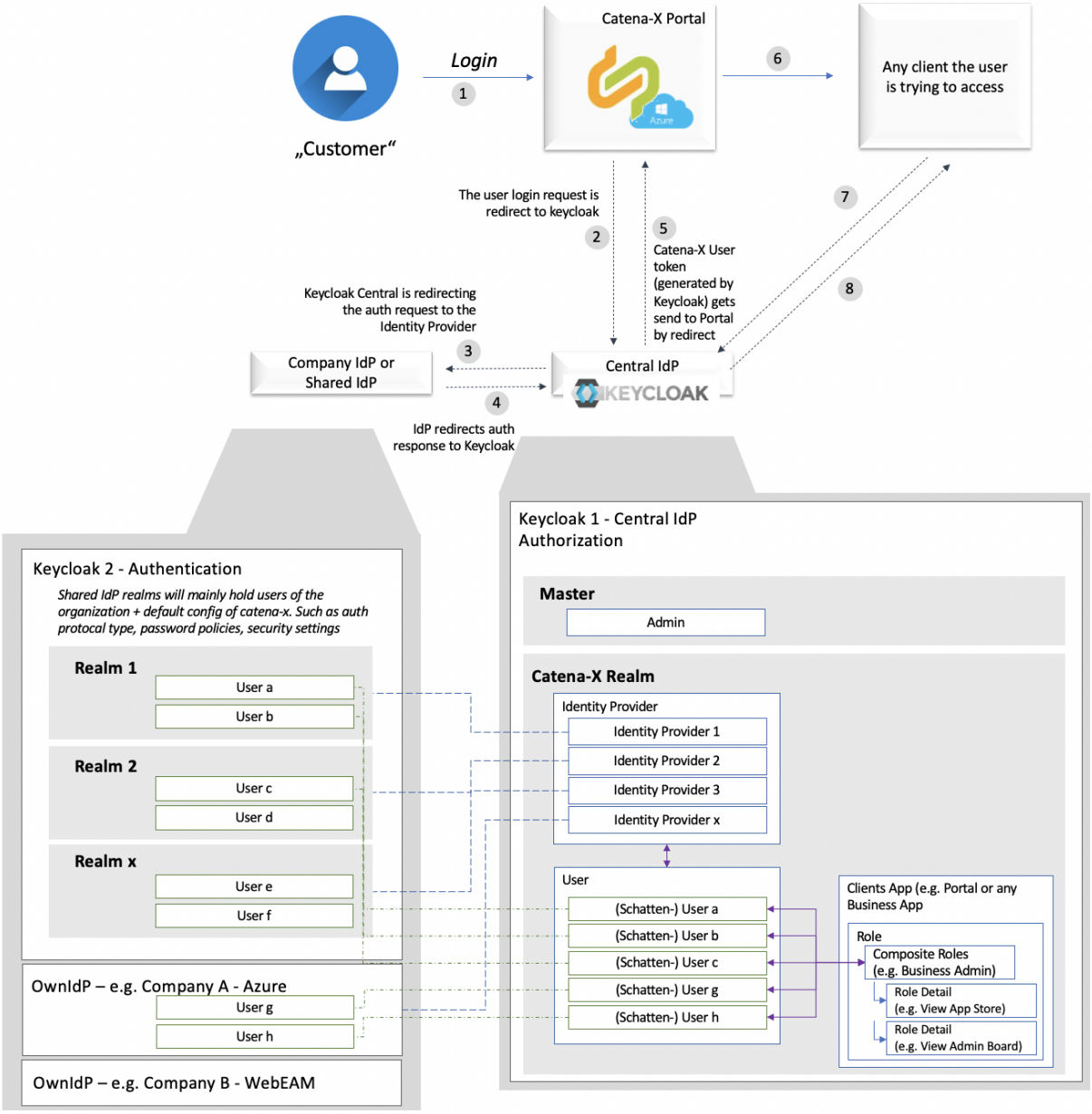
Keycloak Implementation/Setup

Steps to Setup Keycloak

1. Install Keycloak ✅
2. Loadbalancer / Cluster Concept
3. Configure Master ✅
4. Create *Realms* ✅
5. Create Clients
6. Define one or more *Roles* for the client. The roles correspond to EBICS Client permissions that are used by EBICS Client in access control. **Note:** In this version of EBICS Client, there is one unique, global-access role. ✅
7. Optionally, you can create *Groups*, which are logical groupings or sets of permissions. ✅
8. Create *Users*. These are the users who will be able to access the EBICS Client application. ✅
9. Assign roles to the users.

