SaltDNA

Company Details

SaltDNA was formed in 2013 by a group of technology entrepreneurs with a shared history in enterprise security, telecoms, network optimization and mobile application development. It is the first company to provide an enterprise solution for encrypted communications between mobile devices with full centralized control. The company is based in Belfast, Northern Ireland.

SaltDNA has taken a close partnership approach with its customers and focuses on providing a high end custom solution for each customer to fit their unique requirements. Our roadmap is defined and developed by our customers.

Today SaltDNA provides secure communications for many large enterprises, governments, oil & gas companies, legal firms and NGOs.

Systems Functionality

Overview

SaltDNA is a versatile, easy to use application-based secure communications platform utilizing the highest level open source end-to-end encryption. It offers encrypted communications between mobile devices and desktop with full, centralized control delivering a secure capability for calls, conferencing, text and file transfer with complete confidence. Facilities include the ability to define closed user groups within the enterprise, offering person to person and group messaging and voice with secure file transfer over the internet.

SaltDNA is designed for the international user: the service is agnostic of the underlying network and operates globally on 3G/4G, LTE, WiFi and Satellite. Utilizing transport layer encryption, texts are protected with forward secrecy, and can be deleted at both ends by either the sender or receiver.

Unique Features

SaltDNA offers a number of highly desirable and collectively unique features:

- **Closed User Groups** - Centrally control lines of communication.
- **Secure Conferencing** - Connect up to 15 concurrent encrypted call participants.
- **Secure File Transfer** - Encrypt images and files in transit and at rest on the device.

Desktop Application - Cross-platform communication for multiple Operating Systems.
Secure Group Chat - Secure group conversations with multiple participants.
Flexible Deployment - SaaS or fully controlled virtualized on premise installation.

Deployment Options

SaltDNA offers flexible deployment options for Android or iOS mobile devices or Windows and macOS on desktop either as a Software As A Service (SaaS) or through an On-Premise Deployment:

SaaS

Provided as a service with no additional hardware requirements. Customer administrators are granted access via a web portal.

On-Premise

For the On-Premise Deployment, the hardware requirements are described in **Appendix B**. The Communication Management Software is a virtualized software component and is usually provided as an Open Virtual Application (OVA) and licensed as part of the installation process.

Client Management Functions

With centralized enterprise-level control through the Communication Manager, SaltDNA offers the user the ability to manage all aspects of the service, including design of communications circles within the enterprise, management and authorization of users, and the ability to generate usage reports to ensure full system utilization.

Matching Client Requirements

The capability of SaltDNA to fulfil the requirements contained within a large number of technical specification have been tabulated at **Appendix A**. From this it can be seen that the off-the-shelf solution offered by SaltDNA matches most client requirements for high security environments.

Encryption Routines and Processes

The SaltDNA solution includes multiple different secure data exchanges:
Mobile Client to Server: Client apps communicate with the server to download their contact rosters, provide information on their current status, to send and receive messages and also when sending and receiving signalling information relating to voice call setups.
In all cases the client to server communications are protected with a TLS V1.2 / 2048 bit RSA encrypted tunnel using a pinned certificate - ensuring clients can only connect to their assigned server.
Signalling and messaging communications between the mobile client and the server are passed using the XMPP protocol. In addition to the protection offered by the encrypted tunnel, these XMPP packet contents are encrypted using a double ratchet mechanism known as OLM.

Mobile to Mobile - Voice: Voice calls are connected directly from peer to peer, with a fully encrypted media stream running between the two callers. DTLS and SRTP are used for key exchange and encryption.

Mobile - Data At Rest : All data within the apps is stored within the app container in a SqlCipher, password protected, database. SQLCipher is an Open Source SQLite extension that provides transparent 256-bit AES full database encryption.

