

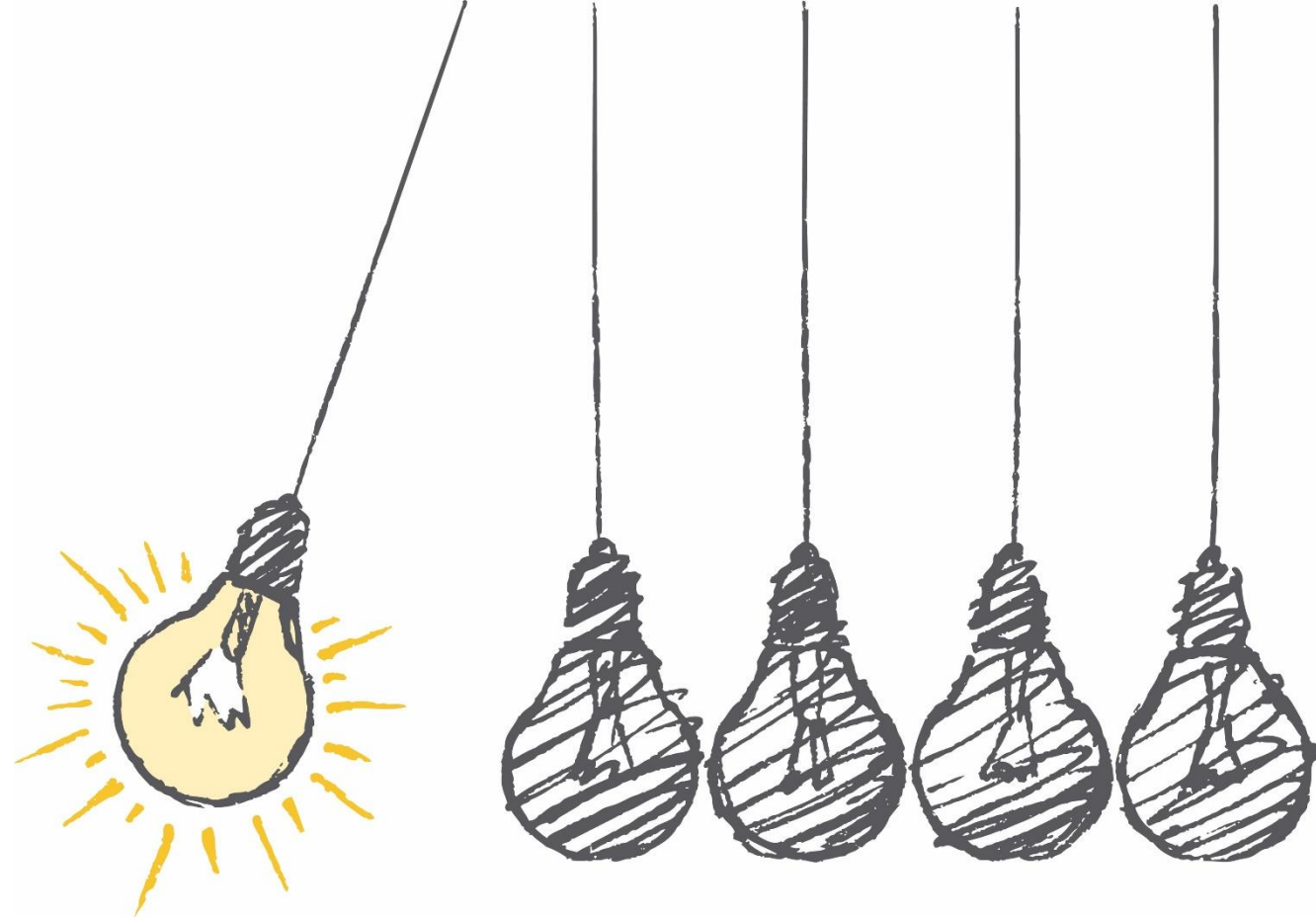
DIME

analytics

Encryption on SurveyCTO

DIME Bootcamp – Data Security

bit.ly/dime-bootcamp



WORLD BANK GROUP



Norad

Encryption on SurveyCTO



Encrypting a form on SurveyCTO to ensure private data remains private

Only authorized team members have access to the data

Can make specific fields publishable to those who don't have the encryption



SurveyCTO uses public-private key pair (asymmetric encryption) to encrypt form data



