Working with Encrypted Data

In ODK Aggregate

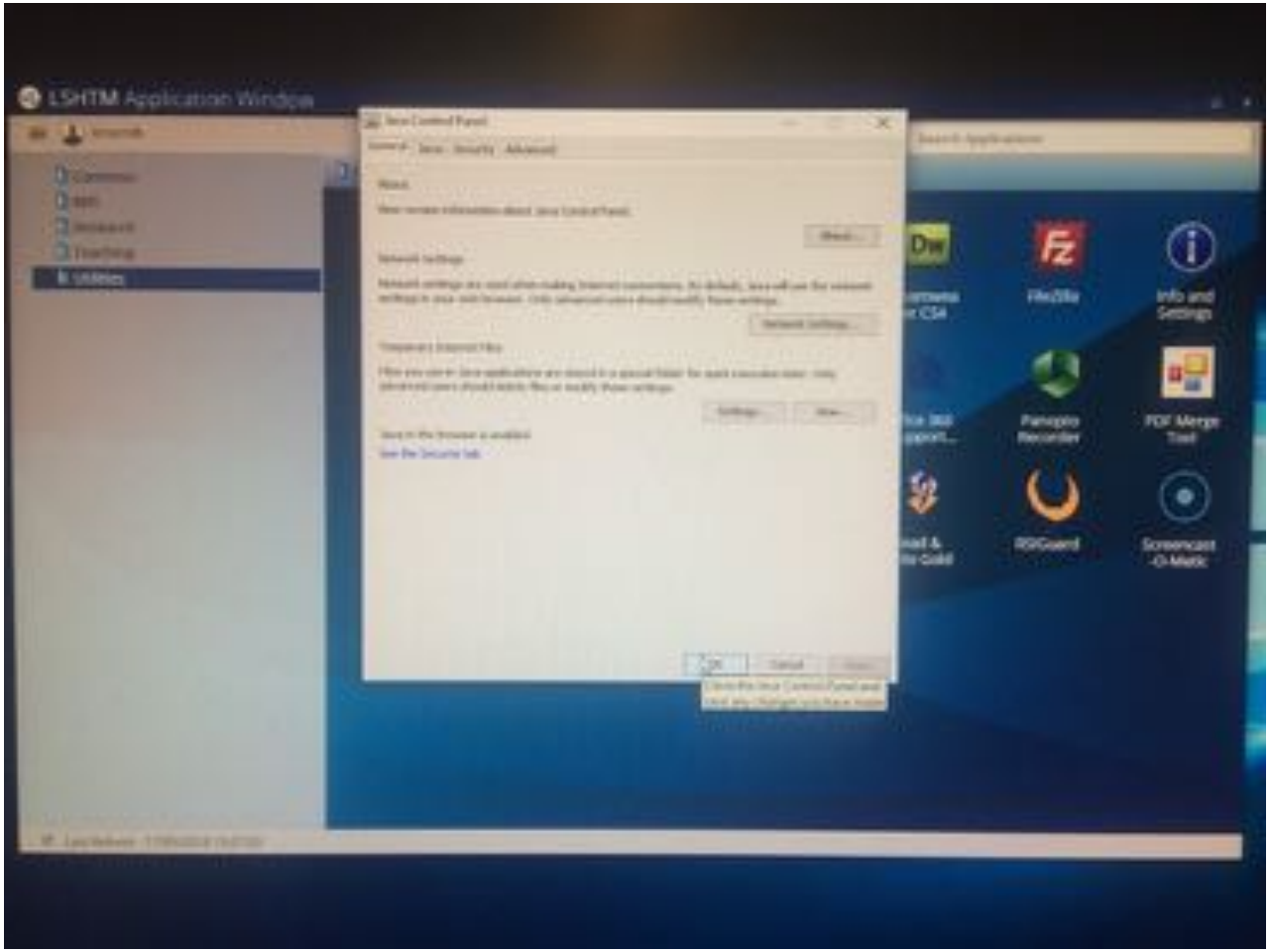
Install Java and Cryptography extensions

In the LSHTM Application Window,
Select ”Utilities”
and double click on the “Java x32”
icon

Install Java and Cryptography extensions

In the LSHTM Application Window, Select ”Utilities”
and double click on the “Java x32” icon
Do not change any settings in the subsequent options, but follow the instructions to update Java and install the cryptography extensions.

i.e. just keep pressing ‘ok’



