Sentinel

safer
smarter
simpler

Sentinel smartcard PC client application

Installation and configuration guidelines

Table of contents

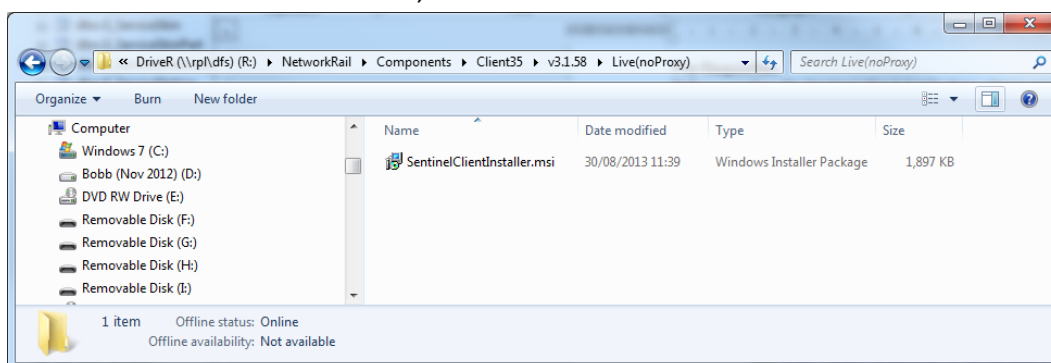# 1. Application installation

1.1.   Pre-requisites

Before installing the Sentinel Client Application, please ensure the following pre-requisites are fulfilled:

- Ensure you are installing to an MS Windows PC running XP (SP2) or later version of MS Windows. The application is compatible with both 32bit and 64bit versions of MS Windows.

- Ensure the Microsoft .NET framework v3.5 (SP1) is installed. The Sentinel Client installation MSI will attempt to download/install this directly from Microsoft if not already installed.

- Ensure you have a PC/SC compatible Smartcard reader connected to your PC and the appropriate manufacturer's device drivers have been downloaded and installed. A list of recommended PC connected readers can be found on the Sentinel website at the bottom of this page HERE

- Ensure you have downloaded the latest version of the Sentinel Smartcard Client software from the Sentinel website, which can be found at the bottom of this page: HERE

- Ensure you have 'administrator' level access to the PC on which you will be installing the software, without administrator level access, you will not be able to install the Sentinel client application – you may need to ask your I.M. department to install this software for you.

- Ensure your PC has internet connectivity. Without connectivity, the Sentinel Client application will not be able to read or updated Sentinel smartcards.

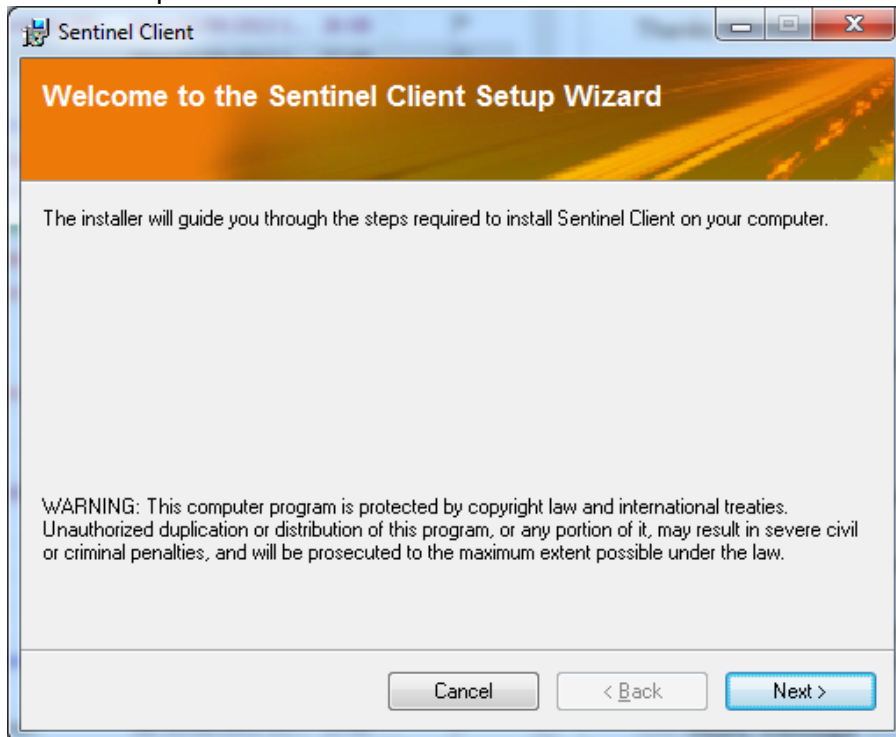## 1.2.   Installing the Sentinel PC client application

