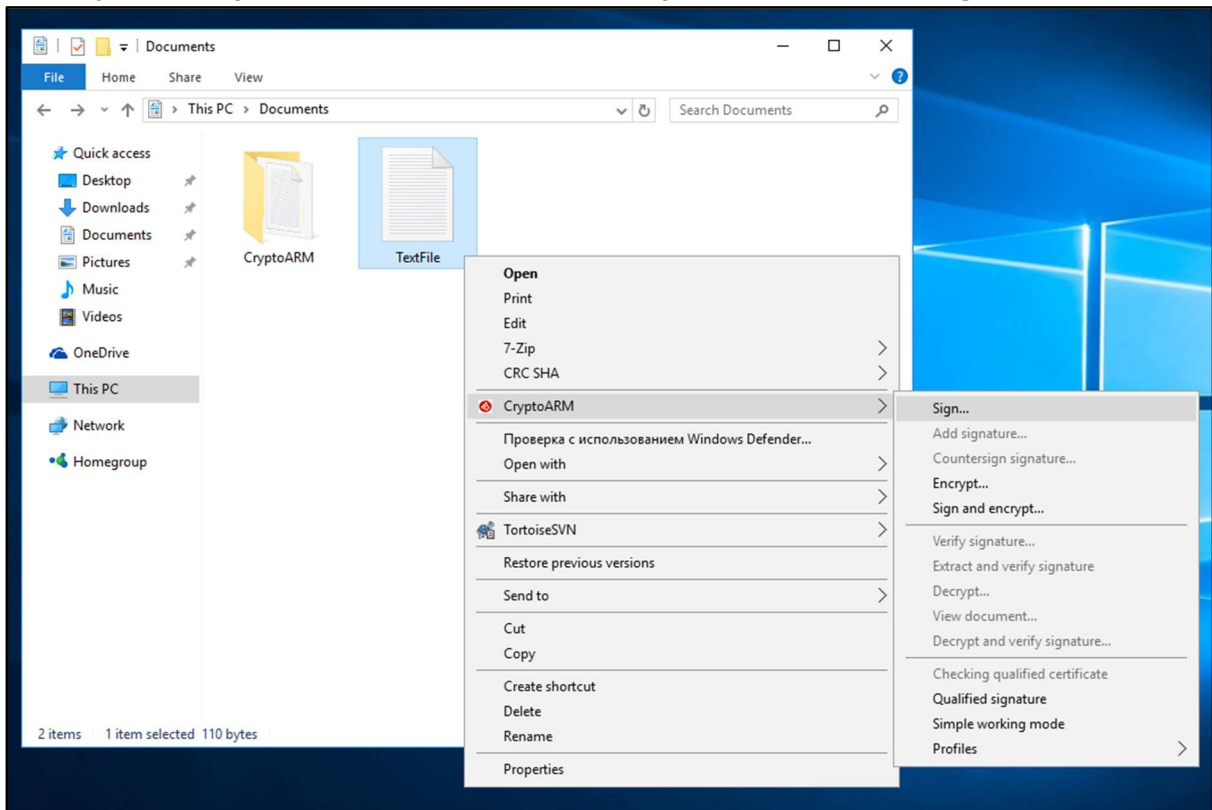


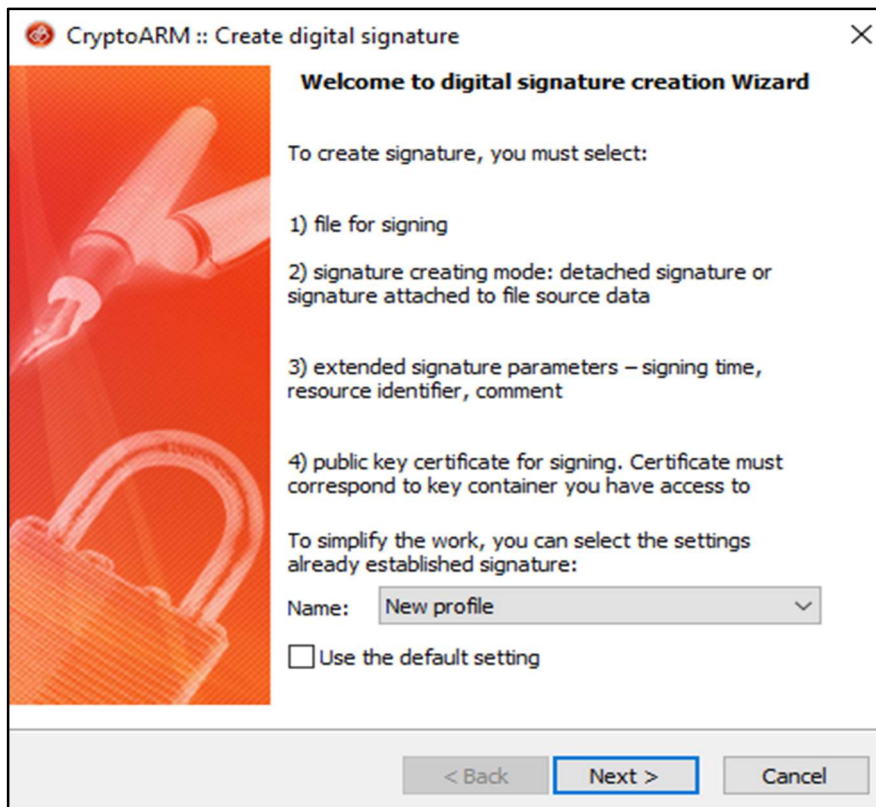
## How to sign & encrypt files with CryptoARM™

