



GUIDE FOR THE SUBMISSION OF THIRD-PARTY DATA USING THE HTTPS CHANNEL

TABLE OF CONTENTS

1	SUMMARY	3
2	INTRODUCTION	3
3	THIRD-PARTY DATA SUBMISSION	3
4	THIRD-PARTY DATA SUBMISSION PROCESS	4
5	ENROLMENT OF THIRD-PARTY DATA SUBMISSION	4
5.1	Enrolling an Organisation	5
6	MANAGING TECHNICAL ADMINISTRATORS	8
6.1	Enrolling a Technical Administrator	8
6.2	Viewing details of a Technical Administrator	11
6.3	Deleting a Technical Administrator	12
7	SECURITY CERTIFICATE FROM SARS	14
7.1	Requesting a certificate from SARS	14
7.2	Electronic request process	16
7.3	Manual request process	18
7.4	Deleting a certificate	20
7.5	Import a Certificate	20
7.6	Export a Certificate	25
8	MANAGING TECHNICAL USERS	31
8.1	Enrolling a Technical User	31
8.2	Viewing details of a Technical User	34
8.3	Deleting a Technical User	35
9	SUBMISSION DASHBOARD	37
10	SUBMISSION OF DATA FILES TO SARS	38
11	DEFINITIONS AND ACRONYMS	41

1 SUMMARY

- a) The purpose of this document is to guide the technical users and technical administrators in uploading third (3rd) party data via the secure web: HTTPS channel. The guide also demonstrates how to enrol, activate, and delete a technical user, administrator, and business administrator on eFiling.

2 INTRODUCTION

- a) The HTTPS 3rd party data platform is one of the digital platforms that enables taxpayers and entities to submit 3rd party data to SARS. The use of this digital platform forms part of SARS modernisation process to simplify the tax process aligning them with best international practices. The 3rd party data digital channels are:
- i) Direct Data Flow (by using the Connect: Direct technology and by using the Secure Web: https)
 - A) Refer to the Connect: Direct™ Guide for how to use this channel.
 - ii) eFiling – electronic capturing of limited volume submissions

Note: This guide only relates to the Direct Data Flow (by using the Secure Web: https) channel.

- b) Direct Data Flow (Secure Web: https) is another channel which can be used to submit a maximum of 50k lines or 10MB volumes of data. This channel reduces the overall administrative burden of large volume data transfer, shorten data processing cycle times, and provide for faster feedback. Taxpayers who want to use the Direct Data Flow channel must have eFiling profiles to enrol for this channel and activate it on eFiling.
- c) Taxpayers choosing to use the Direct Data Flow channel (by using the Secure Web: https) need to be in possession of a certificate to ensure secure file submission. Taxpayers will also be required to declare the accuracy of the data submitted to SARS by authorising the data submission. To enable SARS to administer these certificates and to authenticate file submission, 3rd party data providers must request certificates as part of the enrolment and activation process.
- d) Taxpayers will only be able to activate the Direct Data Flow Channel for the tax data types below. This is because the taxpayer must be issued with a certificate to be used with every file submission and that SARS must be able to authenticate file submissions.
- i) Dividends (Withholding) Tax
 - ii) VAT201 supporting data (in the future)
 - iii) IT3(b), IT3(c), IT3(d), IT3(e), IT3(s), and IT3(t)
 - iv) Medical Scheme Contributions
 - v) Insurance Payments
 - vi) Foreign Tax Information (FTI), and CRS

3 THIRD-PARTY DATA SUBMISSION

- a) To submit your IT3 data file/certificates successfully, you must submit your data on the applicable platform and declare by validating the summary of your submitted data. eFiling registered submitting entities submit data to SARS by utilising one of the following platforms, which is dependent on the size of the data/certificates.
- i) Connect Direct for bulk data,
 - ii) HTTPS for medium sized data, or
 - iii) eFiling for IT3-01 form (max of 20 Certificates).

- b) Manual completions are done via the completion and submission of the IT3-01 form. Electronic or data file submissions are structured and uploaded as described on the file specifications detailed in the External BRS. Upon successful structuring of the file, the file should then be submitted via the HTTPS or Connect Direct platforms.
- c) To ensure that the data/certificates are received and processed by SARS, submitting entities representatives are required to validate the activation of the IT3 submission functionality on eFiling. Additionally, they are to review their submitted data/certificates on the pre-populated IT3-02 return and once reviewed and in agreement with the summary data, they are to declare by submitting the IT3-02 return to SARS via eFiling.

4 THIRD-PARTY DATA SUBMISSION PROCESS

- a) Third-Party data submission process pertains to the following operational segments; registration, activation, enrolment, submission, and the declaration of submitted data. Registration, activation, and enrolment are vital for the use of eFiling, however once successfully completed, submission and declaration are the two operational segments that should be followed during the required periodic third-party data submissions. Connect Direct digital platform is where bulk data can be submitted to SARS.
- b) The electronic data file submissions should be structured and uploaded as described on the file specifications detailed in the External BRS. Upon successful structuring of the file, the file should then be submitted via the Connect Direct platform.
- c) To ensure that the data/certificates are received and processed by SARS, submitting entities tax administrators are required to validate the activation of the third-party data type on eFiling. Additionally, tax administrators are to review their submitted data/certificates on the pre-populated IT3-02 return and once reviewed and in agreement with the summary data, they are to declare by submitting the IT3-02 return to SARS via eFiling.

Important to note:

- For more information on eFiling registration, activation, and enrolment, refer to the following guide.
 - GEN-ENR-01-10 - Manage Submission of IT3 Third-Party Data - External Guide
- For more information on eFiling Submission and declaration, refer to the following guide.
 - GEN-ENR-01-G03 – Guide for the Submission and Declaration of IT3 Third-Party via eFiling – External Guide

5 ENROLMENT OF THIRD-PARTY DATA SUBMISSION

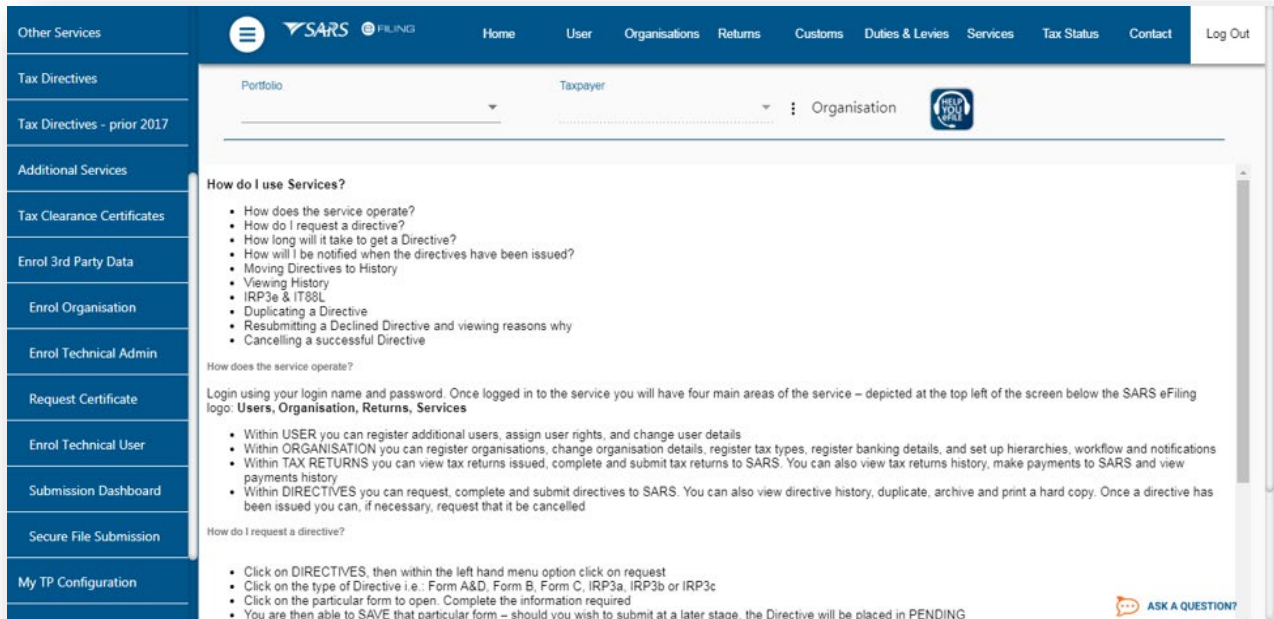
- a) Non-eFilers wishing to use the Direct Data Flow channel should register for eFiling at www.sars.gov.za and follow the guidelines as provided on the page.
- b) To manage 3rd party data submission, the taxpayer must have the following three types of users allocated in the enrolment and submission of 3rd party data to SARS:
 - i) **Business Administrator** – This user is the same as the current eFiling full administrator. The role of this user is to enrol the legal entity/organisation that will be submitting data to SARS and the Technical Administrator. The taxpayer is not required to allocate new eFiling administrators for the purposes of 3rd party data submissions if one already exists.
 - ii) **Technical Administrator** – The role of this user is to request the security certificate and to enrol technical users. If the taxpayer decides to change the Technical Administrator, a new Technical Administrator must be added before the existing one can be removed. There must always be at least one Technical Administrator for each enrolled organisation.
 - iii) **Technical User** – The role of this user is to submit the data files to SARS via the Direct Data Flow channel. An organisation can have multiple Technical Administrators and Technical Users

to allocate work according to the organisation’s requirements. The technical user must be a different person from the technical administrator.

Note: Once enrolment of the organisation is completed, the person who enrolled the organisation becomes the Business Administrator. This implies that he/she (the Business Administrator) cannot enrol to be a Technical Administrator or a Technical User.

5.1 Enrolling an Organisation

- a) To enrol the organisation, the Business Administrator must be logged into eFiling at www.sarsefiling.co.za.

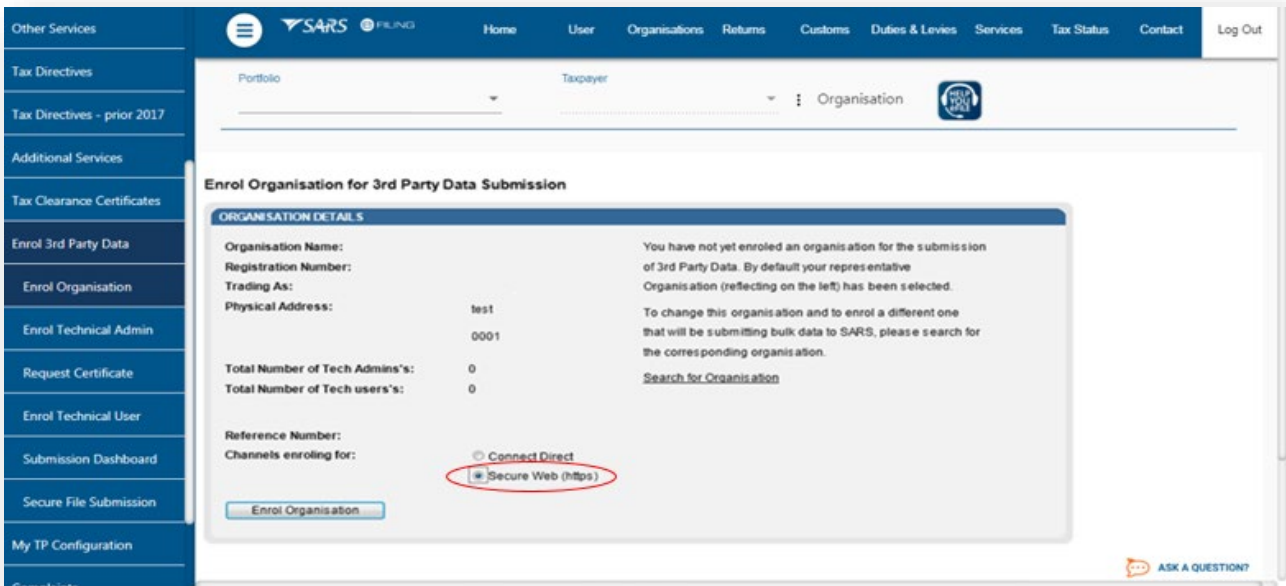


- b) Once logged into eFiling and on your Organisations work page, click **Services** in the top menu bar. From the side menu options, select **Enrol 3rd Party Data**.
- c) Under the **Enrol 3rd Party Data** option the following sub-menus are available:

Enrol 3rd Party Data
Enrol Organisation
Enrol Technical Admin
Request Certificate
Enrol Technical User
Submission Dashboard
Secure File Submission

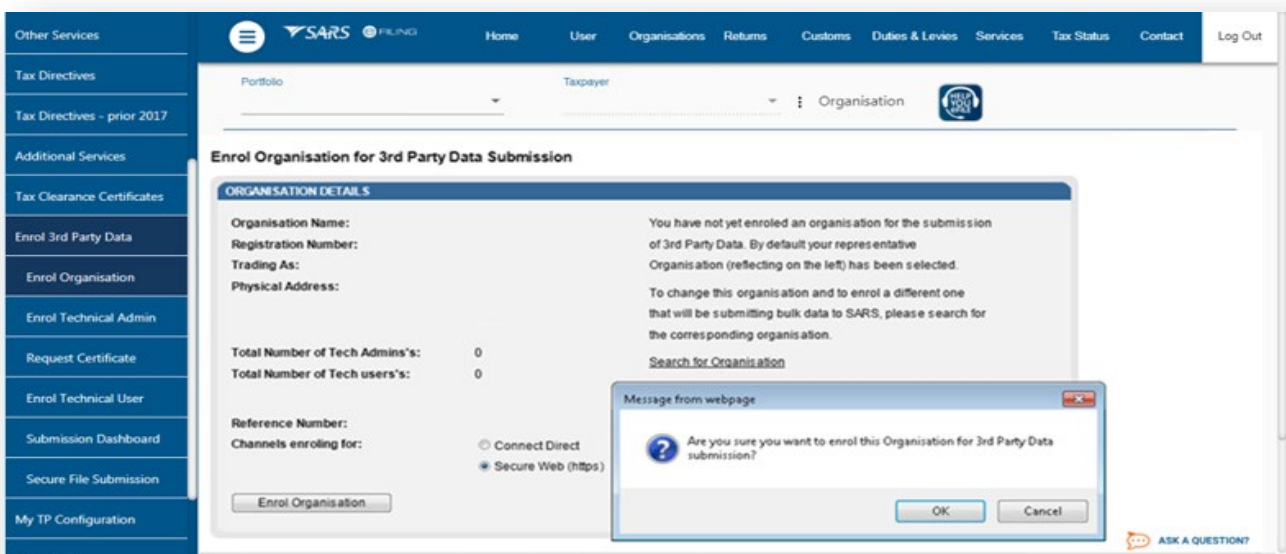
Sub Menu	Accessed by role
Enrol Organisation	Business Administrator (eFiling Administrator)
Enrol Technical Admin	Business Administrator (eFiling Administrator)
Request Certificate	Technical Administrator
Enrol Technical User	Technical Administrator
Submission Dashboard	Technical Administrator Technical User
Secure File Submission	Technical User

- d) Select **Enrol Organisation**
- e) The following screen, containing the organisations details will now appear. Select **Secure Web (https)**

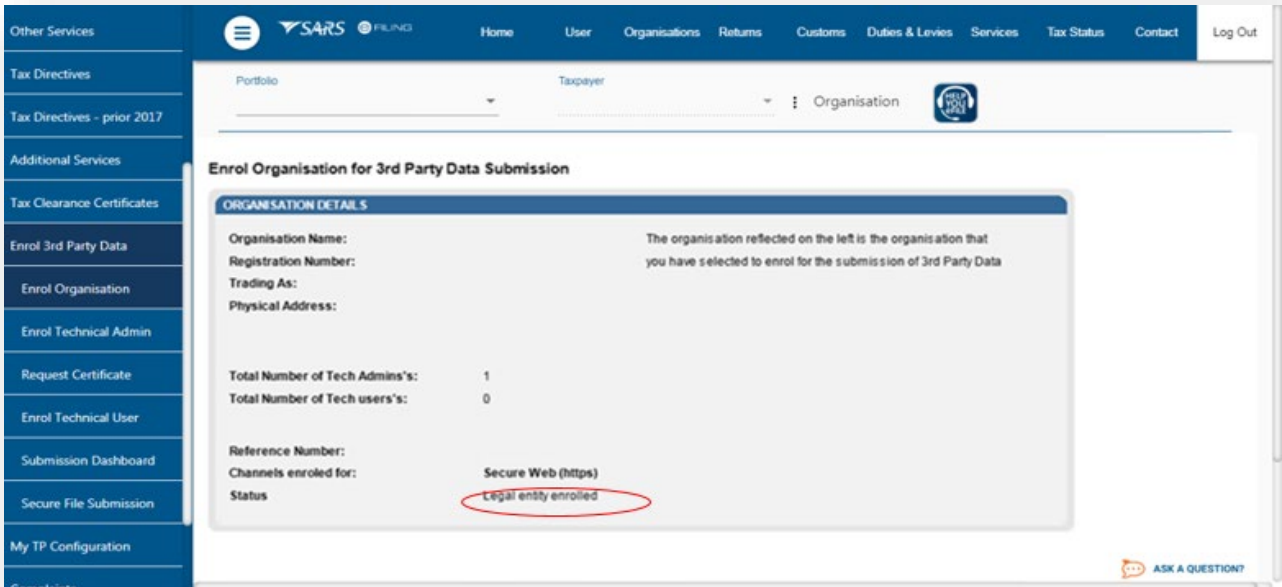


Note: If the **Income Tax, PAYE or VAT** Reference number for the company is not pre-populated on the textbox, enter the number on the textbox before you proceed to the next step.

- f) Click **Enrol Organisation** to retrieve the organisations details.
- g) A pop-up message will be displayed. The message confirms whether the user wants to enrol the organisation for 3rd party data submission. Click **OK** to proceed.