To start the software installation, **double-click** the **Sentinelclientinstaller.msi**
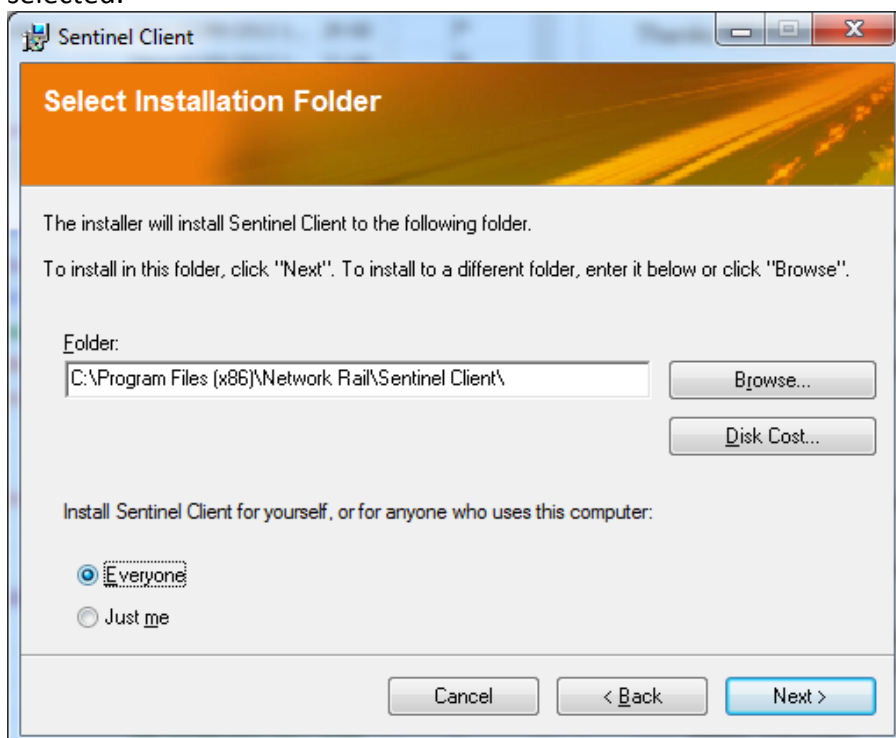
You will be presented with an initial installation confirmation window, click **Next** to proceed.

When prompted to choose an Installation folder, for most users the default installation location should be selected.
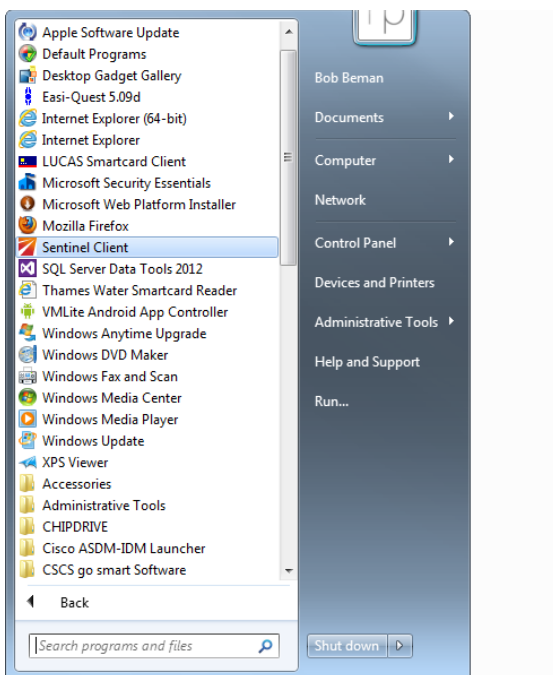
2. Using the Sentinel client

2.1 Starting the Sentinel client

Before starting the Sentinel Client, ensure you have the card reader connected to your PC. A shortcut to the **Sentinel Client** will have been created on your desktop, and also on the start Menu. Launch the Sentinel Client by clicking either of these.

