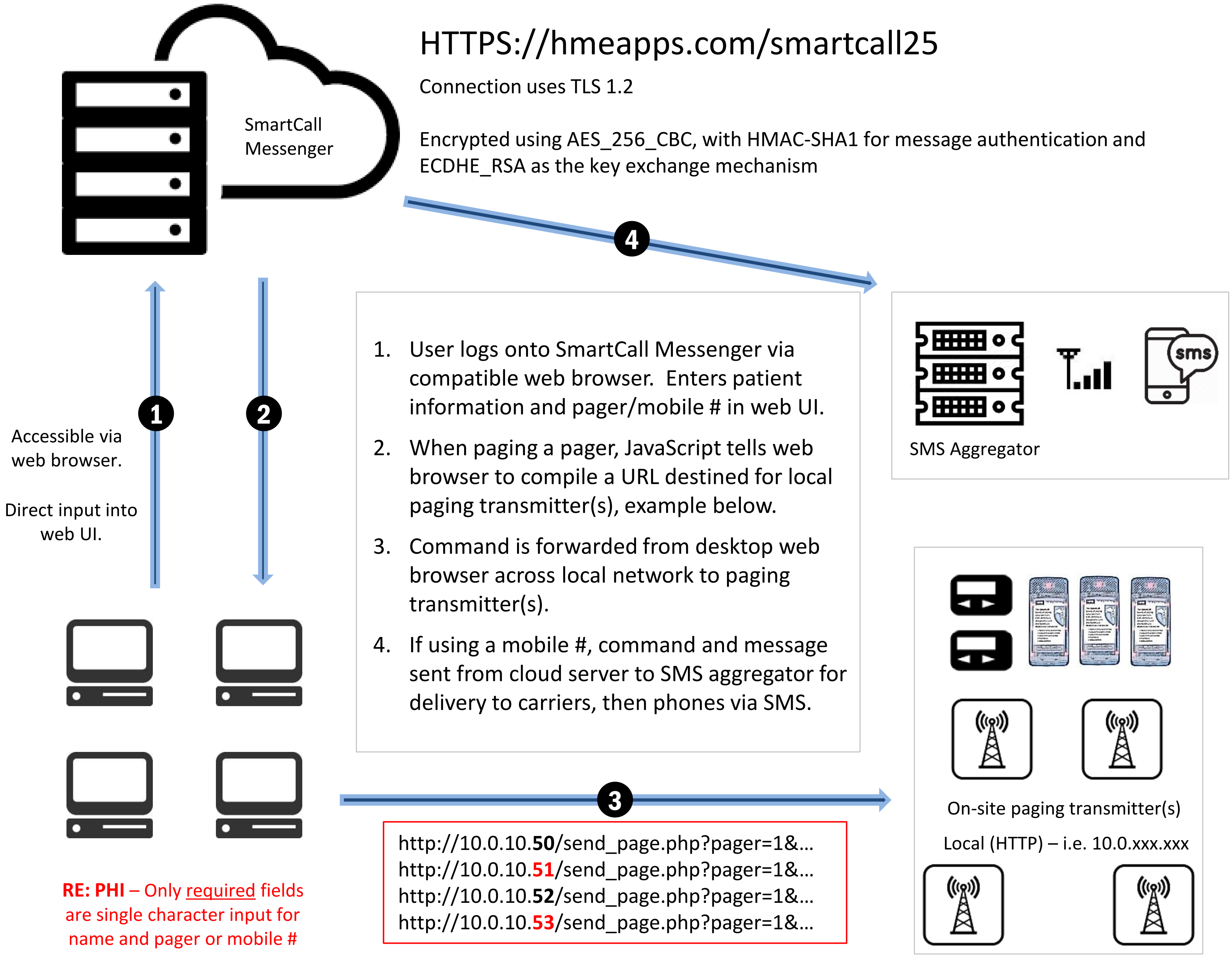
JTECH™
AN HME COMPANY

SmartCall™ Messenger Process Flow



HTTPS://hmeapps.com/smartcall25

Connection uses TLS 1.2

Encrypted using AES_256_CBC, with HMAC-SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism

1. User logs onto SmartCall Messenger via compatible web browser. Enters patient information and pager/mobile # in web UI.
2. When paging a pager, JavaScript tells web browser to compile a URL destined for local paging transmitter(s), example below.
3. Command is forwarded from desktop web browser across local network to paging transmitter(s).
4. If using a mobile #, command and message sent from cloud server to SMS aggregator for delivery to carriers, then phones via SMS.

```
http://10.0.10.50/send_page.php?pager=1&…
http://10.0.10.51/send_page.php?pager=1&…
http://10.0.10.52/send_page.php?pager=1&…
http://10.0.10.53/send_page.php?pager=1&…
```

NOTE: Browser will consider this “mixed” content

RE: PHI – Only required fields are single character input for name and pager or mobile #

JTECH, An HME Company
1400 Northbrook Pkwy
Ste 320
Suwanee, GA 30024
800.925.8091
hmewireless.com
jtech.com

JTECH™
AN HME COMPANY

Managing Mixed Content

Recommended Desktop Browsers

Touch devices, such as tablets and iPads have only limited functionality and are not support by JTECH, An HME Company.

Ver. 10 or 11	Ver. 31.0 or higher	Ver. 42.0 or higher

- Transmitters DO NOT connect externally to the internet.
- Transmitters are assigned a static IP address behind the local firewall, i.e. 10.0.10.50
- Paging commands are directed to the transmitter(s) via URLs on the local network.

- The SmartCall web server is a secure HTTPS environment, the transmitter is on a local HTTP environment.
- Web browsers consider this "**mixed content**."
- Each browser has different configurations for managing mixed content.

The following information for managing mixed content is presented as a guide and does not replace diligence on behalf of the end user to ensure the security of their network. HME Wireless is not liable for any risk occurring as a result of changes to standard browser settings. Contact your IT administrator for any additional information.

Add to Trusted Sites

choose Tools (Alt + x): Select Internet Options > Security > Trusted Sites > Sites > Add https://*.hmeapps.com > Close. While still under Trusted Sites – Click Custom Level > Miscellaneous > Select Enable under Display Mixed Content.

For more information, visit:

http://windows.microsoft.com/en-us/windows/support#1TC=windows-7

http://windows.microsoft.com/en-us/internet-explorer/ie-security-privacy-settings#ie=ie-11

http://windows.microsoft.com/en-us/windows/security-zones-adding-removing-websites#1TC=windows-7

Change Security Configuration

type **about:config** in the address bar. Continue through warning that shows. In the search bar, type "mixed." Double click on the settings to edit the value to show:

Security.mixed_content.block_active_content **FALSE**
Security.mixed_content.block_display_content **TRUE**

For more information, visit:

https://support.mozilla.org/en-US/kb/about-config-editor-firefox

https://support.mozilla.org/en-US/kb/mixed-content-blocking-firefox

Change Shortcut Properties

Right click the Google Chrome icon that is located on your desktop. Select "Properties"; in the box named Target, add 1 space to the end of the command after /chrome.exe" then type: **--allow-running-insecure-content**
(note: there are two dashes (-) in front of allow)

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --allow-running-insecure-content

When completed, click OK.

For more information, visit:

https://support.google.com/chrome/answer/1342714?hl=en

JTECH, An HME Company
1400 Northbrook Pkwy
Ste 320
Suwanee, GA 30024
800.925.8091
hmewireless.com
jtech.com