Obtain a pair of encryption keys

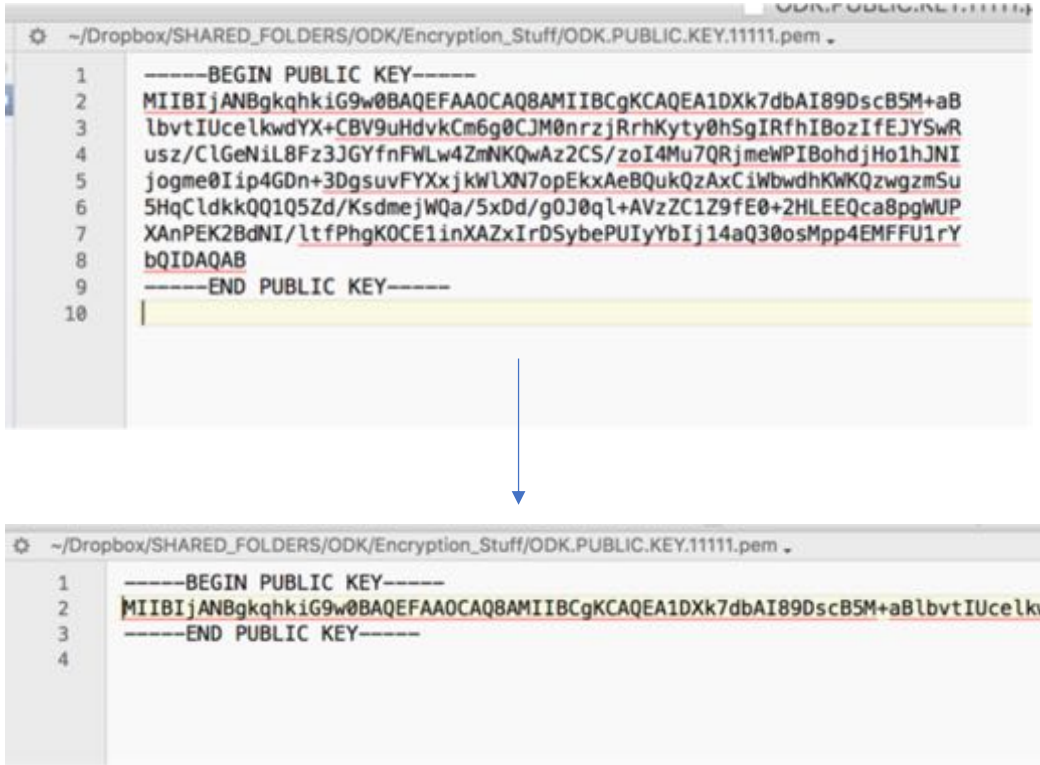
- You can create a pair of keys for encryption using the open source openSSL software
  - https://www.openssl.org

- We can also provide keys and will keep a copy of your keys in our locked safe.
- Email odk@lshtm.ac.uk
- We will send you a pair of asymmetric encryption keys (either via whatsapp or face to face, not by email)

- The Public Key is used for encryption and is included in your ODK forms
- The Private Key is used for decryption
  - It should be kept on a USB thumb drive in a locked room, safe or filing cabinet.

Copy the public key in to your ODK form

- The Public Key is a text file that looks something like this if you open it in textedit or similar
- To use the public key with ODK, you first need to remove the line breaks in this file to get the key on one line
- Copy the single-line version of the key to your clipboard

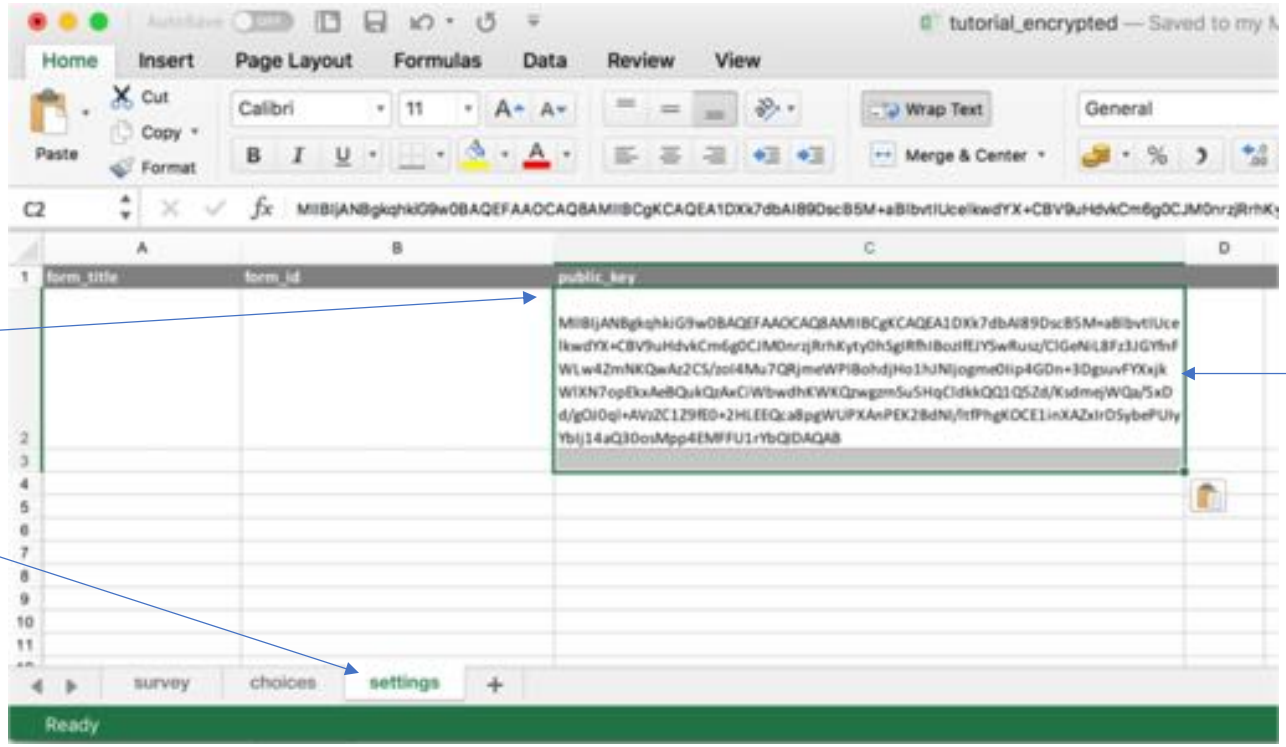


Copy the public key in to your ODK form

- Paste the single-line version of the key in to your ODK form Excel file
- The key needs to go on a tab called ‘settings’ and in a column called ‘public_key’
- Both names are case sensitive and should be lower case.

