NordPass® | Password Manager

NordPass Business Whitepaper

Last updated on 2025/01/08

Version 1.9

Table of Contents

Table of Contents

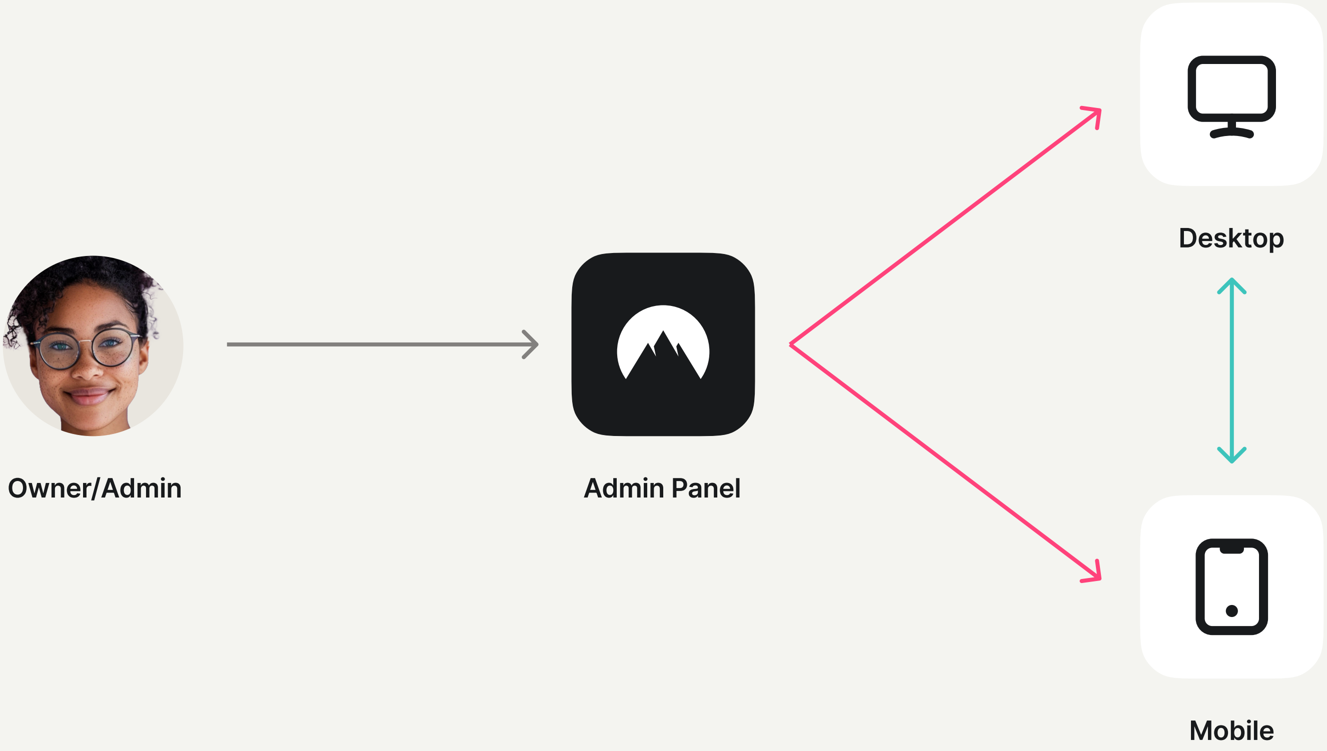
Introduction
What is NordPass Business?

In the digital age, when cyber attacks on companies number in the millions, the NordPass Business password manager has been created to address the access security needs of small and medium-sized enterprises as well as large corporations. It provides organizations with a secure and easy-to-use platform where they can store, access, and share work-related passwords, passkeys, credit card data, personal information, and secure notes.

We focus on supplying users with the best tools to address not only poor password security habits but also broader security concerns. That's why NordPass offers advanced tools such as the Data Breach Scanner, NordPass Authenticator, Email Masking, and Password Health.

The NordPass community is the foundation of our product. We always collect feedback from our users and use it to further improve NordPass. Make sure to share your feedback in the app, via the Admin Panel, or by simply dropping a message in the chat with our Support team at the NordPass Help Center.

The NordPass Business product consists of the Admin Panel (a platform where you can invite and manage users) and the NordPass vault in the form of a browser extension or a mobile app.



Introduction
Main security principles

NordPass uses the following security principles as its foundation:

State-of-the-art encryption algorithms

Encryption is the foundational part of the entire NordPass security structure. We strive to bring our users an easy-to-use, foolproof method for securely storing their passwords and other sensitive data such as passkeys, credit cards, personal information, and secure notes. This is made possible with the help of the top-tier elliptic curve encryption library NaCl.

We chose the ChaCha20 family over AES because the performance of the latter heavily relies on the hardware features (such as the AES instruction set for x86 processors), which are rarely available on mobile devices.

End-to-end encryption

NordPass' end-to-end encryption minimizes the risk of sensitive data exposure at any step of the way. NordPass is built to encrypt data locally and only then move it to the cloud. This means that the NordPass team cannot view or access your items—only you can. And, in the unlikely event that your data ends up in the wrong hands, they would see nothing but gibberish.

Extra security layers

To ensure multifaceted protection, we provide users with multiple layers of security. As an organization, you can require your users to sign in with corporate single sign-on, multi-factor authentication, and replace their Master Passwords with biometric authentication.

Secure item sharing

NordPass doesn't just store your items but also allows you to share them directly or in a Shared Folder. Passwords, passkeys, credit cards, and secure notes are end-to-end encrypted and protected from prying eyes. Additionally, NordPass is capable of storing TOTP codes for logins, improving the security and usability of shared credentials.

Transparency

At NordPass, we believe that any claim we make about cybersecurity must be validated. To this end, we've been thoroughly audited by third-party security auditors. Audits help us find new and better ways to ensure our customers' data protection.

Business authentication

Business authentication is built on the OAuth 2.0 protocol, which acts as a centralized identity provider and authorization server for NordPass. The implementation of the OAuth 2.0 protocol for business authentication is fully compliant with the Internet Standards created and published by the Internet Engineering Task Force (IETF) and is also in line with the current best security practices.

How does NordPass work?
Terminology explained

Identity

Right now, a single user has only one related identity. In the future, a user might have more than one identity, but in the scope of this chapter, an identity is equivalent to a single user.

Item

A record that contains sensitive data such as a password, passkey, credit card number, credentials, etc.

Folder

An item type used as an organizational unit for grouping items. Folders can be segmented into several categories:

- **Root folder:** Invisible folder that contains all identity vault items. Root folder is created with the new identity vault.
- **Personal folder:** A private folder enclosed by a root folder. Created manually by an identity, a personal folder can hold multiple identity-owned items but cannot be shared.
- **Shared folder:** An identity-owned and transferable folder within the organization. Access to Shared Folders can be shared with identities and groups.

Group

An item type used as an organizational unit for grouping identities.

Access grant (or relation):

A linking record in our database that serves two functions:

1. To identify a relation between an item and an identity, folder, or group. This means that if there is no access grant between an item and an identity, the user related to that identity won’t be able to access the item.

2. Provides item access to the private key encrypted with the identity's public key. In other words, it carries cryptographic information about the relation of one identity and one item required to access the item's content. This means that even if a user receives access to a certain item but has no access grant to it (the item), the user will still not be able to access the item’s contents. If a user receives someone else’s access grant, the ability to access the item's contents remains fully restricted.

Accessing and sharing items

Every identity, item, folder, and group has asymmetric access key pairs. It's more complex than that (learn more in the **Encryption** section), but to simplify things in this chapter, let's assume that there is only one asymmetric key pair.

There can be a plethora of identities and items in our database, but only a few of them have access grants (relations). For example, in Figure 1, “Identity 1” has two access grants (relations): “Identity 1” with “Item 2” and “Identity 1” with “Item 6.”

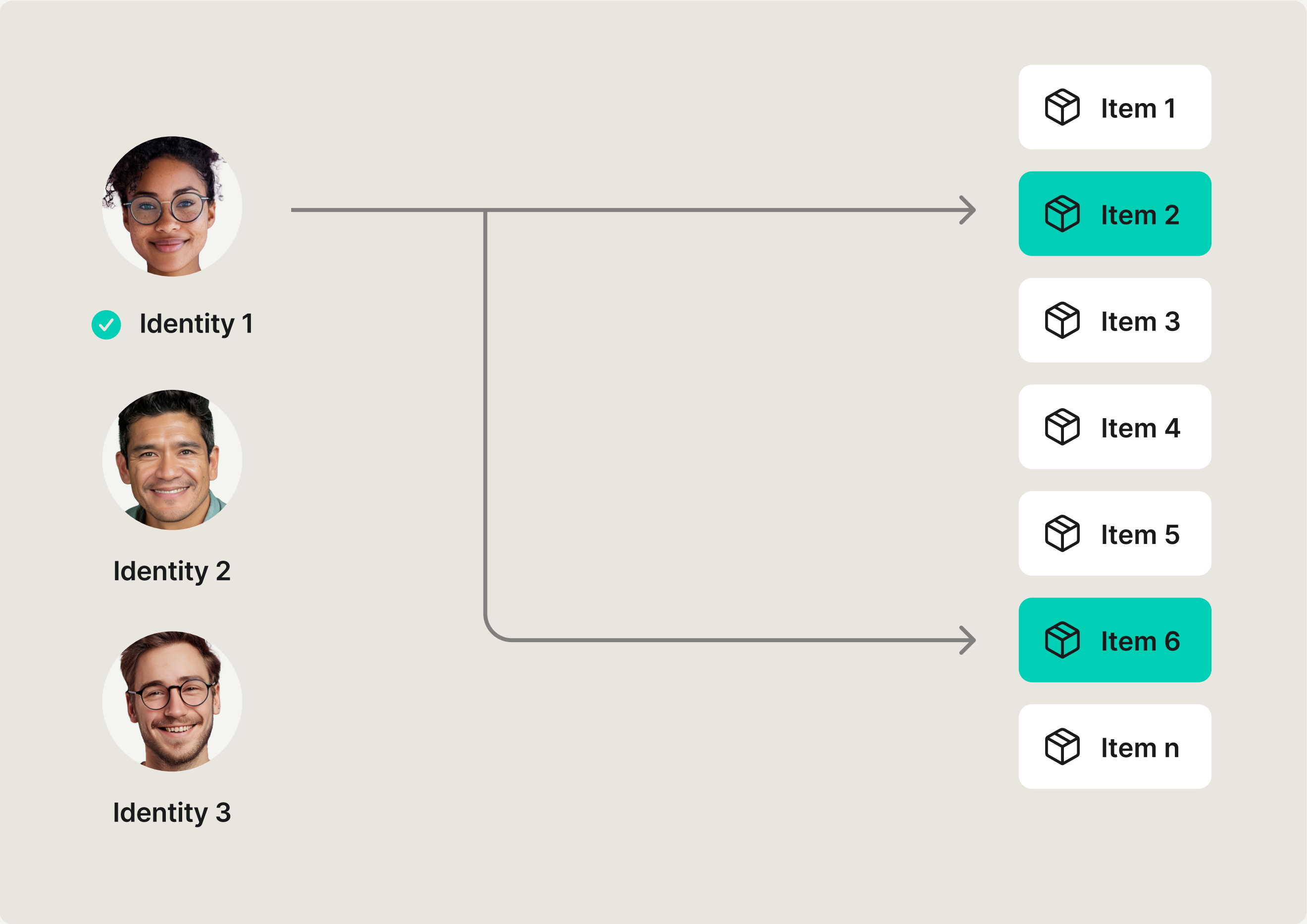


Fig.1 General view

So, when the user associated with “Identity 1” logs in, NordPass:

1. Selects access grants (relations) associated with that identity.
2. Selects items associated with these access grants (relations)

So, we end up with a view as in Figure 2:

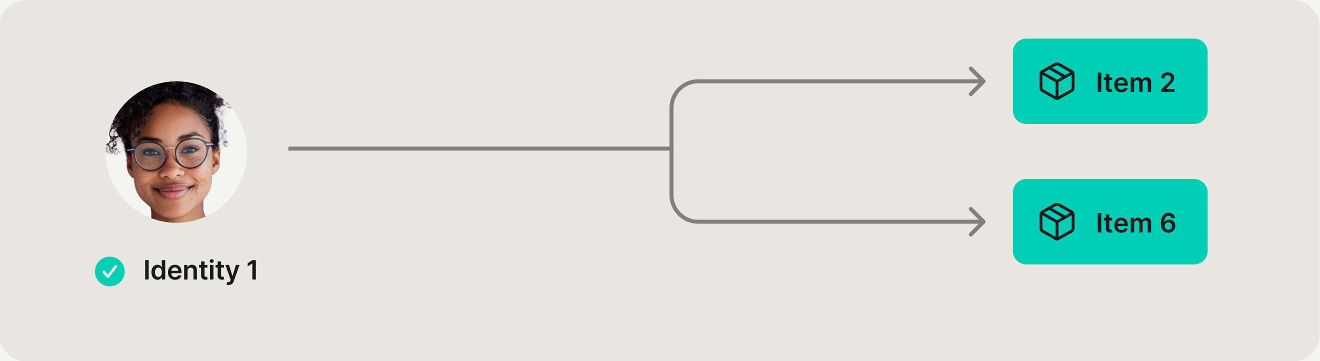


Fig. 2 Identity and related items

As mentioned above, the access grant (relation) isn’t a simple line—it’s a link record (see Figure 3). To create an access grant (relation), the item’s private key has to be encrypted with the identity’s public key (red line). To access the item, the identity has to use its private key with the access grant (relation) (green line) and get the item's private key.

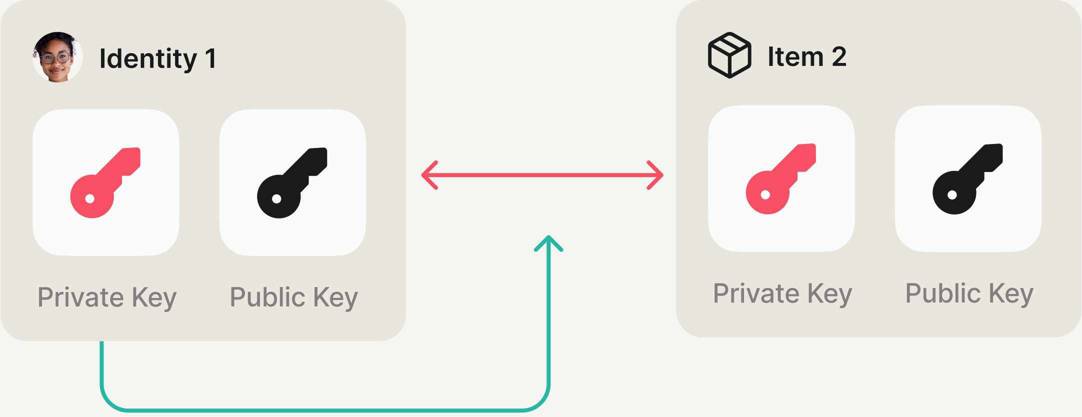


Fig. 3 Access grant (relation)

For **"Identity 1"** to share **"Item 2"** with **"Identity 2,"** the following steps must take place (see Figure 4):

1. An access grant (relation) between **"Identity 1"** and **"Item 2"** must exist (red line).
2. **"Identity 1"** must use its private key on the access grant (relation) (green line).
3. **"Identity 1"** must receive the public key of **"Identity 2"** (black line).
4. Encrypt **"Item 2"** private key with **"Identity 2"** public key (black dotted line) and create a new access grant (relation) (red dotted line).
5. Only now can **"Identity 2"** see **"Item 2"** (Fig. 1 and Fig. 2) and apply its private key to that new access grant (relation) to access **"Item 2"** (green dotted line).

