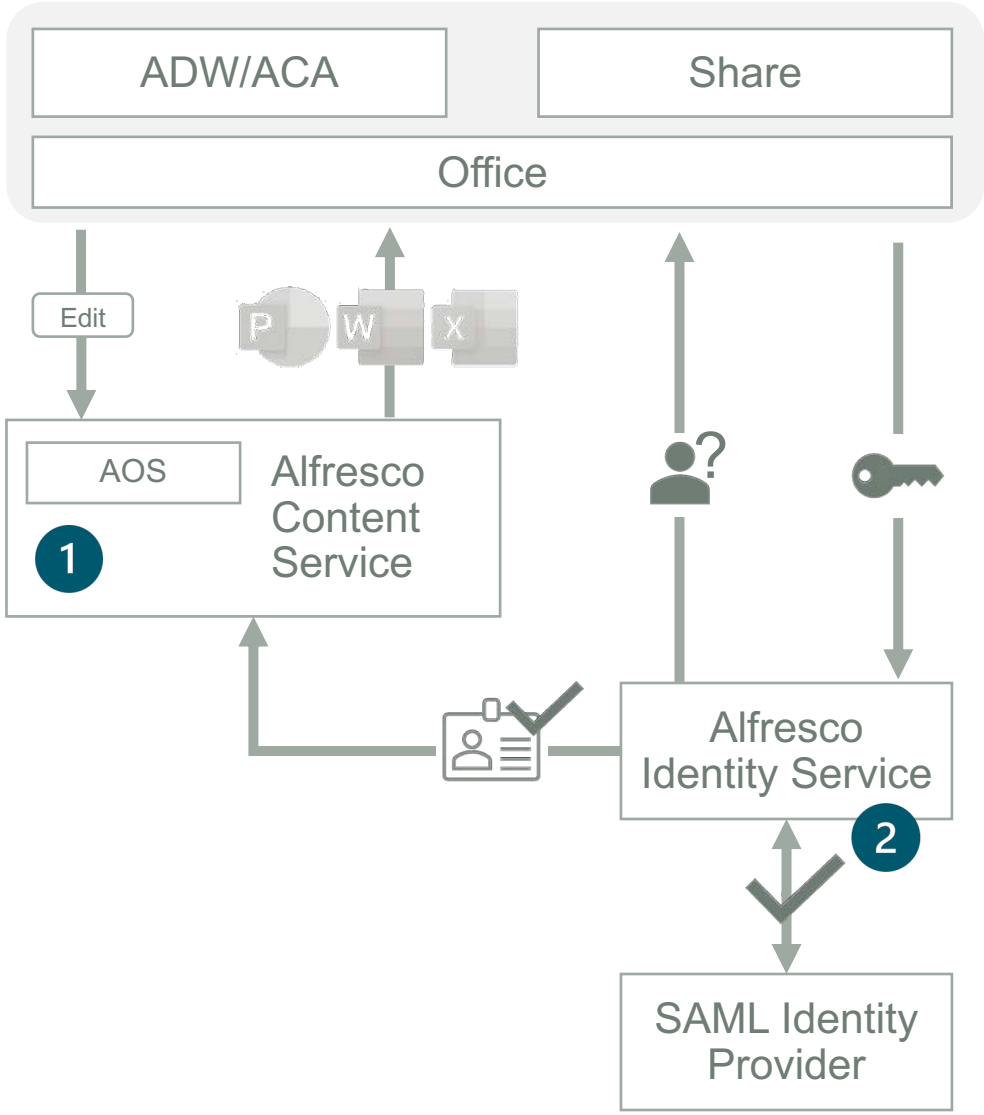
Where I Can find more information?

Admin

1. **Configured secure authentication for AOS**
   - Configure Identity Service in the authentication chain. (https://docs.alfresco.com/content-services/latest/admin/auth-sync/#configure-identity-service)
2. **Configured Identity Service with SAML Identity Provider**
   - SSO Guide v2. (https://docs.alfresco.com/identity-service/1.8/tutorial/sso/saml/)

Single Sign On Guide v2 (ACS 7.3+)

Single Sign On Guide v1 (ACS 7.2 and older)



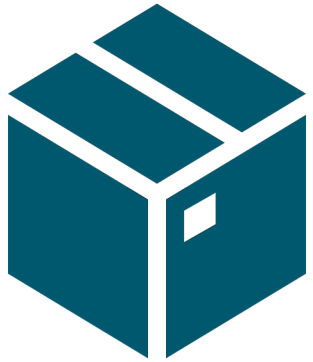
What I get vs what I give away

What I get

- More secure solution
  - Red hat + big community
- More features:
  - Multiple SAML identity provider
  - Easier configuration
    - From 3 forms to configure to 1 in keycloak.
    - Leverage identity provider SAML descriptor

