Oak's External Login Module - Authenticating with LDAP and Beyond

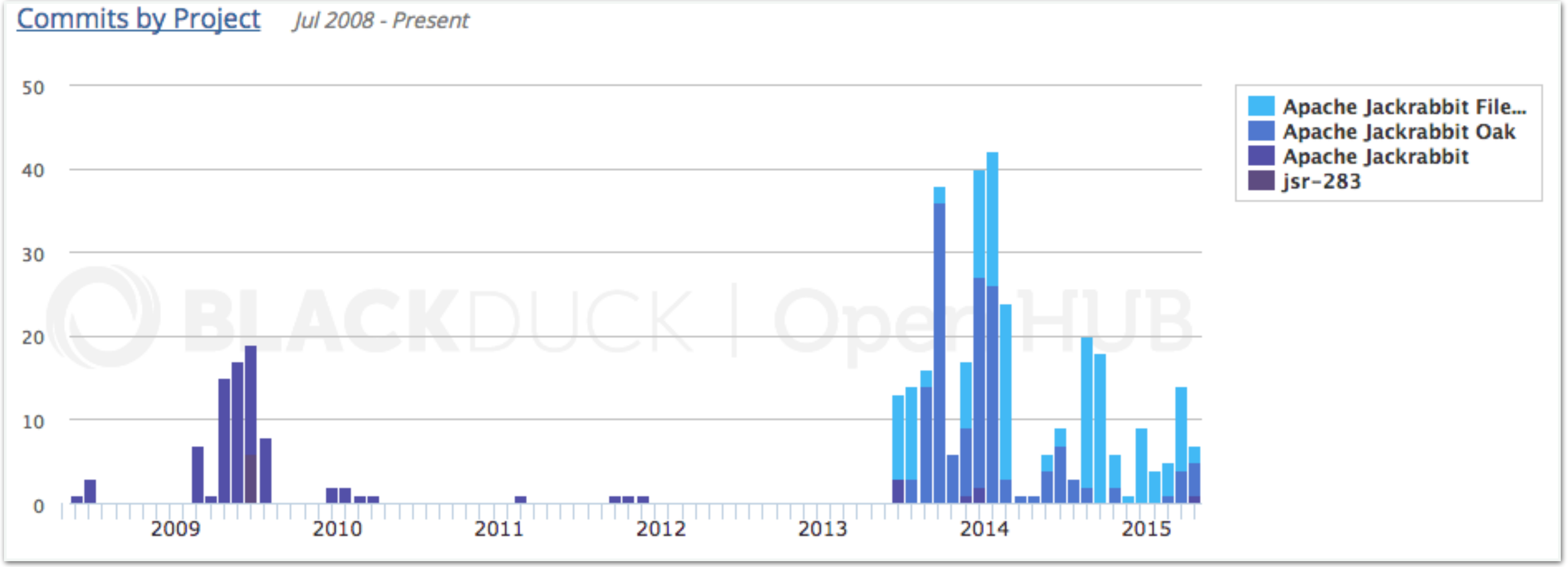
Tobias Bocanegra | Principal Scientist

Bē
Alex Trochut

About

Tobias Bocanegra

Software Engineer at Adobe/Day since 1998
JCR API Specification
Apache Member
Apache Jackrabbit Oak Committer



