Notary Service

ADMINISTRATOR'S GUIDE

Revision: 4/27/2020

Table of contents

1 About the notary service 3

1.1 How notarization works 3

1.2 Administrators and users 3

1.3 Limitations 3

1.4 Supported web browsers 3

2 Using the notary service 4

2.1 Activating the account 4

2.2 Accessing the notary service web interface 4

2.3 Notarizing files 4

2.3.1 Operations with notarized files 5

2.4 Verifying file authenticity 6

2.5 Signing files 7

2.5.1 Operations with signed files 8

3 Administering the notary service 9

3.1 Managing API keys 9

3.2 Administering user accounts and quotas 9

1 About the notary service

The notary service is a complex blockchain-based solution that enables you to do the following:

- Notarize a file.
- Check whether a notarized file (or its copy) is authentic and unchanged since it was notarized.
- Send a file to multiple people to sign it electronically, and then notarize the signature certificate.

The service is available through a web interface called the notary console.

1.1 How notarization works

To notarize a file, you need to upload it to the cloud storage. After the file is uploaded, the notary service calculates a digital fingerprint (known as a hash code) of this file. A hash code is unique for each file.

Note *The notary service application programming interface (API) enables you to notarize a file without uploading it to the cloud storage. Instead, the file's pre-generated hash can be used. For more information about using the API, refer to "Managing API keys" (p. 9).*

The notary service then sends the hash code to the Ethereum blockchain-based database. This database ensures that the hash code remains unchanged.

To verify a file's authenticity, the service calculates the file's hash code, and then compares it to the hash code that is stored in the database. If the codes match, this is a guarantee that it is the same file and it has not been modified.

1.2 Administrators and users

There are two user account types in the notary service: administrator accounts and user accounts.

Both administrators and users have access to the entire notary service functionality in the notary console. Only administrators can manage the notary service API keys and use the notary API.

Additionally, a notary service administrator can be assigned the role of a company administrator. This role grants access to the management portal, where the administrator can manage user accounts, quotas, notifications, and reports.

All users, administrators, and company administrators have access only to their own notarized and signed files. Administrators have access only to their own API keys.

1.3 Limitations

- Files that are larger than 1 GB cannot be notarized by using the notary console. This is possible only via the notary service API, by sending a pre-calculated hash of a file to the notary service.
- Files that are larger than 1 GB cannot be signed by using the notary console. This is possible only via the notary service API, by sending a link to the file to the notary service.

1.4 Supported web browsers

The web interface supports the following web browsers:

- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later
- Windows Internet Explorer 11 or later
- Microsoft Edge 25 or later
- Safari 8 or later running in the macOS and iOS operating systems

In other web browsers (including Safari browsers running in other operating systems), the user interface might be displayed incorrectly or some functions may be unavailable.

2 Using the notary service

2.1 Activating the account

After signing up for the service, you will receive an email message containing the following information:

- **An account activation link**. Click the link and set the password for the account. Remember your login that is shown on the account activation page.
- **A link to the notary console login page**. Use this link to access the console in the future. The login and password are the same as in the previous step.

2.2 Accessing the notary service web interface

You can log in to the notary service if you activated your account.

To log in to the notary service

1. Go to the notary service login page. The login page address was included in the activation email message.
2. Type the login, and then click **Continue**.
3. Type the password, and then click **Sign in**.
4. If you have the company administrator role, click **Notary**.

   Users who do not have the company administrator role log in directly to the notary console.

You can change the language of the web interface by clicking the account icon in the top-right corner.

If **Notary** is not the only service you are subscribed to, you can switch between the services by using the  icon in the top-right corner. Company administrators can also use this icon for switching to the management portal.

2.3 Notarizing files

To notarize a file

1. Click **Notarized files**.
2. If there are no notarized files, click **Browse**. Otherwise, click **Add files**, and then click **Browse**.
3. Specify the files that you want to notarize.

   Once you select a file, the software starts uploading it to the cloud storage.

4. After all of the files are uploaded, click **Notarize**.

   The software calculates a hash code for each file. The statuses of the files change to **In progress**. The usage of the **Notarizations** quota is increased by the number of the files.

5. Wait until each file status changes from **In progress** to **Notarized**.

   The notarization process can take up to 70 minutes. To reduce the cost of each notarization, the notary service collects hashes throughout an hour, then builds a hash tree based on these hashes and sends the hash tree root to the blockchain database. After that, the notary service waits for the transaction to become confirmed in the blockchain database, and then changes the statuses of the files to **Notarized**.

Notarization certificate

After the notarization is complete, the service creates a notarization certificate for each file. This certificate is irrefutable proof that the file was notarized at a specific time. The certificate contains:

- Information about the notarization (the file name, hash, size, notarization timestamp, requestor, requestor GUID, signee, blockchain transaction ID, and certificate ID)
- Instructions on how to verify the file manually without using the notary service

2.3.1 Operations with notarized files

To download a file from the cloud storage

1. Click **Notarized Files**.
2. Find the required file in the list.

   You can filter files by status; sort files by name, status, notarization, and upload dates; or use search.