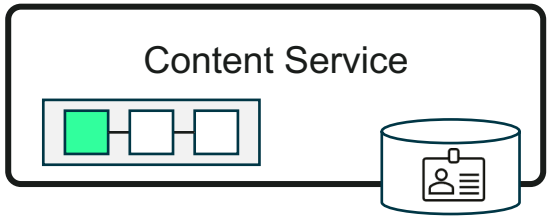
What I give away

- Simpler deployment



ACS 7.3
Enforcing single source of truth

Enforcing Single Source of Truth on SSO



When Identity Service is set in the authentication chain

Share

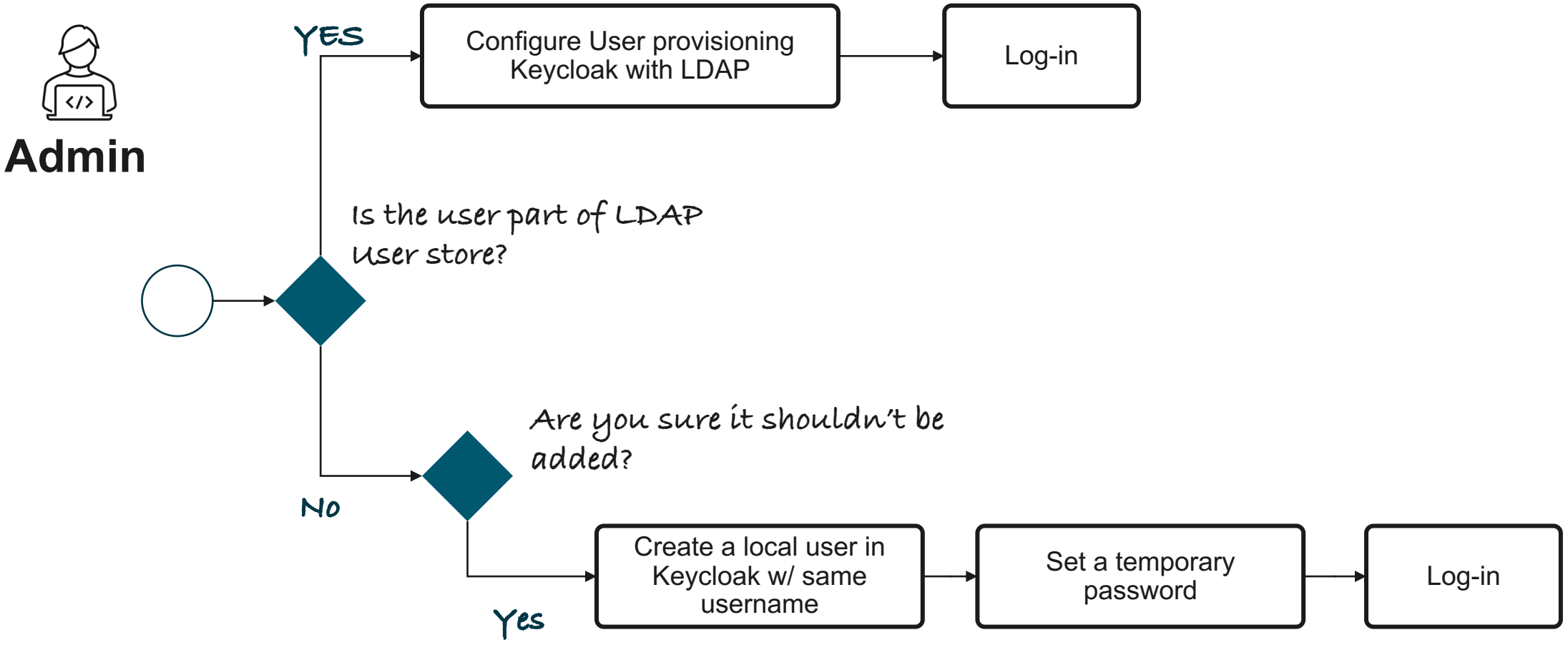
Control Center (ACC)