source: https://www.openhub.net/accounts/tripod

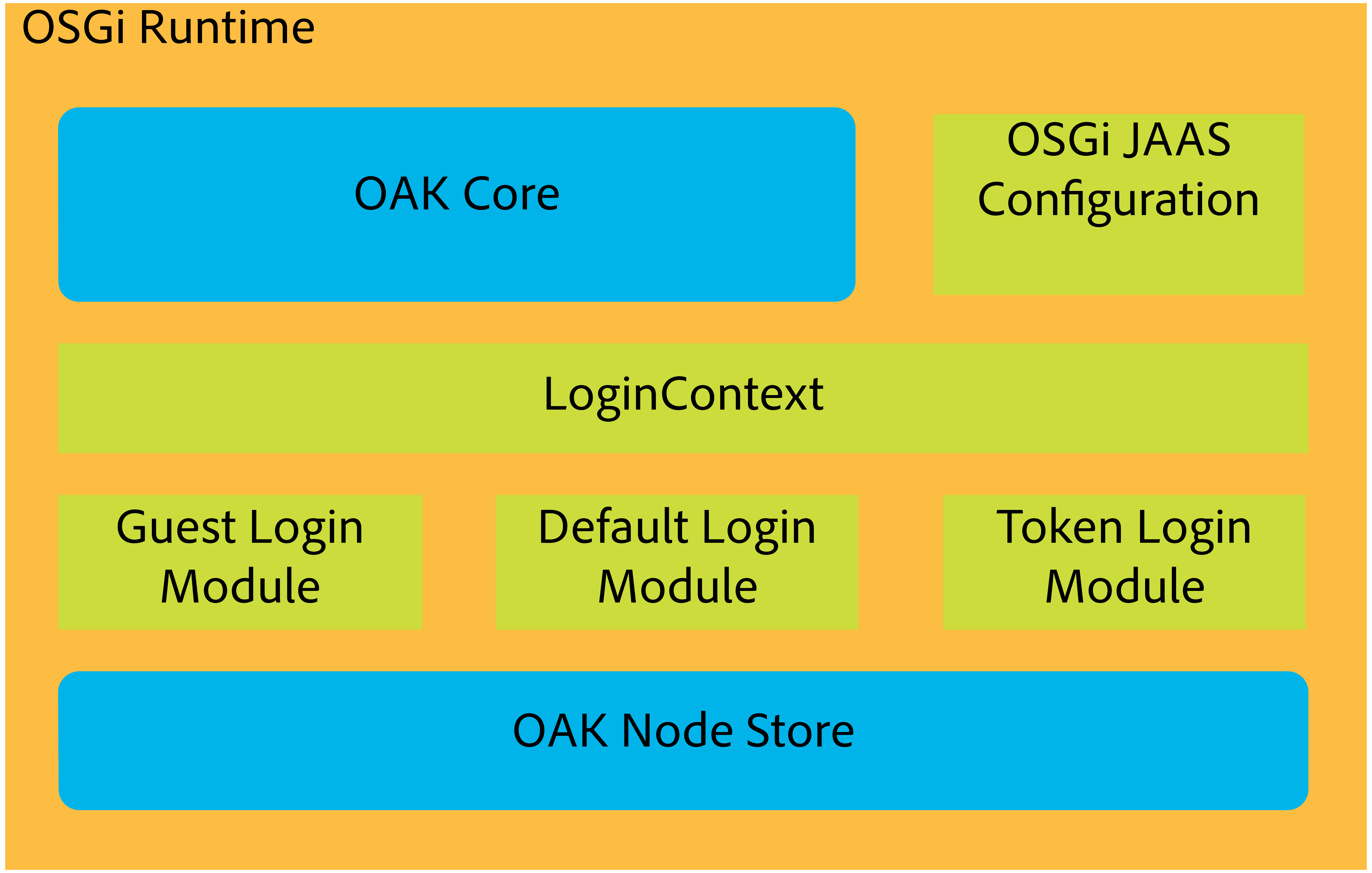
Contents

- Oak Authentication Overview
- Oak External Authentication
- LDAP Integration
- Demo - LDAP Example Setup

- Q & A

Oak Authentication Overview

- Oak uses Java Authentication and Authorization Service (JAAS) [0]
  - Subject
  - Principals
  - Credentials
  - LoginContext
  - **LoginModule**
  - Callback
  - etc.…



[0] http://docs.oracle.com/javase/8/docs/technotes/guides/security/jaas/JAASRefGuide.html

Oak Authentication Overview - Login Modules

- JAAS LoginModules
  - Ordered in lists, grouped by application realms.
  - Control Flags: Required, Requisite, Sufficient or Optional
  - Phases: Initialize, **Login**, **Commit**, Abort, Logout
  - JCR Repository.login -> Oak ContentRepository.login -> LoginModule.login -> LoginModule.commit

Oak Authentication Overview - Login Modules

- Oak LoginModule configuration all OSGI - no more jaas.conf

```
com.day.crx {
   com.day.crx.core.CRXLoginModule sufficient;
   com.day.crx.security.ldap.LDAPLoginModule required
               principal_provider.class="com.day.crx.security.ldap.prin
               host="ldap.example.com"
               port="389"
               secure="false"
               authDn="uid=admin,ou=system"
               authPw="secret"
               userRoot="ou=users, o=example"
               groupRoot="ou=groups, o=example"
               groupMembershipAttribute="uniquemember"
               autocreate="create"
               autocreate.user.membership="contributor"
               autocreate.user.mail="rep:e-mail"
               autocreate.user.cn="rep:fullname"
```

Apache Jackrabbit Oak External Login Module

Description for org.apache.jackrabbit.oak.spi.security.authentication.external.impl.ExternalLoginModuleFactory

JAAS Ranking	50 Specifying the ranking (i.e. sort order) of this login module entry. The entries are sorted in a descending order (i.e. higher value ranked configurations come first). (jaas.ranking)
JAAS Control Flag	SUFFICIENT Property specifying whether or not a LoginModule is REQUIRED, REQUISITE, SUFFICIENT or OPTIONAL. Refer to the JAAS configuration documentation for more details around the meaning of these flags. (jaas.controlFlag)
JAAS Realm	The realm name (or application name) against w LoginModule is registered with a default realm a
Identity Provider Name	ldap Name of the identity provider (for example: 'ldap
Sync Handler Name	default Name of the sync handler. (sync.handlerName)

Configuration Information

Persistent Identity (PID)	org.apache.jackrabbit.oak.s c3d5-4466-afe1-339804d09
Factory Persistent Identifier (Factory PID)	org.apache.jackrabbit.oak.s
Configuration Binding	launchpad:resources/install. Oak External Authentication

Adobe Experience Manager | Tobias Bocaneg...