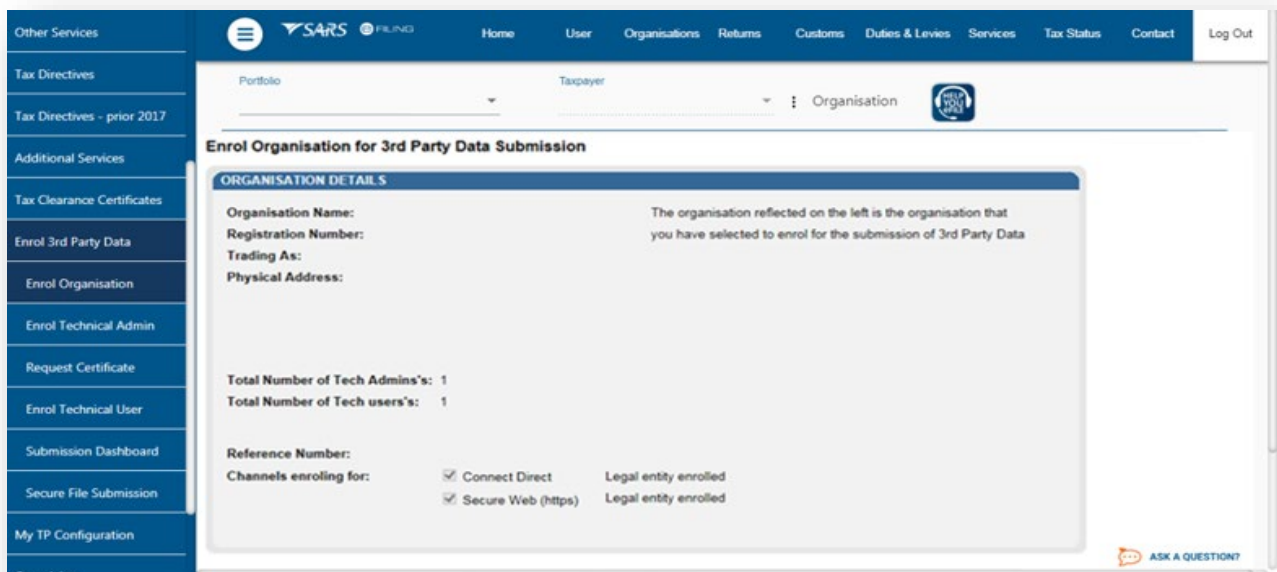
- h) The screen below will be displayed



- i) Once an organisation has been enrolled the **Status** will be **Legal Entity Enrolled**, then the Business Administrator will be able to enrol the Technical Administrator(s).

Note the following:

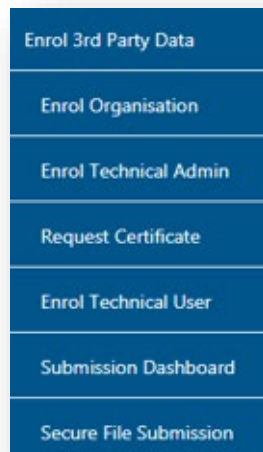
- Users can switch from using Secure Web (http) to Connect Direct and vice versa. This requires users to enrol for the use of both Connect Direct and Secure Web (https).
- To enrol for both, once having enrolled for Secure Web (https), follow the same procedure as described, however when selecting the preferred channel, select Connect Direct. This will result in the user being enrolled for both Secure Web (https) and Connect Direct.



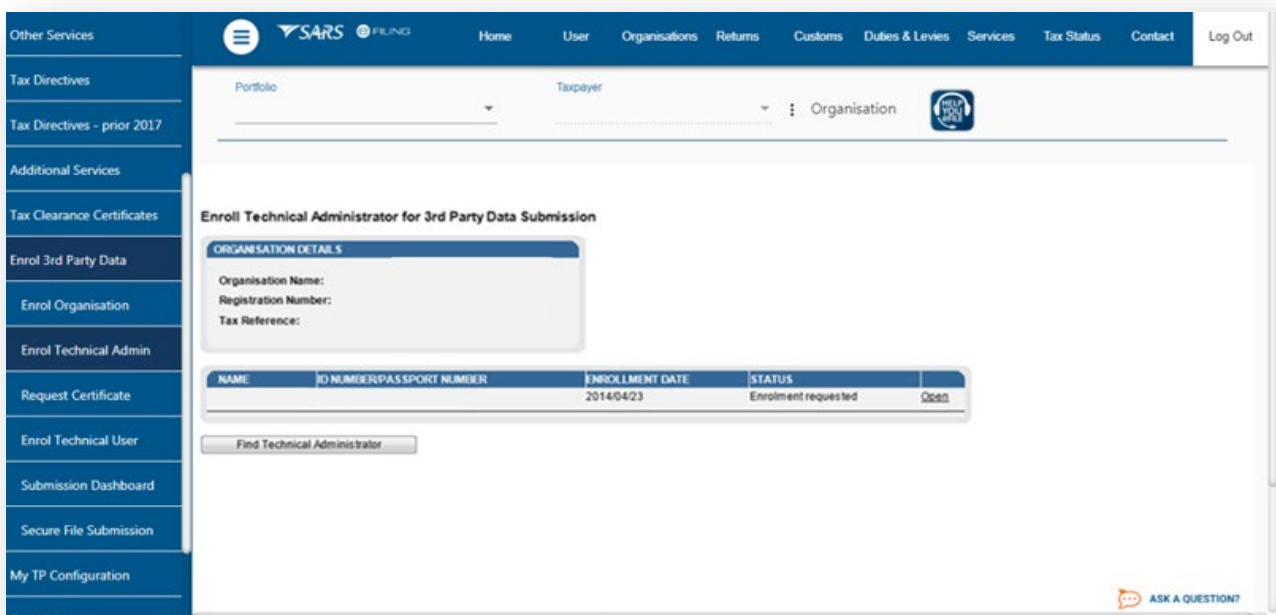
- j) The status will initially read as **Legal Enrolment Requested**. The status will later change to **Legal Entity Enrolled**. The organisation can only enrol a technical administrator if their status reads **Legal Entity Enrolled**.
- k) The status will only change once the user has refreshed the screen.

6 MANAGING TECHNICAL ADMINISTRATORS

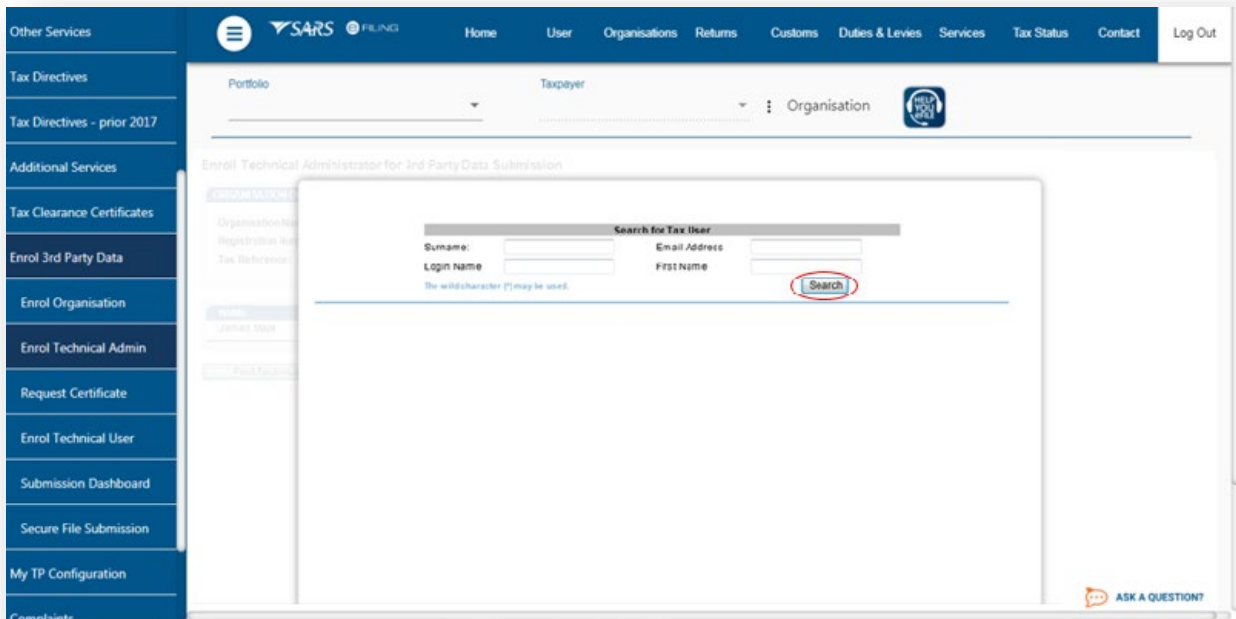
6.1 Enrolling a Technical Administrator



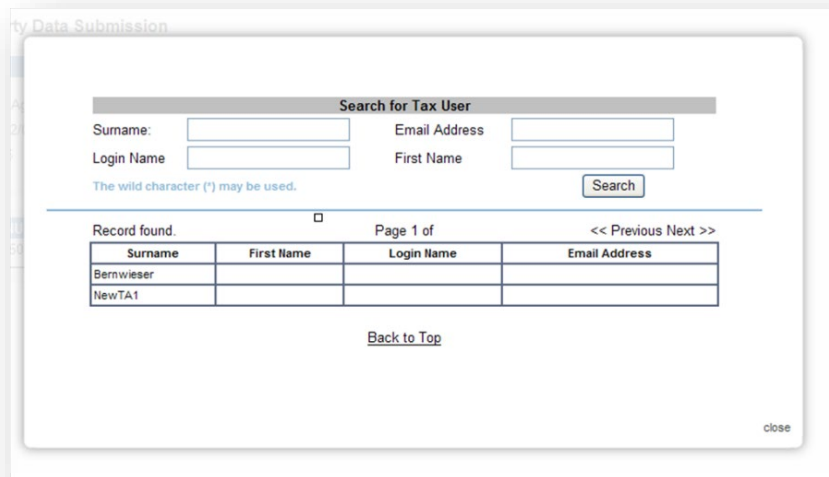
- a) To enrol a Technical Administrator, go to **Services** on the top menu, and then click **Enrol 3rd Party Data** on side menu.
- b) Select **Enrol Technical Admin** from the side menu options



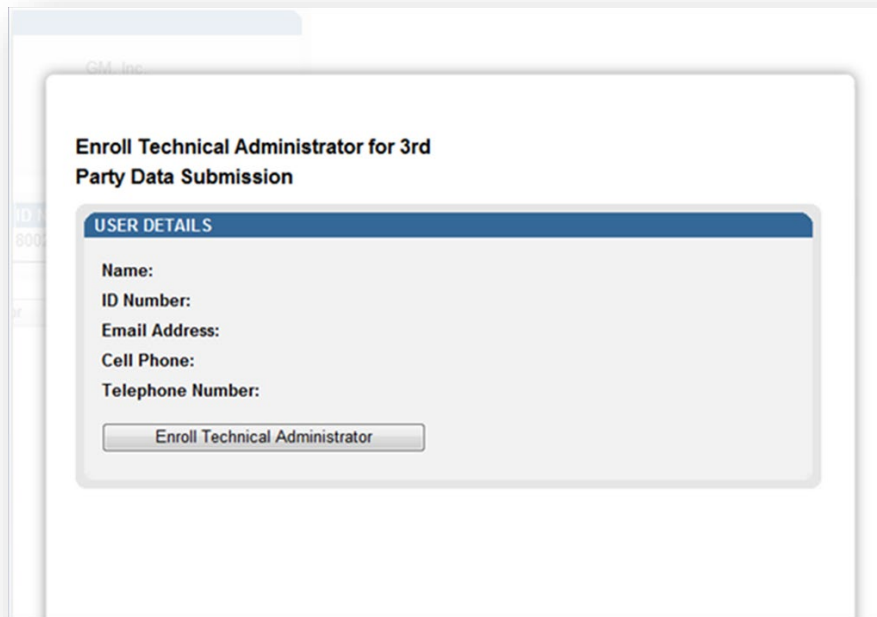
- c) Click **Find Technical Administrator** to search and select a Technical Administrator.



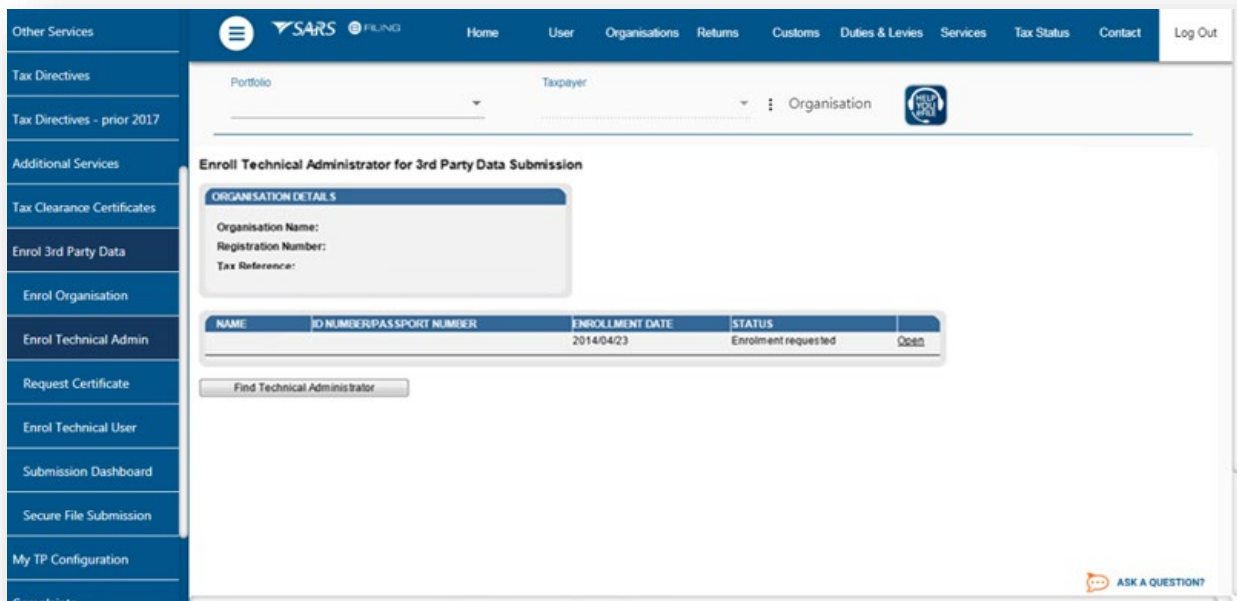
- d) Complete the information required and clicks **Search**. The user can complete one of the fields and click on search. If no values are entered in the above fields, click **Search** and all the registered eFiling users for the relevant organisation will be displayed.



- e) The screen with the user's details will be displayed. Select the user that is to be enrolled as the Technical Administrator



- f) The screen with the details of the selected user will be displayed as a confirmation. Select **Enroll Technical Administrator** to submit the request.



- g) By selecting the **Enrol Technical Administrator** button you will be redirected to the grid page.
- h) In the **Status** column, the status **Enrolment Requested** indicates that SARS is still processing the enrolment. The status **Link Enrolled** will be displayed once the enrolment of the user as the Technical Administrator has been confirmed.
- i) To replace one Technical Administrator with another Technical Administrator, the first enrolled Technical Administrator must have a status **Link Enrolled**. The Business Administrator must then enrol a new

Technical Administrator. Click **Find Technical Administrator** and once a new Technical Administrator has been enrolled, the other Technical Administrator can be deleted.

- j) To delete all Technical Administrator(s), all associated Technical Users and certificates need to be deleted first. Refer to section below on how to delete technical users.

6.2 Viewing details of a Technical Administrator

- a) To view all the Technical Administrators, click **Enrol Technical Admin**

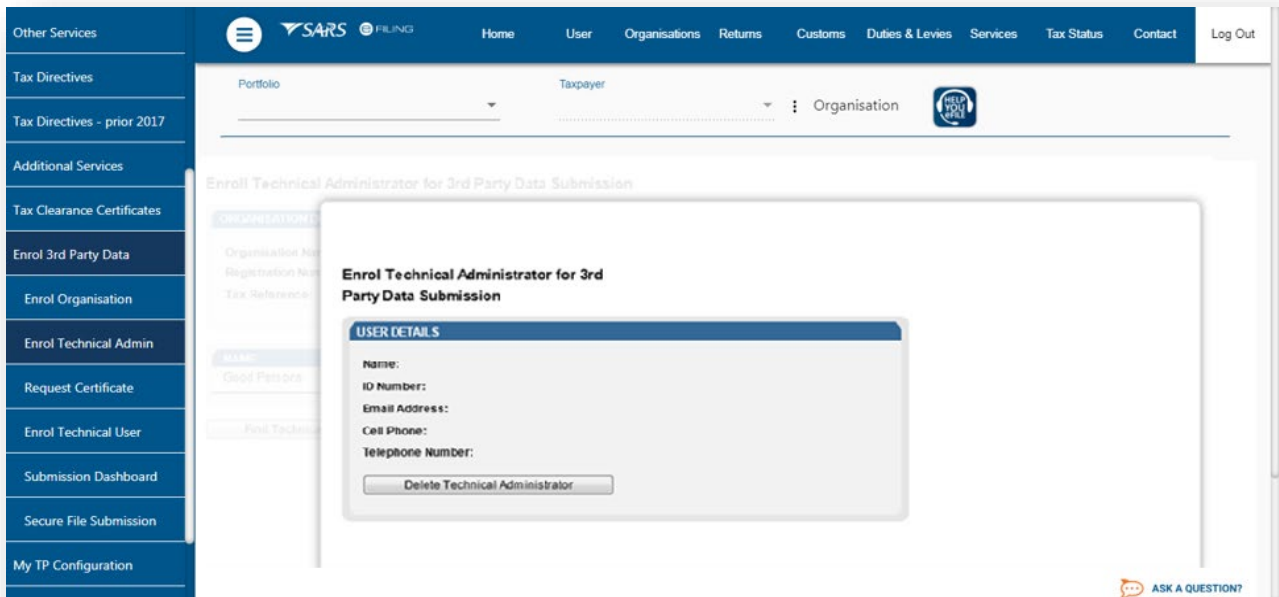


The screenshot shows the SARS eFiling interface. The left-hand navigation menu is expanded to show 'Enrol Technical Admin'. The main content area is titled 'Enroll Technical Administrator for 3rd Party Data Submission'. It features a form for 'ORGANISATION DETAILS' with fields for 'Organisation Name:', 'Registration Number:', and 'Tax Reference:'. Below the form is a table with the following data:

NAME	ID NUMBER/PASSPORT NUMBER	ENROLLMENT DATE	STATUS	
Theshlin Moodley		2015/08/14	Link Enrolled	Open

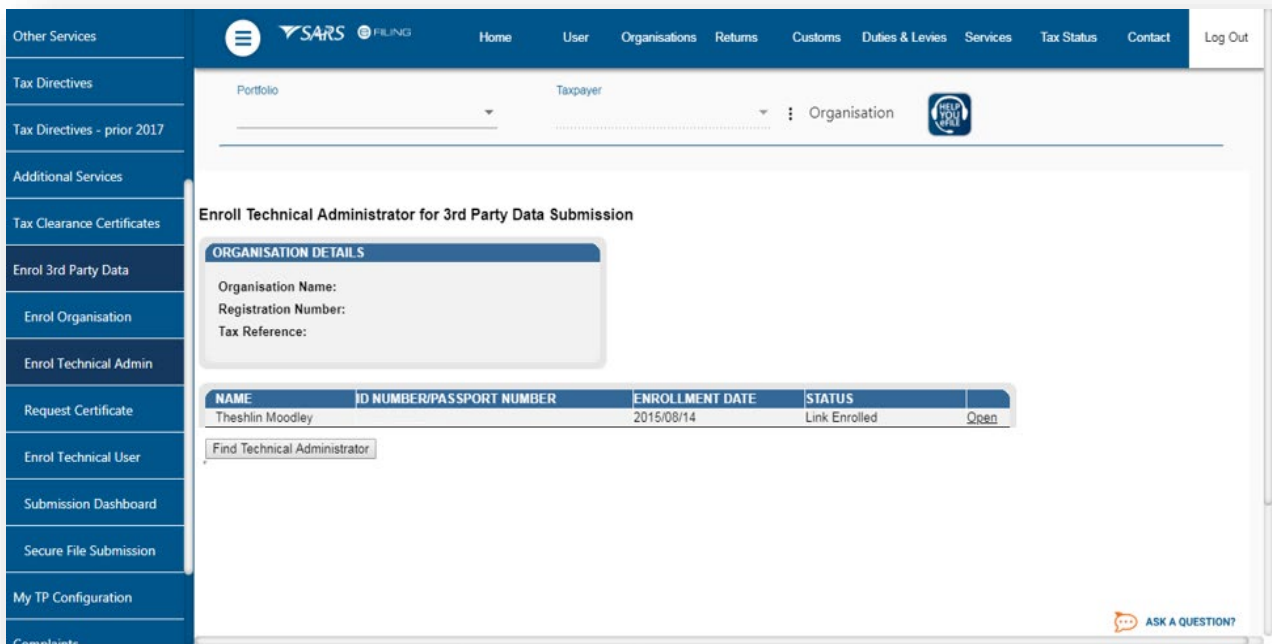
Below the table is a 'Find Technical Administrator' button. At the bottom right of the page, there is an 'ASK A QUESTION?' button.