Admin UI User creation / Deletion disabled

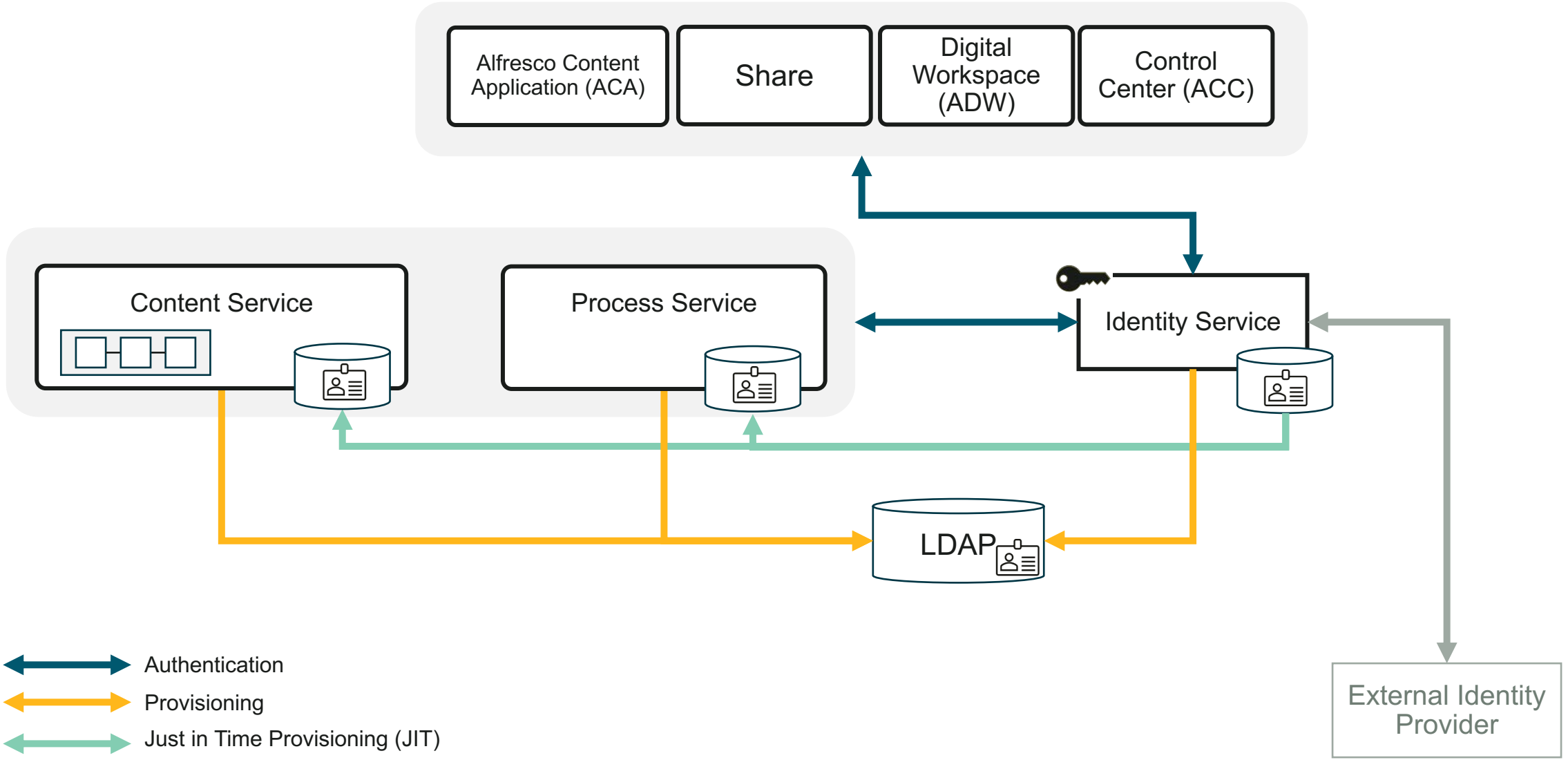
Identity Service

Identity Service is the single source of truth of User Authentication

Local user migration



SSO


Alfresco Content Application (ACA)
Share
Digital Workspace (ADW)
Control Center (ACC)
Content Service
Process Service
Identity Service
LDAP
External Identity Provider
Authentication
Provisioning
Just in Time Provisioning (JIT)

ACS 7.4

Spring Security
Keycloak client

IDS 2.0

Upgrade to
Keycloak 21

The need of Identity Service 2.0

Migrating to Quarkus distribution

Migrate to the new Quarkus distribution from the legacy WildFly distribution

In Keycloak 17 the default distribution is now powered by Quarkus, while the legacy WildFly powered distribution will still be around until June 2022 we highly recommend starting the migration as soon as possible.

The new distribution introduces a number of breaking changes, including:

- Configuring Keycloak has significantly changed
- Quarkus is not an application server, but rather a framework to build applications
- `/auth` removed from the default context path
- Custom providers are packaged and deployed differently
- A new operator and CRDs for Kubernetes and OpenShift

Before undertaking the migration we highly recommend reading through the new Server Guides to understand how to install and configure the new distribution.

https://www.keycloak.org/migration/migrating-to-quarkus

Why releasing a new version with an end of life?

