DIME
analytics

Encryption on SurveyCTO

DIME Continuing Education

Materials - https://bit.ly/dime-ce-scto
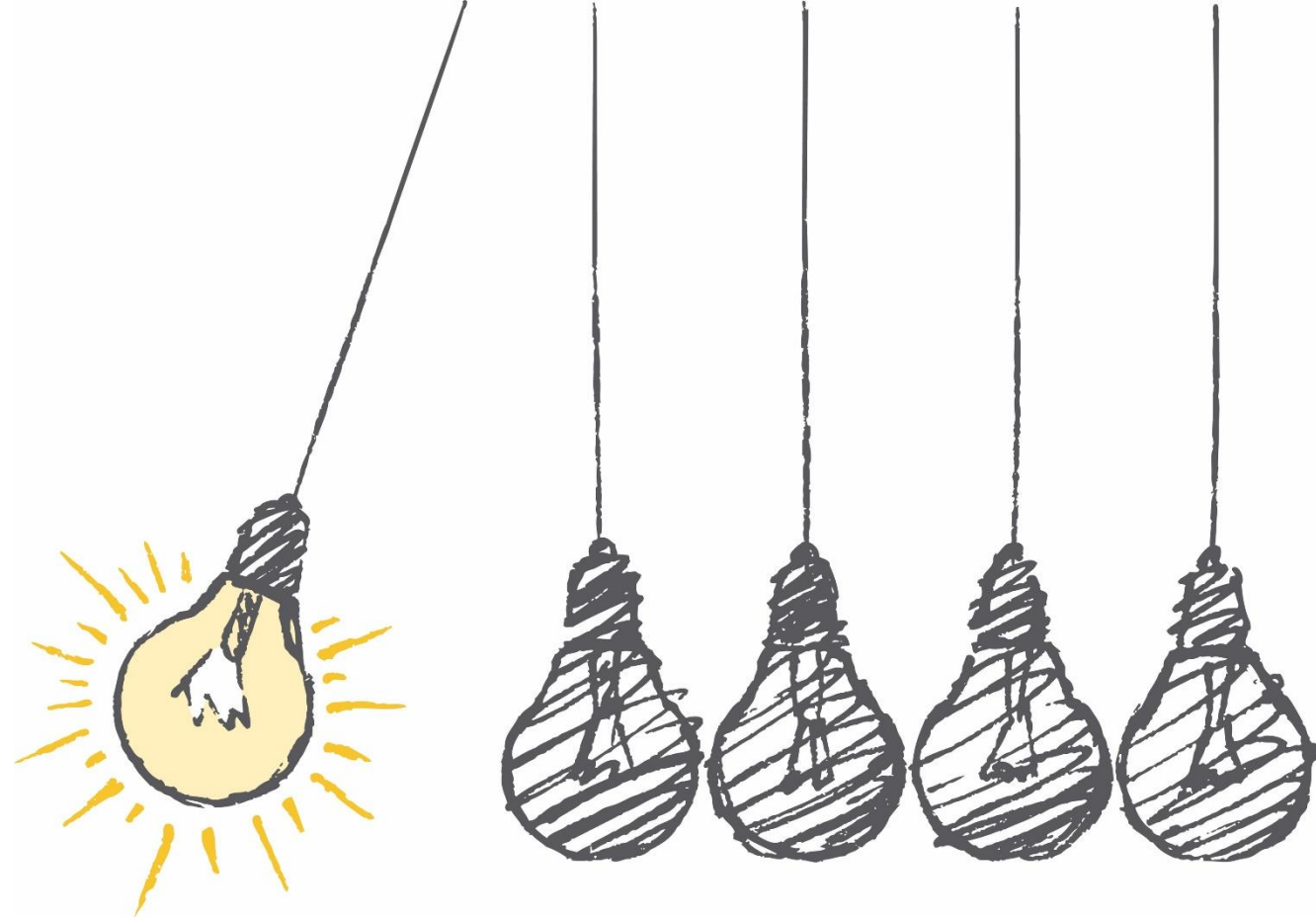
WORLD BANK GROUP   UKaid from the British people   Norad

Encryption

ENCRYPTION IS A METHOD OF PROTECTING DATA FROM PEOPLE YOU DON'T WANT TO SEE IT.

