Public/private key generation and data decryption

This document will explain how to generate a public/private keypair that can be used to encrypt and decrypt sensitive user information for the MediaDiary application.

What is a public/private key pair?

A public/private keypair is a linked pair of keys that can be used to encrypt and decrypt data. In our case encryption can be done with the 'public' key, this key can be shared with anyone without compromising security. Other people can then use this key to encrypt data so that only the person with the corresponding 'private' key can decrypt it and read the information.

Generating a public/private key pair

For the MediaDiary app we are making use of a tool that is already built into all major operating systems (windows, linux and macOs). This tool is called ssh-keygen, and has to be accessed from the command line.

you can generate a key with the command `ssh-keygen -t rsa -b 4096`

Afterwards you have to specify the location and name of the keypair, although a default is provided.

Doing this two files will be generated. in the above example an `example_key` file and an `example_key.pub` file will be generated. the `.pub` file contains the public key which can be used on the MediaDiary app. The `example_key` file (without .pub) is the private key, you should not share this with anyone, and it should not leave the computer you generated it on, as this reduces the security of the private key.

Making a survey with the public key

When making a survey the public key is necessary, the public key file can be opened with a text editor, then you can simply copy paste the key into the public SSH key field.

Public SSH key

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQDqEQcPqs03pyDawjNOU3vh6Tahw
+hj82Kik/duxk5DJ2O1eMDp932QfxqFal0p9hz11uQMp7e4D7g7+bGoNUvhu
zXaqyS4iQ5rehfqxkRPGbZ3WZZhBxrfQGmmjG1Q3fd1dD2+KNiKhVSye13Lla
XydQWH3qL5nBQpLScz3mBqrbD8n/iNcHFpyxpZB6WNezJtO+yxcPkEx+hAB
C1cSr31C+HMKm/bNHWAQ6ifXe6mmBT3LfA0/UJ563IXMdPeABCsUHQ0NIH
WIcweLLgx5U7Wq+/qZnPws3X15fMfVSnjYoyfpmubY4Kyfly6wCrWWOKly+F
HTw/cTq6Q2yP9O/RBKQ86hFGDU/a8IVn7yZyZdejOTaKP+SElem+RfHkE+2C
m/mjA8gjK/esBkF/hMQTZZqVoXfVApinrkmW7XuMB8SscL+PelvxnsOz9nqSnk
fZAgnFHwfA8GX8EViZcdZFqS9i45bQV7LnBySa1m7xkSR00g9ORvmvQeUwM
Fqlo5sljL4bu3PdWx61Vvg/ivP8KNpcU0Z8S4bkj/7wpD5mchGqjPFCQATGPb+
ZNDrrhHDEeKMBP9okLhODc4Ps9dInMqza6Rm9aqccvrEWoJ1s3psWdQFien8

