OX Cloud standardized authentication methods

This document describes the default Authentication methods that are available in the OX Cloud environment without any customization.

Some standards like SAML or OpenID Connect require coordination with OX to be enabled but are still viable options to authenticate the users.

This document will not describe each step required to enable the different authentication methods but focuses on the different Standards and the supported flows that can be enabled. It will also highlight not supported flows or restrictions that apply to the current OX Cloud version.

General information

If the following assumptions about your system are correct, there is no need to get in contact with someone at Open-Xchange to test the authentication.

- You provision your users with their mail as the **username** and provide a working **password** that your users are aware of.
- You do not require SSO login.

If the above is true, you don't need to continue reading in this document as it is mainly required for either SSO login or changes to the default authentication flow.

Terminology in this document

uid	The username of the user used in provisioning
alias	An alias of the user, this also includes the main mail address
saml	Security Assertion Markup Language - A way to authenticate users only via the browser.
oidc	OpenID Connect - A way to authenticate users via the browser. Has a backchannel to fetch more user data.
webmail	Web Access is the user reaching the website with a browser
imap	External imap access handled in the OX Cloud environment
other clients	Other clients may include OX Mail App or a DAV client that connects to OX Cloud. Native IMAP, POP3 or SMTP access is not in scope.

Default Authentication

Without any change to the configuration it is expected that only one Authentication Service is enabled. The default identifier used is the **uid** of the user, which has been set in provisioning. The password used has also been set as part of the provisioning.

A list of clients that would use the password saved in OX Cloud would be:

- OX Mail
- CalDAV/CardDAV
- Webmail, if neither SAML or OIDC is enabled
- external IMAP/POP/SMTP

Note that the **webmail** access can be configured to have SAML or OIDC which is explained later on this page. If you only require access to the **webmail** part, there is no need to sync passwords. However it is strongly advised to do so.

If access for any of the above mentioned clients is expected or if no SAML or OIDC is enabled, you should sync the users passwords with the OX Cloud user database.

IMAP Authentication

The **external imap access** has its own authentication flow but will also use **uid** and password by default. The same options as above are available but can be configured on an independent property.

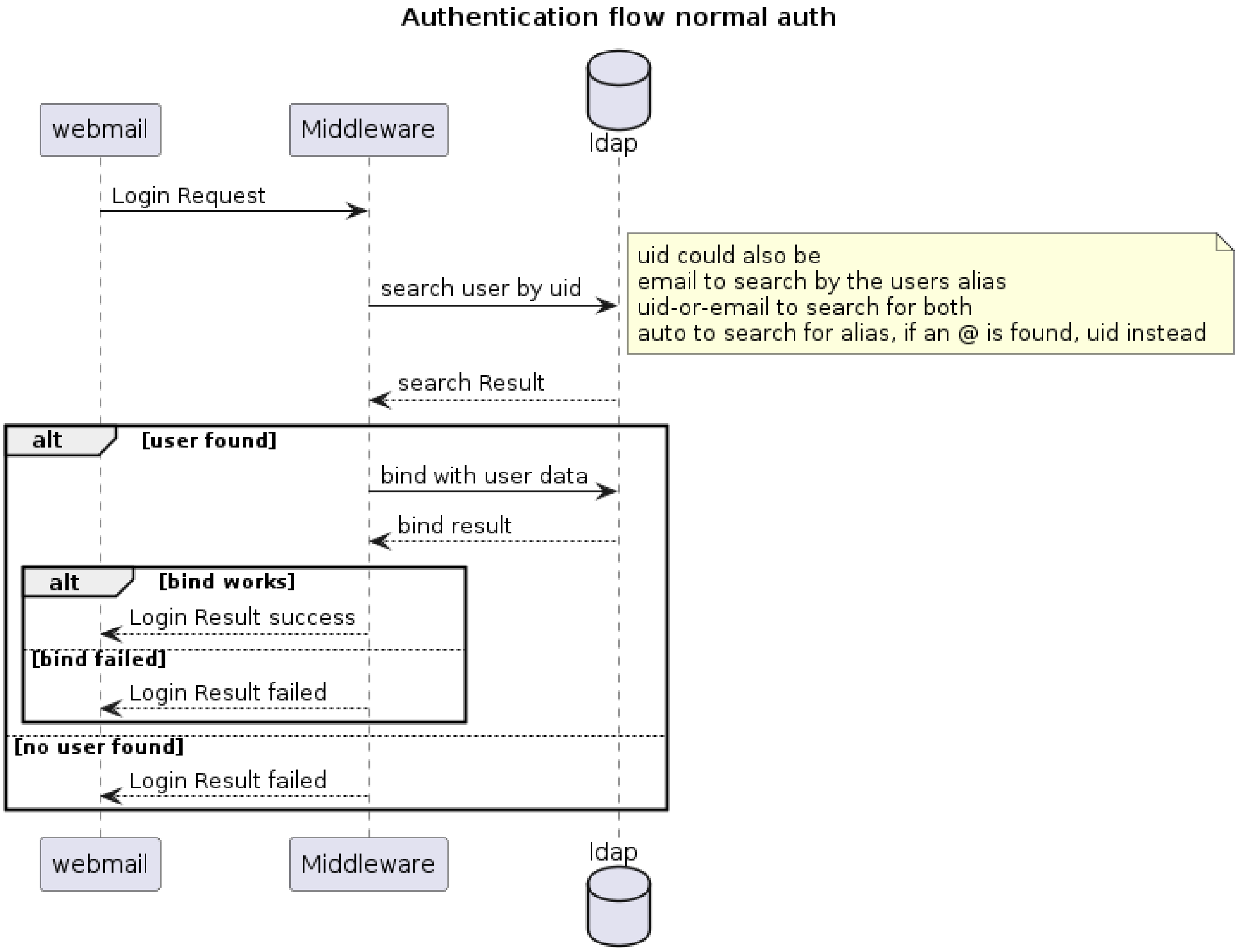
Configurable options for the user lookup in Authentication (these options are only relevant for the OX Cloud Professional variant!)