Once started, the Smartcard client will show the **Sentinel Smart Card Reader** window listing the connected smartcard readers that the application has successfully detected. Also, the Sentinel Client Icon will be displayed in the System tray.
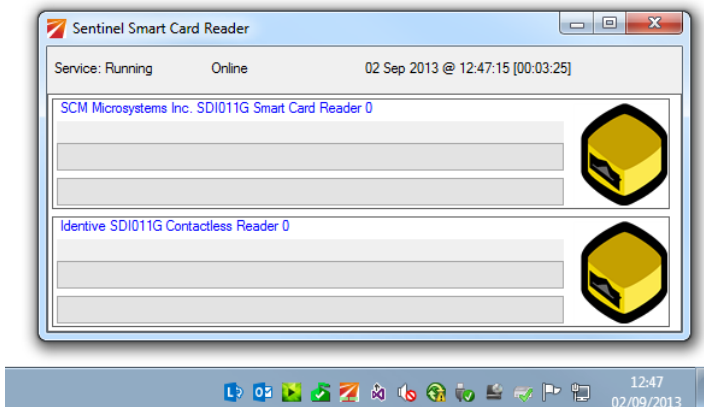
2.2 Checking/synchronising a card with the Sentinel client

The Sentinel smartcards are read electronically using Near Field Communications (NFC). To read/check a Sentinel smartcard, place the card on the Smartcard reader, the Sentinel Client application will detect the card, and provide visual confirmation by means of the green progress indicators that the card is being read/and if necessary synchronised(updated) as shown below.
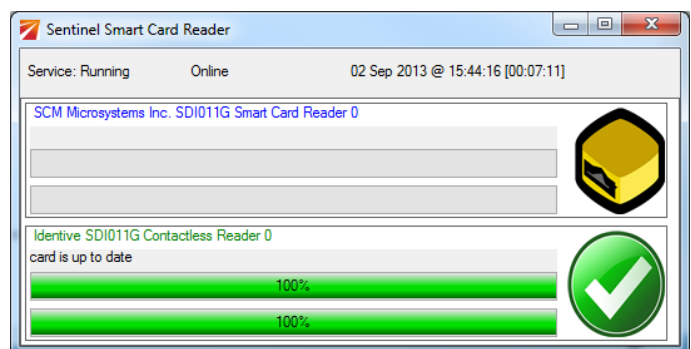
Once the card has been synchronised, a second window will open, to allow the user to choose the cardholders current sponsor.
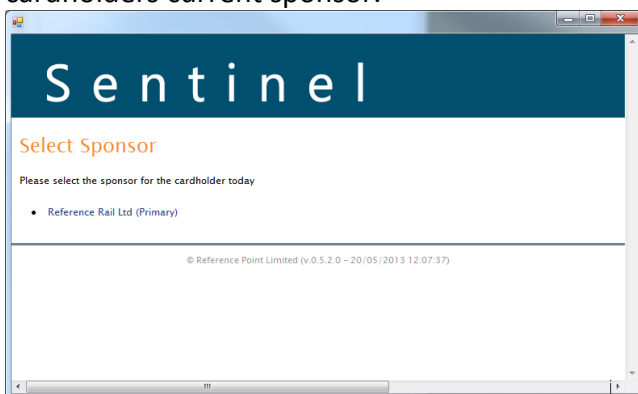
Upon confirmation of the cardholder's sponsor, the option to **View Card** will be presented.   Note, if the cardholder has been authorised to **Spot Check** and **Swipe-In** other cards, these options will also be shown.
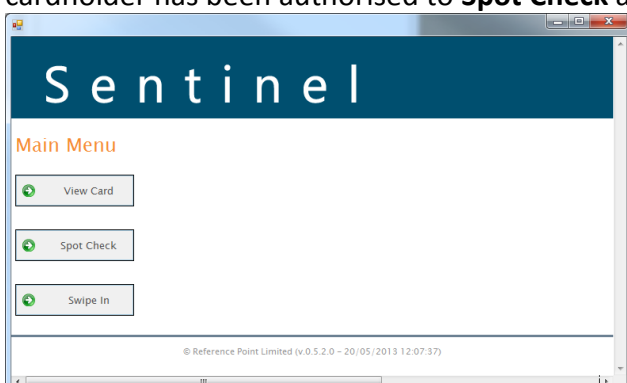
Upon choosing **View Card,** visual confirmation of the card appearance and status and all cardholder comptences can be viewed. To check / synchronise another card, simply place the next card on the reader and repeat the process.
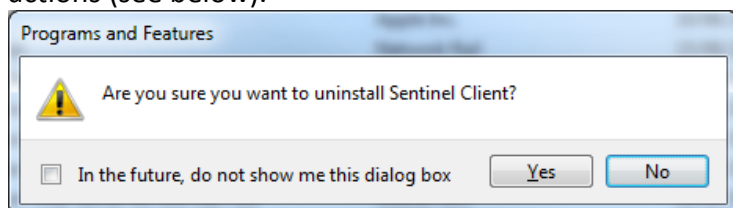