‘public_key’ column

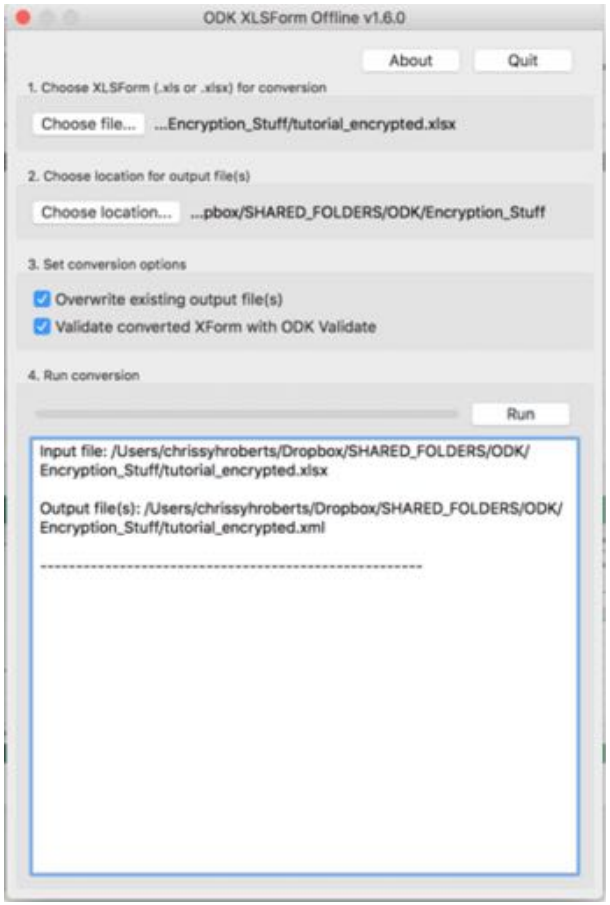
‘settings’ tab



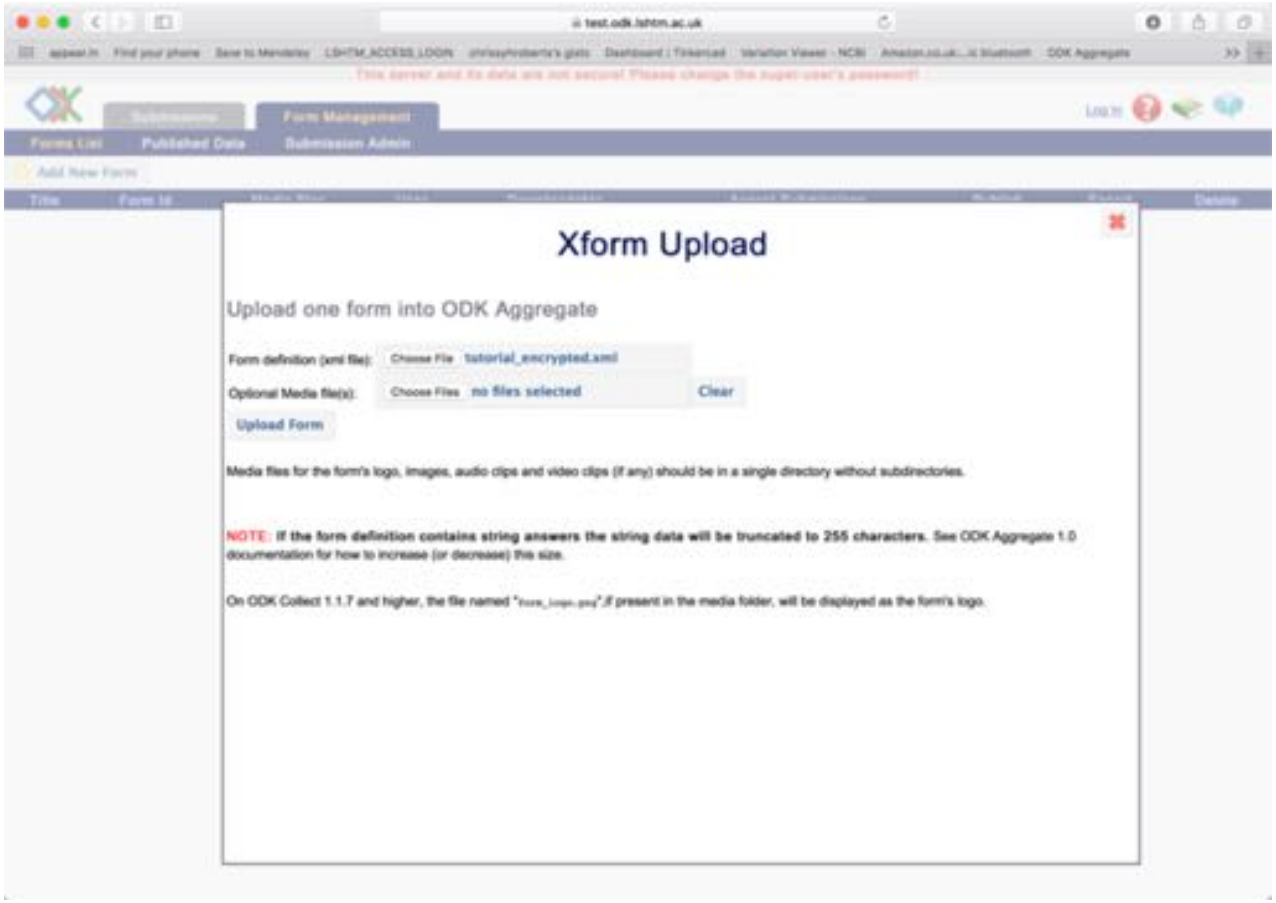
Public key

Convert your form to XML

- Use ODK XLSForm Offline, available here : https://github.com/opendatakit/xlsform-offline/releases



