Notary Service

24.03

Administrator Guide

REVISION: 3/22/2024

Table of contents

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.

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".

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.

User roles

There are two user roles in the notary service: notary administrator and notary user.

Both administrators and users have access to the entire notary service functionality in the notary console.

All users have access only to their own templates, notarized and eSigned files.

Administrators have elevated rights to view and work with the templates, notarized and eSigned files that belong to the other users or administrators in the customer tenant. Administrators and users can manage the notary service API keys and use the notary API. Administrators and users have access only to their own API keys.

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.

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.

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
- 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.

Using the notary service

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.

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 upper-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 upper-right corner. Company administrators can also use this icon for switching to the management portal.

Using the notary service as a notary user

Notary users have access only to their own templates, notarized and eSigned files.

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. Select 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 ledger. After that, the notary service waits for the transaction to become confirmed in the blockchain ledger, and then changes the statuses of the files to **Notarized**. When the status of the file becomes **Notarized**, you are notified by email.

   Note
   If a file is still not notarized 24 hours after it is uploaded, its status changes from **In progress** to **Notarization pending**, and you are notified by email.

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, signer, blockchain transaction ID, and certificate ID)
- Instructions on how to verify the file manually without using the notary service

Note
Be aware that your personal data, such as email and IP address, will be preserved in the audit trail and will be accessible to all signers.

Operations with notarized files

To download a file from the cloud storage

1. Click **Notarized Files**.
2. Find the 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 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 **View and download notarization certificate** to view the certificate in a new tab.

Note
You can copy the values of the **File hash (SHA-256)**, **Certificate ID**, or **BLOCKCHAIN RECEIPT** of the notarization certificate by clicking the corresponding **Copy to clipboard** icon.

To download the notarization certificate of a file

1. Click **Notarized Files**.
2. Find the 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 **View and download notarization certificate** to view the certificate in a new tab.
5. In the new tab, click **Download notarization certificate**.

To delete a file from the cloud storage

1. Click **Notarized files**.
2. Find the 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. Click **Delete** again to confirm your decision.

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" 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" 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" 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

Signing files

The notary service enables you to send a file to multiple people to sign it electronically, or to sign it electronically as a single signer.

To sign a file, you need to upload it to the cloud storage, or to create it from a template.

For files that can be converted to .pdf file format, the hand-written or text-converted signature or initials of the signers can be embedded as images in the signed document. In that case, the content of the signed file is saved with the embedded eSignatures in the signature certificate .pdf file, and that file is then notarized by using the notary service. This feature is supported for the following file formats: .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, and .pdf.

You can use embedded eSignatures to sign electronically the following document types:

- 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

For files that cannot be converted to .pdf format, 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.

Signing a file as the only signer

You can upload a file and sign it electronically as the only signer.

To upload a file and sign it electronically as the only signer

1. Click **Signed files**.
2. [Optional] If you want to add a new file for signing, click **Browse**, or click **Add file**, and then click **Browse**.
3. Select the file to sign.

   Once you select a file, the software starts uploading it to the cloud storage.
4. In the **Add signers** dialog, select **I'm the only signer**, and then click **Next**.
5. In the **Add fields to the document** dialog, drag and drop the fields that you want to add to the document.
6. Click **Preview and send**.
7. Preview the document, and then click **Send**.

   The document appears in the Signed Files list with status **Waiting for me**.
8. In the **Files** tab, click the document, and then click **Sign**.
9. In the **Enter your name, initials and eSignature** dialog, select the method to sign the file.
   - **Suggested eSignature and initials** – the eSignature and initials are generated automatically. If necessary, you can change them manually.
   - **Handwritten eSignature and initials** – you draw your signature and initials in the corresponding fields, and they are included as images in the signed document.

   > **Note**
   > This option is supported for the following file formats: .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, and .pdf.
10. Select the **I have read and agree** check box, and then click **Next**.
11. In the **Sign document** dialog, click in the **eSignature** field to populate it with your eSignature.
12. Click **Preview and sign**.
13. Preview the document, and then click **Sign**.

    The signed file is saved as .pdf file format.
14. When the process is complete, select the signed file, click the **eSignature certificate** tab, and then click **eSignature certificate** to download a .pdf document that contains:
    - The eSignature Certificate section with the collected signatures.
    - The **Audit Trail** section with a history of activities: when the invitation was sent to the signers, when each signer signed the file, and so on.