3. Uninstalling the Sentinel client application

To uninstall the Sentinel Smartcard Client, you must choose the option to **Add/Remove programs** from the windows **Control Panel**.
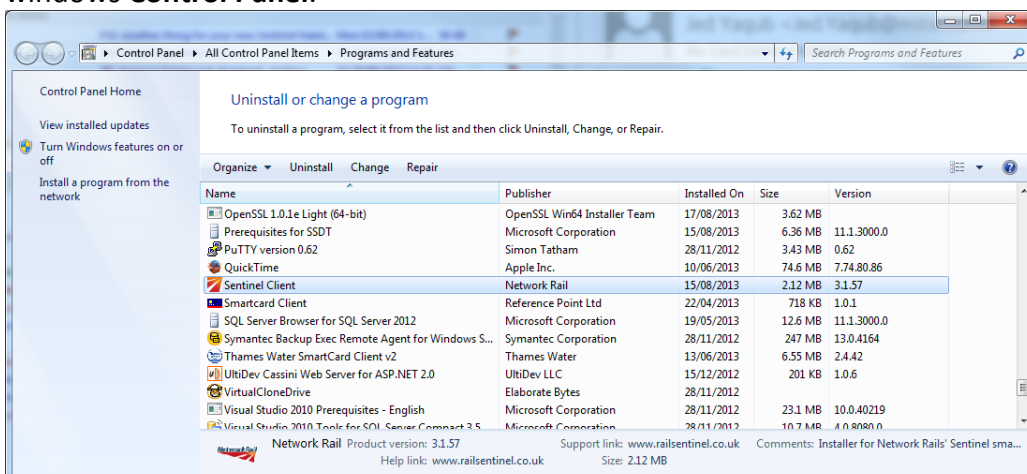
Simply double-click the **Sentinel Client** application to uninstall (you will be prompted to confirm your actions (see below).

By clicking yes to confirm, the uninstaller will remove the Sentinel Client Software from your PC.

4. Configuring the client to use a Proxy Server

If your organisation uses a web proxy to facilitate internet access, you may need to edit the Smartcard Client configuration file to specify the proxy.

The configuration file is named: **WindowsClient35.exe.config**

The configuration file is located in the installation folder. The default installation folder is: **C:\Program Files (x86)\Network Rail\Sentinel Client**

The file can be edited using any simple text editor (e.g. Notepad).

Once you have edited and saved the configuration file, restart the Smartcard Client application and verify successful internet connectivity by ensuring the status of 'Online' is shown. (Refer to Troubleshooting the Smartcard Client for more information).

4.1 Specifying a single Proxy Server

To specify a proxy server, locate the section **<OnlineRPLConfig**… and put the details of your proxy server, including the port number in the **ProxyAddresses** parameter as shown below:

```
<OnlineRPLConfig
  UrlRoot="https://sync.railsentinel.co.uk/serviceApi/"
  Locked="true"
  HeartbeatInterval="5m"
  HeartbeatDisabled="false"
  UseSystemProxy="false"
  UseNoProxy="true"
  ProxyAddresses="mk-proxy1:8080"/>
```

Note: the proxy can be specified either by DNS host name or by IP address

4.2 Specifying multiple Proxy Servers

If your network provides multiple proxies these can be added in the proxy address as shown below with a space separating each:

```
<OnlineRPLConfig
  UrlRoot="https://sync.railsentinel.co.uk/serviceApi/"
  Locked="true"
  HeartbeatInterval="5m"
  HeartbeatDisabled="false"
  UseSystemProxy="false"
  UseNoProxy="true"
  ProxyAddresses="mk-proxy1:8080 mk-proxy2:8080"/>
```

On start-up, the Sentinel Client will attempt to connect to the Sentinel Servers using each of the specified proxies and will select the proxy which provides the fastest response time.

