Frequently Asked Questions (FAQ)

This document is subject for continuous update. The aim is to answer typical questions from various EPIM ID stakeholders as listed below.

Stakeholder	Description
User Organization	Any organization using one or more of EPIM's application Services
Application Users	Any member of staff in a User Organization with access to one or more EPIM application services.
Contract Administrators	Any member of staff in a User Organization's responsible for the contracts towards EPIM available on http://www.epim.no/terms.
Application Super User	Any member of staff in a User Organization administrating user accounts for Application Users in an EPIM application (e.g. L2S Superusers).
EPIM ID Administrators	Any member of staff in a User Organization mandated to approve, suspend and delete EPIM ID accounts. This is a new role introduced by introduction of EPIM ID.
Identity Management and HR Staff	Staff in a User Organization dealing with joiners/ leavers/ movers processes within own organization.

Please issue unanswered questions to operations@norog.no.

Contents

1 Application Users

1.1 What is EPIM ID?

EPIM ID is EPIM's common user authentication service to be gradually taken into use in all relevant EPIM applications. It will allow users to access EPIM's web applications securely from Internet, by re-using existing 3rd Party identities like Bank ID to access the EPIM service.
For more details please have a look at the presentation called "EPIM ID Introduction" available on https://epim.no/epim-id/.

1.2 What can EPIM ID be compared with?

EPIM ID have similarities with how Apple, and Google have established their own user account regime, Apple ID and Google Account allowing their users to access all their services using the same common user account. It also has great similarities how the Norwegian government is using ID-porten as common access regime for access to public facing governmental IT services.

1.3 How do I sign up for an EPIM ID account?

You initiate the EPIM ID sign up process via the "Sign-up" link available on the start page of each EPIM ID integrated EPIM service, or directly on www.epim-id.no. For more information see information resources available or refer to https://epim.no/epim-id/.

1.4 Which 3rd party identities are supported by EPIM ID for authentication?

EPIM ID currently supports the following 3rd party identities for authentication (repetitive log-in):
- Bank ID token
- Bank ID mobile
- BuyPass (software token mobile phone App available for Android and iOS)
- Single-Sign-On (for user organizations federated with EPIM ID) limited to EPIM Members and Norwegian authorities only.

Note that EPIM ID does not support one-time-password on mobile directly. This is on purpose as EPIM ID's approach is to re-use existing identities, rather than trigger yet another username and password.

1.5 Why do non-Norwegian citizens have to scan passport during sign-up?

EPIM ID relies on doing a positive identification of you part of you signing up for an EPIM ID account.

Currently EPIM ID only supports two identification methods for users in non-federated organizations:
- Norwegian Bank ID (limited to Norwegians with a Norwegian Bank ID)
- Signicat ID Paper (for all other nationalities)

The "Signicat ID-paper" method will part of the identification process require you to show and scan your passport via the camera on your mobile phone or PC. As stated in the EPIM ID privacy policy available on www.epim.no/privacy the scanned picture of your passport will be deleted the same day as you have initiated your sign-up process, and will under no circumstances be stored or made available to any other parties.

EPIM have a goal to be able to offer other identification methods for non-Norwegians in the future, but currently the main limitation is the lack of available trustworthy electronic identities that supports the security level required by EPIM ID. EPIM will have great focus on investigating candidate electronic identities on an ongoing basis together with our subcontractors and add support for theses when they become available.

1.6 How does EPIM ID handle my personal information

Please refer to EPIM ID Privacy Policy available on www.epim.no/privacy.

2   For Contract Administrators

2.1   Is EPIM ID GDRP compliant?

EPIM ID is GDPR compliant. End users will, part of establishing their EPIM ID account, be presented the EPIM ID privacy statement as a link to www.epim.no/privacy. This includes easy understandable description of how EPIM ID processes the individual user's Personal Identifiable Information (PII), aligned with the GDPR regulations.

2.2   How is EPIM ID be embedded into the service terms

EPIM services integrated with EPIM ID will have the EPIM ID integration described in the service specific terms on www.epim.no/terms.

3   For EPIM ID Administrators

3.1   What is an EPIM ID Administrator?

Each EPIM user organization will need to appoint, and maintain, at least two individuals acting as EPIM ID Administrators. EPIM ID Administrators responsibilities include but are not limited to:
- Approve or reject EPIM ID account requests from staff in own organization.
- Delete EPIM ID account when staff leaves the organization.
- Suspend EPIM ID account for staff on temporary leave.
- Manage email domains associated with the organization record in EPIM ID.

3.2   What interface is provided for EPIM ID Administrators?

EPIM ID Administrators will have access to administrative functions via the EPIM ID self-care portal available at https://epim-id.no. A separate guide for EPIM ID Administrators will be become available. The interface is very simple and intuitive.

4   For Application Superusers (e.g. L2S Superusers)

4.1   How will existing users in EPIM's applications be enrolled in EPIM ID?

The answer is application specific, but users must sign up for an EPIM ID account as further described on https://epim.no/epim-id. This is to ensure GDPR compliance.

4.2   How does the EPIM ID account relate to Application Accounts?

Each EPIM service, e.g. L2S, will still have user application account after having taken EPIM ID into use. But the application account will have 1:1 association to an EPIM ID account, where:

- EPIM ID account is used for authentication (prove identity) of the user,and will be re-used across EPIM applications.
- Application account is used by the application to set up application specific access rights for the application (authorization).

When logging into an EPIM application, user is first requested to prove own identity (authenticate) using his/her EPIM ID account. After successful authentication the application will look up any application account associated with the given EPIM ID account. If a match is found the user is granted access into the application, based on the access privileges defined by the applications internal user account.

4.3 What happens to Application user account if user's EPIM ID account is suspended or deleted?

This is an application specific design decision. EPIM ID do not push information about EPIM ID account closure but offers a machine interface for applications to request information about EPIM ID user account state.

4.4 How do I handle staff leaving my company?

It is the EPIM ID Administrator (ref section 3.1) responsibility to close EPIM ID accounts for staff leaving the organization. This will lead to the user no longer being able to log into any applications using EPIM ID as log-in method.

As the second barrier, EPIM ID will automatically suspend accounts after two months if account verifications are not received. Six months after an EPIM ID account has been suspended it will automatically be deleted.

Superusers must close the user application accounts unless the application caters for this automatically. Check application superuser guide for details.

5 For Identity Management and HR staff

5.1 May Federation be used to improve the user experience and usage efficiency?

Yes, EPIM's members may apply for Federation between own Active Directory and EPIM ID using ADFS. Generally, the member applying for federation must document that internal authentication has a two-factor security level, equivalent to methods offered by EPIM ID.

5.2 Does EPIM ID offer an API for automatic status update of EPIM ID accounts?

EPIM plan to offer such integrations in a later phase.

5.3 How will EPIM ID provide "Leavers" handling

Initially the following leavers functionality will be set up to challenge users on monthly basis to confirm that their account is still in use. EPIM ID will then suspend any accounts where user does not confirm access to own company email account within 1 month. EPIM ID Administrators will receive information about any suspensions in progress.

5.4 How will existing EPIM user organizations be enrolled into EPIM ID

EPIM will facilitate enrolment for existing user organizations. This will be part of transition activities when an EPIM service take EPIM ID in use. This will involve information packs from EPIM both towards the user organisation administrative contact points as well directly to end users of the services to ensure a smooth transition.