Nordea

Web Services, SHA1 – SHA256 changes

Quick Guide for customers to adapt to SHA256 service

Nordea

Table of Contents

1. About the Change in Web Services of closure of SHA1 service:

In Q1 2024, SHA1 service will stop working. This is one of the steps finalizing SHA1-SHA256 change in Web Services. To understand in details about the SHA1-SHA256 change, please read documents in Nordea.fi ([link](#))

If customer still uses SHA1 service links in own Web Services client, customer will get errors. Instead, the SHA256 service should be used.

This is one of the change step in SHA1-SHA256 migration in Web Services.

The SHA256 service links:
https://filetransfer.nordea.com/services/CorporateFileService/sha2
https://filetransfer.nordea.com/services/CertificateService/sha2

The SHA1 service links:
https://filetransfer.nordea.com/services/CorporateFileService
https://filetransfer.nordea.com/services/CertificateService

Please note, the SHA256 service works slightly differently than the SHA1 service. In general, the incoming flow from customers to Nordea work the same way, but in the outgoing flow when Nordea sends customers the responses, the responses are signed with SHA256 certificate and algorithm in the SHA256 service. Customers can find more details from documentation on "Web Services" page in Nordea.fi, under a new tab called "SHA256 Change and Migration".

2. Troubleshooting steps for customers to start to use SHA256 service

2.1 Change endpoint links

Change the endpoint links from the old SHA1 links to SHA256 links.

The IP addresses of both services are the same, so there is no need to change firewall settings for this.

2.2 Try commands other than UploadFile

As already mentioned in section 1, the SHA256 service works slightly differently than the SHA1 service. It is more safe to try some other commands then UploadFile for sending in payment files.

Customers can try GetUserInfo, DownloadFileList or DownloadFile instead.

2.3 If other commands work, try UploadFile

When it is confirmed that other commands like GetUserInfo, DownloadFileList or DownloadFile work ok, then customer can send in payment files using UploadFile command

2.4 In case of errors when trying commands in SHA256 service

If customers get errors with commands, and if the error is triggered by UploadFile command, customers should not try to execute the command again because it might trigger duplicates.

The difference between SHA1 and SHA256 service is how the Web Services Responses from Nordea to customers are formulated.

In SHA256 service, ApplicationReponses and SOAPResponse from Nordea to customers are signed with

new SHA256 certficiates and with SHA256 signing algorithm. Please read document **Web Services SHA256 - Technical Change Description** , Charpter 4 to understand the details.

2.4.1 Steps to fix errors in SHA256 service

2.4.1.1 Install Nordea's new SHA256 signing certificate and the Root CA certificate

Customer's software might require the installation of the Nordea's signature certificate or/and CA certificate. If this is the case, new certificates used in SHA256 service should be installed.

Certificates are published in Nordea.fi

https://www.nordea.fi/en/business/our-services/mobile-online-services/web-services.html#tab=SHA256-Change-and-Migration

After installation of the certificate(s), try command like GetUserInfo again.

2.4.1.2 Develop client to accept SHA256 signing algorithm

If the previous step of installing the Nordea's signature certificate didn't help, the problem might be that customer's client is not able to valide the signature when SHA256 signing algorithm is used in ApplicationResponse and SOAPResponse.

Development work is needed to solve the problem. Please read documentations: **Web Services SHA256 - Technical Change Description** and **Web Services SHA1-SHA256 Migration FAQ**

3. Other coming changes in SHA1-SHA256 migration

In Q2 2024 (exact time to be informed later): The incoming Web Services requests sent by customers with SHA1 signature will be rejected in the SHA256 service

In Q2 2024 (exact time to be informed later): Nordea will stop supporting of TLS 1.0 and 1.1 in the new SHA256 service

Please read documents published on Web Services page of Nordea.fi to understand the change and its impact.