Alfresco Identity Service end of life

AL Andrew Leach (Hyland Employee) | August 24, 2023 | 4 | 170

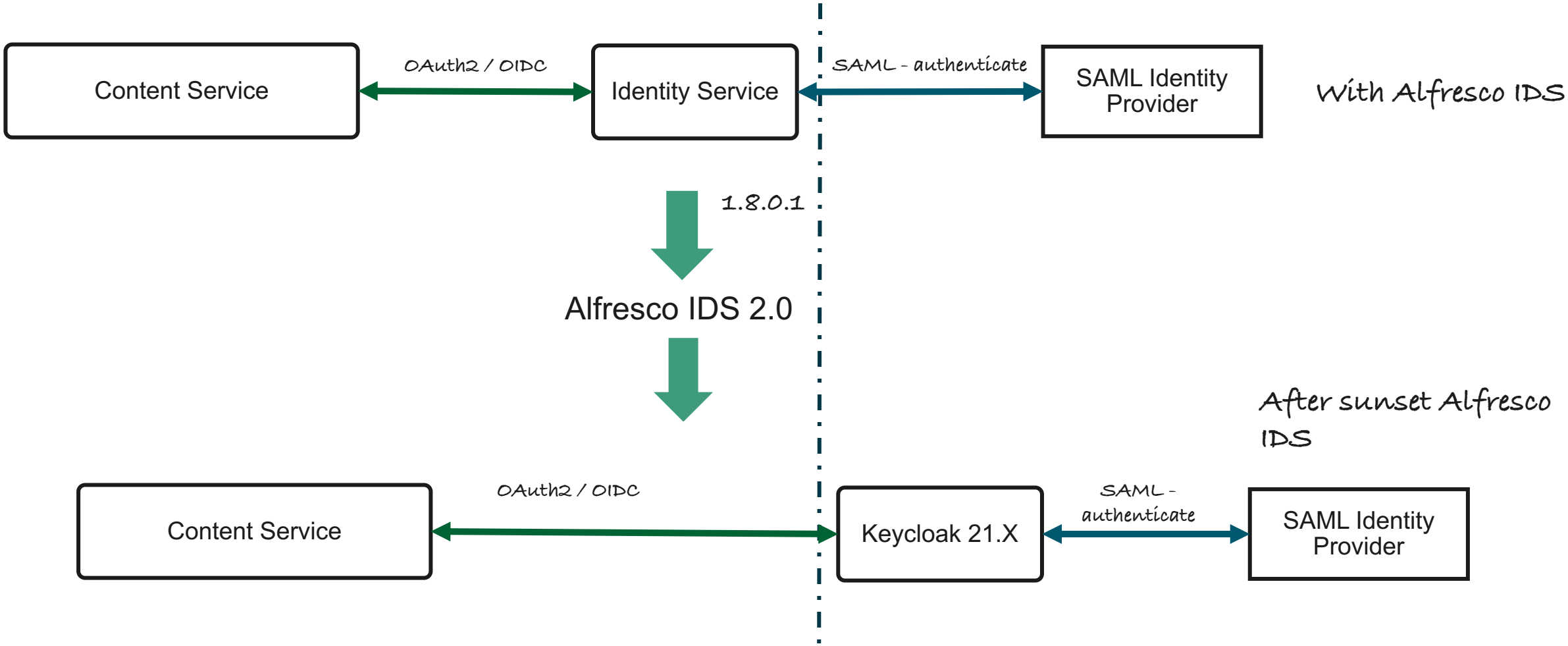
At Hyland, we regularly assess our product offerings to ensure they serve customer needs, meet industry requirements and align with our market focus. After review and with the upcoming release of Alfresco Content Services (ACS) 23.1* in Q4 2023, Hyland has chosen to begin the retirement process for **Alfresco Identity Service (IDS)**. The end-of-life date is Sunday, September 1, 2024. More information is shared below.

Replacement option

Moving forward, we suggest customers use the original Keycloak project, a mature open-source project backed by Red Hat. Currently, Alfresco IDS is a thin customized layer on top of Keycloak. Because of this, customers will not lose capabilities when transitioning from Alfresco IDS to Keycloak and the user experience will not be disruptive for existing customers.

Compatible and supported versions of Keycloak will be listed in the official documentation compatibility matrix.