Keycloak Instances

Interaction Keycloak & CX-WebApplication

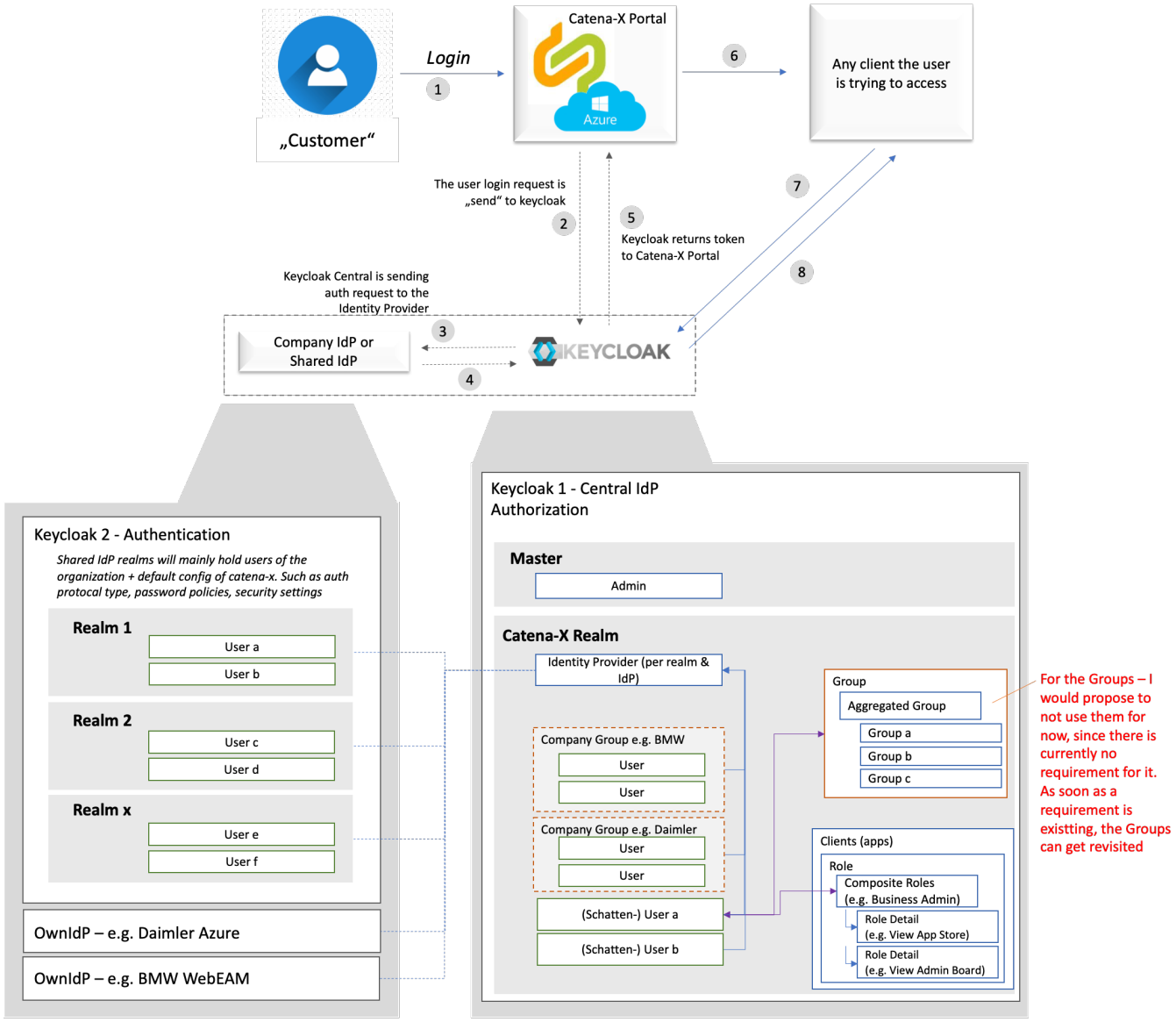


*(Schatten-) User: The „Schatten-User“ is defined as an empty User frame holding limited information. The actual user is managed in the respective Identity Provider.

