User Guide - Aurora Networks PKIWorks

CableLabs PKI Operations
Version: 5.1
Date: October 27, 2026

TABLE OF CONTENTS

TABLE OF CONTENTS 2

1 INITIAL SETUP AND SYSTEM ACCESS 3

1.1 Sign Up for a My Vistance Networks Account 3

1.2 Sign In 3

1.3 Select Account 3

1.4 Home Screen 4

2 GENERATING AND DOWNLOADING NEW CERTIFICATES 4

2.1 Generating Certificates 4

2.1.1 Certificate generation by MAC range - PKCS#8 4

2.1.2 Certificate generation with user-generated certificate signing request (CSR) PKCS#10 7

2.1.3 Certificate generation with an upload file PKCS#12 9

2.2 Accessing Certificates 11

2.2.1 Request Status Explanation 11

2.1.2 View Requests and Status 11

2.1.3 Download Output File 12

2.1.4 Confirm File Download 13

2.1.5 PKCS#8 Output File Using PGP Key Decryption 14

3 DOWNLOADING ROOT AND INTERMEDIATE CERTIFICATES 14

4 REVOKING CERTIFICATES 15

4.1 New Revocation Request 15

5 APPENDIX A – PGP PUBLIC KEY MANAGEMENT 20

5.1 View PGP Public Key 20

5.2 Manage PGP Public Key 21

5.3 Verify PGP Key 27

5.4 Remove PGP Public Key 29

1 INITIAL SETUP AND SYSTEM ACCESS

1.1 SIGN UP FOR A MY VISTANCE NETWORKS ACCOUNT

To create an account, follow the instructions in the My Vistance Networks Sign Up Instructions document. Be sure to use the same email address currently registered to your PKIWorks user account.

1.2 SIGN IN

Go to the PKIWorks web portal. Sign in using your organization email address and password. Complete multifactor authentication (MFA) steps as directed. Unless your company has Single Sign On (SSO) enabled for the PKIWorks Portal, expect an email verification as part of MFA verification. Once MFA is completed, review and accept the agreement to continue.

1.3 SELECT ACCOUNT

After signing in and accepting the agreement, the **Select Account** dialog is displayed. This dialog lists your authorized user accounts and company accounts, along with their expiration dates, if applicable. Select an active account to access available functions, including submitting, viewing, and downloading requests.

If either the user account or company account has expired, contact pkiops@cablelabs.com for assistance.

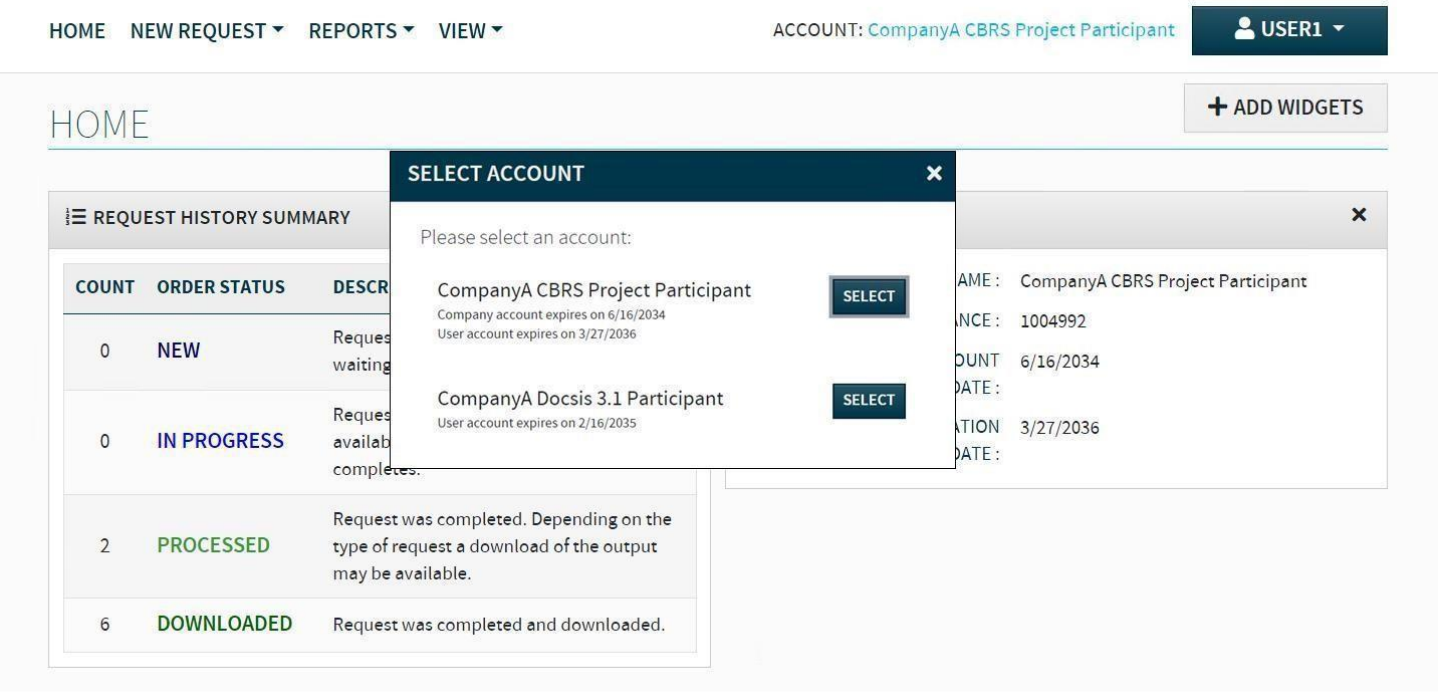

Figure 1 – Select Account

1.4 HOME SCREEN

After selecting an account, the **Home** page for that account is displayed. The default home page contains **Account Summary** and **Request History Summary**.
The **Account Summary** section displays information about the selected account, including the account name, remaining balance, company account expiration date (if applicable), and user account expiration date (if applicable).

The **Request History Summary** section provides an overview of requests submitted under the selected account, including the total number of requests and a summary of their current statuses. To view detailed information for a request, go to View Request page.

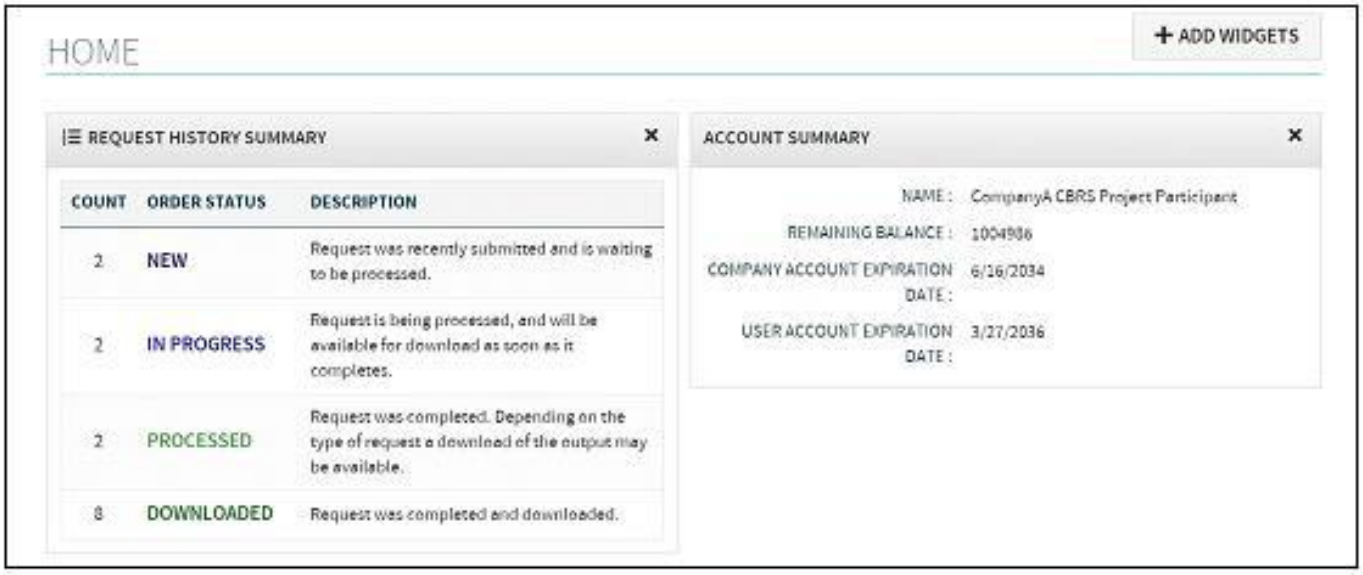

Figure 2 – Home Screen

2 GENERATING AND DOWNLOADING NEW CERTIFICATES

2.1 GENERATING CERTIFICATES

This section describes how to submit a new request.
To create a new request, navigate to New Request and select + Key and Certificate Generation Request.
Next, select a profile. Each account is preconfigured with one or more profiles, and the selected profile determines the type of request that can be submitted. To request additional profiles, contact pkiops@cablelabs.com.

2.1.1 CERTIFICATE GENERATION BY MAC RANGE - PKCS#8

This request type generates keys and certificates for one or more identifiers (IDs). The generated keys and certificates are packaged in the request output.

First, select a PKCS#8 profile. After the profile is selected, a warning reminds the subscriber to confirm possession of the corresponding PGP private key and passphrase.

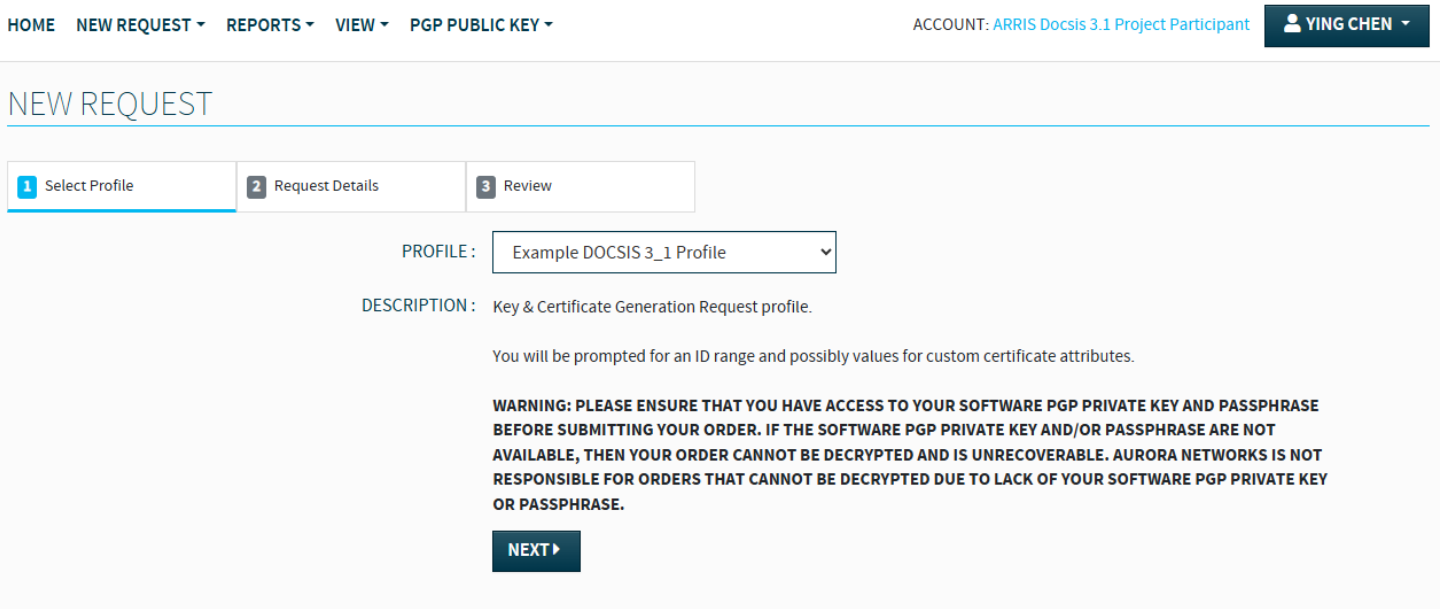

Figure 3 – Select a PKCS#8 Profile

Click **Next** to fill in the request details.

