EPIM ID

Special terms

Version: April, 2018

Content

1 Definitions and Abbreviations

In addition to definitions and abbreviations in the General terms section 1, the following shall apply to the Agreement with regards to EPIM ID:

Term	Definition
Identity provider	An issuer of digital identity being integrated with EPIM ID, e.g. Norwegian BankID, User organisation itself or EPIM.
Applicant	A member of staff in a User organisation who has a need to sign-up for an EPIM ID account.
Authentication	The process of challenging a User with the aim of doing a positive confirmation of the User's identity.
Authorization	The process of verifying a User's access rights/privileges to resources within an application service after first having been Authenticated.
Single sign-on (SSO)	A mechanism allowing Users to re-use an active EPIM ID authentication token when accessing other EPIM ID integrated applications, without a need for Users to authenticate again.

2 Service

2.1 Description

EPIM ID is a common login solution for Authentication used across EPIM's Service portfolio. It allows Users to re-use the same log-in method in all EPIM Services.

EPIM ID is based on these principles:

1) The Applicant requests creation of an EPIM ID account by completing a sign-up process.
2) The EPIM ID Administrators, in the Applicant's User organisation, approve/decline creation of account requested.
3) The EPIM ID Administrators are responsible for deleting EPIM ID user accounts when staff leave the User organisation.
4) The users must reconfirm their relation to the User organisation periodically to remain active.

The Applicant signup for an EPIM ID account is further described in section 2.3.1, and as part of the sign-up process the account will establish a direct relation to:

- User organisation, by account name being the personal company email address.
- Identity provider, to be used for recurring Authentication purposes.

Identity provider may belong to one of the categories below:

1) **3rd Party Identity providers** such as e.g. Norwegian BankID, where the list of EPIM ID supported 3rd Party Identity providers will change over time.
2) **User organisation** via an established federation (for detail refer to section 2.2)
3) **EPIM** as a fall-back solution for Applicants that cannot use the above methods.

EPIM ID do not store any passwords, but instead require the User to authenticate itself through dialog with the Identity provider linked to the EPIM ID account. Note that Users may only link one Identity provider to their EPIM ID

account at a time. Changing Identity provider requires User to initiate self-service based deletion of own user account, followed by a sign-up for a new account.

EPIM ID only handles Authentication, while Authorization is handled by each individual EPIM Service according to Service specific access management procedures. Refer to Special terms for at www.epim.no/terms for details.

EPIM ID by default provides Single sign-on (SSO) experience for Users with application accounts in multiple EPIM Services integrated with EPIM ID, when already authenticated towards one Service.

For more functional descriptions of EPIM ID please refer to information on www.epim-id.no.

2.2 Federation

EPIM ID allows certain User organisations to establish an integration with EPIM ID, allowing the User organisation to act as Identity provider. This offer is limited to User organisations being EPIM Member organisations and selected Norwegian government agencies. Note that User's from federated User organisations cannot use the other Identity Provider options for log-in purposes to Services.

2.3 EPIM ID Account management

Section below provides a high-level description of the various EPIM ID account lifecycle processes.

2.3.1 Sign-up

EPIM ID account creation process:

1. Applicants sign up for an EPIM ID account via a sign-up form available from the individual EPIM Service log-in page, and on www.epim-id.no. Part of sign-up process Applicant must:
    a. Prove access to the personal company email address to be associated to the account.
    b. Applicants from non-federated User organisations must prove own identity using one of the supported methods, e.g. Norwegian BankID, or use the supported manual identification methods e.g. web based dialog involving scanning passport in combination with face recognition.

2. Following a successful identification of the Applicant in step 1, an EPIM ID Administrator, in the Applicant's organisation, receives a notification from EPIM ID, about a pending EPIM ID user account request, and must approve or reject the account request via the EPIM ID Administration module, that EPIM ID Administrators will have access to.

3. After EPIM ID administrator approval Applicant will be informed about successful account registration and may log-in to their EPIM ID account by use of the chosen Identity provider.

2.3.2 User Profile updates

Non-federated Users can manage their personal information via their EPIM ID personal profile on www.epim-id.no. For federated User's, EPIM ID maintains the EPIM ID account automatically with information from the User organisation, without Users being allowed to modify their EPIM ID profile themselves.

2.3.3 Suspension

EPIM ID supports users to be suspended. A User's EPIM ID account can be suspended by:

1. An EPIM ID administrator suspending the User from the EPIM ID Administration module.
2. EPIM ID automatically suspending the account based on built-in polices implemented for security reasons, where examples of such policies are:
    a. User do not respond to re-confirmation requests sent on email to the User's company email.
    b. Suspect use patterns indicating misuse of an EPIM ID user account.