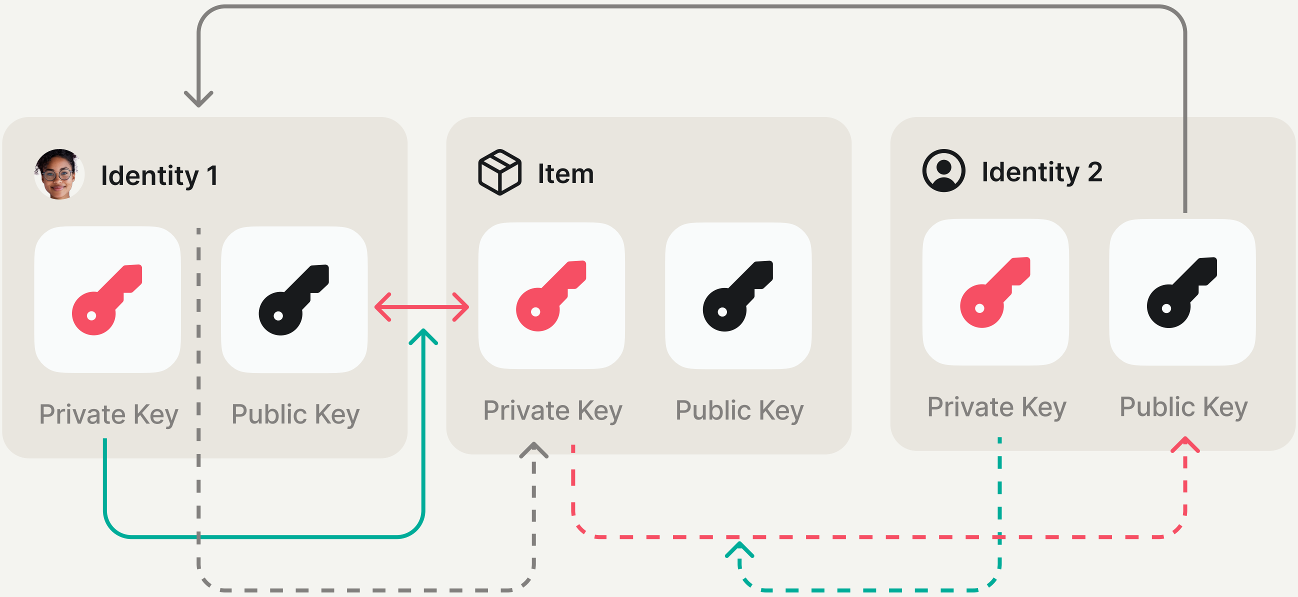


Fig. 4 Sharing an item with another identity

IMPORTANT NOTE: Notice that after **"Identity 1"** shared **"Item 2"** with **"Identity 2,"** a new access grant (relation) was created, but only one instance of **"Item 2"** remains. This means that we neither share a snapshot of the item nor duplicate it. It also means that if either identity makes any changes to **"Item 2,"** it will instantly affect all the identities (folders, groups) that have access grants (relations) to **"Item 2"**—they will all be able to access the updated version of the item.

Item access via folders

Now that we have an understanding of access grants (relations) and sharing, let's take a look at a more complex example (see Figure 5). Here, the identity is accessing items not directly but via an organizational item type called a folder (folders have their own key pair).

1. A folder has access grants (relations) with items, or, in other words, each item's private key is encrypted with the folder's public key (red dotted lines).
2. To access the item, the folder's private key has to be used on an access grant (relation) (green dotted lines).
3. Identity has an access grant (relation) with the folder (red line).
4. To access the folder, identity has to use its private key on that access grant (relation) (green line). By getting access to the folder's private key, identity inherits its access grants (relations) with items (red dotted lines).

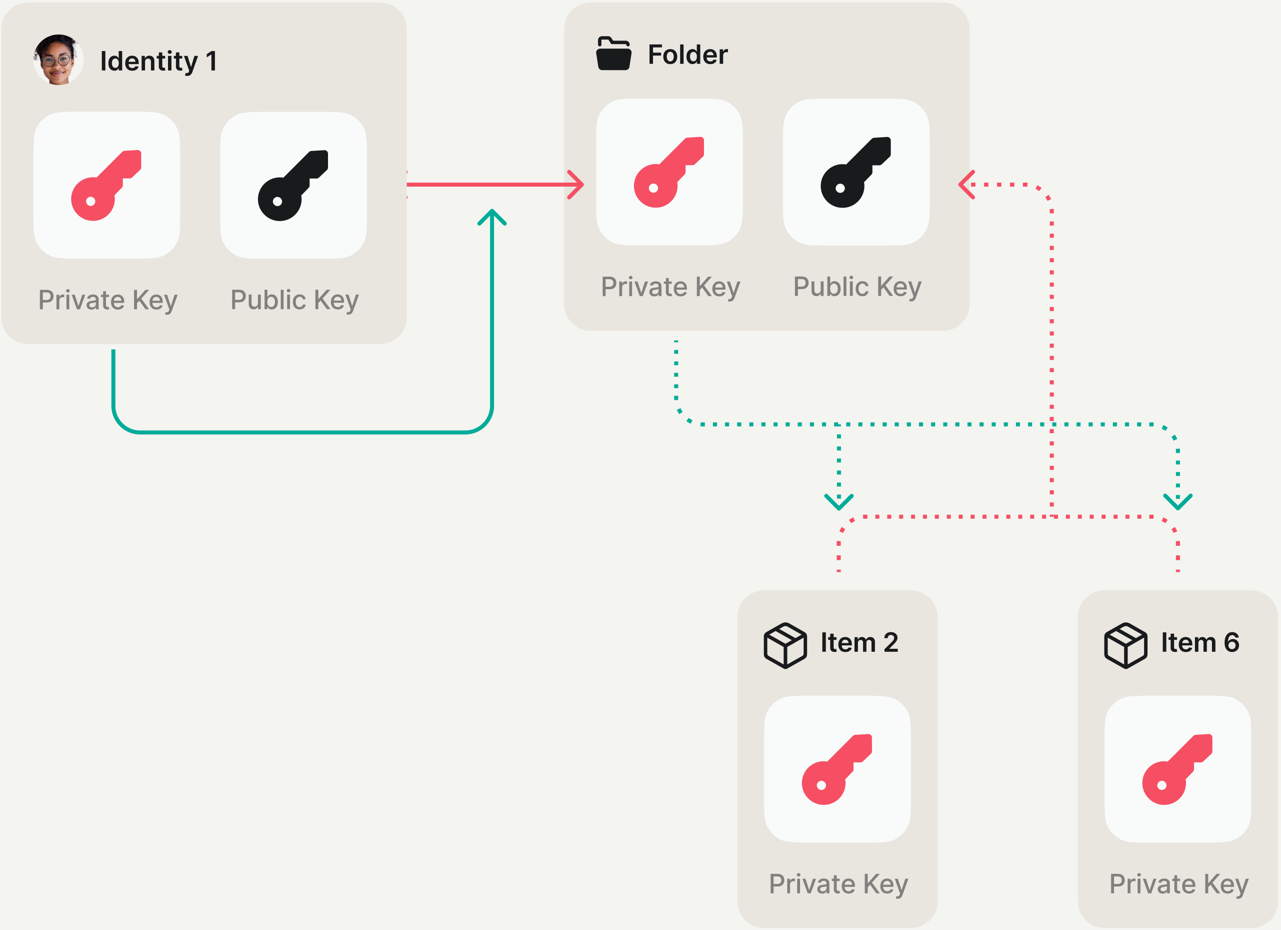


Fig. 5 Accessing items grouped in a folder

Shared Folder access via Groups

Let's take one step further and group not only items into folders, but identities into groups, which have their own key pairs (see Figure 6).

1. A folder has access grants (relations) with items (red dotted lines).
2. To access items, the folder's private key has to be used on an access grant (relation) (green dotted lines).
3. The group has access grant (relation) with the folder (red dashed line).
4. To access the folder and inherit access grants (relations) with the items (dotted lines), the group's private key has to be used on an access grant (relation) (green dashed line).
5. Identities have access grants (relations) with the group (red lines).
6. To access the group, identity has to use its private key on the appropriate access grant (relation) (green line). By getting access to the group's private key, identity inherits its access grant (relation) with the folder (dashed line) and items (dotted lines).

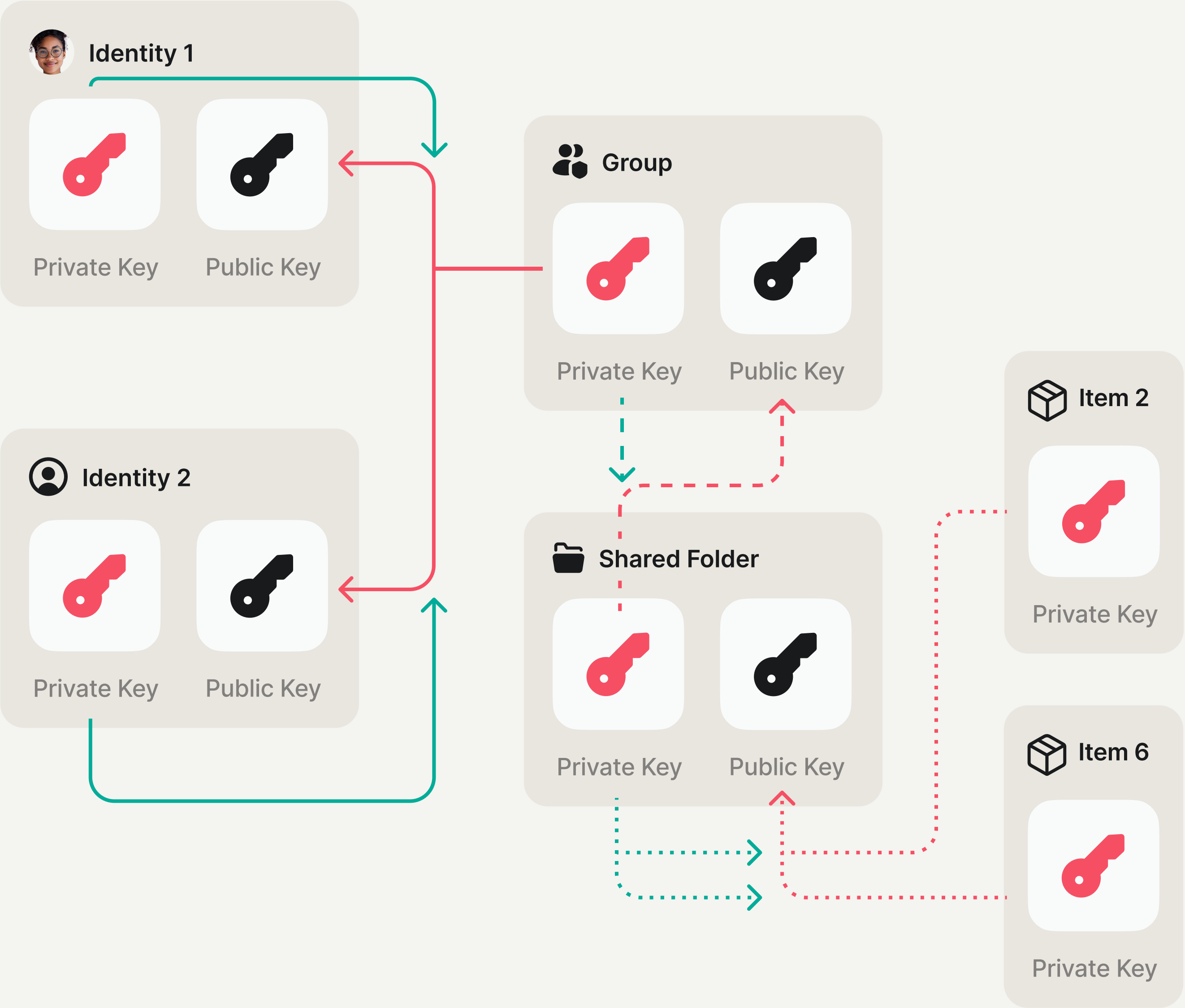


Fig. 6 Accessing items grouped in a folder

NordPass Business structure

Now that we've covered all the building blocks, we can take a look at the actual (although simplified) structure of the NordPass Business solution:

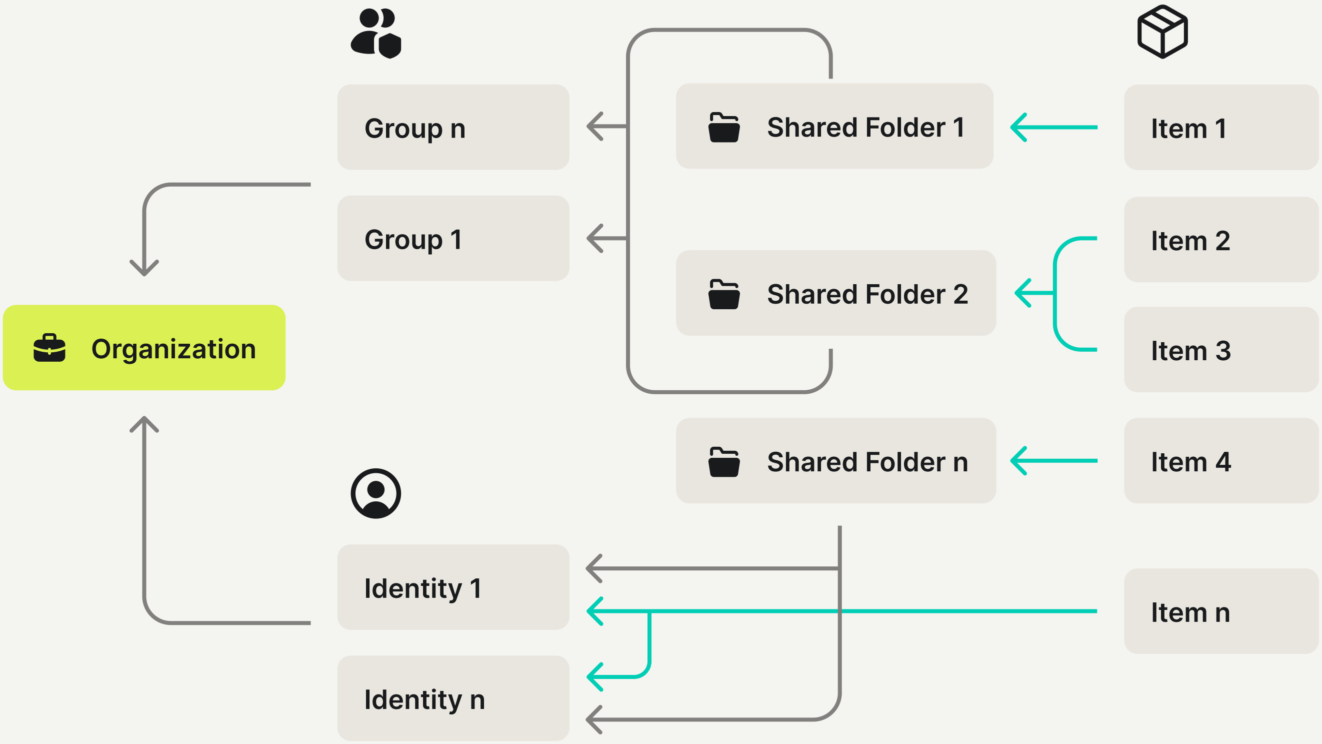


Fig. 7 Simplified architecture of the organization

In this diagram of the organizational structure, we see a refined approach to access management, with a focus on the role Shared Folders play in permission management.

