Guide for Enterprise Approvers

HARICA's CertManager Portal

Contents

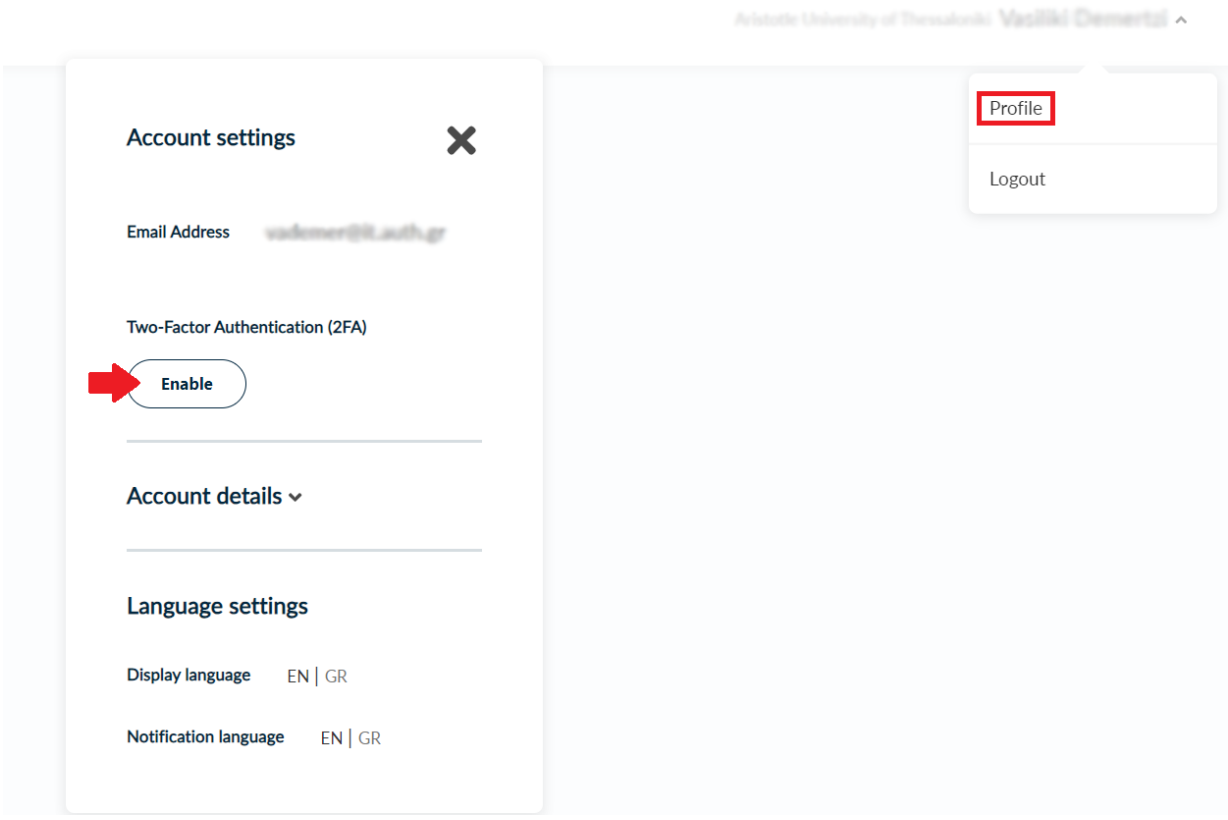
A) Enterprise Approver Role

1. Visit HARICA's CertManager and sign up to create your account.

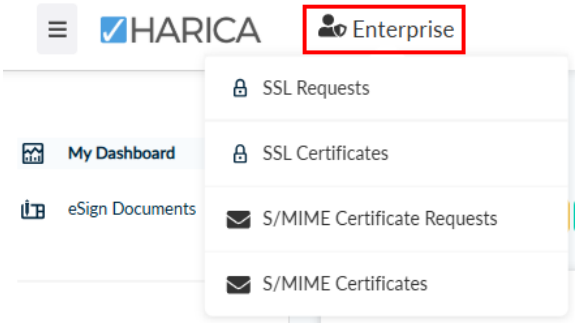
   Your personal information must be accurate and fully matched (letter-by-letter) with a government-issued identification document.