2.3.4 Re-activation

EPIM ID Administrators can, from the EPIM ID Administration module, re-activate any suspended user accounts limited to users from own organisation.

2.3.5 Deletion

An EPIM ID account can be deleted in following ways:

1. An EPIM ID Administrator in a User organisation deletes the EPIM ID account, when the User no longer require having an EPIM ID account, e.g. in case of leaving the User organisation.
2. Non-federated Users can initiate deletion of own account from the EPIM ID personal profile available www.epim-id.no.

2.3.6 Account review

EPIM ID will part of internal automatic processes sometimes require the EPIM ID Administrators to do certain review activities of own users. This includes but is not limited to:

- Review of the list of appointed EPIM ID Administrators in own organisation.
- Review of suspicious activity on a User's account.

Such notifications will be sent via email regarding pending actions within the EPIM ID Administration module.

2.4 Email domain management

A User organisation may have multiple email domains in EPIM ID. EPIM ID Administrators can manage email domains within the EPIM ID Administration module. For more info refer to help section on www.epim-id.no.

2.5 Support

1. Problems related to log-in to Services using EPIM ID for Authentication must be routed via that Applications support arrangements, as described in each Specific terms on www.epim.no/terms.
2. Support, related to problems a User's third party Identity provider's electronic identity, must be routed to the given Identity provider's support option.

2.6 Service level

EPIM ID for Authentication is an integral part of the Services that have taken EPIM ID into use. For details, reference is made to section "Service level" in the Specific terms of the given Service available on www.epim.no/terms.

2.7 Data management

EPIM ID only stores limited non-sensitive data related to User's EPIM ID account. For more information see EPIM ID Privacy Policy available at www.epim.no/privacy.

3 Service fees

EPIM ID does not impose any extra Service fees, but is integrated into the fees for the given Service using EPIM ID for user Authentication.

4 Security

Terms as stated in General terms section "Security" applies with following additions:

- EPIM ID will assure that 3rd Party Identity Providers supported by EPIM ID require multi-factor Authentication.
- EPIM ID only shares limited user information with the Services for the distinct purpose of managing User Authentication.

5 Processing of personal data

Terms in the General terms section 5 – "Processing of personal data" applies. The EPIM ID Privacy Policy is available at www.epim.no/privacy.

6 Termination

EPIM ID is not delivered as a stand-alone EPIM Service, but is an integrated part of the log-in process in each Service integrated with EPIM ID. The User organisation is responsible for deleting EPIM ID accounts concerning own Users prior to terminating the last EPIM Service using EPIM ID for Authentication purposes. Lack of such account deletion will otherwise trigger EPIM to delete all the accounts no later than 6 months after.

7 EPIM's additional obligations

EPIM shall use commercially reasonably efforts to ensure that:

1. EPIM ID includes functionality for evaluating and handling account security, with the goal of preventing unauthorised use of EPIM ID accounts.
2. EPIM ID includes an automated re-confirmation of Users' relation to User Organisations to ensure accounts for staff leaving a User Organisation is suspended automatically.
3. EPIM ID is developed in a way that has the correct balance between usability and security.

8 User organisation's additional obligations

The User organisation is responsible for:

1. Appointing and maintaining minimum two EPIM ID Administrators for managing the User organisation's use of EPIM ID.
2. Continuously ensuring the EPIM ID user accounts are valid, so that if a member of staff quits or no longer have a valid need for an EPIM ID account, the EPIM ID account is deleted as soon as possible and at latest within 2 business day.
3. Integrating management of EPIM ID accounts into internal procedures.
4. Ensuring that the User organisation's own Users:
    a. Comply with the security and administrative regulations as notified by EPIM in conjunction with registration and use of the EPIM ID account, by e-mail, via EPIM Service web pages, or in any other manner.
    b. Understand that the EPIM ID Account registration form should be filled out by the individual requesting an EPIM ID account.
    c. In conjunction with registration, provide correct information regarding the User's identity and a correct and legitimate e-mail address.
    d. Do not share their EPIM ID accounts or allow others to use their EPIM ID accounts.
    e. Notify relevant staff in own organisation regarding any suspected breach of security.
    f. Are at least 16 years old when creating an EPIM ID account.

9 Governance

EPIM ID is governed in dialog with EPIM's Members, using EPIM's governance model.