Z5 Technical FAQ

1) Explain how patch management and updates will be handled and by whom:

Application updates are sent out periodically from ZVRS engineering team. Upon application start, it will check to see if there's an update to download. The auto-update process requires admin access on desktop to successfully update the application. However, we offer PC and OSX installers for Z5 desktop application updates upon your request. iOS and Android versions can be downloaded/updated via their respective Appstores.

2) System Requirements – Only include what will actually be utilized:

- Windows XP/2003/Vista/7/8.1 (including 64 bit versions), DirectX 9.0c or higher
- Core 2 Duo class, 2.33 GHz (H264, 720p video calls)
- Core 2 Quad class, 2.66 GHz (H264, 1080p video calls)
- 1 GB Ram (2GB recommended on Vista)
- 30Mb hard-disk space
- Web camera

3) How does the user access the program?

The user will login the application using their credentials. The username field can accept either phone number or username. The password is the same as the one for logging into the user's profile at www.zvrs.com.

4) How is data entered into the application?

The application accepts user input via tablet's capacitive touchscreen or via PC Desktop keyboard/mouse.

5) Does product pull data or transmit data to any other devices/systems/servers?

The application and MCS (Media Control Server) server sends and receives SIP signaling and H.263/H.264 video streams. User login/authentication and profile information is sent to and retrieved between the application and MCS/Zdial server.

6) Where is data saved to?

Call history is stored locally while the user profile and address book of contacts are stored on our servers. No video calls are recorded.

7) What is the size of a typical network transaction in kilobytes?

384kbps - 512kbps

8) Required transaction response time? (max latency(ms))

100ms

9) Is it encrypted?

The user login and SIP authentication is encrypted. The calls are not encrypted. A point to point edge VPN to company's DMZ may be used to encrypt the media streams.

10) What type of packet capture would you see during a call?

Z5 uses one of its local ports to connect to our MCS server on port 5060 outbound for SIP signaling. MCS identifies the port the Z5 is on and remembers it. During a call, video and audio packets are transmitted back and forth over the same ports.

11) Would incoming calls require inbound ports to be opened?

No. Incoming calls to the Z5 are part of the original TCP session that has been established when Z5 registers with MCS during the login process.

This means that the firewall should allow incoming calls to Z5 since it is already part of the established session started internally.

12) If the RTP media ports are narrowed down to less than 10000-65535, would there be issues?

Yes. Our server is set to a larger range and if the application decides to use a port outside the set range, there will be connection issues.

On special case-by-case basis, we offer AnyConnect VPN using a certificate which would bring all of the ports down to just HTTPS or 443 TCP. This is a client based Cisco AnyConnect VPN loaded on the client. If you are a government agency, we could extend the client VPN for your use. We would support you on an IPSEC tunnel at the edge from your DMZ.

13) What is MCS? Media Control Server.

14) Where are the locations of the servers mentioned in whitepaper? Equinox data centers are outside of Washington D.C. with a secure hosting site in Reston, VA.