5. Troubleshooting the Smartcard PC client

For most users, there should be no need to change the default configuration. However, the Sentinel client is dependent on two key technologies without which it will not function correctly.

Firstly, the Sentinel Client is heavily dependent on internet connectivity. In some corporate network environments it may be necessary for your I.M. department to configure the Sentinel client to use specific proxy settings and possibly even to specify firewall/proxy exceptions to allow the installed Sentinel Client to communicate with the Sentinel Service.

Secondly, the Sentinel Client requires compatible smartcard reader devices and associated drivers to be properly installed. If the Sentinel Client fails to detect a compatible smartcard reader at start-up the application will report that no compatible readers were found and the application will close. Generally speaking these two potential problems can be easily identified as outlined below, along with specific technical details to enable your I.M. department to make the required configuration changes.
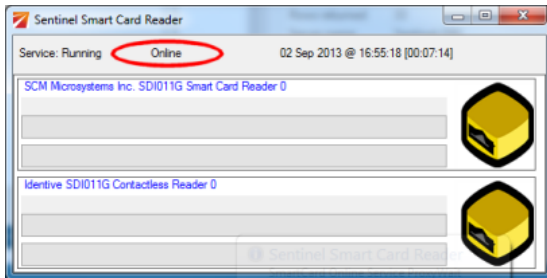
5.1 Checking internet connectivity

When the Smartcard client starts-up it will attempt to connect to the Sentinel Servers. Whilst attempting to connect the status 'Connecting' will be displayed as shown below.
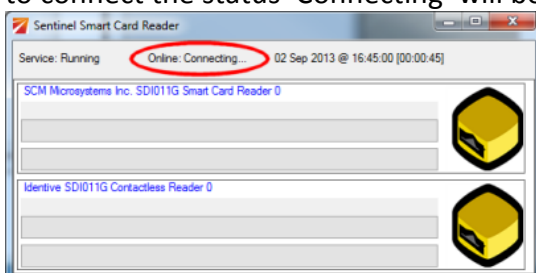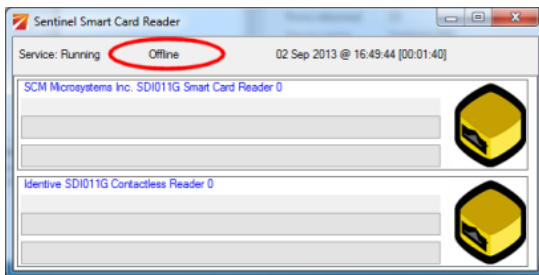
Provided internet connectivity with the Sentinel servers can be established, the status will be updated to show a status of 'Online' as shown.

After a short period, if connection with the Sentinel Servers cannot be established, the status will be shown as 'Offline' as shown below.

If a card should be presented to the smartcard reader but the Sentinel Client application is offline (owing to no internet connectivity with the Sentinel Servers), a window with the following message will be displayed.
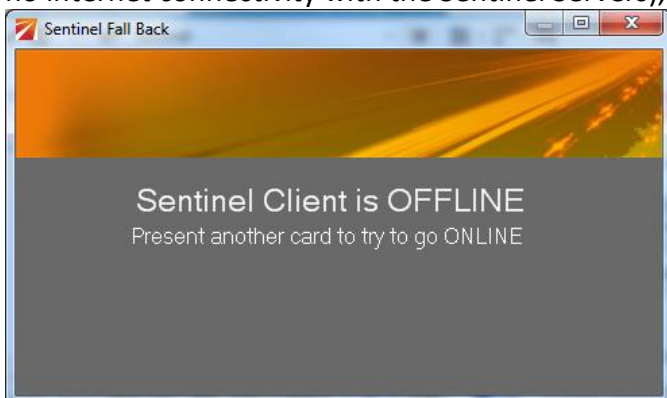

## 5.2 Troubleshooting internet connectivity issues

There are a number of possible reasons why the Sentinel Client may be unable to establish internet connectivity but mainly these will be due to the configuration of your PC or network and access restrictions imposed by your IM dept. If the Sentinel Client cannot establish online connectivity with the Sentinel Servers, there are key two sources of information from within Sentinel that should be checked to identify how the Sentinel Client is trying to access the internet from your PC and what (if any) connection success it is having.