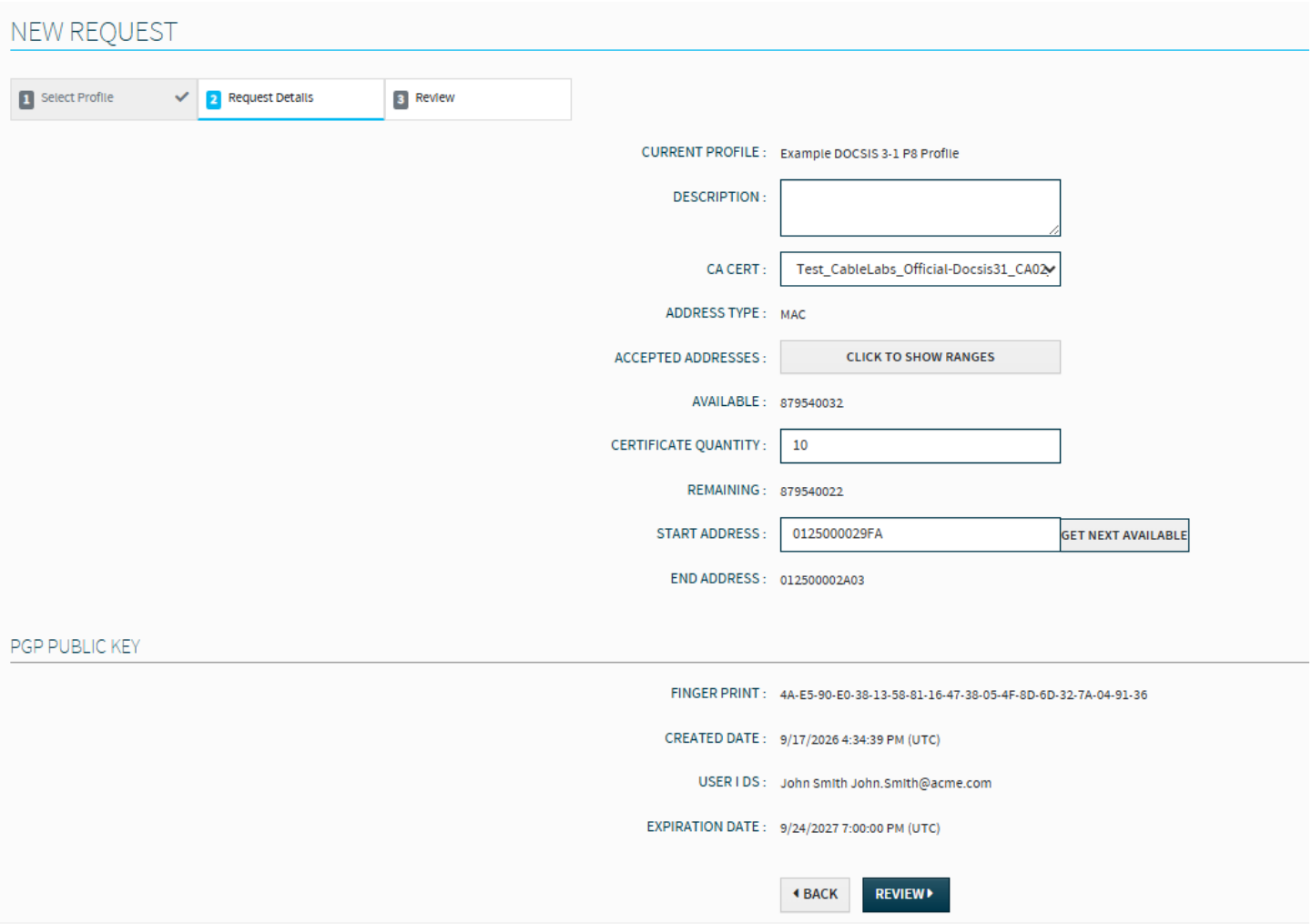

Figure 4 – PKCS#8 Request Details

1. *Description*, this field is an optional description of the request. Enter any desired text.
2. *CA Cert*, this field is prepopulated with the CA cert that matches the selected profile.
3. If the request is for IEEE MAC, select CLICK TO SHOW RANGES link to see what ranges are available. This will show a list of MAC address ranges that have been assigned for use by this profile.

Available is the remaining balance for the account. If it is lower than the requested amount, please contact pkiops@cablelabs.com to place a certificate order.

Certificate Quantity, enter the number of certificates requested. (100,000 is the maximum quantity in one batch).
Start Address is a required field. Specify the MAC address range for this request by entering a chosen *start address* or select the ***Get Next Available*** button to automatically populate this field.

The ***End Address*** will be calculated and displayed automatically. The address must be a 12-digit hex string, e.g., 0000010001B0.

4. *Remaining*, this field shows the account balance after deducting this order's certificate quantity.
5. *PGP Public Key* of the subscriber is displayed at the bottom of the page for confirmation.

Click on the **Review** button to review the request, then click "**NEW ORDER**" to submit the request.

Please visit Appendix A for additional PGP creation and management details.

2.1.2 CERTIFICATE GENERATION WITH USER-GENERATED CERTIFICATE SIGNING REQUEST (CSR) PKCS#10

This request type generates one or more certificates from subscriber-provided Certificate Signing Requests (CSRs).
Begin by selecting a profile. When a profile is selected, a brief description is displayed.



Figure 5 – Select Profile

Select Next to enter the request details and provide the information required to generate the certificate request.

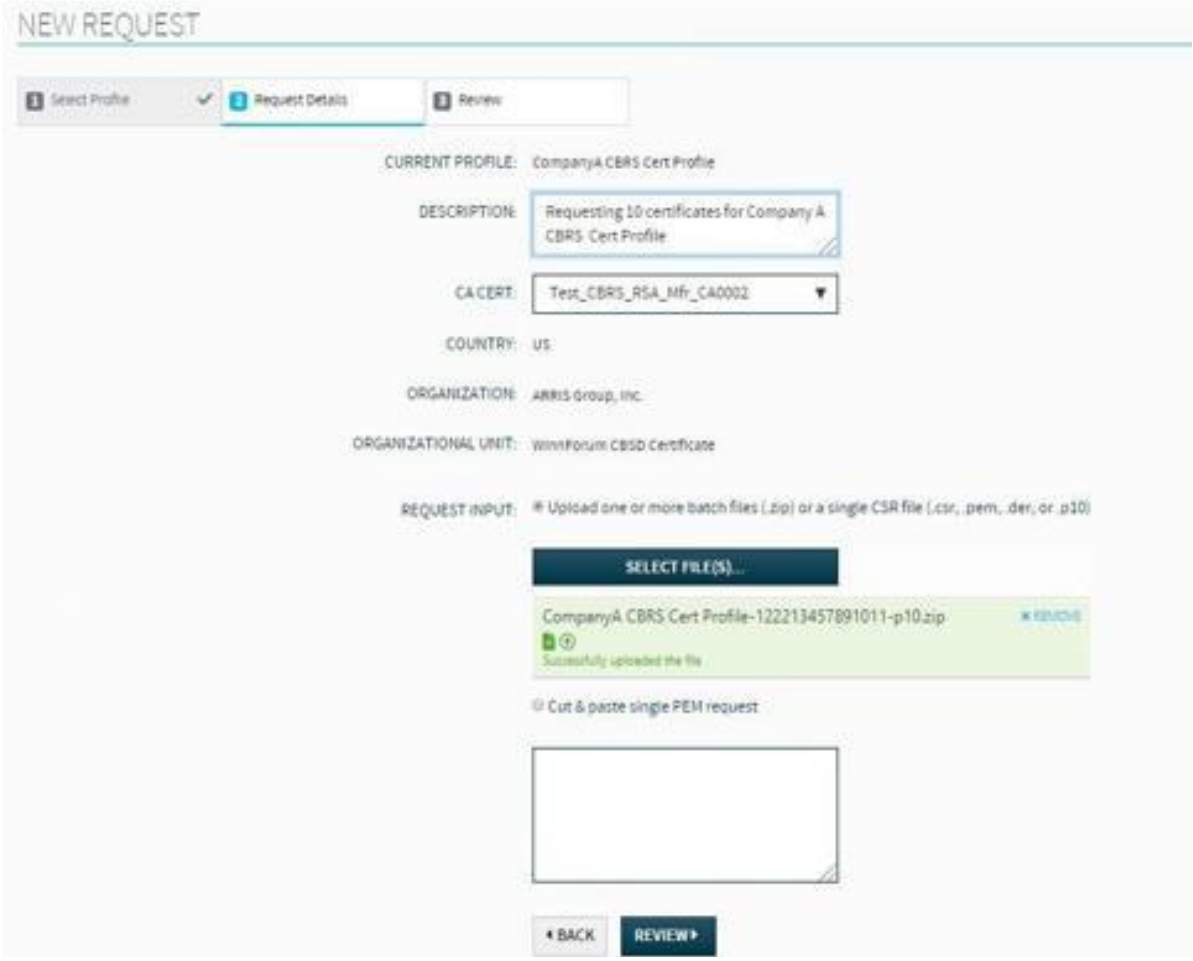

Figure 6 – Request Details

1. Description, this field is an optional description of the request. Enter any desired text.

2. CA Cert, this field is prepopulated with the CA cert that matches the selected profile.

3. If the selected profile has any variables, they will appear in this section. In this case, all the subject fields are pre-populated. Fill in any variable fields that do not already have a value specified.

4. Request Input, you must select the request file. This can be either a zip file with one or more certificate requests or a single certificate request in DER format.

After completing all required fields, select Review to verify the request details. If the information is correct, select NEW ORDER to submit the request.

2.1.3 CERTIFICATE GENERATION WITH AN UPLOAD FILE PKCS#12

This request type generates PKCS#12 files for one or more identifiers (IDs). Each PKCS#12 file contains the certificate and its associated private key, protected with a subscriber-specified password.

First, select a PKCS#12 profile. When selected, a brief description is displayed. Click **Next** to fill in the request details.

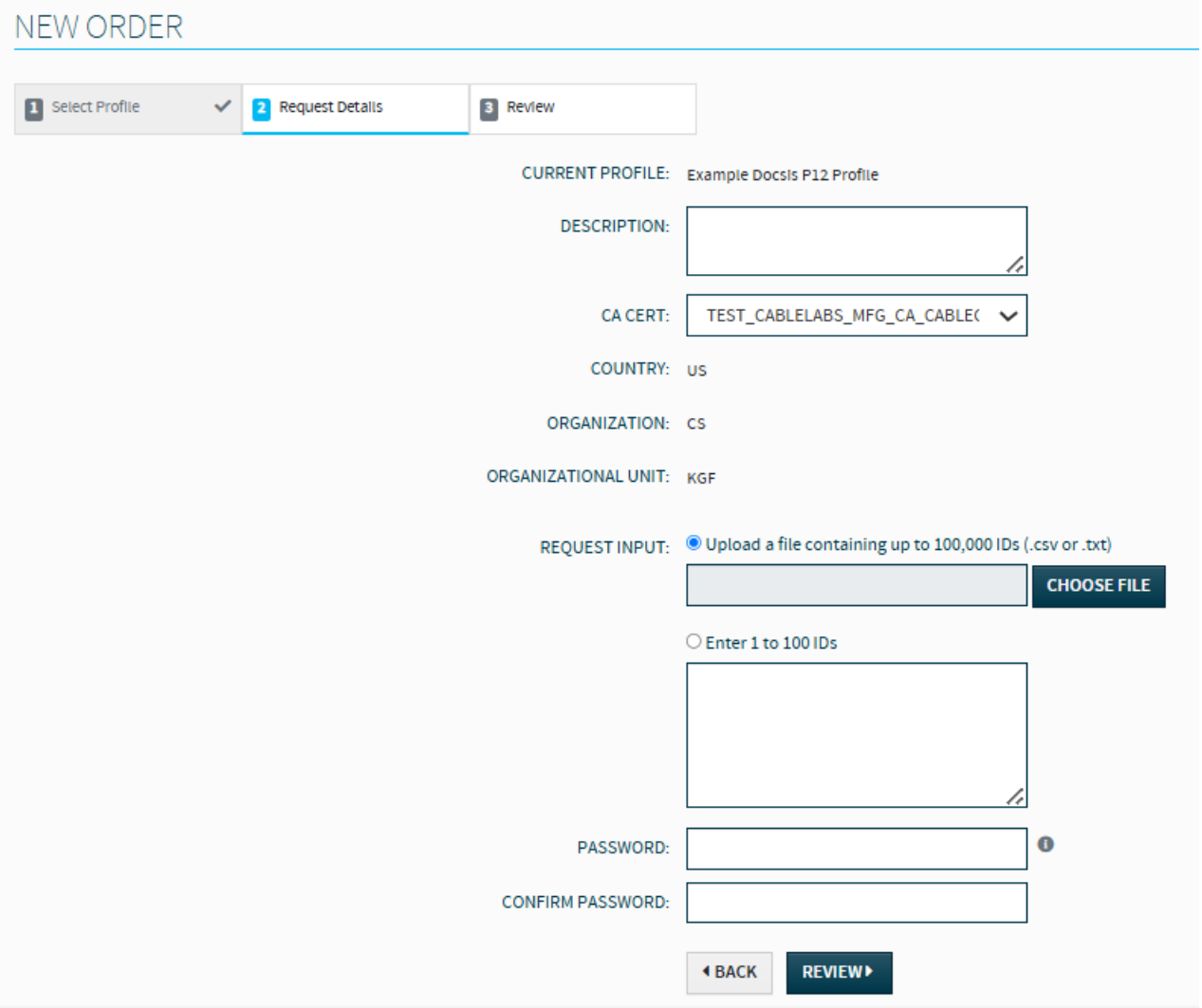

Figure 7 – PKCS#12 Request Details

1. Description, this field is an optional description of the request. Enter any desired text.

2. CA Cert, this field is prepopulated with the CA cert that matches the selected profile.

3. Submit PKCS#12 requests by uploading a CSV or text file containing up to 100,000 ID entries, or by entering up to 100 IDs on the form. The below example shows IDs entered in the form.

