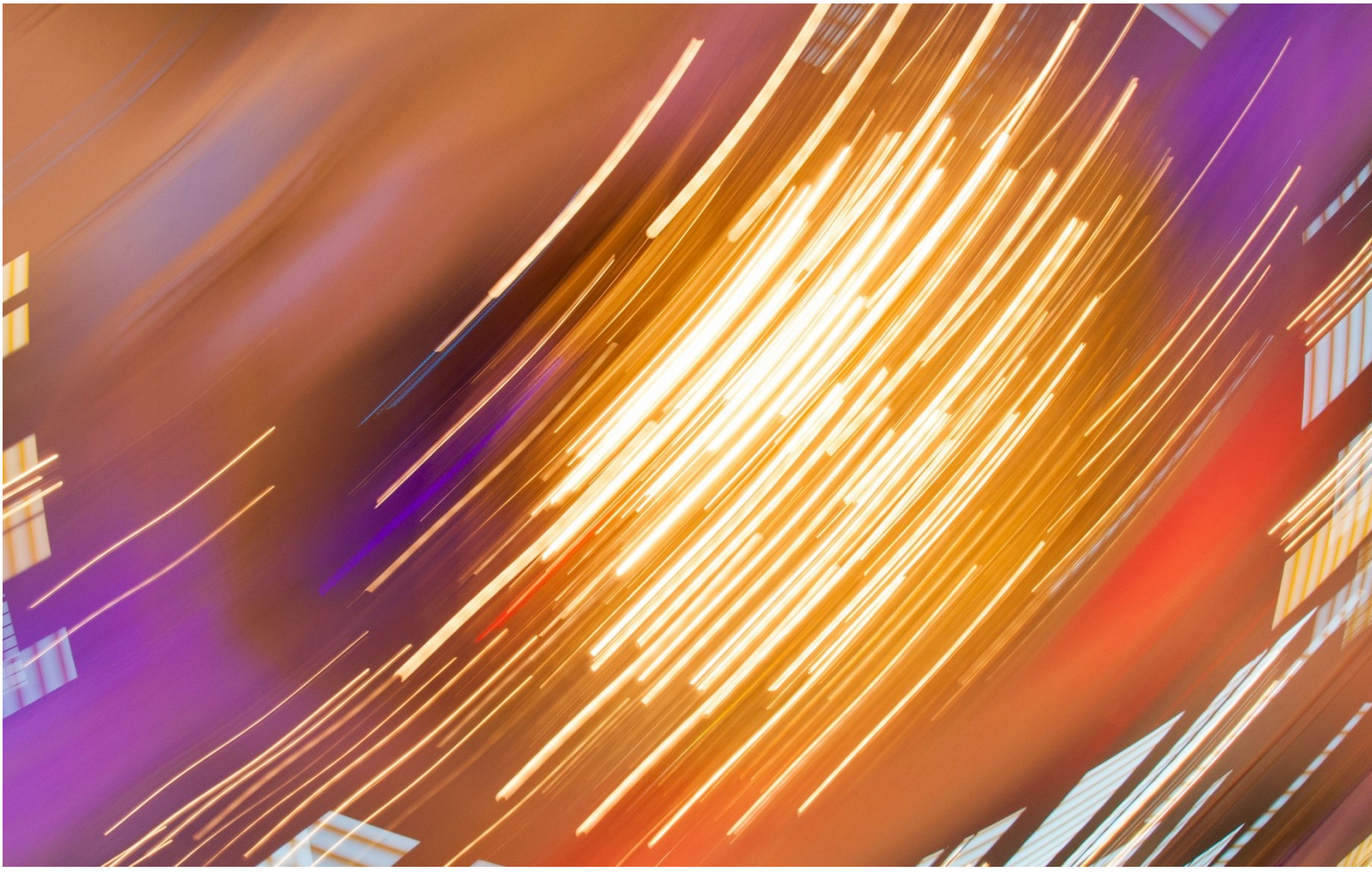
NHS e-Referral Service API Connectivity Guide v1.9



Information and technology for better health and care

Document filename: NHS e-Referral Service API Conenctivity Guide - 1.9.pdf			
Directorate / Programme	e-Referral Service	**Project**	API Integration
Document Reference			
Project Manager	Tony Marsh	**Status**	Draft
Owner	Phil Nixon	**Version**	1.9
Author	Sami Mohammed	**Version issue date**	08/04/2020