Shared Folders provide the basic building block of this structure. They can hold multiple items and be shared with both identities and groups.

Due to the kind of structure displayed above you can directly share an item with an identity, as well as multiple identities at once, but not with a group. All of this enables an identity to manage and access numerous items as well as multiple Shared Folders.

It is important to note that in this kind of structure, an item can only exist within a single Shared Folder at a time.

Encryption technology explained

Now, let’s have a deeper look into encryption. When using NordPass Business, your organization always retains ownership and control over its data. In other words, if an employee creates an item, the access is instantly granted to that employee, and they can manage that item in NordPass. But, if the employee leaves the company, their items stay within the organization and can be reassigned to another member. The organization can also recover employees’ accounts without the risk of losing any data.

This functionality is facilitated through the framework of public-key cryptography, which generates data security at all times while allowing for smooth management, recovery, and reassignment of items.

NordPass uses the highly secure **Argon2id function,** combined with a unique 16-byte salt, to derive your Master Key, which is used to encrypt your private key. This approach ensures your data remains protected and that only authorized users can access the sensitive data stored in NordPass.

- **Symmetric encryption (secret-key cryptography)**
  NordPass uses **XChaCha20** for encryption, along with **Poly1305** for message authentication (MAC).

  - XChaCha20 encrypts data in a continuous stream, offering faster performance compared to traditional block ciphers like AES, particularly when handling large or variable-sized data. Thanks to its lightweight design, XChaCha20 ensures quick encryption and decryption, making it ideal for real-time encryption needs, like password management.

- **Asymmetric encryption (public-key cryptography)**
  NordPass uses a combination of **X25519** and **XSalsa20** encryption for key exchanges, **XSalsa20** stream cipher for encryption, and **Poly1305** for MAC authentication.

  - The **X25519 key exchange** is an elliptic-curve Diffie-Hellman (ECDH) algorithm that enables two parties to securely exchange cryptographic keys over an insecure channel. Even if someone intercepts the communication, they won’t be able to access the shared secret key.
  - The **XSalsa20 stream cipher,** similar to XChaCha20, is highly efficient, offering both speed and security across various hardware platforms. It's especially useful in scenarios where low-latency encryption is critical.

Each NordPass user possesses their own cryptographic key pair. The public key is sharable, while the private key never leaves your device; it is encrypted with XChaCha20-Poly1305-IETF on the user’s device before being stored, making sure that it remains secure even in case of interception.

When you unlock your vault, your private key is temporarily stored in secure memory, and it is wiped upon locking—there is no way for someone to gain access thereafter.

Your Master Key is freshly generated each time a Master Password is entered. This process ensures a higher level of security, keeping you in control of your data at all times.

At NordPass, we divide items such as passwords or credit card details into two types:

- **Metadata:** Titles and non-sensitive details which are visible but don't compromise security.
- **Secret data:** Sensitive information, encrypted and accessible only with the right permissions.

This separation allows for flexible permissions, ensuring that your team can see the existing item without accessing its secure contents unless they are authorized to do so.

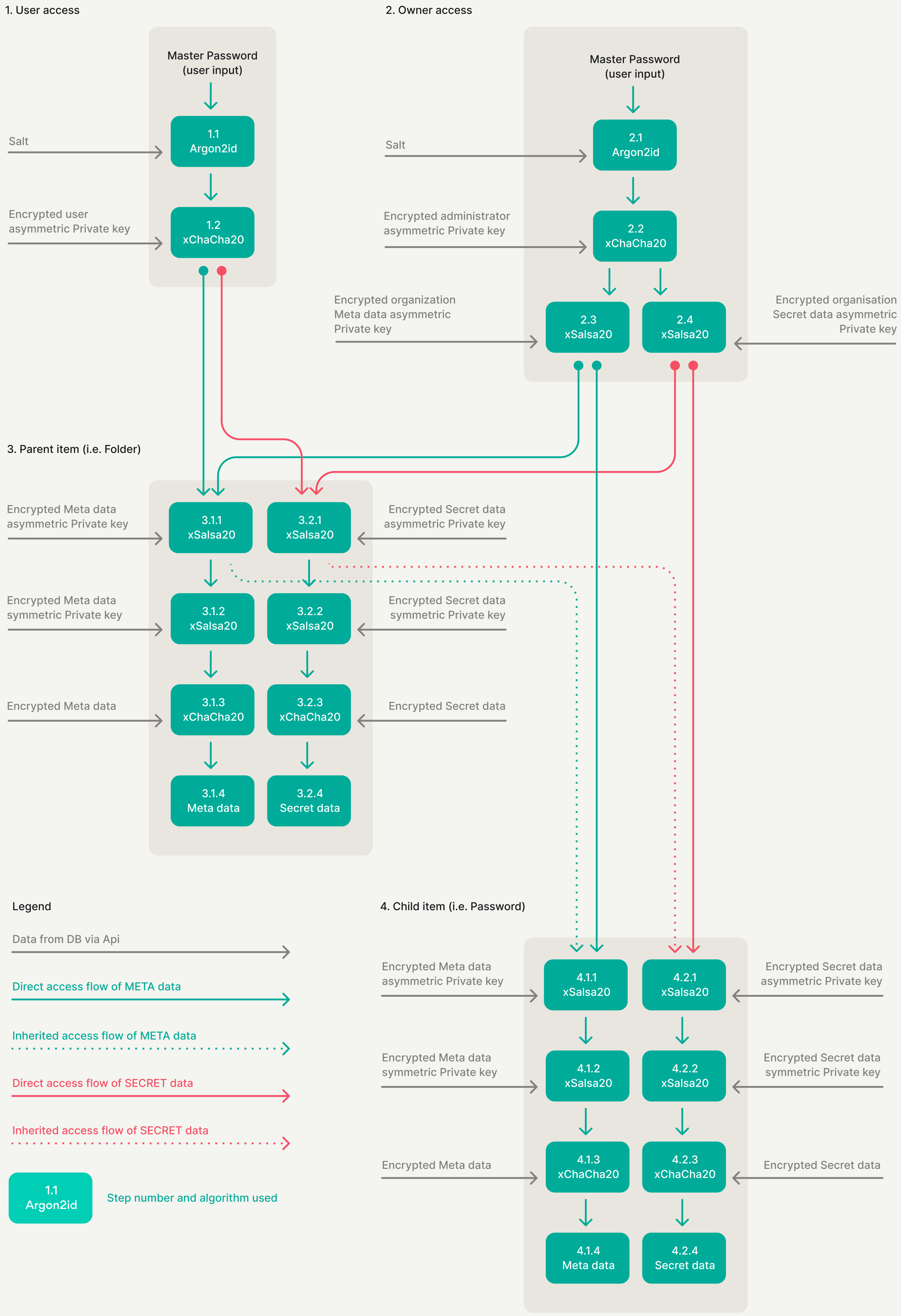
Item access

There are two ways you can access every item stored in NordPass. Let's take a look at what we call the **direct access workflow:**

a. The user is asked to input the Master Password, which, together with the unique-per-user cryptographic 16-byte salt, is used in the key derivation function Argon2id. The result (we call it the Master Key) is used as a key to decrypt the user's private key.
b. The user's encrypted private key is decrypted locally (on their device) with the XChaCha20-Poly1305-IETF algorithm using the Master Key as a decryption key.
c. Since the item comprises two parts (metadata and secret data), the user's private key is used to decrypt the item's metadata private key and secret data private key (or only one of them, depending on the permissions granted to the user).
d. The private key of the item's asymmetric key pair (either the metadata or secret data private key) is used to decrypt the item's symmetric key using the xSalsa20 algorithm.
e. The symmetric key is used to decrypt either an item's metadata or secret data using the XChaCha20-Poly1305-IETF algorithm.

In NordPass, all items are created on the organization’s behalf, and each item’s asymmetric keys are encrypted with the organization’s public keys. This approach guarantees that users who have access to the organization’s keys can access any item as described in the direct access flow.

The key difference between **direct** and **organizational** access is that the user has only one asymmetric key pair, and the organization has two separate key pairs—one for the metadata and another for the secret data. This allows for improved permission granularity, i.e., access only to the metadata of all the organization's items without permission to read the secret data.


1. User access
Master Password (user input)
Salt
1.1 Argon2id
Encrypted user asymmetric Private key
1.2 xChaCha20
2. Owner access
Master Password (user input)
Salt
2.1 Argon2id
Encrypted administrator asymmetric Private key
2.2 xChaCha20
Encrypted organization Meta data asymmetric Private key
2.3 xSalsa20
2.4 xSalsa20
Encrypted organisation Secret data asymmetric Private key
3. Parent item (i.e. Folder)
Encrypted Meta data asymmetric Private key
3.1.1 xSalsa20
3.2.1 xSalsa20
Encrypted Secret data asymmetric Private key
Encrypted Meta data symmetric Private key
3.1.2 xSalsa20
3.2.2 xSalsa20
Encrypted Secret data symmetric Private key
Encrypted Meta data
3.1.3 xChaCha20
3.2.3 xChaCha20
Encrypted Secret data
3.1.4 Meta data
3.2.4 Secret data
Legend
Data from DB via Api
Direct access flow of META data
Inherited access flow of META data
Direct access flow of SECRET data
Inherited access flow of SECRET data
1.1 Argon2id
Step number and algorithm used
4. Child item (i.e. Password)
Encrypted Meta data asymmetric Private key
4.1.1 xSalsa20
4.2.1 xSalsa20
Encrypted Secret data asymmetric Private key
Encrypted Meta data symmetric Private key
4.1.2 xSalsa20
4.2.2 xSalsa20
Encrypted Secret data symmetric Private key
Encrypted Meta data
4.1.3 xChaCha20
4.2.3 xChaCha20
Encrypted Secret data
4.1.4 Meta data
4.2.4 Secret data

Functionality and features
Roles and permissions

In NordPass Business, users are assigned specific roles, each associated with defined permission levels within the organization:

Owner: The Owner is the individual who establishes the NordPass Business account, automatically assuming the highest-level role in the organization. In the NordPass ecosystem, Owners have complete control over member management via the Admin Panel and can set organization-wide settings and policies. Owners also hold exclusive control of the organization's encryption keys and are responsible for all vault items. To mitigate the risk of losing access to critical data, we highly recommended that organizations designate at least two Owners, ensuring recovery in case one Owner forgets their credentials.

Admin: In NordPass, Admins have direct access to the Admin Panel, where they can invite, manage, suspend, or remove members. Admins can also set organization-wide settings and policies but cannot manage or revoke the permissions set or enforced by Owners.

User: Users are provided access to the NordPass vault only. They cannot manage members or enforce company-wide settings. Any user in the NordPass organization can be promoted to Admin by another Admin or Owner.

The table below provides a more detailed overview of each role's permissions:

	Owne	Admin	Use
Access to the NordPass user Vault	✓	✓	✓
Access to the Admin Panel	✓	✓	✗
Invite and manage members	✓	✓	✗
Grant Admin rights	✓	✓	✗
Grant Owner rights	✓	✗	✗
Revoke Owner rights	✓	✗	✗
Revoke Admin rights	✓	✓	✗
Manage account recoveries	✓	✗	✗
Manage Groups	✓	✓	✗
Apply company-wide settings	✓	✓	✗
Access and manage billing information	✓	✓	✗
Transfer items of a deleted member	✓	✗	✗

User accounts

The very first step to using NordPass Business is setting up a Business Account with your professional email. This account allows you to access both your NordPass vault and the Admin Panel.

During the initial setup, you need to create your Master Password, which is primarily used to unlock your NordPass vault and decrypt stored items.

Who are you?

Authentication

Authenticate the user with **Business Account** (email & Business Account password).

Your data

Unlock NordPass

Access encrypted data in NordPass. This can be done using the **Master Password, biometrics, or Recovery Code.**

The Business Account is kept separate from the Master Password, providing an extra layer of security.