IDS 2.0 -> Keycloak

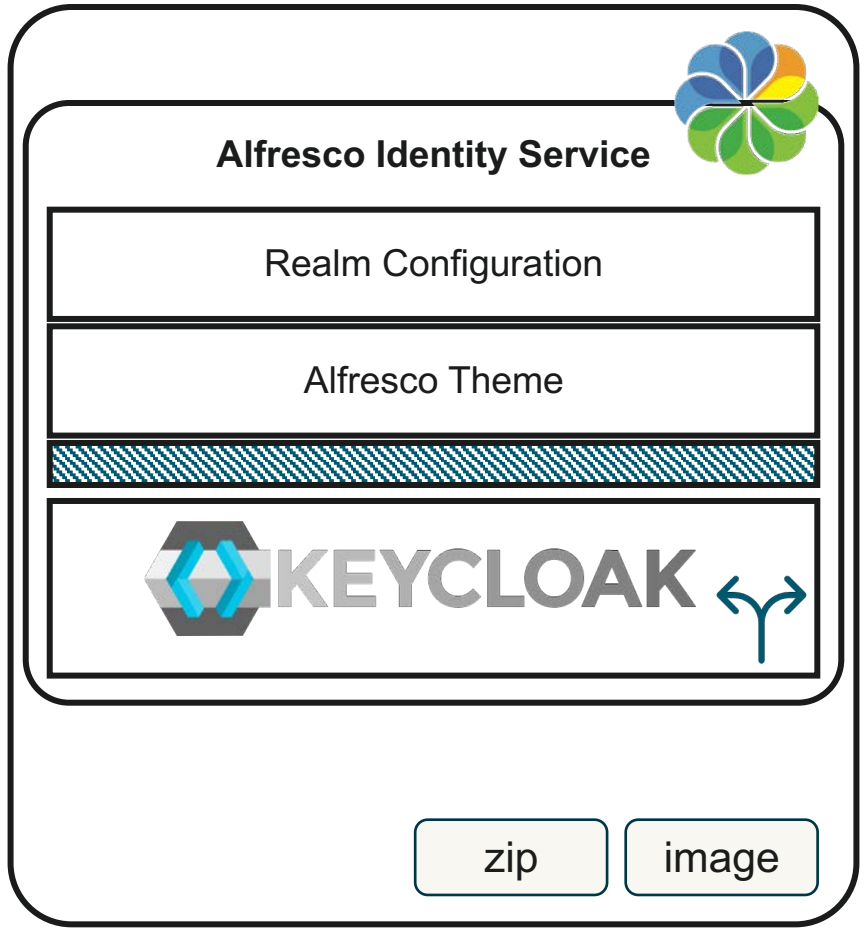


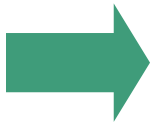
Alfresco Identity Service – X ray

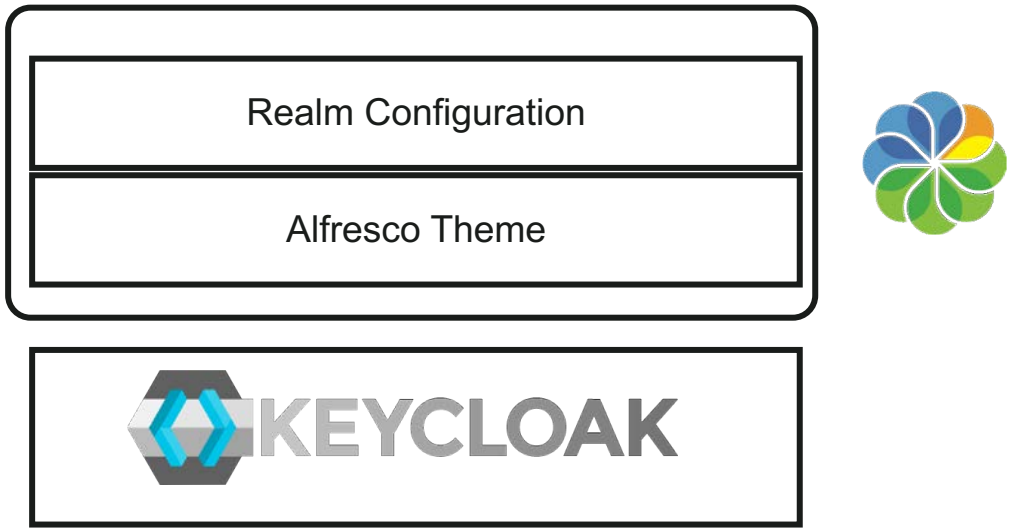
Role:
A central component responsible for identity-related capabilities needed by other Alfresco software, such as managing users, groups, roles, profiles, and authentication

