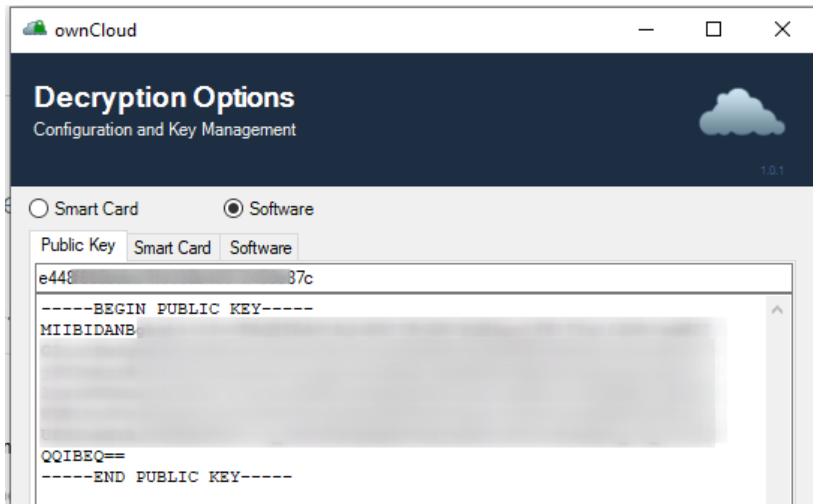


# Outlook Add-In - E2ee Configuration

The End-To-End Encryption works with the epiKshare E2ee ownCloud plugin. In this combination you can not only send, but also receive end-to-end encrypted files and let the integrated ownCloud Client decrypt the files for you.

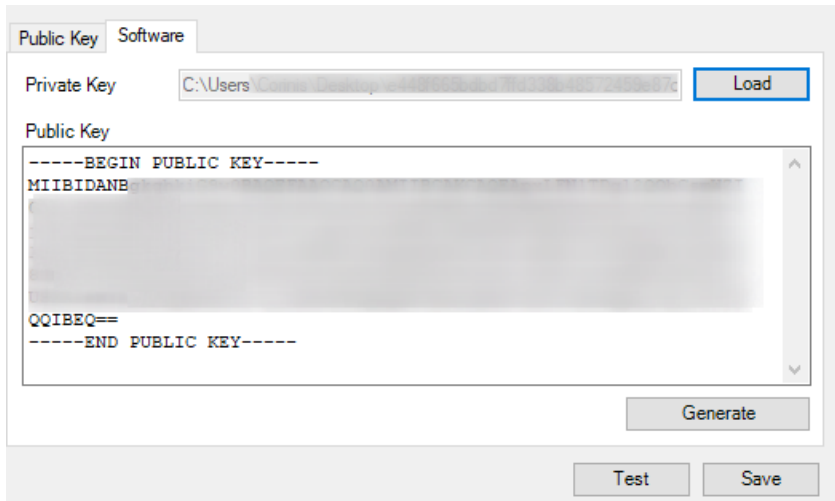


Depending on your License, you will have to decide if you want SmartCard supported decryption (Enterprise only) or software. Once you setup everything click the save button and the configuration will be available for all tools.

## Software

Software Decryption uses a private key that is available in the file system.

For extra security, you can put the private key on a usb drive, make sure you insert it before you decrypt!



If you do not have a private key, simply click generate and the tool will create a new RSA Keypair and ask you where to save it. Alternatively you can simply load a private key you already saved previously.

## Smart Card

This is the most secure way to handle your private key. The key is generated and stored on a smart card (**PKCS#11** compatible with **2048bit RSA** support) and cannot be exported onto the computer and thus also never be compromised unless you loose the smart card or dongle.

Make sure you have the smart card reader and card driver (incl. the PKCS#11 driver package!) installed and the smart card you want to use for decryption in the device.

Then select the correct PKCS#11 driver for your system (it might already be automatically detected):

- Gemalto: "C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS11.dll"
- OpenSC (i.e. YubiKey): "C:\Program Files\OpenSC Project\OpenSC\pkcs11\opensc-pkcs11.dll"

Public Key Smart Card Software

PKCS#11 Library C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS11.dll Select

Card Reader Cherry SmartTerminal XX44 0

Card Token Smartusers Testaccount FRD FIID1 # Check Card

Card Keys 'cccf9e1a-25...' v

Key ID b264359f55...

Read Public Key Create Key

Supported mechanisms:

- CKM\_RSA\_PKCS\_KEY\_PAIR\_GEN
- CKM\_RSA\_PKCS
- CKM\_RSA\_X\_509
- CKM\_MD5\_RSA\_PKCS
- CKM\_SHA1\_RSA\_PKCS

If the card is not detected automatically click on the "Check Card" button.

Depending on your driver and key you can automatically generate certificates. Most setups require a separate utility to generate a certificate. Make sure it is **RSA2048**

In case no key has been identified you can use the "Create Key" Button.

Autodetection works by having a certificate with the rsa 2048 key with an X509EnhancedKeyUsageExtension OID of 1.3.6.1.5.5.7.3.4 (id\_kp\_emailProtection)

Once you selected a key, make sure to test encryption once to see if en- and decryption work.