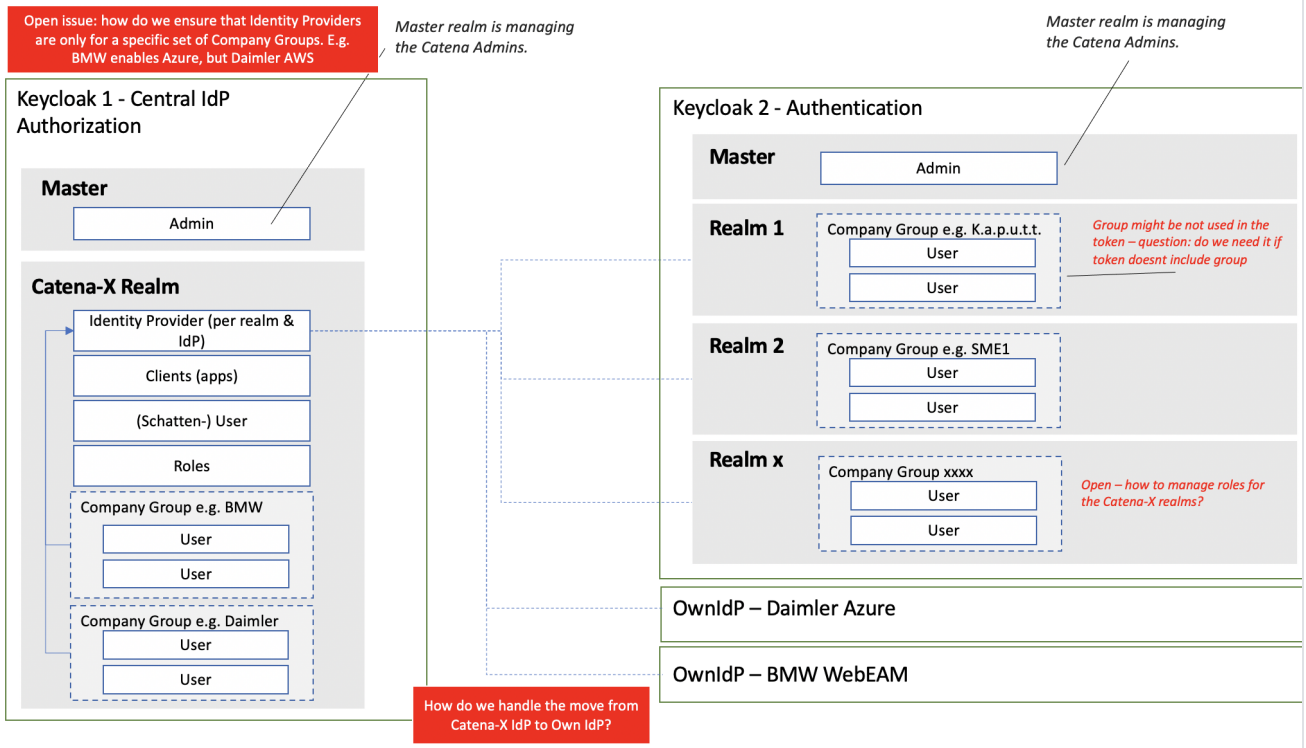
The Schatten-User are always federated identities.

Info:

Groups are currently not used in the IAM design since the groups do not deliver any benefit in the current design / implementation state. The usage of groups will get revisited with the extension of the scope / requirement.


„Customer“
Login
1
Catena-X Portal
Azure
6
Any client the user is trying to access
The user login request is „send“ to keycloak
2
5
Keycloak returns token to Catena-X Portal
7
8
Keycloak Central is sending auth request to the Identity Provider
3
4
Company IdP or Shared IdP
KEYCLOAK
Keycloak 2 - Authentication
Shared IdP realms will mainly hold users of the organization + default config of catena-x. Such as auth protocal type, password policies, security settings
Realm 1
User a
User b
Realm 2
User c
User d
Realm x
User e
User f
OwnIdP – e.g. Daimler Azure
OwnIdP – e.g. BMW WebEAM
Keycloak 1 - Central IdP
Authorization
Master
Admin
Catena-X Realm
Identity Provider (per realm & IdP)
Company Group e.g. BMW
User
User
Company Group e.g. Daimler
User
User
(Schatten-) User a
(Schatten-) User b
Group
Aggregated Group
Group a
Group b
Group c
Clients (apps)
Role
Composite Roles (e.g. Business Admin)
Role Detail (e.g. View App Store)
Role Detail (e.g. View Admin Board)
For the Groups – I would propose to not use them for now, since there is currently no requirement for it. As soon as a requirement is existting, the Groups can get revisited

Keycloak: Realm Setup / Design



pptx: PI2-Portal Keycloak Setup.pptx

Cookie Management

Mit Keycloak findet eine Authentifizierung des Benutzers beim ersten Server, auf den ein Zugriff erfolgt, mit einem Benutzernamen und einem Kennwort statt. Nach der Authentifizierung empfängt der Benutzer einen Keycloak Token, das nur für eine einzige Sitzung gültig ist. Das Token wird verwendet, um den Benutzer auf anderen Servern in demselben Domain Name System, in dem die Server für die Verwendung von Keycloak konfiguriert sind, zu identifizieren. Deshalb gibt der Benutzer einen Benutzernamen und ein Kennwort nur ein einziges Mal ein und es wird auch nur ein einziges Mal auf das Benutzerverzeichnis zugegriffen, um die Identität dieses Benutzers zu überprüfen.