2. Once you log in, from the top right corner, click on your name and select **Profile**. From the *Account Settings* menu, click **Enable** and follow the on-screen instructions to activate **Two-Factor Authentication (2FA)** as it is required for this role.

   After the process is completed, please inform an Enterprise Admin of your Enterprise in order to provide you access as Enterprise Approver.



3. When you gain access, a new menu *Enterprise* will appear on the portal.

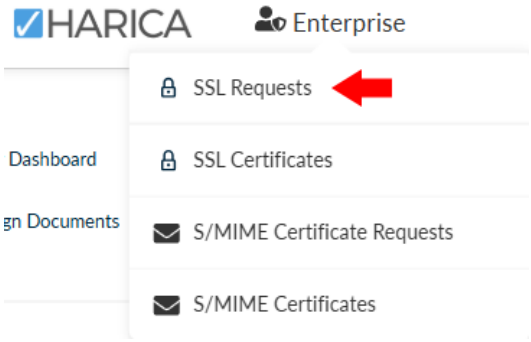


4. As an *Enterprise Approver*, you will be able to:
   - view and verify SSL and S/MIME certificate requests, and
   - manage SSL and S/MIME certificates,

   These features are described in detail below.

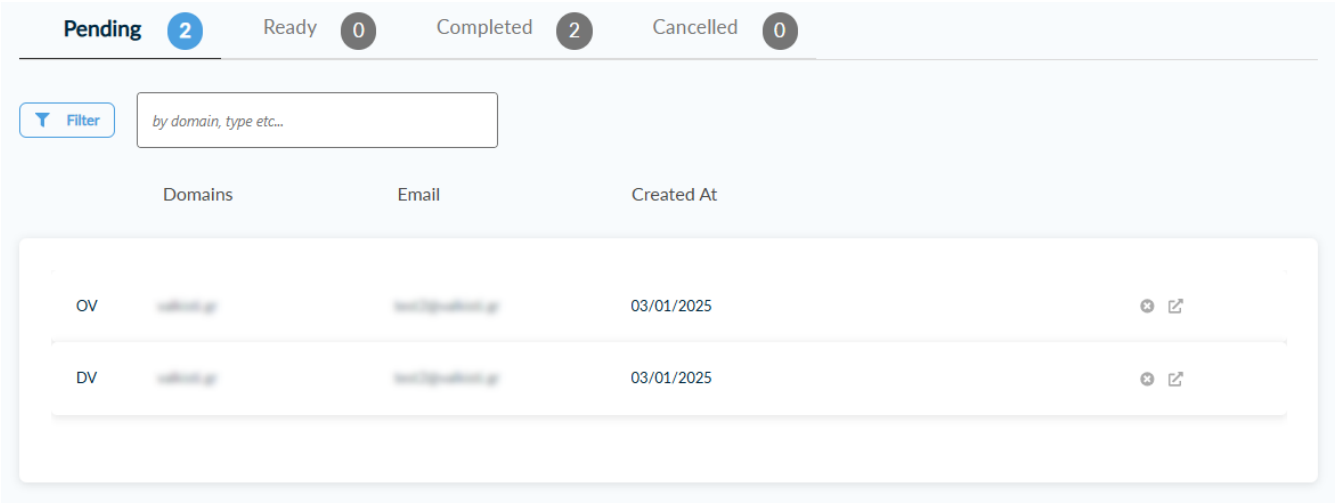
B) SSL Certificate Requests

1. To view all SSL certificate requests, go to **Enterprise → SSL Requests**.

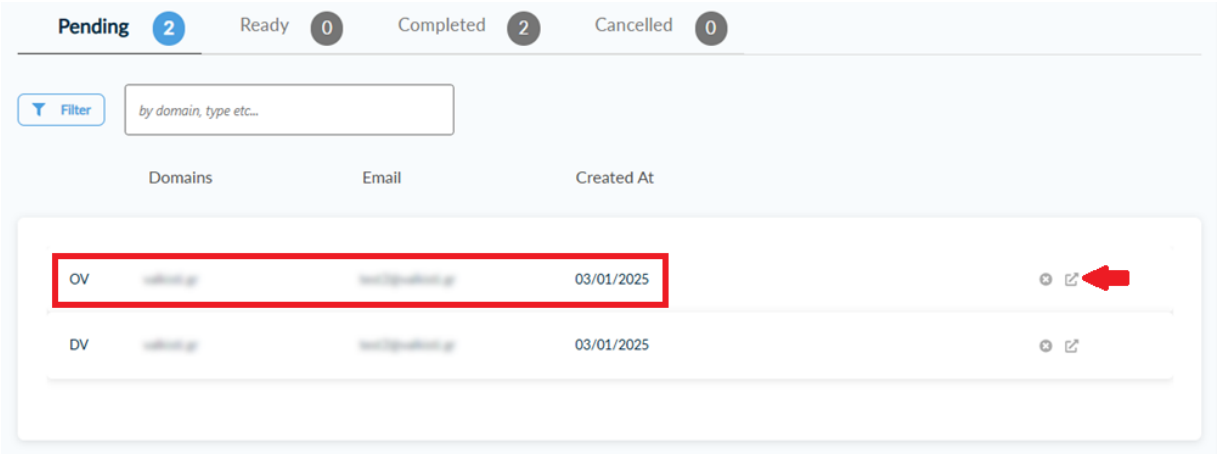


2. As an SSL Approver, you will be responsible for reviewing and approving SSL certificate requests. This involves verifying that the users submitting these requests have control or ownership of the domains included in their requests.
   Certificate requests can have one of four statuses:
   - **Pending**: Requests that require your approval.
   - **Ready**: Approved requests where the user has not yet enrolled their certificate.
   - **Completed**: Requests where the certificate has been successfully issued.
   - **Cancelled**: Requests that have been cancelled, either by the user or the SSL Approver.

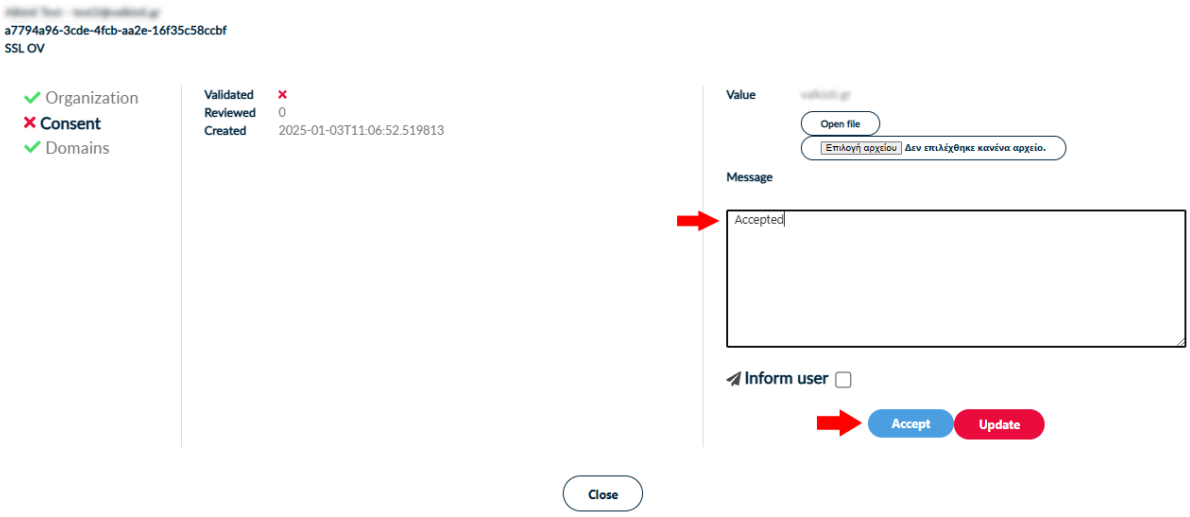
   You can view and manage requests in the corresponding tabs based on their status.



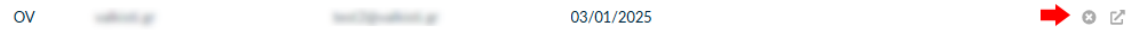
3. To view a pending certificate request, click on it or on the **Show details** button located on the far-right side.



4. A pop-up window will appear, displaying the details of the request. On the left side, you will find three tabs: **Organization** (applicable for SSL OV, not DV), **Consent**, and **Domains**. Go to the **Domains** tab to review the domains included in the request and verify that the user has control or ownership of the submitted domains.
Once verification is complete, go to the **Consent** tab, add a note in the corresponding field (for internal use only; this message will not be sent to the user) and click **Accept** to approve the request.