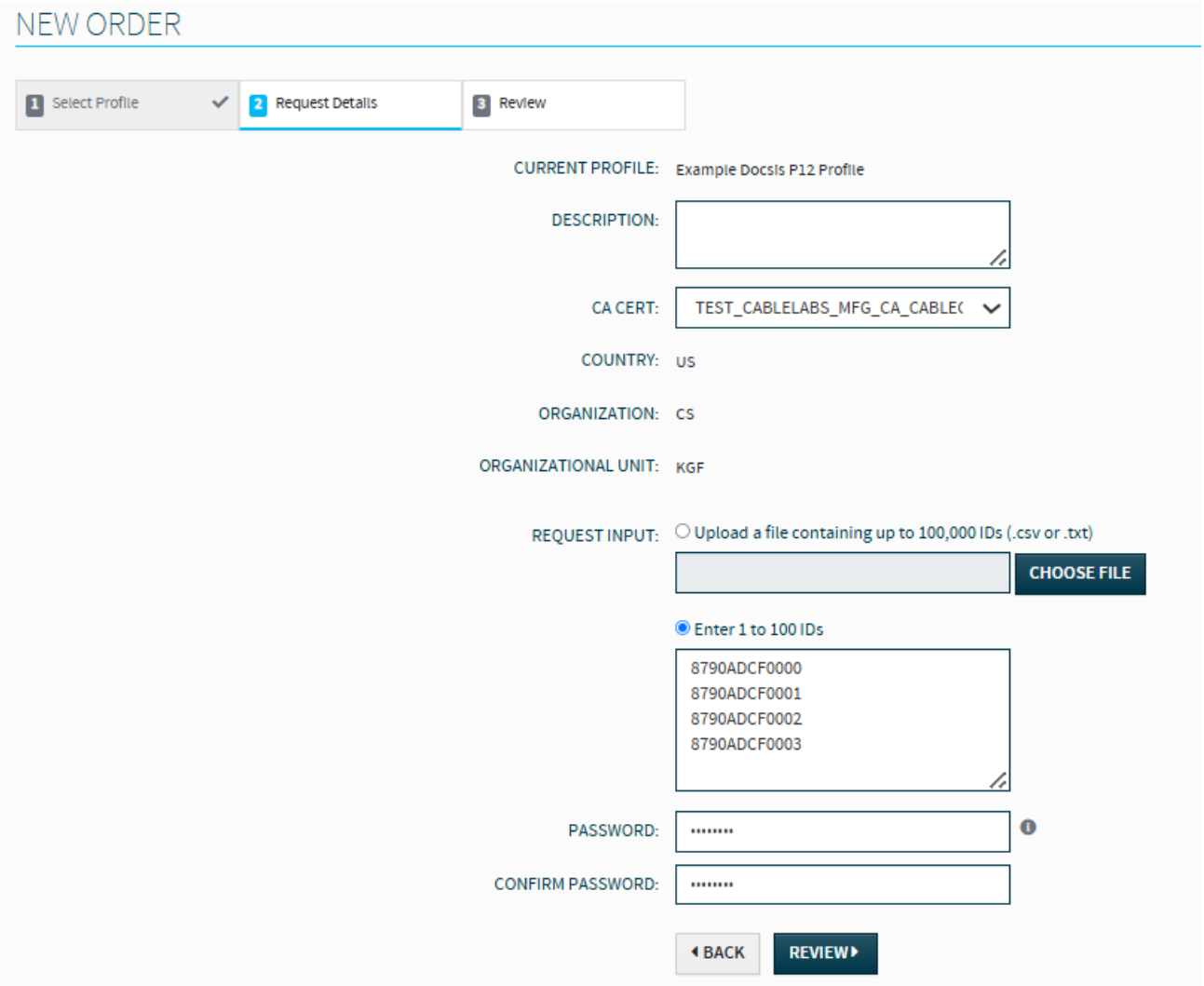

Figure 8 – PKCS#12 Request for MAC

4. Enter a password for private key encryption. The password must contain at least one letter, one digit, and one of these special characters: @, $, !, %, #, ?, or &. No other special characters are permitted. PKCS#12 files will not be generated if ID is invalid according to validation policy. Note that if multiple PKCS#12 files are generated, the same password applies to all the generated PKCS#12 files.

5. Country, Organization and OU are the custom variables for this profile. If the selected profile has any variables, they will appear in this section. In this example, all these fields are already pre-populated values that are displayed for information. Fill in any variable fields that do not already have a value specified.

Click on the Review button to review the request, then click “NEW ORDER” to submit the request.

2.2 ACCESSING CERTIFICATES

PKIWorks sends an email notification when a request has been processed and is ready for download. The current status of each request can also be monitored through the PKIWorks portal.

2.2.1 REQUEST STATUS EXPLANATION

Requests progress through several status states during processing. The following descriptions explain each status and its meaning.

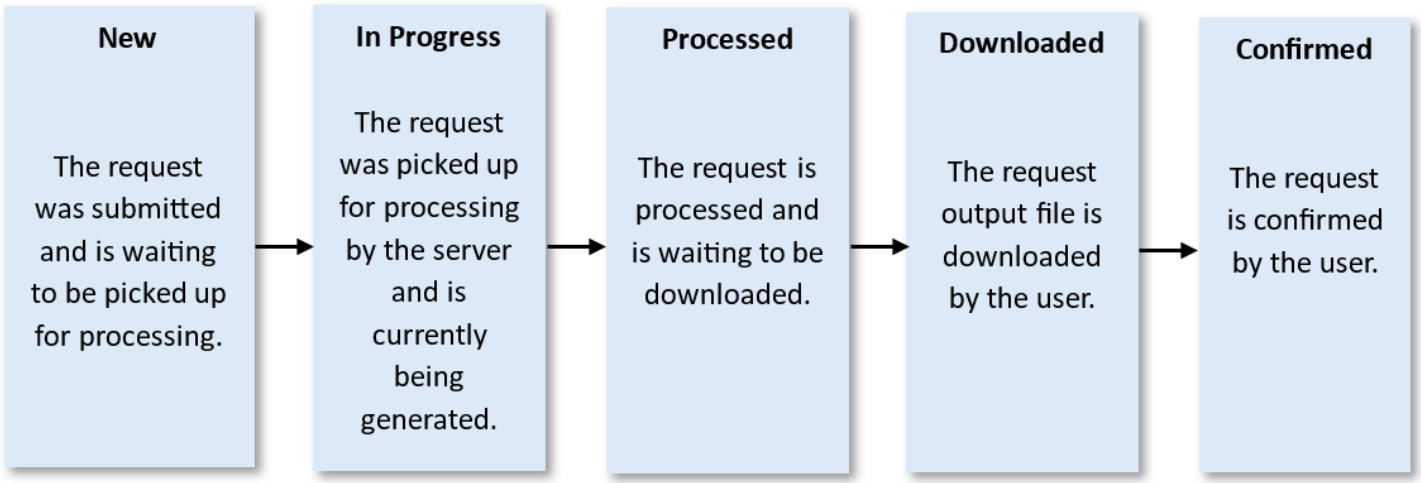

Figure 9 – Request Status Diagram

2.1.2 VIEW REQUESTS AND STATUS

Select the View Requests tab to monitor request progress, review previously submitted requests, view request details, and download available output files.

Processing time varies depending on the size and complexity of the request. Once processing is complete, PKIWorks sends an email notification to the primary account email address, or if configured, to the backup notification email address. You can also monitor the request status through the PKIWorks portal.

REQUEST ID	TYPE	STATUS	ACTUAL/REQUESTED QTY	DATE SUBMITTED (UTC)	ACTIONS
339346144715301	Cert	NEW	0/32	6/3/2025 9:57:00 PM	
339346134854901	Cert	PROCESSED	25/25	6/3/2025 9:56:00 PM	DOWNLOAD
3393461179238	Cert & Private Key	IN PROGRESS	0/10000	6/3/2025 9:53:00 PM	
3393461080898	P12	PROCESSED	11/11	6/3/2025 9:51:00 PM	DOWNLOAD
3393460681720	P12	DOWNLOADED	4/4	6/3/2025 9:47:00 PM	DOWNLOAD CONFIRM
3393449347713	CRL	PROCESSED	1/1	6/3/2025 6:36:00 PM	
3393448890798	CRL	PROCESSED	1/1	6/3/2025 6:28:00 PM	
339283645446801	Cert	CONFIRMED	5/5	5/27/2025 4:21:00 PM	
3392256727670	Cert & Private Key	CONFIRMED	10/10	5/20/2025 11:19:00 PM	
3392256297543	Cert & Private Key	DOWNLOADED	0/10 ⚠	5/20/2025 11:12:00 PM	DOWNLOAD CONFIRM

Figure 10 – View Requests

ACTUAL/REQUESTED QTY indicates the number of certificates successfully generated compared to the number of certificates requested. If a request ZIP file contains invalid CSRs, certificate generation is skipped for those CSRs, while certificates are generated for all valid CSRs included in the request.

REQUEST ID	TYPE	STATUS	ACTUAL/REQUESTED QTY	DATE SUBMITTED (UTC)	ACTIONS
324459483591501	Cert	DOWNLOADED	0/58 ⚠	9/14/2020 10:07:00 PM	DOWNLOAD CONFIRM
324424456013401	Cert	PROCESSED	10/10	9/10/2020 8:49:00 PM	DOWNLOAD
324424241692601	Cert	CONFIRMED	0/15 ⚠	9/10/2020 8:14:00 PM	
323577967609001	Cert	CLOSED	10/10	6/4/2020 9:28:00 PM	
3235011963502	Cert & Private Key	CLOSED	20/20	5/27/2020 12:13:00 AM	

Figure 11 – Actual/Requested Quantity Display

2.1.3 DOWNLOAD OUTPUT FILE

Once a request has been processed and an output file is available, a Download icon is displayed next to the request. Select the Download icon to begin downloading the output file.
The browser prompts the subscriber to save the file. Store the downloaded file in a secure location.

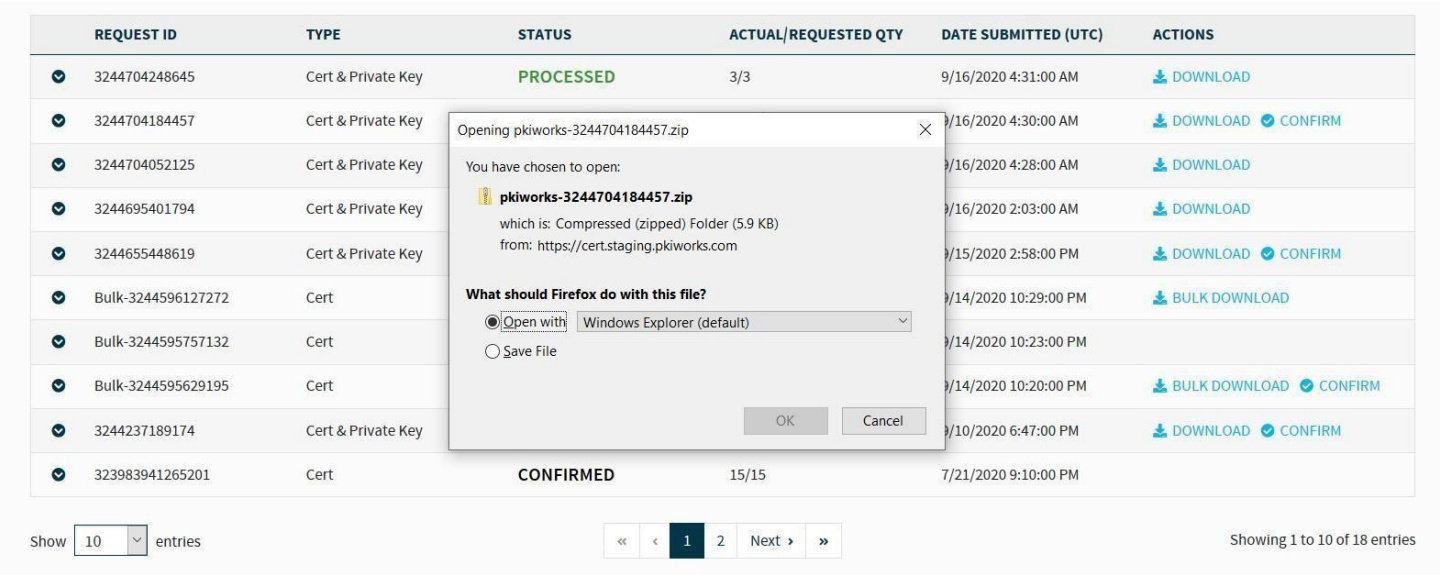

Figure 12 – Download the Output File

If one or more certificates are not generated because of invalid CSRs in the request ZIP file, an error log file is included in the downloaded output package. The error log provides details about each failed CSR and the reason it could not be generated.

2.1.4 CONFIRM FILE DOWNLOAD

After an output file has been downloaded, a CONFIRM action is displayed in the ACTIONS column. Selecting CONFIRM acknowledges that the downloaded file has been received and verified and permanently removes the output file from the system. If the CONFIRM action is not selected, the output file is automatically deleted after the number of retention days configured for the profile.

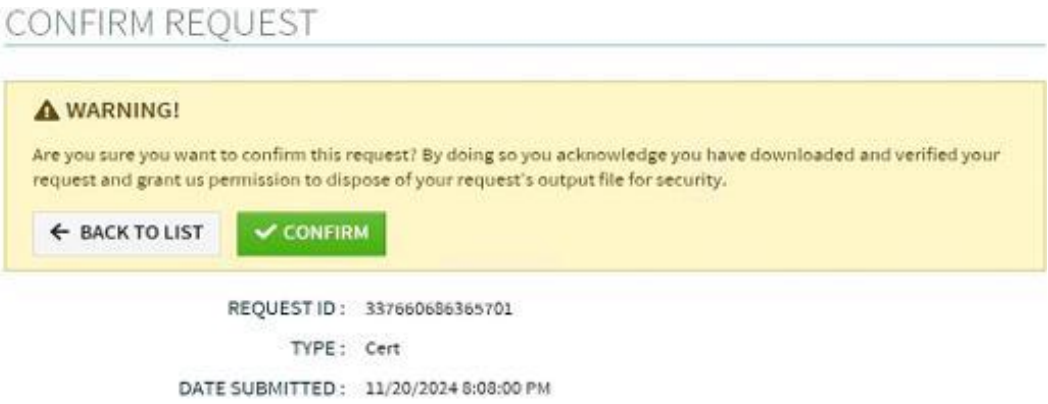

Figure 13 – Confirm the Request

Once the request is confirmed, its status changes to CLOSED, as shown in Figure 11 above – Actual/Requested Quantity Display. After the status changes to CLOSED, the DOWNLOAD action is no longer available, and the output file can no longer be downloaded.

2.1.5 PKCS#8 OUTPUT FILE USING PGP KEY DECRYPTION

Download the output package and extract the ZIP file using the operating system's built-in file extraction utility. After extraction, the package contains a single file, innerPackage.pgp, as shown below.

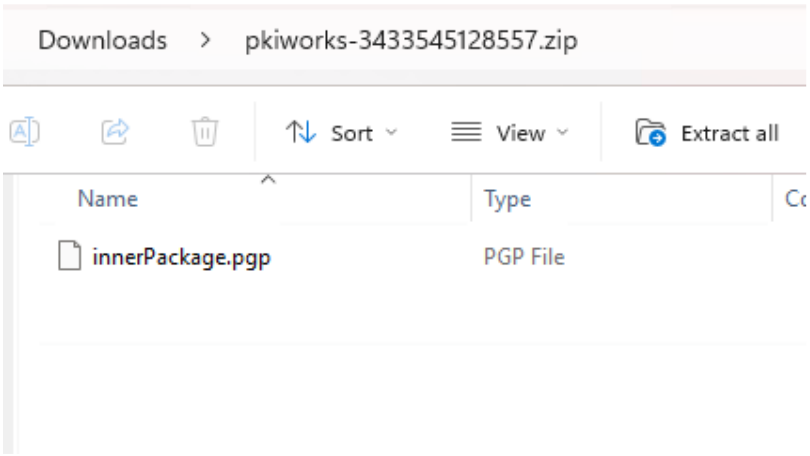

Figure 14 – Zip file contains PGP

Use PGP/GPG software with the subscriber's PGP private key and passphrase to decrypt innerPackage.pgp. After successful decryption, the output package contains the generated keys, certificates, and an order log. If an error occurred during package generation, the package also contains an error log.