YOU HAVE A MESSAGE, YOU ENCODE IT USING A SECRET CIPHER, AND ONLY OTHER PEOPLE WITH THE CIPHER CAN READ IT. ANYONE ELSE JUST SEES GIBBERISH.

Password managers

- A safe for all your passwords and keys
- Only need to remember **one password**
- Can be used to securely share passwords
- Examples: LastPass, Bitwarden
- World Bank has free subscription to LastPass premium

LastPass •••|

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

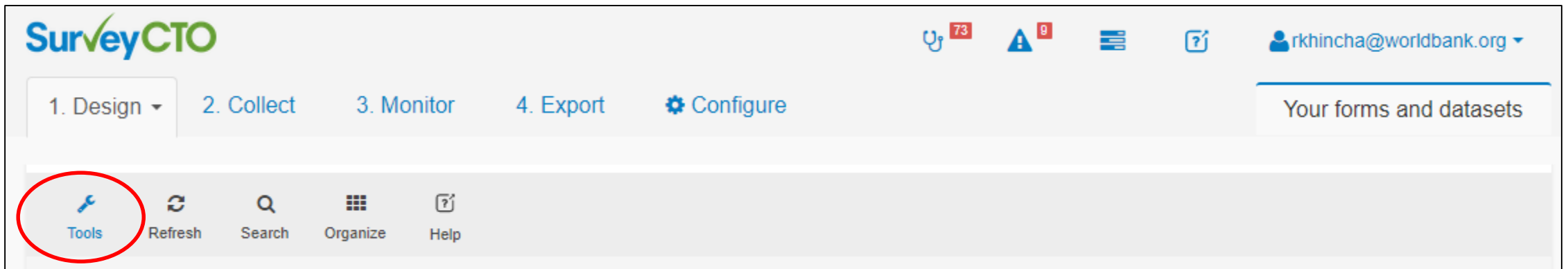SurveyCTO uses public-private key pair (asymmetric encryption) to encrypt form data

We will go through a step-by-step guide for how to create and use an encryption key pair on SurveyCTO
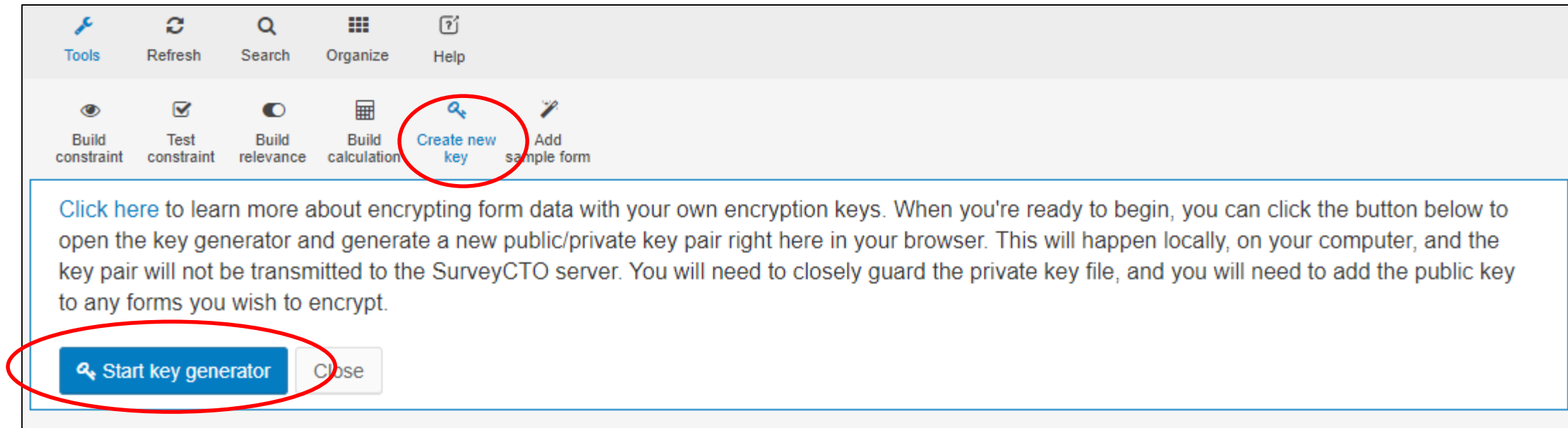
Step 1: Generate public-private key pair