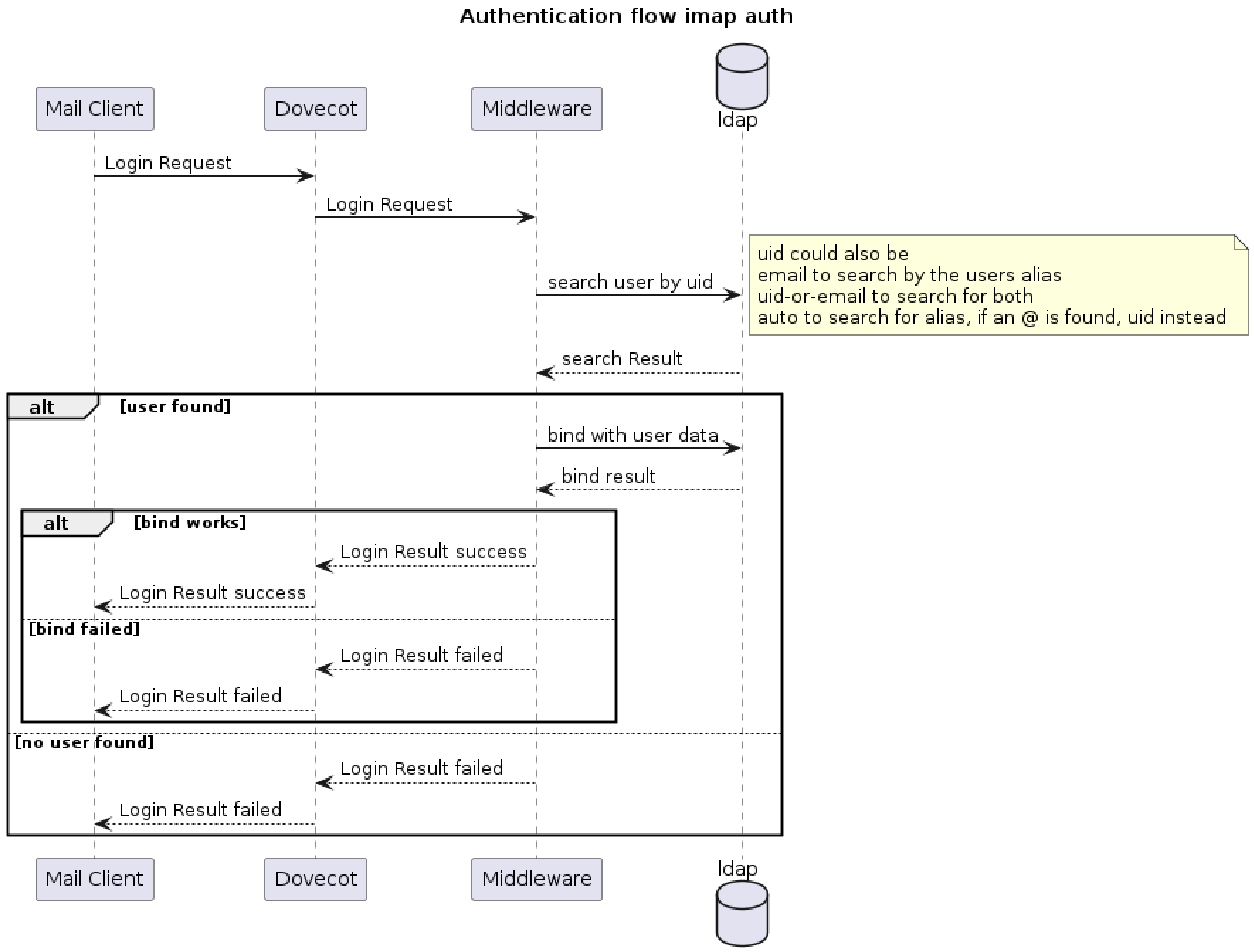
It is possible to configure the lookup of the user identifiers to other keys than **uid**. The list below shows the different options available.

