SALUS - Secure Mobile Platform

Introduction

SALUS is a custom built high-end secure mobile platform designed to protect users from Communication Interception, IMSI Catchers, Spywares, Trojans, Phishing and Malware attacks. The system uses strong encryption, a hardened operating system and state-of-the-art scanning and blocking techniques for protection. The system has been designed keeping in mind security concerns faced by enterprises, government agencies, high-net-worth individuals, etc.

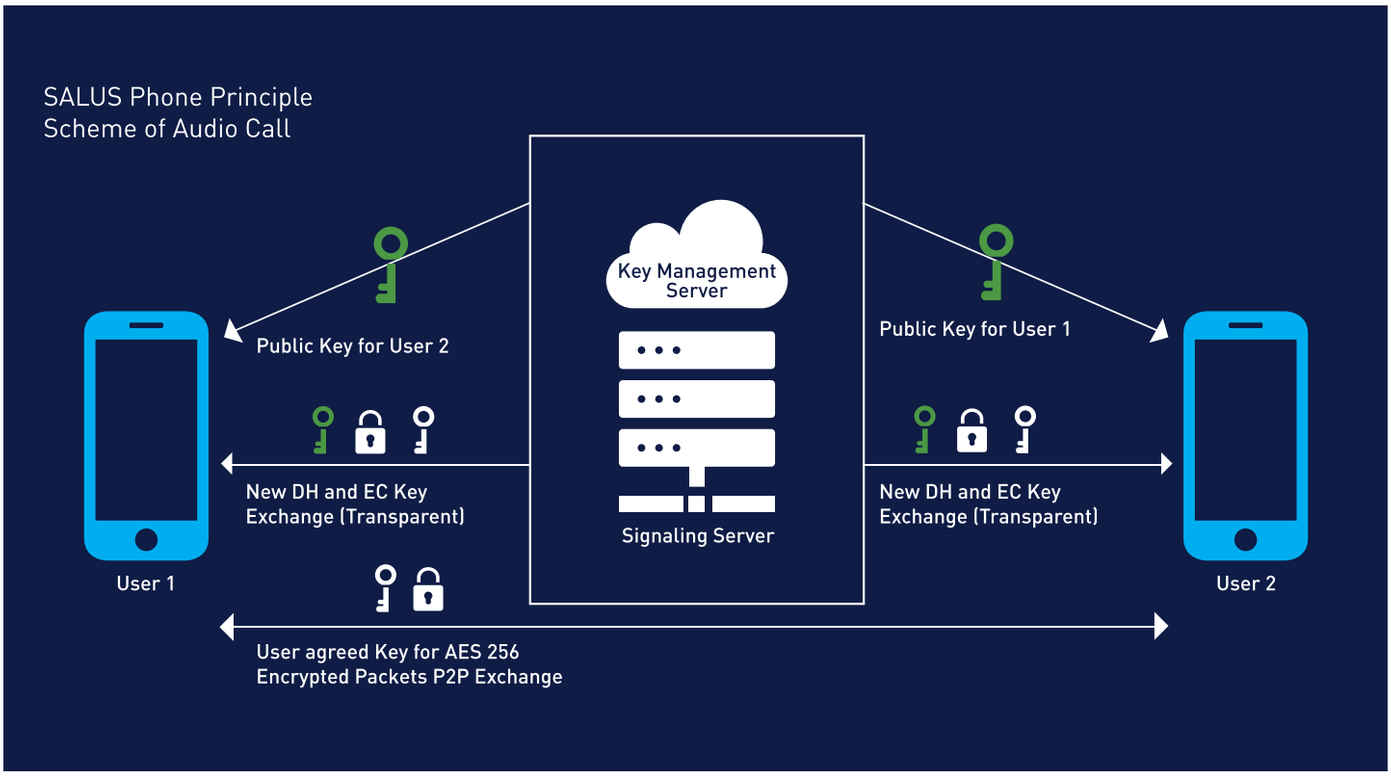
In the current socio-economic scenario, most of the top government officials or corporate bosses require secure communication to discuss classified information. Though there are many platforms available which allows you to make secure calls, all these calls are initiated and/or going through the 3rd party servers (solution provider, Apple, Google, Facebook]. This can act as a single point of attack allowing to steal the information of hundreds of millions of users, with one shot.

Another method to have secure means of communication is by use of a crypto phone; however, it draws unnecessary attention and can be even confiscated for example when crossing borders/or at airports. Besides that, low profile methods can also be applied as soon as the user reveals that he is using a special phone.

Traditional software based secure phones offers no protection against viruses and spyware, viruses, trojans and exploits which can capture the phone audio or screen view, steal user credentials, etc.

Stratign's SALUS is the world's most secure mobile phone for organizations. This high-end smartphone is built from the ground-up to provide you the ultimate defense against mobile Cyber Crime. The phone runs a purpose-built security-rich operating system, fused command-and-control application, built-in secure communications, and multiple security and performance assurance utilities. These components form the Mobile Security platform protects you from eavesdropping, malware, data breaches and any attempts to hack or tamper with your mobile communications and data. It enables you to establish and enforce a best-of-all-worlds mobile device security and compliance framework to match your specific enterprise mobile security requirements.

The SALUS Phone runs on a a custom-built security-rich operating system enhanced to address mobile security concerns facing enterprises today. The Android-like Customised OS is built from the ground up to provide in-depth protection against cyber-attacks by blocking the security breaches found in commercial operating systems. The customised OS is free of bloatware, hooks to carriers, and leaky data.



Features and Specifications:

- Holistic, best of-all-worlds mobile security platform
- Protected against any installation of Spyware, Trojans, Malwares, Ransomware and Phishing protection.
- Protection against IMSI Catcher / Wi-Fi Catcher.
- Emergency Distruction in case of device compromise.
- Hardware of trust, secure boot loader, and official drivers
- Highly certified architecture with no / hybrid Google services.
- Fused central intelligent and advanced defense controls across devices.
- Runs on a custom built, security-rich operating system, enhanced to address mobile security concerns facing enterprises today.
- Provides security and privacy by encrypting voice over IP calls through ZRTP.
- Centralized user groups and policies management console
- Military grade security delivers end-to-end messaging encryption, based on AES256 message encryption with 256-bit key length, and RSA 2048.
- Built-in phone book allows secret identity for users along with a flexible definition of user exposure policies across organizational groups.
- Mobile communications archiving for both voice calls and messages.
- Fused governance and control application ensures the safe use of corporate devices via configurable security profiles.
- Highly Secure & Encrypted Data Storage ensures information stored on the device is only accessible to users who enter the password/PIN.
- Detects behavior-based anomaly across Wi-Fi connectivity, cell tower connectivity, and in applications to discover evasive attacks.
- Flexible Deployment Options either as a hosted solution to reduce operating costs or as an on-premises deployment to provide complete control by the customer.