Upload the XML file to your server



Connect your Android device to the server

Get the blank form from the server, then fill and submit a test form

The data in the submissions view is now encrypted

Download ODK Briefcase

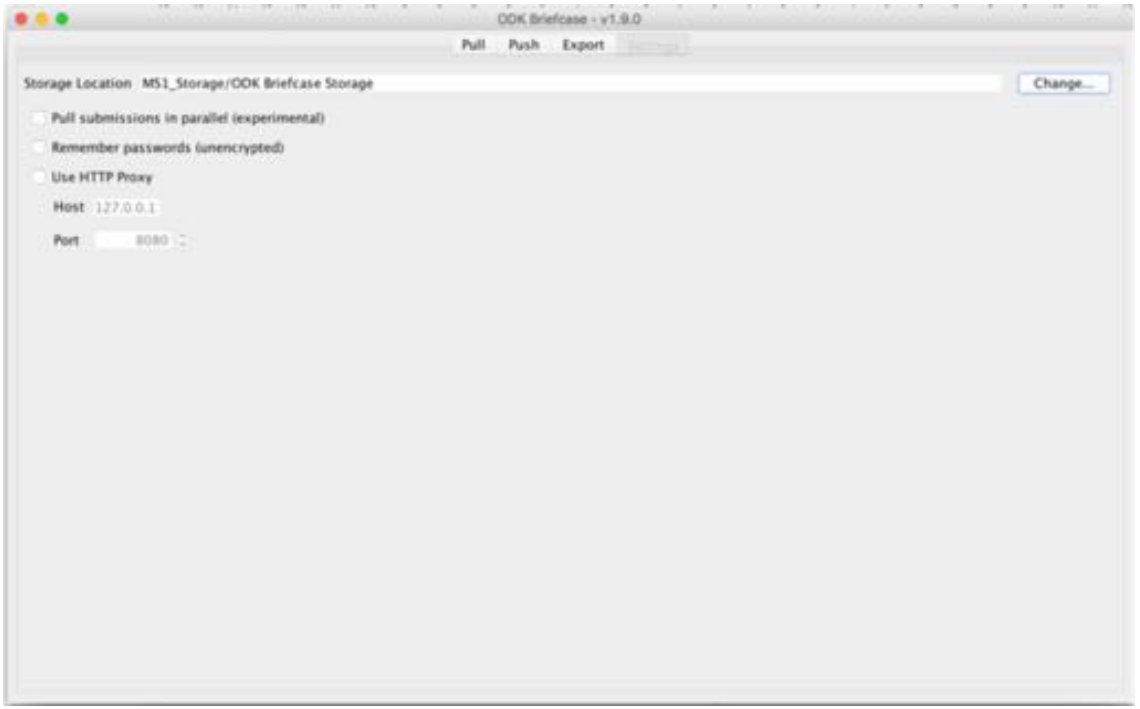
https://github.com/opendatakit/briefcase/releases

Copy the latest release of ”ODK Briefcase vx.x.x.jar” file to a folder on your hard drive

Double click to open the ODK Briefcase Software.

You may have to allow security privileges on some computers.

On Mac OS you may need to go to “system preferences > security & privacy” then unlock the preference pane and click ‘Anywhere’ under the ”Allow apps downloaded from” section.

