Nordea

Web Services SHA1 – SHA256 Change

FAQ Document

Nordea

1. Why do you make this SHA1-SHA256 change

Nordea wants to provide secure services and solutions to our customer. SHA1 certificate and signing signature should be deprecated because of it is security weakness.

a. The signature from SHA1 certificate and signing cannot fully protect the integrity of the file content.

b. There is means an attacker could essentially impersonate another person by creating another key.

2. Why didn't you make the change earlier

a. Web Service security and communication standard defined by Finanssiala was updated in middle of 2020, in which SHA1 is not anymore mentioned as required algorithm.

b. Nordea have thousands of Web Services customers, we want to make the solution upgrade and migration smooth so that we limit the customer impact in the change. So it takes time to analyze, develop, and plan.

3. What are the changes

Document "Web Services, SHA1 – SHA256 changes Technical Description" describes the change in detailed way.

On high level, the areas of changes are:

a. The customer signing certificate (linked to each logon ID) used to create digital signatures will be changed to use SHA256 signature hash algorithm.

b. The customer need to use SHA256 signing algorithm when creating the digital signature. You can look into the provided example request files in "Web Services, SHA1 – SHA256 changes Technical Description" document.

c. When Nordea sends customers responses, the responses are signed with Nordea's new SHA256 certificate and with SHA256 signing algorithm. Nordea's new certificates can be found from Nordea.fi, and you can also look into provided example responses files in "Web Services, SHA1 – SHA256 changes Technical Description" document.

d. Nordea supports key length of 2048 for the customers' signing certificates and we recommend customer to use key length of 2048

e. Nordea will stop support of TSL 1.0 and 1.1

4. How can customers make the change

a. Please first understand the scope of the change. You can refer to question no.3

b. Please look as the example files "Web Services, SHA1 – SHA256 changes Technical Description", and you can compare with your current messages.

c. Based on Nordea's own experiences in making the similar change in our side, the development and testing effort is about 70-300 manhours (2-6 weeks)

d. You can get our test SHA256 certificates, and test, while still perform daily operation using existing setup

e. Nordea is not able to support in detail how to make the changes since our customers have own solutions build with different technologies and platforms. We at Nordea won't be able to understand, and don't have the resource to look into these solutions specifically. We only provide the change specification and example files. However, we will assist as much as we possibly can.

5. What do Nordea provide to support the change

a. Technical specification document and FAQ document

b. Example files in Appendix of Technical specification document

c. Customer TEST certificates in SHA256 format

d. Nordea's new signing certificate and ROOT CA certificate in SHA256 format

e. Nordea deployed new service running with SHA256 responses in the outbound flow (response messages from Nordea to customers), parallel to the existing Web Services in PRODUCTION service running with SHA1. Customers can develop and test SHA256 solution while still running daily operations without changes in existing service. You can refer to question no.6 for more details

f. Customer support team will answer customers questions as best as we can but as explained in question No.4, we are not able to promise we always have answers when it comes to specific questions on customer changes.

Nordea

Migration related

6. How is the setup of parallel services of SHA1 and SHA256

Existing site for file operations:

https://filetransfer.nordea.com/services/CorporateFileService

No change and the same as of today:

- Support for SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm
- Responses from Nordea is signed with SHA1 certificate and signing algorithm as it has always been.
- We will close this service in Q2 of 2023. We will inform the exact date later.

New site for file operations:

https://filetransfer.nordea.com/services/CorporateFileService/sha2

- Support for SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm
- Responses from Nordea are signed with SHA256 certificate and signing algorithm.
- Nordea's SHA256 server signing certificate and its Root CA certificate are published on Nordea.fi
- We will remove the support of SHA1 algorithm in Q2 of 2023. We will inform the exact date later.

Existing Certificate service site:

https://filetransfer.nordea.com/services/CertificateService

No change and the same as of today:

- Support both SHA1 and SHA256 signing algorithm for incoming customer requests
- Responses from Nordea is signed with SHA1 certificate and signing algorithm as it has always been.
- Issue SHA1 certificate for now, but will issue SHA256 certificate from Q3 2022

New Certificate service site:

https://filetransfer.nordea.com/services/CertificateService/sha2

- Support both SHA1 and SHA256 signing algorithm for incoming customer requests
- Responses from Nordea is signed with SHA2 certificate and signing algorithm.
- Nordea's SHA256 server signing certificate and its Root CA certificate are published on Nordea.fi
- Issue SHA1 certificate for now, but will issue SHA256 certificate from Q3 2022

7. How do I manage my customer certificates

a. Nordea plans to switch to SHA256 certificate issuing in Q3 2022. We will inform the exact date and time later.

