SPOK User Guide

Version 3.0
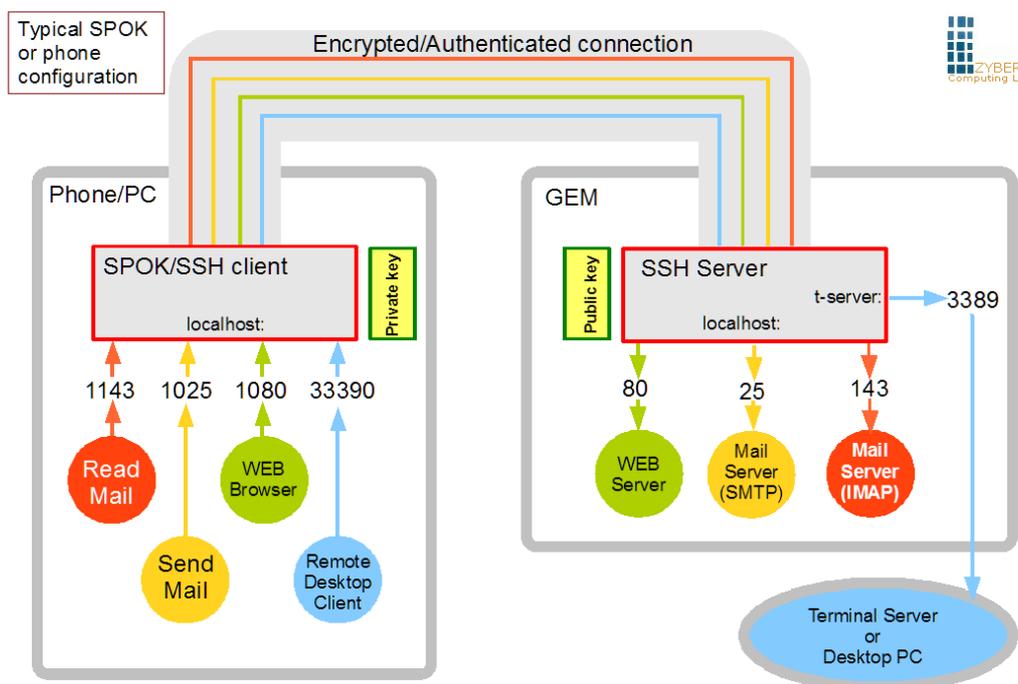
4 May 2014

1   Introduction

SPOK (Secure Portable Office Key) is a system providing secure remote access to ZYBERT servers from Internet.

SPOK uses SSH tunnelling and RSA public/private key authentication to ensure security of the connection.

For Windows or Mac PCs SPOK would usually run directly from a dedicated USB key, although it can only be installed on a computer. For phones and tablets SPOK app is installed on a device.

2   How it works

SPOK connects and authenticates to the target Z1 GEM server and sets up an encrypted communication tunnel. Then it opens local ports on the device used and connects them through the tunnel to corresponding ports on the Z1 GEM. The user applications connect to local ports and the communication with the Z1 GEM proceeds through the tunnel.

ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

3   Setup

3.1   Site Internet connection

In order to be able to access the site, SPOK will require an address. Therefore it is important that the site has a fixed IP address or, as a minimum DDNS setup, mapping dynamically a well define name to the current IP address. With fixed IP address, Zybert will, on request provide a DNS subdomain name <NAME>.z1server.co.uk.

3.2   Router settings

SPOK uses a single port (by convention it is an SSH port – 22, but any port will do) to connect to the Z1 GEM. In order for this connection to reach the target, the broadband router has to be set-up to forward a chosen port to port 22 on the WAN interface of the Z1 GEM. The IP address of the WAN interface can be obtained by a right-click anywhere in the Z1 GEM administration panel window in the browser. Some routers will also allow the user to find out the address once the Z1 GEM is connected.

For detailed instructions for your specific router, see

http://portforward.com/english/routers/port_forwarding/

3.3   SPOK Configuration

(assuming your Z1 GEM is accessible via http://www)

In your WEB browser, go to http://www/Spok and login if necessary.