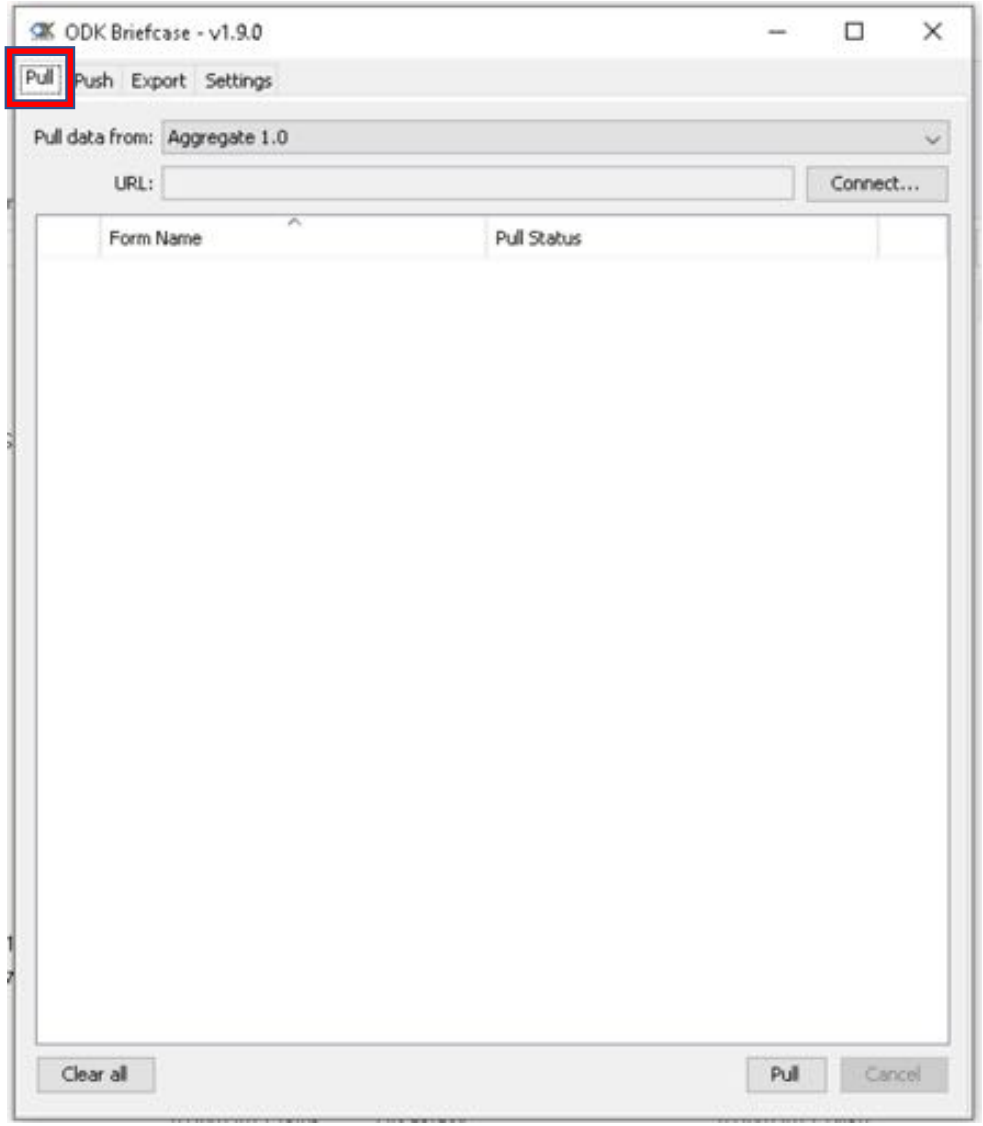


ODK Briefcase

Set the download folder

This is the folder in which all of your data will be saved and decrypted

It should not be a folder on a filesharing system such as Dropbox, nor a folder which is automatically backed up to an unsecured drive.



Connect to the ODK aggregate server

Click the ‘connect’ button

ODK Briefcase

Connect to the ODK aggregate server

Change the url to match the location of your server

Enter the user name and password of an administrator account and press the ‘Connect’ button.

IMPORTANT

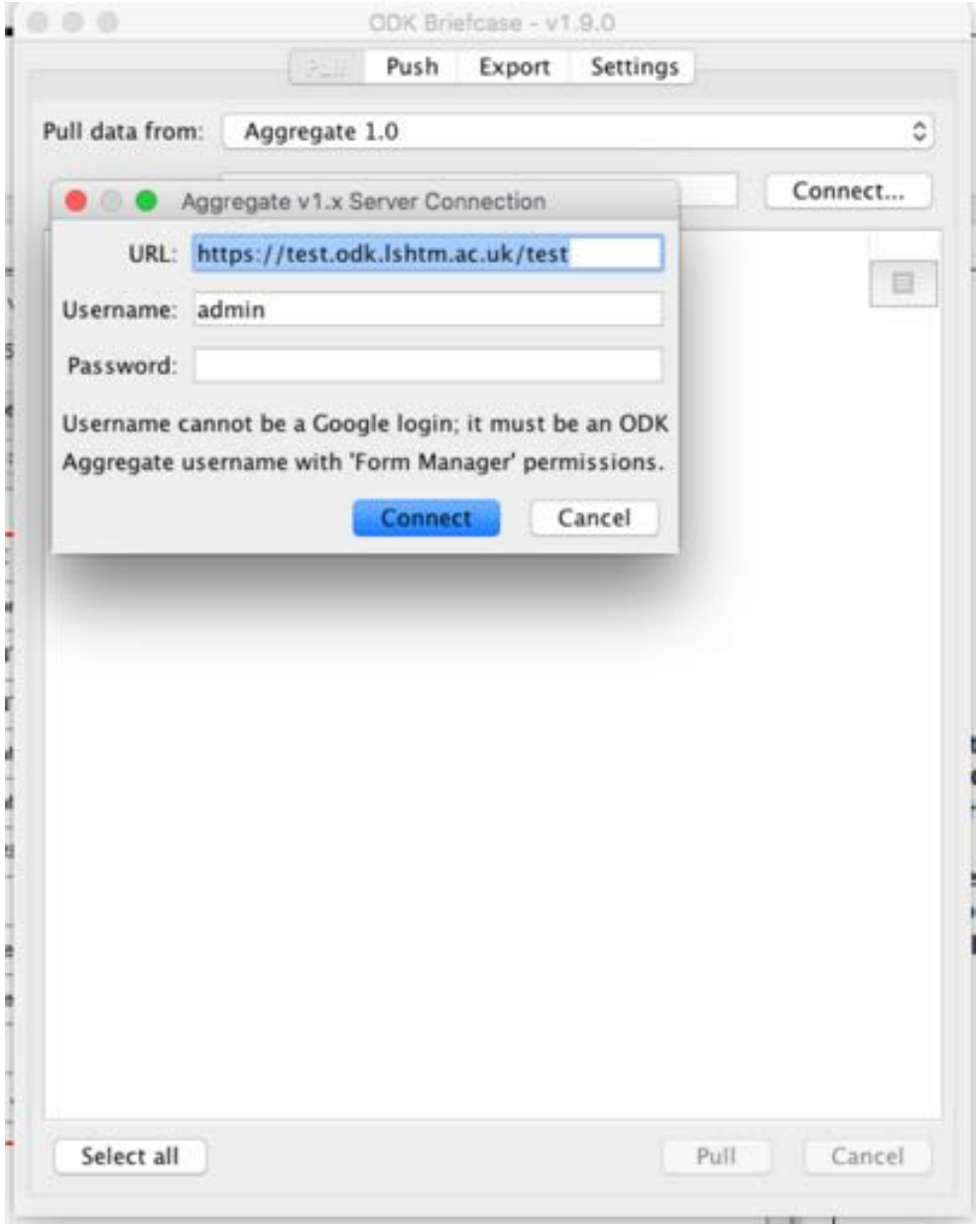
The URL needs to include the main folder for the data. This folder’s name is the same as your server’s name