https://github.com/Alfresco/alfresco-identity-service

Same role, better solution





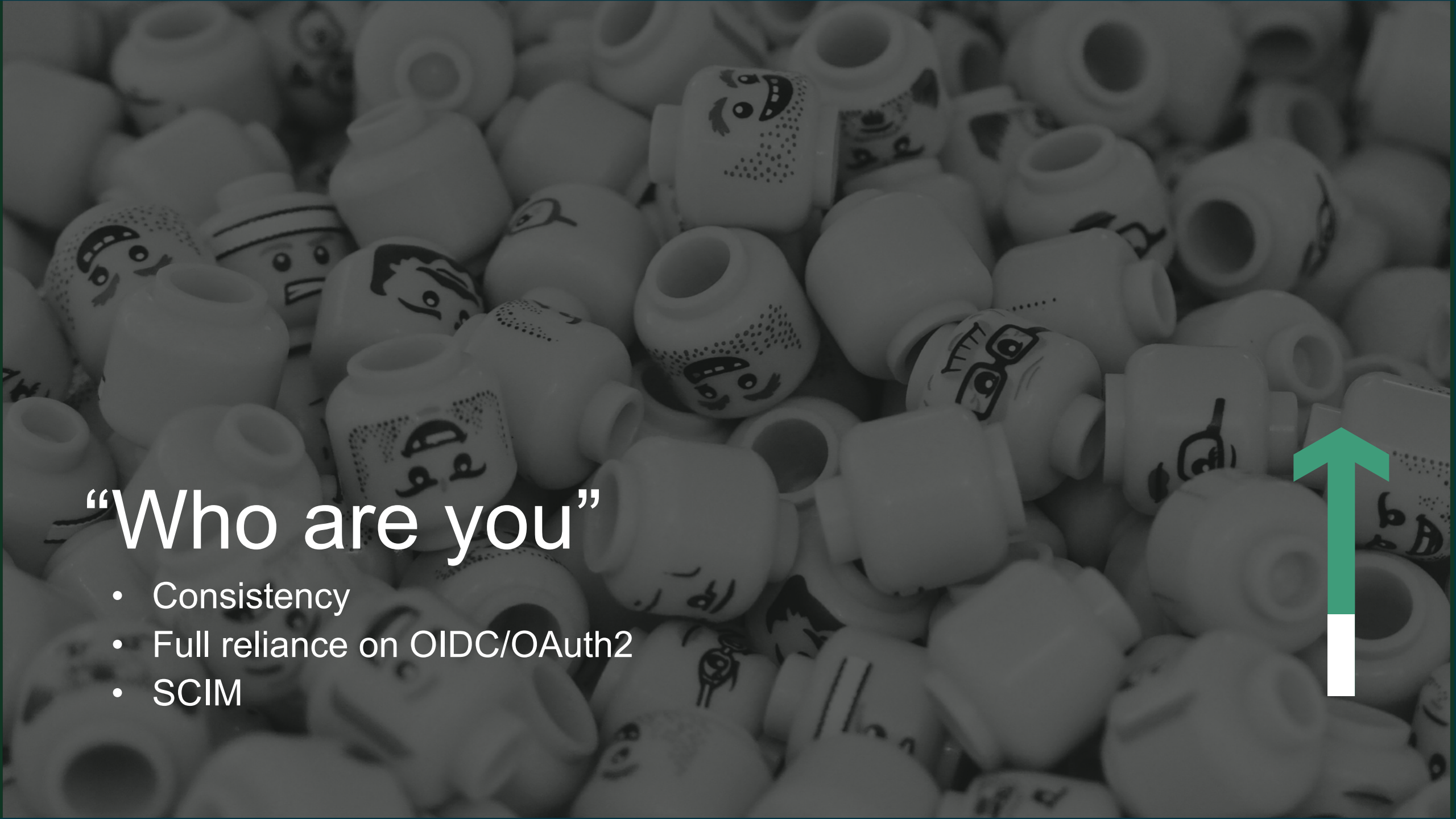


Keycloak distribution

- https://www.keycloak.org/downloads

Migration from Identity Service 2.0 to Keycloak

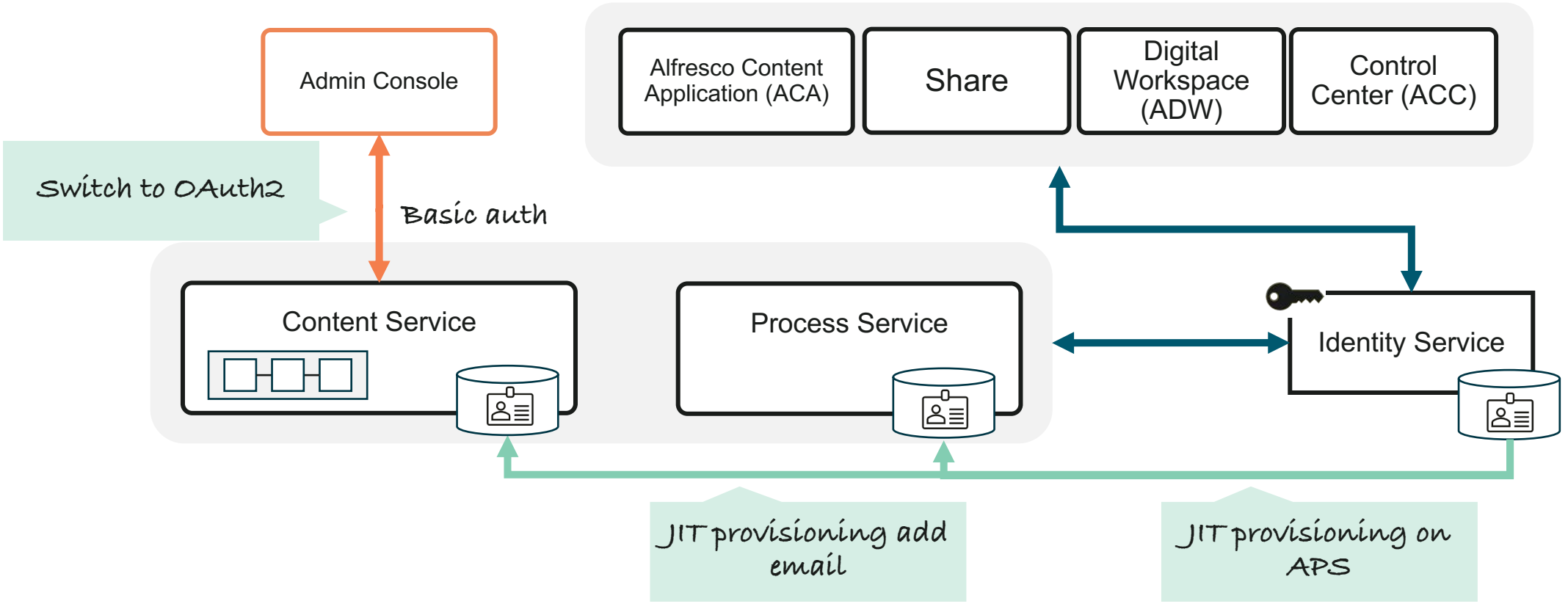
- Main actions
  - Theme configuration - https://github.com/Alfresco/alfresco-keycloak-theme/releases
  - Realm configuration