- **`uid`**
  - LDAP search queries will be performed to match the login string with the **`uid`**
- **`email`**
  - LDAP search queries will be performed to match the login string with the **`alias`** (which also contains the primary email)
- **`uid-or-email`**
  - LDAP search queries will be performed to match the login string with the **`alias`** (which also contains the primary email) or **`uid`** (hence matching either of them)
- **`auto`**

- LDAP search queries will be performed to match the login string with the
  - **`alias`** if the login string contains the character @,
  - or **`uid`** if the login string doesn't contain the character

⚠ While it is possible to have different lookups available, those must be configured by Operations and should not be switched once a System is running. If e.g. the username (**uid**) should be an internal identifier, the lookup must be changed to e.g. **mail** instead.





SSO flows for webmail

It is possible to offer **SAML** or **OpenID Connect** to the webmail access. Neither **IMAP access** nor **other clients** can use this approach.
If it is expected to have e.g. **DAV** access enabled, a normal Authentication flow as mentioned above must still be enabled and passwords must be provisioned, otherwise the users are not able to login.
You need to have your **own URL** registered in the OX Cloud environment as it is not possible to differentiate access to the OX Cloud System before users have logged in.
It is possible to enable SSO login for **webmail** users. The SSO stack does not disable the normal Authentication, which is then only used for **other clients** like **DAV** or OX Mail.
Please note that it is not possible to have SSO login and normal Authentication enabled for **webmail** access at the same time on the same URL.

⚠ SSO integration needs alignment with Open-Xchange

SAML

The following minimal data has to be provided to register a client for SAML.

- IDP certificate
- Identifier information of the userlookup
    - either some key in AttributeStatement
    - or the Subject:NameID
- the entityID of the IDP
- Url, where authnRequests are to be send to

After this data is available or in the meantime, someone from OX will share the following data with you