- b) All the Technical Administrators will be displayed. Click **Open** next to a Technical Administrator to view the details of the Technical Administrator.

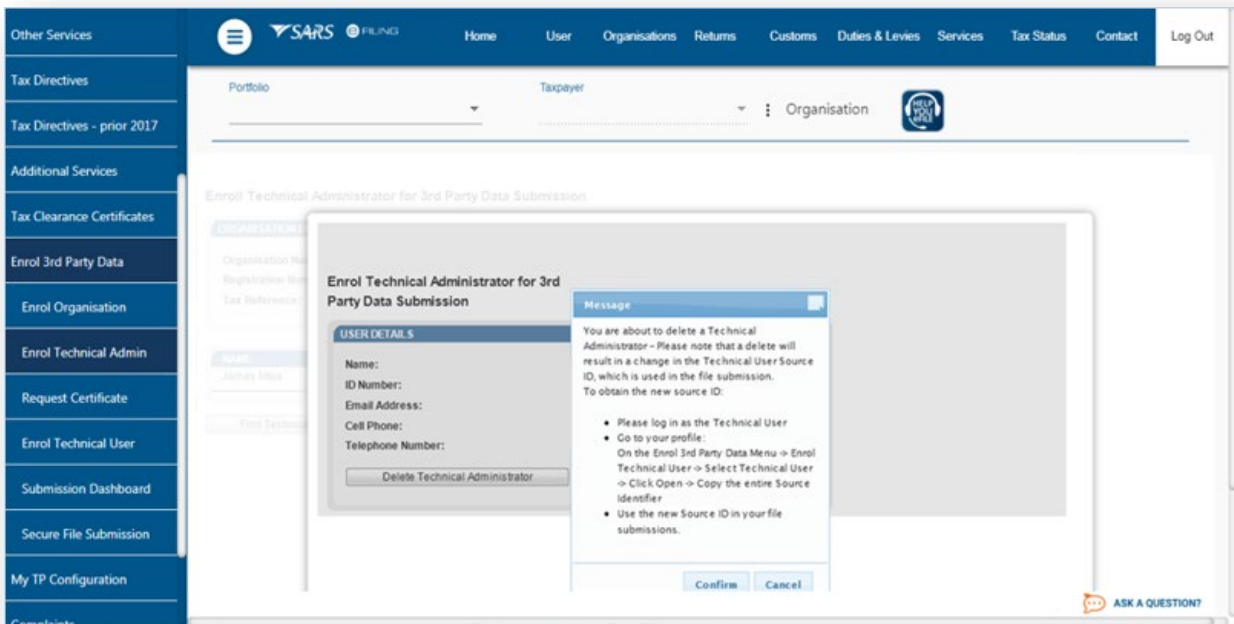


c) Details of the Technical Administrator will now open.

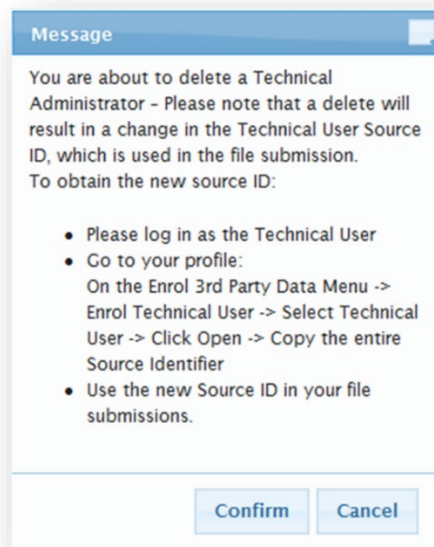
6.3 Deleting a Technical Administrator



- a) To delete a Technical Administrator ,
 - i) Click **Open** next to the Technical Administrator that should be removed.



b) Click **Delete Technical Administrator** to remove the Technical Administrator.



c) You will be prompted to confirm that the user must be deleted.

- i) If you select **Confirm**, the Technical Administrator will be deleted.
- ii) To cancel the deletion,
 - A) Select **Cancel**.

d) To delete all Technical Administrator(s), all associated Technical Users and certificates need to be deleted first. Refer to section below on how to delete Technical Users.

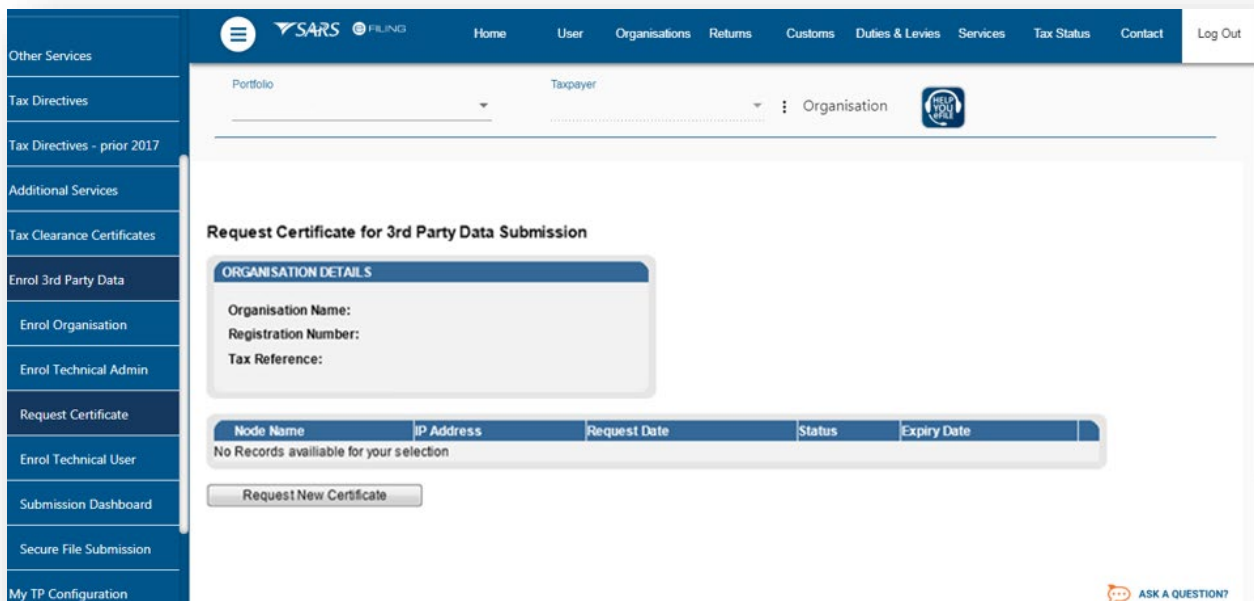
7 SECURITY CERTIFICATE FROM SARS

7.1 Requesting a certificate from SARS

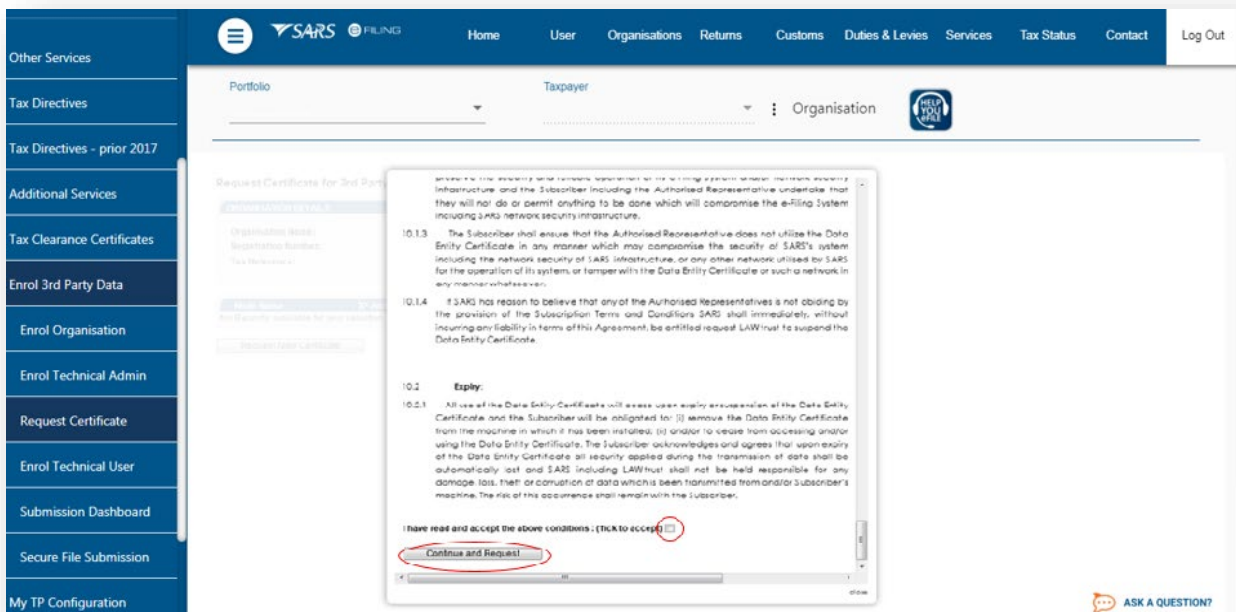
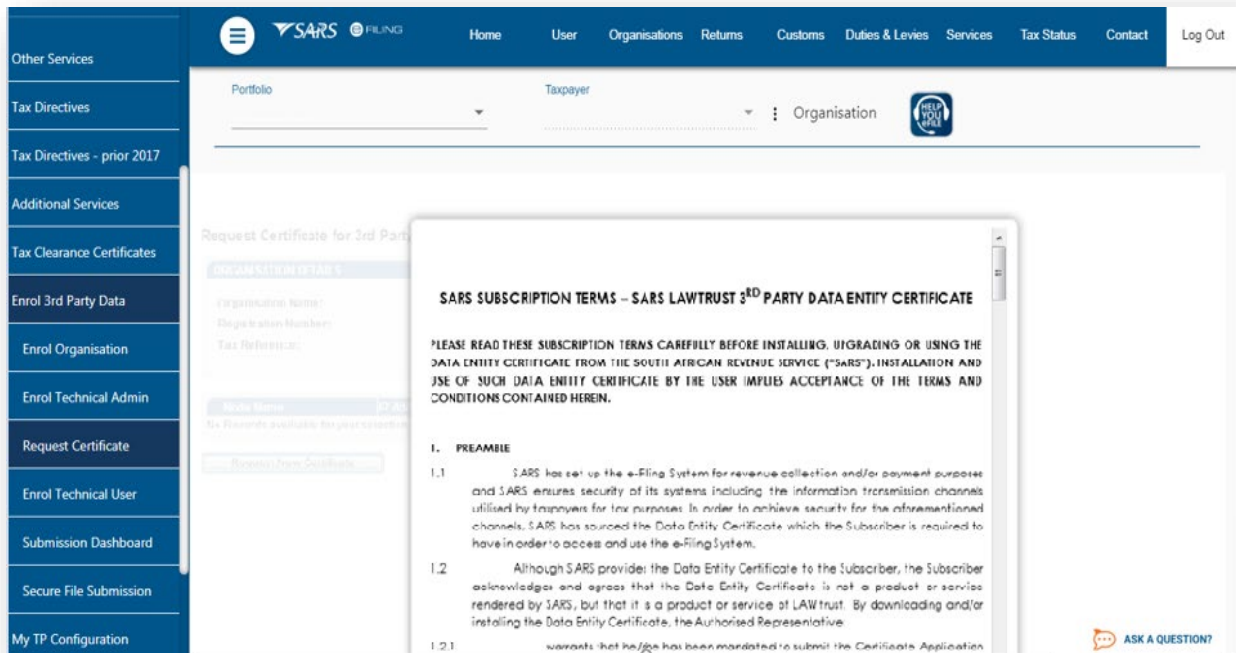
- a) Once a Technical Administrator has been enrolled successfully, the Technical Administrator can request the security certificate from SARS. This certificate is required for submission of data via the websecure (https) channel.



- b) To request the security certificate from SARS, select **Request Certificate** from the side menu options, on your Organisations work page under the **Enrol 3rd Party Data** menu.



- c) To request the certificate from SARS, go to **Services** on the top menu, then click **Enrol 3rd Party Data** on side menu then select **Request Certificate**
- d) The **Request Certificate** screen will list all certificates that were issued previously for that taxpayer. Initially this list will be empty.
- i) Click **Request New Certificate** to start a new certificate request process.



- e) You will be requested to accept the Terms and Conditions (T&C) that govern the use of this service by ticking the box next to **I have read and accept the above conditions**.
- f) Once the terms and conditions have been accepted,
 - i) Click on **Continue and Request**.
 - ii) Do note that unless the terms and conditions are accepted, you will not be able to proceed to the next step.

7.2 Electronic request process

Other Services | SARS eFILING | Home | User | Organisations | Returns | Customs | Duties & Levies | Services | Tax Status | Contact | Log Out

Portfolio | Taxpayer | Organisation

Request Certificate for 3rd Party Data Submission

ORGANISATION DETAILS

Organisation Name:
Registration Number:
Tax Reference:

Please capture the following detail of the Channel that will be connecting to SARS

Channel: Secure Web (https)
Interface Name:

Do you want to generate the certificate request manually or do you want eFiling to assist in the process?

Electronically - the eFiling system will automatically generate the certificate request and will send the request for fulfillment. Once the certificate has been issued eFiling will assist in the installation of this certificate.

Manually - eFiling will provide you with the CN that you have to use to generate the certificate request. You will then have to upload the certificate request. Once the certificate has been issued you will have to download the certificate and manually install the certificate on the appropriate server

[Continue](#)

ASK A QUESTION?

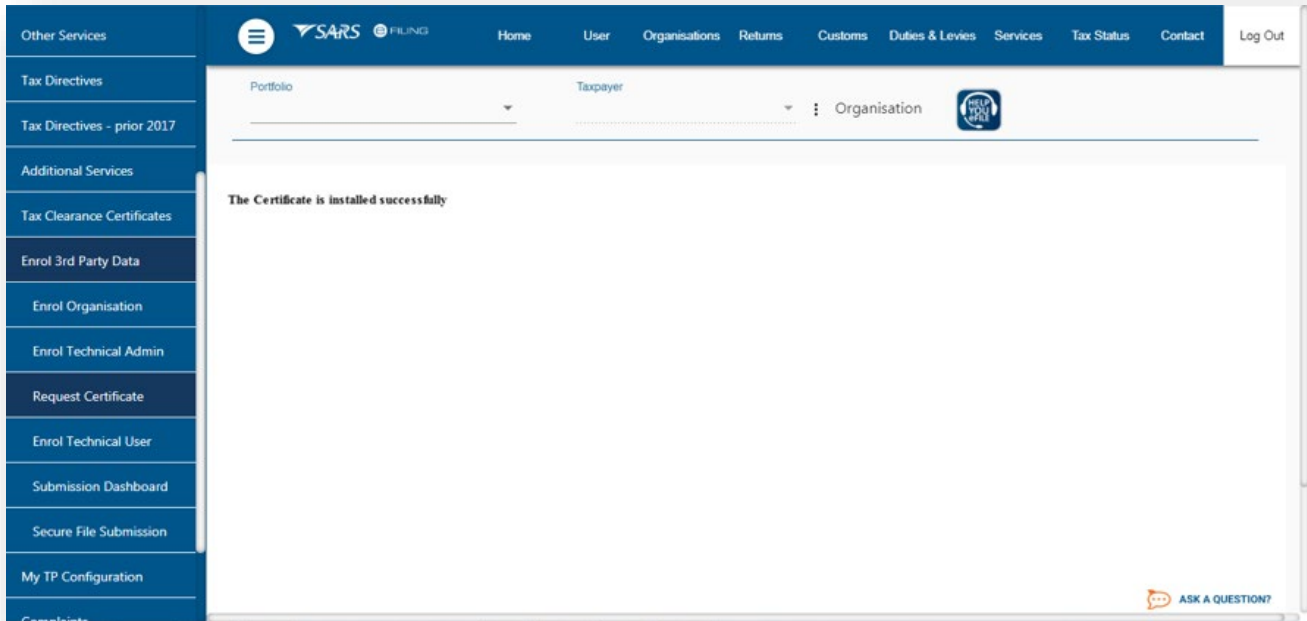
- Capture the **Interface Name** i.e your company name. Select either the **Electronic** or **Manual** options for issuing the certificate. It is recommended for secure web https channel that you select **Electronic**. This means that the eFiling system will automatically generate the certificate request and will send the request for fulfillment. Once the certificate has been issued, eFiling will assist in the installation of the certificate.
- To generate the certificate request electronically, select **Electronically** button.
- To use the electronic request process complete the screen above and once you are done, click **Continue**.