“Who are you”

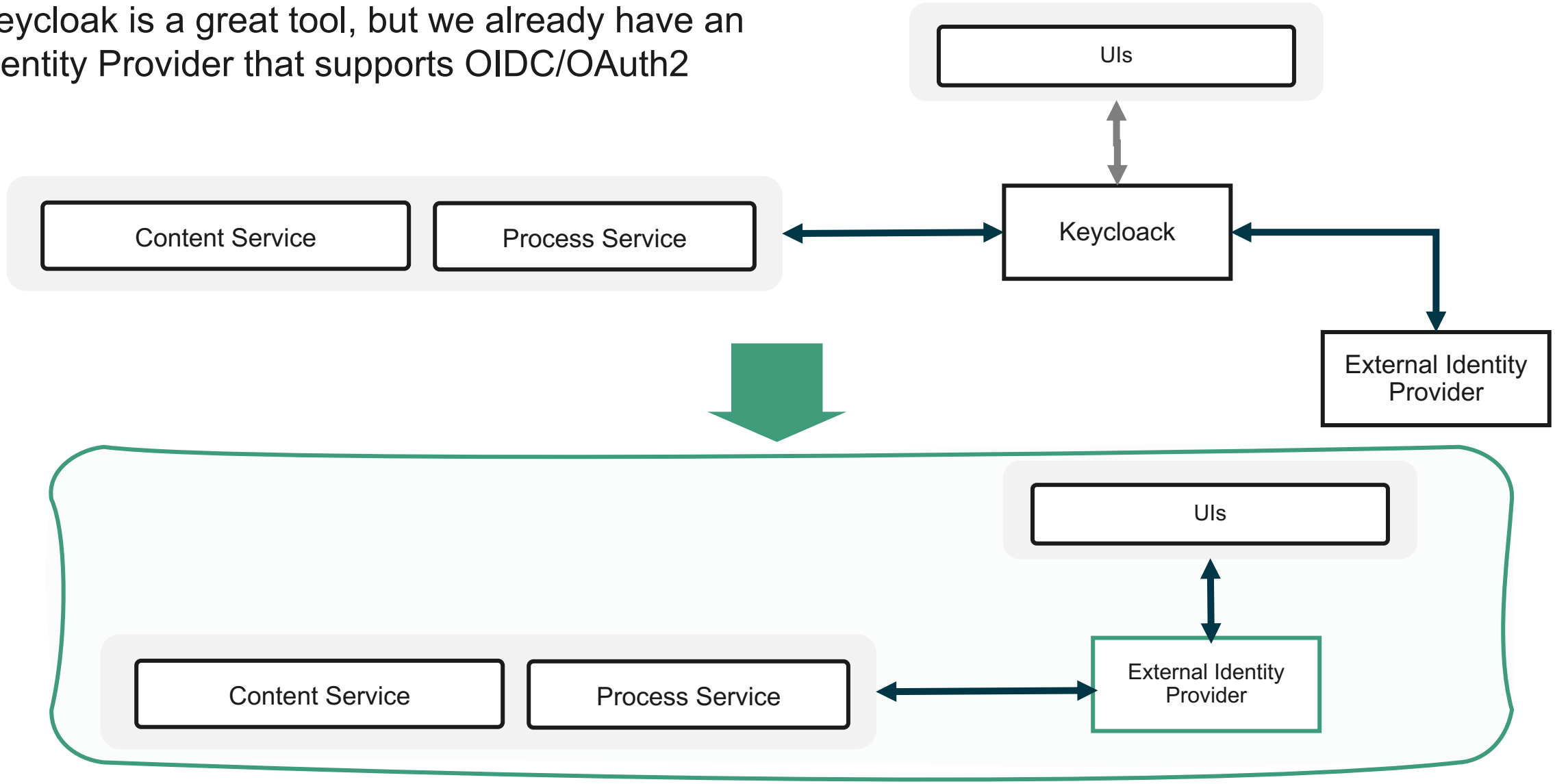
- Consistency
- Full reliance on OIDC/OAuth2
- SCIM