Generate public-private key pair

- Log-in to a SurveyCTO server (such as survey.wb.surveycto.com)
- 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.
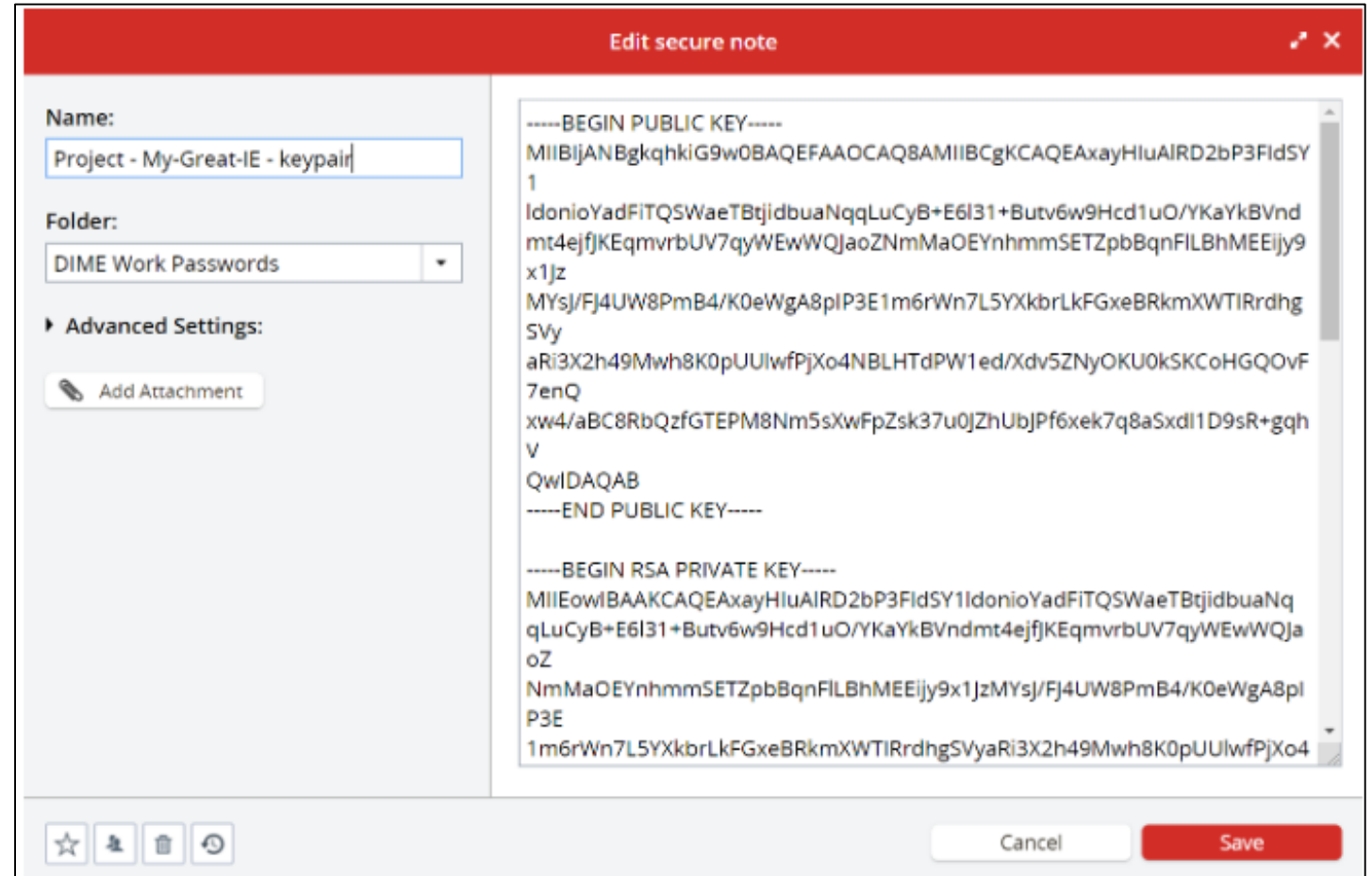
Key name:

bootcamp_test

➜ 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*
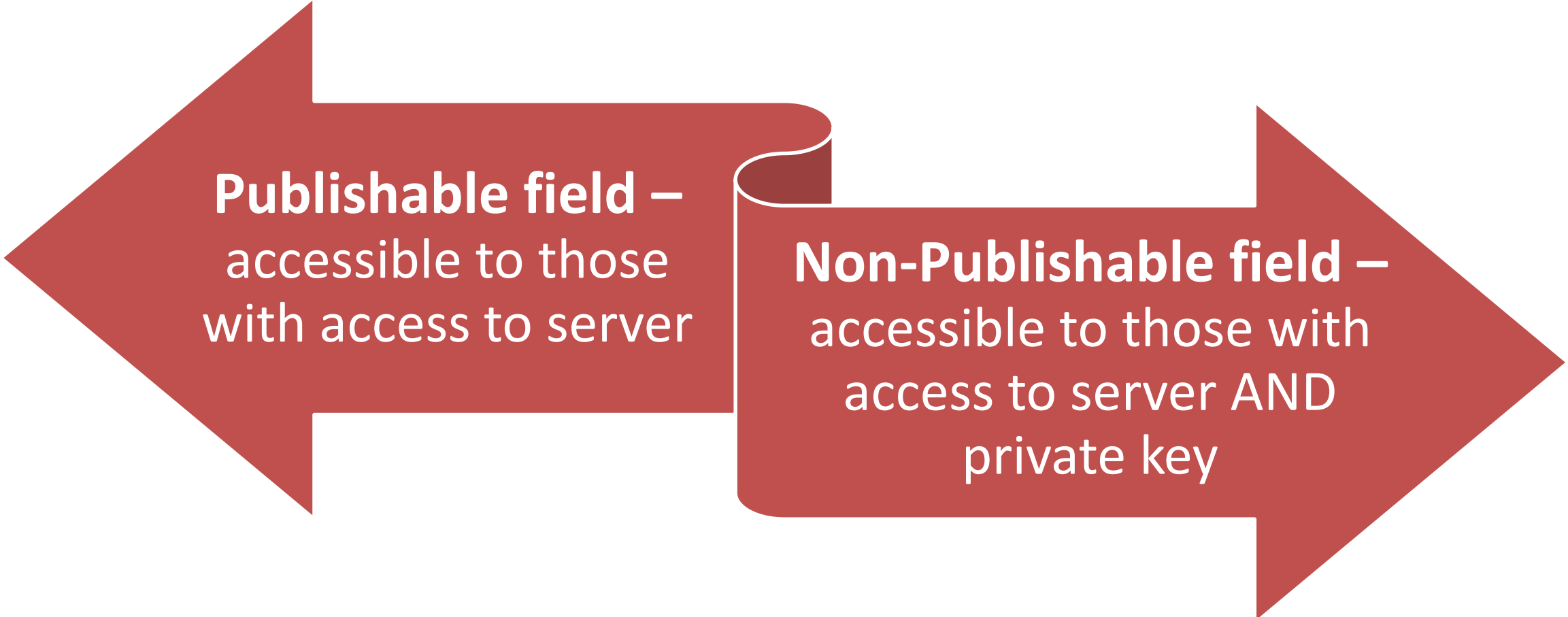 - *<filename>_PRIVATEDONOTSHARE.pem*