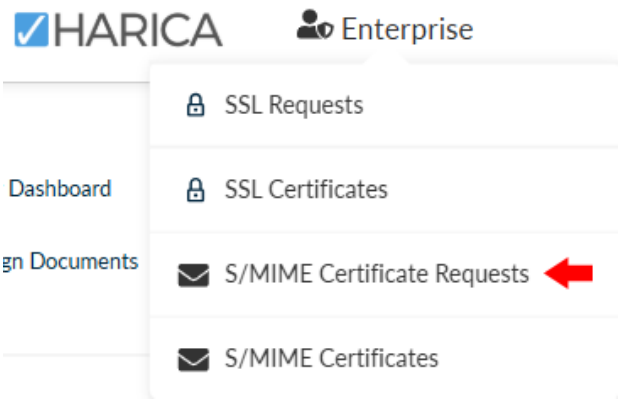


5. Press on the **X** button to reject the transaction and cancel the request, if necessary.



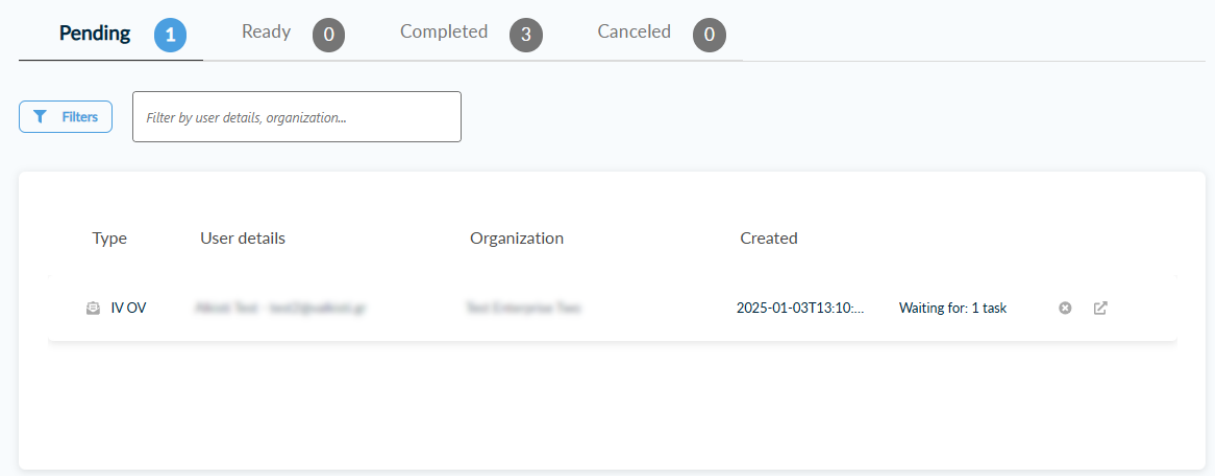
C) S/MIME Certificate Requests

1. To view all S/MIME certificate requests, go to **Enterprise → S/MIME Certificate Requests**.

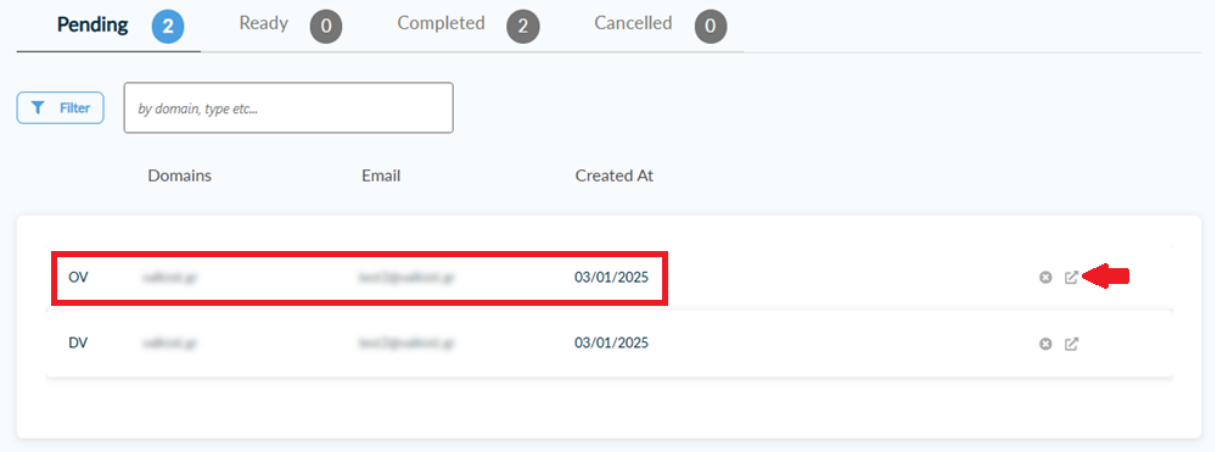


2. As an S/MIME Approver, you will be responsible for reviewing and approving S/MIME certificate requests. This involves verifying users' personal information in correspondence with their identification document which is submitted during the request process.
Certificate requests can have one of four statuses:
   - **Pending**: Requests that require your approval.
   - **Ready**: Approved requests where the user has not yet enrolled their certificate.
   - **Completed**: Requests where the certificate has been successfully issued.
   - **Cancelled**: Requests that have been cancelled, either by the user or the SSL Approver.