Make sure to leave no extra spaces or new lines behind the key, this could potentially change the key and mess up encryption.
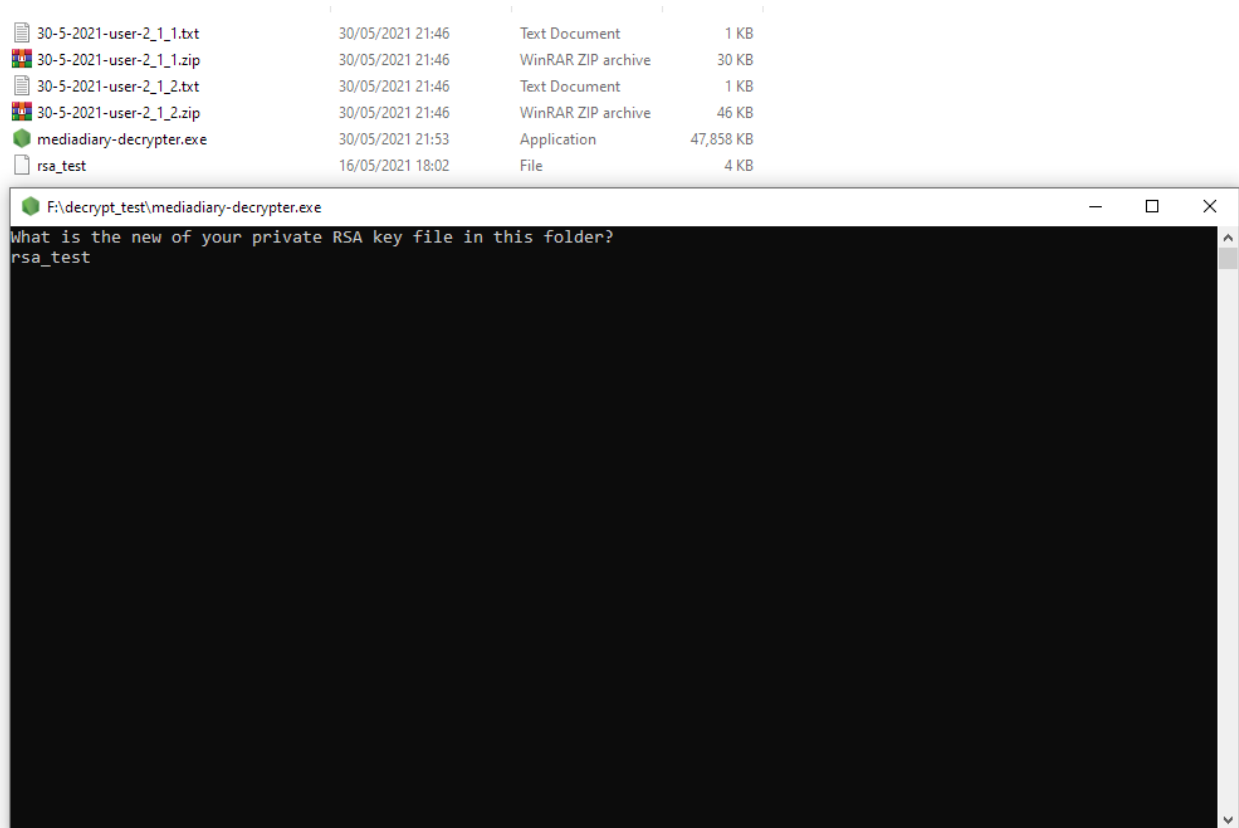
Decrypting survey responses with the private key

When you receive responses you receive named pairs of encrypted zip files and text files containing the encrypted password.

A tool has been created to simplify the decryption of the responses: mediadiary-decrypter. This tool will decrypt the contents of the zip files and place them into corresponding folders:

How to use the mediadiary-decrypter:

1. Place the .zip files and their passwords into a folder

2. Place the mediadiary-decrypter.exe in the same folder

3. Place or copy your private key file into the same folder

4. Run the mediadiary-decrypter.exe

5. Enter the name of your private key file

30-5-2021-user-2_1_1.txt	30/05/2021 21:46	Text Document	1 KB
30-5-2021-user-2_1_1.zip	30/05/2021 21:46	WinRAR ZIP archive	30 KB
30-5-2021-user-2_1_2.txt	30/05/2021 21:46	Text Document	1 KB
30-5-2021-user-2_1_2.zip	30/05/2021 21:46	WinRAR ZIP archive	46 KB
mediadiary-decrypter.exe	30/05/2021 21:53	Application	47,858 KB
rsa_test	16/05/2021 18:02	File	4 KB

```
F:\decrypt_test\mediadiary-decrypter.exe                    —    □    ✕
What is the new of your private RSA key file in this folder?
rsa_test
```

Now the executable will create a folder for each user and date, containing the responses for that user on that day

30-5-2021-user-2	30/05/2021 22:15	File folder	
30-5-2021-user-2_1_1.txt	30/05/2021 21:46	Text Document	1 KB
30-5-2021-user-2_1_1.zip	30/05/2021 21:46	WinRAR ZIP archive	30 KB
30-5-2021-user-2_1_2.txt	30/05/2021 21:46	Text Document	1 KB
30-5-2021-user-2_1_2.zip	30/05/2021 21:46	WinRAR ZIP archive	46 KB
mediadiary-decrypter.exe	30/05/2021 21:53	Application	47,858 KB
rsa_test	16/05/2021 18:02	File	4 KB

30-5-2021-user-2

Name	Date modified	Type	Size
1	30/05/2021 22:15	File folder	
2	30/05/2021 22:15	File folder	