- 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 – 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)
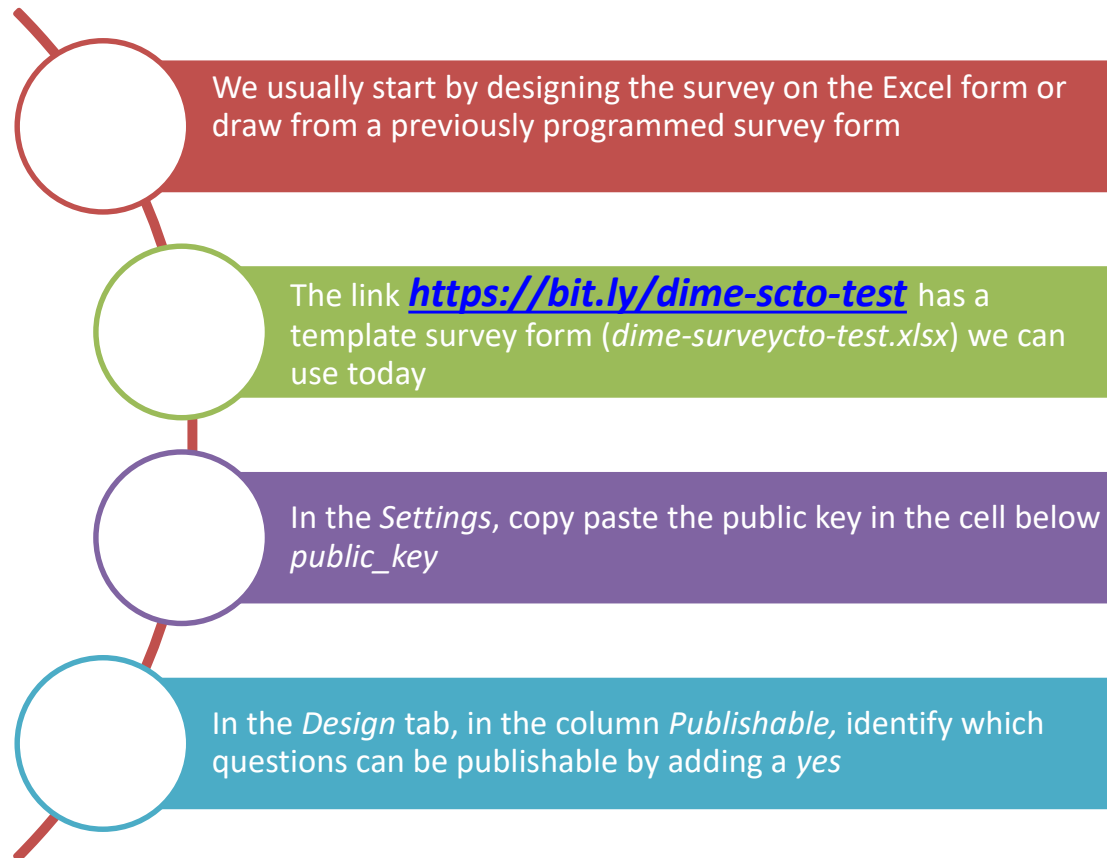
Examples:
Sharing only parts of the data with government counterparts or survey firms
Quick check for duplicates on unique IDs

Encrypting using an Excel survey form on Excel

We usually start by designing the survey on the Excel form or draw from a previously programmed survey form

The link **https://bit.ly/dime-scto-test** has a template survey form (*dime-surveycto-test.xlsx*) we can use today

In the *Settings*, copy paste the public key in the cell below *public_key*

In the *Design* tab, in the column *Publishable,* identify which questions can be publishable by adding a *yes*