5.3 Internet connectivity – show messages

When the Sentinel client attempts to connect to the internet, information about connections that are being attempted (both direct and proxied connections) are logged and displayed in the System Messages window. To display these messages, right click on the Sentinel Client icon in the Windows System Tray and select **Show Messages**
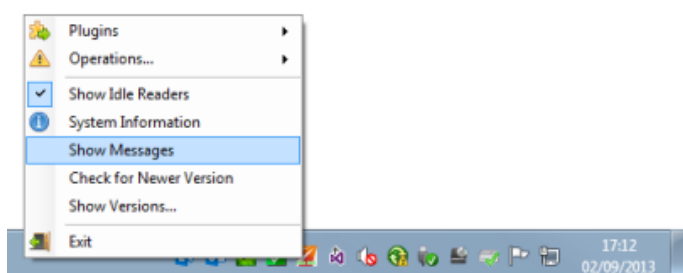

The System Messages window will show each connection attempt and confirm if connection was established or not. From this window, it's possible to see if the Sentinel client is attempting to make direct (unproxied) or proxied connections as shown below.
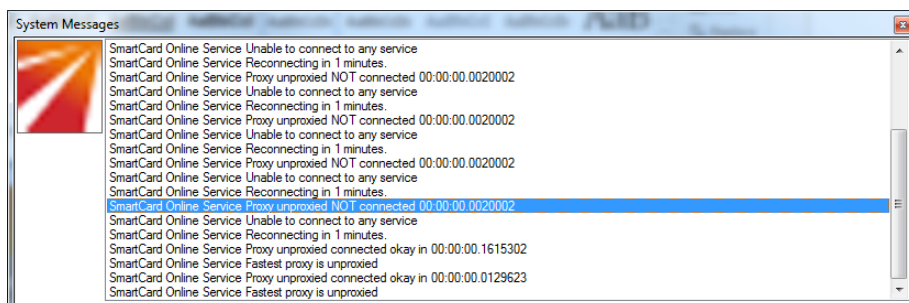
## 5.4 Internet connectivity – system information

The online status and current connection information for the Sentinel Client can be viewed by accessing the System Information window. To display this window, right click on the Sentinel Client icon in the Windows System Tray and select **System Information**
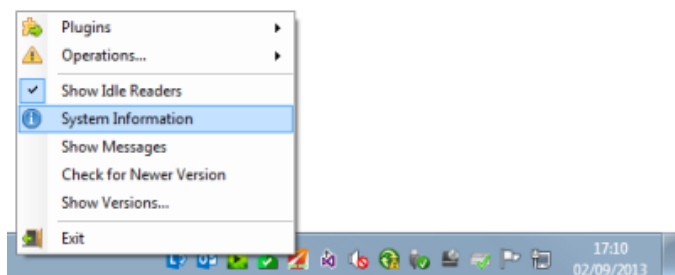
When the window has opened, select the **Smartcard Online Service** tab. On this tab, the URL of the Sentinel service that the Sentinel Client is connecting to is shown, along with the Online/Offline status. Also shown on this tab are details of the proxy server that the Sentinel Client has connected through (if applicable).
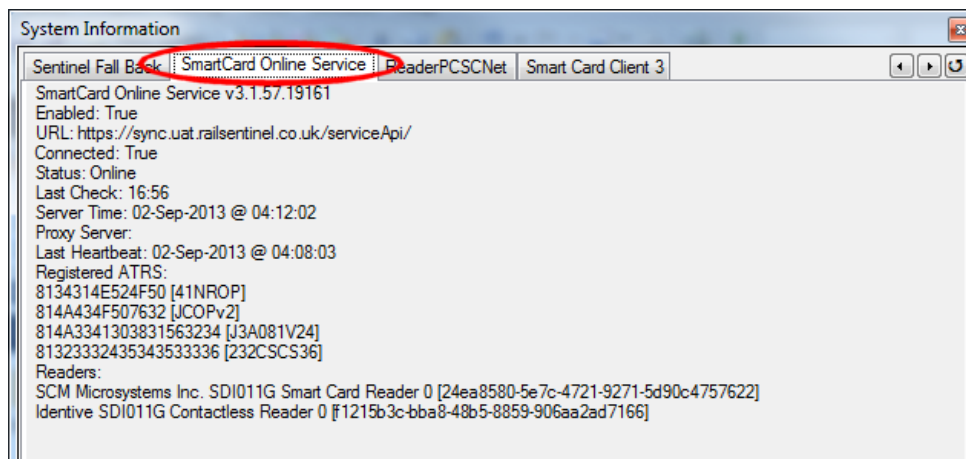
6. Technical requirements