15. Click **View and download notarization certificate**, and then click **View and download notarization certificate** to download the notarization certificate for the eSignature certificate. The notarization certificate becomes available within 70 minutes after the signing process is complete.

Sending a file for signing by multiple signers

You can upload a file and send it for eSignature to multiple signers.

To send a file for signing by multiple signers

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

   Once you select a file, the software starts uploading it to the cloud storage.
4. In the **Add Signers** dialog, click **Add signers**, and then type the email address of the signer. Repeat the step for each signer that you want to add.

   Important
   It is not possible to add or remove signers after sending the invitations. To remove a signer, click the trash can icon. Ensure that the list of signers is complete, before continuing to the next step.
5. Click **Next**.
6. In the **Add fields to the document** dialog, add the necessary signer and custom fields.
7. Click **Preview and send**.
8. Preview the document, and then click **Send** to send invitations to the signers.

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

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

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

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 eSignature certificate is also deleted. If you may need the eSignature 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" 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 eSignature certificate or save the direct link to it prior to confirming the deletion.

Document templates

You can create document templates, and use them to facilitate the process of creating new files for eSignature.

The document template is a blueprint for repeatable transactions. With document templates you create the document content, including a set of required or optional fields, and assign exact signers later. The recipients and signers can change every time you use a document template to create a new file.

You create a document template by:

1. uploading a file that is in a PDF file format, or a format that can be converted to a PDF file format - TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX, and PDF.
2. adding at least one signer field to the template
3. adding fields for each additional signer, if necessary
4. adding custom fields, if necessary
5. saving the template

Note
You can save a document template only if it includes at least one Signer field.

Document template fields

The process of creating a document template consists of uploading a file that contains the main information, and adding predefined or custom template fields to it.

There are two kinds of document template fields: **Signer** fields and **Custom** fields.

Signer fields are strictly predefined fields for the signer's information. You can add and remove signer fields from a template, and configure if they are required or optional, but you cannot change their name.

Signer field name	Description
Name	Name of the signer of the document.
Signature	Signature of the signer of the file. By default, the field is required. To make it optional, select the **Optional** checkbox.
Initials	Initials of the signer of the file. By default, the field is required. To make it optional, select the **Optional** checkbox.

Custom fields are free text fields that you can add to the template, depending on your needs. You can set the name of the custom field (for example, **Date**, or **Billing address**) when you create the template, and fill its content when you create a new file from the template.

Note
The content of the custom fields always appears in the same font and size.

Creating a document template

You can create a template and use this template to easily generate new files for eSignature.

To create a document template

1. Click **Signed files**>**Templates**.
2. Click **Create template**.
3. In the **Upload document for your template** window, use one of the following options to upload the file:
   - drag and drop the file.
   - click **Browse**, navigate to the file, and select it.
4. **Important**
   The file format of the template must be PDF, TXT, DOC, DOCX, XLS, XLSX, PPT, or PPTX.
5. In the **Signers** tab, click at least one of the predefined fields for **Signer 1**.

Note

After you click a field, it appears on the template. You can drag the field to change its position in the template. You can also drag the corresponding edges of the field to change its size.

6. [Optional] For each additional signer that you want to add:
   a. Click **Add signer**.
   b. Add at least one of the Signer fields to the template.
7. [Optional] To add a custom field, in the **Custom fields** tab:
   a. Click the pencil icon next to the Custom field label.
   b. In the **Rename custom field** window, type a name of the custom field. The maximum allowed length for the name is 30 characters.
   c. Click the field to add it to the document template, and use the mouse to move it to the appropriate position.
8. [Optional] For each additional custom field that you want to add:
   a. Click **Add custom field**.
   b. Click the pencil icon next to the Custom Field label.
   c. In the **Rename custom field** window, type a name of the custom field. The maximum allowed length for the name is 30 characters.
   d. Click the field to add it to the document template, and use the mouse to move it to the appropriate position.
9. Click **Preview and create**.
10. If the information in the template is correct, click **Create**.

    The new template becomes visible on the **Templates** page. For more information about the actions that you can perform from the **Templates** page, see "Managing document templates" (p. 14).

Managing document templates

After you create a template, it is listed on the **Templates** page. On the **Templates** page, you can view additional information about the existing templates, and perform the following actions:

- Preview a document template
- Create a file from a document template
- Rename a document template
- Delete a document template

The following table describes the information that is available on the **Templates** page.

