SaltDNA

FAQ SHEET

HOW DO I KNOW THIS IS SECURE?

We use open source, publicly verifiable cryptography libraries. You don't have to rely on our engineers to develop the strongest levels of encryption – the code running your communications infrastructure has been peer reviewed by a joint consortium of the best cryptographic minds in the world.

The open source libraries and protocols we build upon include the following security features:

- **Pinned TLS – Transport Layer Security – for encrypted connections**
- **Messages encrypted using Axolotl secure protocol (with Diffie-Hellman key exchange and a tamper proof hash (HMAC))**
- **Voice call signalling and setup using pinned TLS connections**
- **SRTP – Secure Real-time Transport Protocol for peer to peer voice call transfer**

We are the only secure communications platform which allows our customers to install the infrastructure on premises, on their hardware, behind their firewalls.

Our solution has been penetration tested by multiple different organisations. Many of our partners and customers have funded their own, independent, research to ensure our product is secure.

To date, none of these test initiatives have discovered any security vulnerability or compromise. Some have offered minor recommendations, which we take on board and enhance if appropriate.

CONFERENCING

The SaltDNA app allows users to attend a secure conference call. All callers attached to a central conferencing hub which allows the call to continue even if one person drops off. Ongoing conference calls are shown within the SaltDNA app, allowing callers to leve and rejoin at will.

BURN

The Burn feature in the SaltDNA app gives you full control over your message history, allowing you to remove all traces of a message after it has been sent, with no record stored anywhere of the content of the message once it has been burnt.

Any instant message can be removed from both devices (sender and receiver) by either party. Messages have a small burning flame icon beside them – pressing the flame will delete the message from your device and simultaneously send a burn request to the other device to do the same. Users can also configure their auto burn settings for a range of times. Enabling an auto burn time has the effect that all messages sent will self destruct after a preset time.

APP SECURITY

Users can enable an additional passcode for the app itself, over and above that used on their device. This feature is enabled, disabled and reset through the Settings menu.

A 5 digit passcode can be configured and additional settings allow the user to determine if the passcode must be entered before answering an incoming call. The use of a passcode can be enforced and controlled centrally, customer wide, if required.

NETWORK LATENCY & BANDWIDTH

Messaging: Messages are asynchronous, so are not subject to latency issues. A 100 character message will use approximately 1500 bytes (1.5kB). When it is received, the response/ acknowledgement back to the sender is approximately 900 bytes.

Voice: The SaltDNA app uses the WebRTC standards and protocols for handling the voice transmission functions. This includes the OPUS codec for adapting voice quality to varying network bandwidth. The codec can operate with bandwidths between 6Kbps and 510 Kbps.

On an unrestricted network, the app will consume approximately 70Kbps in each direction for a peer to peer connection. The figure may vary depending upon network conditions and restrictions. When less bandwidth is available the app will reduce consumption while maintaining call quality.

For 4G networks we see typical bandwidth usage of around 40Kbps in each direction.
Our testing includes running the solution on many different types of simulated networks. These include WiFi, 3G, 4G and a specially tuned high latency, low bandwidth network with a profile of 15Kbps available capacity and 500ms latency.

WHAT ARE THE MESSAGE STATES?

Message Queued Your message is queued and waiting for onward delivery to the SaltDNA app messaging server. **Note**: First time messages to a new contact can sometimes remain in the queued state until both the sender and receiver have been online in order to create the initial encryption cypher.

Sent Your message has left your device and is waiting on the SaltDNA app server for onward delivery to the recipient.

Delivered Your message is now delivered onto the recipient’s device and they have been alerted to its presence.

Read Your contact has opened the message screen and looked at the message.