6.1 Application software dependencies

The Sentinel Smartcard Client application has a number of software and hardware dependencies as listed below:

- Microsoft .NET Framework v3.5 (Available from Microsoft) http://www.microsoft.com/en-gb/download/details.aspx?id=21

- Microsoft PC/SC (Pre-Installed with MS Windows) http://technet.microsoft.com/en-us/library/bb742533.aspx

- Smartcard Reader Drivers (Available from reader manufacturers websites e.g.) http://www.hidglobal.com/products/readers/omnikey/5321-cl

  http://www.identive-group.com/products-and-solutions/identification-products/desktop-readers-terminals/rfid-desktop-readers/scl011-contactless-nfc-desktop-reader

  http://support.gemalto.com/?id=prox-du_prox-su

6.2 Internet connectivity requirements

The Sentinel Client provides a minimal user interface to facilitate communication between smartcards and the Sentinel Service. All communications between the Smartcard and the Service are secured using industry standard encrypted Global Platform SCP02 (AES256) smartcard communications. The communications between the smartcard client and the Sentinel service is facilitated using a JSON Web Service secured using HTTPS (HTTP over SSL/TLS).

Diagram: Sentinel Client Communications
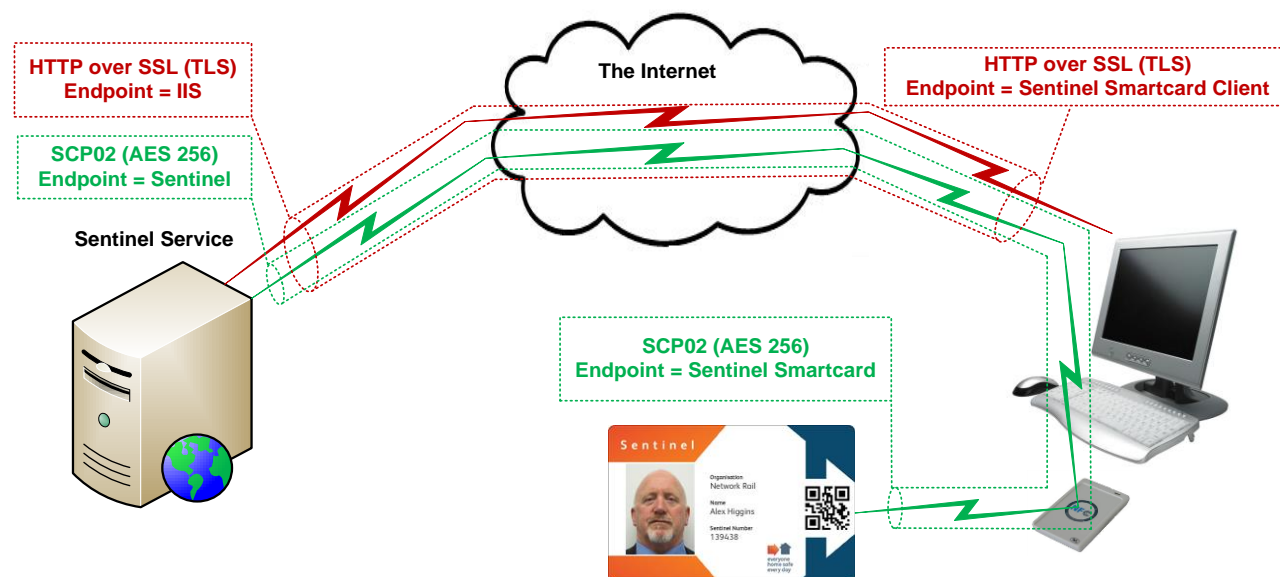
6.3 External Sites accessed by the Sentinel Client

The Sentinel Client connects to the Sentinel Servers via the URL https://sync.railsentinel.co.uk