3 DOWNLOADING ROOT AND INTERMEDIATE CERTIFICATES

On the PKIWorks portal, navigate to RESOURCES | CA & CRL. A list of available CA certificate chains and Certificate Revocation Lists (CRLs) is displayed.

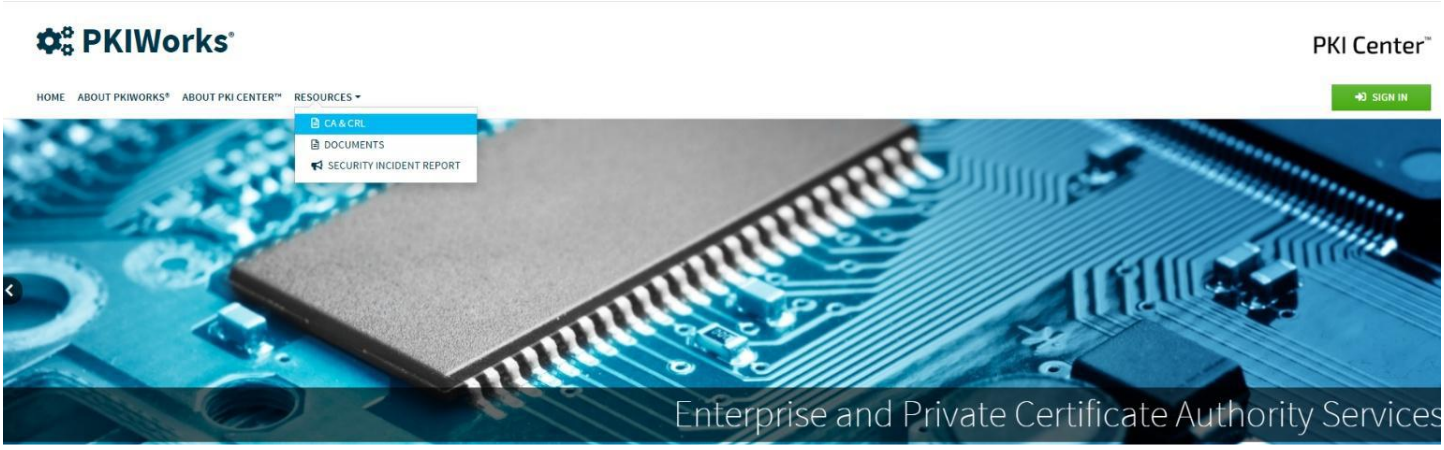

Figure 15 – View CA/CRL

4 REVOKING CERTIFICATES

This request type is used to revoke active certificates. If revocation is enabled for the selected company account, authorized users can submit certificate revocation requests.

NOTE: Revoking certificates does NOT return certificates to your balance. Once certificates are issued and downloaded, they are considered used and cannot be returned to your balance. Certificate revocation should only be used if a certificate has been compromised.

4.1 NEW REVOCATION REQUEST

1.) To create a new revocation request, navigate to New Request and select + Certificate Revocation Request.

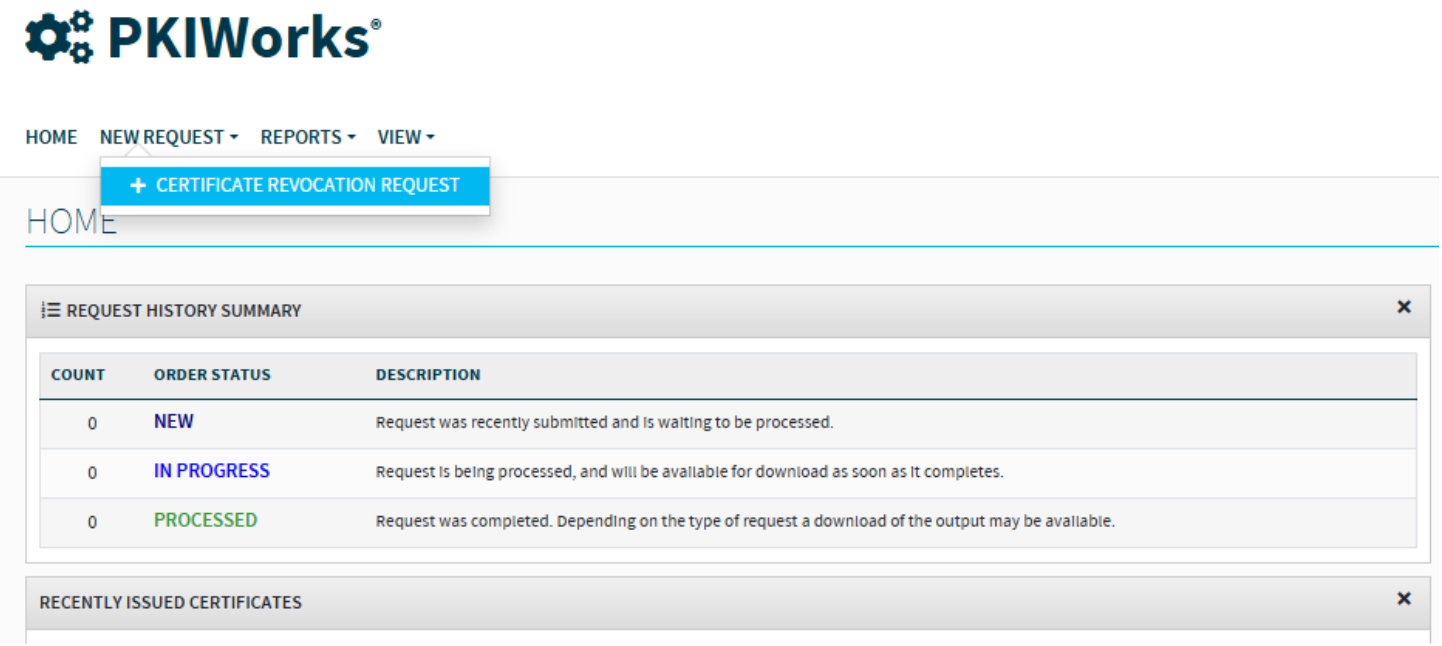

Figure 16 – Certificate Revocation Request Menu

2.) New Revocation Request page is displayed. Revocation Reason is set to 'Unspecified' by default.

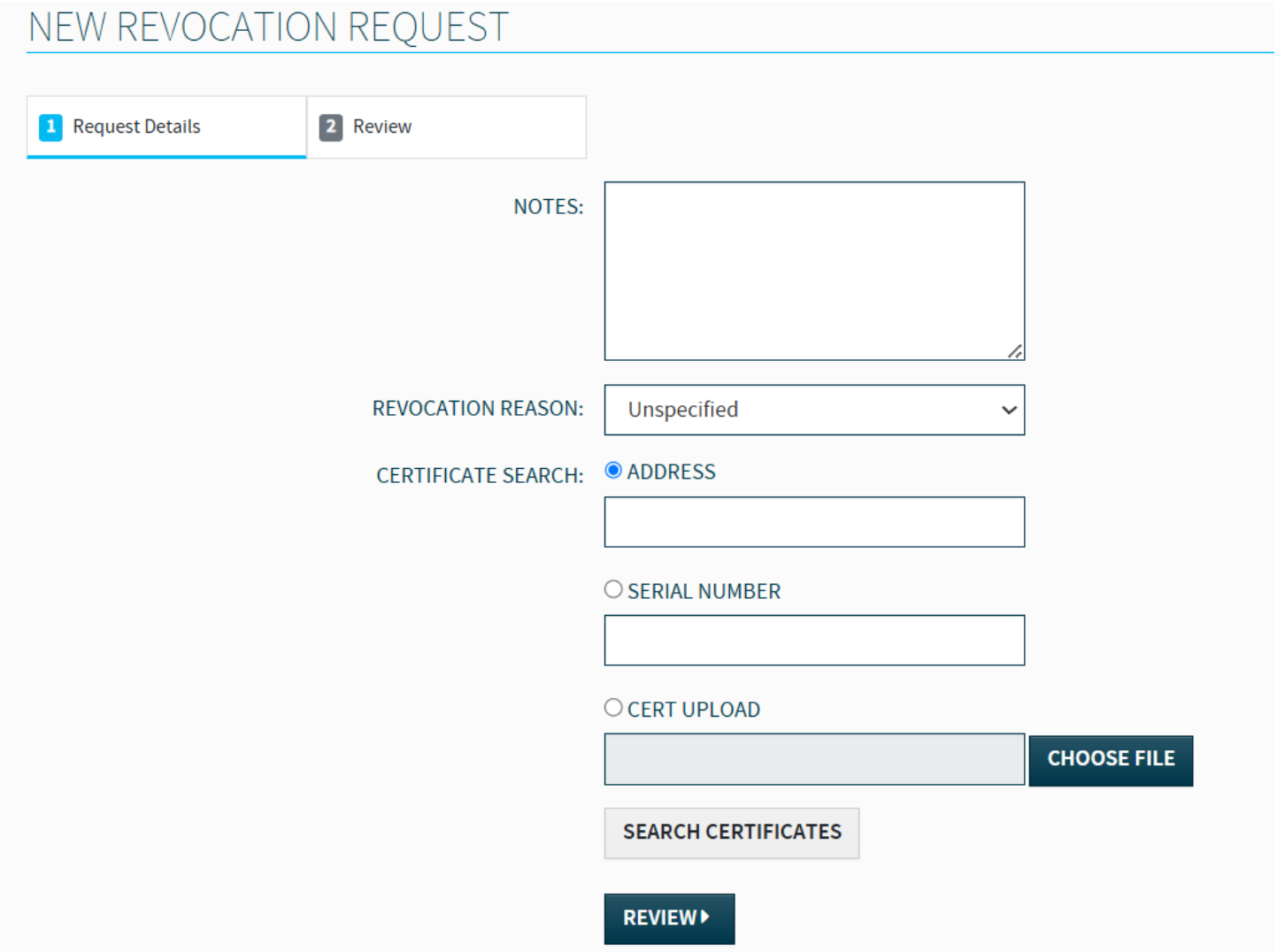

Figure 17 – Certificate Revocation Request

3.) You can change the Revocation Reason to other available options.
A confirmation message appears when you select a Revocation Reason other than Unspecified. The subscriber can confirm or cancel the change.

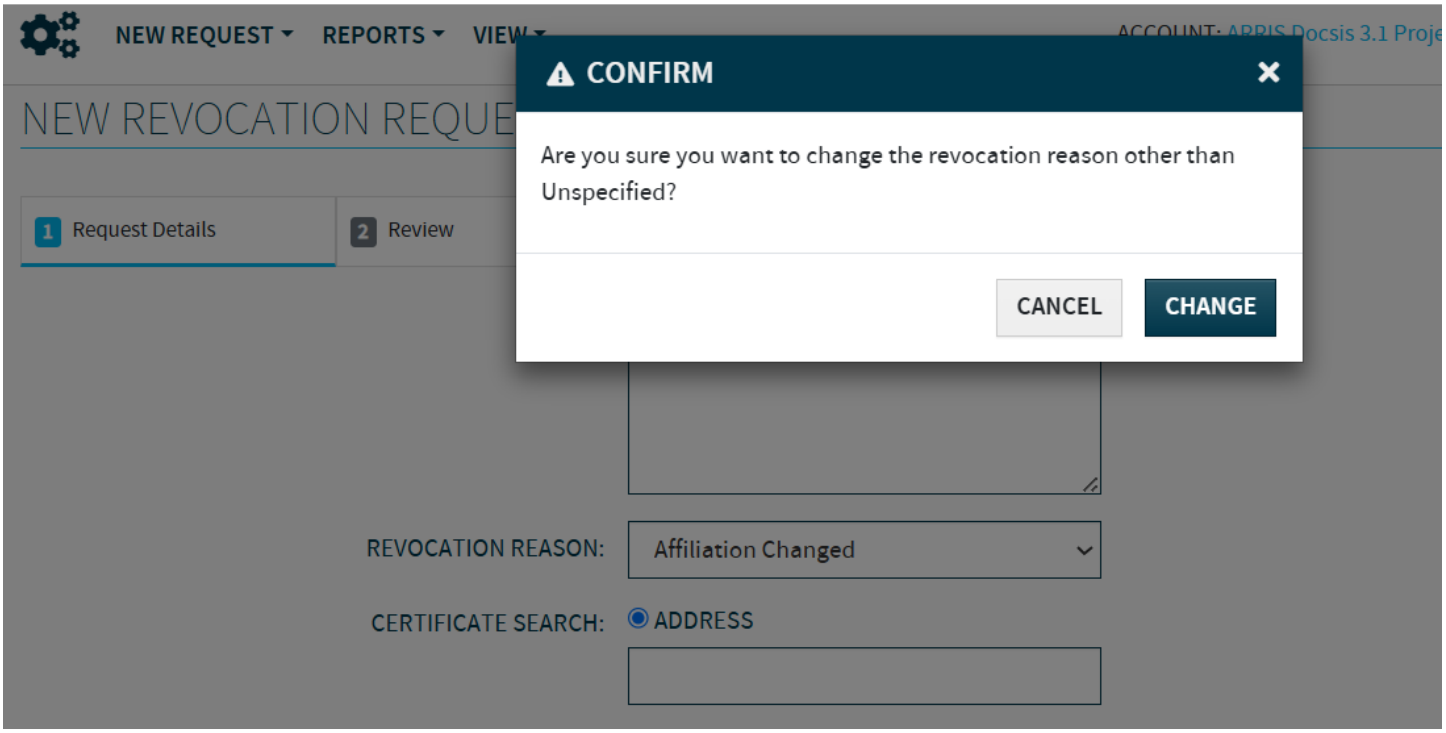

Figure 18 – Revocation Reason Change Confirmation

4.) Provide certificate Address or Serial Number, or by uploading the certificate file to search for a certificate to revoke. In the below scenario, we are using certificate Serial Number to perform the search.
5.) Click on the SEARCH CERTIFICATES button.