localhost:4502/system/console/jaas

Adobe Experience Manager Web Console
JAAS

Main OSGi Sling Status Web Console Log out

Registered LoginModules

Realm	Rank	Control Flag	Type	Classname
jackrabbit.oak				
	300	OPTIONAL	Configuration	org.apache.jackrabbit.oak.spi.security.authentication.GuestLoginModule(Details)
	200	SUFFICIENT	Configuration	org.apache.jackrabbit.oak.security.authentication.token.TokenLoginModule(Details)
	100	SUFFICIENT	Configuration	org.apache.jackrabbit.oak.security.authentication.user.LoginModuleImpl(Details)
	50	SUFFICIENT	Service	org.apache.jackrabbit.oak.spi.security.authentication.external.impl.ExternalLoginModuleFactory(3722)

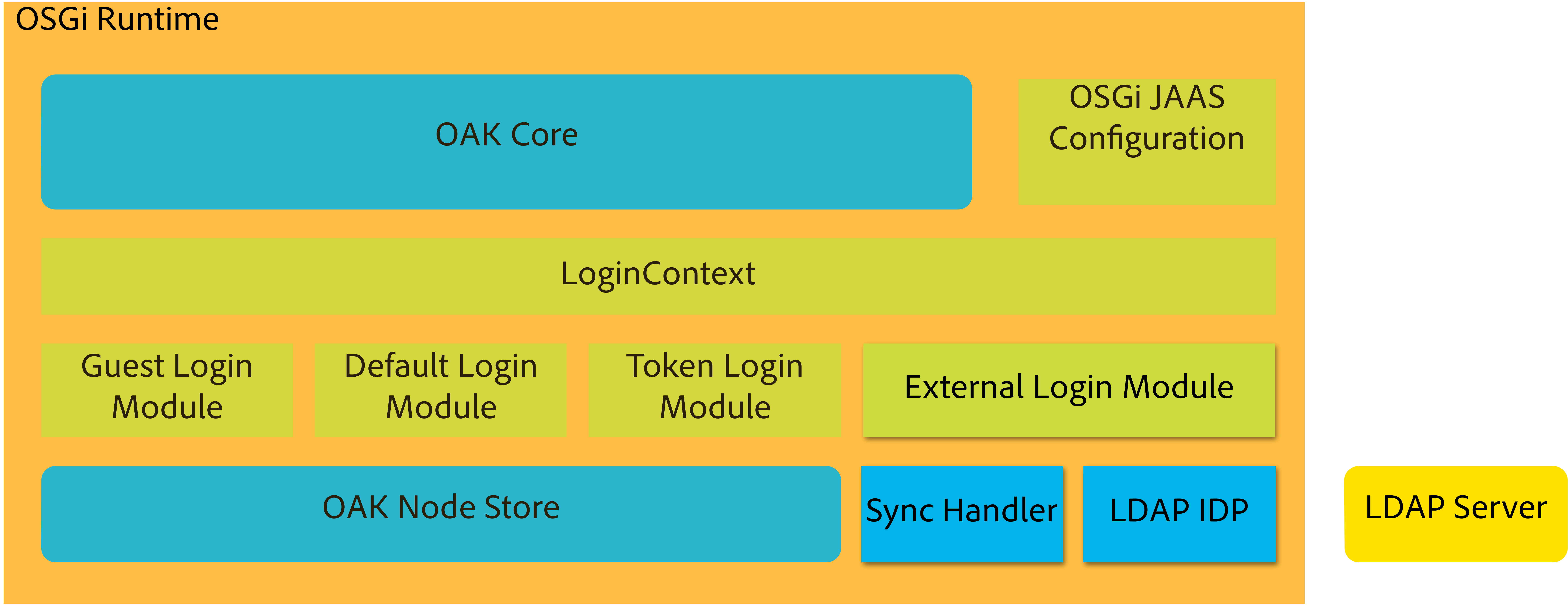
Available LoginModules

Bundle	Classes
org.apache.jackrabbit.oak-core (95)	org.apache.jackrabbit.oak.security.authentication.token.TokenLoginModule org.apache.jackrabbit.oak.spi.security.authentication.GuestLoginModule org.apache.jackrabbit.oak.security.authentication.user.LoginModuleImpl