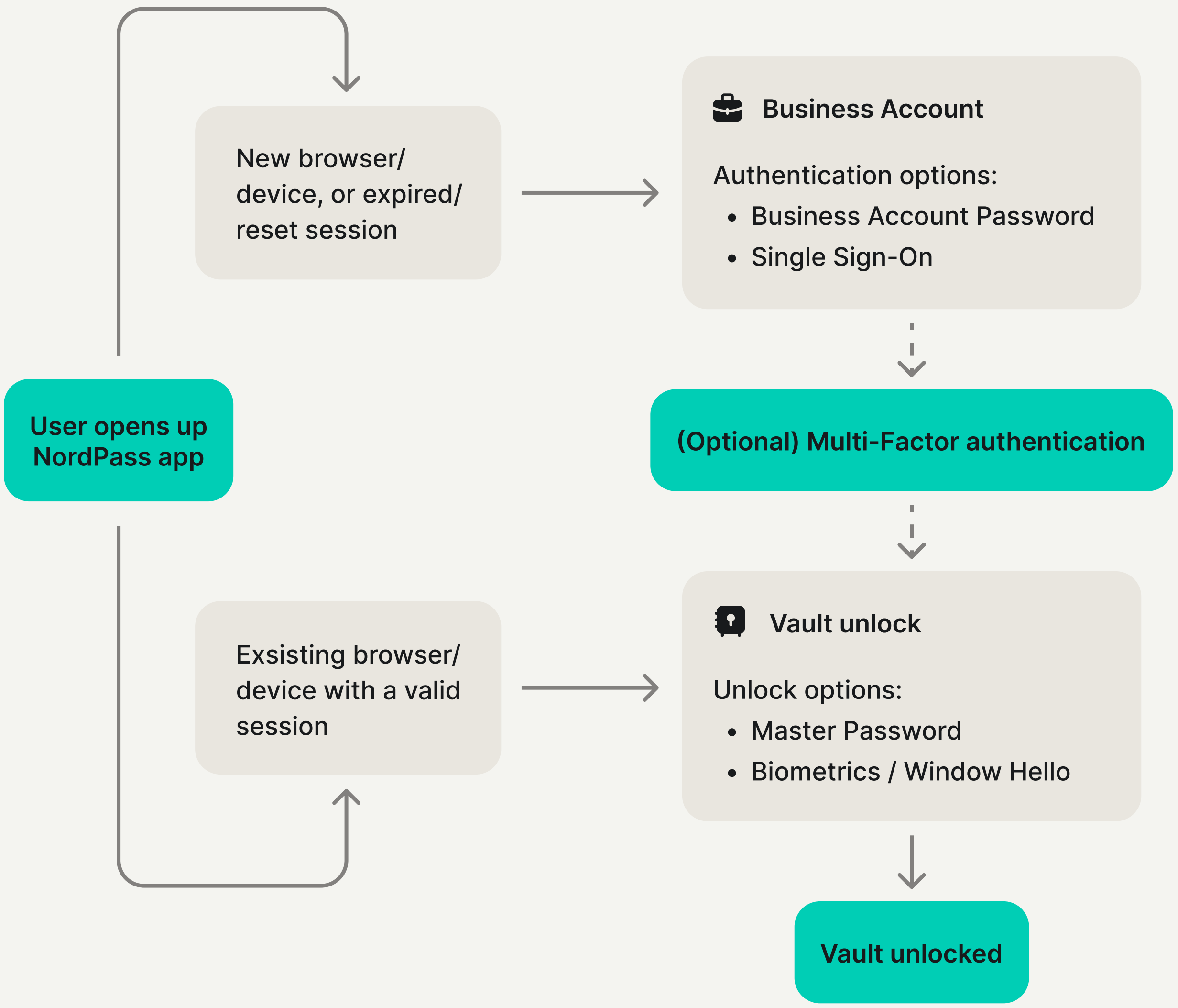
Because the Business Account and Master Password are separated, users must complete two authentication steps to log in to NordPass and access its contents.

You can access your Business Account using:

- **Business Account password:** For users who do not use a managed organizational account or prefer not to log in via corporate single sign-on (SSO).
- **Single sign-on:** Authentication can be optionally or mandatorily integrated with identity providers such as Microsoft, Google, or Okta.
- **Multi-factor authentication:** An additional layer of security for companies not using SSO or offering flexible options, ensuring enforcement of two-factor authentication (2FA).

You can access your vault using:

- **Master Password:** A user-generated password, known only to the user, used to derive encryption keys and unlock the vault.
- **Biometrics/Windows Hello:** A user-enabled feature that provides an alternative to typing the Master Password by allowing access via biometric authentication.



User opens up NordPass app

New browser/ device, or expired/ reset session

Business Account

Authentication options:

- Business Account Password
- Single Sign-On

(Optional) Multi-Factor authentication

Exsisting browser/ device with a valid session

Vault unlock

Unlock options:

- Master Password
- Biometrics / Window Hello

Vault unlocked

When using NordPass Business, authentication to your Business Account is required only when accessing the service from a new browser, utilizing a new device, or after logging out of an active session. This eliminates the need for daily re-authentication on the same device.

Business Account sessions are maintained for 30 days and are stored locally within your browser.

IMPORTANT NOTE: Clearing your browser's cache may reset your session, necessitating a new login.

If your organization has single sign-on (SSO) enabled, the system will automatically verify your SSO token upon access. Provided that the token is valid and unexpired, you will proceed directly to the next step in the authentication process, such as multi-factor authentication (MFA) or unlocking your vault.

What is a Recovery Code?

To boost security and accessibility of your NordPass Business Account, we have designed the Recovery Code functionality. This code serves as a secure fallback method for resetting your Master Password in the unlikely situation that it is forgotten.

The NordPass Recovery Code is a randomly generated 24-symbol code that can be used to reset your Master Password. The Recovery Code is generated once the user has created the Master Password.

The Recovery Code always comprises 24 characters that are a mix of uppercase letters and numbers. It's generated using 32 bytes of random data parted by hyphens. The Recovery Code looks like this: VJZX-4RE9-J7XT-94SE-84JX-CU8H.

IMPORTANT NOTE: Given the complexity of the Recovery Code, memorization is highly impractical. Therefore, we strongly recommend downloading it as a PDF file, printing it out, and keeping it somewhere safe. Once you have a physical copy, delete the digital copy stored on your computer.

The Master Password is:

- Always private;
- Used to access and decrypt items locally on the user's device;
- Never transferred over the internet;
- Not known to the NordPass team;
- Known to you only.

Biometric authentication

To further bolster security while simultaneously simplifying access, we have equipped NordPass Business with biometric authentication capabilities.

During the setup, NordPass generates a unique biometric ID and two secure keys: **clientSecret** and **backendSecret**. These keys are combined using the **HKDF** (HMAC-based Extract-and-Expand Key Derivation Function) algorithm to produce an **authKey,** which encrypts your identity key with **AES-GCM** encryption.

The encrypted identity key and biometric identifier are stored locally on your device.

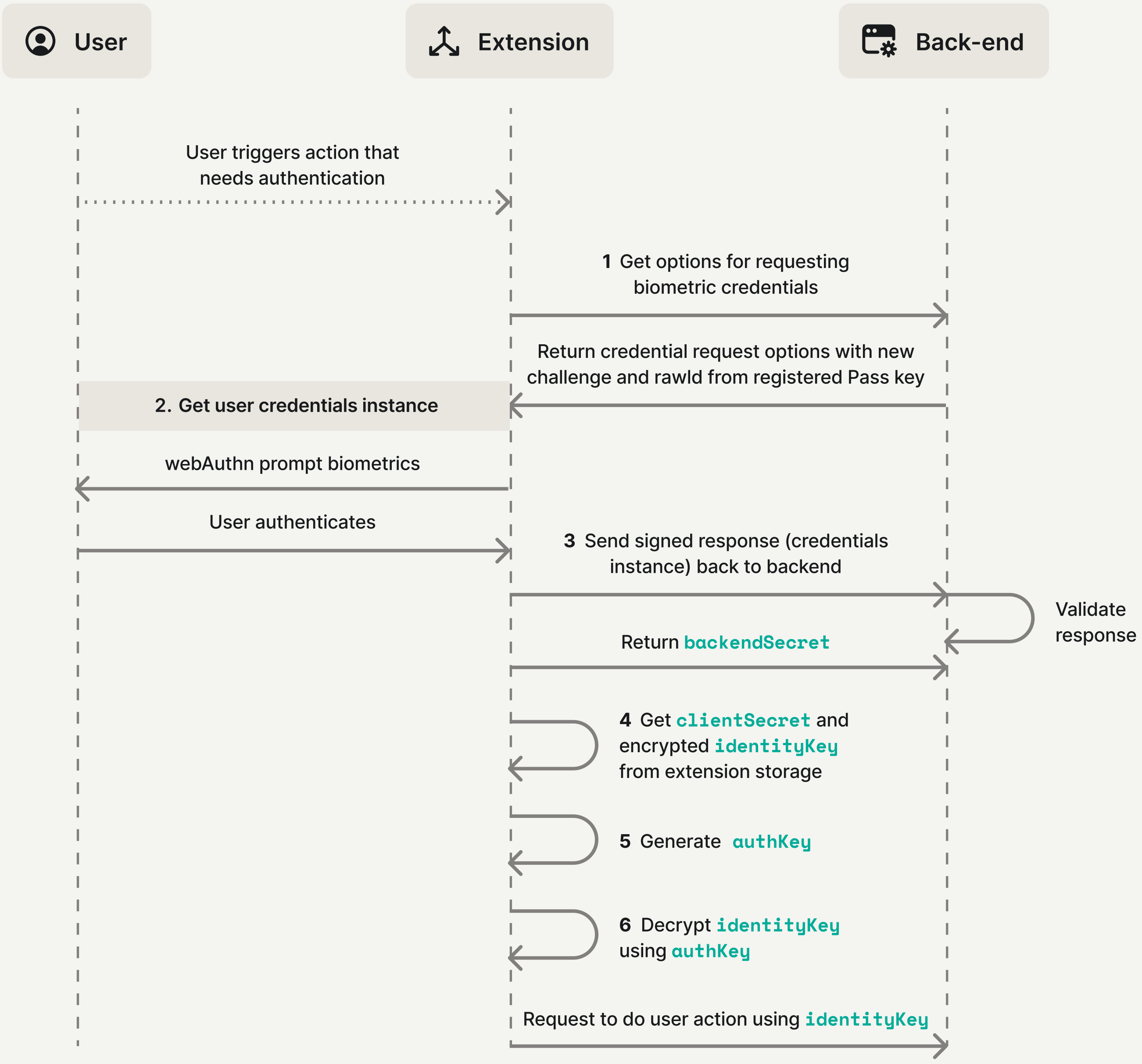
IMPORTANT NOTE: Sensitive biometric data is stored on your device and is never transmitted anywhere else.

NordPass uses a challenge-response method for biometric authentication:

1. When the user initiates the authentication, the encrypted credentials are retrieved from local storage.
2. The **authKey** decrypts the identity key.
3. With the identity key decrypted, the vault is unlocked.
4. A challenge is sent to the server, which verifies the **passkey.**
5. Access is granted only after successful validation.

NordPass supports biometric authentication across mobile and desktop platforms:

1. On mobile, **Touch ID** and **Face ID** are integrated.
2. On desktop, **Windows Hello** and **Touch ID** work through the NordPass extension.
3. Using **WebAuthn,** a secure web standard, NordPass ensures both security and ease of use, allowing users to access their vault without needing to re-enter their Master Password.



User
Extension
Back-end
User triggers action that needs authentication
1 Get options for requesting biometric credentials
Return credential request options with new challenge and rawId from registered Pass key
2. Get user credentials instance
webAuthn prompt biometrics
User authenticates
3 Send signed response (credentials instance) back to backend
Validate response
Return backendSecret
4 Get clientSecret and encrypted identityKey from extension storage
5 Generate authKey
6 Decrypt identityKey using authKey
Request to do user action using identityKey

If the biometric setup fails or the user intentionally disables it, NordPass automatically removes all related biometric data from both the device and the server. This includes the biometric ID, clientSecret, and the encrypted identity key.

When the user changes their Master Password, biometric authentication is automatically disabled. This action invalidates the previously encrypted identity key, preventing the security risk associated with obsolete encryption keys. The user is then prompted to re-enable biometric authentication, which generates new keys and re-encrypts the identity key.

Single sign-on

NordPass utilizes OpenID Connect (OIDC) to deliver a secure single sign-on (SSO) solution, integrating smoothly with platforms such as Microsoft, Microsoft Entra, AD FS, Okta, and Google. This allows users to access multiple applications with a single set of credentials.
To guarantee security, SSO tokens are decoupled from the Master Password. This separation ensures that neither NordPass nor the identity provider can access any vault data, maintaining strict data privacy and integrity.

For Business and Enterprise users, corporate credentials are incorporated into the SSO workflow, eliminating the necessity for separate Business Account passwords. Organization Admins in NordPass can efficiently manage and configure these SSO options through the Admin Panel, providing centralized control over authentication settings.

1. **User initiates login:**
- The user clicks on the NordPass login page to log in with IDP.

2. **Request authentication URL:**
- The NordPass frontend requests an authentication URL from the backend.

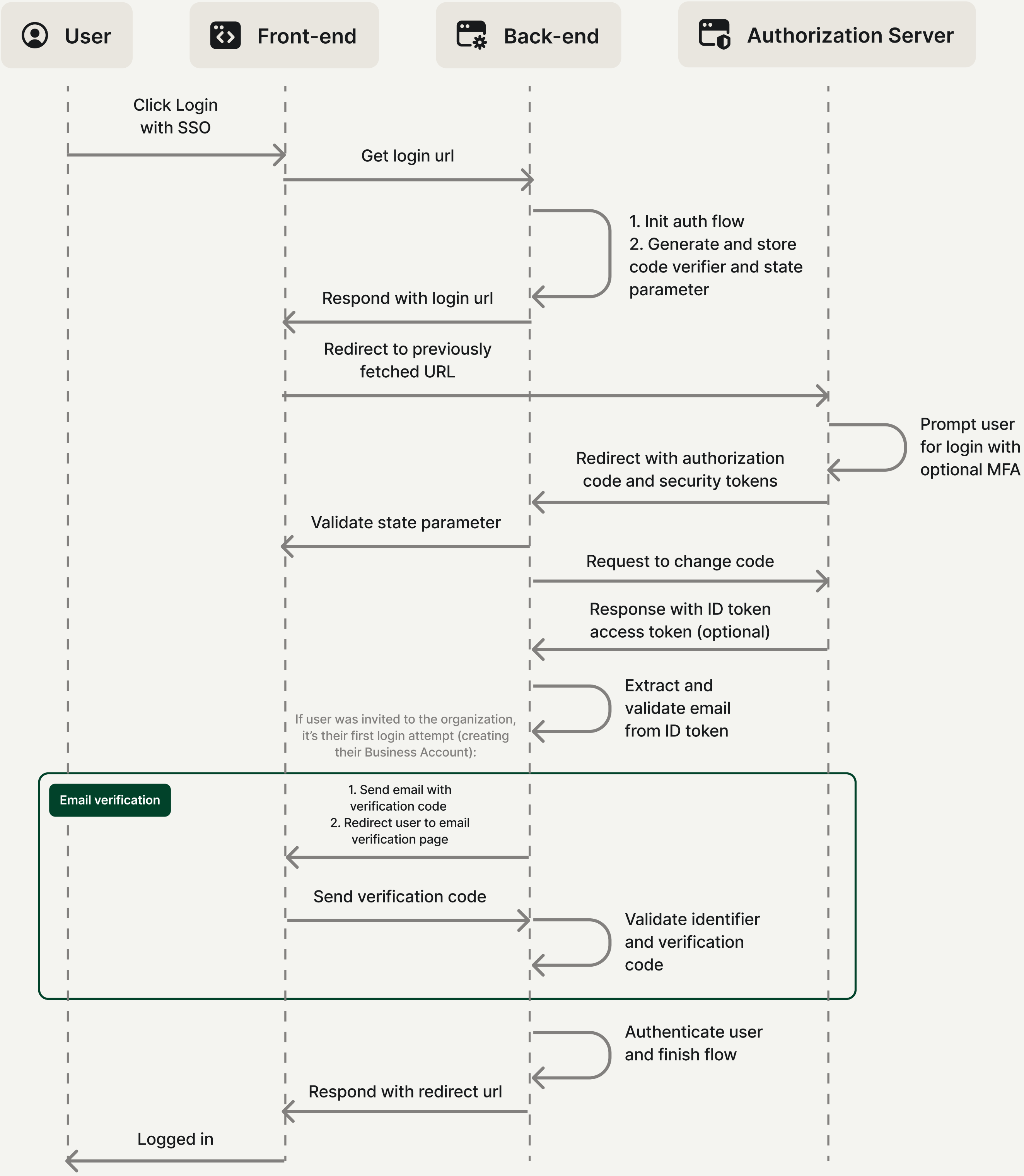
3. **Redirect to IDP:**
- The user is redirected to the IDP login page for authentication.
- IDP handles the user's login and any required multi-factor authentication (MFA).