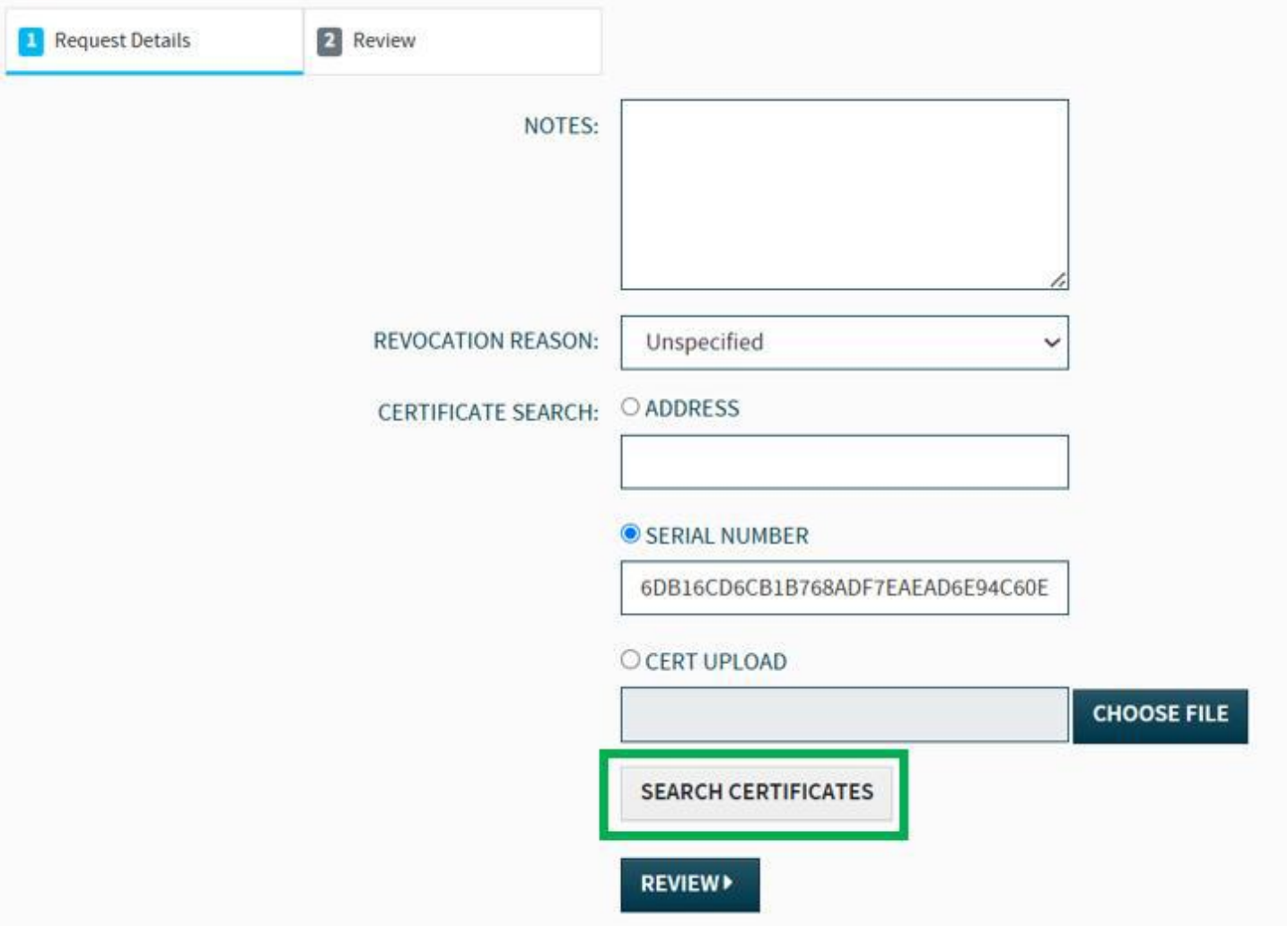

Figure 19 – Search Certificate using Serial Number

6.) The certificate information is returned. Click on SELECT CERTIFICATE.

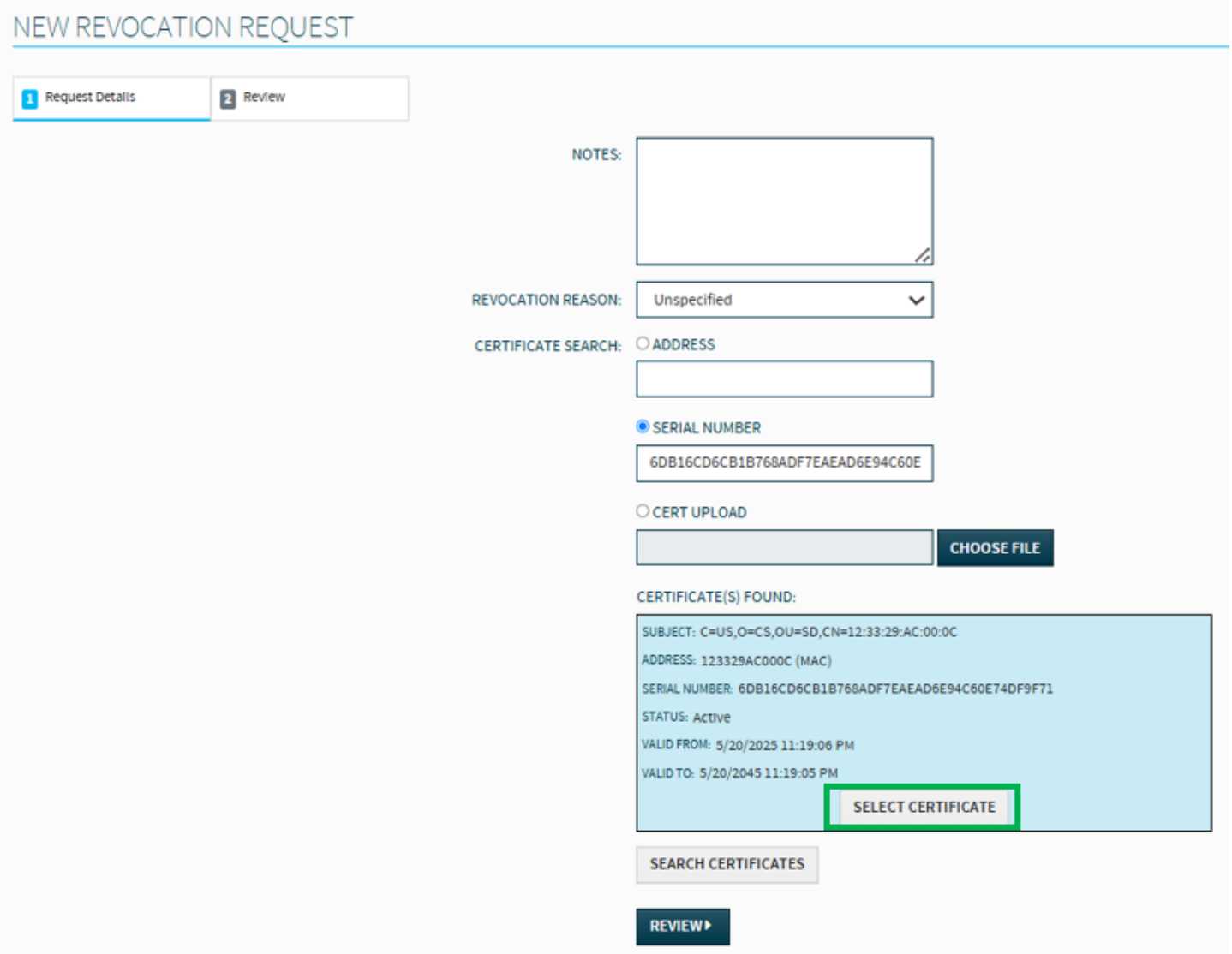

Figure 20 – Select Certificate for Revoke

7.) Click on the Review button to review the request,
8.) Click CREATE REQUEST to submit the request.

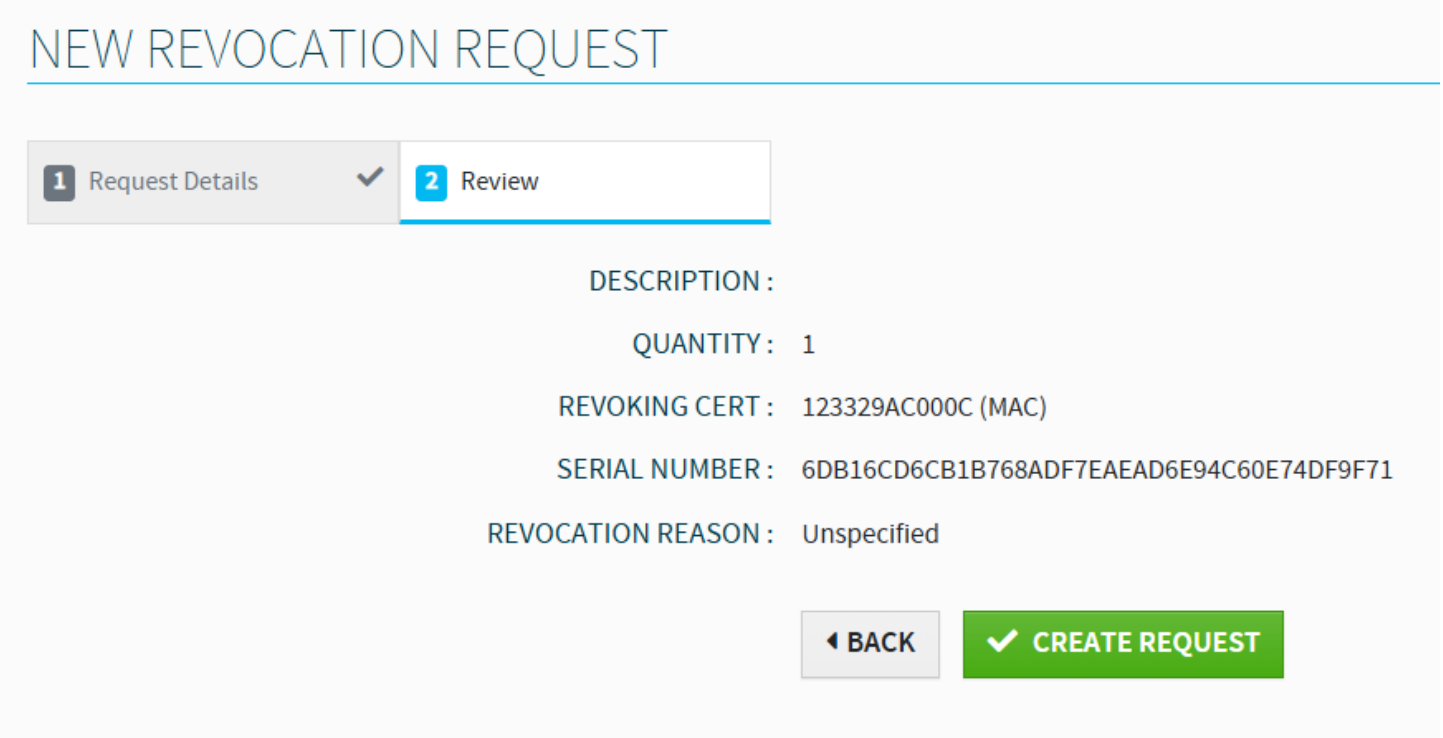

Figure 21 – Create Revocation Request Final Submission

5 APPENDIX A – PGP PUBLIC KEY MANAGEMENT

If the selected account is configured to encrypt PKCS#8 output packages using a PGP public key, and you do not already have a PGP key pair, you will be required to generate one. The PGP public key must be configured for your user account before submitting a new order. You can use any standard PGP package (such as GPG) to generate a key pair that meets the minimum requirements of RSA 2048-bit key strength and SHA-256 hashing, or equivalent cryptographic strength. You can configure and manage your PGP public key through the portal.

5.1 VIEW PGP PUBLIC KEY

To view the current PGP public key, navigate to PGP Public Key and select + View PGP Public Key

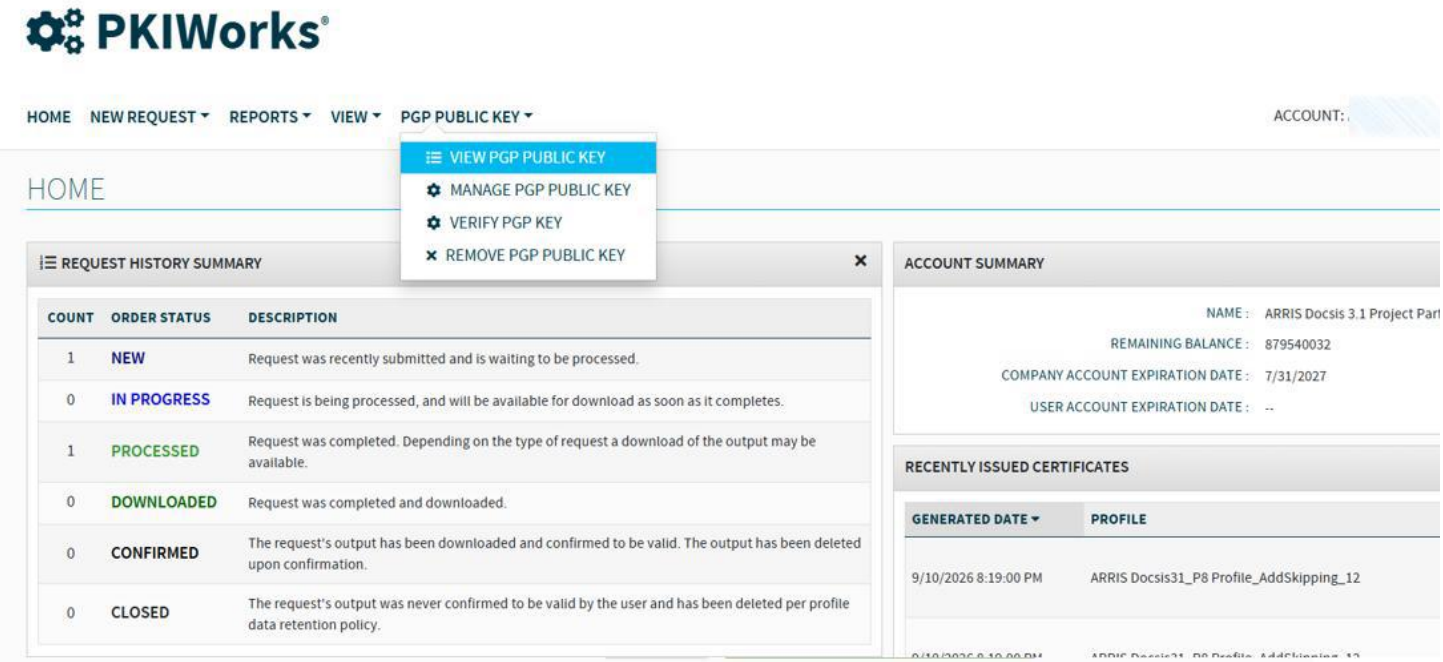

Figure 22 – View PGP Public Key Menu

If a PGP public key is already configured, the View PGP Public Key page will display the key details, as shown below.