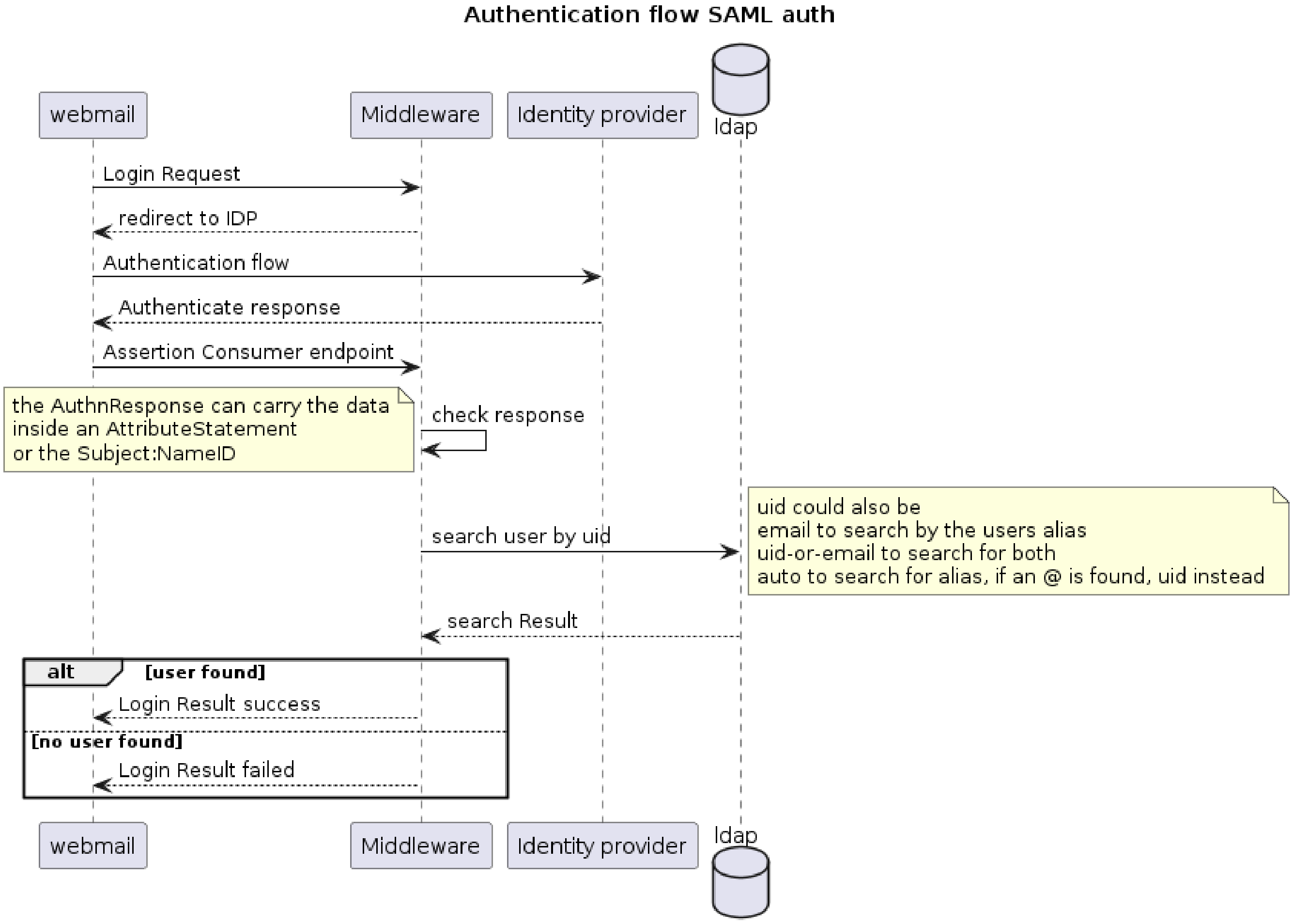
- The Assertion Consumer URL
- the EntityID of the Service Provider

If SSOLogout is required, the following data needs to be shared

- URL, where logout requests are to be send to

After this data is available or in the meantime, someone from OX will share the following data with you

- The Single Logout Service URL



OIDC

The following minimal data has to be provided to register a client for OIDC.

- URL of the Authorization Endpoint
- URL of the JwkSetEndoint
- The jwsAlgorithm
- The clientId and clientSecret of the RP
- Identifier information of the userlookup inside the idtoken
    - either the **subject**
    - or any other **claim**

After this data is available or in the meantime, someone from OX will share the following data with you

