SecuGen Registered Device Connectivity

Deployment and Troubleshooting

Version 1.1

July 2017

The SecuGen Registered Device Service (RD Service) requires network access at multiple levels in order to function correctly. This document provides a checklist and debugging mechanism to ensure that proper access is allowed for the RD Service.

1. BETWEEN THE AUA APPLICATION AND THE RD SERVICE.

The RD Service binds on the **loopback adapter (localhost) or IP 127.0.0.1**. It listens on the first port available between **11100 and 11120**.

Please check that the following permissions are given

- ✓ The process (sgirdsrv.exe) is allowed to run on the system and is not blocked by any firewall or antivirus.
- ✓ The process (sgirdsrv.exe) is allowed to bind on the loopback interface (127.0.0.1)
- ✓ The process (sgirdsrv.exe) is allowed to listen on any port between 11100 and 11120.
- ✓ The process (sgirdsrv.exe) is allowed to receive and send data on TCP connections setup on the above ports (11100 - 11120)
- ✓ The process (sgirdsrve.exe) is allowed to access the biometric device via a local USB port.

2. BETWEEN THE RD SERVICE AND THE MANAGEMENT SERVER

The RD Service is required to connect to an external Management Server for the primary purposes of Device Registration and Device Certificate Signing.

Please check that the following permissions are given (in addition to section 1)

If you are providing direct access through your firewall

- ✓ On the client, please ensure that the process (sgirdsrv.exe) is allowed to open **TCP connections to www.secugenindia.in on HTTPS port 443**. Please check network traces to confirm that the process is allowed to open the required network connection.
- ✓ On the firewall, please allow **TCP** based traffic in both directions to the host **www.secugenindia.in on HTTPS port 443**. Check logs or traces on both client system and firewall to confirm that TCP / HTTPS traffic is indeed flowing in both directions between the client system and the Management Server . A tool such as telnet.exe can be used to check connectivity.

If you are providing access through your proxy server

- ✓ On the client, please ensure that the process (sgirdsrv.exe) is allowed to open **TCP** connections to your proxy server. Please check network traces to confirm that the process is allowed to open the required network connection.
- ✓ Confirm the exact **type of proxy server authentication** if it is enabled (basic , digest , Windows Domain etc).
- ✓ On the proxy server, please allow access to the proxy server from the client system. Also, ensure that the proxy server is enabled to allow **TCP based data to www.secugenindia.in on HTTPS port 443**.
- ✓ On the proxy server, check logs or traces to confirm that there is no authentication failure and that traffic is indeed flowing in both directions from the client system to the Management Server.

3. GENERAL PRE-REQUISITES FOR USING THE DEVICE

- ✓ Install the device. On Windows, you need to install the drivers. You can download them from **http://www.secugen.com/download/drivers.htm** or contact SecuGen support for the exact drivers to be installed. On Android, you do not need drivers. The library files ensure communication with the USB device.

- ✓ The correct operating system.
  - Windows 7, 8 and 10.
  - Android 4.4 and above.