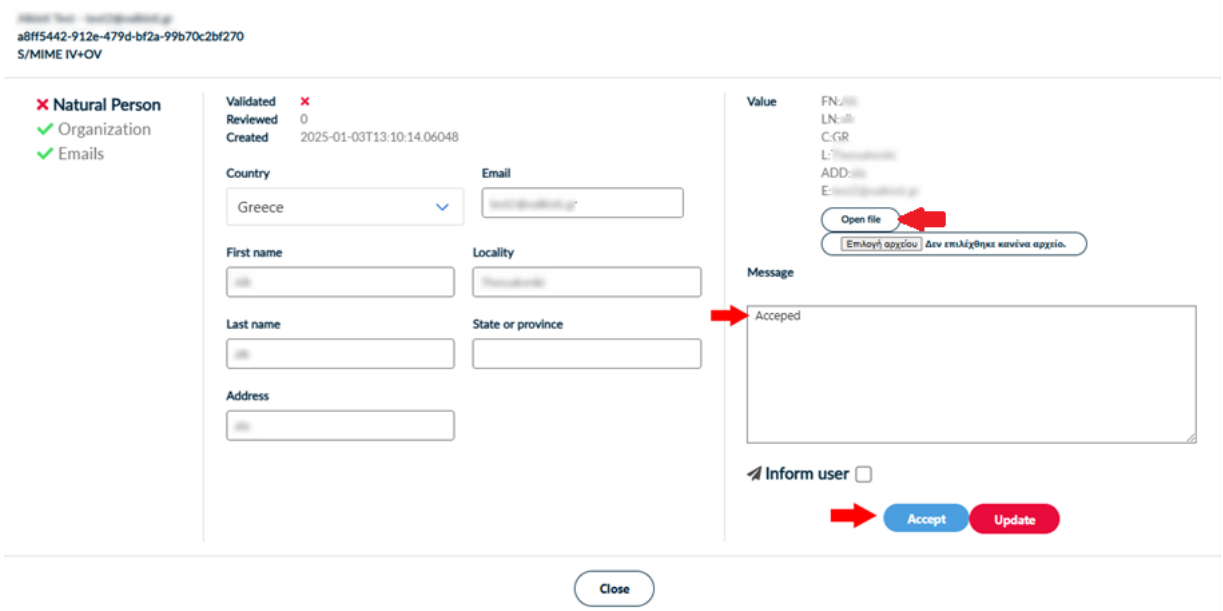
   You can view and manage requests in the corresponding tabs based on their status.



3. To view a pending certificate request, click on it or on the **Show details** button located on the far-right side.

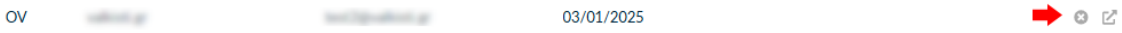


4. A pop-up window will appear, displaying the details of the request. On the left side, you will find three tabs: **Natural Person** and **Organization** (applicable for S/MIME IV+OV (SV), not Email-Only), and **Emails**. Go to the **Natural Person** tab to review user's personal information in correspondence with their identification document. You can view the document by pressing the **Open file** button.
Once verification is complete, add a note in the corresponding field (for internal use only; this message will not be sent to the user) and click **Accept** to approve the request. (Press the **Update** button only if you need to modify the user's information before accepting the Natural Person review)