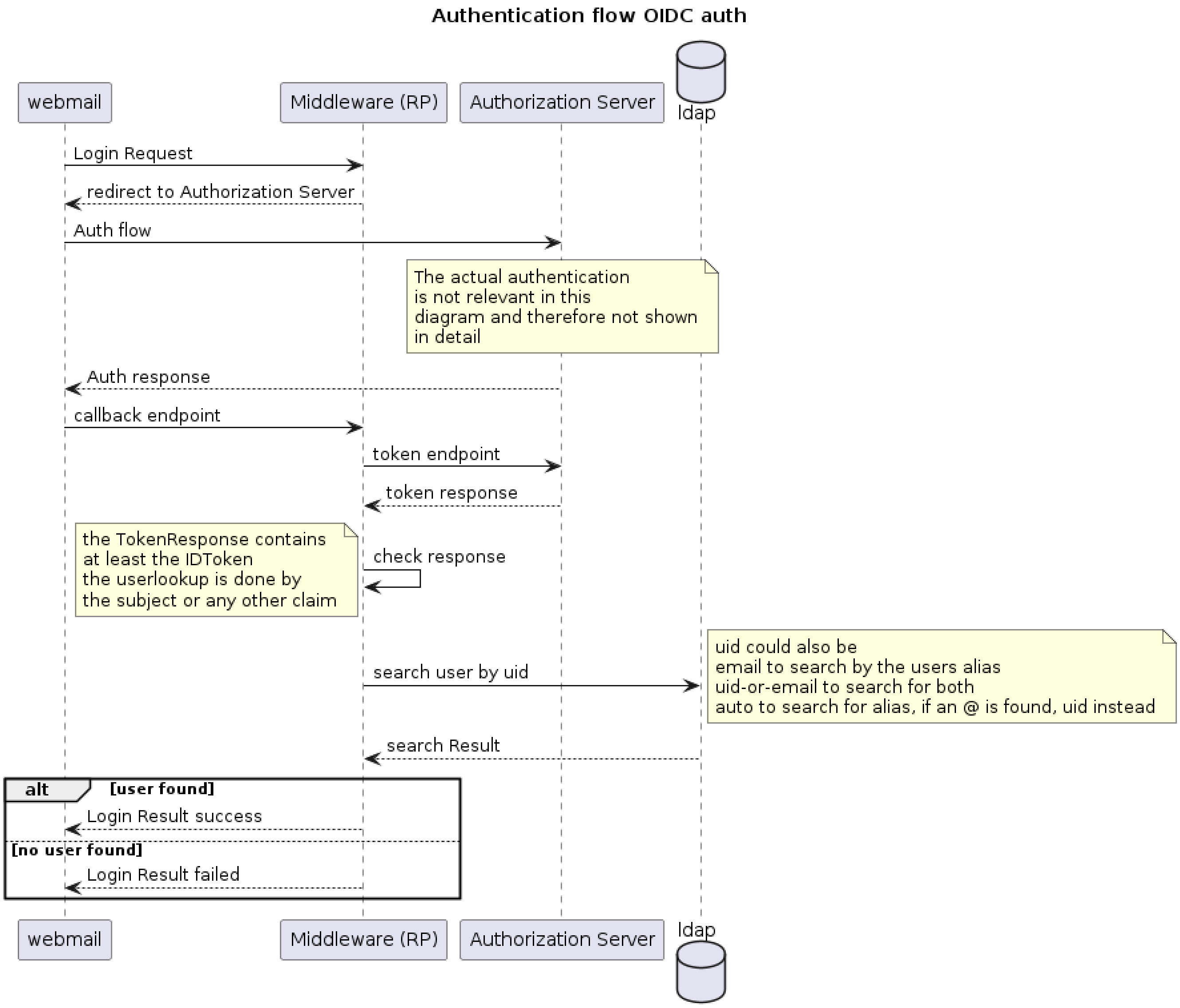
- The redirect URL of the RP

If SSOLogout is required, the following data needs to be shared

- URL, where logout requests are to be send to

After this data is available or in the meantime, someone from OX will share the following data with you

- The Single Logout URL of the RP



The actual authentication
is not relevant in this
diagram and therefore not shown
in detail

the TokenResponse contains
at least the IDToken
the userlookup is done by
the subject or any other claim

uid could also be
email to search by the users alias
uid-or-email to search for both
auto to search for alias, if an @ is found, uid instead

SSO systems that work with OX Cloud

The following list contains IDP software that is known to work with the OX Cloud Authentication stack without any custom development. You will still need to make configuration changes.

- Keycloak
  - SAML and OIDC
- Pingfederate
  - OIDC
- Shibboleth
  - SAML