D
public_key
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8 AMIIBCgKCAQEAvljjIq8PJbtDlQtnJYEM 5t6x9cexdgqf1swSl6xJPopjm2Bvq2yLHq s7N/asJwQLFH82dY1ZU62zwb14Od0C 7Y9w+ygDinw0BrRH3kR1RAJMw/cL5+Jl HzRCRyAzCLo2p329xeI7R/JCe454AuA8 rmskThmYTG2dbbA4z3Czfo+UvrSq6Ua5 Ux9CC4ZQnw2iOYD1N/GinhoMnqN/91+ L vztnf6vNG7nQmo0gP3L85xV2HFCq75ryK 3nZjlZVo3YTz9v+7+bzzhW6LBii83Bh uS3RabHvjPa8UIsjC3Q2tjuzo7iY93UyX1 OZHvGzMvMjpE73ssdL/RaOsBuqfWTg GQIDAQAB

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 between the text between-----*BEGIN PUBLIC KEY* ----- and -----*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
- Click on the *Export* tab → Locate the form
- Click *Download* → Select *all fields*
- Upload the private key
- Download the data
- Delete the key file

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
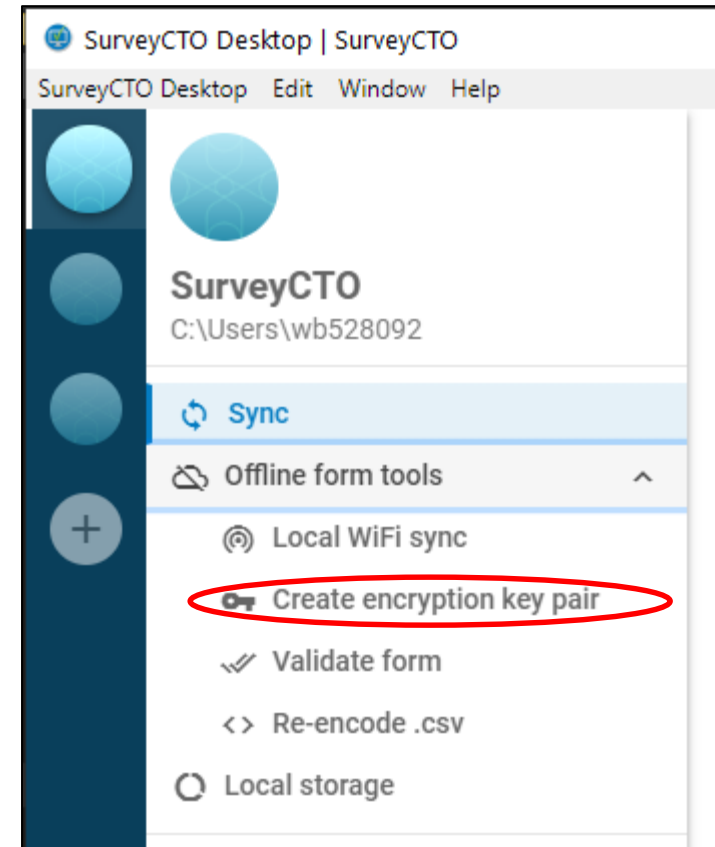
Thank you!

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.)

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-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxayHIuAlRD2bP3FIdSY1
ldonioYadFiTQSWaeTBtjidbuaNqgLuCyB+E6l31+Butv6w9Hcd1uO/YKaYkBVnd
mt4ejfJKEqmvrbUV7gyWEwWQJaoZNmMaOEYnhmmSETZpbBgnFILBhMEEijy9x1Jz
MYsJ/FJ4UW8PmB4/K0eWgA8pIP3E1m6rWn7L5YXkbrLkFGxeBRkmXWTIRrdhgSVy
aRi3X2h49Mwh8K0pUUlwfPiXo4NBLHTdPW1ed/Xdv5ZNyOKU0kSKCoHGQOvF7enQ
xw4/aBC8RbQzfGTEPM8Nm5sXwFpZsk37u0JZhUbJPf6xek7g8aSxdl1D9sR+gghV
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