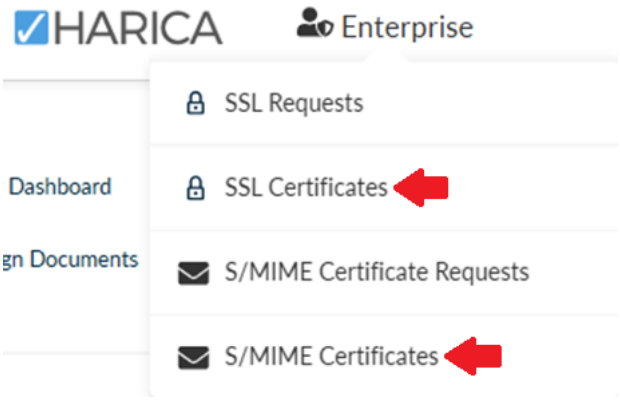
Please note that the **Emails** tab will be check marked once the user completes email validation for the specified email addresses.

5. Press on the **X** button to reject the transaction and cancel the request, if necessary



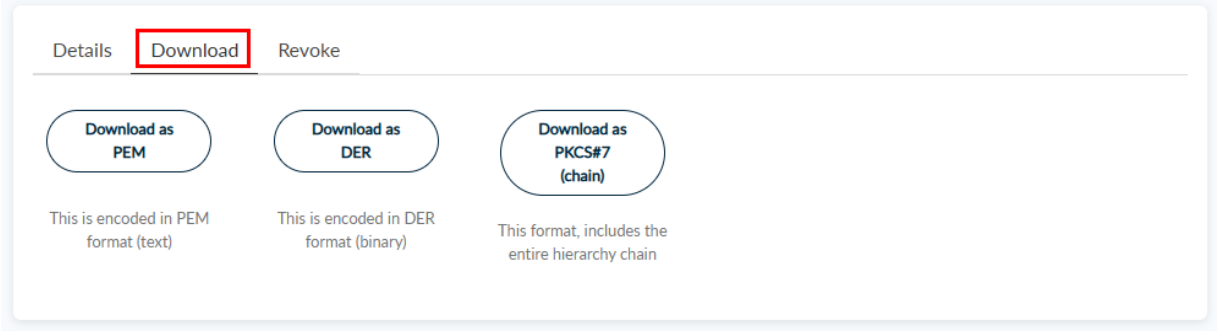
D) Manage Certificates

1. To view all issued certificates, from the *Enterprise* menu, go to **SSL Certificates** or **S/MIME Certificates**.

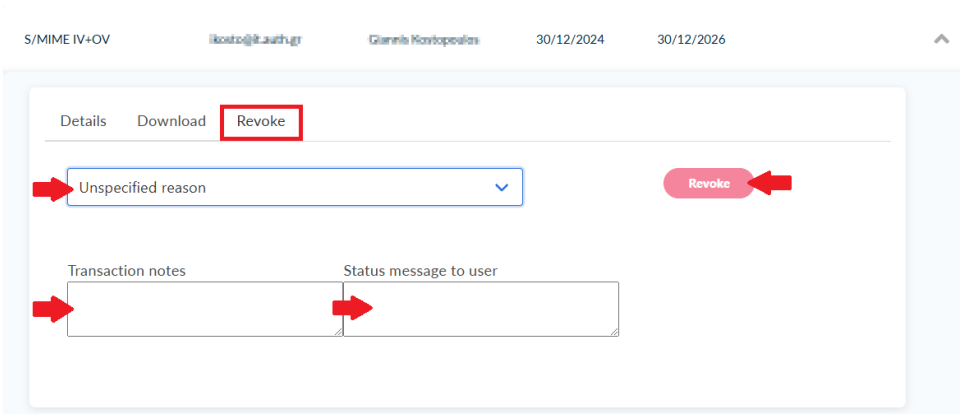


2. Click on a certificate to view the certificate details.

3. Go to the **Download** tab to download the certificate's public key in various formats.



4. Go to the **Revoke** tab to revoke the certificate, if necessary.


S/MIME IV+OV
30/12/2024
30/12/2026
Details
Download
Revoke
Unspecified reason
Revoke
Transaction notes
Status message to user