### Step one: How to sign.

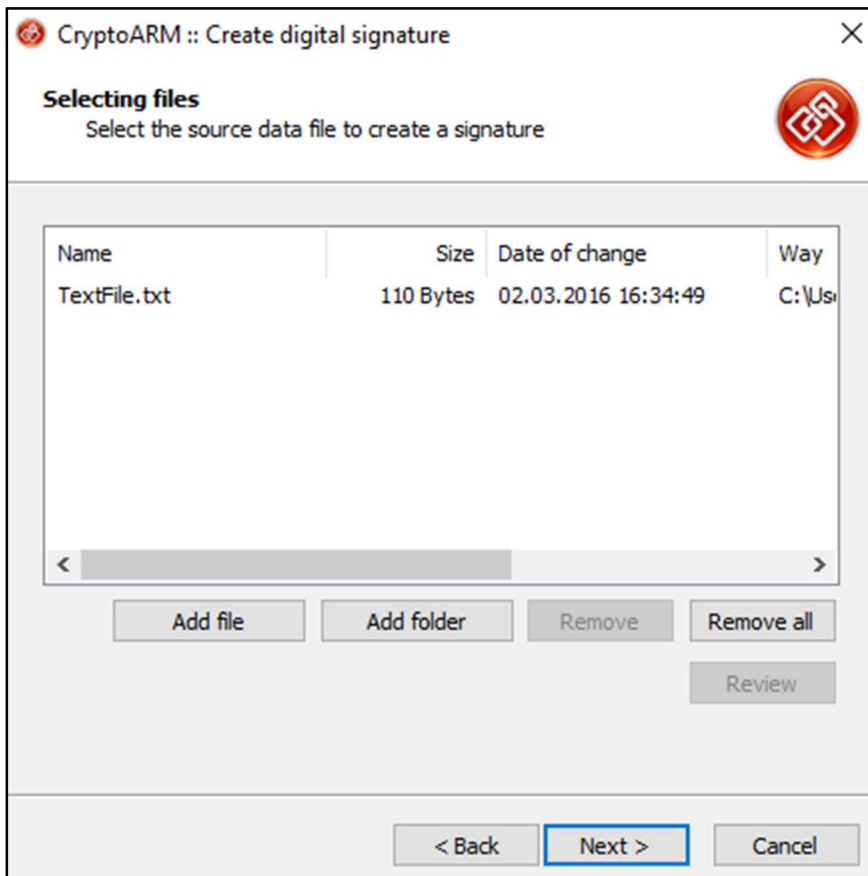
1. Select your file, right-click and press menu item **CryptoARM** then click **Sign...**



2. Press **Next >**.



3. Press **Next >**.



**CryptoARM :: Create digital signature**

**Selecting files**  
Select the source data file to create a signature

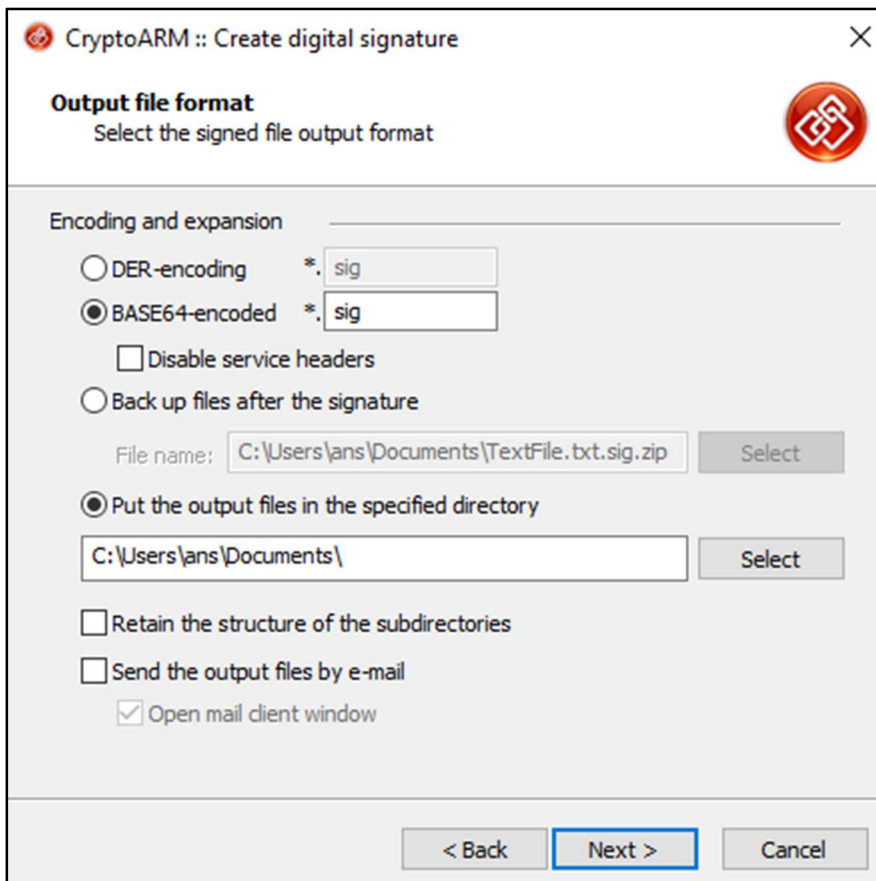
Name	Size	Date of change	Way
TextFile.txt	110 Bytes	02.03.2016 16:34:49	C:\Usi

< >

Add file Add folder Remove Remove all Review

< Back **Next >** Cancel

4. Press **Next >**.



**CryptoARM :: Create digital signature**

**Output file format**  
Select the signed file output format

Encoding and expansion

☐ DER-encoding \*.sig

☒ BASE64-encoded \*.sig

☐ Disable service headers

☐ Back up files after the signature

File name: C:\Users\ans\Documents\TextFile.txt.sig.zip Select

☒ Put the output files in the specified directory

C:\Users\ans\Documents\ Select

☐ Retain the structure of the subdirectories

☐ Send the output files by e-mail

☒ Open mail client window

< Back **Next >** Cancel

5. Press **Next >**.

The screenshot shows a dialog box titled "CryptoARM :: Create digital signature" with a close button (X) in the top right corner. The main heading is "Digital signature parameters" with the subtitle "Set required signature parameters". A red circular icon with a white geometric design is in the top right. The "Signature" section contains the following fields and options:

- Signature usage: [Not assigned] (dropdown menu)
- Comment to the signature: (text input field)
- Resource ID: TextFile.txt (text input field)
- ☒ Put the name of the source file in the "Resource identifier"
- Add to structure: Signer's certificates only (dropdown menu)
- ☐ Save the signature in a separate file
  - ☐ Delete the original file after the operation
  - Level safe removal: Disabled (dropdown menu)
- ☒ Include the time of the signature creation
- ☐ Include time stamp data to be signed
- ☐ Include time stamp signature
- ☐ Include in the signature proof of identity

At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

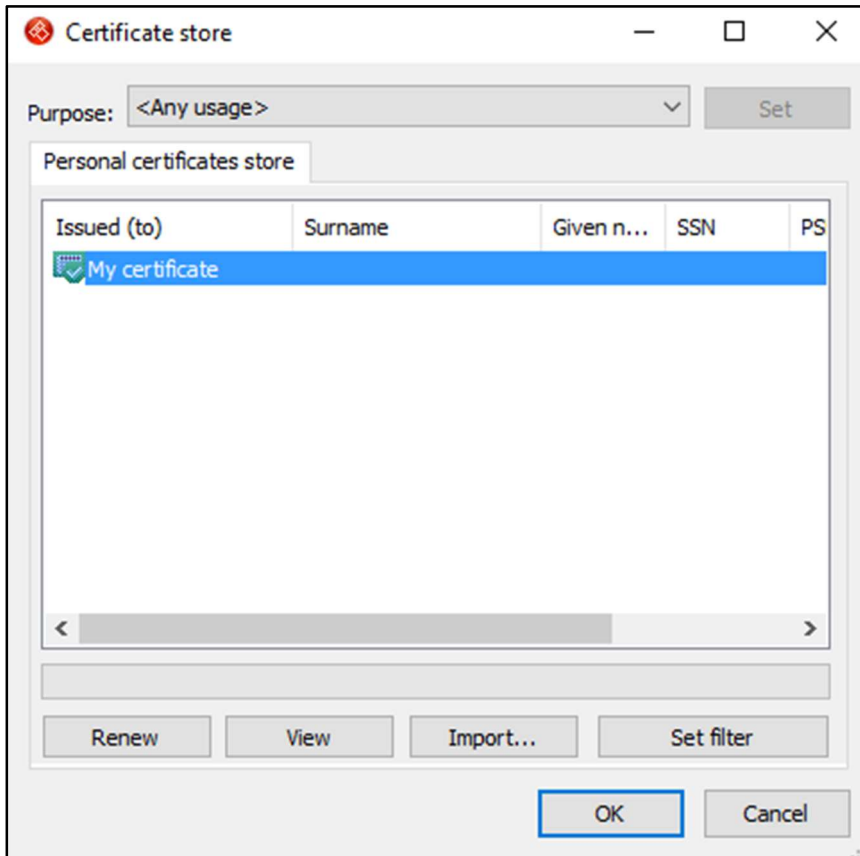
6. Press **Select** to open the window of certificate store.

The screenshot shows the same dialog box, but the tab is now "Select a certificate signing" with the subtitle "Select a signing certificate". The red circular icon remains in the top right. The "Certificate for signing" section contains the following fields and options:

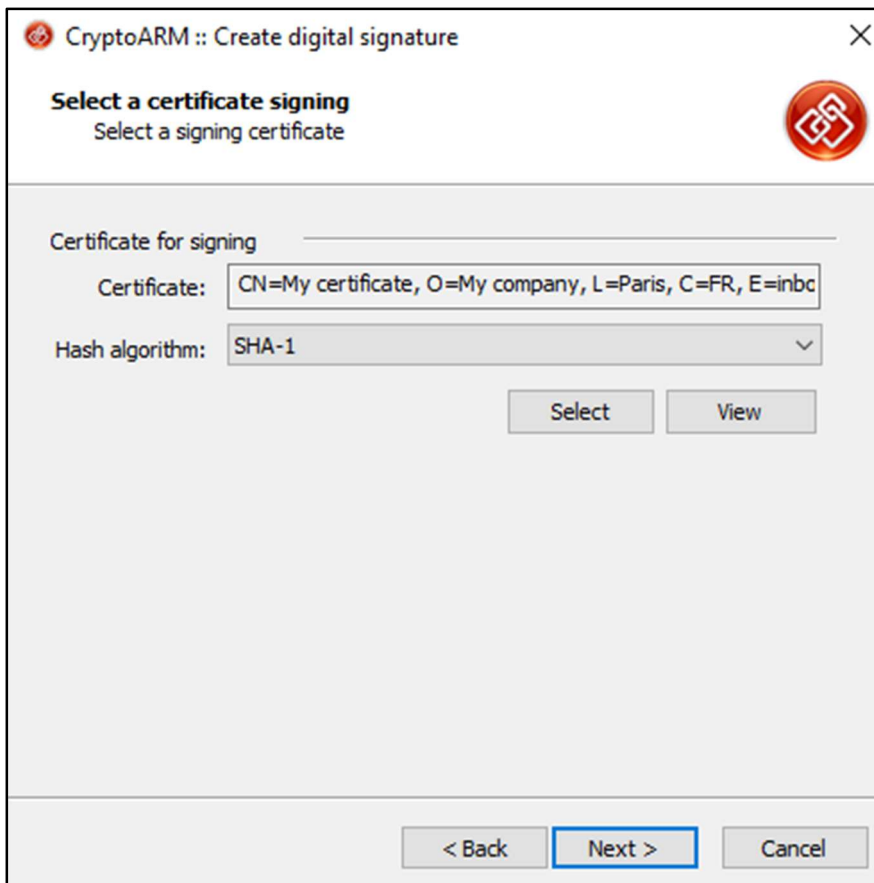
- Certificate: (text input field)
- Hash algorithm: (dropdown menu)

Below these fields are two buttons: "Select" (highlighted with a blue border) and "View". At the bottom, there are three buttons: "< Back", "Next >" (disabled), and "Cancel".