Key Exchange Mechanisms, Interception Avoidance and Key Protection

The following methods are used:
Pinned certificates for TLS tunnels, ensuring mobile clients can only connect to their allocated server.
OLM message encryption - using ephemeral key exchange - ensuring forward secrecy.
Voice Peer-to-Peer set up with DTLS : Datagram Transport Layer Security (DTLS) is used to provide communications privacy in a secure signalling channel that cannot be tampered with. Eavesdropping or message forgery cannot occur on a DTLS encrypted connection. A new set of encryption keys are generated as part of the negotiation between both parties during call setup.
Voice Peer-to-Peer Streaming with SRTP : Before the media stream starts both endpoints perform a mutual DTLS handshake on the media ports. The shared symmetric key that was established for the resulting DTLS session is then used to derive an SRTP key. Then the encrypted SRTP media stream is started.
Cryptographic primitives : the following primitives are used within the solution.

- DH ratchet : Elliptic curve Diffie–Hellman (ECDH) with Curve25519
- Message authentication codes (MAC, authentication) : Keyed-Hash Message Authentication Code (HMAC) based on SHA-256
- Symmetric encryption : the Advanced Encryption Standard (AES), partially in Cipher Block Chaining mode (CBC) with padding as per PKCS #5 and partially in Counter mode (CTR) without padding
- Hash ratchet : HMAC.[7]

System Availability

AWS Availability

SaltDNA currently supports a private AWS installation for a number of select customers with specific security and availability requirements. SaltDNA will work with the customer to provision and test this system fully before handing over full control to the customer.

On-Premise High Availability

Those customers who chose to install the server components within their own network will be provided with an OVA file, suitable for installation on a virtual infrastructure such as VMWare ESXi. This platform offers multiple options, including HA clustering, VMWare Fault Tolerance, VMWare Site Recovery Manager and many 3rd party alternatives.

Standard Service Level Agreement (SLA)

SaltDNA provides 24/7 premium support for all customers. The standard SLA's related to support and release management are outlined in **Appendix C**.

SaltDNA

APPENDIX A

Matching SaltDNA Capabilities

This table maps SaltDNA's current capabilities to the requirements defined for many organisations when they are asking about a "Secure Communications Solution".

Requirement Brief Description	SaltDNA Feature Availability
User-User Chat	**Available**
Picture and File Sharing	**Available**
Ad-hoc group creation without administrator	**Available**
Temporal Chats which are erasable	**Available**
Admin configurable groups	**Available**
End-to-end encryption	**Available**
Secure end-to-end encrypted calls	**Available**
15 Participant Secure Conference Calling	**Available**
Secure Contact list and closed user groups	**Available**
Role Based Access Control	**Available**
Customer may act as "operator" with multiple internal customers	**Available**
Add, delete, modify end users and closed user groups via web interface	**Available**
Admin has no access to private user content	**Available**
Intuitive app: iOS / Android / PC /MAC OS	**Available**
Multi-device Support per user	**Available**
Notifications by APNS and out-of-band, if required	**Available**

SaltDNA

Globally available free downloadable iOS App	**Available**
Confidentiality of messages - encryption / privacy	**Available**
Strict authentication	**Available**
Message and Comms Integrity	**Available**
Identity Protection	**Available**
Available over 3G / Edge / UMTS / 4G / LTE / Wifi and Satellite	**Available**
Internal network support for enterprise networks	**Available**
No reliance on other other services	**Available**
Secure comms wrapping	**Available**
AES+ Bulk Encryption	**Available**
TLS+ Cipher Suites	**Available**
Scalable from 500 to 10000+ users	**Available**
Voice Security Assurance (SRTP)	**Available**
TLS support	**Available**
No self-signed PKI certificates	**Available**
Ephemeral end-to-end message encryption	**Available**
Key exchange - DHEC	**Available**
Removing client component deletes all data	**Available**
Back door protections - browsable code	**Available**
Covert channel & statistics aggregation	**Available**
Logging & Monitors for on-Premise solution	**Available**
Performance and availability monitoring	**Available**
Email / Telephone / Web Technical support	**Available**
Notifications via iOS Notification Center	**Available**

Notifications via iOS APNS	**Available**
Windows client support	**Available**
Android client support	**Available**
Mac OS client support	**Available**
Installation of On-Prem solution	**Available**
Training of customer staff	**Available**
Copies of Operations & Technical manuals	**Included**

SaltDNA

APPENDIX B

On Premise Installation Hardware and Network Requirements

The following hardware and network requirements only apply if the customer wishes to install the platform within their own environment.