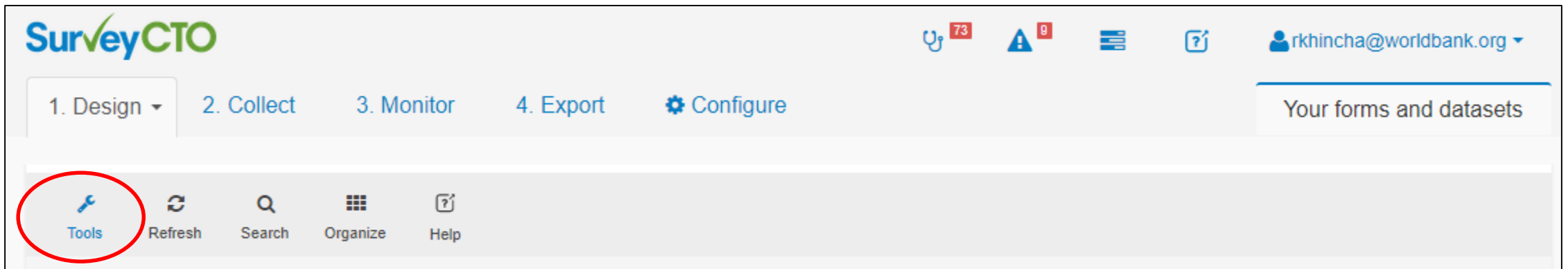
We will go through a step-by-step guide for how to create and use an encryption key pair on SurveyCTO

Step 1: Generate public-private key pair



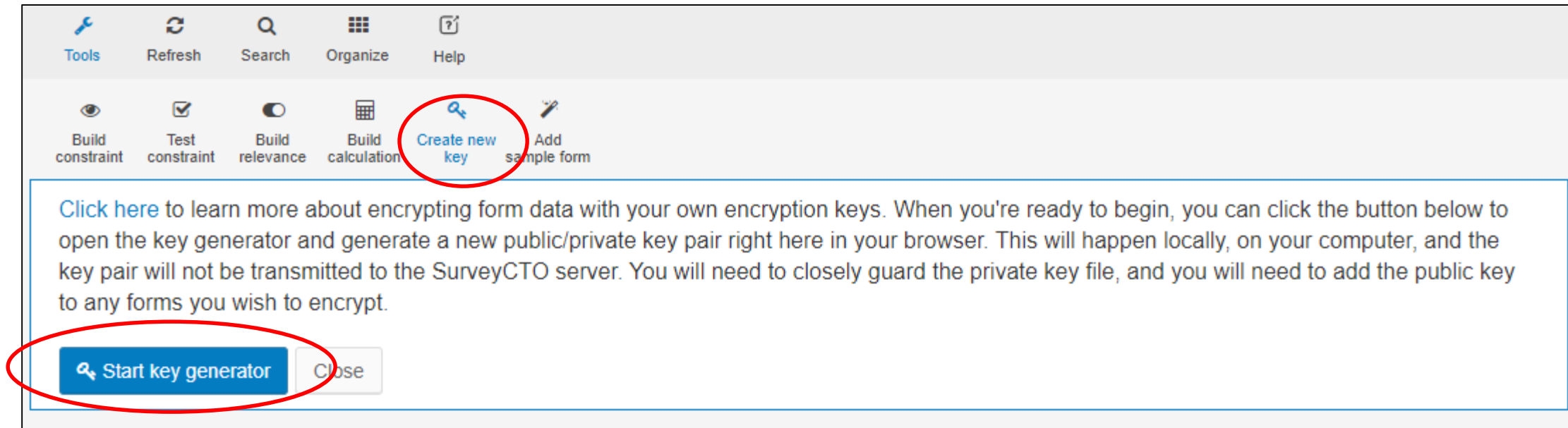
Generate public-private key pair

- Log-in to survey.wb.surveycto.com
 - *Your WB email ID should be registered on the server*
- On the *Design* tab, select *Tools*



Generate public-private key pair (cont.)

- Select *Create new key*
- Click on *Start key generator*



Generate public-private key pair (cont.)

- Enter a name for the private key

Step 1. Choose a name for your private key

Please enter a short name for your encryption key. This will be used to name the encryption key files that you will download in the following steps.