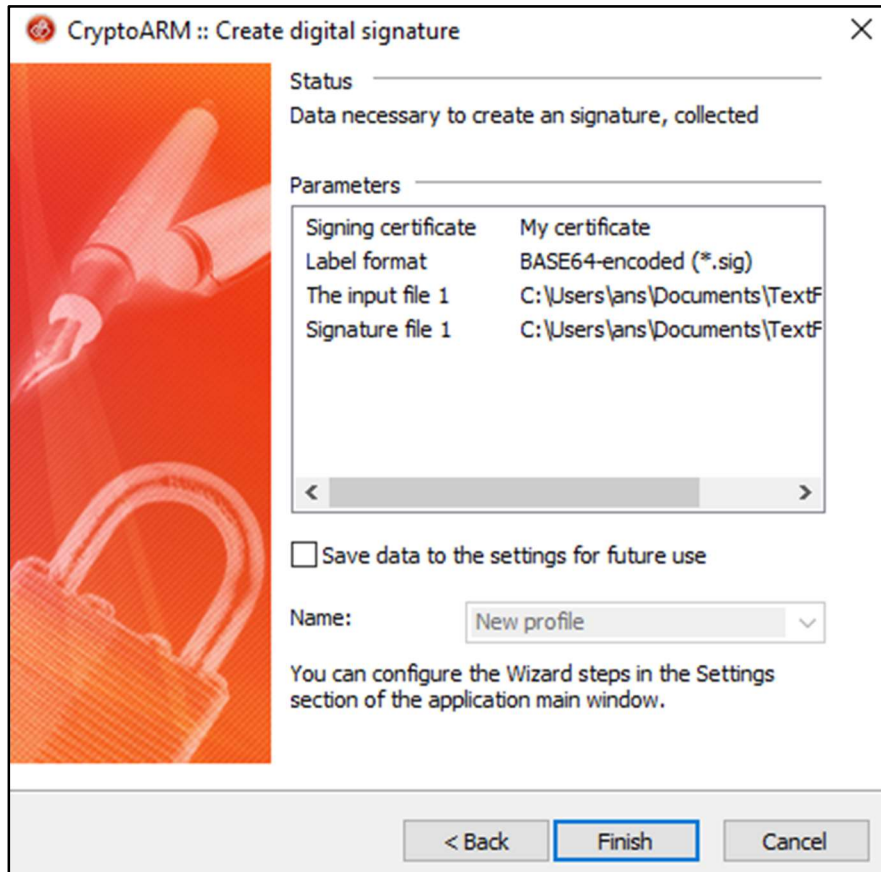
7. Select the certificate from the list. Press **OK**.



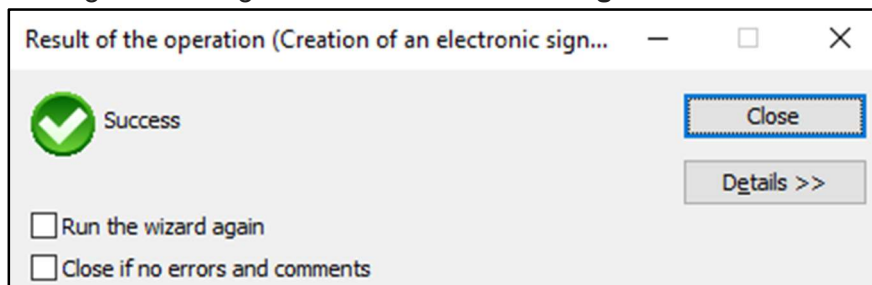
8. Press **Next >**.