4. **IDP redirects back to the NordPass backend:**
- After successful authentication, IDP redirects the user to NordPass's backend callback URL with code, id_token, and state parameters.

5. **Backend validates tokens:**
- The NordPass backend validates the state parameter to ensure the authenticity and integrity of the request.
- The backend exchanges the authorization code for an access token and ID token from IDP.

6. **User authentication and final redirect:**
- The backend validates the ID token's signature and parses the claims to fetch user information, such as email.
- If the ID token and nonce are valid, the backend authenticates the user and redirects them to the frontend.

Here's a technical outline of the SSO authentication process in NordPass:


User
Front-end
Back-end
Authorization Server
Click Login with SSO
Get login url
1. Init auth flow
2. Generate and store code verifier and state parameter
Respond with login url
Redirect to previously fetched URL
Prompt user for login with optional MFA
Redirect with authorization code and security tokens
Validate state parameter
Request to change code
Response with ID token access token (optional)
Extract and validate email from ID token
If user was invited to the organization, it's their first login attempt (creating their Business Account):
Email verification
1. Send email with verification code
2. Redirect user to email verification page
Send verification code
Validate identifier and verification code
Authenticate user and finish flow
Respond with redirect url
Logged in

Multi-factor authentication (MFA) for NordPass organizations

Multi-factor authentication (MFA) enhances NordPass's security framework by requiring users to complete a secondary verification step before accessing their accounts.

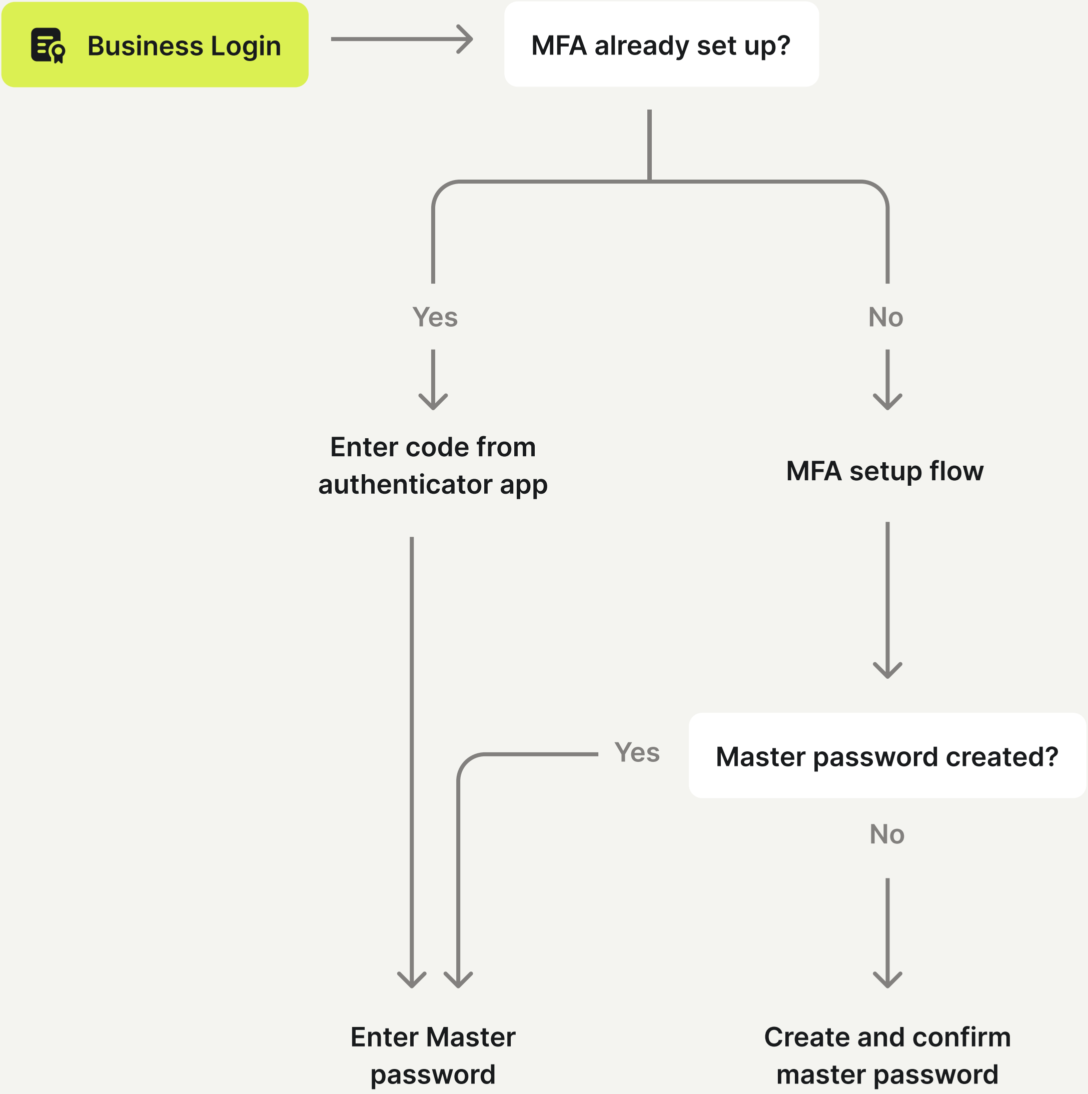
Active users can turn on multi-factor authentication (MFA) at any time through their vault settings. However, Admins and Owners can enforce a company-wide MFA policy via the Admin Panel. Once enforced, this policy applies to both current users and new members.

Key enforcement parameters include:

- **Mandatory setup:** Users are required to configure MFA during the sign-up process for new accounts or upon their next login if MFA has not been previously activated.
- **Non-disableable option:** Once enforced, users cannot disable MFA unless the policy is revoked at the organizational level.
- **Reset capability:** Users may reset their MFA using Recovery Codes. Admins and Owners can also initiate MFA resets for users who have lost access to their devices, enabling reconfiguration upon the user's next login attempt.

Once MFA has been enforced across the organization in the Admin Panel, the setup process is integrated into the user login flow, which looks like this:

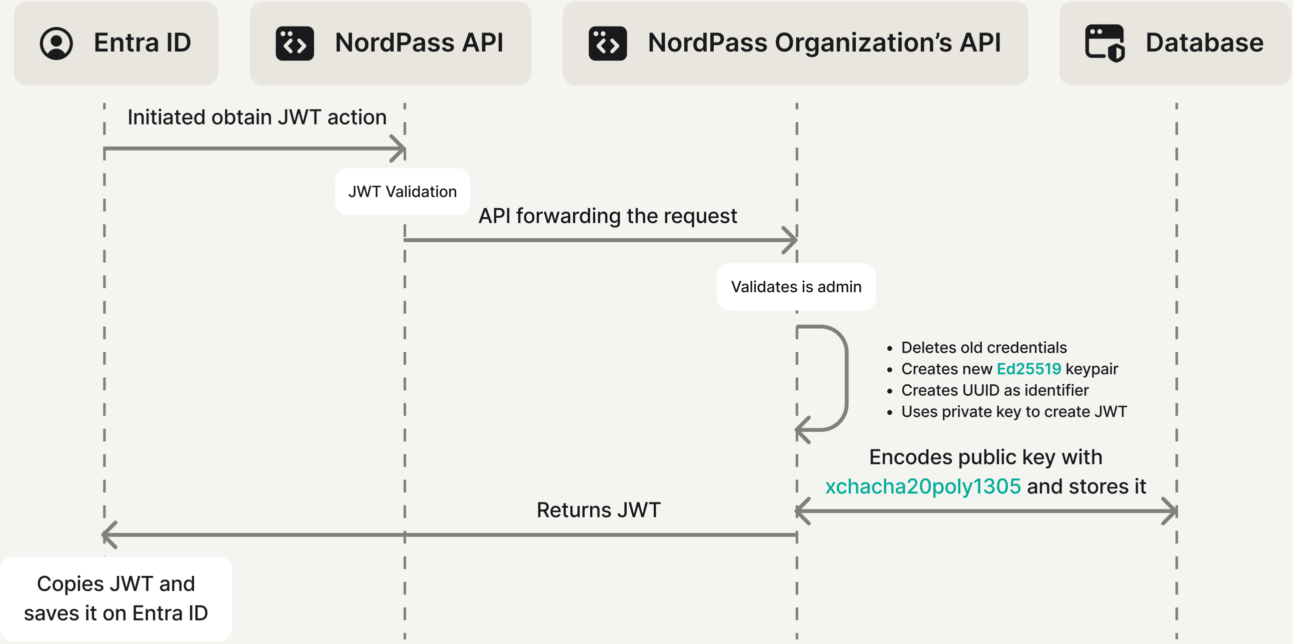
- Users log in to their NordPass Business Account.
- The system verifies whether MFA has already been configured for the user.
  - If MFA is not set up, the user is prompted to complete the MFA setup process.
  - If MFA is already configured, the user must provide the authentication code from their MFA application.
- After successfully completing the MFA step, users proceed to enter their Master Password.



User and group provisioning

Effective identity management is fundamental to maintaining security and operational efficiency within organizations. NordPass employs the System for Cross-domain Identity Management (SCIM) protocol to integrate seamlessly with identity providers such as Entra ID and Okta. This integration automates both user and group provisioning, ensuring consistent and secure access management across diverse platforms.

User provisioning is automated via Entra ID or Okta, ensuring that new users are systematically created and managed. The following steps detail the Entra ID user provisioning process:


Entra ID
NordPass API
NordPass Organization's API
Database
Initiated obtain JWT action
JWT Validation
API forwarding the request
Validates is admin
• Deletes old credentials
• Creates new Ed25519 keypair
• Creates UUID as identifier
• Uses private key to create JWT
Encodes public key with xchacha20poly1305 and stores it
Returns JWT
Copies JWT and saves it on Entra ID

1. **User creation initiation:**
   - Entra ID initiates the process by sending a request to our API via the SCIM endpoint to create a new user.
   - The API verifies the request's authenticity using JWT validation through a secure authentication endpoint.
2. **User creation and response:**
   - Upon successful validation, the API forwards the request to the Organization's API, which creates the user invite within our system using a specified user creation endpoint.
   - A response is then sent back to Entra ID, confirming the user's creation.
3. **User management operations:**
   - Updating User: A PATCH request to a specific user update endpoint updates user details, following a similar JWT validation and processing flow.
   - Deleting User: Deleting a user involves sending a DELETE request to a user-specific endpoint, which removes the user from our system.
   - Retrieving user information: A GET request to a user-specific endpoint retrieves specific user details. A GET request to a general user query endpoint allows for querying multiple users.

Let’s move beyond user provisioning and focus on group provisioning, which supports the efficient management of user groups. This process is essential for maintaining organized, secure access to resources across your organization. The following steps showcase the group provisioning process:

1. **Handling SCIM request:**
    - Group provisioning begins similarly to user provisioning, with a SCIM request from Entra ID. The process starts with validating the token and obtaining the organization_uuid.
    - The request is forwarded to the appropriate service to manipulate the group (e.g., creation, update, or deletion).

2. **Group cryptography handling:**
   The system ensures the integrity and confidentiality of group cryptographic data:
    - An Encryption Service token is validated to secure group data.
    - Cryptographic data is retrieved from the vault.
    - Group operations are performed securely.
    - The processed cryptographic data is then returned to the system.

3. **Pushing and storing group data:**
   Once the group data is manipulated:
    - The updated encrypted group data is pushed to the vault.
    - The system acknowledges the event and records the status.
    - An audit trail is created to track group provisioning actions.

Encryption Service
The Encryption Service is an integral part of NordPass' security architecture, designed to process the cryptographic operations related to group provisioning. By delegating encryption and decryption tasks, sensitive cryptographic operations are decoupled from the main application logic, thus reducing potential exposure.

The EEC uses the latest encryption algorithms, such as XChaCha20-Poly1305 and Ed25519. This mechanism of isolation ensures that cryptographic keys and sensitive data are secure, even if the main application is compromised. For your convenience, the EEC can be hosted on a cloud provider of your choice: Amazon Web Services, Docker, or Azure.

Zero-knowledge security model
NordPass strictly adheres to the zero-knowledge security model in terms of user and group provisioning. At no point does NordPass have access to unencrypted data. All operations related to sensitive data are encrypted and handled by the external encryption components.

Account recovery process

The account recovery process is exclusively available for the NordPass Business users by request form the organization’s Owner. This process enables users to restore access to the accounts when both the Master Password and Recovery Code are missing.

Member sends request

Member initiates recovery process by selecting “Forgot Recovery Code?” and creates a new Master Password

Owner receives request

Account recovery request appears in the Admin Panel where Owner can approve or decline it

Member recovers account

Once approved, the member can unlock their NordPass using the new Master Password

Members can initiate the account recovery process upon logging in to the NordPass or Admin Panel. Once on the login page, they need to click “**Forgot Master Password?**” and then **“Forgot Recovery Code?”** This will start the account recovery process:

1. The new unique-per-user cryptographic salt is generated.
2. The user creates a new Master Password, which, together with the new cryptographic salt, is used to derive the new Master Key.
3. The user’s new key pair is generated.
4. The user’s new private key is encrypted with the new Master Key.
5. The new Recovery Code is generated, which, together with the new cryptographic salt, is used to derive the new Recovery Key.
6. The user’s new private key is encrypted with the new Recovery Key.
7. The 4-digit confirmation code is generated and encrypted with the organization's public key.
8. The user’s new public key, cryptographic salt, private key encrypted with the Master Key, private key encrypted with the Recovery Key, and encrypted confirmation code are sent to the API, which saves them as a recovery request. It shows up on the Recoveries page in the Admin Panel.

