Contents

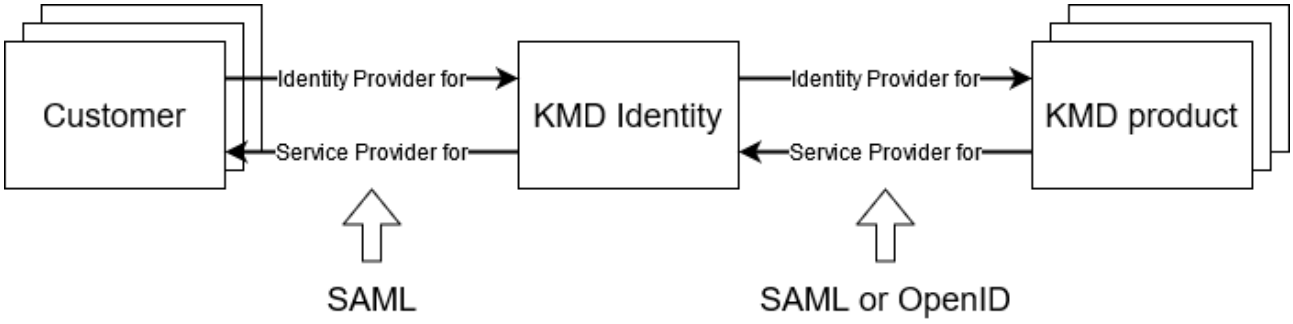
1 Introduction to KMD Identity

KMD Identity is a technical platform that acts as an identity broker between various KMD products and their customers. This simplifies federation for both parties involved as they only need a single federation partner to implement Single-Sign On for multiple products or customers.

KMD products acting as Service Providers can federate with KMD Identity using either **SAML** or **OpenID Connect**.

Customers acting as Identity Providers can federate with KMD Identity using **SAML**.

Support for OpenID Connect federation with customers is planned but not yet implemented.



2 Scope

This document describes the technical requirements for an Identity Provider to federate with KMD Identity and how to get started.

3 Intended audience

The intended audience of this document is customers who would like to federate with KMD Identity. Separate documentation exists for KMD products.

4 Terminology

The field of federated identity uses different, sometimes overlapping terminology to describe similar concepts across multiple protocols.

For the purposes of this document, we will be using these terms regardless of protocol context:

- **Identity Provider (IDP)** - A service that can authenticate requests.
- **Service Provider (SP)** - A service that can accept authenticated requests.
- **Claim** – A unit of information that describes an authenticated entity.

In this scenario, our customers are the ones that can authenticate the user and are therefore the **Identity Provider**.

KMD Identity is the party that would like to have users authenticated and receive claims about them. It is therefore the **Service Provider**.

5 SAML Federation

This chapter describes the technical requirements when setting up a SAML based federation with KMD Identity.

5.1 Name ID

After a user has been authenticated with the Identity Provider, KMD Identity expects the SAML response to contain a subject with a Name ID that is both unique and a persistent identifier of that user.

To be unique, no two users in the customer's organization may receive the same Name ID value.

For it to be persistent, the Name ID must not change between sessions, and it should specify the Name ID format:

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

Here are some example attributes that can be used as Name ID (but not limited to):

- UPN
- Object ID

5.2 Claims

In addition to a subject containing a Name ID as described above, KMD Identity would like to request that the following claims describing user attributes are present in the SAML response after authentication:

Claim name	Claim type	Optional
E-mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	False
Given Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	False
Surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	False
Otherphone	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	True

NB: Note that if specific KMD products require additional claims that are not listed above we support this by setting up an app-specific federation to our customers. The list of additional claims is agreed upon in collaboration between the KMD product and the customer.

5.3 Identity Provider metadata endpoint

The customer must provide for KMD Identity a link to the SAML metadata that describes their identity provider configuration. This metadata must be publicly accessible from the Internet so that it can be periodically read and monitored for changes.

KMD Identity monitors the endpoints frequently and changes configuration based on the metadata file. The customer must ensure at least 24 hours has passed, after adding new certificates to the metadata file, before deleting old certificates.

This metadata must contain organization information including an e-mail and/or phone number that we may use to contact the customer if there are issues with the federation setup.

5.4 Service Provider metadata endpoint

Once KMD Identity has received the SAML metadata of the identity provider, we will create and provide a link to a SAML metadata endpoint with the configuration describing our service provider.

This metadata endpoint is unique per customer.

When setting up a trust for our service provider, make sure to monitor the metadata endpoint for changes. At minimum our metadata must be monitored, and any changes applied daily. This is essential to avoid downtime when we renew our certificates.

6 Getting started

To get started simply write to identity@kmd.dk verifying that you understand and accept the requirements described in this document. Include in the mail the URL to your identity provider's metadata endpoint.

We will then perform the necessary configuration on our end and reply with a link to the metadata endpoint of our service provider and the domain hint that we have associated with your identity provider.

Once you have configured the trust to our service provider as described in this document, things are in place to test the new federation. This can be done using any of the test applications listed here: https://test.identity.kmd.dk/ and the domain hint we have provided.

Please inform us of the outcome of this test, as we do not have the means to authenticate as a user in your organization.

6.1 Special circumstances

Some identity provider solutions generate metadata URLs that are unique per trust relationship. As an example, Microsoft's Entra ID (formerly known as Azure AD) supports "Single-Sign On" via SAML using their "Enterprise Applications" feature.

This can potentially result in a "chicken and egg"-type situation where both parties in the trust relationship would like to receive the metadata of the other before providing a link to their own.

With Entra ID, there exists a workaround in the sense that you do not need to complete the setup of the enterprise application fully before being able to copy its "App federation metadata url".

If you cannot provide a link to the metadata of the identity provider solution that you are using, before having received the metadata from the service provider, then KMD Identity can generate service provider metadata using placeholder data. We will then update the configuration on our end after having received the true metadata URL of the identity provider. Once this bootstrapping has been done, testing can commence.

If this “chicken and egg” scenario applies to your identity provider solution, please specify so when contacting us.

7 Contact

For general questions and support write to: identity@kmd.dk

Secure mails can be sent to: identity@sikker.kmd.dk

The certificate used to verify our digital signature, and to send us encrypted mails, can be looked up at this url: https://erhvervsadministration.nemlog-in.dk/search

8 Version

Version	Date	Description	Edited by
1.0	2021-07-23	Initial version	MTA
1.1	2022-03-28	Added information about which claims are optional. Minor changes.	MTA
1.2	2024-06-12	Made clarifying changes to sections 4 and 6.1. Updated link to website in section 7.	MTA