9. Press **Finish**.

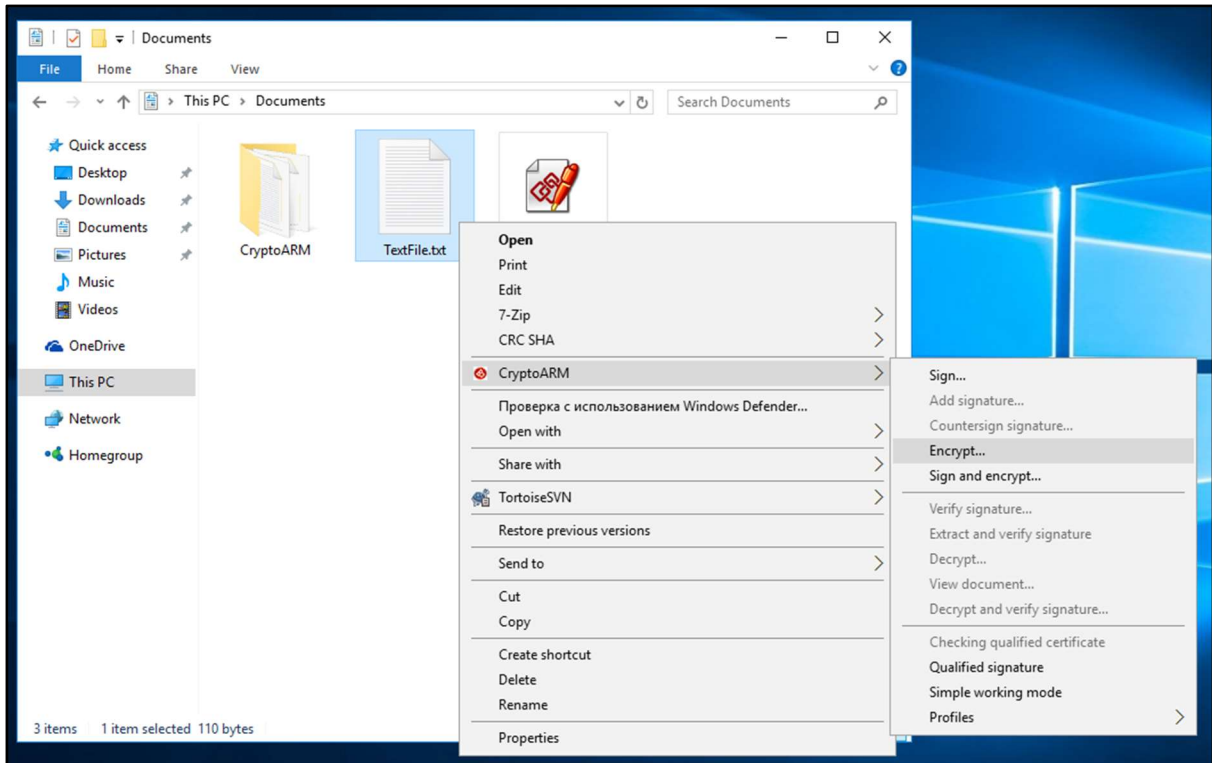


10. If you see a success, it means the signature is completed. You can open the folder and find signed file. Signed file have extension **.sig**.