Only the organization’s Owner can approve requests to recover members’ accounts because they are the only ones holding the organization’s encryption keys.

Here’s how the Owner can recover an account:

1. The Owner goes to the Recovery page in the Admin Panel and selects a recovery request.
2. The confirmation code is decrypted with the organization's private key and displayed in plain text.
3. The Owner checks if the confirmation code matches with the one provided by the user out-of-band. If it does, the Owner accepts the recovery request.
4. The confirmation of the recovery request initiates the following actions:
    a. Decrypts user’s root folder metadata and secret data private keys with the organization’s metadata and secret data private keys and encrypts them with the user’s new public key.
    b. Encrypts the organization’s metadata and secret data private keys with the user’s new public key (executed optionally if the requesting user’s role has to have access to the organization’s keys).
    c. Encrypts the organization’s group folder metadata and secret data private keys with the user's new public key (executed optionally if the requesting user's role has to have access to the organization’s group keys).

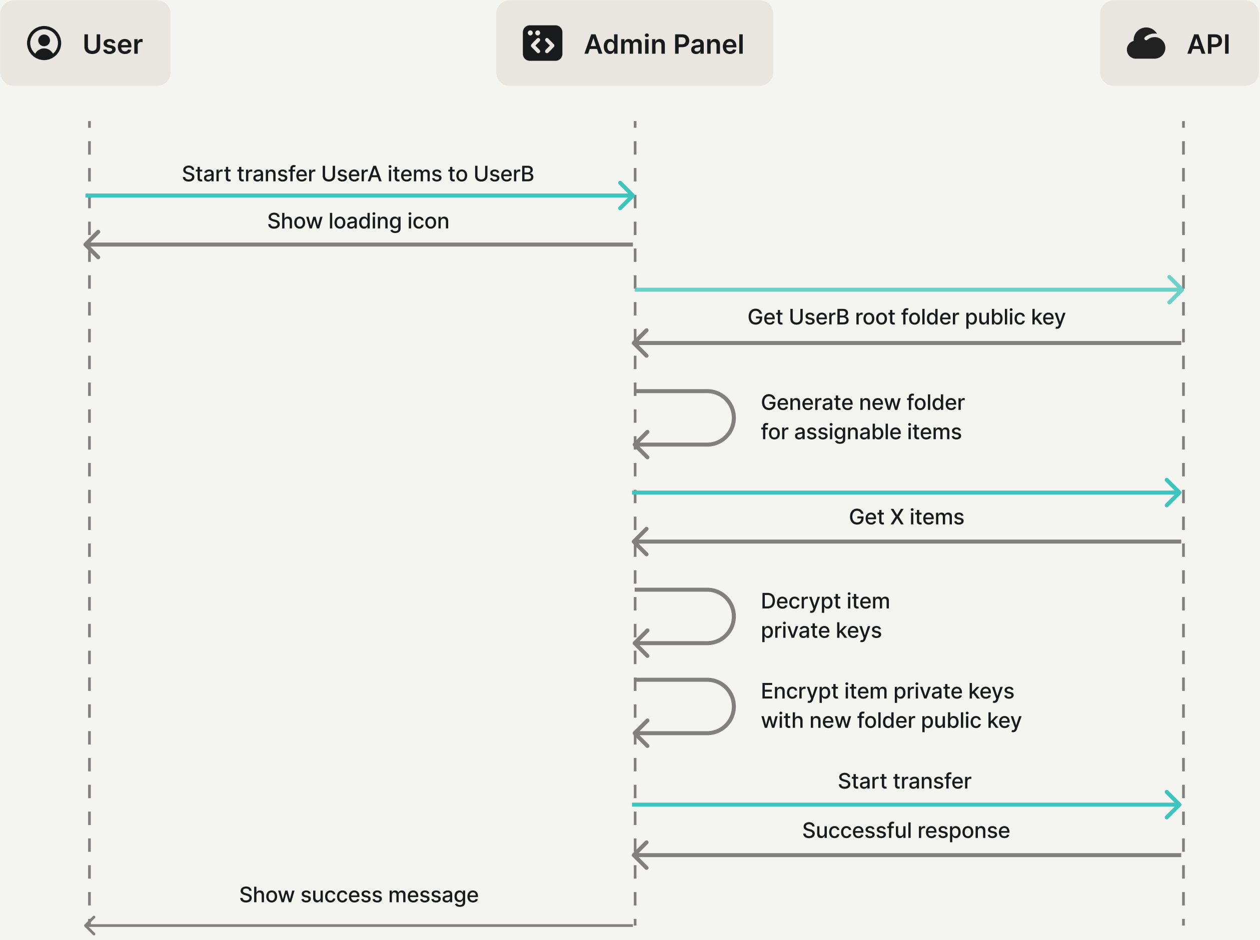
If an Owner decides to deny account recovery, the request will be deleted. Users can then either initiate a new request or try to remember their existing Master Password.

Once the request is initiated, the Owner must approve it within 5 days. Otherwise, the account recovery request will expire, and the user will need to submit a new recovery request.

Item transfer from deleted members

With the Items Transfer feature, organization's Owners can reassign items from a deleted member to an active member in order to ensure continuity and secure access to important data.

During the transfer, the organization's Owner decrypts the items' private keys and re-encrypts them with the recipient's public key. The items are placed in a newly created folder, with its private key encrypted using the recipient's root folder public key. If an MFA key pair is present, it is also re-encrypted.



User
Admin Panel
API
Start transfer UserA items to UserB
Show loading icon
Get UserB root folder public key
Generate new folder for assignable items
Get X items
Decrypt item private keys
Encrypt item private keys with new folder public key
Start transfer
Successful response
Show success message

When a member is deleted, their items are listed under the Deleted tab in the Admin Panel. The organization's Owner can either assign a new Owner or delete the items permanently. If no action is taken within 180 days, the items will be automatically deleted.

Here’s an overview of the item transfer process:

1. The organization’s Owner starts the transfer by obtaining the receiving user’s root folder public key.
2. A new folder is created for the reassigned items, with its private key encrypted using the recipient’s root folder public key.
3. The organization’s Owner retrieves items owned by the deleted member, including items that were shared with other members retaining sharing permissions.
4. The items’ private keys are decrypted using the organization key pair and re-encrypted with the new folder's public key.
5. The new folder and re-encrypted item keys are sent to the API, completing the transfer. The new item owner is notified via an in-app notification, and the items appear in a folder named "Transferred" in their vault.

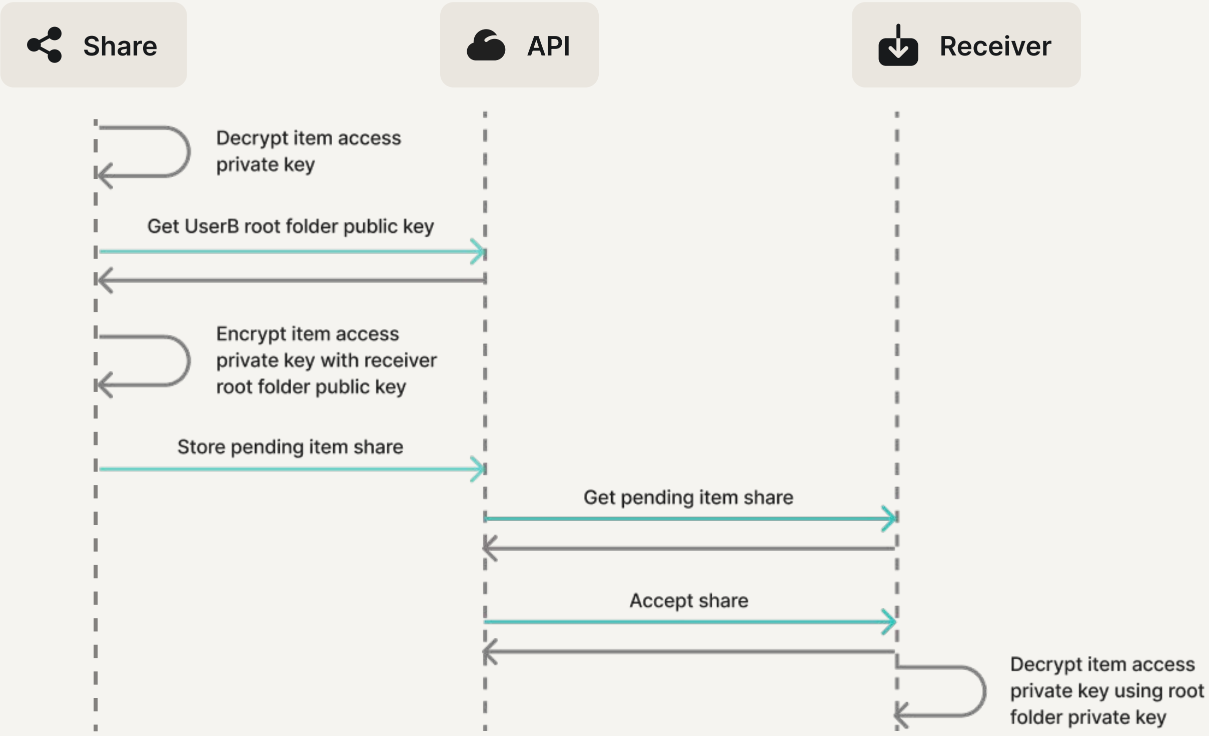
Password sharing

NordPass allows users to share items, including passwords, passkeys, credit card details, secure notes, and personal info.

Here's how secure item sharing looks from a technical standpoint:

1. The sharer chooses an item and decrypts its access private key with their private key.
2. The sharer gets the receiver's root folder's public key from the API.
3. The sharer encrypts the item access private key with the receiver's root folder public key.
4. The receiver gets an email with a pending item shared from the API.
5. If the sharing is accepted, the receiver can decrypt the item access private key using his root folder private key.

IMPORTANT NOTE: If the item is shared with a NordPass B2C account user, the root folder steps are skipped as it's only applicable to Business users.


Share
API
Receiver
Decrypt item access private key
Get UserB root folder public key
Encrypt item access private key with receiver root folder public key
Store pending item share
Get pending item share
Accept share
Decrypt item access private key using root folder private key

IMPORTANT NOTE: We share access to the item—not the data snapshot. This means that if the user changes any data of that item, it changes for everyone who has access to the item.

Shared access levels

When sharing items with others, NordPass offers 4 access levels a user can choose from, and an extended set of permissions that belong to the owner of the item.

- **Owner:** Can autofill, view, share, edit, and delete items if you are the owner of the items.
- **Can edit:** With this permission, you can edit the items that are shared with you.
- **Can share:** With this permission, you can share, view, and autofill data.
- **Can view:** With this permission, you can view and copy item details, and autofill data.
- **Can autofill:** With this permission, you are allowed to only autofill the data.

The owner of an item or a Shared Folder can transfer ownership to another user in the organization. Once ownership is transferred, the previous owner retains the ability to edit with the "Can edit" permission level assigned.

IMPORTANT NOTE: Some websites might display sensitive information when it's autofilled. NordPass is not responsible for and cannot control how sensitive information is displayed outside of NordPass.

Time-limited Sharing

Time-limited sharing allows users to securely share credentials or other sensitive information with external parties for a predefined period. This feature is a convenience feature that is designed to address scenarios where temporary access is needed without compromising long-term security.

When creating a time-limited share, users can choose from different expiration time options, after which access will automatically be revoked. During this time, recipients interact with data based on defined permissions.

Advantages of time-limited sharing:

- **Controlled Access:** Data is accessible only during the specified period.
- **Encryption:** Information stays encrypted in transit and at rest.
- **Automatic Revocation:** Access ends without manual action.
- **Audit Logs:** All interactions are logged.
- **Clock Tamper-Proof:** Prevents bypassing expiration via system clock changes.

If users have access more than one way (direct share, shared folder, etc), the highest level takes precedence, ensuring consistent access behavior.

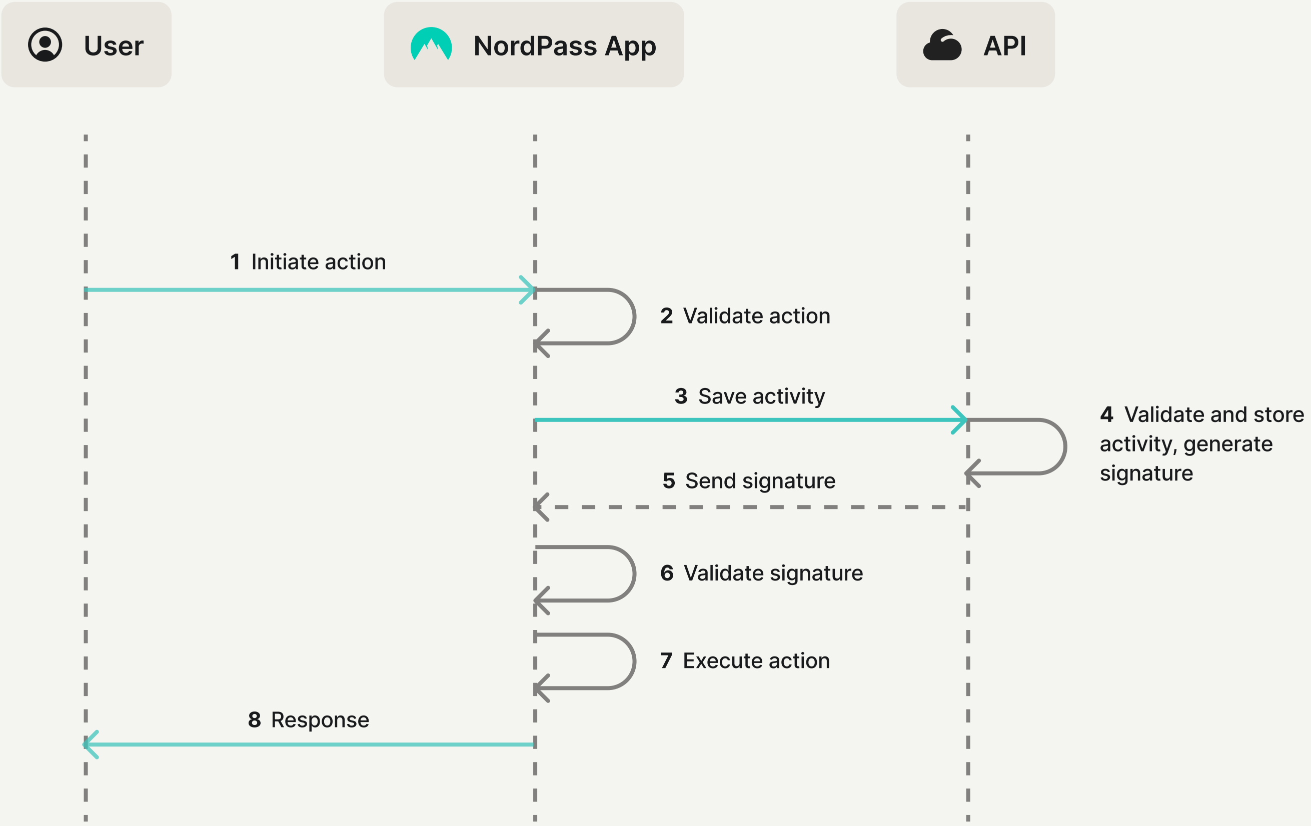
However, time-limited sharing doesn’t support **'Can Edit'** or **'Can Share'** permissions. To avoid scenarios where users might alter data in ways that interfere with expiration timelines and impact other users' access, and to prevent situations where shared access could be repeatedly extended or duplicated, making it difficult to enforce expiration timelines effectively, both permissions are excluded from time-limited sharing.