Document management

Revision History

Version	Date	Summary of Changes
1.0	21/07/17	Approved version
1.1	01/11/17	Updated content for API Client Demonstrator Tool
1.2	22/12/17	Changes to Client Demonstrator Tool
1.3	11/01/18	Updated the snapshots
1.4	03/05/18	Made changes to the URL reference from mhsin to api
1.5	21/05/18	Added pre-requisite steps for Postman connectivity
1.6	31/05/18	Added pre-requisites for IA Agent and unblock the IP addresses
1.7	20/07/18	*SA Service Desk* references replaced with *Platforms Support Desk*
1.8	21/05/19	Made minor amendments
1.9	08/04/20	Removed reference to the discontinued ‘API Demonstrator Tool’

Contributors

Contributor name	Title/ Responsibility	Date	Version
Sami Mohammed	Test & Assurance Manager	21/05/2019	V1.8
Nick Hay	Product Owner - eRS APIs	18/04/20	V1.9

Contents

1 Introduction

This document explains how a to connect to the NHS e-Referral Service APIs using an API testing tool, in this case Postman has been used. There are some pre-requisite steps, detailed in the next section, to carry out before these tools can be used to check the API connectivity.

Prior to these steps a Test Pack and Smartcards for DEV1 must be issued by platforms.supportdesk@nhs.net, for more details please visit the Get Connected page on the e-RS API Hub.

2 Pre-requisites

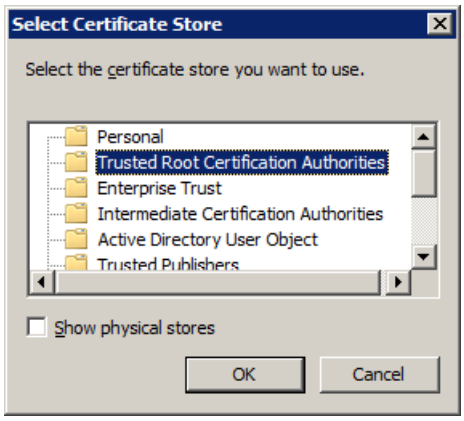
1) *CSR (Certificate Signing Request) and Private Key*. If you don't have already then please generate CSR and Private Key for your FQDN going through "How to generate CSR and KEY" section at the end of the document.

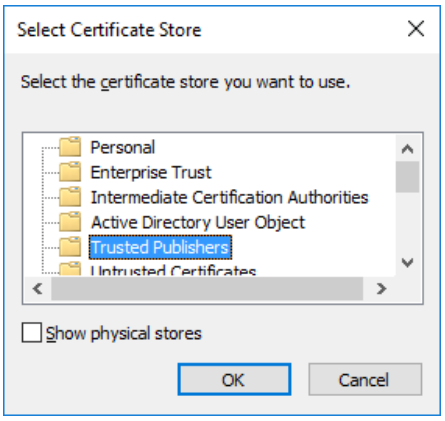
2) *Endpoint Certificate*. If you don't have already please raise a service request with Platforms Support Desk platforms.supportdesk@nhs.net for registering your endpoint using the EPR Form and CSR above.

   Note: Platforms Support Desk will create and provide an Endpoint Certificate, ASID (Accredited System Identifier) and MHS Party key for your endpoint. The endpoint certificate and Private Key can be used to create a client certificate.

3) *RootCA and SubCA Certificates* – The RootCA and SubCA certificates are available at http://www.assurancesupport.digital.nhs.uk/downloads under "Root and SubCA Certificates" to install. Copy the certificates content into a notepad file and save as RootCA.der and SubCA.der.

   Note: Instead of Windows automatically selecting a certificate store, you specify a location of Trusted Root Certification Authorities or Trusted Publishers for the Root CA certificate and Intermediate Certification Authorities for Sub CA certificate as per your Windows configuration.





4) *Registry Settings* – Install the "IAConfig2.msi" from IAConfig.zip file from http://nww.hscic.gov.uk/dir/downloads/index.html#ia_config. Once installed you should be able to apply the DEV Registry settings to access the e-RS/DEV3 environment.

5) *Identity Agent* – Install Identity Agent and Middleware from here http://nww.hscic.gov.uk/dir/downloads/index.html.

6) *Unblock IP Addresses* – Ensure the below IP addresses are unblocked from your firewalls.

   api.dev3.ers.ncrs.nhs.uk 155.231.120.230 port:443
   nww.dev3.ers.ncrs.nhs.uk 155.231.120.233 port:443
   gas.vn03.national.ncrs.nhs.uk 10.196.94.119 port:443
   portal.vn03.national.ncrs.nhs.uk 10.196.94.116 port:443

7) *Smartcard* – Ensure a valid DEV smartcard with e-RS roles is available
Note: Platforms Support Desk would have sent this along with the API Test Pack.