Oak Login Modules

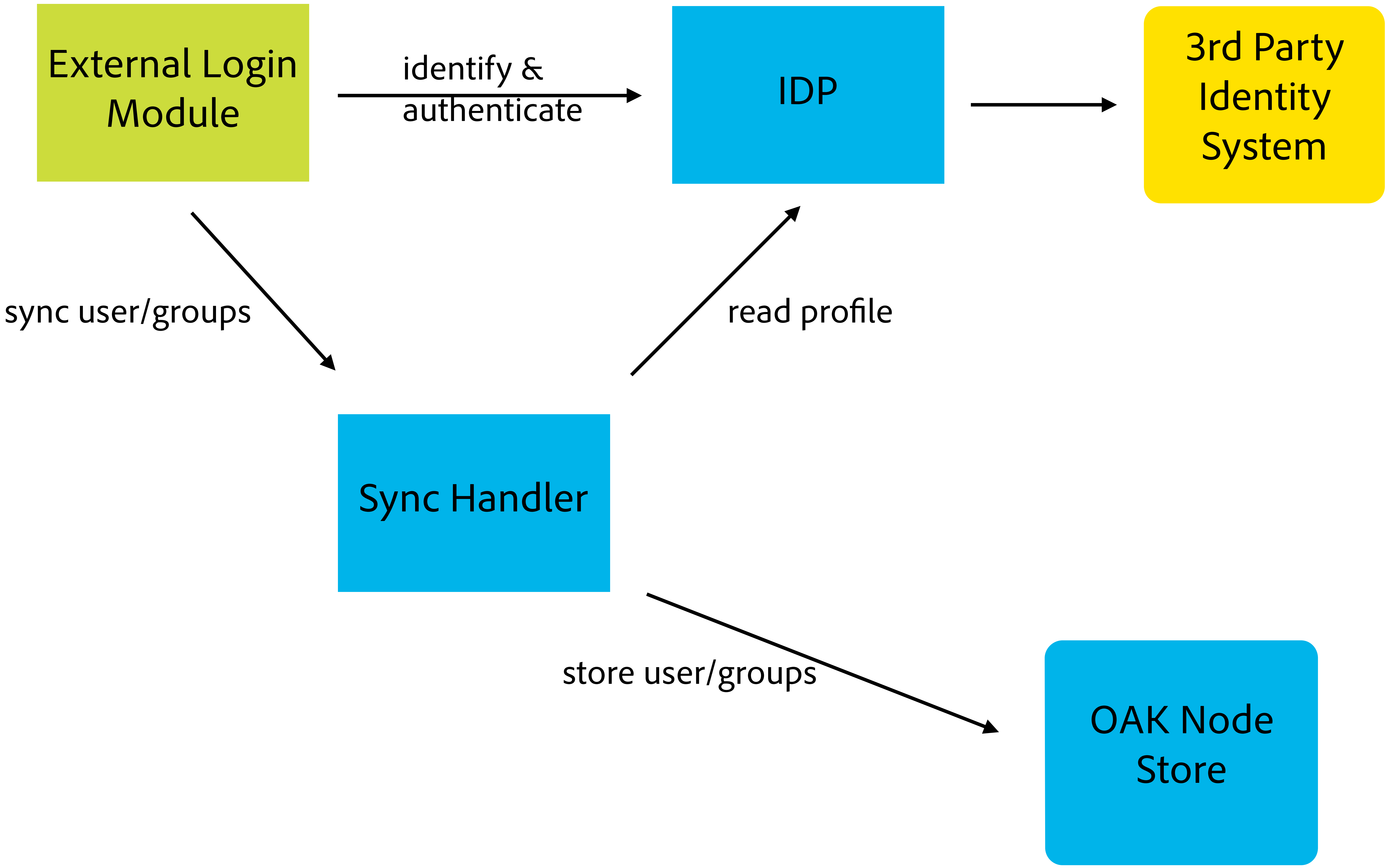
- AbstractLoginModule
- LoginModuleImpl (aka default login module)
- GuestLoginModule
- TokenLoginModule
- **ExternalLoginModule**

Oak External Authentication



Oak External Authentication

- 3 Parts:
  - External Login Module
  - External Identity Provider
  - External SyncHandler