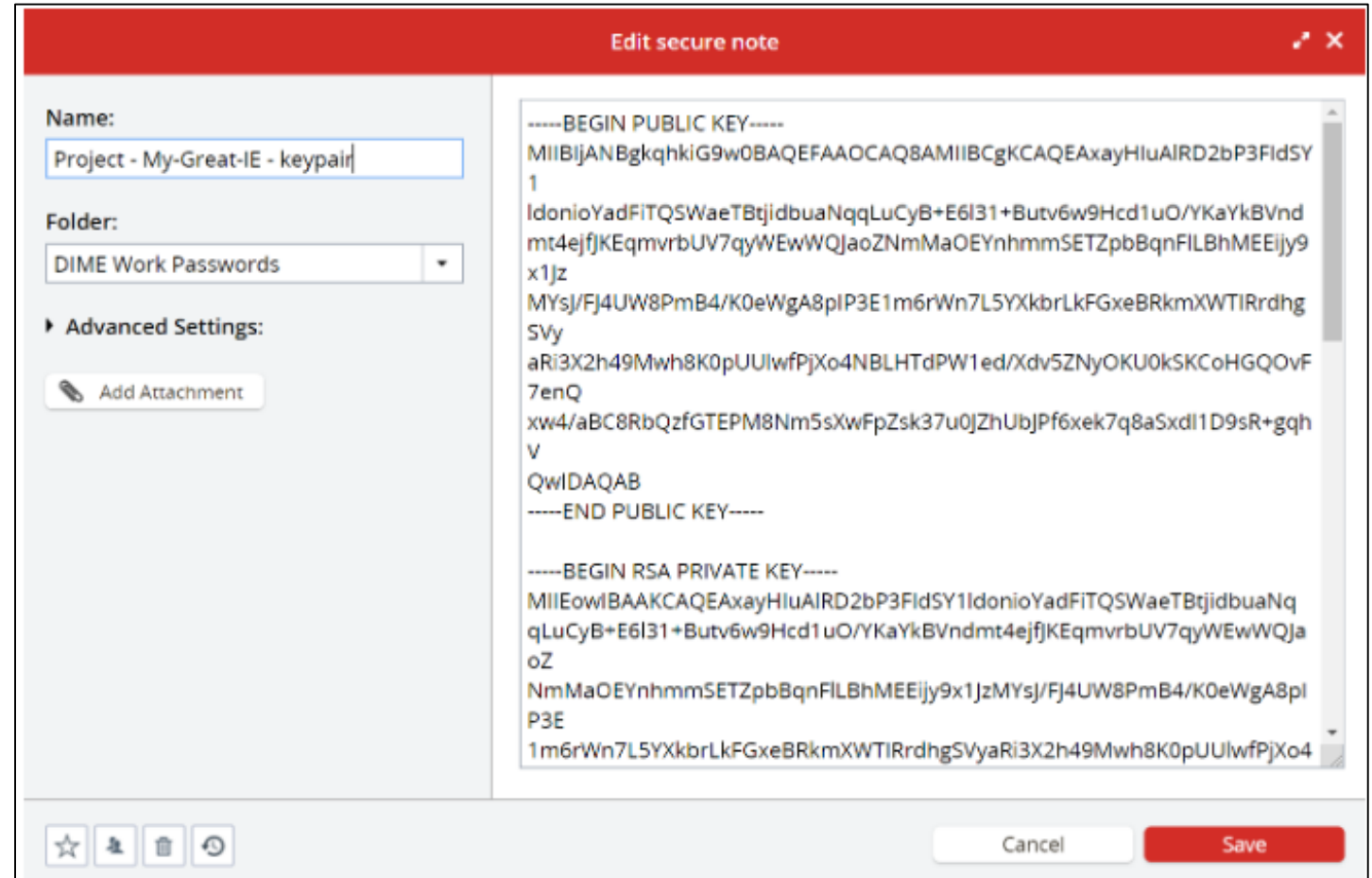
Key name:

[→ Next](#)

- Download the private key file & the public key file
- You will find 2 *.pem* files saved on your system – this is your public-private key pair

Securely store the key-pair on LastPass

- Create a new *Secure Note* on LastPass
- Copy-paste the contents of each file
 - *<filename>_Public.pem*
 - *<filename>_PRIVATEDONOTSHARE.pem*
- Delete the files from your system