3. Click  or click the file name, and then click **Download**.

To view the notarization certificate of a file

1. Click **Notarized Files**.
2. Find the required file in the list. Notarization certificates are available only for files with the **Notarized** status.

   You can filter files by status; sort files by name, status, notarization, and upload dates; or use search.

3. Click the file name.
4. Click **Notarization certificate** to view the certificate in a new window.

To delete a file from the cloud storage

1. Click **Notarized files**.
2. Find the required file in the list.

   You can filter files by status; sort files by name, status, notarization, and upload dates; or use search.

3. Click  or click the file name, and then click **Delete**.

   If the file has been notarized, it will remain notarized. We recommend that you save the notarization certificate or save the direct link to it prior to confirming the deletion.

   Important *If the notarization is in progress, it will not be canceled. However, there will be no way to view or download the file's notarization certificate.*

4. Confirm your decision.

2.4 Verifying file authenticity

You can verify file authenticity by uploading the file to the cloud storage or by using the blockchain receipt from the file's notarization certificate.

Files that are uploaded for verification do not use the **Notary storage** quota. They are deleted from the cloud storage after the verification process is complete.

To verify the file authenticity by uploading the file to the cloud storage

1. Access the notarization certificate as described in the "To view the notarization certificate of a file" (p. 5) procedure.
2. Find the certificate ID and copy it.
3. In the notary console, click **Verification**.
4. Click **Browse**, and then select the file whose authenticity you want to verify. You can select multiple files.

   Once you select a file, the software starts uploading it to the cloud storage.
5. Specify the file certificate ID to confirm your right for this file verification.
6. Click **Verify**.
7. The software displays the verification reports for the selected files.
   - If a file is authentic, its status is **Notarized**.
   - If a file is not authentic or has never been notarized, its status is **Not notarized**.
   - If a file is still being notarized, its status is **In progress**.

To verify a file by using a blockchain receipt

1. Access the notarization certificate as described in the "To view the notarization certificate of a file" (p. 5) procedure.
2. Find the **Blockchain receipt** section and copy the following contents, including the brackets:

   ```
   {
    "key": "filename.pdf",
    "eTag": "52bf7a18744b384afba39f3646d8e245...",
    "size": 1267387,
    "sequencer": "B56C3FE5ED984F5337"
   }
   ```

   These strings present the file name, SHA-256 hash, size in bytes, and the blockchain transaction number.
3. In the notary console, click **Verification**.
4. Click **Verify by using the blockchain receipt**.
5. Paste the contents that you copied from the **Blockchain receipt** section to the blank field.
6. Click **Verify**.
7. The software displays the verification report.
   - If the file is authentic, its status is **Notarized**.
   - If the file is not authentic or has never been notarized, its status is **Not notarized**.
   - If the file is still being notarized, its status is **In progress**.

To verify a file by using a file hash

1. Access the notarization certificate as described in the "To view the notarization certificate of a file" (p. 5) procedure.
2. Find the file hash and certificate ID, and copy them.

3. In the notary console, click **Verification**.
4. Click **Verify by using the file hash**.
5. Specify the file hash.
6. Specify the file certificate ID to confirm your right for this file verification.
7. Click **Verify**.
8. The software displays the verification report.
   - If the file is authentic, its status is **Notarized**.
   - If the file is not authentic or has never been notarized, its status is **Not notarized**.
   - If the file is still being notarized, its status is **In progress**.

Public verification page

There is also a public verification page where a non-authorized user can verify a file authenticity by using one of the following three ways:

- Uploading a file itself and certificate ID
- Specifying a file's hash and certificate ID
- Providing a blockchain receipt and certificate ID

2.5 Signing files

The notary service enables you to send a file to multiple people to sign it electronically.

To sign a file, you need to upload it to the cloud storage. After the file is signed, the notary service generates a signature certificate that contains the collected signatures. This certificate is then notarized by using the notary service. The signed files are not notarized.

For example, you can electronically sign the following files:

- Rental or lease agreements
- Sales contracts
- Asset purchase agreements
- Loan agreements
- Permission slips
- Financial documents
- Insurance documents
- Liability waivers
- Healthcare documents
- Research papers
- Certificates of product authenticity
- Nondisclosure agreements
- Offer letters
- Confidentiality agreements
- Independent contractor agreements

To sign a file

1. Click **Signed files**.
2. If there are no signed files, click **Browse**. Otherwise click **Add file**, and then click **Browse**.

3. Specify the file to sign.

   Once you select a file, the software starts uploading it to the cloud storage.
4. Click **Add signees**, and then add signees by specifying their email addresses.

   To remove a signee, click the trash can icon.

   Important *It is not possible to add or remove signees after sending the invitations, so ensure that the list includes everyone whose signature is required.*
5. Click **Send to sign** to send invitations to the signees.