Oak External Authentication

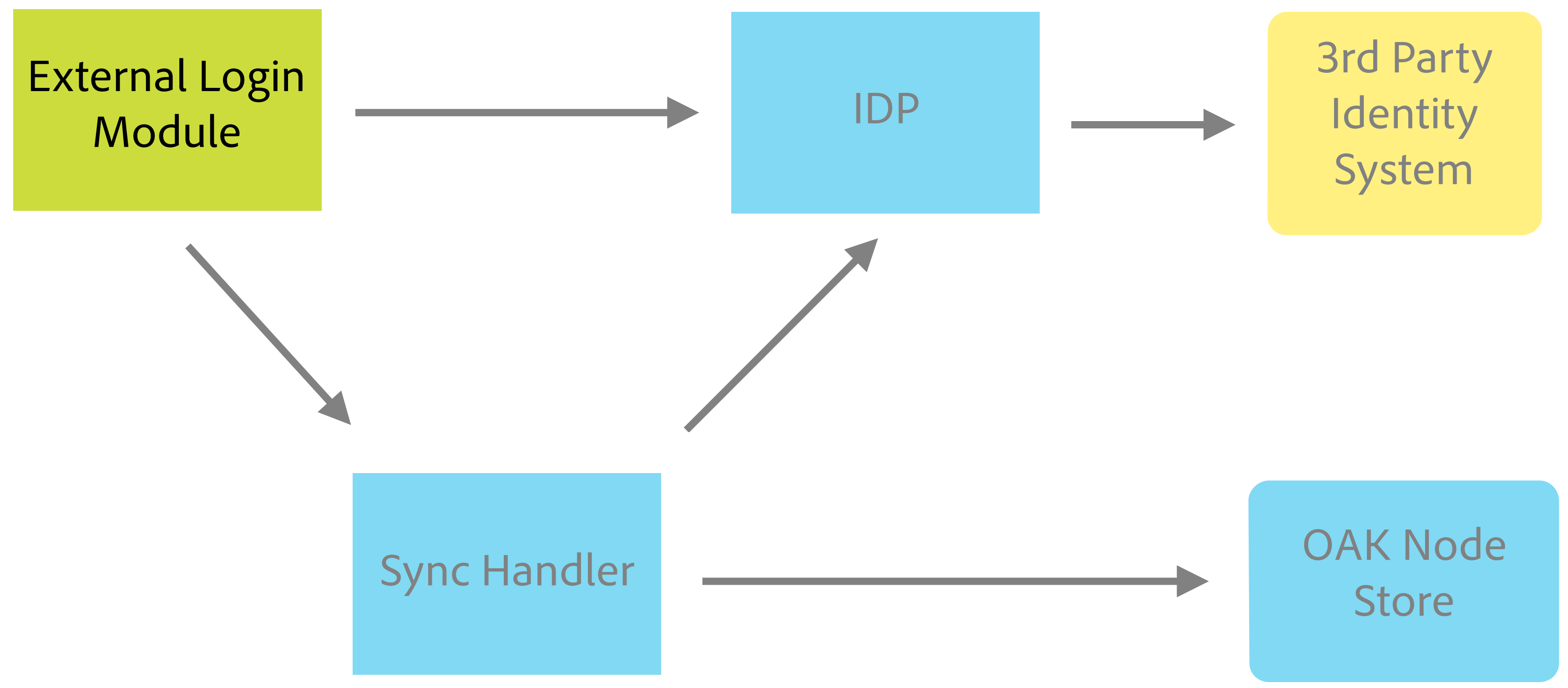
- Base implementation for easy integration of 3rd party authentication and identity systems

- what it does:
  - facilitate the use of a 3rd party system for authentication
  - simplify populating the oak user manager with identities from a 3rd party system

- but:
  - does not provide a transparent oak user manager
  - does not provide a transparent oak principal provider.
  - does not offer services for background synchronization of users and groups