Step 2: Configure a survey form for encryption



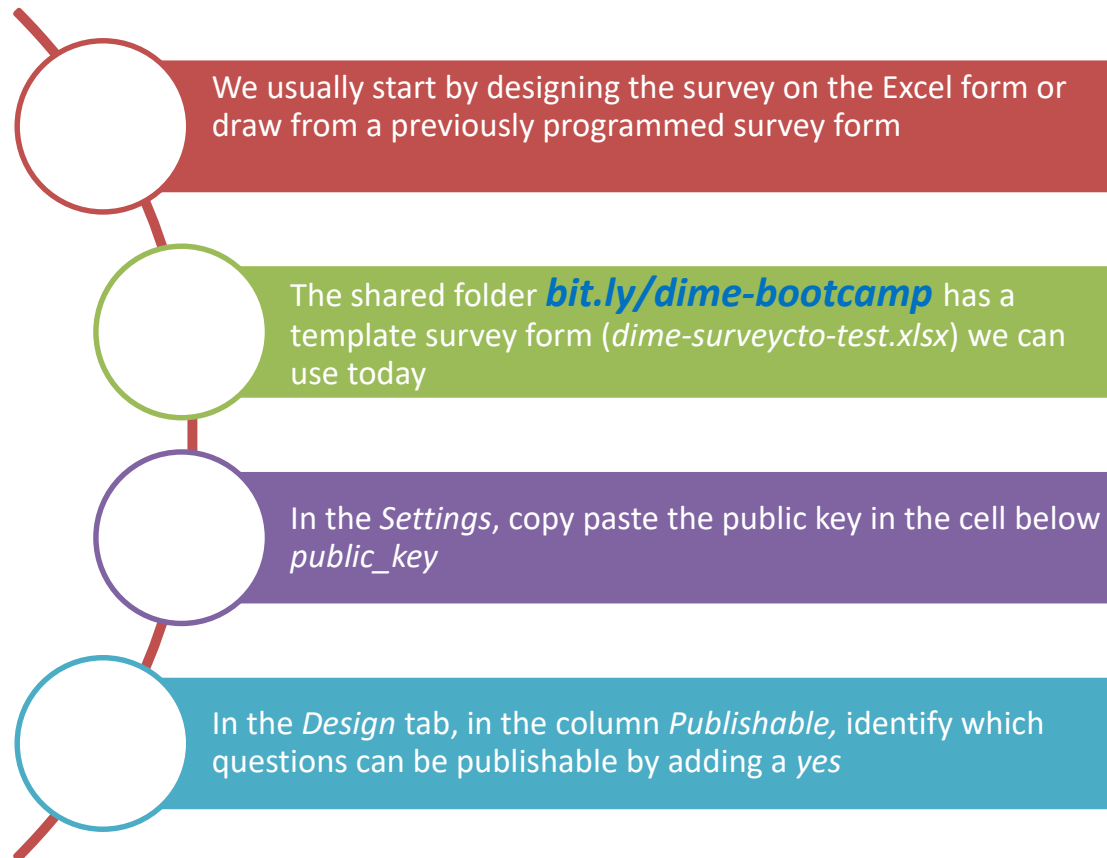
Publishable vs Non publishable fields

- Publishable field – accessible to those with access to server
- Non-Publishable field/question – accessible to those with access to server AND private key

Why make questions publishable?

- Questions marked as publishable can be downloaded without the private key
- Helps ensure no-PII data is shared with those without key (and not on the IRB)
- Examples
 - Sharing only parts of the data with government counterparts or survey firms
 - Quick check for duplicates on unique IDs

Encrypting using an Excel survey form on Excel



public_key
MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvljjlq8PJbtDIQtnJYEM5t6x9cexdgqf1swSl6xJPopjm2Bvq2yLHqs7N/asJwQLFH82dY1ZU62zwb14Od0C7Y9w+ygDinw0BrRH3kR1RAJMw/cL5+JlHzRCRyAzCLo2p329xel7R/JCe454AuA8rmskThmYTG2dbbA4z3Czfo+UvrSq6Ua5Ux9CC4ZQnw2iOYD1N/GinhoMnqN/91+Lvztmf6vNG7nQmo0gP3L85xV2HFCq75ryK3nZjIZVo3YTz9v+7+bzzhW6LBii83BhuS3RabHvjPa8UlsjC3Q2tjuzo7iY93UyX1OZHvGzMvMjpE73ssdL/RaOsBuqfWTgGQIDAQAB

Remember...