Other Services | SARS eFILING | Home | User | Organisations | Returns | Customs | Duties & Levies | Services | Tax Status | Contact | Log Out

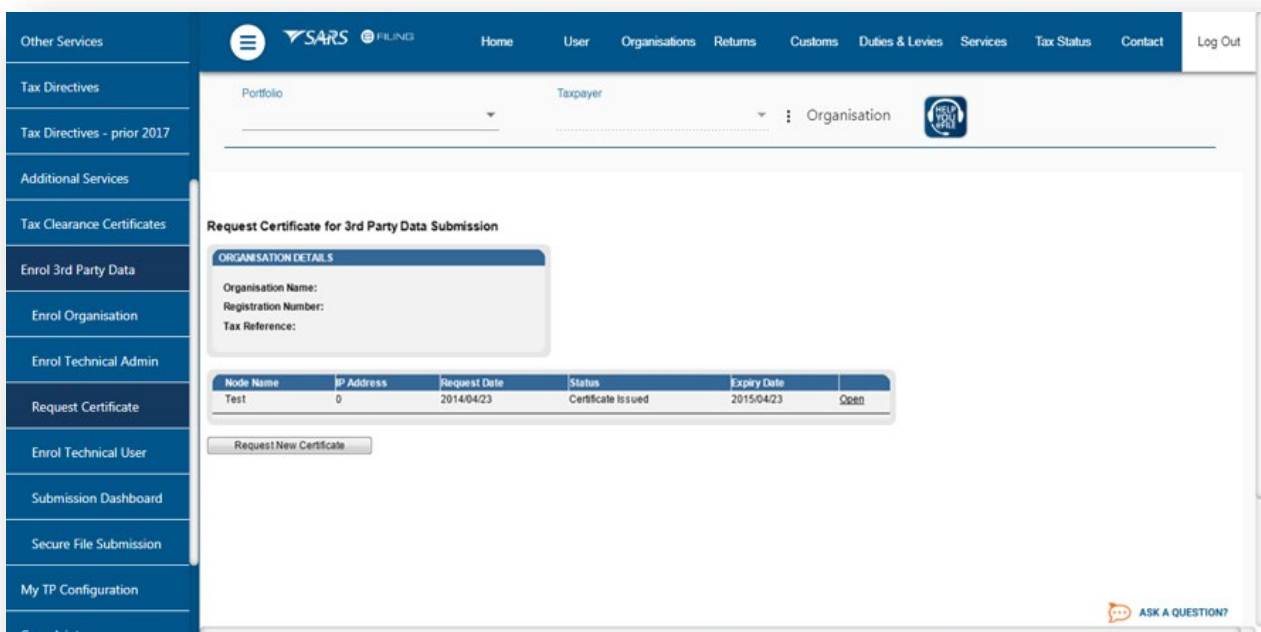
Portfolio | Taxpayer | Organisation

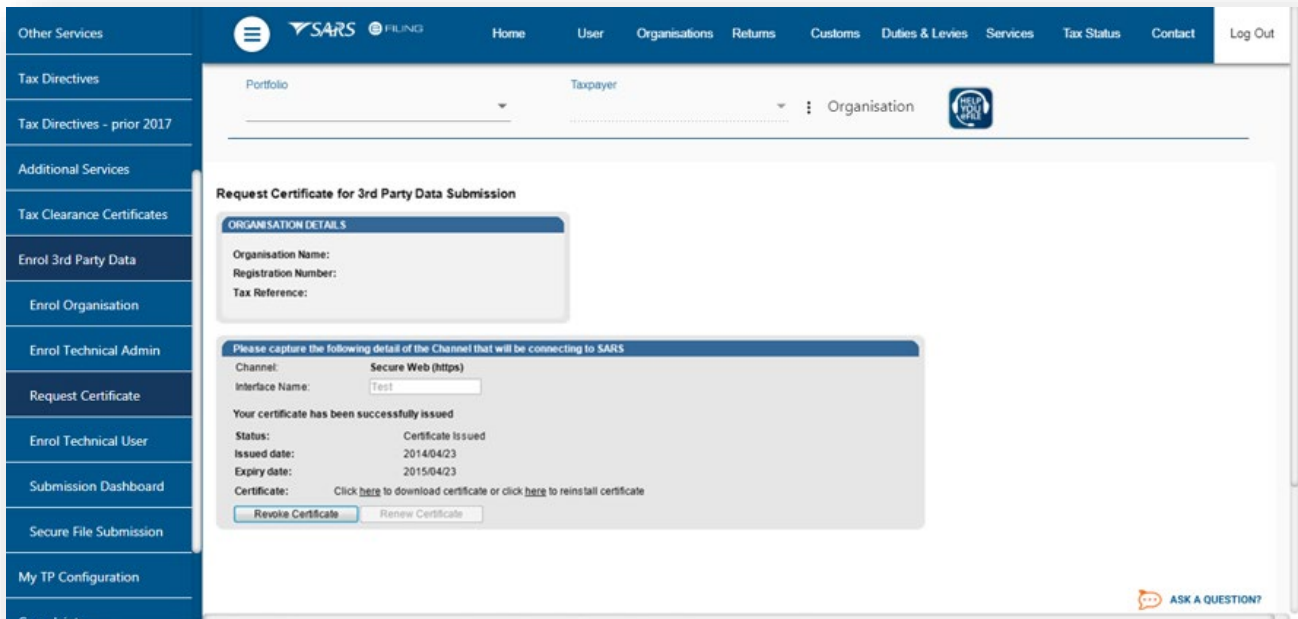
Java

ASK A QUESTION?

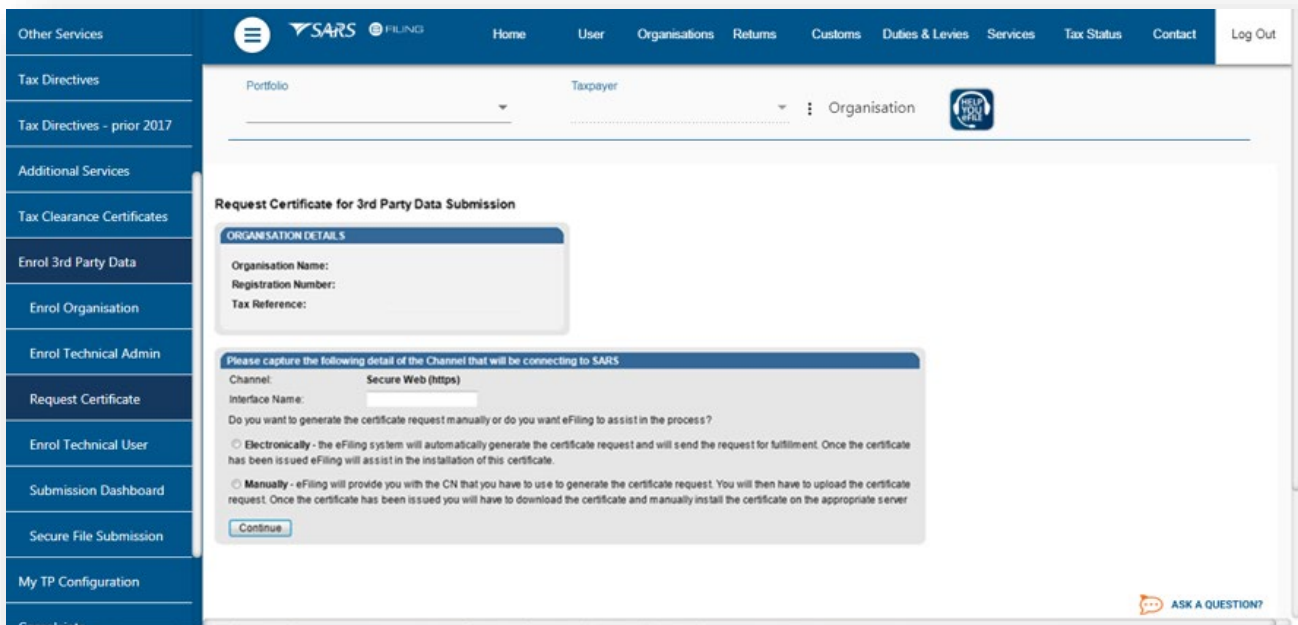


d) The message will appear confirming that your certificate has been successfully installed.

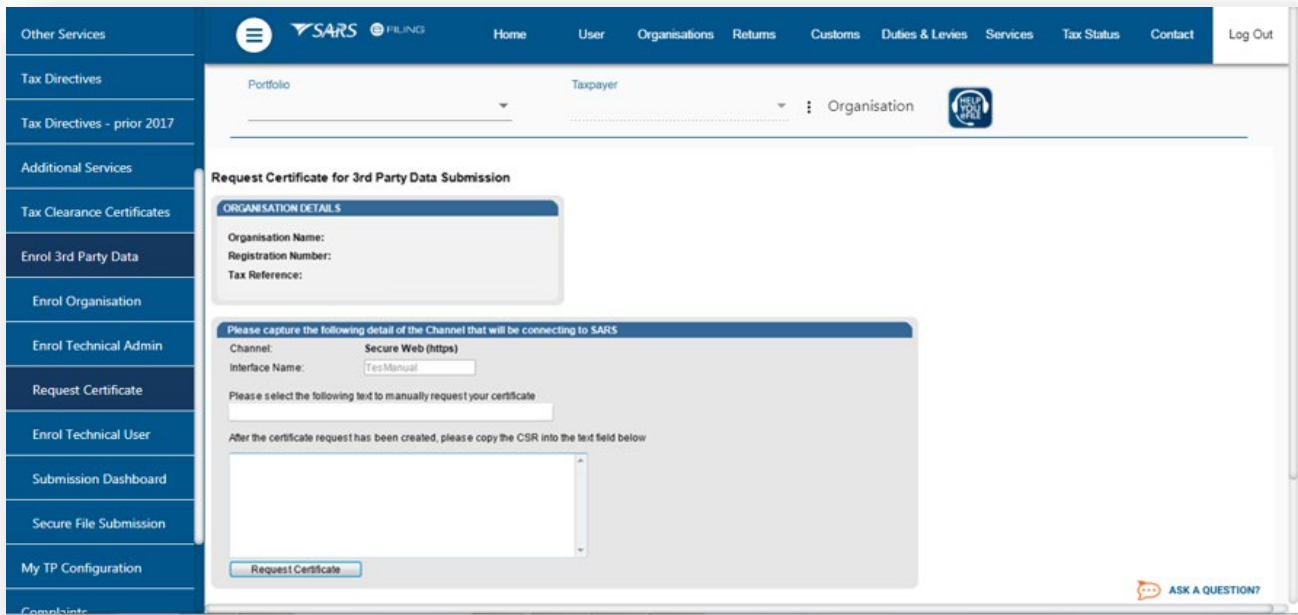




7.3 Manual request process



- a) To use the manual process to request a certificate, select **Manually** and click **Continue** button to proceed.



b) Copy the **Certificate Signing Request (CSR)** into the textbox. then click **Request Certificate**.

Note: SARS does not provide the CSR however it is generated by the user

```

-----BEGIN CERTIFICATE REQUEST-----

MIIC3jCCAcYCAQAwgZoxFTATBgNVBAMMDFJlaW5oYXJkIDAuMTEUMBIGA1UECwwL
QmVocmVucyAwMDExETAPBgNVBAoMCExBV3RydXN0MRlWEAYDVQQHDAIDZW50dXJp
b24xEDAObgNVBAgMB0dhdXRlbmcxZzAJBgNVBAYTAipBMSUwIwYJKoZIhvcNAQkB
FhZzdXBwb3J0QGxhd3RydXN0LmNvLnphMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAh2bZmV0r1yPG/DLRRQXDpwR/hy4fCleaQDXzX4P4h8LFBRLFY88N
ceuUJDISYbtME/sS4+z7+sIK/ubTJLrZEmoaO/gj5JvJhGffYWG69ZEOsGssN8Tq
w9pA4XgIobB+ExzvrmgMvq7ro4EwiWZ6+URBxUqwsRsThakmbZdejtBUqSWckldr
a2XgDvHgDqhX/CKPPJ84qa3+eLONQXAMV2Mmy0YI7qrOxjDUh9jD1T/ce+6M/1C9
NHfwMjAvKFXLvsVAW+MOuK50qo6GeYUy8ZxfFCMADhyxHW7qK2COBQZmqtpR7PT
3jmcMb7axyJ6PolK8iaQIFRWa3SATH1kywIDAQABMA0GCSqGSIb3DQEBBQUAA4IB
AQAY5/Ug6bA1lrAIM954hkhyJGMSmGJA8w+TkrTI5KGUoc7fMV1bqkDvt+aToGxV
ftengEf98JrGi48W13diazynLMvyNnaOCIK5xy144SpliLBWUvHHXVP0obnDjnsN
HKX+BBHiBI/9nyVYkM0Jgqepa4PNLjPSjyvxbc/Git1cb2bC0svHWWcnIB1J1Htq
iwZVbEdknzGEmRY3fjrChf5dTdenroavythyKbsNlgJpinlowrLEDjnMqmQIYNxi
7gJWOx2S6IP1vva1iYuf5KRJMSaF+3OxmK7qZR+j/08/HuBatOZ1+3gwpL5oPpxx
iCb1hDfnib25L3kWQe4JtNKd

-----END CERTIFICATE REQUEST-----

```

c) Please note that a typical request string will look as above

- d) You will now have the option to download the security certificate and then install it on the relevant server or to reinstall the security certificate.

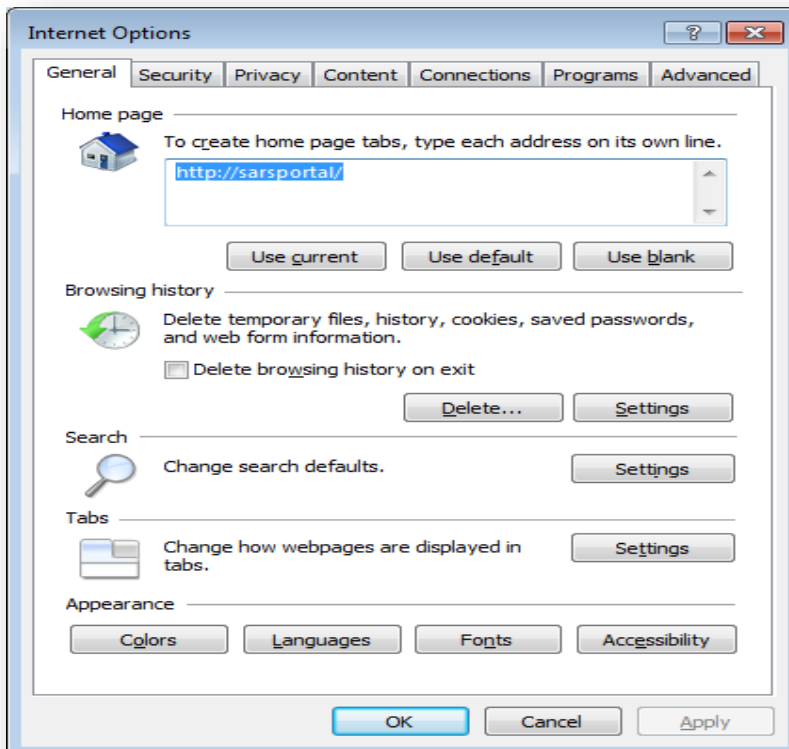
7.4 Deleting a certificate



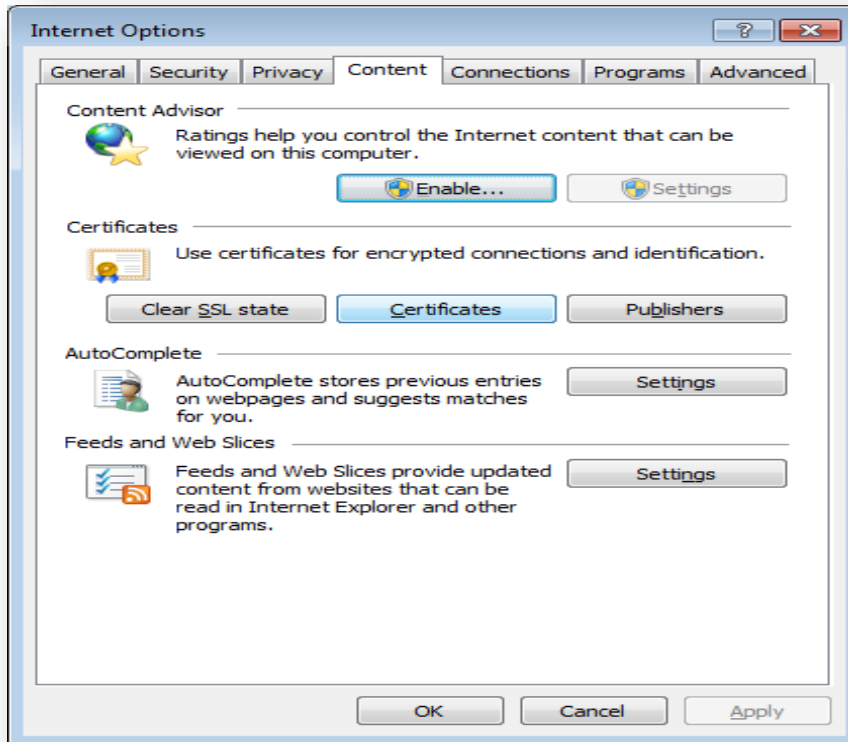
- a) Click **Revoke Certificate** to cancel the certificate.
- b) **Revoke Certificate** – You have the option to revoke a certificate. If **Revoked Certificate** is clicked, the certificate will be revoked and the status of the certificate will change to indicate that it was cancelled. The revoked certificates will still be on the list of certificates.
- c) **Renew Certificate** – Certificates are only valid for 12 months from date of issue. The **Renew Certificate** button will only be available 30 days prior to the expiry date.

