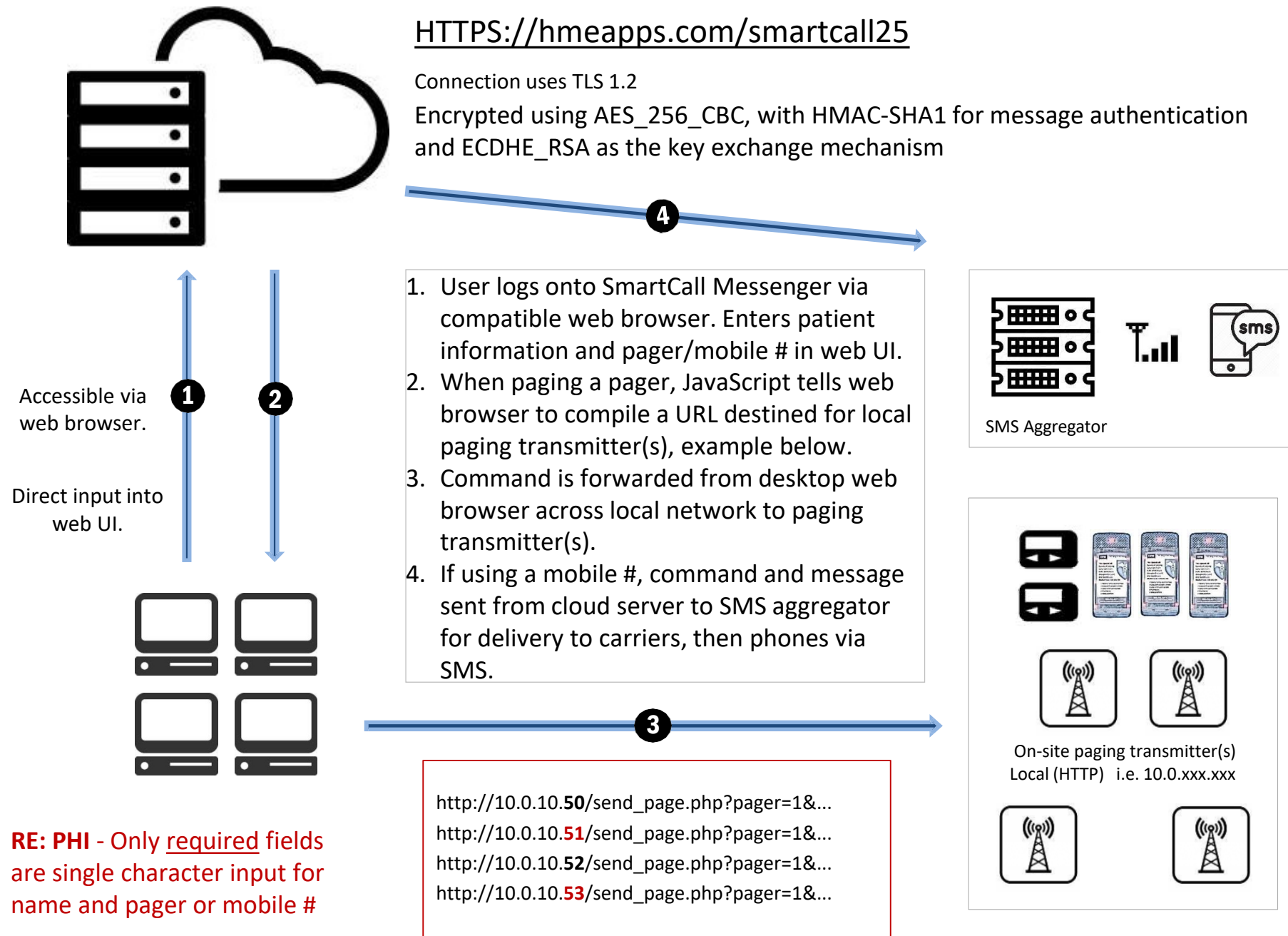


# SmartCall Messenger Process Flow



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


*Note: Browser will consider this "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. JTECH is not liable for any risk occurring as a result of changes to standard browser settings. Contact your IT administrator for any additional information.

### Microsoft Edge Ver. 109 or Higher

Allow Insecure Content



1. Open **Microsoft Edge**.
2. Go to the website you want to allow:  
<https://hmeapps.com/smartcall25/>
3. Click the **lock icon**  next to the URL in the address bar.
4. Select **Permissions for this site** or **Site permissions**.
5. Scroll down and find **Insecure content**.
6. Change it from **Block (default)** to **Allow**.
7. Refresh the page to apply the changes.

**Direct access to site settings:**

<edge://settings/content/siteDetails?site=https://hmeapps.com/smartcall25/>

**For more information:**

[Learn how Microsoft Edge handles mixed content downloads](#) | [Microsoft Learn](#)

- 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.

### Mozilla Firefox Ver. 114 or Higher

Allow Mixed Content




1. Open **Firefox**.
2. In the address bar, type: `about:config`
3. Press **Enter** and click **Accept the Risk and Continue**.
4. In the search bar, type: `mixed content`
5. Locate these two settings and double-click them to set as follows:
  - a. `security.mixed_content.block_active_content` → **false**
  - b. `security.mixed_content.block_display_content` → **true**
6. This allows functions to work while locking only non-essential visuals.

**For more information:** [Mixed content blocking in Firefox](#) | [Firefox Help](#)

### Google Chrome Ver. 110 or Higher

Allow Insecure Content



1. Open **Google Chrome**.
2. Go to the website where you want to allow:  
<https://hmeapps.com/smartcall25/>
3. Click the **lock icon**  next to the URL in the address bar.
4. Click Site settings.
5. Scroll down to find Insecure content.
6. Change the setting from Block (default) to **Allow**.
7. Refresh the page to apply the changes

**Direct access to site settings:**

<chrome://settings/content/siteDetails?site=https://hmeapps.com/smartcall25/>

**For more information:**

<https://support.google.com/chrome/answer/99020>

Note: Touch devices, such as tablets and iPads have limited functionality and are NOT supported by JTECH.