If an item is already shared with **'Can Edit'** rights and a time limit is set, the permission will automatically downgrade to the highest possible **'Can View'** level to ensure consistent and predictable time-limited access.

Only **'Can View'** and/or **'Can Autofill'** are allowed for time-limited shares, ensuring predictable and secure temporary collaboration.

Activity Log

The Activity Log in NordPass is a key feature that enhances the platform's security and audit capabilities, providing a clear record of actions performed within the system. This section outlines how activity logs are collected, stored, encrypted, and accessed, as well as the role-based controls that manage who can view and handle these records.



NordPass systematically generates activity logs to record significant user actions within the platform, such as creating, modifying, deleting, or sharing items, in real time.

- Each action triggers an event that captures details, including the action type, user involved, affected data, and timestamp.
- These events are compiled into structured messages and transmitted to a logging service, which efficiently handles and stores multiple log entries from various users and actions without delay.
- The logs are then securely stored in an indexed database, organized by date and activity type to facilitate efficient search and retrieval.

Access to activity logs is controlled through role-based access control (RBAC), where different organizational roles have varying levels of access based on their responsibilities.

- Organization’s Owners have the authority to decrypt and view specific item metadata in logs using the organization key, which is never stored in plain text, ensuring its security.
- Admins can view item types and relevant log details such as action type, date, time, and the user who performed the action, but cannot access item titles.

The decryption process varies depending on ownership.

- For items owned by the organization, logs are decrypted using the organization’s key pairs, involving decryption of the organization’s private key with the user’s identity key pair, followed by decrypting the item’s private key with the organization’s key pair, and finally decrypting the item’s value.
- For external item actions, which involve items not owned by the organization, the decryption process may utilize keys from external sources such as folders or groups outside the organization, ensuring secure access by authorized users.

NordPass Business and Enterprise users can extract activity logs via a dedicated API, enabling organizations to retrieve comprehensive records of user actions in a structured JSON format for integration with Security Information and Event Management (SIEM) tools. Each log entry includes detailed information such as action type, timestamp, and user identifiers.

- To extract logs, users send a POST request to the activity logs API, including the necessary headers: an Authorization header with a valid JSON Web Token (JWT) and a Content-Type header set to application/json. The API responds with JSON-formatted logs, ensuring compatibility with various data processing systems.

Password Health and password policy

The NordPass Business provides the Password Health tool to help organizations improve password security and address common password-related issues like password reuse, weak passwords, and exposed passwords.

Owners or Admins can create tailored password policies that define specific requirements for passwords stored in NordPass. These policies can set rules for minimum password length, complexity (including uppercase and lowercase letters, numbers, and special characters), and expiration periods for mandatory password resets.

When a user unlocks the NordPass app:

- The app requests the organization's password policy which is set in the Admin Panel.
- If no specific policy is set, default policies are applied.

Exposed Password Handling:

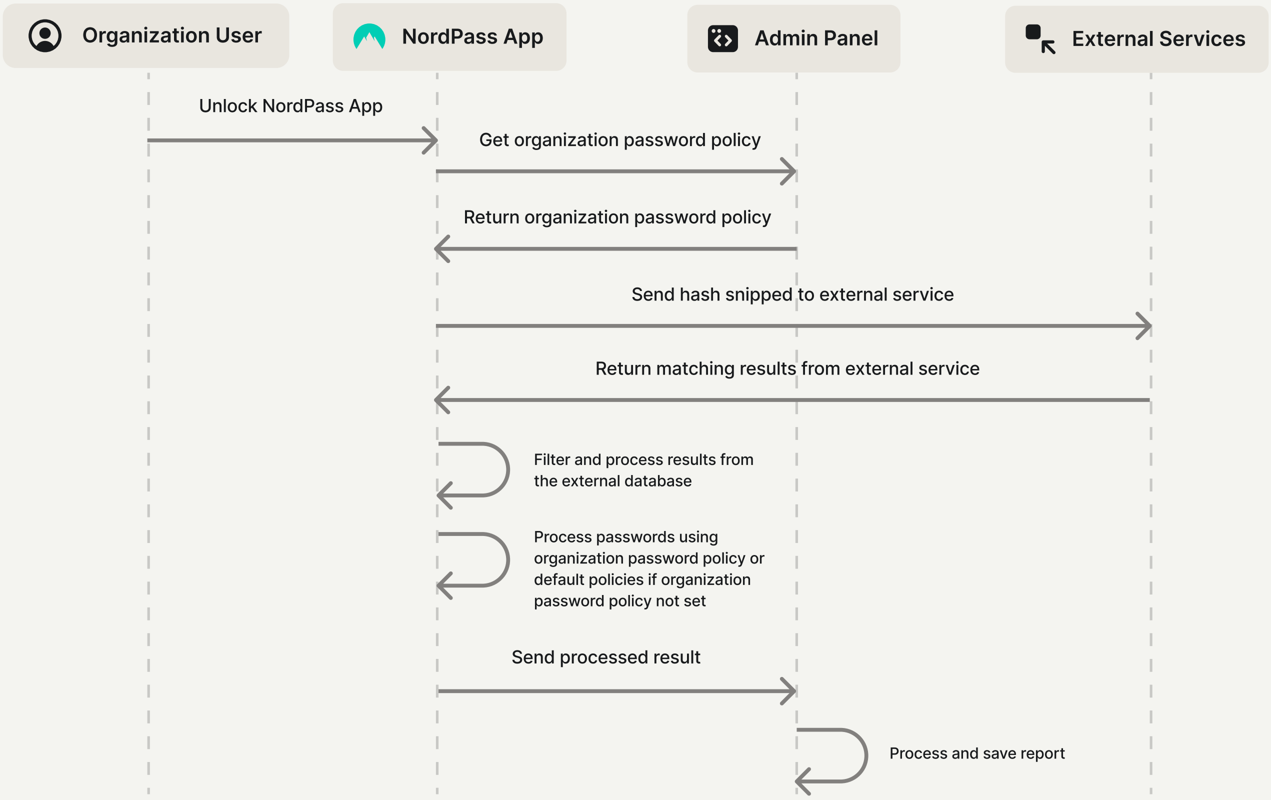
- Password hashes are securely transmitted to external breach databases for comparison.
- Matches are sent back to the user's application.
- Results are filtered and processed locally.

The app then processes the stored passwords locally:

- Passwords are evaluated against the retrieved policy
- Factors such as complexity, uniqueness, and expiration are checked to ensure compliance.

Once the evaluation is complete:

- The results are sent back to the organization's Admin Panel.
- A summary is generated, providing insights into password compliance
- Admins can use this report to identify and address any security vulnerabilities.


Organization User
NordPass App
Admin Panel
External Services
Unlock NordPass App
Get organization password policy
Return organization password policy
Send hash snipped to external service
Return matching results from external service
Filter and process results from the external database
Process passwords using organization password policy or default policies if organization password policy not set
Send processed result
Process and save report

Data Breach Scanner

Another incredibly useful tool in NordPass is the NordPass Data Breach Scanner, which is designed to help users identify whether their sensitive information—such as passwords, email addresses, and credit card details—has been exposed in a data breach.

Before using the Data Breach Scanner:

- Users must agree to the NordPass Privacy Policy, which is synchronized across all devices.
- This ensures user consent is obtained in line with NordPass's privacy commitments.

Once consent is given:

- The scanner checks stored items, including passwords, email addresses, and credit card numbers, against a database of known breaches.
- The scan is conducted locally, ensuring that no plaintext data is accessed by NordPass, in line with its zero-knowledge architecture.

During the scanning process:

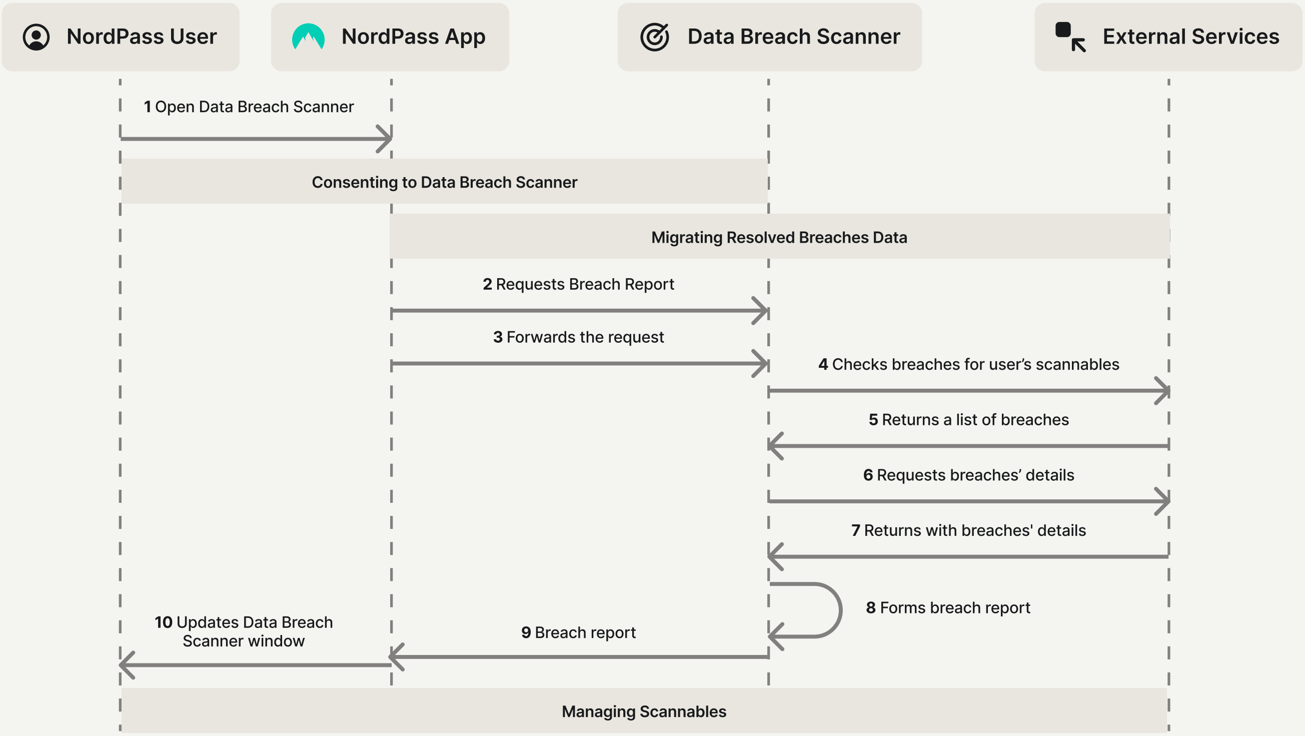
- All data transmissions are encrypted to ensure data security in transit.
- The scanner retrieves breach data from external services like Serity to ensure up-to-date and accurate results.

If the scan identifies exposed information:

- The results are sent back to the user, along with specific security recommendations.
- For example, if a password is compromised, users are advised to change it immediately.

After addressing the issue:

- Users can mark the breach as resolved.
- Unresolved breaches are prioritized in the scan results, helping users focus on the most critical security risks first.


NordPass User
NordPass App
Data Breach Scanner
External Services
1 Open Data Breach Scanner
Consenting to Data Breach Scanner
Migrating Resolved Breaches Data
2 Requests Breach Report
3 Forwards the request
4 Checks breaches for user's scannables
5 Returns a list of breaches
6 Requests breaches' details
7 Returns with breaches' details
8 Forms breach report
9 Breach report
10 Updates Data Breach Scanner window
Managing Scannables

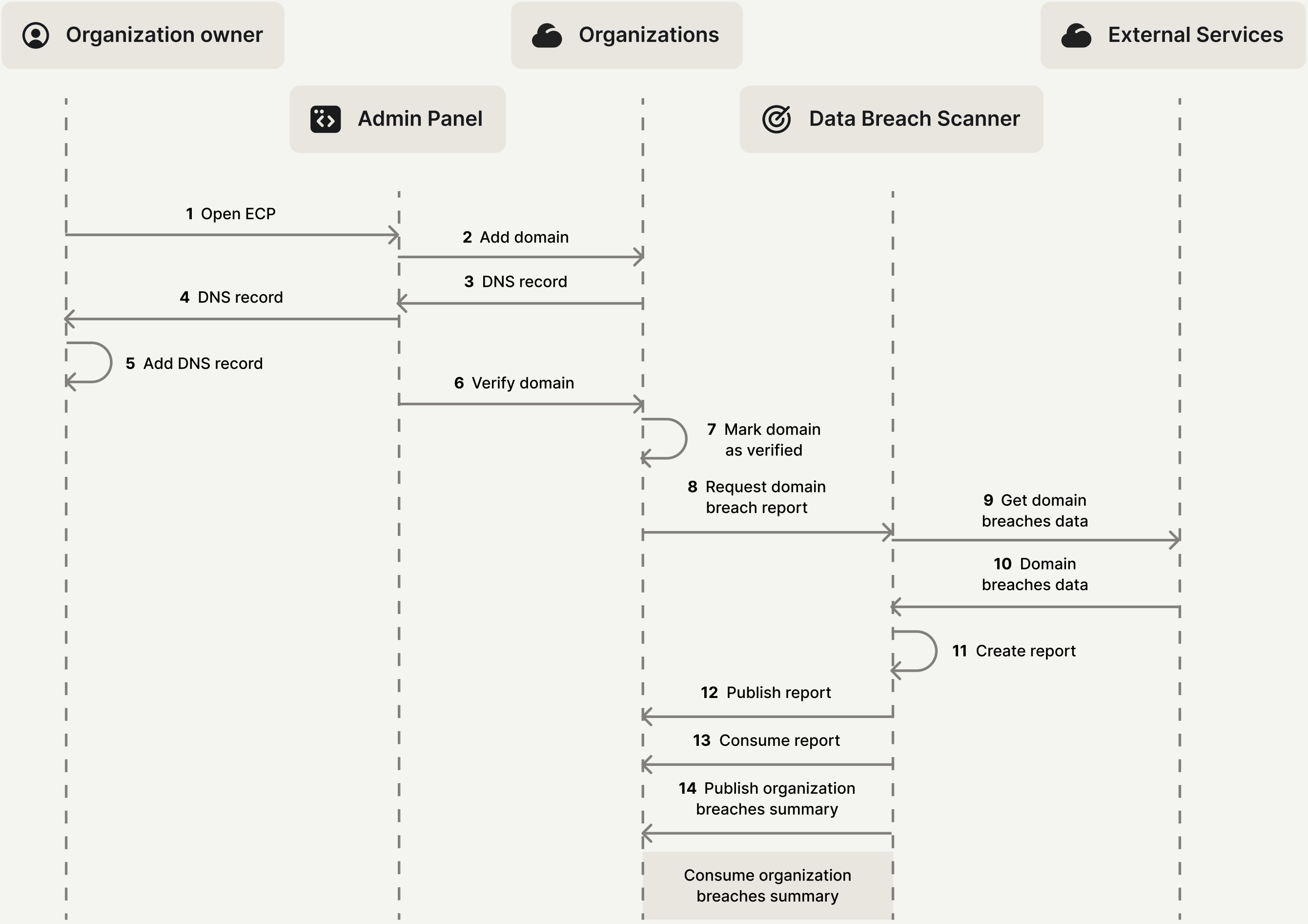
Organization’s Data Breach Scanner

The organizational Data Breach Scanner, located in the NordPass Admin Panel, enables both Admins and Owners to monitor and manage security risks associated with data breaches. The scanner allows domains to be examined for exposed credentials and sensitive information, providing detailed reports for immediate action.