7.5 Import a Certificate

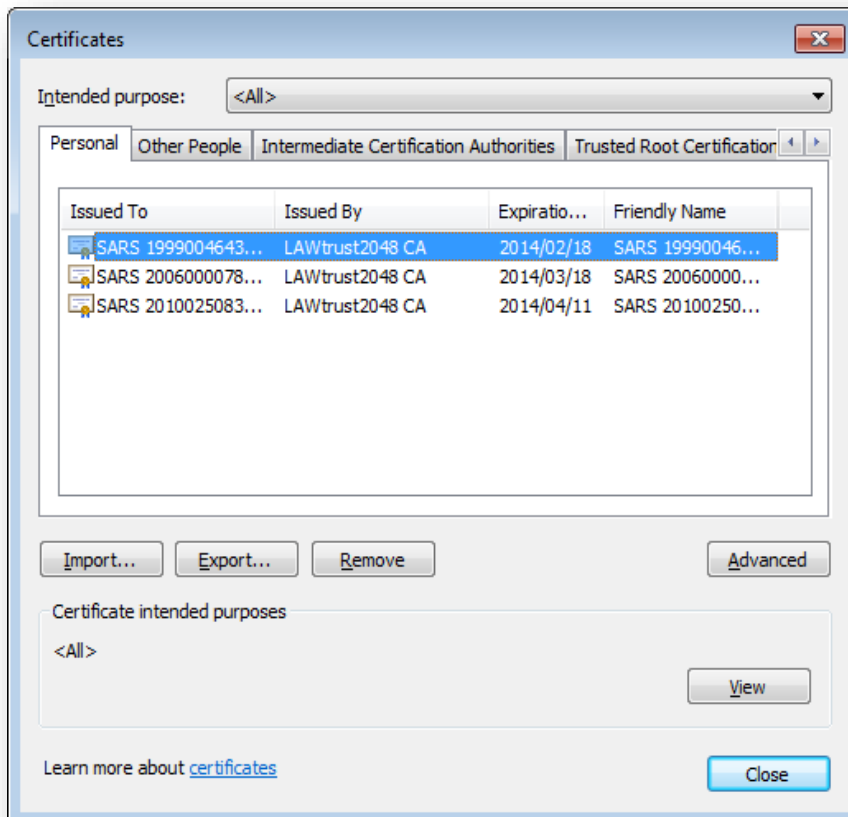
- a) To access, click **Tool**, and then Internet options.



b) Click on **Content**



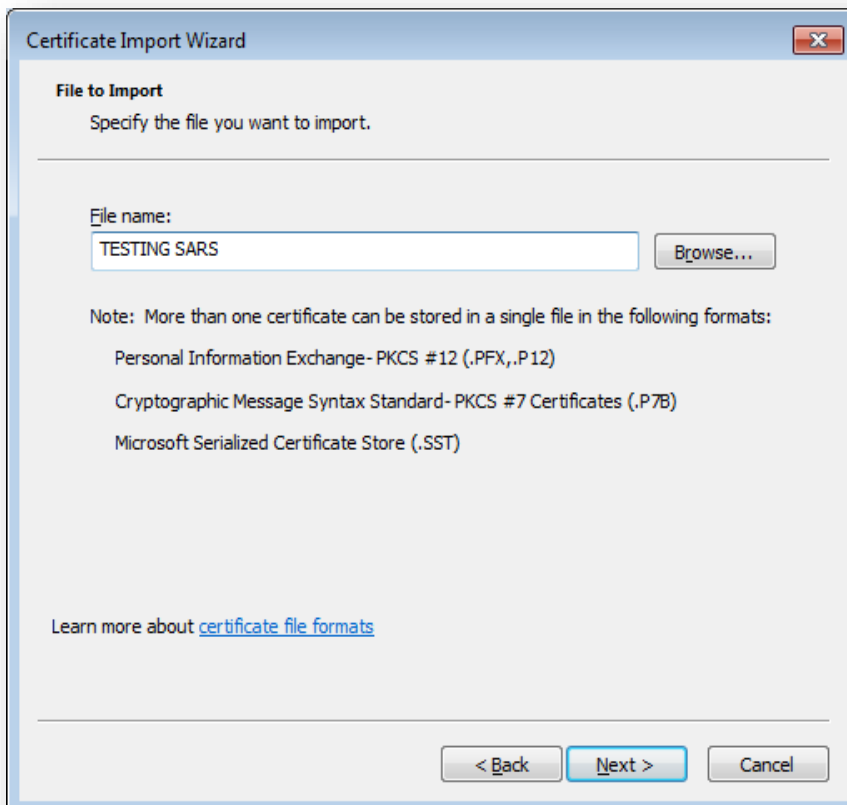
c) Click **Certificates**



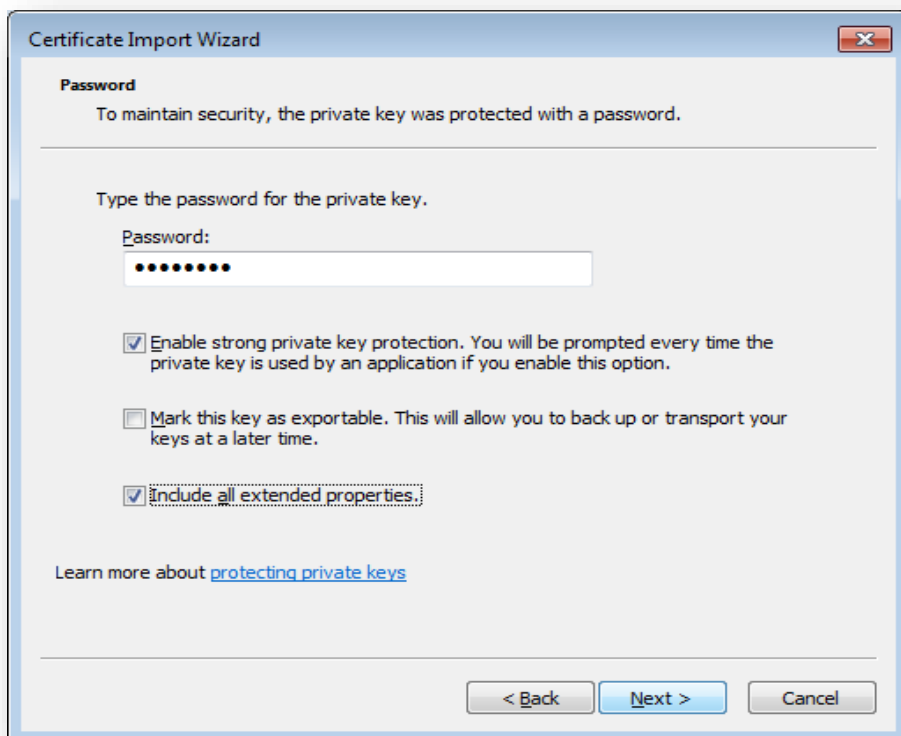
d) Select the Certificate and click **Import**



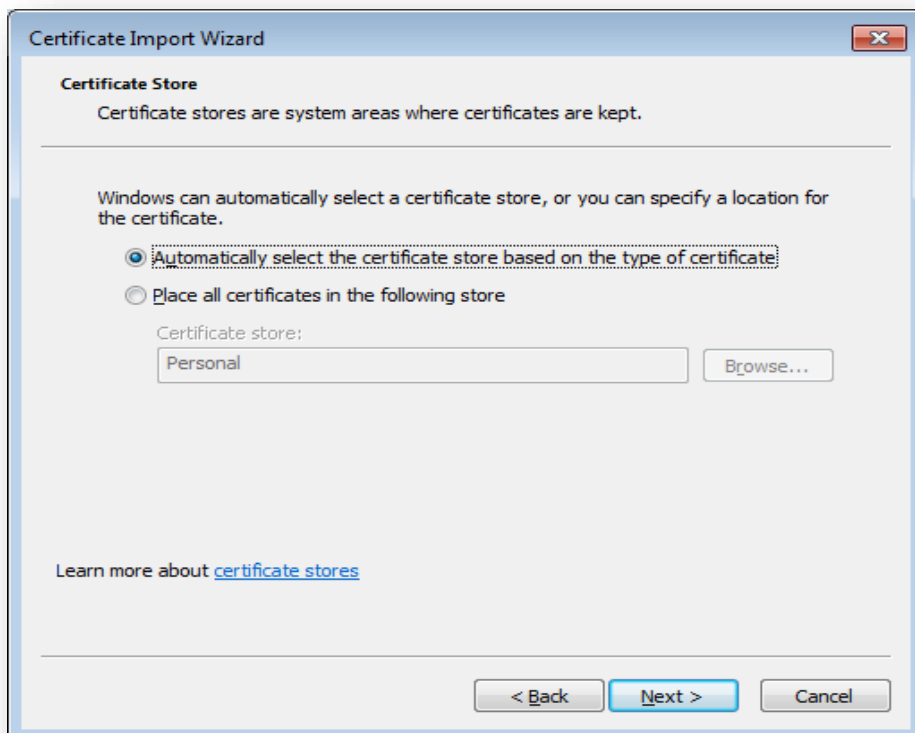
- e) Click **Next**.
- f) Give the name of the file when you have exported it



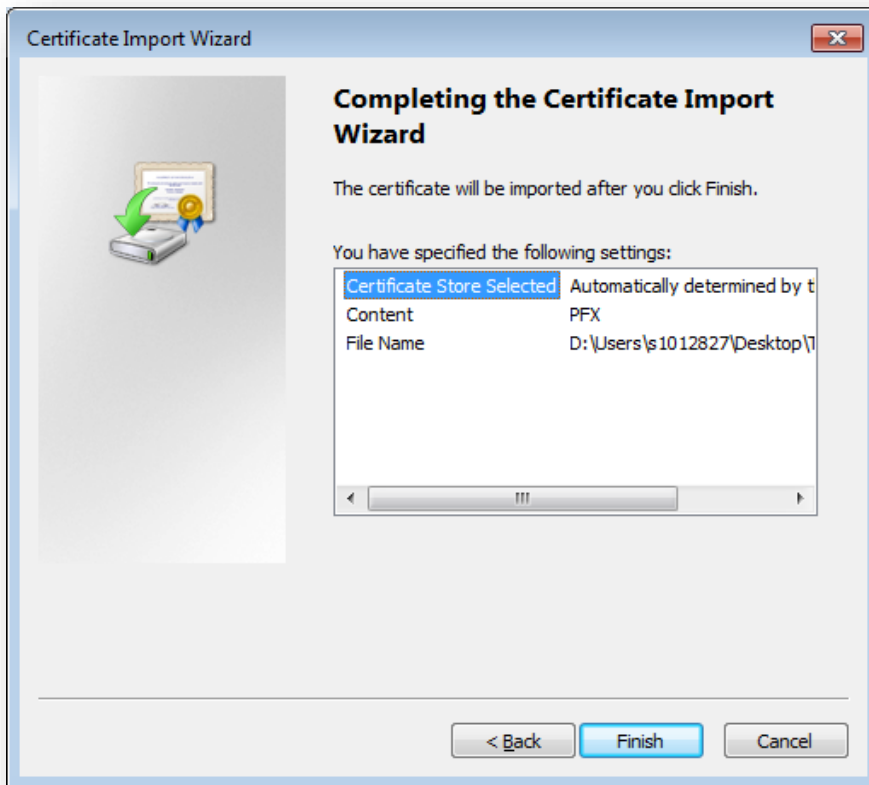
- g) Click **Next**.



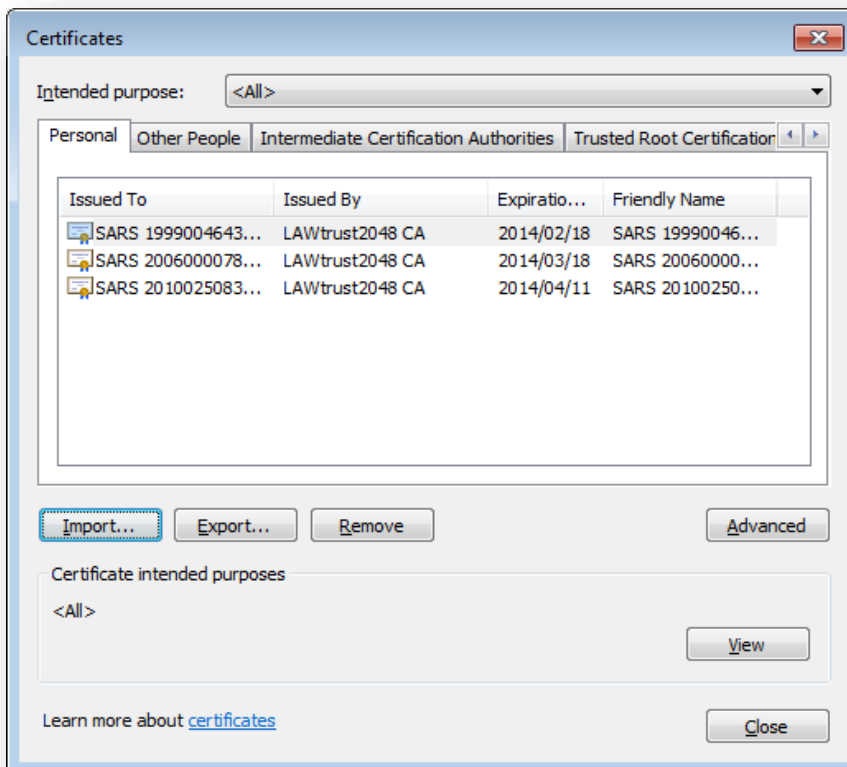
- h) Enter a password and click **Next**.
- i) Select **Automatically select the certificate store based on type of certificate**.



- j) Click **Next**.



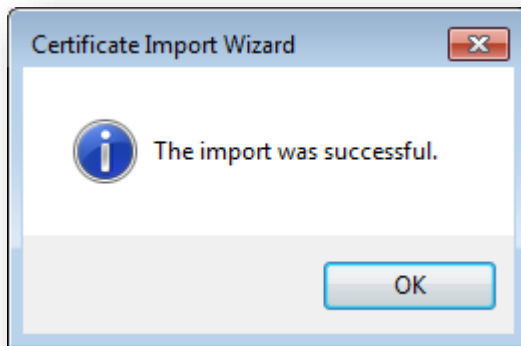
k) Click **finish**.



l) Select the import file and click on **Import**

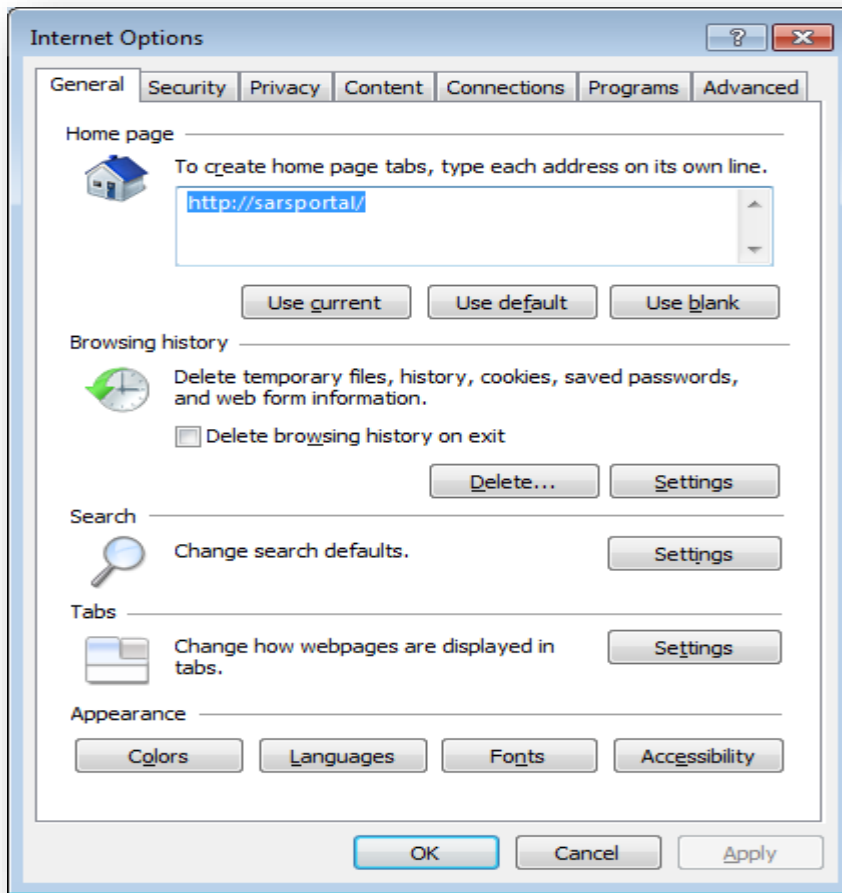


m) Click **OK**

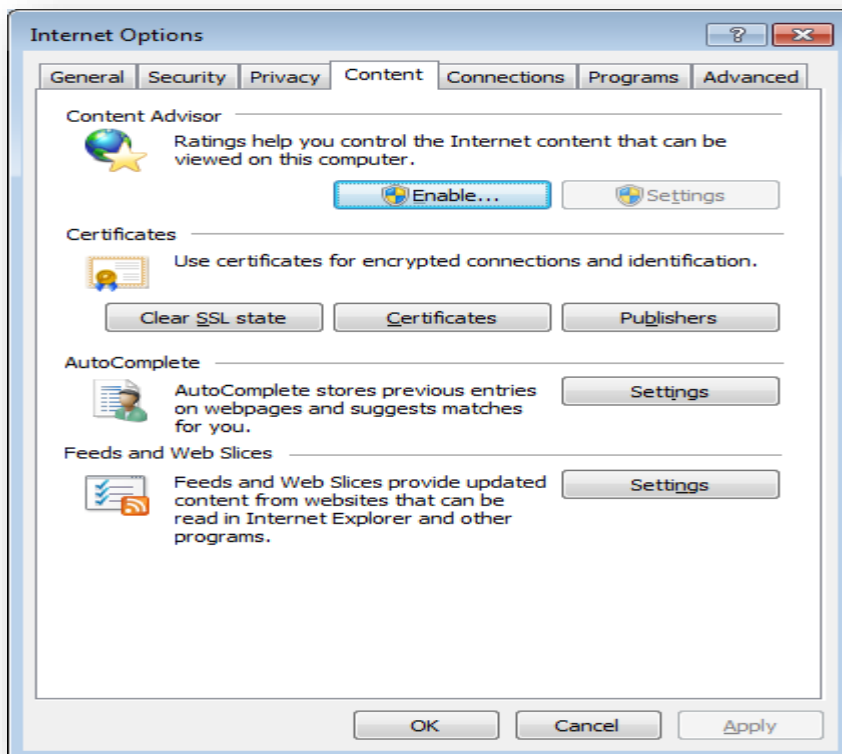


7.6 Export a Certificate

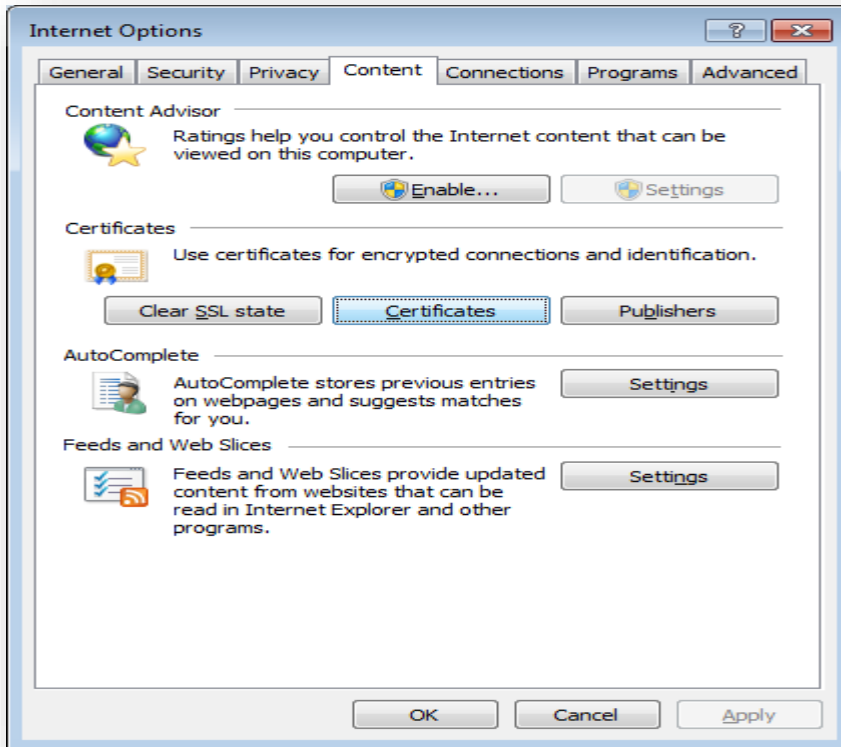
- a) Go to explorer.
- b) Click **Tools**.
- c) Select **Internet Options**
- d) Click **OK**