## Step two: How to encrypt.

1. Select your file, right-click and press menu item **CryptoARM** then click **Encrypt...**

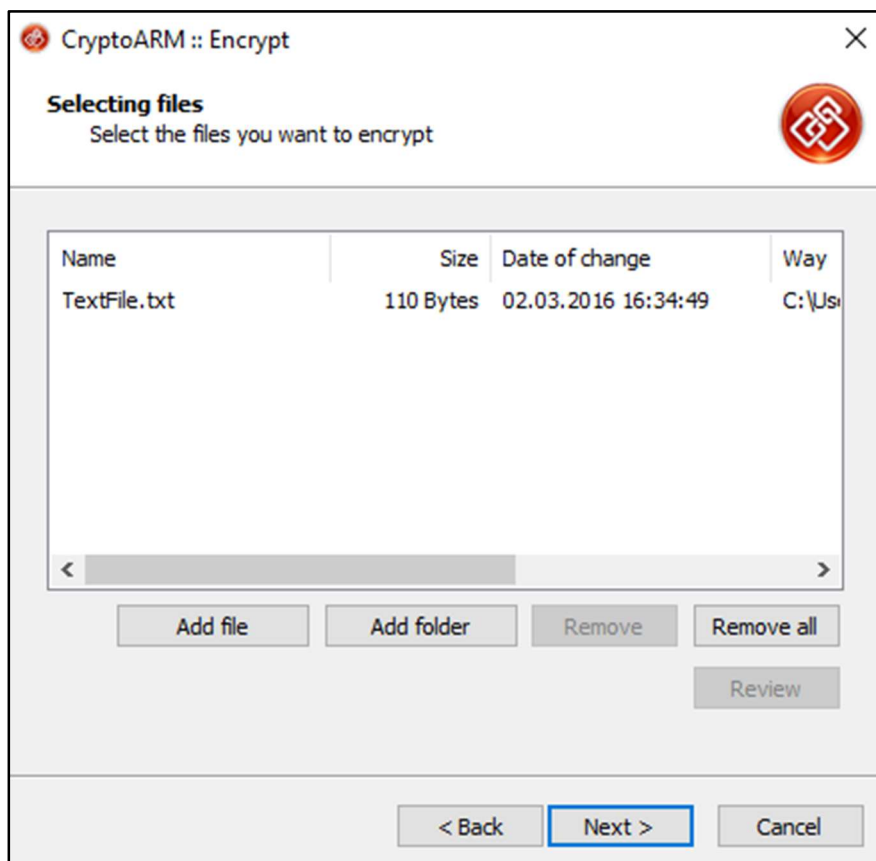


2. Press **Next >**.





3. Press **Next >**.

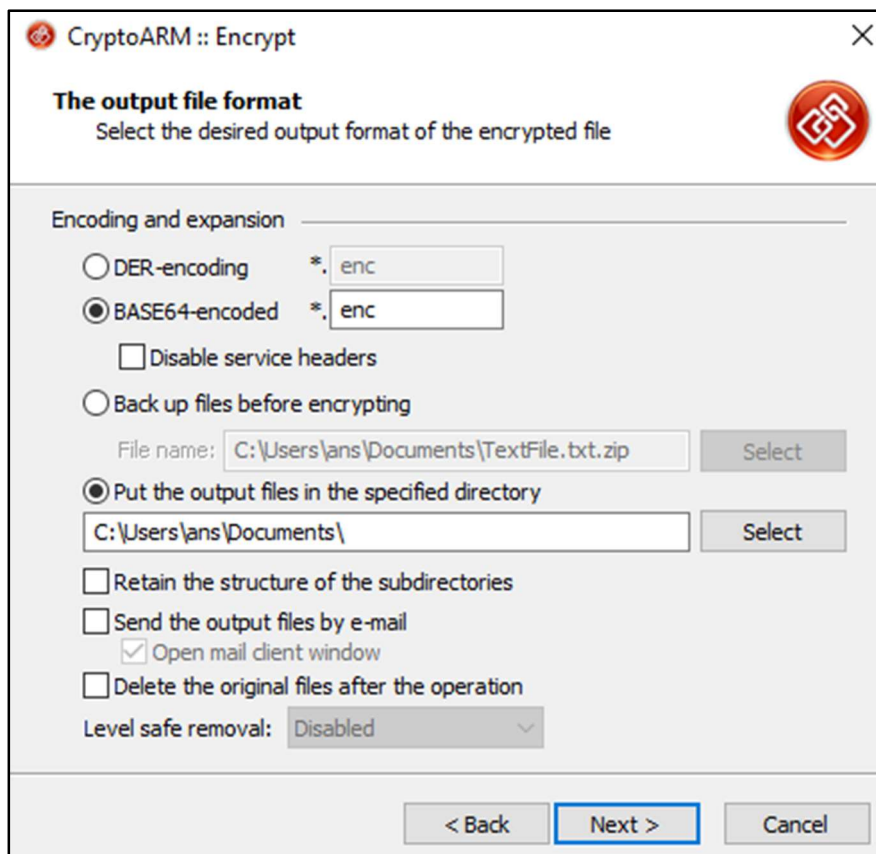


The screenshot shows the 'Selecting files' window of the CryptoARM :: Encrypt application. The window title is 'CryptoARM :: Encrypt'. Below the title bar, there is a section titled 'Selecting files' with the instruction 'Select the files you want to encrypt'. A table lists the selected files:

Name	Size	Date of change	Way
TextFile.txt	110 Bytes	02.03.2016 16:34:49	C:\Usr

Below the table, there are buttons: 'Add file', 'Add folder', 'Remove', 'Remove all', and 'Review'. At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

4. Press **Next >**.



The screenshot shows the 'The output file format' window of the CryptoARM :: Encrypt application. The window title is 'CryptoARM :: Encrypt'. Below the title bar, there is a section titled 'The output file format' with the instruction 'Select the desired output format of the encrypted file'. The window contains several options for encoding and expansion:

- ☐ DER-encoding \*.enc
- ☒ BASE64-encoded \*.enc
- ☐ Disable service headers
- ☐ Back up files before encrypting

Below these options, there are two sections for file naming and directory selection:

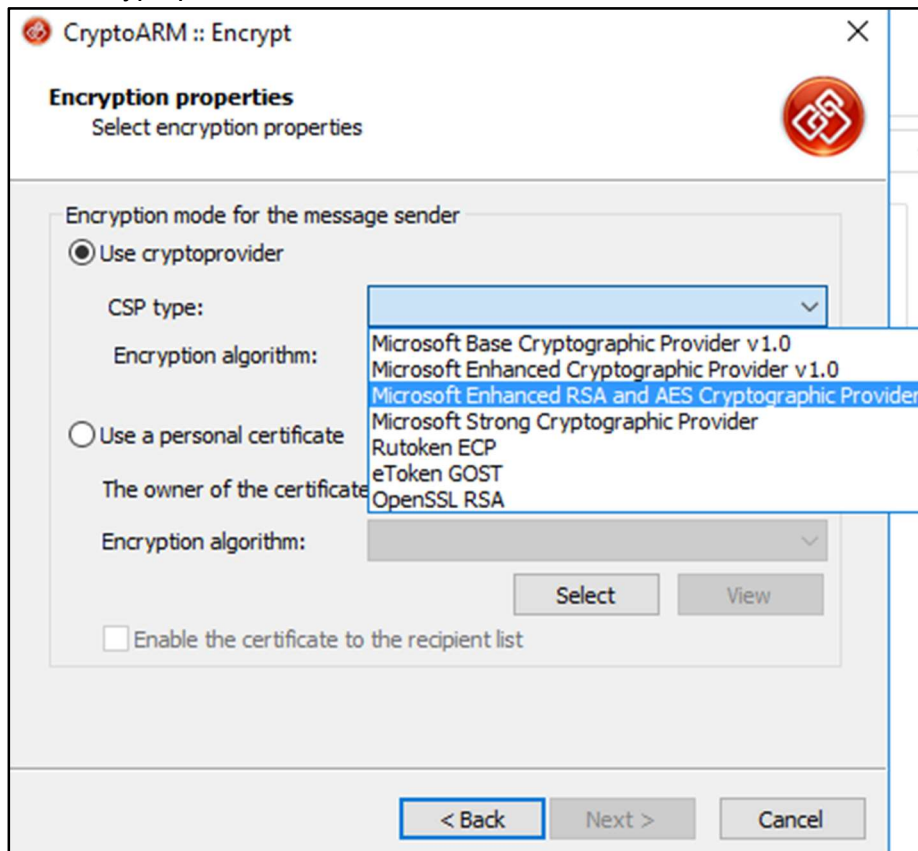
- File name: C:\Users\ans\Documents\TextFile.txt.zip (with a 'Select' button)
- ☒ Put the output files in the specified directory

Below this, there is a text box containing 'C:\Users\ans\Documents\' and a 'Select' button. Further down, there are more options:

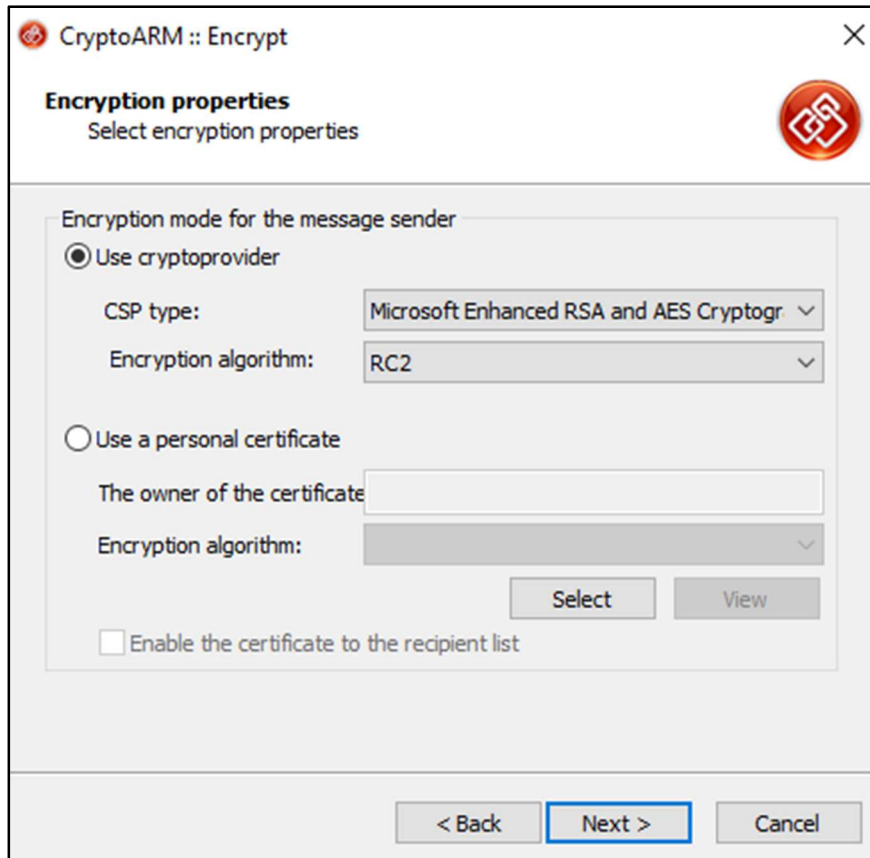
- ☐ Retain the structure of the subdirectories
- ☐ Send the output files by e-mail
- ☒ Open mail client window
- ☐ Delete the original files after the operation
- Level safe removal: Disabled (with a dropdown arrow)