i.e. if your url is

https://test.odk.lshtm.ac.uk

then the url you enter in ODK Briefcase should be

https://test.odk.lshtm.ac.uk/test

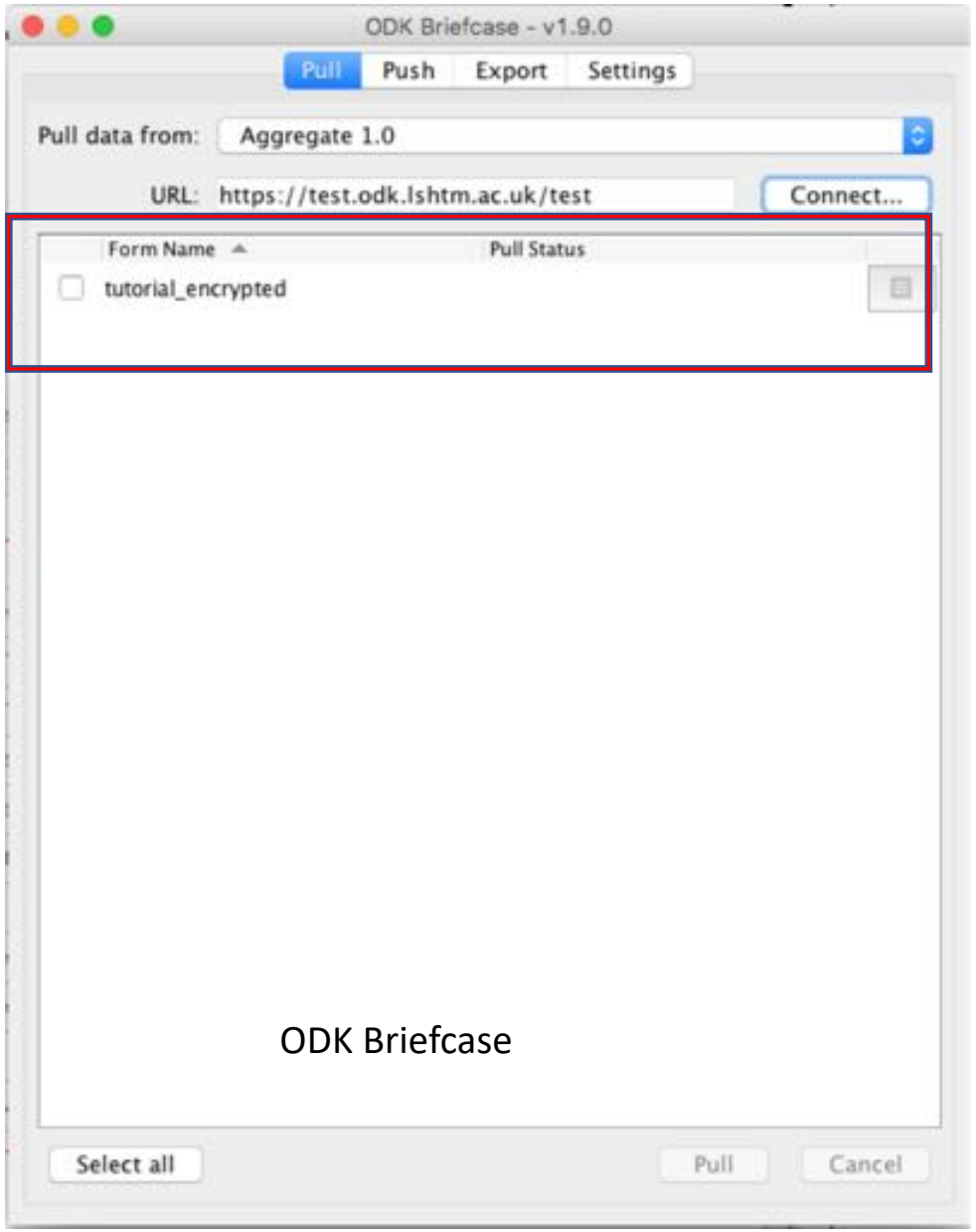


Pull data from the ODK aggregate server

ODK Briefcase will now list all the forms that you can copy from the server on to your machine. This action is called a ‘pull’.

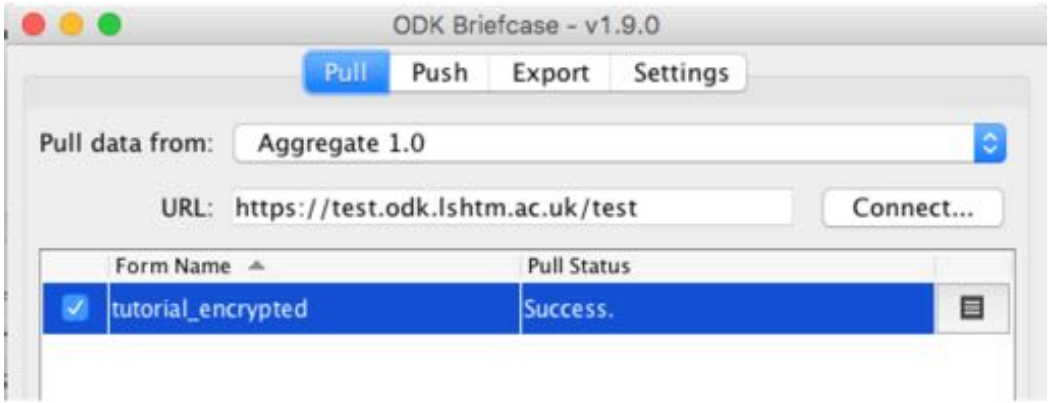
Tick the box next to the forms you want to pull or press the ‘select all’ button

Press the ‘Pull’ button to pull your data in to the folder you specified earlier.