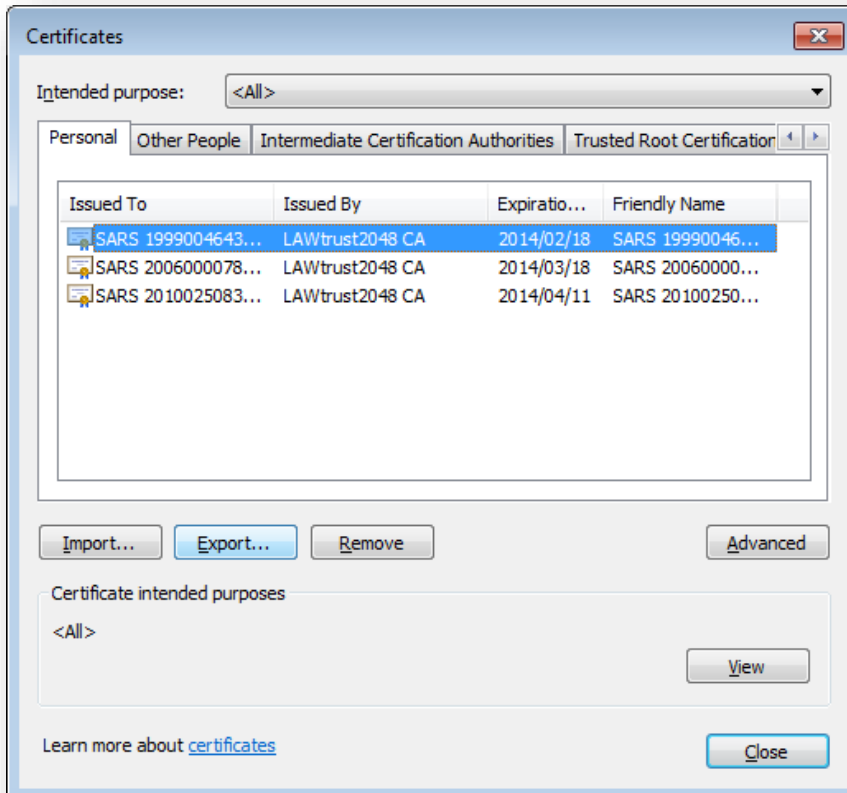
e) **Select Content**



f) Select **Certificate**



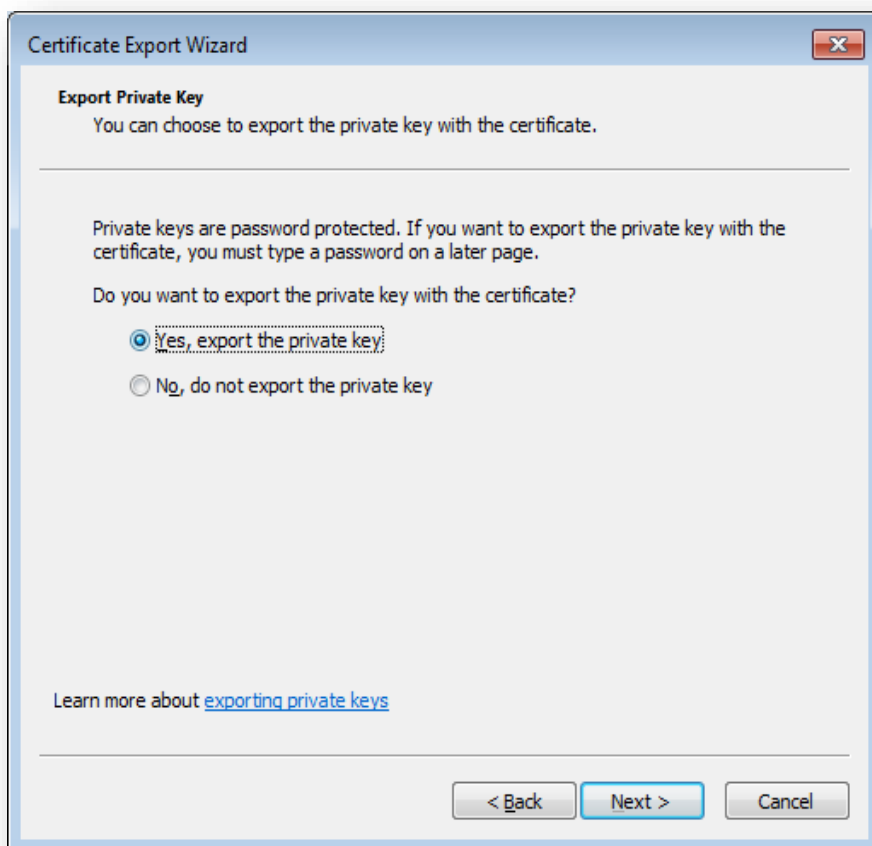
g) Select the Certificate you want to export.



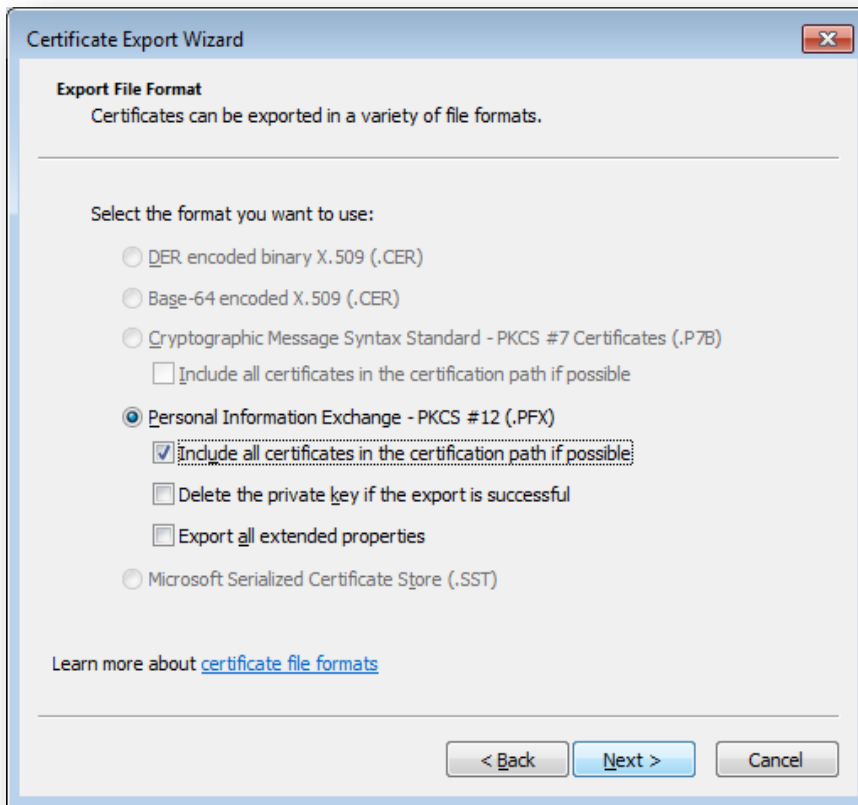
h) After you selected the certificate, click **Export** and then **Next**



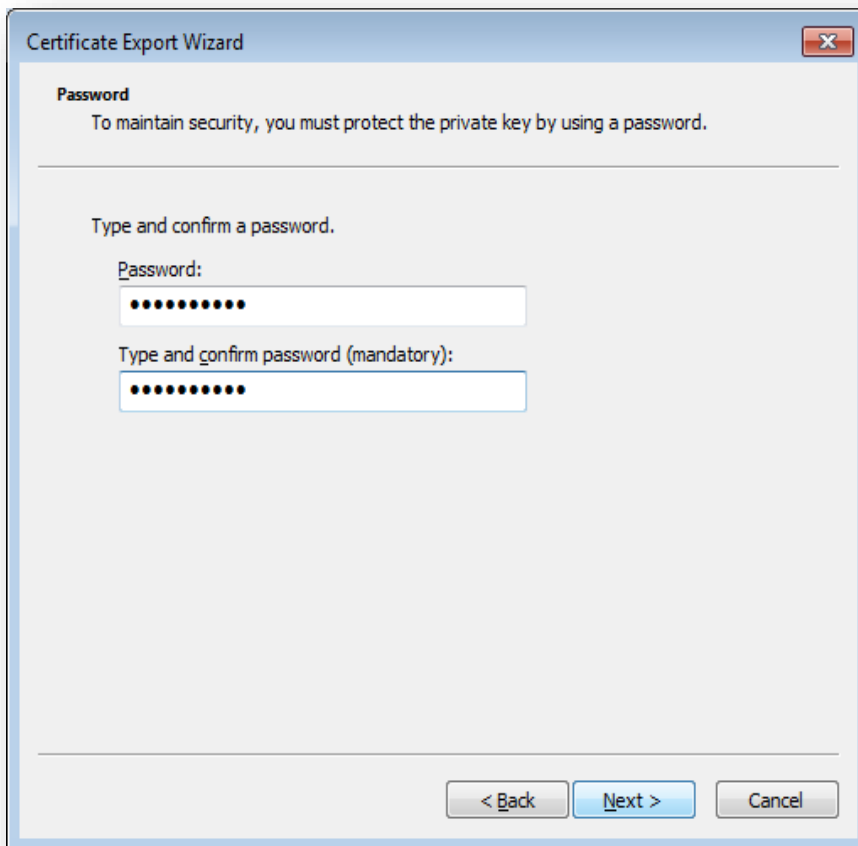
- i) Click **Yes, export the private key** and then **Next**



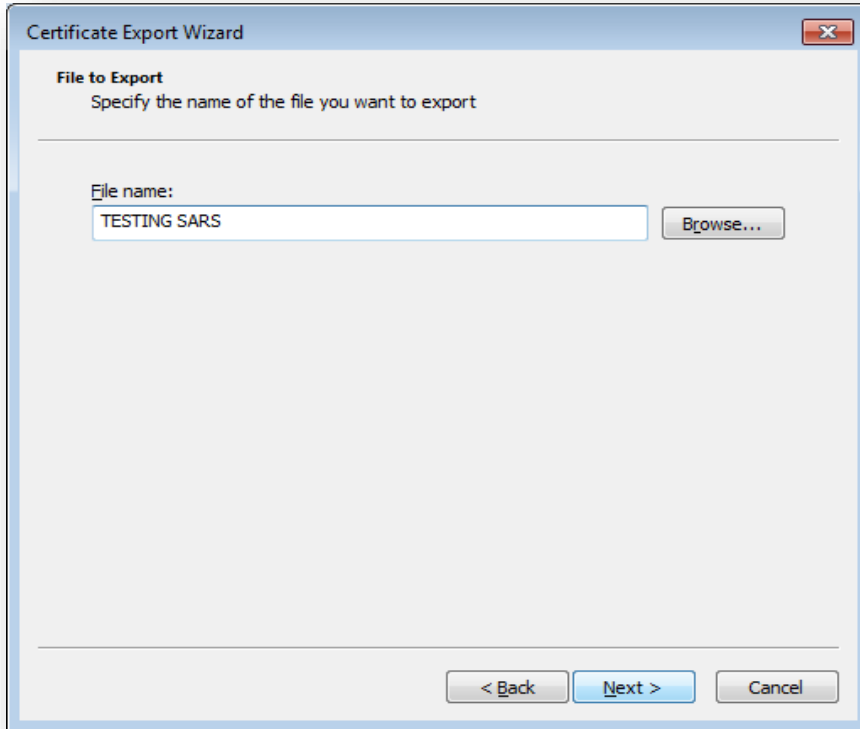
- j) Select **Personal Information Exchange** and click **Next**



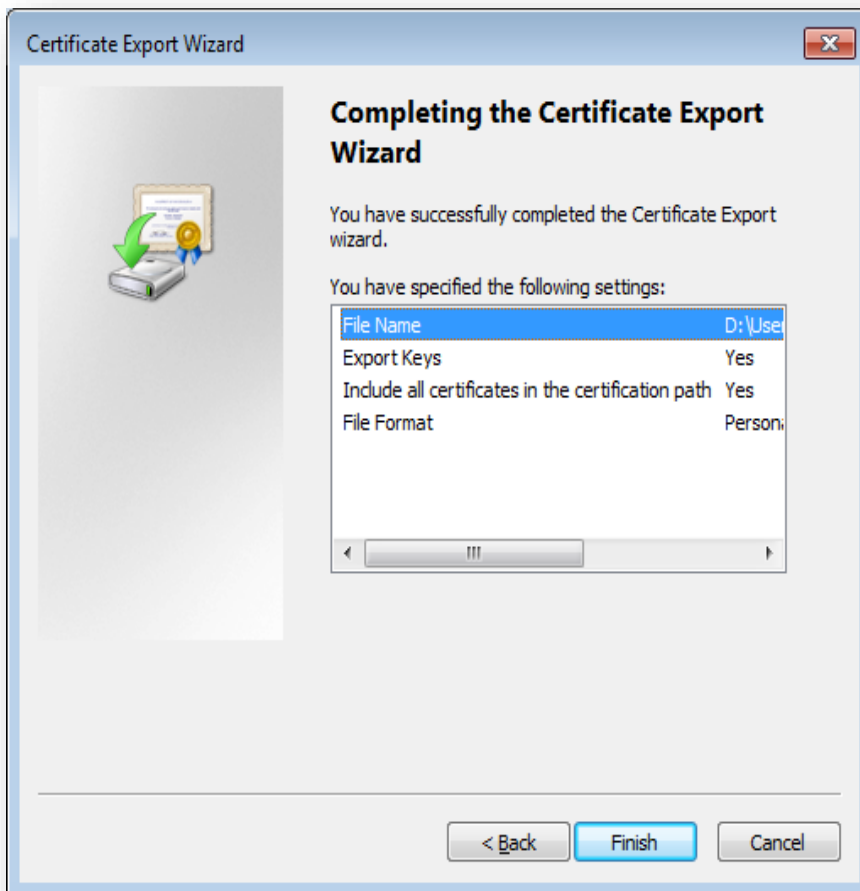
k) Select a password for the private key



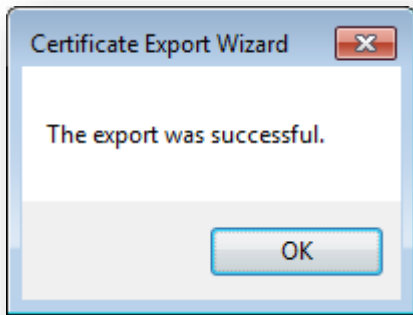
l) Enter a file name and click on **Next**



m) Click **Finish**



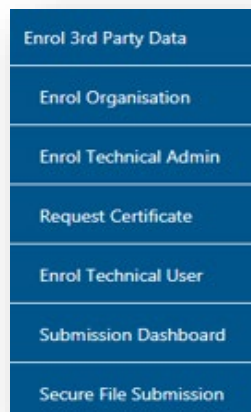
- n) The export was successful.



8 MANAGING TECHNICAL USERS

8.1 Enrolling a Technical User

- a) To enrol a Technical User,
 - i) Click on **Services** on the top menu, and
 - ii) Click **Enrol 3rd Party Data** on side menu.



- b) Select **Enrol Technical User** from the side menu options.
 - i) Do note that a Technical Administrator may not enrol as a Technical User.

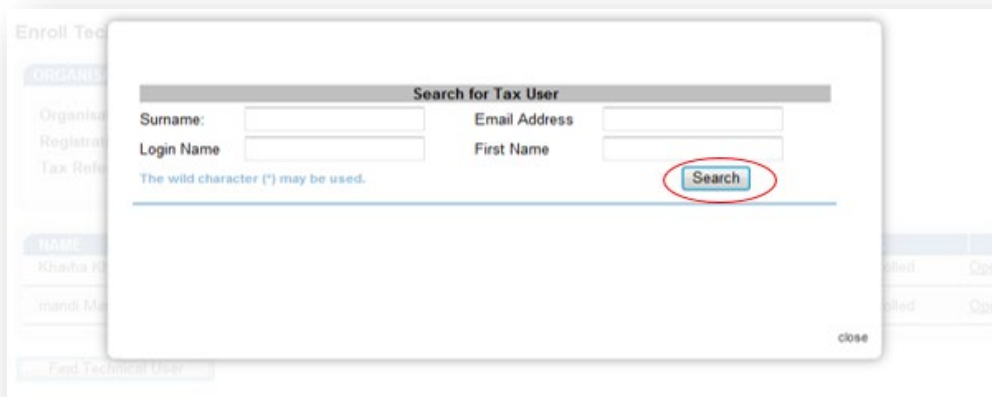
Enroll Technical User for 3rd Party Data Submission

ORGANISATION DETAILS

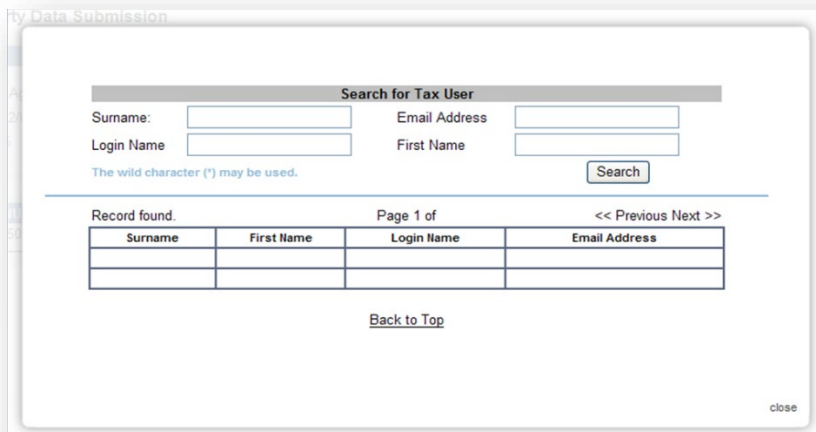
Organisation Name:
Registration Number:
Tax Reference:

NAME	ID NUMBER/PASSPORT NUMBER	ENROLLMENT DATE	STATUS
			Open

- c) Click **Find Technical User** to search and select a Technical User.