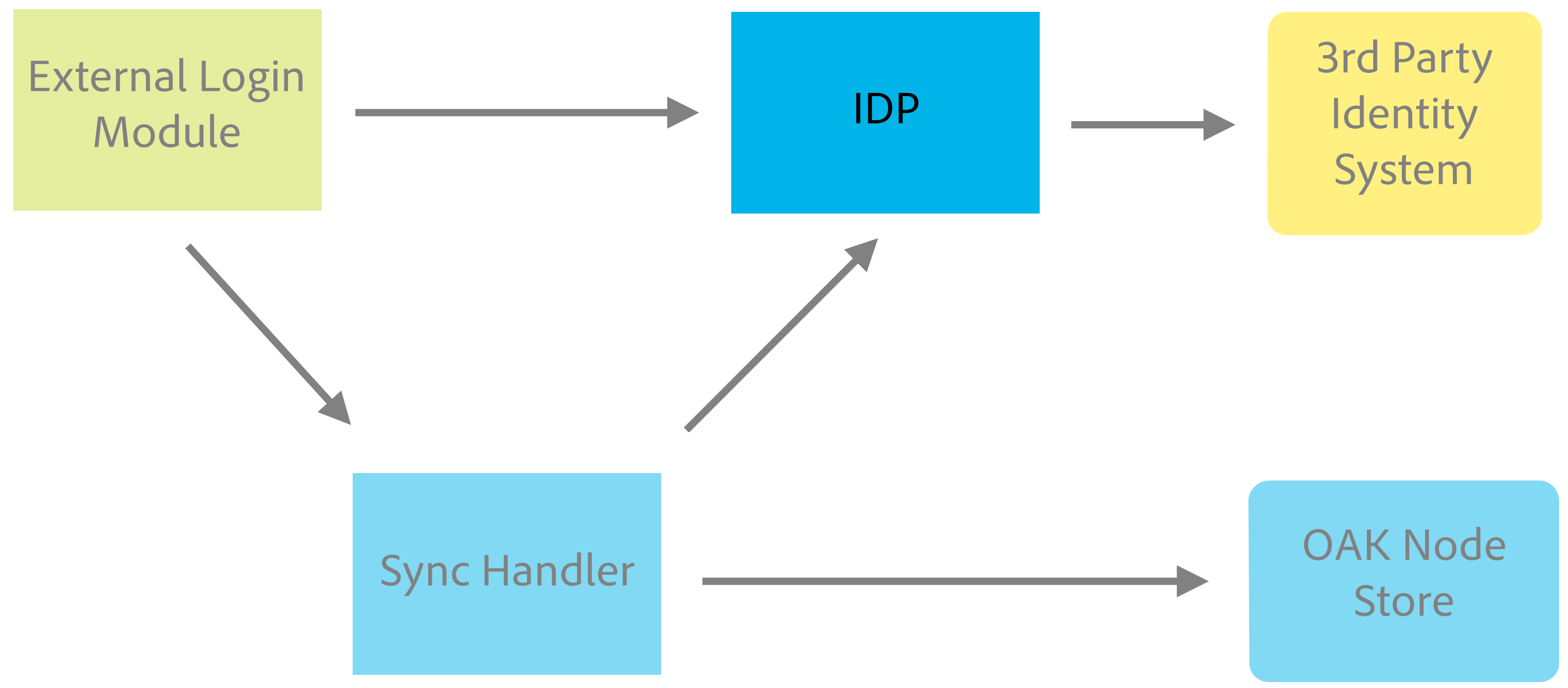
External Login Module - Overview

- 2 Main Tasks
  - Authenticate credentials against the IDP
  - Coordinate syncing of the respective users and groups with the JCR repository
- Notes
  - only **SimpleCredentials** are supported



External Identity Provider - Overview

- External Identity Provider (IDP)
  - Authenticate credentials against 3rd party systems
  - Provide profile information of external users and groups



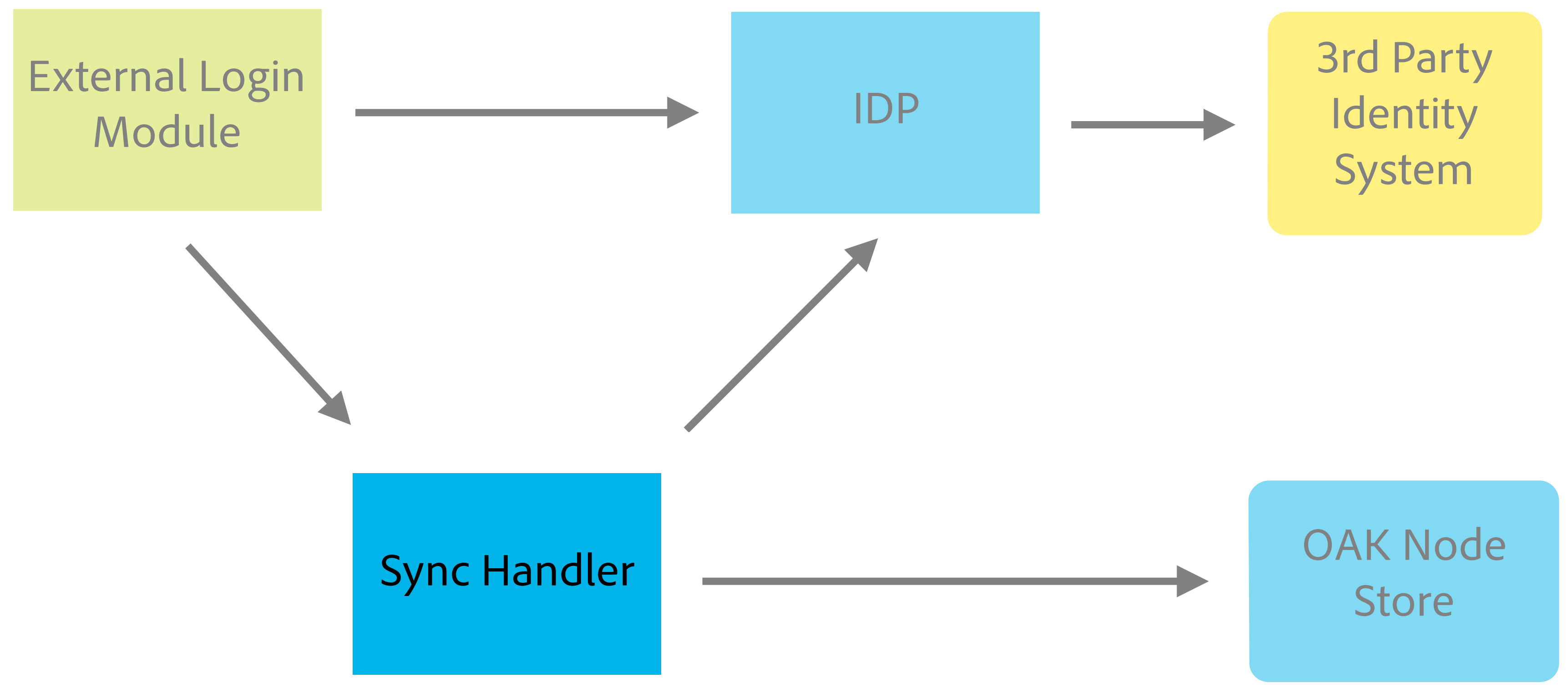
- API Highlights:
  - ExternalIdentityProvider[0]
  - ExternalIdentity, ExternalGroup, ExternalUser
  - ExternalIdentityRef

[0] http://jackrabbit.apache.org/oak/docs/apidocs/org/apache/jackrabbit/oak/spi/security/authentication/external/ExternalIdentityProvider.html

User and Group Synchronization - Overview

- External Sync Handler
  - primarily triggered by the ExternalLoginModule
  - Oak default implementation: DefaultSyncHandler