- Processor: 8 core Intel(R) Xeon(R) CPU E3-1240 v3 @ 3.40GHz
- Memory: 16 GB
- Hard Drive: 1TB

With the platform installed, and configured for licensing and DNS, then the administrator must also open network ports to allow access from clients and for remote support and administration:

- HTTPS (443) for remote support and maintenance from development address
- XMPP (5223) for all addresses
- STUN/TURN (3478) for all addresses

Additional Requirements:

- Access to a transactional email service and an SMS sending account are required for invite message distribution.
- An externally visible hostname, resolving to the newly installed virtual appliance: example: securecomms.yourcompany.com
- An SSL certificate linked to the hostname.

SaltDNA

APPENDIX C

Support Service Structure

While SaltDNA spends huge effort on ensuring the stability and availability of its communications service it acknowledges that issues do happen due to both internal and external factors. SaltDNA will always endeavour to repair and restore the affected services within the following response framework:

Severity Classification	P1	P2	P3	P4
Time to Respond	60 Minutes	2 Hours	3 Hours	4 Hour
Diagnosis	2 Hours	4 Hours	12 Hours	24 Hours
Time to Fix	4 Hours	8 Hours	24 Hours	Scheduled

Severity Classification	Definition
P1	Whole of or a critical part of the service(s) provided by the relevant Product (the "**Service**") is unusable, causing immediate and significant business impact to RESELLER and its End Users. A large number of End Users are not able to access the system where access is fundamental to the usage of the Service and demands immediate attention. Typically this would include but not be limited to: • The inability to register new End Users • The inability for existing End Users to use the Service
P2	A significant, but not immediately critical, part of the Service is unusable, creating some business impact. Some End Users are unable to access offerings of the Service where no alternative methods of access are available.
P3	Disruption of a single minor element of the Service.

	One or more End Users are unable to access the Product's system. Alternative access or workarounds are available.
P4	Non-urgent or cosmetic problem, causing inconvenience only. Acceptable workarounds are available and the Service remains unaffected.

“1st Line Support” – the first human contact point of support for the End User. 1st Line support teams traditionally receive issues, complaints and technical requests. They will seek to resolve all queries directly to the complete satisfaction of the End User.

“2nd Line Support” – a SaltDNA support contact for 1st Line Support who can’t resolve End Users' issues themselves and require a greater degree of technical diagnosis. 2nd Line Support does not interface with the End User direct unless requested to do so.

“3rd Line Support” – support provided by SaltDNA will test, diagnose and resolve valid issues that the 2nd Line Support team raise which 2nd Line Support in accordance with Good Industry Practice has not been able to resolve. These issues usually involve problems with the service capability and performance rather than with the End User.

"Good Industry Practice" - acting with a level of skill, diligence and judgement that would reasonably be expected from a skilled person engaged in the same type of undertaking under the same or similar circumstances.

The Reseller will provide its active users with 1st Line Support (as defined above) and SaltDNA will provide 2nd and 3rd Line Support direct to the Reseller.

The Reseller shall provide 1st Line Support at all times in accordance with Good Industry Practice.

Release Cadence

Frequent feature and bug fix updates are distributed to the clients each 4-8 weeks. Sometimes, in order to patch new security vulnerabilities due to iOS and Android updates, clients releases may be more frequent than planned.

The SaltDNA Management portal is updated on a regular basis with security and feature updates.