Only new forms can be encrypted (A form can not be encrypted once it's deployed)



SurveyCTO will accept any key shorter than 1024 characters which starts with -----BEGIN PUBLIC KEY ----- and ends with -----END PUBLIC KEY -----



It is easy to identify if one is copying the private key instead of the public key (as the private key is longer than 1024 characters)



The private-public key pair is unique



Any error in copy pasting the key will result in lack of access to all data on the form



ALWAYS test a dummy data entry each time you create a form

Step 3: Downloading data collected using an encrypted survey form



Different ways to download data

- Data can be downloaded using
 - The server online (i.e. on SurveyCTO website)
 - SurveyCTO Desktop
- You can download just the publishable fields
 - For instance, when you need to quickly share de-identified data with government officials

Downloading data from the browser

For publishable data

- Export tab → Locate the form → Download form data
- Select *Publishable fields only*
- Download the data

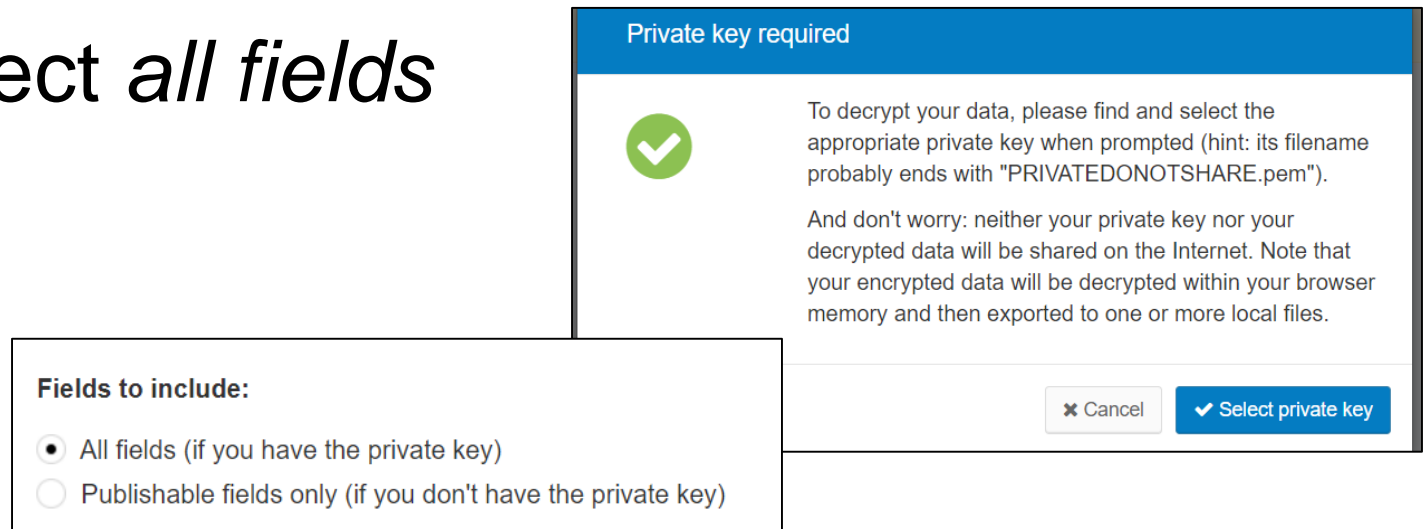
Fields to include:

- ☐ All fields (if you have the private key)
- ☒ Publishable fields only (if you don't have the private key)

Downloading data from the browser

For both publishable & non-publishable data download

- Copy paste private key into a .txt file and save on desktop
- Log in to the server. survey.wb.surveyc.to.com
- Click on the *Export* tab → Locate the form
- Click *Download* → Select *all fields*
- Upload the private key
- Download the data
- Delete the key file



The image shows two overlapping dialog boxes from a web application. The background dialog box is titled "Private key required" and features a green checkmark icon. It contains text explaining that a private key is needed to decrypt data and that the data will be decrypted within the browser's memory. It also includes "Cancel" and "Select private key" buttons. The foreground dialog box is titled "Fields to include:" and contains two radio button options: "All fields (if you have the private key)" which is selected, and "Publishable fields only (if you don't have the private key)".