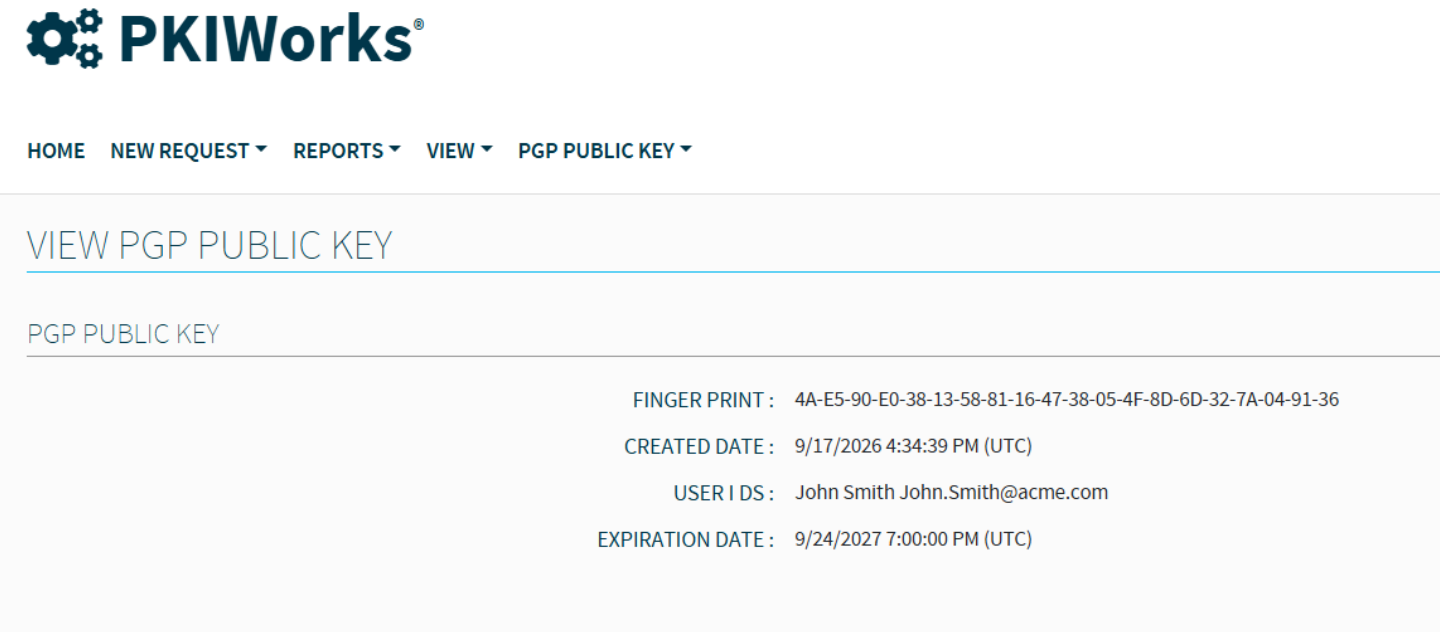

Figure 23 – View PGP Public Key Details

5.2 MANAGE PGP PUBLIC KEY

To configure a new PGP public key or replace/renew a PGP public key, navigate to PGP Public Key +Manage PGP Public Key.

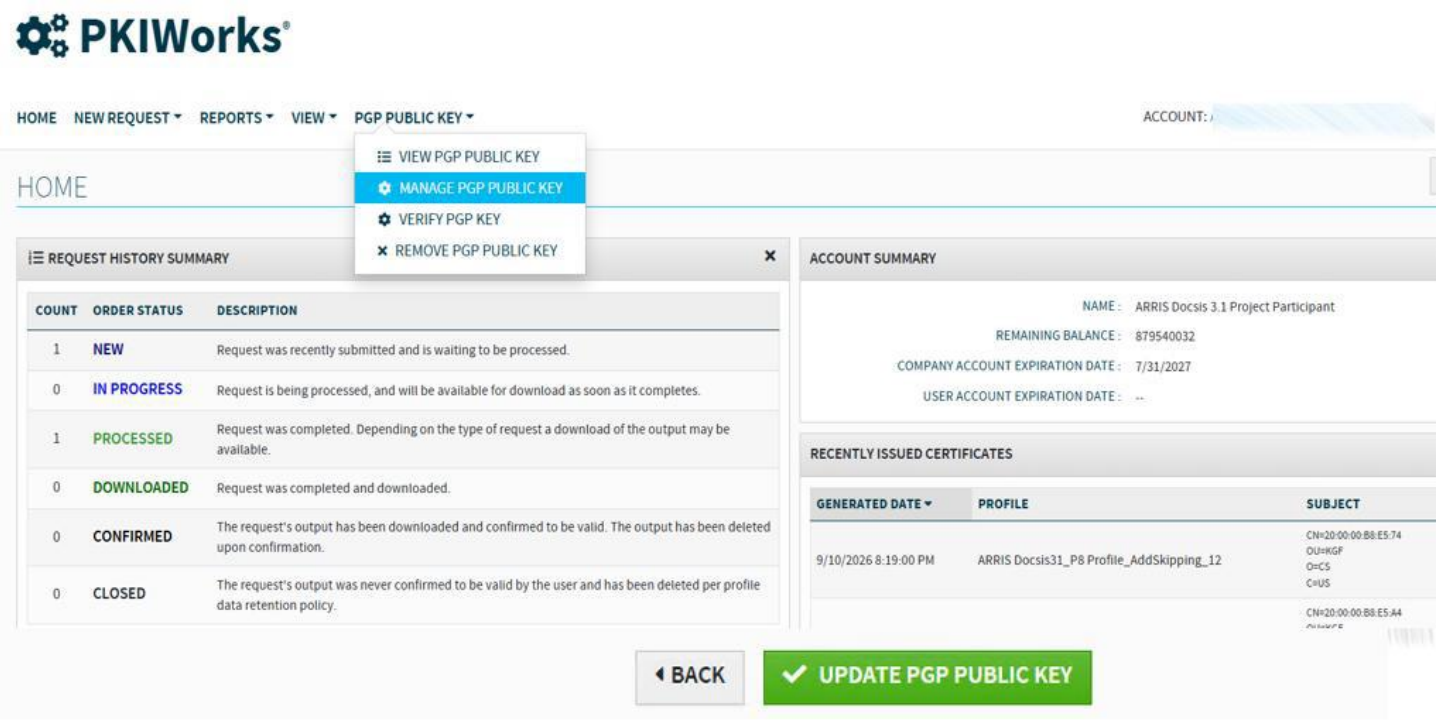

Figure 24 – Manage PGP Public Key Menu

Replacing or renewing a PGP public key involves multiple steps, as shown below.

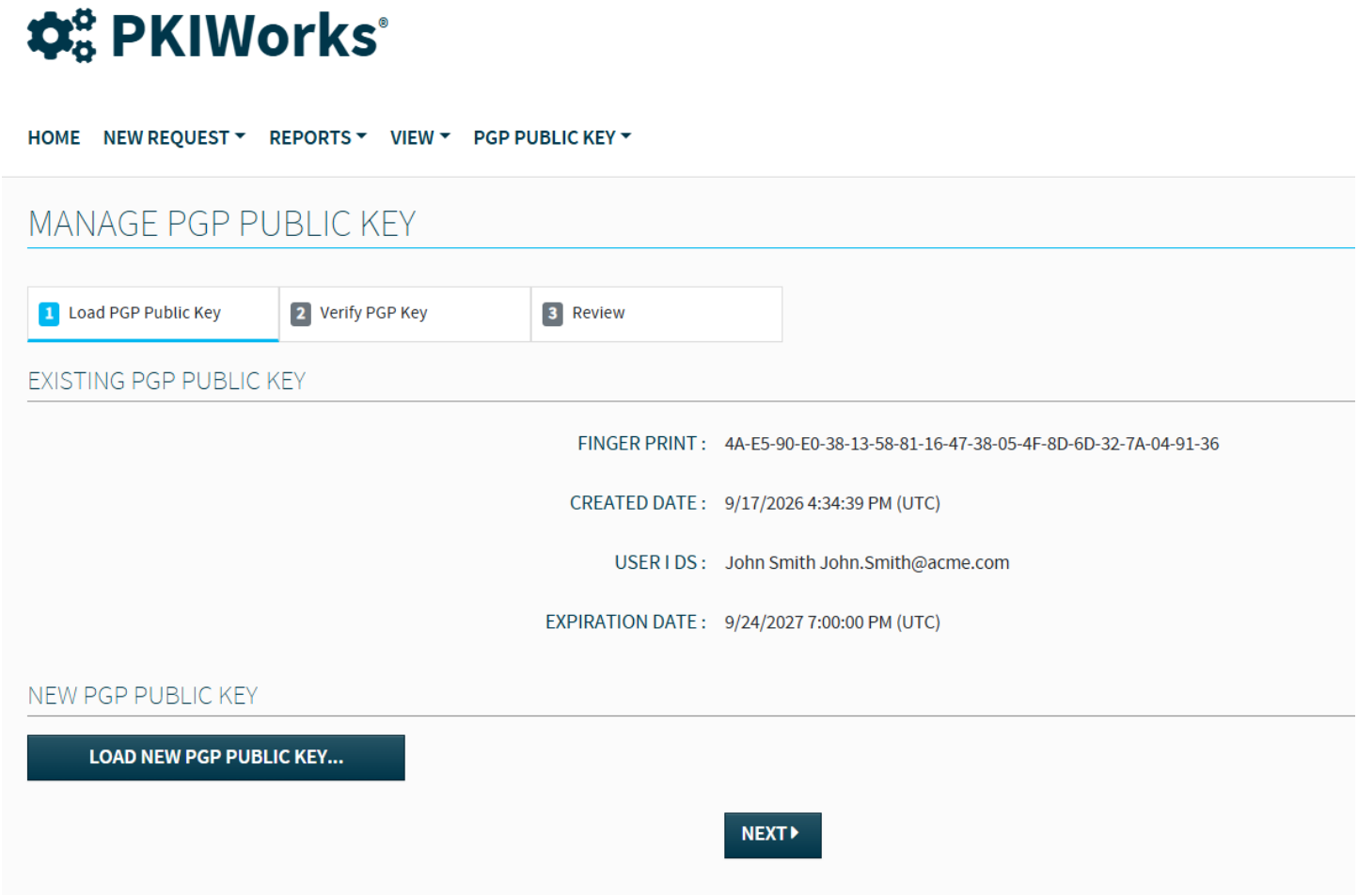

Figure 25 – Manage PGP Public Key Details

Step 1, click LOAD NEW PGP PUBLIC KEY to open a file browser and select the new PGP public key file.

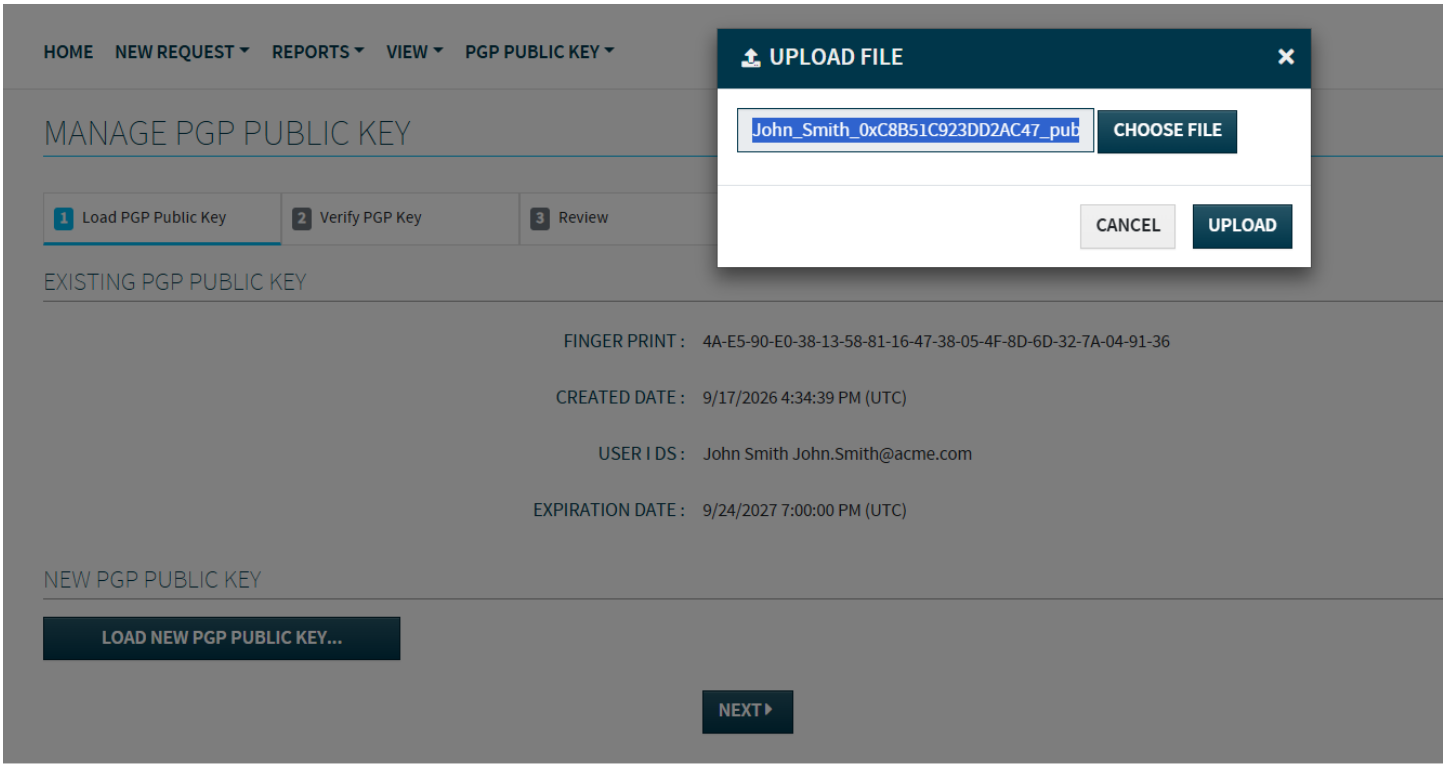

Figure 26 – Browse new PGP Public Key

The new PGP public key details are displayed for verification. Confirm that the information is correct, then click NEXT.

