Nordea

Corporate Access Secure Envelope SHA1 – SHA256 Change

FAQ Document

Open

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. Nordea have thousands of Corporate Access File Transfer 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.

b. Web Service as one of the protocol supported in Corporate Access File Transfer, its security and communication standard defined by Finanssiala was updated in middle of 2020, in which SHA1 is not anymore mentioned as required algorithm.

3. What are the changes

Document "Corporate Access Secure Envelope SHA1 - SHA256 Technical Description" describes the change in detailed way.

On high level, the areas of changes are:

a. The customer signing certificate (linked to each Signer 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 "Corporate Access Secure Envelope, 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.com, and you can also look into provided example responses files in "Corporate Access Secure Envelope, 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 "Corporate Access Secure Envelope, 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. 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 (these will be published in Q4 2022)

e. In incoming flow for files customers send to Nordea, Nordea supports both SHA1 and SHA256 certificates and SHA1 and SHA256 signing algorithms from now on till Q2 2023. Customers can develop and test SHA256 solution while still running daily operations without changes in existing service. You can refer to question no.7 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.

Migration related

6. 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.

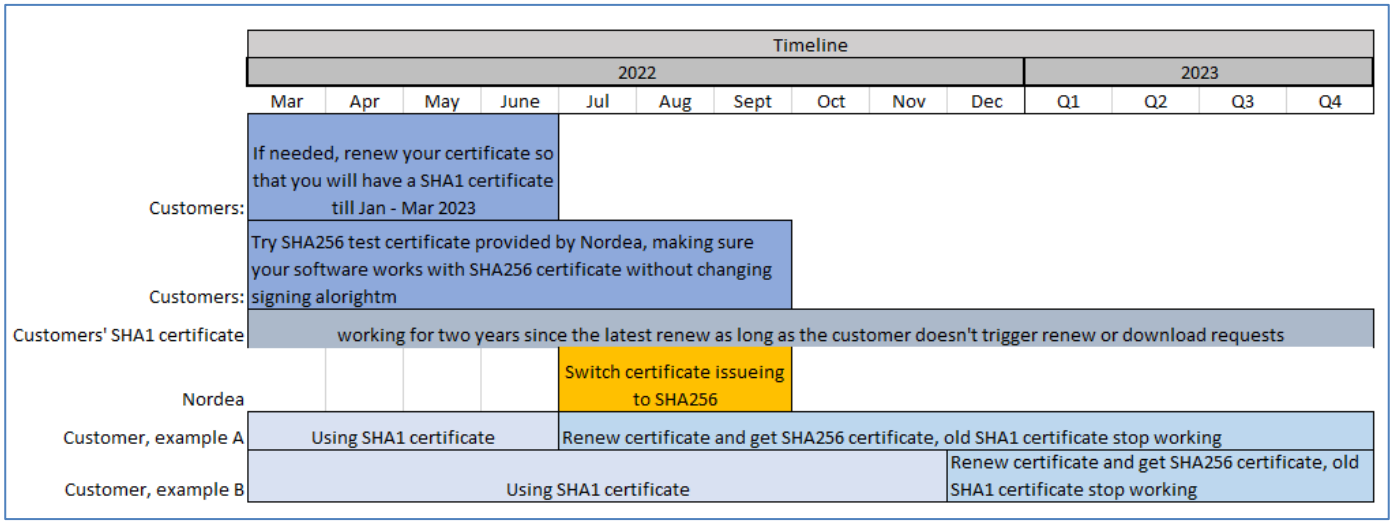
b. Before our change in Q3 2022, please consider to renew your SHA1 certificate so that you will have a new SHA1 certificate valid for 2 years, and can use it till we close the support of SHA1 in Q2, 2023. By doing this, you would have more time to use the current service without changes made to your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



7. How is SHA1 and SHA256 supported

Incoming flow for files sent from customers to Nordea

No change and the same as of today:

Nordea

- Support for SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm. So customers can use
    - SHA1 certificate + SHA1 signing algorithm in signature
    - SHA1 certificate + SHA256 signing algorithm in signature
    - SHA256 certificate + SHA1 signing algorithm in signature
    - SHA256 certificate + SHA256 signing algorithm in signature

- We will close the support of SHA1 certificate and SHA1 signing algorithm in Q2 2023. We will inform the exact date later.

Outgoing flow for files sent from Nordea to Customers

- No change and the same as of today till Q2 2023:
    - Responses/Files from Nordea is signed with SHA1 certificate and signing algorithm as it has always been.

- During Q2 2023, change will be made so that
    - Responses/Files from Nordea is signed with SHA256 certificate and signing algorithm.

For customers who download certificates with own software

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.com
- Issue SHA1 certificate for now, but will issue SHA256 certificate from Q3 2022

Nordea

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.com

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.