Private key required

✓

To decrypt your data, please find and select the appropriate private key when prompted (hint: its filename probably ends with "PRIVATEDONOTSHARE.pem").

And don't worry: neither your private key nor your decrypted data will be shared on the Internet. Note that your encrypted data will be decrypted within your browser memory and then exported to one or more local files.

✕ Cancel ✓ Select private key

Fields to include:

☒ All fields (if you have the private key)

☐ Publishable fields only (if you don't have the private key)

Remember...

Always test with one dummy data entry to ensure encryption is set up correctly

Always delete the private key file once used

Just copy + paste (do not cut + paste) the public or private key from LastPass

Thank you!

Questions?

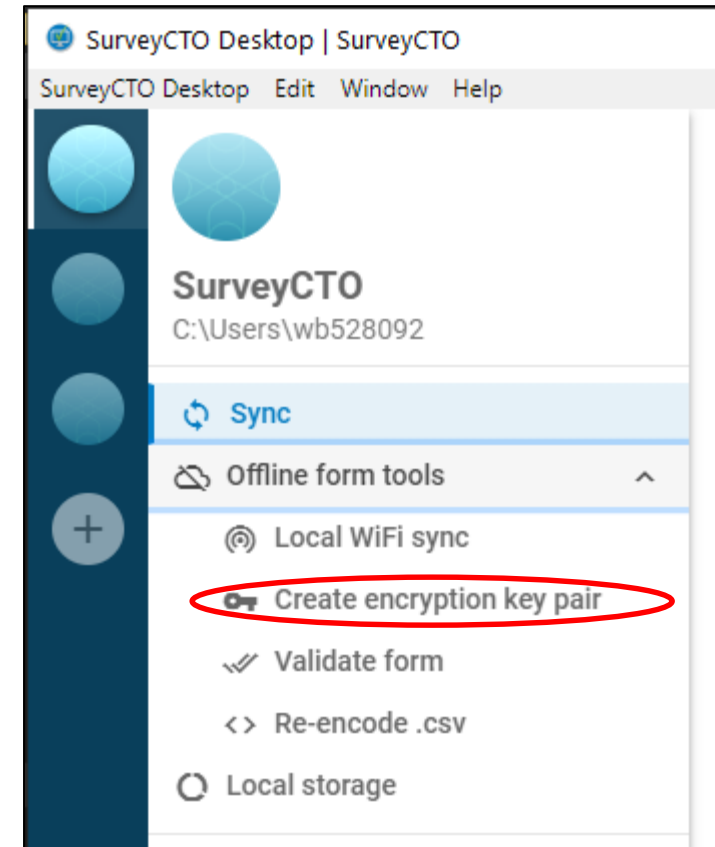


APPENDIX: Creating key pair using SurveyCTO Desktop



Using SurveyCTO Desktop

- You can also create a key pair using SurveyCTO Desktop
- Select *Offline form tools* → *Create encryption key pair*




Appendix: Configuring an encrypted survey form using the form designer



Creating an encrypted survey form (cont.)

Start new form - Step 1

 Help

→ Next

Get started by giving your new form a title and unique ID, then click *Next* to continue.

Form title:

Enter the form's title, as it should appear to users. You can change it later.

Form ID:

Enter a short, unique ID for this form. It cannot include spaces or punctuation and you cannot change it later.

☐ OFF Use a sample form as your starting point?

☒ ON **Advanced options**

☒ Do you want this form's data to be encrypted?

☐ Auto-generate fields necessary for pre-loading data?

Cancel

→ Next

Start a new form on the *Design* tab of the console



Turn *Advanced options* ON



Select the encryption option



Click *Next*

Creating an encrypted survey form (cont.)

Start new form - Step 2: Configure encryption ?