ODK Briefcase

Pull data from the ODK aggregate server



All successfulls pulls will be flagged 'success' in the "Pull Status" column.

In your download folder you will now find this directory structure

There will be one uuid folder for each form you submitted to the server.

Inside each of these folders you will find encrypted files

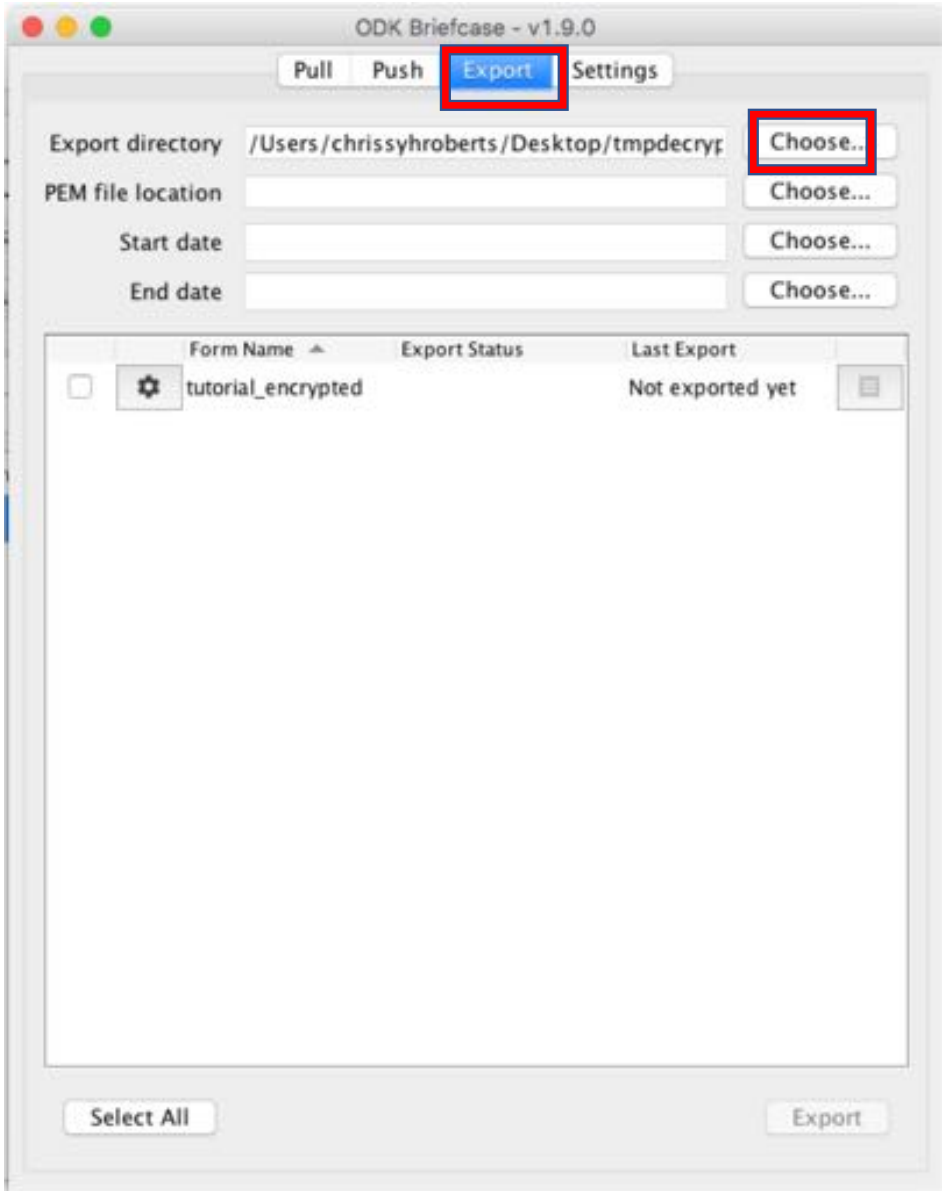
Download Folder
> ODK Briefcase Storage
>forms
>tutorial_encrypted
>instances
>uuid….

Export and decrypt the data from Briefcase

Click the ‘export’ tab

Click the ‘choose’ button next to ”Export Directory” and choose a directory in which to export the decrypted data

This folder should not be on Dropbox etc., nor on folder backed up to enencrypted media.