8) *Postman Tool* - Install full version of Postman tool e.g. Postman-win32-5.0.2-Setup and not just the Chrome add-in for Postman.

9) *Keystore Explorer* - Install Keystore Explorer tool e.g. KeyStore Explorer 5.2.2 to create a Keypair.

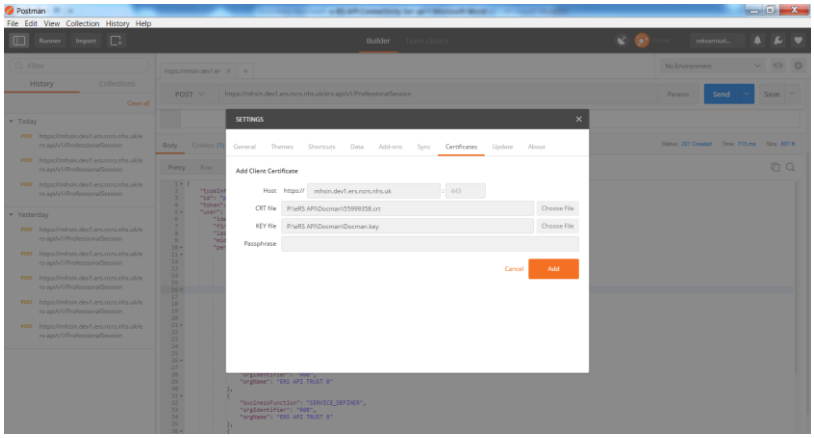
10) User will need to have admin privileges to install some of the above installable such as Postman, Keystore Explorer, IA Agent etc.

3 Postman Set up

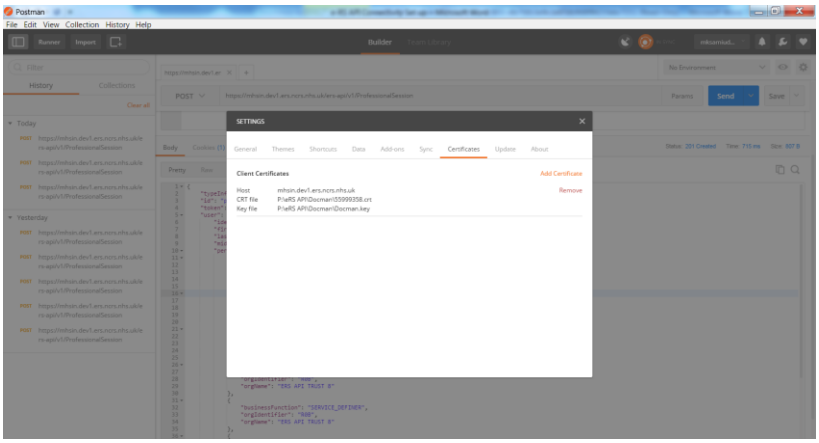
Postman is a Google Chrome app for interacting with HTTP APIs. It presents you with a friendly GUI for constructing requests and reading responses. It can be used to establish initial connectivity with the APIs after which you can use your own solution to talk to the APIs.

1) Navigate to File -> Settings -> Click on Add Certificate to enter the following details:

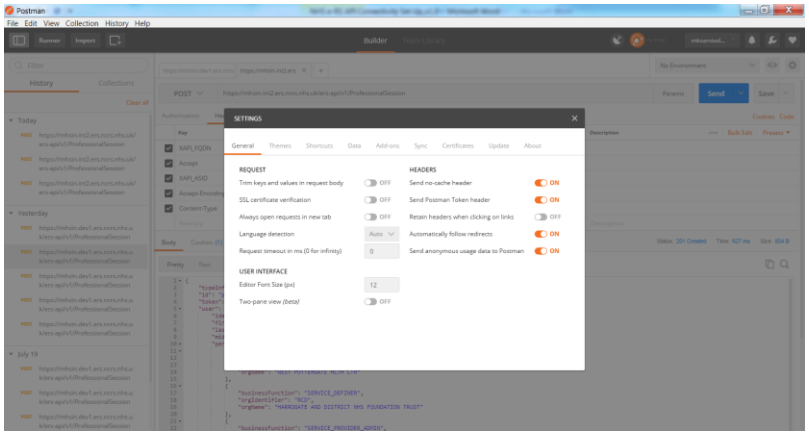
   Host: The URL for e-RS API e.g. https://api.dev1.ers.ncrs.nhs.uk/ers-api/
   CRT file: Choose the endpoint certificate provided by Platforms Support Desk
   KEY file: Choose the private key file that you have generated



   Clicking on Add button should add a client certificate which looks as below.