Help Back Next

To encrypt your form data, you will need your own encryption key, which you can get from the *Tools...Create new key* option at the very top of this "Your forms" section. [Click here to learn more...](#)

☐ Upload public key
☒ Paste public key text

Paste public key here:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxayHluAIRD2bP3FIdSY1
ldonioYadFiTQSWaeTBtiidbuaNqqLuCyB+E6l31+Butv6w9Hcd1uO/YKaYkBVnd
mt4ejfJKEgmvrUUV7qyWEwWQJaoZNmMaOEYnhmmSETZpbBqnFILBhMEEijv9x1Jz
MYsJ/FJ4UW8PmB4/K0eWgA8pIP3E1m6rWn7L5YXkbrLkFGxeBRkmXWTIRrdhgSVy
aRi3X2h49Mwh8K0pUUIwfPiXo4NBLHTdPW1ed/Xdv5ZNyOKU0kSKCoHGQOvF7enQ
xw4/aBC8RbQzfGTEPM8Nm5sXwFpZsk37u0JZhUbJPf6xek7q8aSxd1D9sR+gqhV
QwIDAQAB
-----END PUBLIC KEY-----
```

Cancel Back Next

Copy the public key from
your LastPass note and
paste it in the key text



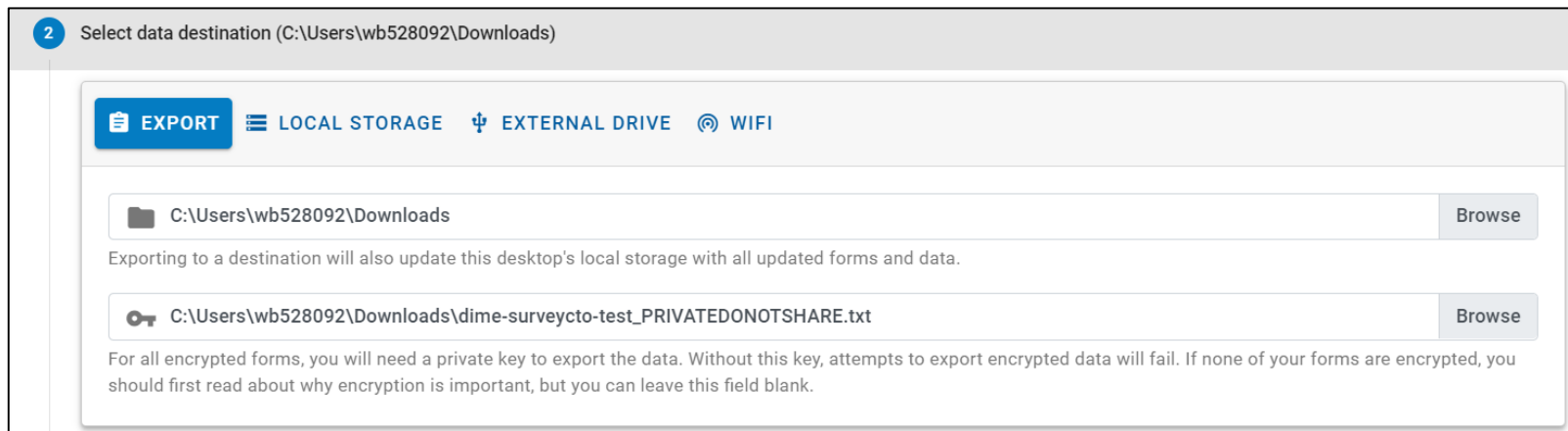
Make sure to include the
-----BEGIN PUBLIC KEY -----
&
-----END PUBLIC KEY -----
text

APPENDIX: Downloading encrypted data using SurveyCTO Desktop



Downloading data using SurveyCTO Desktop

- Copy paste private key into a .txt file and save on desktop
- Open SurveyCTO Desktop
- Add file path for
 - Where to download data
 - Where you saved the private key
- Download the data
- Delete the private key file



The screenshot shows the 'Select data destination' dialog box in SurveyCTO Desktop. The title bar indicates the current step is '2 Select data destination (C:\Users\wb528092\Downloads)'. The dialog has a tabbed interface with 'EXPORT' selected, and other tabs for 'LOCAL STORAGE', 'EXTERNAL DRIVE', and 'WIFI'. Under the 'EXPORT' tab, there are two input fields. The first field shows the path 'C:\Users\wb528092\Downloads' with a 'Browse' button to its right. Below this field is a note: 'Exporting to a destination will also update this desktop's local storage with all updated forms and data.' The second field shows the path 'C:\Users\wb528092\Downloads\dime-surveycto-test_PRIVATEDONOTSHARE.txt' with a 'Browse' button to its right. Below this field is a detailed note: 'For all encrypted forms, you will need a private key to export the data. Without this key, attempts to export encrypted data will fail. If none of your forms are encrypted, you should first read about why encryption is important, but you can leave this field blank.'