- API Highlights:
  - SyncHandler[0]
  - SyncContext



[0] http://jackrabbit.apache.org/oak/docs/apidocs/org/apache/jackrabbit/oak/spi/security/authentication/external/SyncHandler.html

User and Group Synchronization - Default Implementation

- Default Implementation (DefaultSyncHandler)
  - Oak 1.0 provides a default implementation of the user synchronization API
  - The **DefaultSyncHandler** highly configurable
  - synced authorizables have extra properties:
    - **rep:externalId**
    - **rep:lastSynced**

User and Group Synchronization - Default config

Name	Property	Description
Sync Handler Name	`handler.name`	Name of this sync configuration. This is used to reference this handler by the login modules.
User auto membership	`user.autoMembership`	List of groups that a synced user is added to automatically
User Expiration Time	`user.expirationTime`	Duration until a synced user gets expired (eg. ‘1h 30m’ or ‘1d’).
User Membership Expiration	`user.membershipExpTime`	Time after which membership expires (eg. ‘1h 30m’ or ‘1d’).
User membership nesting depth	`user.membershipNestingDepth`	The maximum depth of group nesting when membership relations are synced. A value of 0 effectively disables group membership…
User Path Prefix	`user.pathPrefix`	The path prefix used when creating new users.
User property mapping	`user.propertyMapping`	List mapping definition of local properties from external ones. eg: ‘profile/email=mail’.Use double quotes for fixed values. eg:
Group auto membership	`group.autoMembership`	List of groups that a synced group is added to automatically
Group Expiration Time	`group.expirationTime`	Duration until a synced group expires (eg. ‘1h 30m’ or ‘1d’).
Group Path Prefix	`group.pathPrefix`	The path prefix used when creating new groups.
Group property mapping	`group.propertyMapping`	List mapping definition of local properties from external ones.

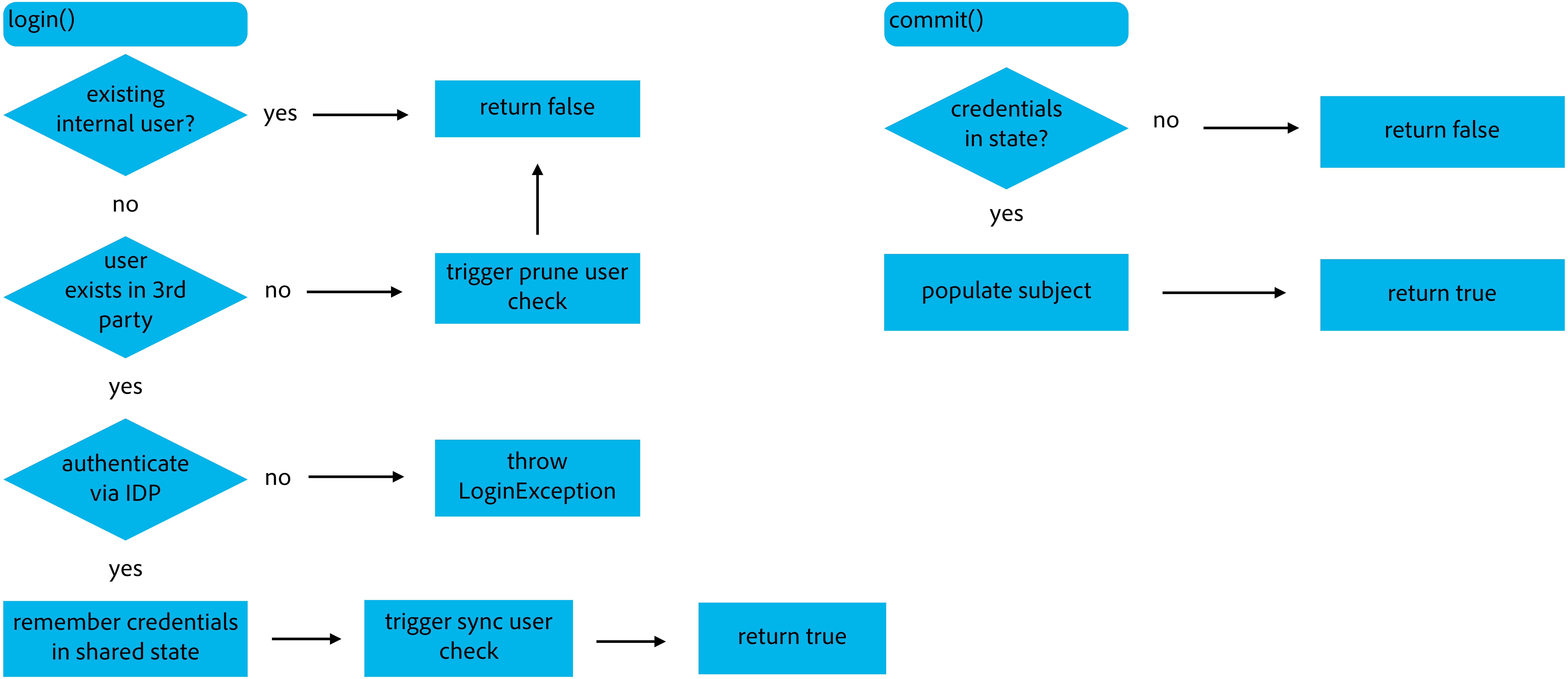
- see http://jackrabbit.apache.org/oak/docs/apidocs/org/apache/jackrabbit/oak/spi/security/authentication/external/impl/DefaultSyncConfigImpl.html