Select the location of the private key

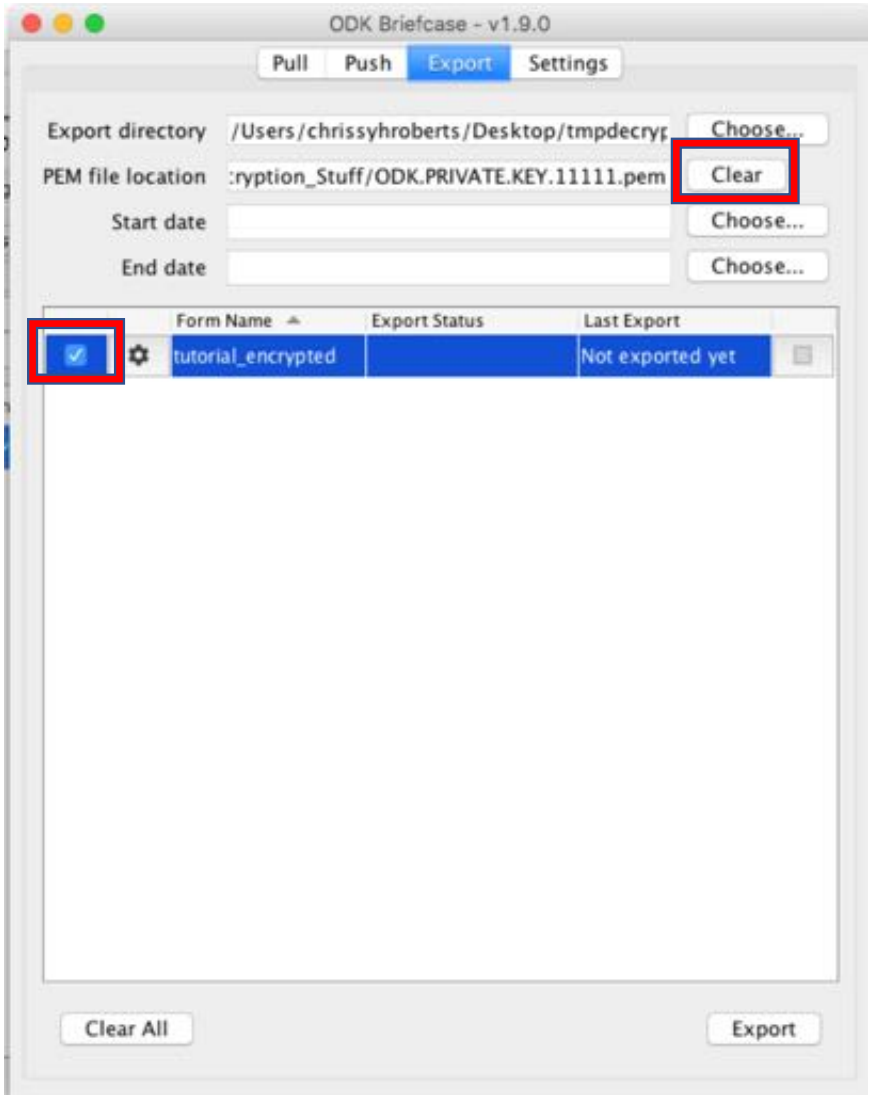
Click the ‘export’ tab

Click the ‘choose’ button next to “PEM File location”

Find the private decryption key

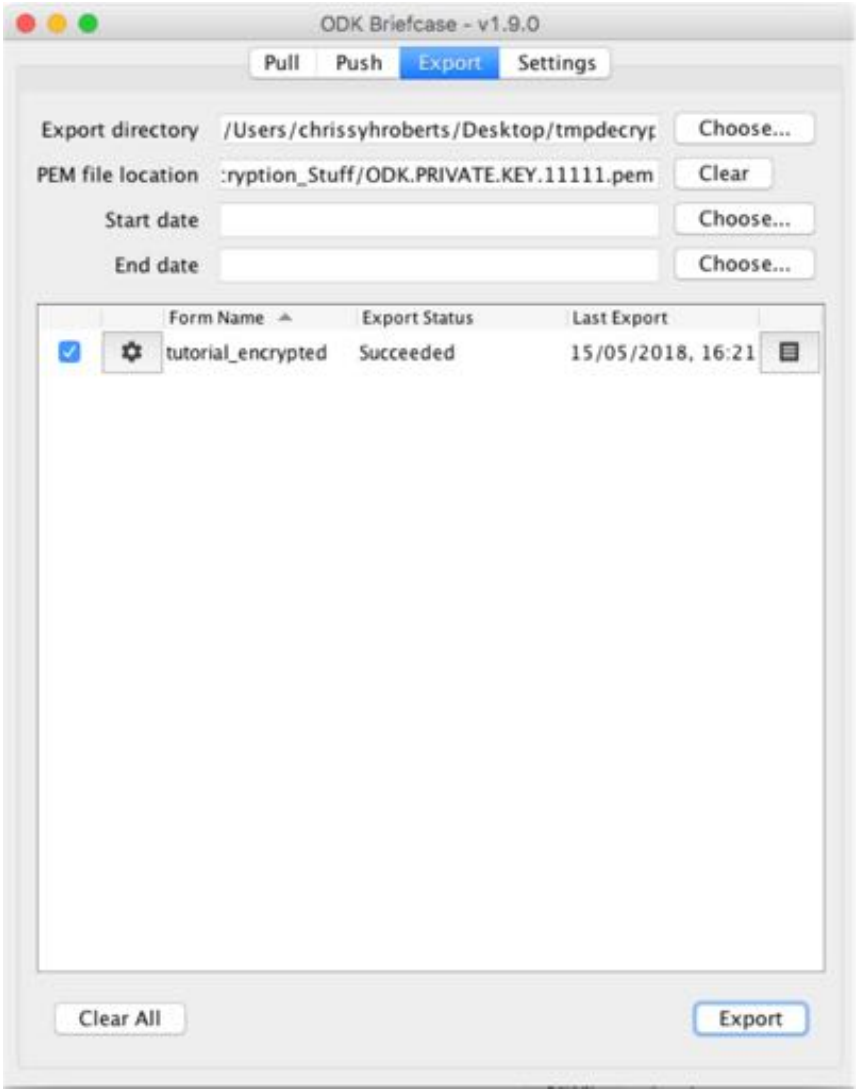
Select the forms you wish to decrypt

Press ‘Export’



Export and decrypt the data from Briefcase

Export Status will change to ‘Succeeded’ if everything went well.



Export and decrypt the data from Briefcase

In the export directory you will find a new folder called

‘decrypted’

Inside should be a csv file, which can be opened by R, STATA, Excel or text editors.

If there are photos, videos or sound recordings in your form, there will be a ‘media’ folder which contains these. The file paths to these media files will be updated automatically in the CSV document.