- d) Complete the information required and click **Search**. If no values are entered in the above fields, click **Search** and all the registered eFiling users for the relevant organisation will be displayed.

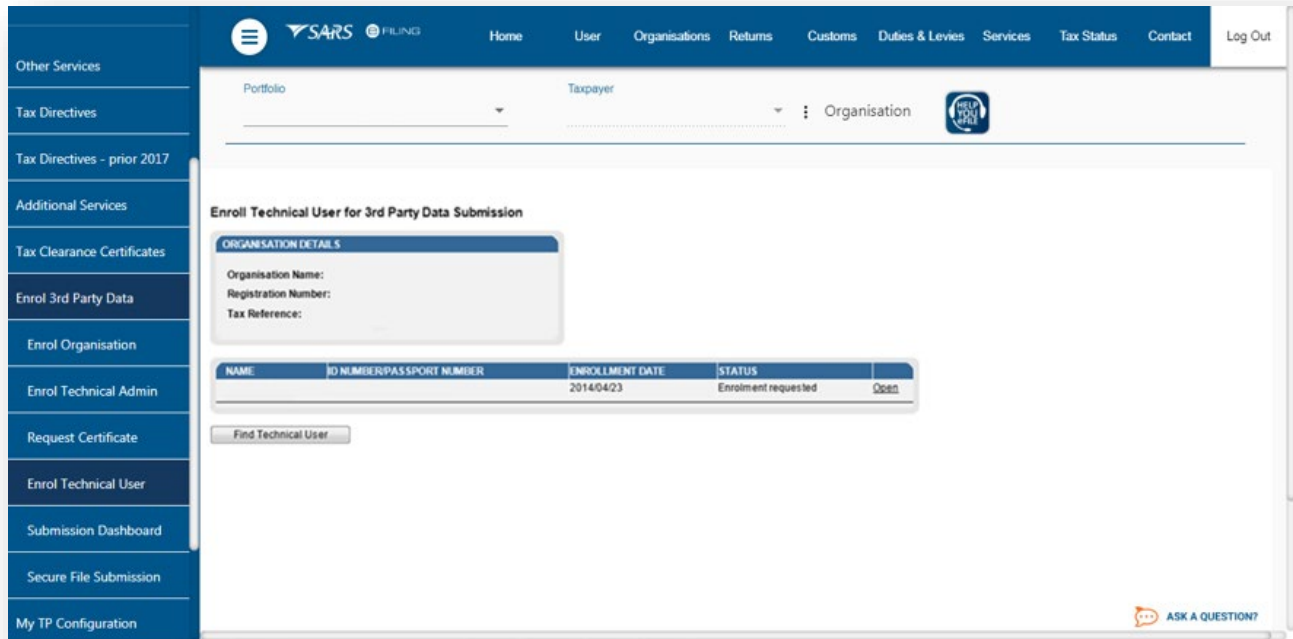


- e) Select the user to be enrolled as a Technical User.



- f) To enrol the selected user,
 - i) Click on **Enrol Technical User**.

Note: It is mandatory to complete the cell phone number of the Technical User as SARS will SMS the log in credentials to this cell phone number.



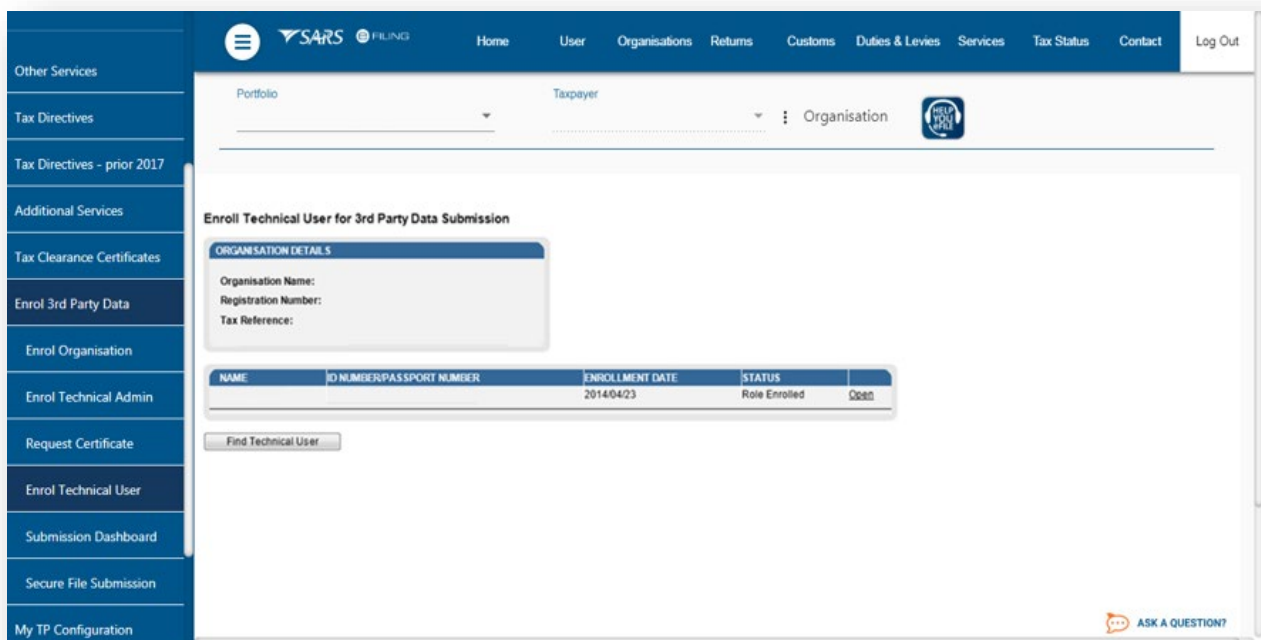
- g) You will be redirected back to the grid page.
- h) In the **STATUS** column, the status **Role Enrolment Requested** will be displayed while SARS is processing the enrolment.
- i) The status **Role Enrolled** will be displayed once the enrolment of the user as a Technical User has been confirmed.
- j) Once the Technical User has been enrolled, a SMS with the above information will be sent to the Technical User.
 - i) The password should be used to sign-in the **SARS Secure File Gateway** The Technical User password will be sent via SMS.
- k) A Technical User can only be deleted once their status has been **Enrolled**.

8.2 Viewing details of a Technical User

- I) To view a Technical User,
 - i) Click on **Services** on the top menu, and
 - ii) Click **Enrol 3rd Party Data** on side menu.



- a) To view all the Technical Users, click **Enrol Technical User**



- b) All the Technical Users will be displayed on the screen. To view the details of a Technical User,
 - i) Click on **Open** next to the relevant user.

Enrol Technical User for 3rd Party Data Submission

USER DETAILS

Name:

ID Number:

Email Address:

Cell Phone:

Telephone Number:

Source Identifier:

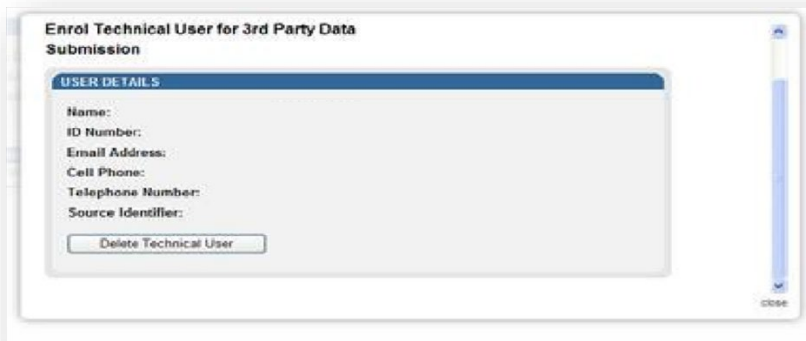
ConnectDirect Username:

close

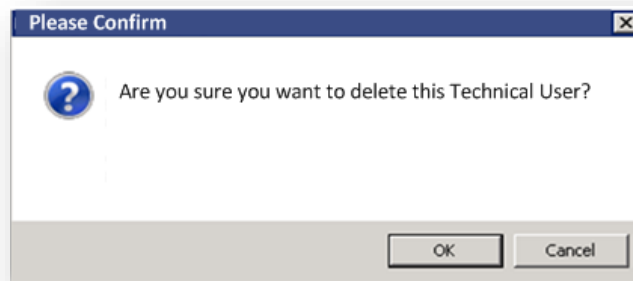
- c) Details of the Technical User will be displayed.
 - i) The **Source Identifier** field must be used in all files submitted by that Technical User on the Direct Data Flow Channel.

8.3 Deleting a Technical User

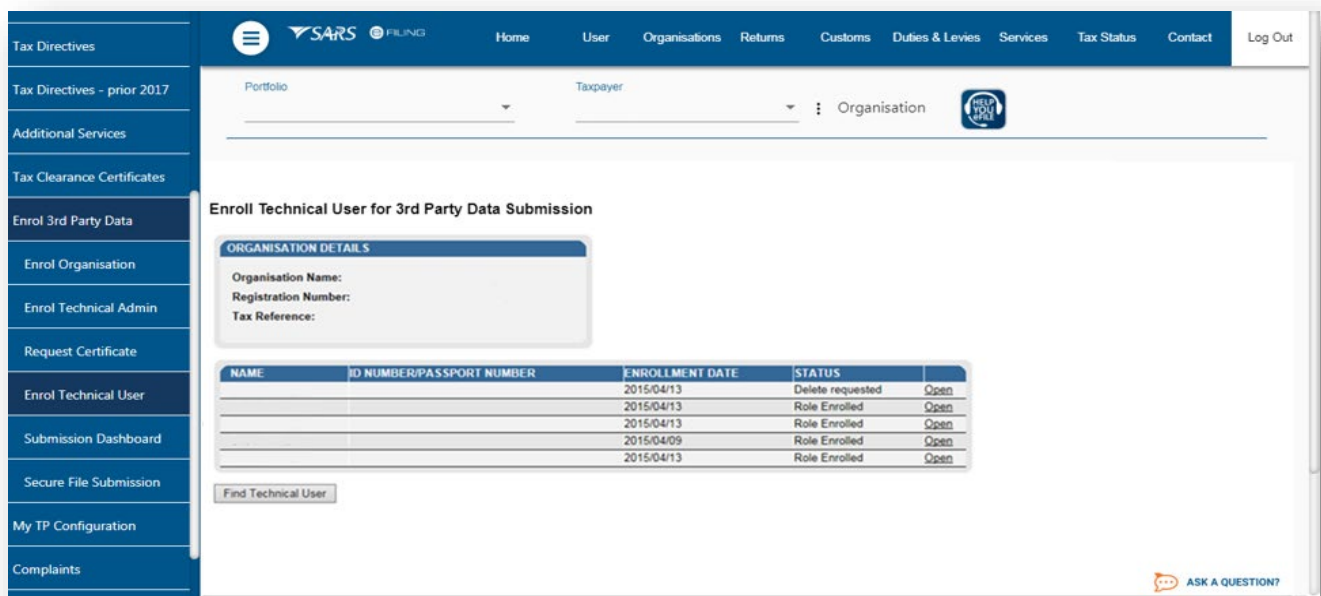
- a) To delete a Technical User,
 - i) Click on **Open** next to the Technical User that is to be removed on the **Enrol Technical User for 3rd Party Data Submission** page.



b) Click **Delete Technical User** to remove the Technical User.



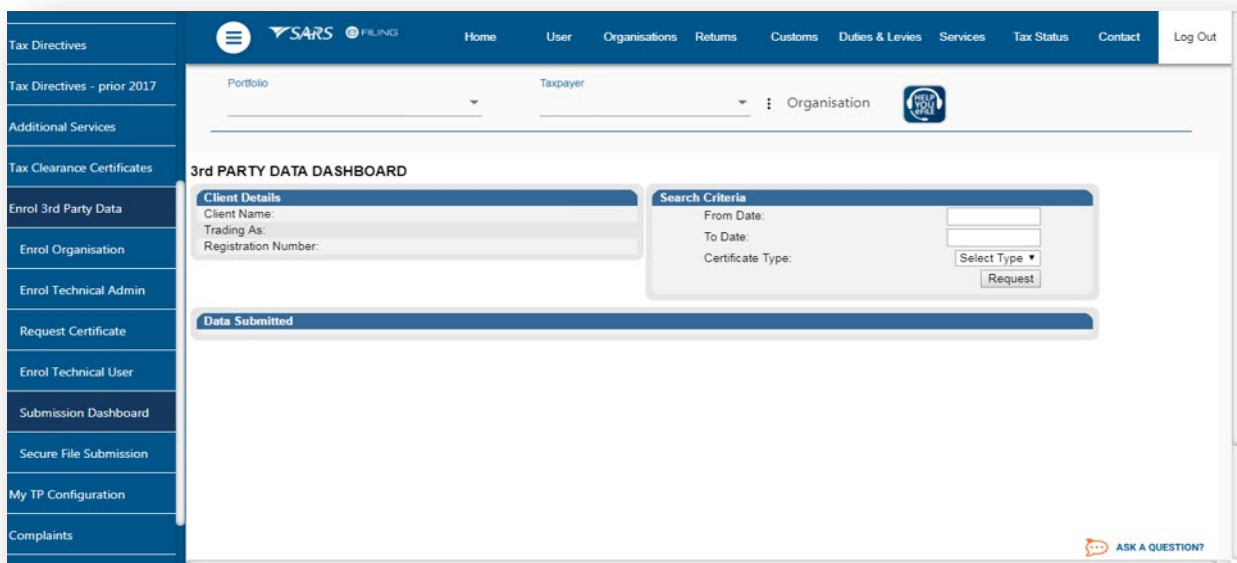
c) You will be prompted to confirm if the Technical User must be deleted. Selecting **OK**, will delete the Technical Administrator. To cancel the deletion, select **Cancel**.



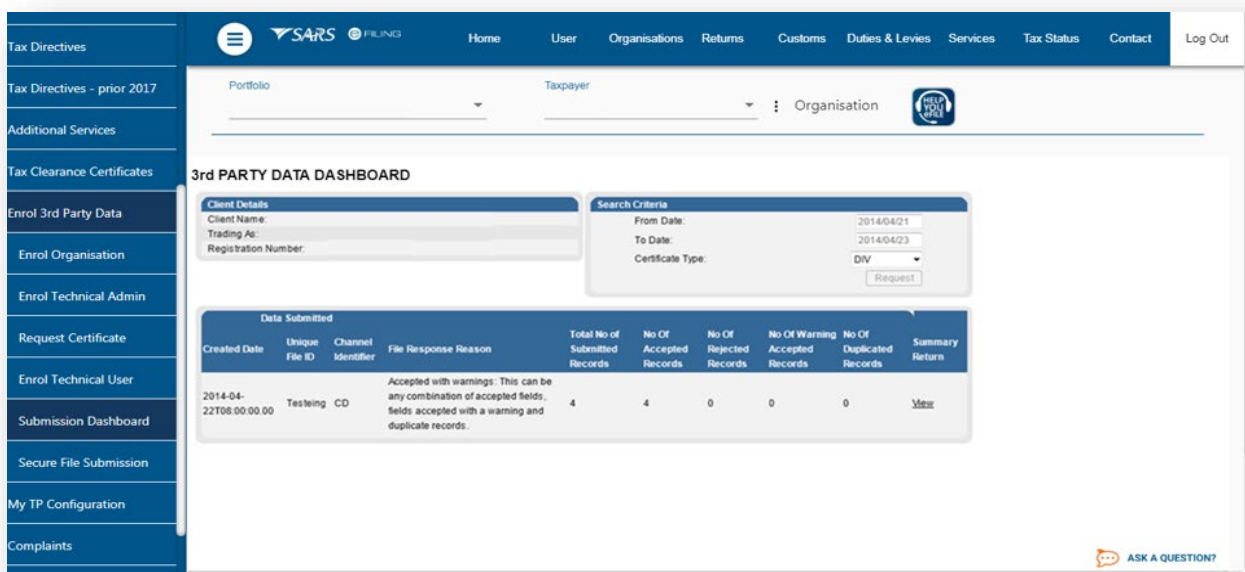
- d) In the **Status** column, the status **Delete Requested** indicates that the request to delete the user as a Technical User has been submitted to SARS. The status **User Deleted** will be displayed once the enrolment of the Technical User has been cancelled on SARS's systems.
- e) The deleted Technical Users will not be displayed on the screen.

9 SUBMISSION DASHBOARD

- a) The user must be logged in as a Technical Administrator or Technical User to be able to view the **Submission Dashboard**.



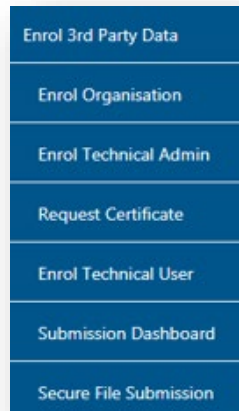
- b) To view the **Submission Dashboard**, go to **Services** on the top menu, then click **Enrol 3rd Party Data** on side menu. Select **Submission Dashboard** from the side menu.