At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

5. Select cryptopriver from the list.

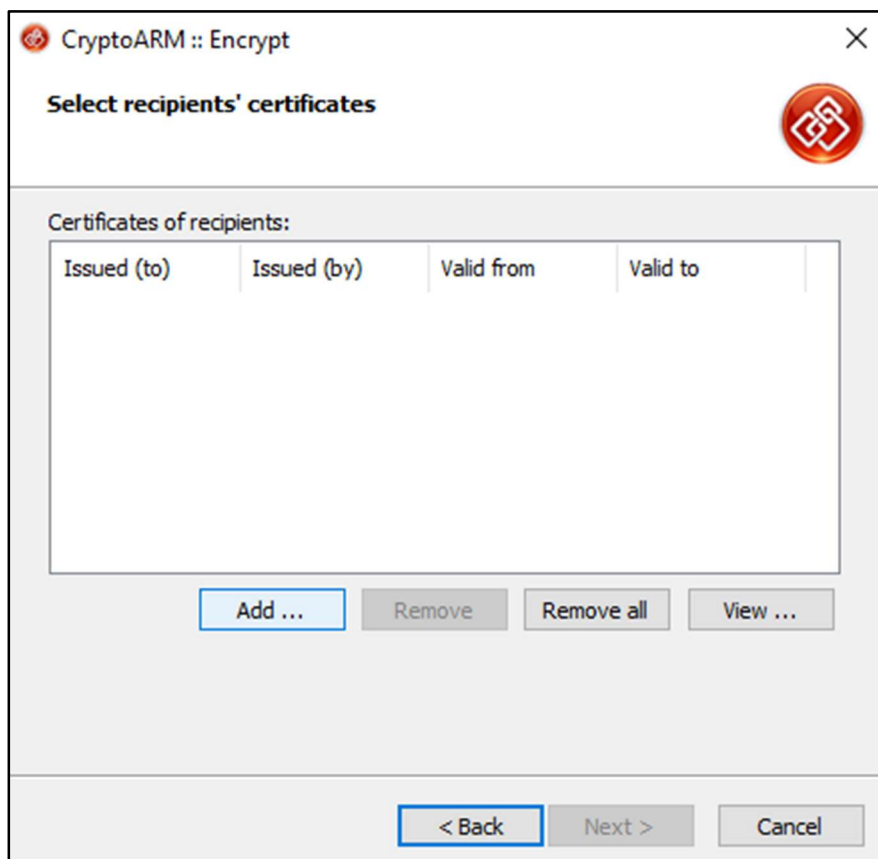


6. Press **Next >**.

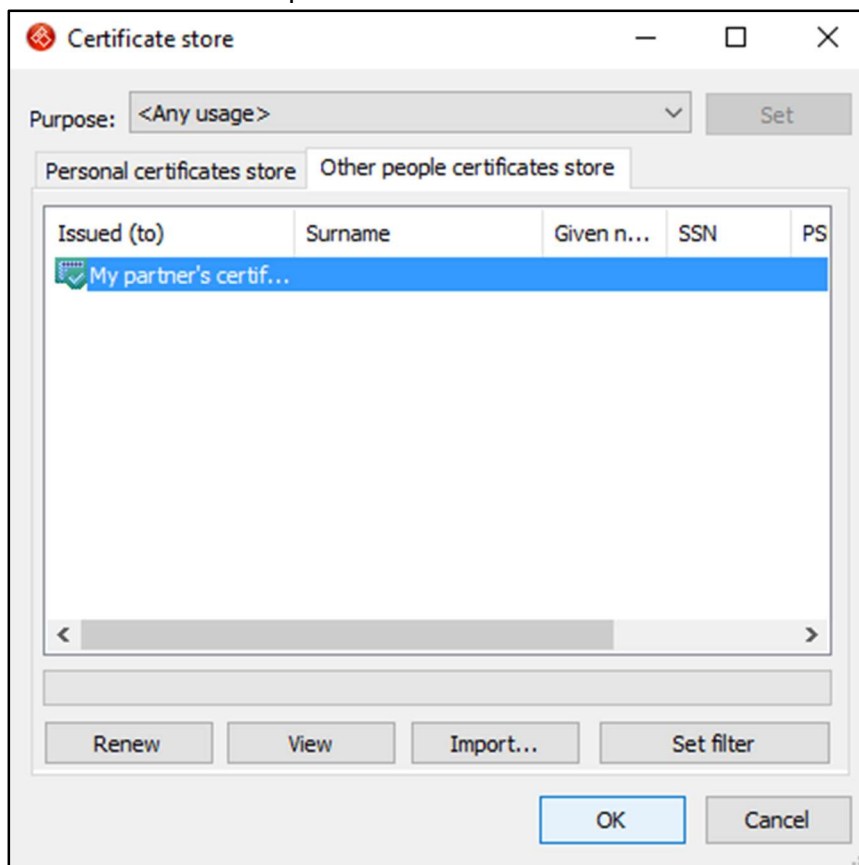




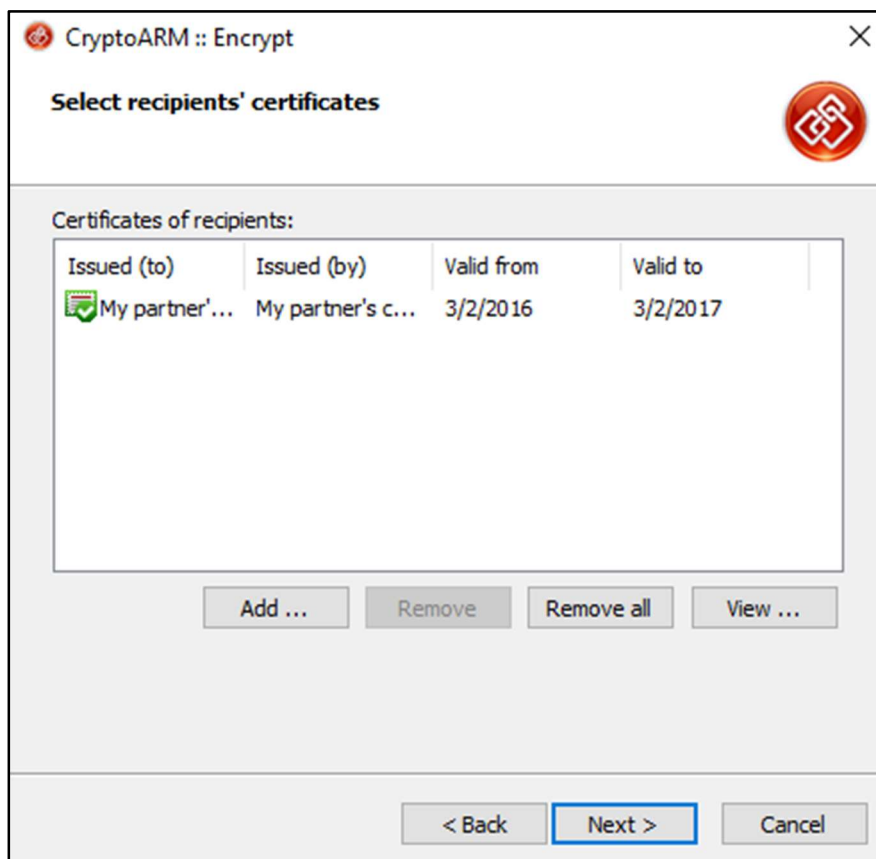
7. Press **Add ...**



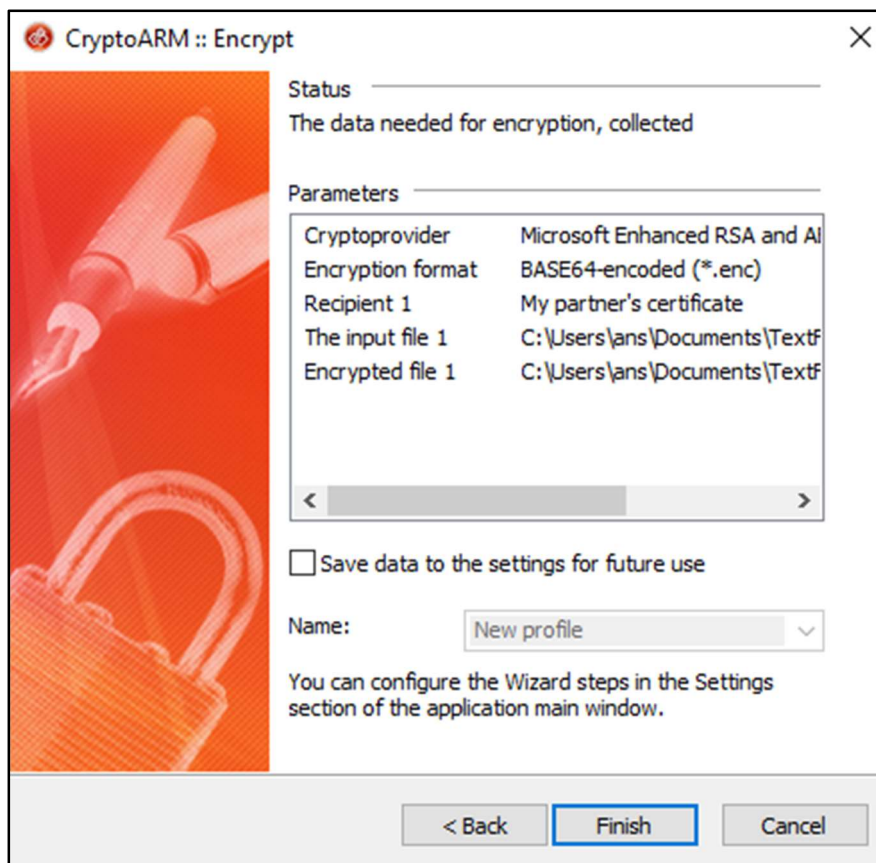
8. Select certificate and press **OK**.



9. Press **Next >**.



10. Press **Finish**.



11. Press **Close** if operation has been successfully completed.



12. You can open the folder and find encrypted file. Encrypted file have extension **.enc**.