Consistency



Fully reliant on OIDC/OAuth2

Keycloak is a great tool, but we already have an Identity Provider that supports OIDC/OAuth2

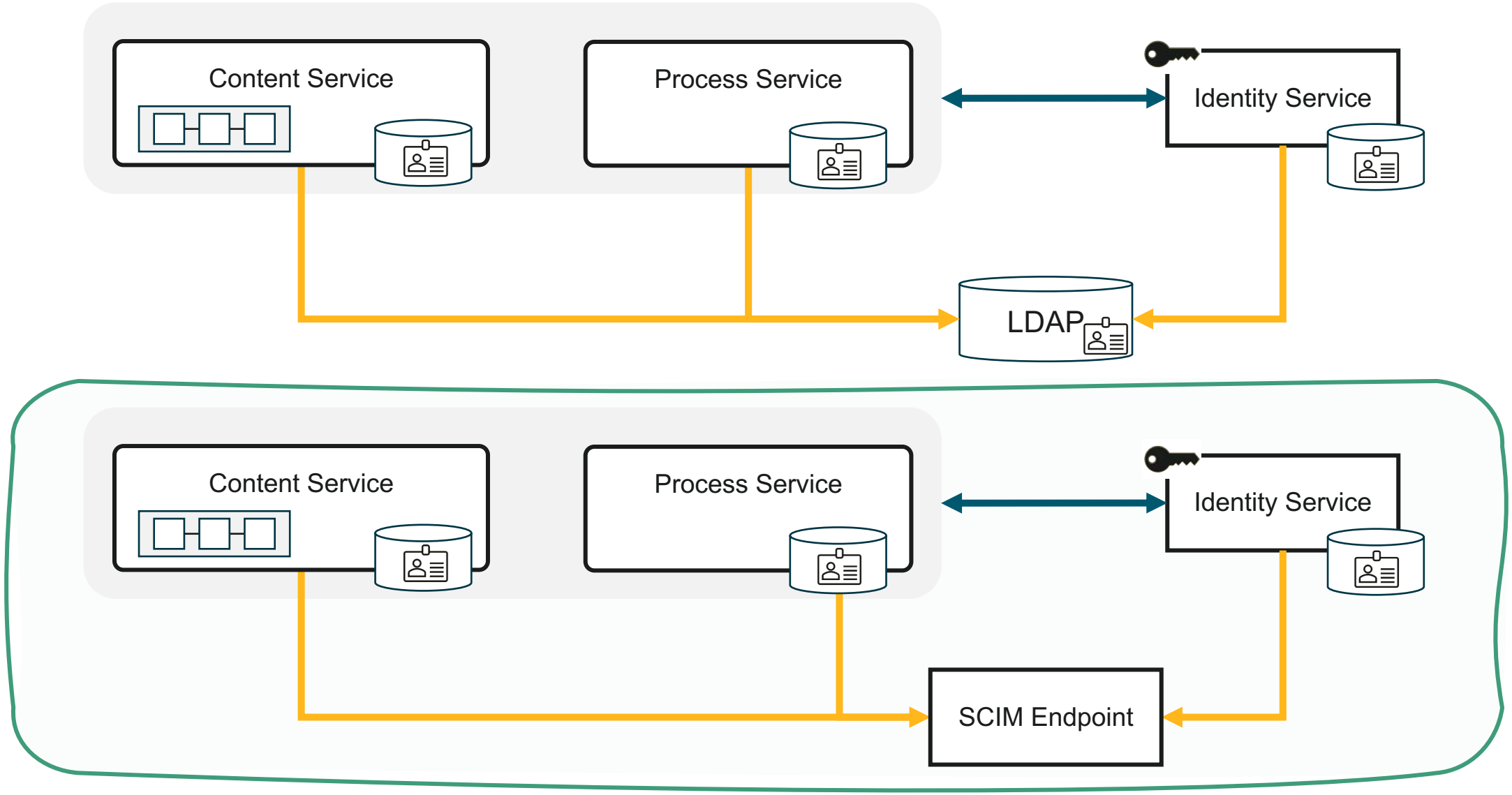


SCIM - System for Cross-domain Identity Management

Why?

- SCIM uses REST API
- Why not relying on OIDC/OAuth2?
  - https://github.com/Acosix/alfresco-keycloak/blob/master/docs/Simple-Configuration.md 🙌
- Supported by major cloud providers

SCIM Synchronization – User Provisioning



The journey - IAM

Connected

Full reliance on OIDC/OAuth2
SCIM as alternative to LDAP sync

Consistent

More effective Just in Time Provisioning
SSO on Admin Console
PKCE over Implicit flow

More secure

SAML Module EOL
Spring security instead of Keycloak client
Identity Service 2.0

Hyland™

Thank You!