2) Make sure the 'SSL certificate verification' in Settings - General tab is turned off.



3) Close the Settings dialog and go back to Postman editor to carry out the following configuration for Header:

3a) Select the request type - 'Post'.

3b) Enter the request URL for the API.

https://api.dev3.ers.ncrs.nhs.uk/ers-api/v1/ProfessionalSession

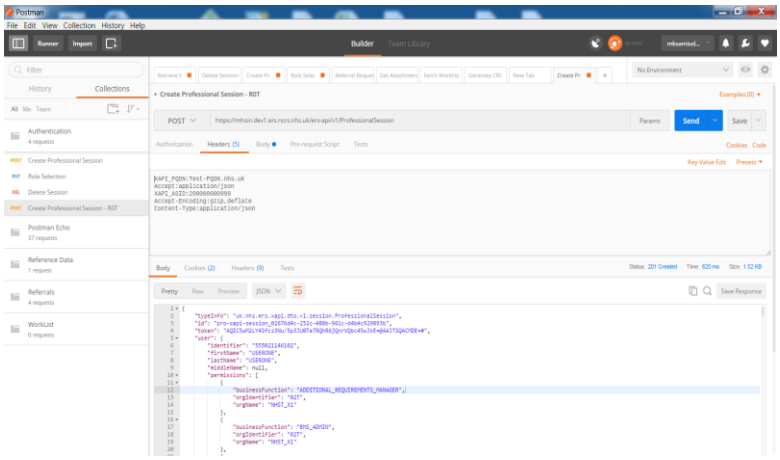
3c) Click on 'Bulk Edit' option under Headers to enter multiple request Header values at a time otherwise add them individually.

XAPI_ASID:200000000220 (Please ensure you are using the ASID provided by Platforms Support Desk for your endpoint and NOT the one provided in this example)

Accept:application/json

Accept-Encoding:gzip,deflate

Content-Type:application/json



4) Navigate to the Request Body and select the type as 'raw' and enter the body content as below.

{

"typeInfo": "uk.nhs.ers.xapi.dto.v1.session.ProfessionalSession",

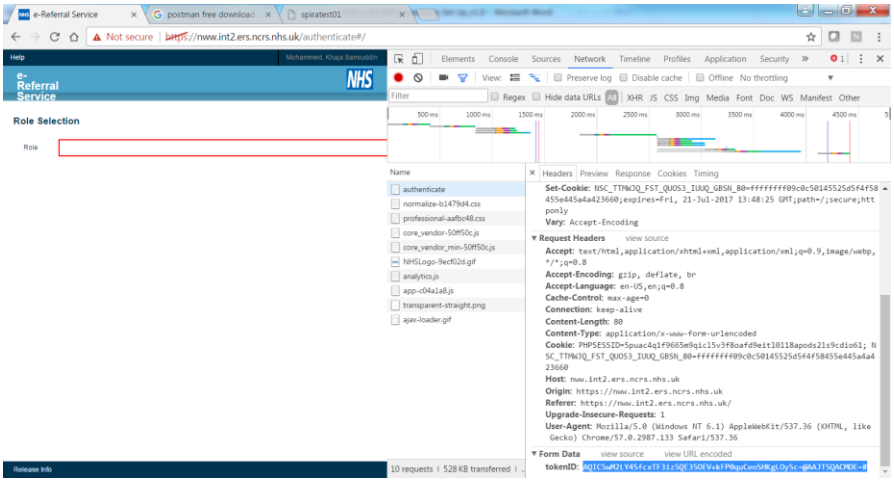
"token":
"AQIC5wM2LY4SfcxCJrmZROc+po/eHhoaoR4apy5SUQ+fFYE=@AAJTSQACMDE=#"