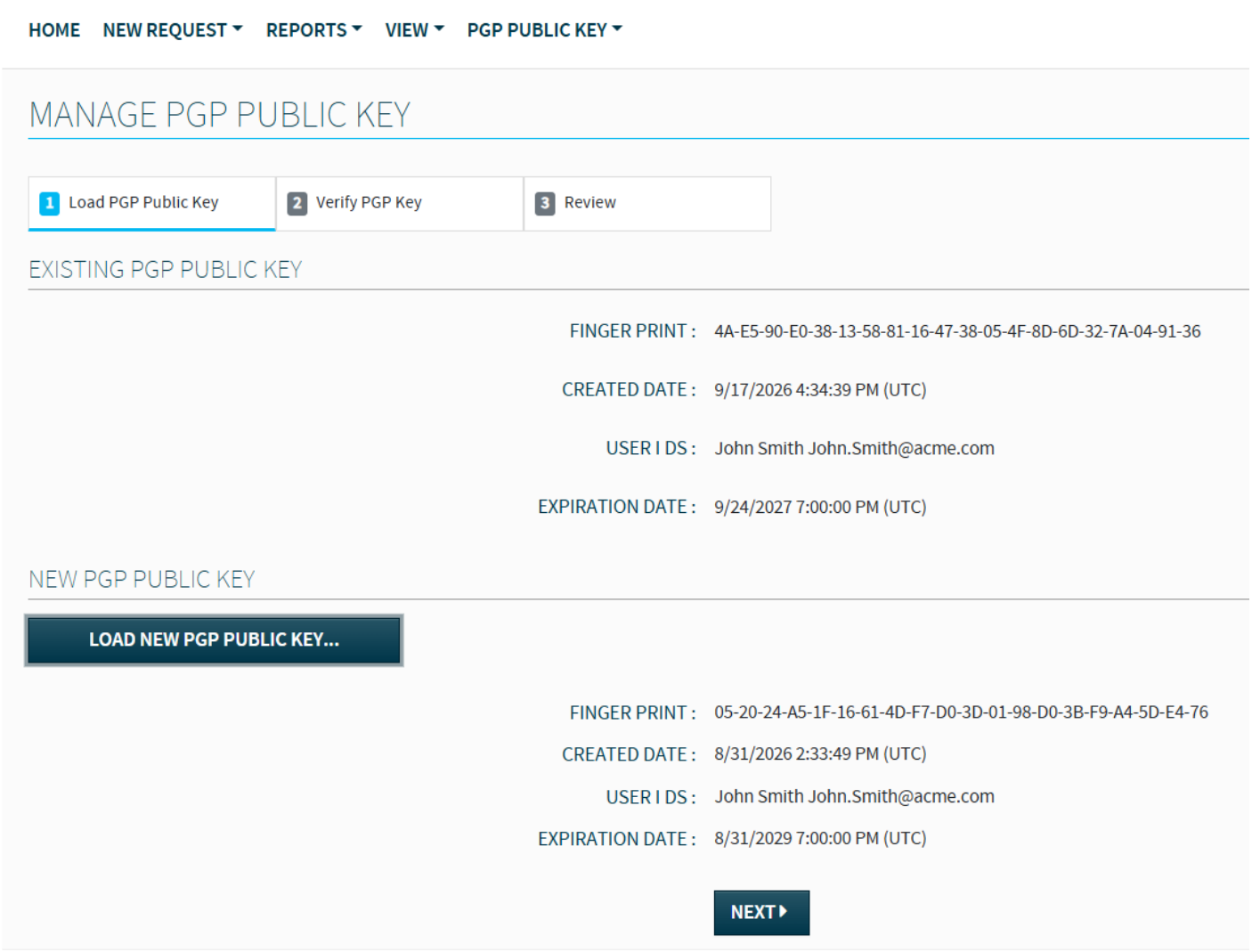

Figure 27 – New PGP Public Key Display

Step 2, verify the uploaded PGP public key. Click DOWNLOAD ENCRYPTED TEST FILE to download the test file, then follow the PGP Key Pair Verification procedure displayed at the top of the page to decrypt and verify the file.

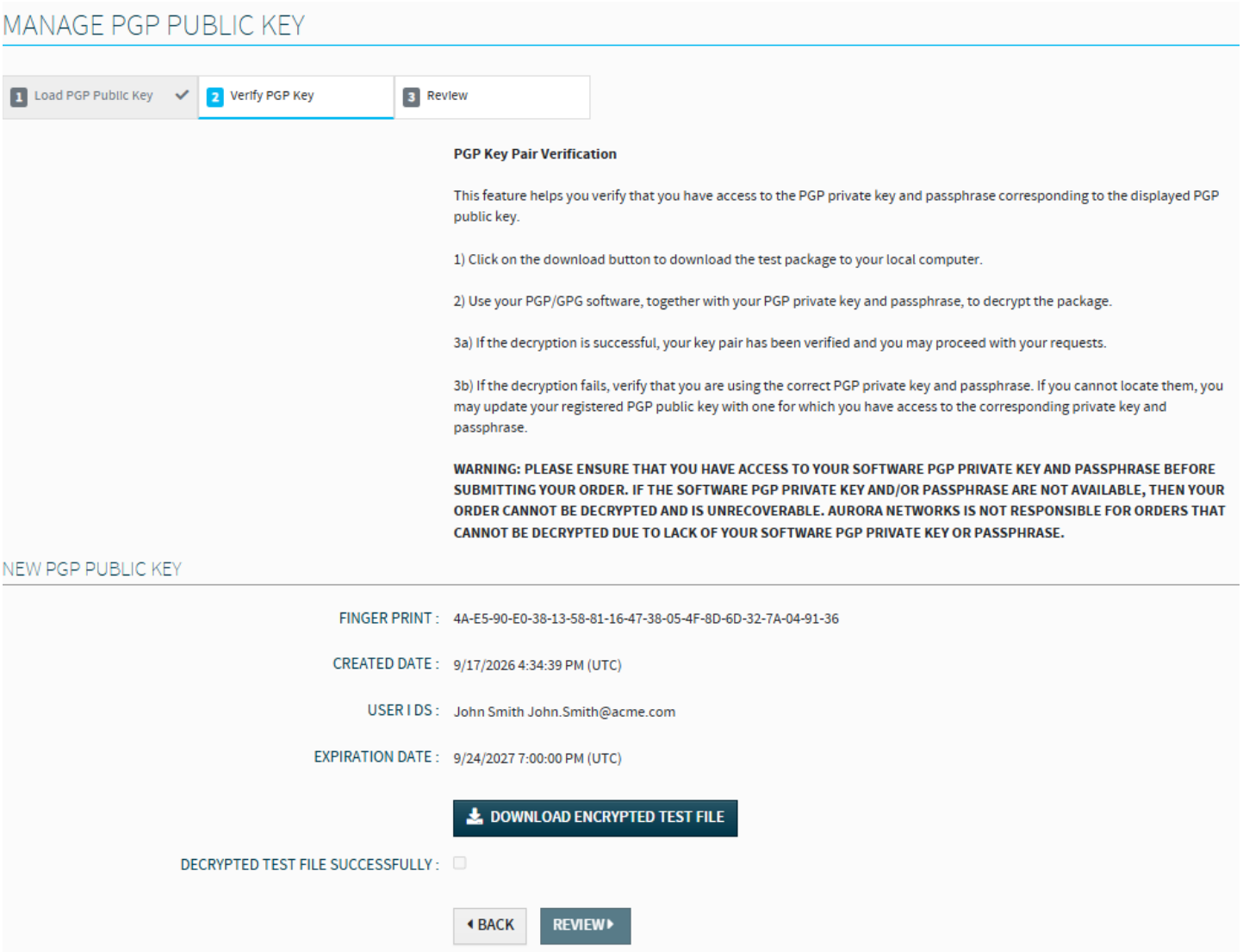

Figure 28 – Second Step to Verify Key

Once the file has been successfully decrypted, select DECRYPTED TEST FILE SUCCESSFULLY and click REVIEW to proceed to the final step.

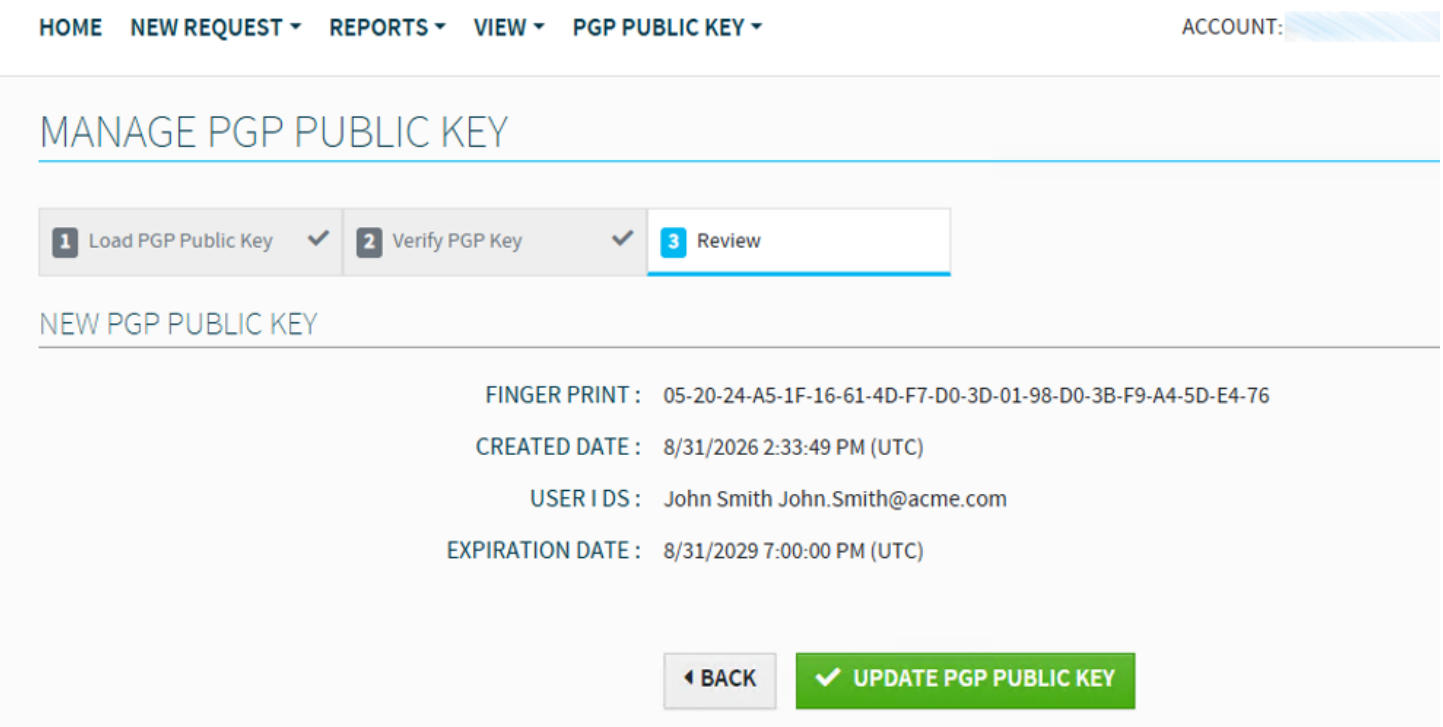

Figure 29 – Final Step to Review

Click UPDATE PGP PUBLIC KEY to complete the PGP public key update process.

5.3 VERIFY PGP KEY

To verify the PGP key at any time, navigate to PGP Public Key and select + VERIFY PGP KEY.