   Each signee receives an email message with the signature request. You will receive notifications when each signee signs the file and when the entire process is complete.
6. Once the process is complete, select the signed file, and then click **Signature certificate** to download a .pdf document that contains:
   - The Signature Certificate section with the collected signatures.
   - The Audit Trail section with a history of activities: when the invitation was sent to the signees, when each signee signed the file, and so on.

Once the process is complete, each signee receives a notification that contains:

- A link to the signed file.
- A link to the signature certificate.
- A link to the notarization certificate for the signature certificate. The notarization certificate becomes available within 70 minutes after the signing process is complete.

2.5.1 Operations with signed files

To download a signed file from the cloud storage

1. Click **Signed Files**.
2. Find the required file in the list.
   You can filter files by status; sort files by name, status, signature, and upload dates; or use search.
3. Click  or click the file name, and then click **Download**.

To delete a signed file from the cloud storage

1. When you delete a signed file from the cloud storage, its signature certificate is also deleted. If you may need the signature certificate in the future, ensure that you have saved a local copy of it as described in step 6 of the "To sign a file" (p. 7) procedure.

   The signature certificate will remain notarized.
2. Click **Signed Files**.
3. Find the required file in the list.
   You can filter files by status; sort files by name, status, signature, and upload dates; or use search.
4. Click  or click the file name, and then click **Delete**.
5. Confirm your decision.

   We recommend that you download the notarization certificate of the signature certificate or save the direct link to it prior to confirming the deletion.

3 Administering the notary service

This section describes the functionality that is available only to the notary service administrators.

3.1 Managing API keys

The notary service can be integrated with third-party systems by using the notary service application programming interface (API). For more information about using the API, refer to the developer's guide at https://dl.managed-protection.com/u/baas/api/NotaryDeveloperGuide/.

A notary service administrator can create and manage API keys for the integrations.

To create an API key

1. Click **API Keys** > **Create API key**.
2. Create and enter a unique name for the API key.
3. Click **Create**.
4. The API key is created with the **Enabled** status by default.

   Important *Copy and save the key. For security reasons, the key is displayed only once. There is no way to retrieve the key if you lose it.*

To disable an API key

1. Click **API Keys**.
2. Find the required key in the list.

   You can filter keys by status; and sort keys by name, status, and creation date.
3. Click  , and then click **Disable**.
4. Confirm your decision.

   All integrations that use this key will stop working. It will be possible to re-enable the key at any time.

To enable a disabled API key

1. Click **API Keys**.
2. Find the required key in the list.

   You can filter keys by status; and sort keys by name, status, and creation date.
3. Click  , and then click **Enable**.

To delete an API key

1. Click **API Keys**.
2. Find the required key in the list.

   You can filter keys by status; and sort keys by name, status, and creation date.
3. Click  , and then click **Delete**.
4. Confirm your decision.

   All integrations that use this key will stop working. There is no way to recover a deleted API key.

3.2 Administering user accounts and quotas

Administering user accounts and service usage quotas is available in the management portal. To access the management portal, click **Management Portal** when logging in to the notary service or

click the  icon in the top-right corner, and then click **Management portal**. Only users that are assigned the company administrator role can access this portal.

For information about administering user accounts and their quotas, refer to the Management Portal Administrator's Guide. To access this document, click the question mark icon in the management portal.

This section provides additional information related to managing the notary service.

Quotas

Quotas enable you to limit the users' ability to use the service. To set the quotas, select the user on the **Users** tab, and then click the pencil icon in the **Quotas** section.

When a quota is exceeded, a notification is sent to the user's email address. If you do not set a quota overage, the quota is considered "soft". This means that restrictions on using the notary service are not applied.

You can also specify the quota overages. An overage allows the user to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the notary service are applied.

Managed-service providers can also specify quotas for their customer companies in a similar way.

The following quotas are available:

- **Notary storage**

  The notary storage is the cloud storage where the notarized files, signed files, and files whose notarization or signing is in progress are stored. This quota defines the maximum space that can be occupied by these files.

  To decrease this quota usage, you can delete the already notarized or signed files from the notary storage.
- **Notarizations**

  This quota defines the maximum number of files that can be notarized by using the notary service. A file is considered notarized as soon as it is uploaded to the notary storage and its notarization status changes to In progress.

  If the same file is notarized multiple times, each notarization counts as a new one.
- **eSignatures**

  This quota defines the maximum number of files that can be signed by using the notary service. A file is considered signed as soon as it is sent for signature.

Notifications

To change the notifications settings for a user, select the user on the **Users** tab, and then click the pencil icon in the **Settings** section. The following notifications settings are available:

- **Quota overuse notifications** (enabled by default)

  The notifications about exceeded quotas.
- **Scheduled usage reports**

  The usage reports described below that are sent on the first day of each month.

All notifications are sent to the user's email address.

Usage reports

The report about using the notary service includes the following data about a company or a unit:

- Size of files stored in the notary storage (except for the files being verified) by unit, by user.
- Number of notarizations by unit, by user.
- Number of signed files by unit, by user.
- The total size of files stored in the notary storage (except for the files being verified).
- The total number of notarizations.
- The total number of signed files.