User and Group Synchronization - JMX Synchronization Tool

- JMX Synchronization Tool
  - Accessible with any JMX client

  - Available tasks:
    - **syncUsers**: Syncs a list of internal users
    - **syncAllUsers**: Syncs all internal users that have a rep:externalId property
    - **syncExternalUsers**: Syncs a list of external users
    - **syncAllExternalUsers**: Syncs all external users provisioned via `IdentityProvider.listUsers()`
    - **listOrphanedUsers**: lists all internal users that have a rep:externalId property that don't exist on the IDP anymore
    - **purgeOrphanedUsers**: removes the orphaned users returned with **listOrphanedUsers.**

External Login Module - Flow



LDAP Integration - Overview

- LDAP Identity Provider
  - LDAP Identity Provider implementing the ExternalIdentityProvider interface.
  - Highly configurable through OSGi

- Configuration
  - configure the LDAP IdentityProvider
  - configure the DefaultSyncHandler
  - ensure ExternalLoginModule forms part of the systems JAAS Configuration

LDAP Integration - Config

- Connection Config

Name	Property	Description
LDAP Provider Name	`provider.name`	Name of this LDAP provider configuration. This is used to reference this provider by the login modules.
Bind DN	`bind.dn`	DN of the user for authentication. Leave empty for anonymous bind.
Bind Password	`bind.password`	Password of the user for authentication.
LDAP Server Hostname	`host.name`	Hostname of the LDAP server
Disable certificate checking	`host.noCertCheck`	Indicates if server certificate validation should be disabled.
LDAP Server Port	`host.port`	Port of the LDAP server
Use SSL	`host.ssl`	Indicates if an SSL (LDAPs) connection should be used.
Use TLS	`host.tls`	Indicates if TLS should be started on connections.
Search Timeout	`searchTimeout`	Time in until a search times out (eg: ‘1s’ or ‘1m 30s’).

- see http://jackrabbit.apache.org/oak/docs/apidocs/org/apache/jackrabbit/oak/security/authentication/ldap/impl/LdapProviderConfig.html

LDAP Integration - Config

- User and group settings

Name	Property	Description
User base DN	`user.baseDN`	The base DN for user searches.
User extra filter	`user.extraFilter`	Extra LDAP filter to use when searching for users. The final filter is formatted like: `(&(<idAttr>=<userId>)(objectclass=<objectclass>)<extraFilter>)`
User id attribute	`user.idAttribute`	Name of the attribute that contains the user id.
User DN paths	`user.makeDnPath`	Controls if the DN should be used for calculating a portion of the intermediate path.
User object classes	`user.objectclass`	The list of object classes an user entry must contain.
Group base DN	`group.baseDN`	The base DN for group searches.
Group extra filter	`group.extraFilter`	Extra LDAP filter to use when searching for groups. The final filter is formatted like: `(&(<nameAttr>=<groupName>)(objectclass=<objectclass>)<extraFilter>)`
Group DN paths	`group.makeDnPath`	Controls if the DN should be used for calculating a portion of the intermediate path.
Group member attribute	`group.memberAttribute`	Group attribute that contains the member(s) of a group.
Group name attribute	`group.nameAttribute`	Name of the attribute that contains the group name.
Group object classes	`group.objectclass`	The list of object classes a group entry must contain.

LDAP Integration - Setup LDAP

- DEMO
  - Install and configure Apache Directory
  - Import example user data
  - Configure Oak (using AEM 6.1)
  - Test

- Requisites:
  - Apache Directory Server
  - Apache Directory Studio
  - Example User Data in LDIF format
  - AEM 6.1

How to Debug

- Increase logging
  - External login module: `org.apache.jackrabbit.oak.spi.security.authentication.external`
  - LDAP IDP: `org.apache.jackrabbit.oak.security.authentication.ldap`
  - LDAP Client: `org.apache.directory`

Oak Authentication - Bonus

- DEMO
  - Create your own IDP
  - Tutorial available on github: https://github.com/Adobe-Marketing-Cloud/aem-ldap-tutorial/

References

- AEM LDAP Tutorial on github
  https://github.com/Adobe-Marketing-Cloud/aem-ldap-tutorial/

- Apache Jackrabbit Oak
  http://jackrabbit.apache.org/oak/
- Oak Security Documentation
  http://jackrabbit.apache.org/oak/docs/security/overview.html

- Apache Directory
  http://directory.apache.org/apacheds/
- JAAS Authentication
  http://docs.oracle.com/javase/8/docs/technotes/guides/security/jgss/tutorials/AcnOnly.html

Questions ?

???

Thank you!

Adobe