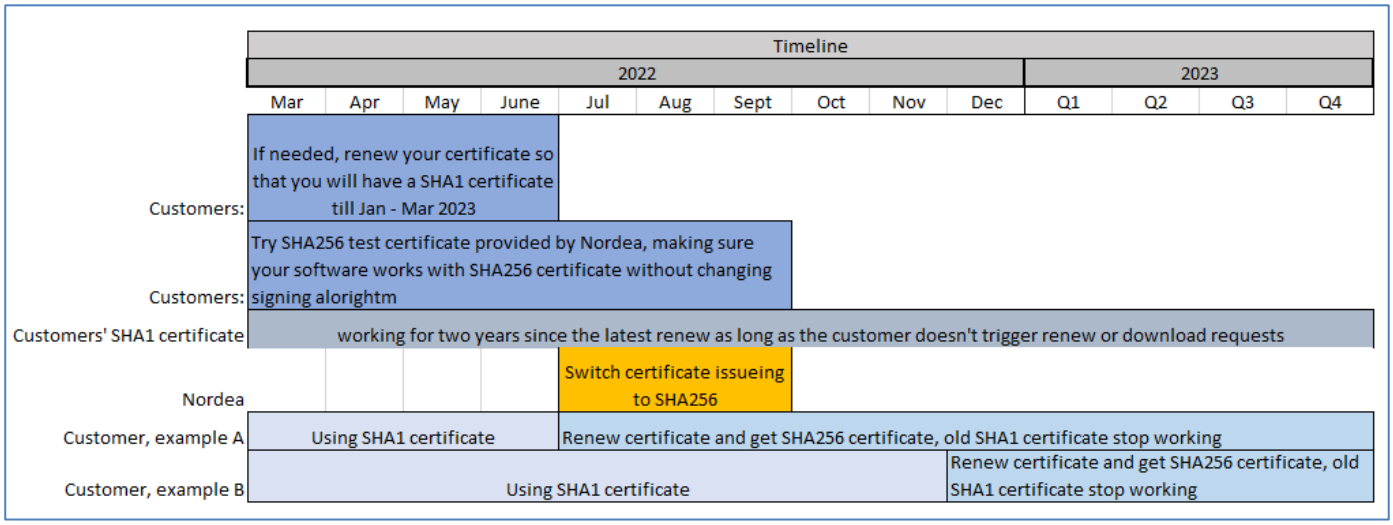
b. Before our change in Q3 2022, please consider to renew your SHA1 certificate so that you will have a new SHA1 certificate valid for 2 years, and can use it till we close the support of SHA1 in Q2, 2023. By doing this, you would have more time to use the current service without changes made to your software.

c. After we switch the certificate issuing in Q3 2022, and when you initiate certificate download or renew, no matter through which of the two services, will get SHA256 certificate from us, and your old certificate will be revoked

d. So before you are sure that SHA256 certificate works in your software, please don't renew so that you keep the old SHA1 certificate working.

e. Nordea provides several SHA256 test certificates on Nordea.fi and you can use those to test how your software works with SHA256 certificates

Chart below shows customers can have different timeline to adapt to SHA256 certificates



8. We get errors when downloading certificate, but we need the certificate urgently. What can we do?

You can use the NSC client offered by Nordea, and it is available in Nordea.fi.

9. We got own SHA256 certificate, can we still use SHA1 signing because we have not changed our software

Yes, you can even though we don't recommend this way. But it will work ok. Please refer to question number 6 to see the supported setup in two services.

However please develop the SHA256 algorithm signing and response processing in your software. We will stop support of SHA1 in Q2 of 2023.

10. What are the important things to be noted when trying to use SHA256 service

1. **Most customers would need to Install our new server signature certificate and/or its Root CA certificate to their client software**

The difference between SHA256 service and the existing SHA1 service is how Nordea's response messages are signed. In SHA256 service, Nordea's response is signed with a SHA256 server signature certificate and with SHA256 signing algorithm.

The SHA256 server signing certificate is a different certificate then the one in existing service, its Root CA certificate is also a new one. Certificates are published in "SHA256 Change and Migration" section in Web Services page on Nordea.fi So customers need to install either of them or both of them depending on how the client software works.

2. **Try "GetUserInfo" first, only when succeed, try other commands**

When you try SHA256 solution first time, try with command "GetUserInfo" first, and only proceed with other commands after you have succeeded with "GetUserInfo". If you get error, and the error is related to certificate validation, please check whether you have installed our new SHA256 server signature certificate and/or its Root CA. Please also check question no. 12

3. **Define Environment = "TEST" in ApplicationRequest when first time trying UploadFile**

By doing this, the payment will not be executed. You can refer to question no.11

4. **If you get error after uploading a payment file, please don't try to send in payment again.** Please look into question No. 12.

11. Is it possible for us with our own certificates to send in test files which won't be processed and paid

Yes. You can do that by defining the Environment as "TEST" in ApplicationRequest.

When the message is received, we validate whether the files are in the correct format, certain parts of their content are in order, and the IDs are as agreed and the customer's payment agreement is valid. Nordea also produces authentic transmission feedback file which customers can download, only once though. Payments are not entered into accounts and no account statement is formed.

Please note that If the value in the Environment field is not TEST, the files will be paid.

Nordea

12. We get errors while trying SHA256 service, what could be wrong

If the error you get is about certificate validation problem, please make sure you have installed our SHA256 server signature certificate and/or its Root CA certificate. You can refer to question no.10. Please don't try to send in payment files again because it might cause duplicated payments.

If the error you get is not in proper form of SOAP and Application response from Nordea, it means that most likely the signing of the request has some problem.

- In this case, our log systems would not have information about the connection try so that our support won't be able to help you much.
- Please look at the your Application Request and SoapRequest messages and compare with our examples to locate the difference and errors.
- Please make sure both the ApplicationRequest and SOAPRequest are signed with correct algorithm

If the error you get is in responses from Nordea

- you can look at the error code and message table in Web Services Security and Communication Description document in Nordea.fi.
- if more information is needed, you can contact our customer support.