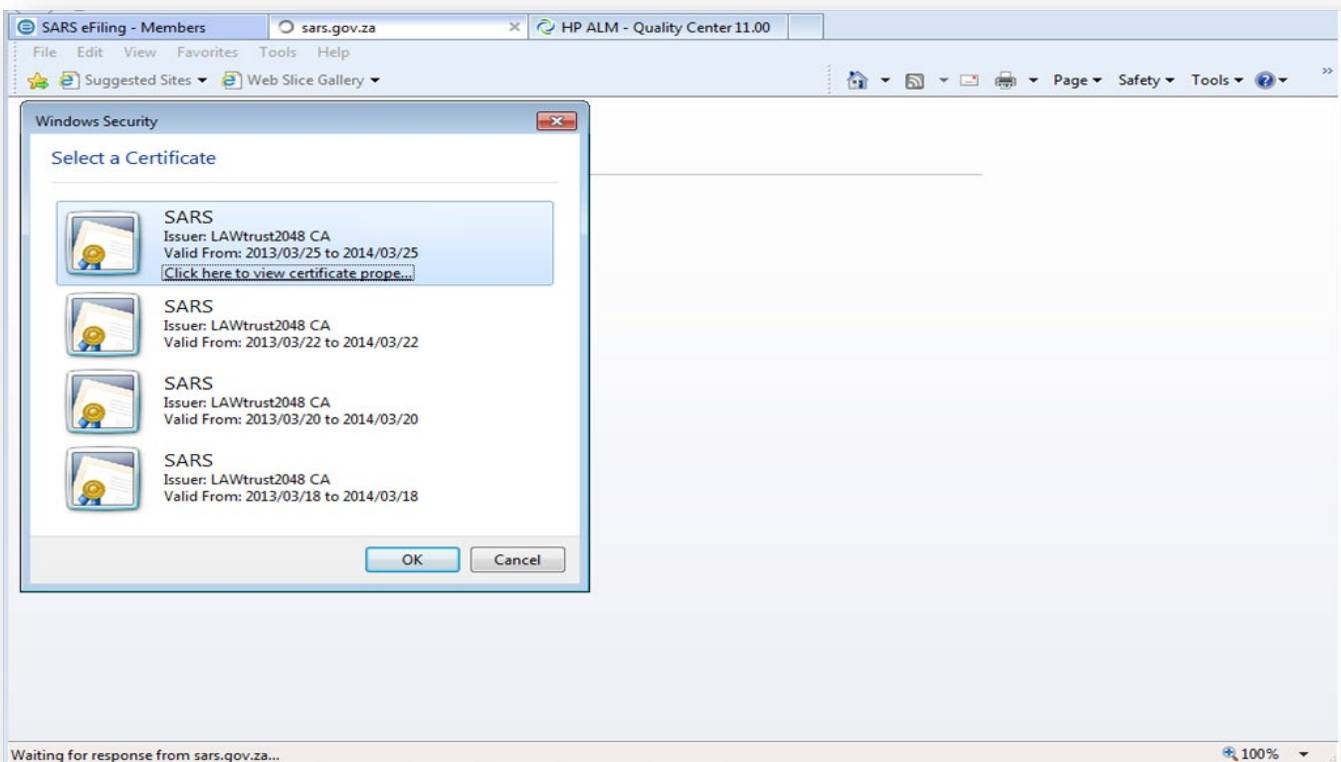
- c) In the **Search Criteria**, you will not be able to enter the **From Date** and **To Date** fields. You will have to click **Request** to ensure that the latest status information is displayed on the dashboard.

10 SUBMISSION OF DATA FILES TO SARS

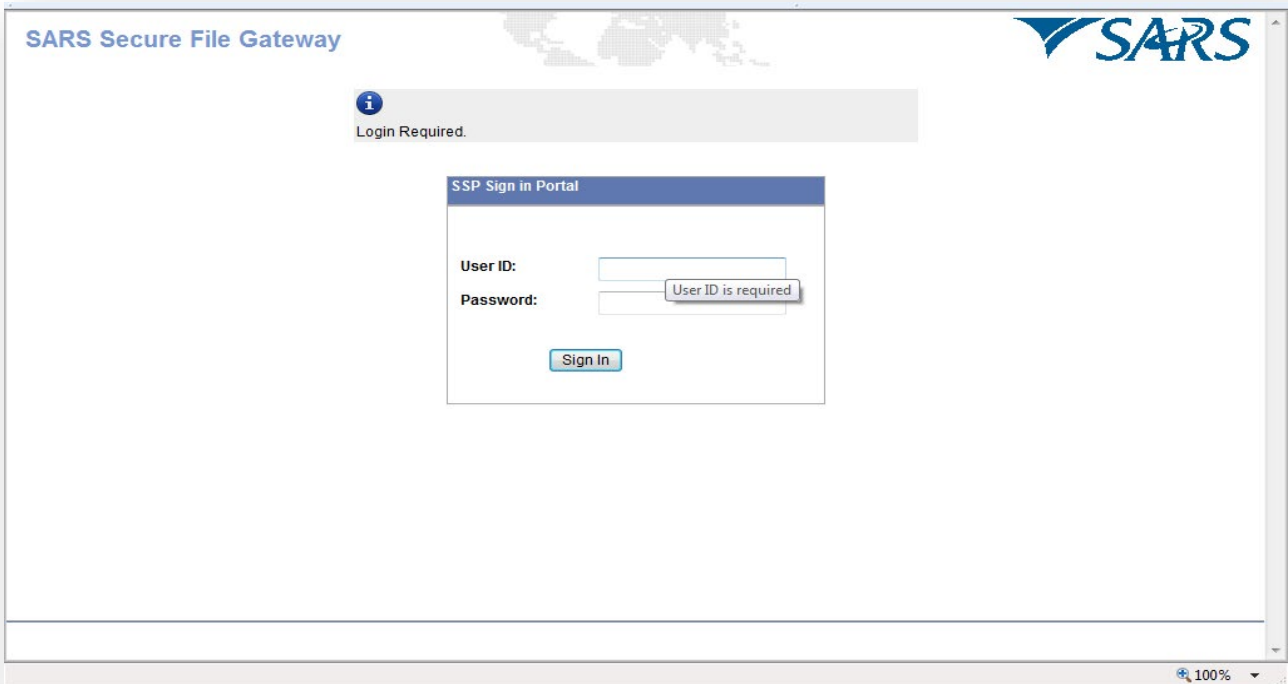
- a) To access the **Secure File Submission**, Click on **Services** on the top menu, and then click **Enrol 3rd Party Data** on side menu.



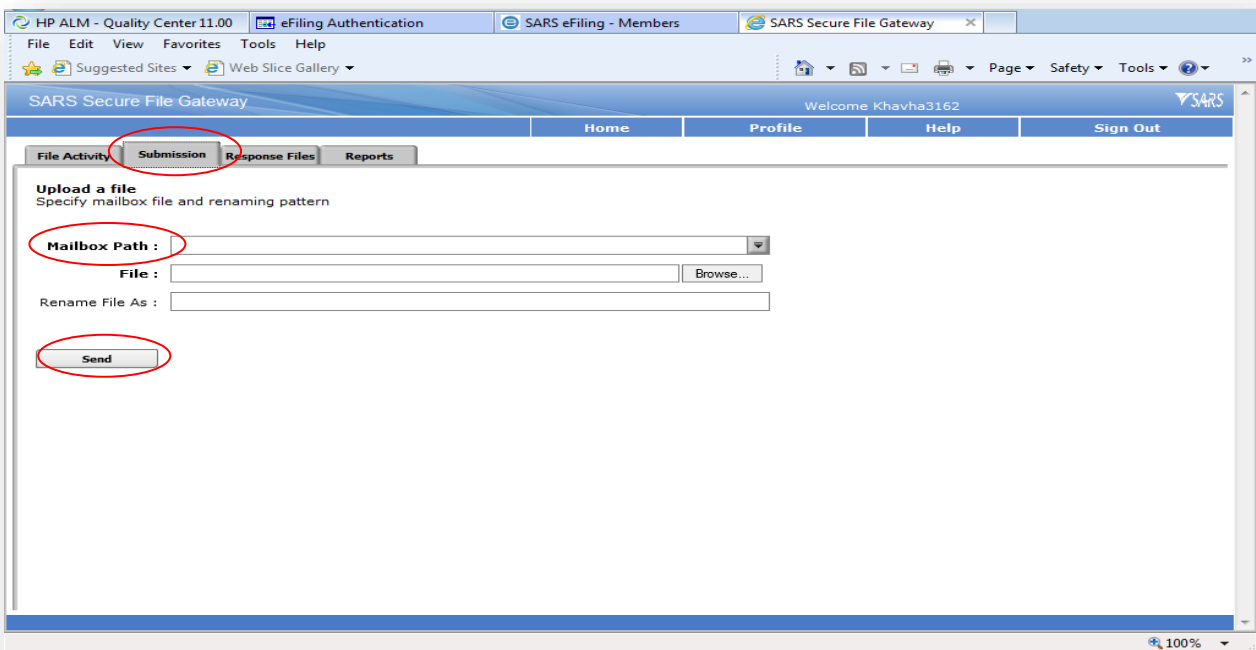
- b) Select **Secure File Submission** from the side menu
- c) Note that port 60600 (Login page) and 60666 (password resend) should be enabled on your network. Your IT department should be able to assist you with opening the ports.

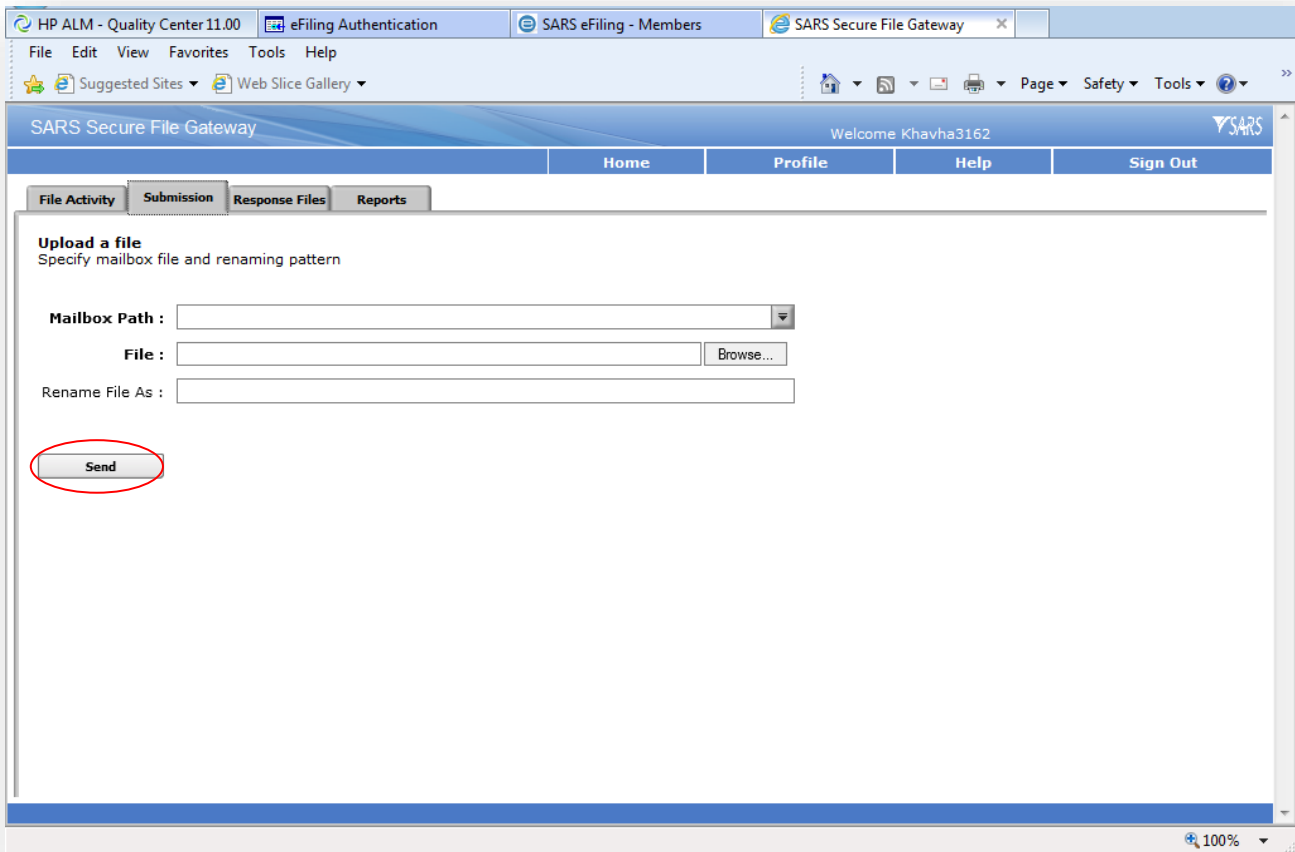


- d) A list of certificates ready for submission will display. Select the certificate you want to submit to SARS.
- e) You will be routed to the Secure File Gateway site.

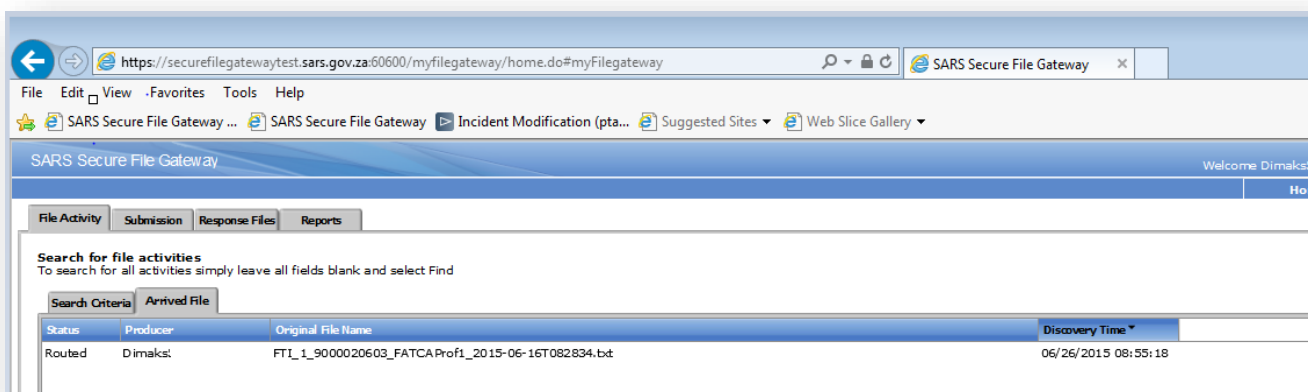


- f) Use the user ID and password as provided to a Technical User as per sms received from SARS.
- g) Click on the **Submission** tab.
- h) From the Mailbox Path' drop-down box you should always select “/” only, then select **Browse** to attach file to be submitted to SARS.





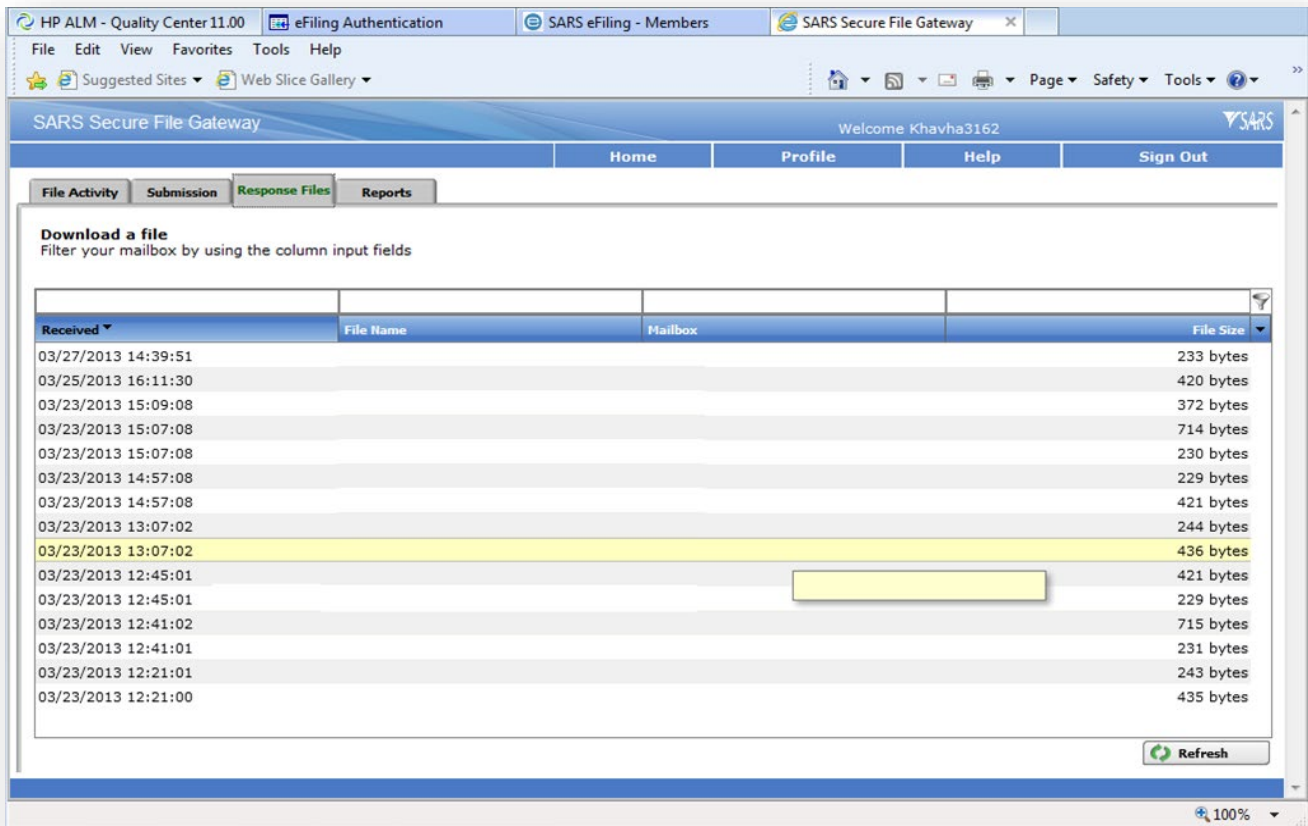
i) Select **Send** button to submit the file to SARS.



j) The status should show as "Routed".

i) This indicates that the file was send to SARS successfully.

k) Click on the **Response Files** tab to view statuses of other files submitted to SARS via this channel. Depending on the size of the file a response file will be send from SARS within few minutes.



- l) Note: Save the file immediately before opening it because once it has been opened it is going to be moved from the list/mailbox. Submitted files can be viewed by using the submission dashboard.

11 DEFINITIONS AND ACRONYMS

Link for centralised definitions, acronyms, and abbreviations: [Glossary A-M | South African Revenue Service \(sars.gov.za\)](https://www.sars.gov.za/glossary)

DISCLAIMER

The information contained in this guide is intended as guidance only and is not considered to be a legal reference, nor is it a binding ruling. The information does not take the place of legislation and readers who are in doubt regarding any aspect of the information displayed in the guide should refer to the relevant legislation or seek a formal opinion from a suitably qualified individual.

For more information about the contents of this publication you may:

- Visit the SARS website at www.sars.gov.za;
- Make a booking to visit the nearest SARS branch;
- Contact your own tax advisor / tax practitioner;
- If calling from within South Africa, contact the SARS Contact Centre on 0800 00 SARS (7277); or
- If calling from outside South Africa, contact the SARS Contact Centre on +27 11 602 2093 (only between 8am and 4pm South African time).