Welcome demo. Users - Logout

demo Devices

Name	Link Name	Host	Port	Auto Reconnect	Password Once	Created	Last Upload	
Add Device								

Click on **Add Device**

Welcome demo. Users - Logout

Add Device to demo

demo Devices

Name*

iphone

Link Name

office

Host Address*

demo.z1server.co.uk

Port*

22

Auto Reconnect?

Yes ▼

Request Password Once Only?

Yes ▼

[Add Device]

Name: Unique device name

Each device you use for remote access has to have its own configuration (USB key may be used for both, Windows and Mac and each will have its own device configuration. Once you make one configuration you can easily clone it for other devices, but each of them has to have a unique device name)

ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

Link Name: Unique link name

Name displayed for this connection on your device

Host Address: Your site IP address or DNS name

Port: Connection port that your router forwards to port 22 on the WAN interface of Z1 GEM

You can also decide here whether your SPOK will automatically try to reconnect if the connection is interrupted and whether the SPOK key passphrase will be required every time it reconnects. By default SPOK tries to reconnect quietly – the passphrase is only required on the first connection or – for security reasons if the connection is down for a long time.

Click on Add Device to save

Name	Link Name	Host	Port	Auto Reconnect	Password Once	Created	Last Upload	
iphone	office	demo.z1server.co.uk	22	Yes	Yes	2014-05-05 12:53:23		✎✖⊘🖶🖨
Add Device								

Click on device name to set tunnels.

Tunnels:

Name	Direction	Local Port	Remote Name	Remote Port	Actions
Add Tunnel					

Click on Add Tunnel

Add Tunnel to iphone

demo Devices > iphone

Name*

`http`

Direction

`Local ▼`

Local Port*

`1080`

Remote Name*

`localhost`

Remote Port*

`80`

[Add Tunnel]

Name: Name of the protocol or application to be served (for instance HTTP, IMAP, SMTP... etc)

Local Port: The port number used on your device to connect – for all platforms except Windows, only port higher than 1024 are allowed, so – adding 1000 to the 'standard' port would usually be a convenient way of remembering – for instance:

- http: port 2080 to map to Z1 GEM port 80

- imap: port 1143 to Z1 GEM port 143

- smtp: port 1025 to Z1 GEM port 25

etc.

These ports will then be used when connecting through the tunnel. For instance, to connect to the Z1 GEM WEB server would require http://localhost:2080

(most applications – like email allow the user to specify ports for connections. For instance with the tunnels as above the user would use host localhost, port 1143 for incoming email and host localhost and port 1025 for outgoing email)

ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

Remote Name: Name or IP address of the host on the Z1 GEM network to connect to. Usually – for a connection to Z1 GEM, this would be **localhost**. To connect to a computer on the LAN, specify its IP address.

Remote Port: The target port to connect – in the example above it would be 80, 143, 25 etc

Tunnels:

Name	Direction	Local Port	Remote Name	Remote Port	Actions
http	Local	1080	localhost	80	
imap	Local	1143	localhost	143	
smtp	Local	1025	localhost	25	
Add Tunnel					

Go back to device list and **Enable** the device. (enable/disable icon on the right)

The device configuration is ready for use.

3.4   Load Configuration

Usually the first time the configuration is loaded to your new device would require your device to be in the office and connected to your LAN. (so http access would be available via http://www)

Start SPOK application. From the menu select load configuration from the GEM. Specify the host (if www is the accessible GEM host name – just enter **www**)

Enter device name and your GEM password.

The configuration loaded contains new private key, encrypted with your GEM password. Therefore, when you connect for the first time, the application will ask you for the GEM password and for the new passphrase – your private key will then be encrypted with the new passphrase and the application will ask for it when it needs to load the key.

Once this is done you can connect and disconnect. When the connection is running, the local ports defined in the configuration are open on your device and other applications can use them to connect through the tunnel to your network.

So – with the example above:

- Z1 GEM WEB server is on http://localhost:2080

- Z1 GEM IMAP (reading mail) is on localhost, port 1143

- Z1 GEM SMTP (sending mail) is on localhost, port 1025

- etc.