Here’s how the Data Breach Scanner works on the organizational level:

- The process starts with the organization’s Owner adding the domain(s) to the NordPass Admin Panel. A DNS record is added to verify domain ownership, and once confirmed, the domain is marked as secure.
- After the domain is verified, NordPass retrieves breach data related to the organization’s domain(s) from external sources. This includes any compromised emails or credentials linked to the domain.
- The retrieved breach data is compiled into a summary report. The report provides an overview of the breaches detected, including the type of data exposed and the date of the breach.

The breach report is published in the Admin Panel. Admins can access detailed breach information, including the type of compromised data and any other relevant details.
The Data Breach Scanner continuously monitors the verified domains. Whenever new breach data is detected, the report is updated in real time.



NordPass Authenticator

The NordPass Authenticator adds an extra layer of security to your vault through time-based one-time passwords (TOTP). This section explains its functionality, detailing the security mechanisms, including the double encryption process, and walks through the steps of enrollment and daily use.

- Upon launching the NordPass extension, the system checks whether the TOTP feature is enabled for the user and their organization.
- If TOTP is enabled but not yet configured, the extension generates a unique Device ID (UUIDv4) and stores it securely.
- The extension then sends a request to the API to verify whether a TOTP device has already been enrolled.
- If a TOTP device is not enrolled, the user is prompted to initiate the enrollment process.
- A device-ound MFA key pair is generated using X25519 encryption.
- The private key is securely stored on the device, encrypted with AES-256-GCM, while the public key is transmitted to the NordPass server.

Encrypting and decrypting TOTP secret:

When a TOTP secret (used to generate the one-time passwords) is added to a vault item, it undergoes a double encryption process:

- **Client-side Encryption (First Layer):**
  The TOTP secret is encrypted on the client side using a newly generated symmetric key with the XChaCha20-Poly1305 algorithm. This key is then encrypted using the vault item's secret public key.
- **Server-side Encryption (Second Layer):**
  The encrypted TOTP secret undergoes further encryption with the device-bound MFA public key, ensuring that only the enrolled device can decrypt and utilize the TOTP secret.

When a user requests to view the TOTP code for a vault item, the system verifies if the TOTP device is enrolled and if biometrics are enabled. If these conditions are met, the decryption process begins:

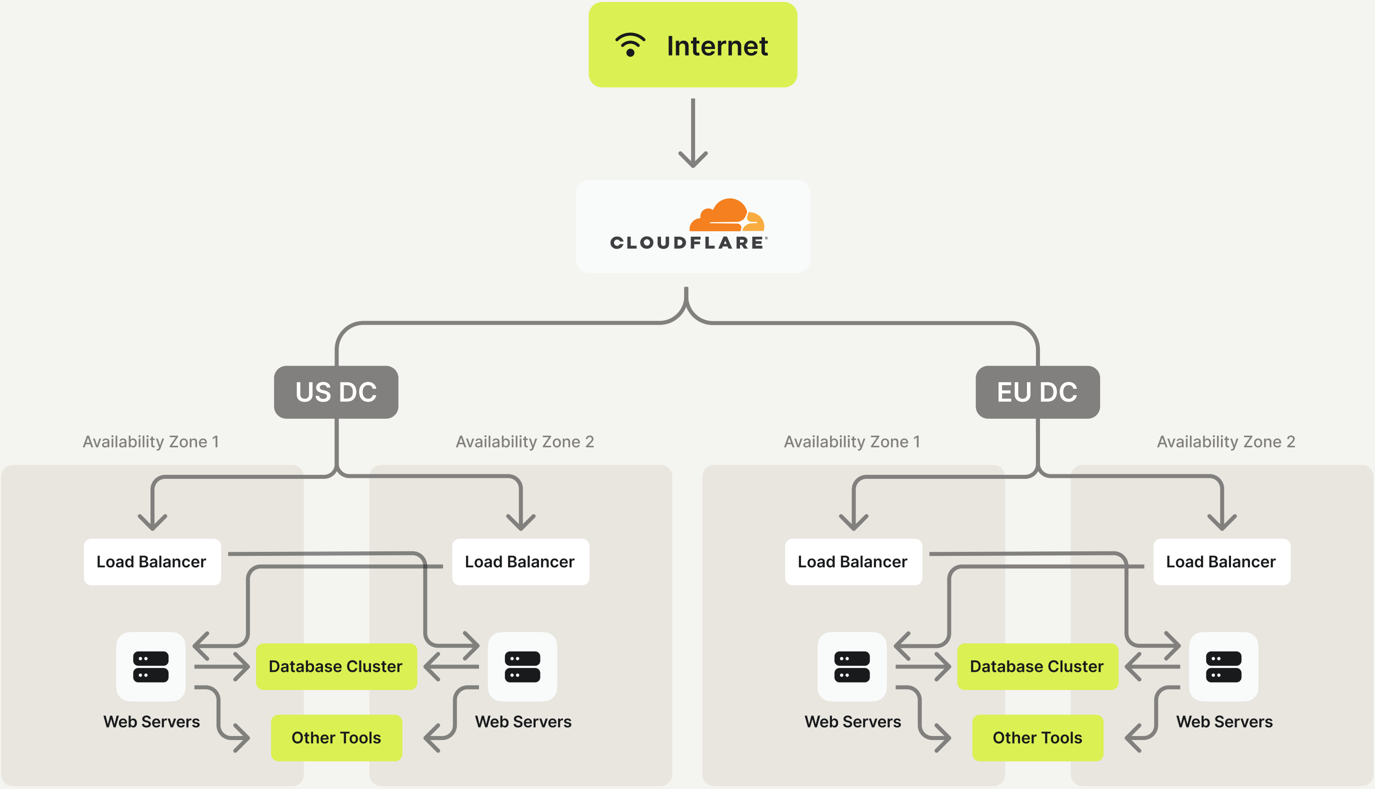
- The server sends the encrypted TOTP secret to the device.
- The encrypted TOTP secret is first decrypted using the device-bound MFA private key.
- The symmetric encryption key used for the client-side encryption is then decrypted using the vault item’s secret private key.
- The TOTP secret is decrypted and displayed as a 6-digit time-based code for use in multi-factor authentication.

The NordPass Authenticator feature leverages a double encryption mechanism alongside biometric authentication to provide a secure solution for protecting sensitive vault items.

Infrastructure

NordPass Business is built on a resilient infrastructure designed for high availability and data security. This section details how our system architecture ensures seamless performance through database clustering, active replication, and secure data encryption at every layer.

- NordPass uses Amazon Web Services as a cloud provider with its own key management solution for hardware encryption.
- NordPass Business clients can choose to host their data on US or EU (Frankfurt) AWS data centers.
- Item storage is processed from the database cluster with active replication. Each cluster member is stored in a different availability zone and meets all the high availability requirements. If one database goes down for any reason, the others will seamlessly distribute the load, and our team will be immediately notified.
- Our service is backed by end-to-end encryption architecture, meaning that your data is encrypted and decrypted at the device level. Therefore, the data stored on our servers is always encrypted.
- NordPass is a multi-tenant vault as our infrastructure serves multiple clients.



IMPORTANT NOTE: One group or system consists of multiple microservices and groups.

Other ways we keep your data safe and private

External audits

At NordPass, we feel that working with independent third-party auditors is critical. Having an independent team of security experts look into and review our code allows us to improve our service and maintain the highest standards of security. We believe that building a truly secure product is not a one-time project but an ongoing process. We hope that it also showcases our dedication to transparency and helps us build trust.

The audit process

We provided the auditors with all the possible information about NordPass, including access to various materials, documentation, source code, and other data NordPass operates and relies on.
The auditors reviewed our cryptographic premise, the NordPass Business suite software (NordPass vault, Android, iOS, Admin Panel, and Business Account), as well as the background application and its codebase.

The results? No critical issues were identified, which helped NordPass Business to progress from its beta version.

We will continue to conduct external audits to ensure the highest security standards. For results and more information on future audits, please follow our blog at nordpass.com/blog/

Internal audits

We have a dedicated Product Security team that continuously performs vulnerability assessments and pentests alongside many other responsibilities. Assessments and pentests are used interchangeably to assess risk posture and identify potential security issues (cataloged in the OWASP Top 10).

This is done as a precautionary measure, and we fix all the security issues as soon as they are identified. However, no matter how big a security issue is, it will never directly affect the user. Even in the unlikely event of NordPass being hacked or the database leaking, none of the information would be accessible to bad actors. NordPass uses end-to-end encryption, and users' data is encrypted locally, which means that any breached data would look like gibberish to intruders.

Secure software development life cycle

During every product’s development, Nord Security implements Secure Software Development Life Cycle (SSDLC), while Software Development Life Cycle (SDLC) was invented to organize all the phases of the software development process (using various methodologies and tools) to improve the efficiency of production. Secure SDLC represents an advanced version of the traditional software development life cycle, incorporating security measures at every stage of development. This approach ensures that all participating teams consider both the functional needs and security considerations of the project.

At its core, the distinction arises from the emphasis placed on security. Please refer to the table below for a concise summary:

Traditional SDLC	Secure SDLC
• The focus is on developing efficient, and productive applications at minimum coss and as fast as possible.	• The focus is on developing secure applications without having an impact on costs, time of delivery, and efficiency.
• Security testing and secure coding aren’t included in its process phases.	• Security testing and secure coding are fundamental parts of the process.
• Testing comes toward the end of the process.	• Testing starts at early stages and continues throughout the whole process.
• Security is an afterthought.	• Security is incorporated at every stage of the life cycle.

Logs

App logs are saved on the user's device and are mainly used for troubleshooting. Logs do not contain any data that could be used to identify the user or their device. The user is the only one who can view the logs, which can then be shared with the Support team to help them identify any issues and fix them. You can find logs on Windows, macOS, Linux, Android, or iOS devices by following this guide. Some logs of critical errors are automatically sent to the API, but only if the user has enabled crash reporting in their settings. These logs are not tied to any account in any way and cannot be used to identify the user.

Data privacy

Your privacy is important to us. We take all the necessary steps to secure your data, whether it's technical, physical, or administrative.

When providing our services, we are committed to the principles of data privacy laws and make every effort to comply with them, aiming to ensure the lawfulness of processing, data minimization, risk-based approach, and proper security measures.

You can read more about how we protect your privacy in the NordPass Business Privacy Policy.

Bug bounty

At NordPass, we strive to maximize the security and integrity of our infrastructure and our customers' data. With our bug bounty program, we employ the help of white hat hackers to discover bugs and vulnerabilities and make NordPass more secure.

https://hackerone.com/nordsecurity

The program’s policy describes the reference payout range for vulnerabilities depending on their severity levels.

Industry standards and certifications

NordPass Business adheres to the highest industry standards for security and data protection. Through independent audits and recognized certifications, we ensure compliance with rigorous data protection regulations.

ISO

The NordPass Business Information Security Management System (ISMS) has been independently audited and certified according to the ISO/IEC 27001:2022 standard, which ensures high efforts in the protection of confidential data.

SOC 2 Type 2

NordPass Business has undergone a thorough audit according to the SOC 2 Type 2 procedures. SOC 2 Type 2 audit ensures that NordPass Business can securely manage data to protect the interests and privacy of its clients.

Cure53

We take security and transparency seriously. That is why NordPass Business has been subjected to and has undergone an extensive security audit performed by Cure53—an independent German auditor.

GDPR

NordPass makes every effort to comply with GDPR and can help you become GDPR-compliant, too. Read the guide to learn how to become GDPR-compliant by protecting the most sensitive information your employees have—their passwords—and protect your customers' data as a result.

HIPAA

NordPass Business is HIPAA-compliant. If you process sensitive health information, NordPass can help you get one step closer to being HIPAA-compliant, too. Read the HIPAA compliance guide to learn how to do so.

California Consumer Privacy Act (CCPA)

Businesses are required to implement and maintain reasonable security procedures and practices under the CCPA. NordPass is an essential tool that helps its customers to ensure the security of processed personal information and, therefore, can help you with CCPA compliance.

NordPass® | Password Manager

If you have any questions or observations, please contact us.

For sales inquiries
sales@nordsecurity.com

For partners / MSPs / resellers
partners@nordsecurity.com

Account management
success@nordsecurity.com

NordPass B2B customer support
support.business@nordpass.com

Legal disclaimer

This document contains information that is applicable on the day of its issue (as provided above). The document is periodically updated. Nevertheless, as we regularly develop our services and introduce new features to our products, the information provided herein might not correspond to the then-current factual situation. The information is provided for general information purposes only and in good faith. However, we make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information provided in this document.

This document contains privileged and confidential information. It is intended only for the use of the intended recipient(s). If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this document is strictly prohibited.