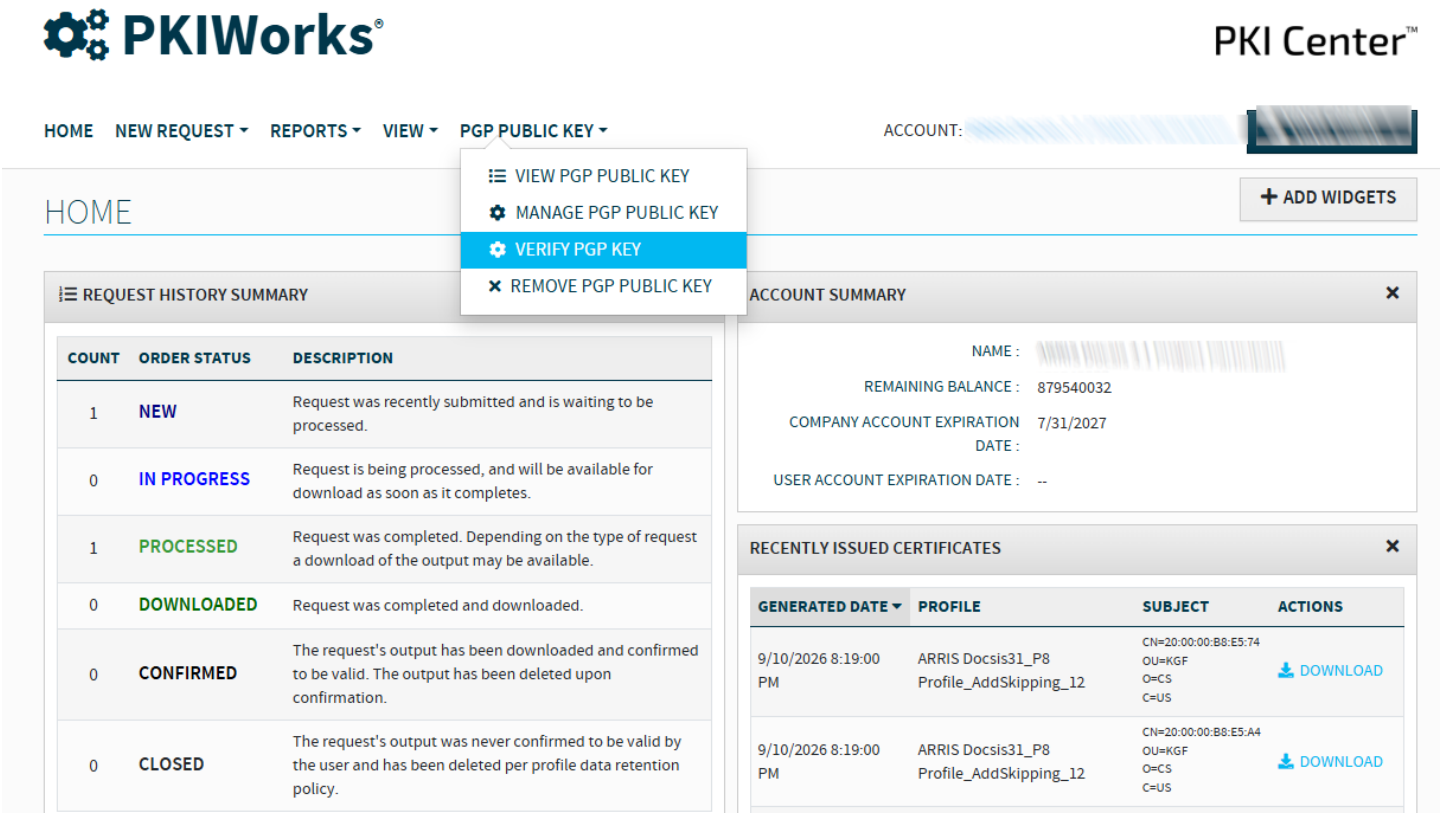

Figure 30 – Verify PGP Key Menu

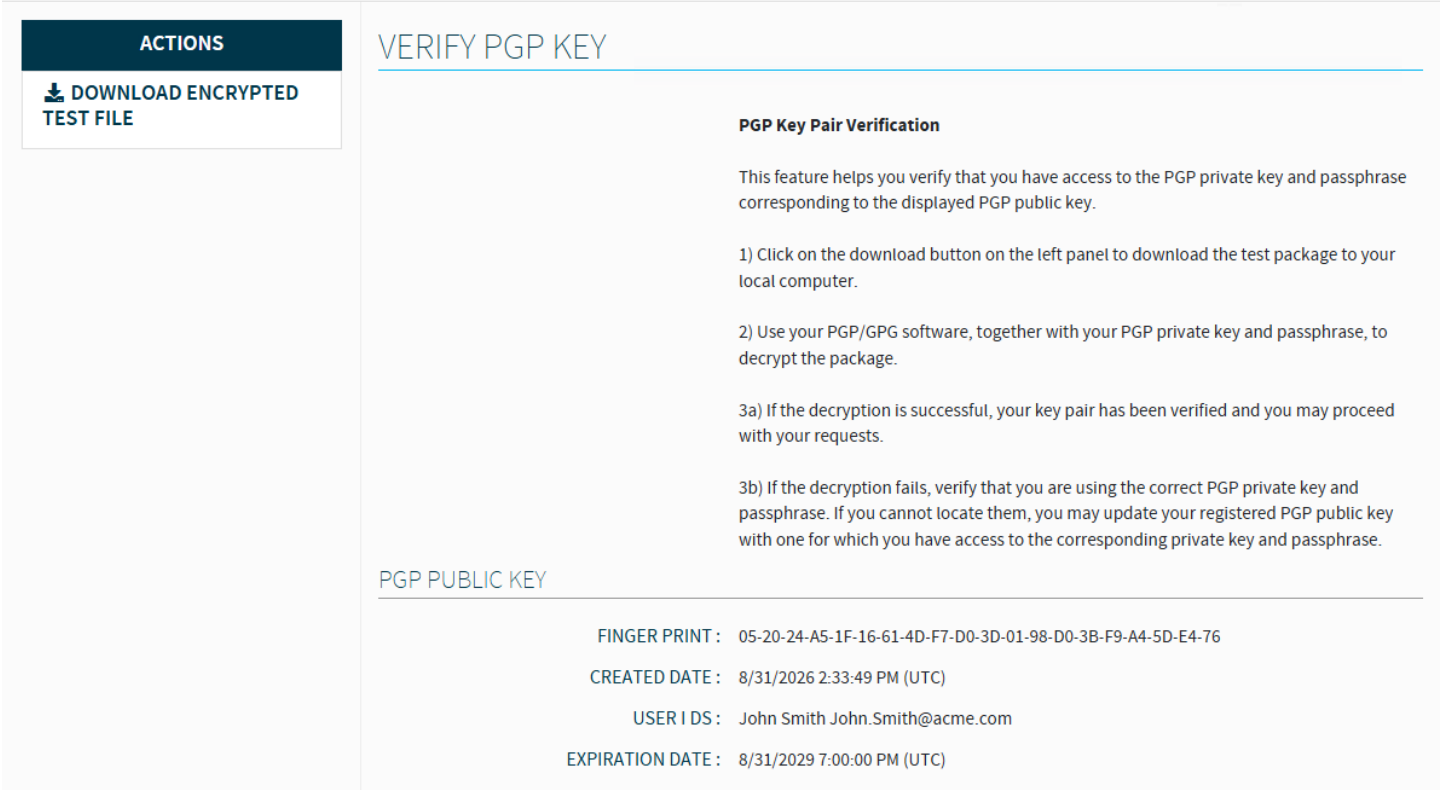

Figure 31 – Verify PGP Key Details

Click DOWNLOAD ENCRYPTED TEST FILE action on the upper left corner to download the test file, then follow the PGP Key Pair Verification procedure displayed to decrypt and verify the file.

5.4 REMOVE PGP PUBLIC KEY

To remove the currently configured PGP public key, navigate to PGP Public Key and select + REMOVE PGPPUBLIC KEY.

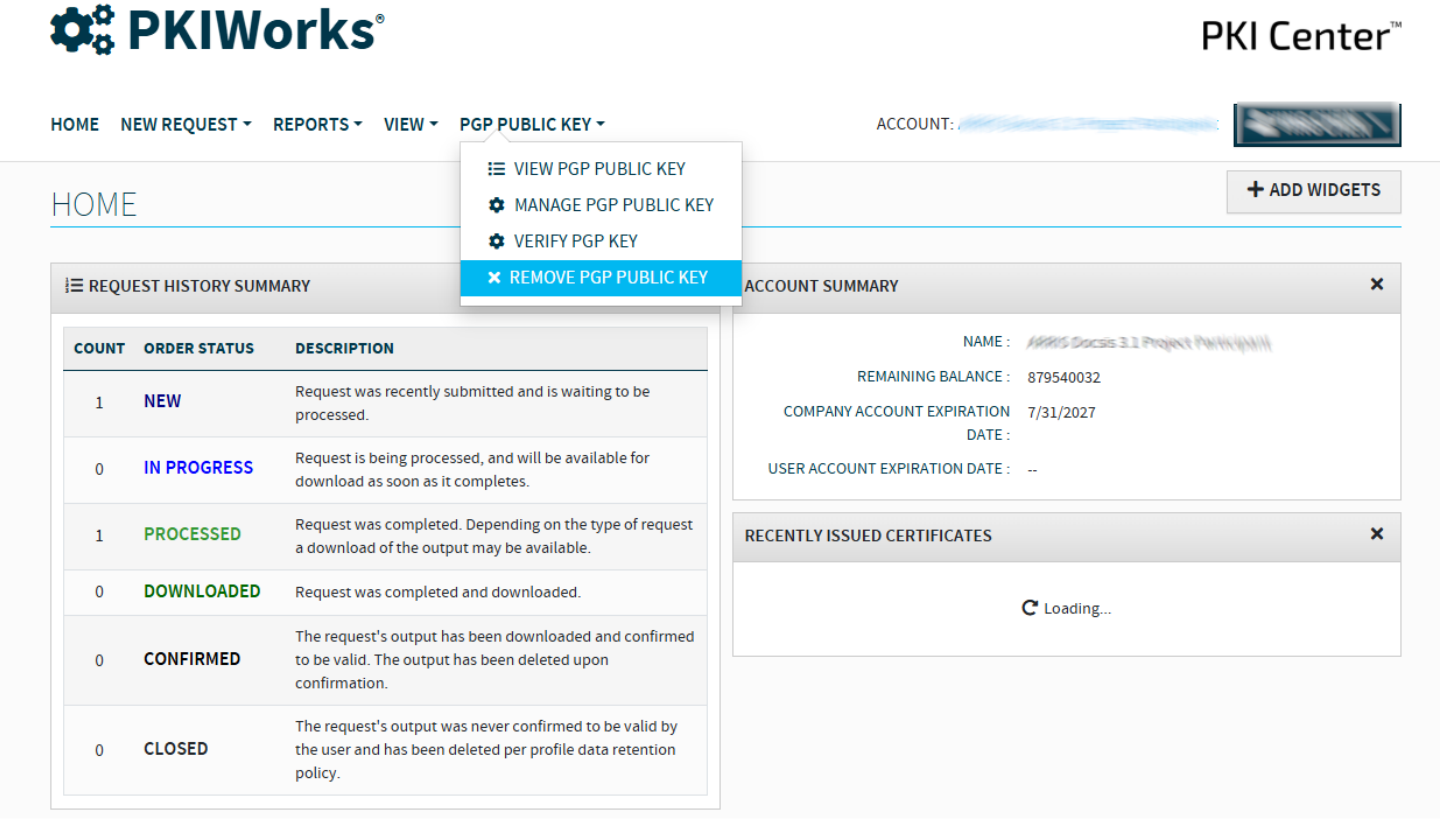

Figure 32 – Remove PGP Public Key Menu

Existing PGP public key is displayed for removal. Click REMOVE in the upper-left corner of the page to remove the currently configured PGP public key.



Figure 33 – Remove PGP Public Key

A warning dialog is displayed to confirm the action. Click **REMOVE** in the confirmation dialog to remove the PGP public key.

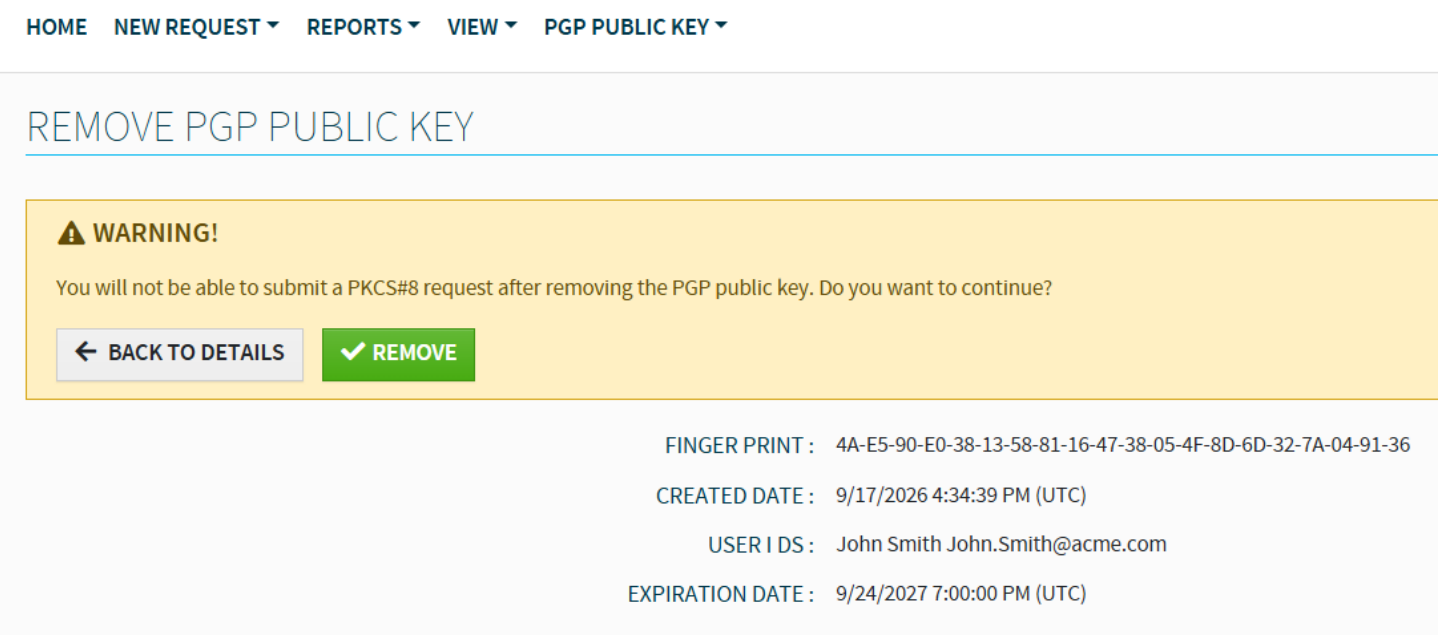

Figure 34 – Remove PGP Public Key Confirmation