Column name	Description
Template name	Name of the template.
Uploaded document	Name of the file from which the template was created.

Column name	Description
Created documents	Number of files that were created using this template.
Created	Date and time when the template was uploaded.
ID	System ID number of the template; generated automatically.

Previewing a document template

To preview a document template

1. In **Signed files** > **Templates**, find the document template that you want to preview.
2. Click ••• and then click **Preview**.
3. After you finish the preview process, click **Done**.

Renaming a document template

To rename a document template

1. In **Signed files** > **Templates**, find the document template that you want to rename.
2. Click ••• and then click **Rename**.
3. In the **Template name** field, update the template name.
4. Click **Rename**.

Deleting a document template

To delete a document template

1. In **Signed files** > **Templates**, find the document template that you want to delete.
2. Click ••• and then click **Delete**.

Creating a document from a template

You can easily create a new document from an existing document template, and send it for eSignature.

To create a document from a document template

1. Click **Signed files**>**Templates**.
2. In the list of document templates, find the document template that you want to use.
3. Click ••• and then click **Create document**.
4. In the **Create document from the template** window, in the **Document name** field, type the name of the file.
5. Type the email addresses of the document's signers.

Note

The email addresses that you enter will be used to send an email to all the signers of the file. This email contains a link that the signers can use to view and sign the file electronically.

6. If the template includes custom fields, click **Next**. If not, go to step 8.
7. In the custom fields, fill the information.

Note

The length of the custom fields is limited to 250 symbols.

8. Click **Preview and create**.
9. If the information in the file is correct, click **Create**.

Note

The file is created and becomes visible in **Signed files**->**Files**. You can see the name of the template that you used to create the document in the **Template name** column.

An email that contains a link to view and sign the file electronically is sent to all the signers of the document. Each signer of the document can sign it following the "Signing a file that is created from a template" (p. 16) procedure.

Signing a file that is created from a template

After a file is created from a template, all signers of the file receive an email with a link that they can use to sign the file using eSignature.

To electronically sign a file that was created from a template

1. In your email, find the email notification from sender notaryacronissg@gmail.com, and open it.
2. Click **Review and sign**.
3. In the **Enter your name, initials and signature** window, enter your name, initials, and eSignature.
4. Select **I have read and agree**.
5. Click **Done**.
6. In the **Sign document** window, click the relevant fields to populate the content from step 3.
7. Click **Preview and sign**.
8. When you are ready with the file preview, click **Sign**.

The signed file is saved in a PDF file format. A Signature Certificate, and a Notarization certificate for the signature certificate are created. The notarization certificate becomes available within 70 minutes after the signing process is complete. You can download the file and the certificates.

Using the notary service as a notary administrator

When working with templates, notarized and electronically signed files that he or she owns, the notary administrator can perform the same functions as a notary user. For more information, see "Using the notary service as a notary user" (p. 5).

Additionally, the notary administrator can perform several functions that are not available to the notary user:

- View the templates, notarized and electronically signed files that are created by the other users or administrators in the customer tenant.
- View the owner of all templates, notarized and electronically signed files in the customer tenant. The owner is visible in the **Owner** column in the notary service console, in the **Notarized files**, **Signed files**, and **Templates** tabs.
- View the progress of the signing process for all documents that are created by the other users or administrators in the customer tenant.

Note
The administrator cannot sign documents on behalf of other users. The administrator can sign only documents when he or she is added as a signer.

- Resend invitations to the signers of a document that is created by another user or administrator in the customer tenant.
- Download the original templates, notarized and electronically signed files that are created by the other users or administrators in the customer tenant.
- Download the eSigned files (if the process of signing the document using eSignature is completed) that are created by the other users or administrators in the customer tenant.
- Download the signature certificate files (if the process of signing the document using eSignature is completed) of the eSigned files that are created by the other users or administrators in the customer tenant.
- Delete the templates, notarized and eSigned files that are created by the other users or administrators in the customer tenant. The owners of the deleted templates or files are notified through email.
- Create new documents from the document templates that are created by the other users or administrators in the customer tenant. The owners of the document templates are notified through email.

Administering the notary service

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

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://developer.acronis.com/doc/notary/v2/guide/.

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.

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 upper-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.

- **Document templates**

  This quota defines the maximum number of document templates that the customer can save.

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.

Index