}

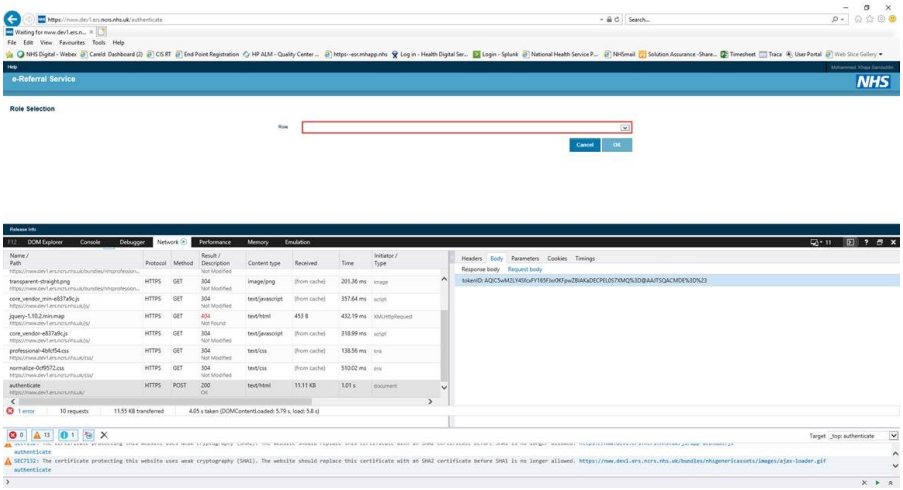
The token value can be accessed by inserting Smartcard into the Reader; authenticating to Spine and then logging onto e-RS Professional Application using Google Chrome/Internet Explorer at https://nww.dev3.ers.ncrs.nhs.uk/authenticate#/

Press F12 -> Network -> All -> then F5 -> Select the authenticate option to get the TokenID.

Google Chrome:

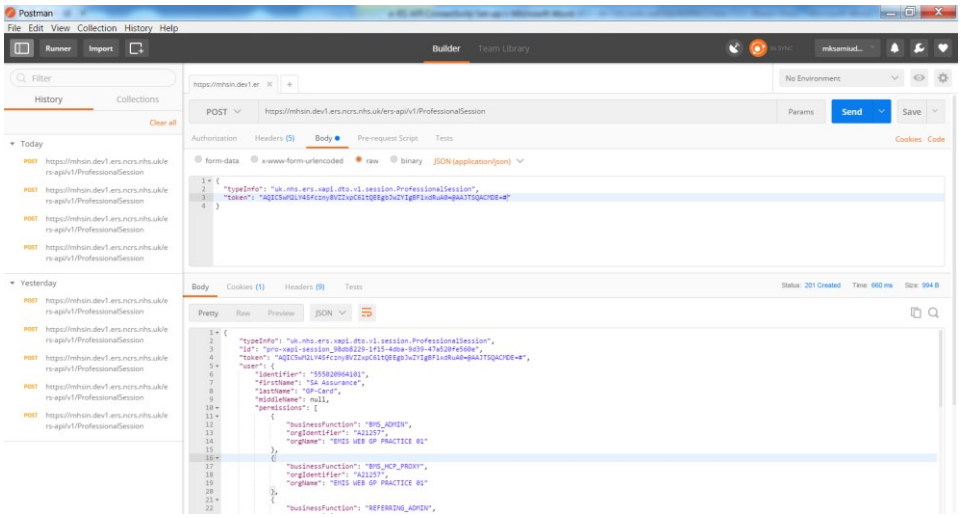


Internet Explorer:



Note: If the token is generated using Internet Explorer, it will be available in encoded format. So, make sure it is decoded before using it. This can be done using https://www.urldecoder.org/

5) Clicking on the 'Send' button should return the successful response with a status 201 Created as below. This request then can be saved for future use under Collection.



Note: If 'Unauthorised access' or some other error occurs, it could be that the configuration was not done properly or some firewall issues.

4 How to generate CSR and Private Key

1) Install openssl using the below link:

https://www.tbs-certificates.co.uk/FAQ/en/openssl-windows.html

or

http://slproweb.com/products/Win32OpenSSL.html

2) Once installed, Open Command Prompt and run the below command to configure the openssl.cfg file

   C:\OpenSSL-Win32\bin>**set OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg**

3) Change the dir to OpenSSL-Win32/bin and run the below command to generate the CSR by replacing the blue coloured FQDN and org code e.g. O=ROB with yours:

   openssl req -new -newkey rsa:2048 -nodes -out Test-FQDN.cfh.nhs.uk.csr -keyout Test-FQDN.cfh.nhs.uk.key -subj "/C=GB/ST=/L=na/O=ROB/OU=na/CN=Test-FQDN.cfh.nhs.uk"

4) The CSR along with the Private Key will be generated and available in C:/OpenSSL-Win32/bin folder as per the above FQDN details.