Monitor

LIVE UNDERCOVER OPERATIONS
COUNTER TERRORISM
CRIMINAL INVESTIGATION
EVIDENCE ANALYSIS

LOCAL PARTNER:

Mobilemonitor
Leeghwaterstraat 6a
4251LM Werkendam
The Netherlands
info@mobilemonitor.eu

INTRODUCTION

Due to complexities in today's profile of a Target User where the daily use includes Mobile and PC it is imperative to gather data from all available nodes. Criminals are using smartphones to circumvent government control to execute local, national or international crimes. Advanced Monitoring is driving criminals towards being increasingly suspicious leading to an increased pat-downs and scans in Undercover, sting and Counter Terrorism operations.

Our products span the complete Mobile and PC range to ensure that Law Enforcement officers have enough Attack and Defense Technology to facilitate Counter terrorism operations, Criminal Investigations and Undercover Operations.

All solutions are stealth that can be deployed without being detected via patdowns, physical or electronic signature scanning.

POSSIBLE USES

LIVE UNDERCOVER OPERATIONS

Any Law Enforcement officer when going in a Sting or Undercover has the threat of its cover being blown by subject to a pat down or electronic sweep for bugs. Our Long Range GSM / CDMA Controllers enable an off-the-shelf mobile device to be converted into a Long Range Undetectable Microphone. This ensures that electronic sweeps, pat downs or scanners cannot detect the bug. Since the Long Range Controllers work over Cellular Networks there is no range limitation of monitoring a target either from a van located a few meters away or from HQ located half the way around the world. Our products work under any circumstance and are ideally suited for Sting operations, detecting moles within an organization and intelligence gathering.

- Undetectable by Body pat down
- Undetectable by Microphone scanners
- Undetectable during monitoring
- Works anywhere with a GSM/CDMA Signal
- Can be monitored from few yards to half way across the world

COUNTER TERRORISM

Getting a warrant will enable a Law Enforcement agency to monitor the Target's conversations, SMS, Emails. However it will not enable the agency to read the mind of a terrorist. Our solutions are installed on a Target Phone or PC that enable the monitoring of conversations around the Mobile, PC or Laptop. A warrant gives insight into two way communications; however, our products enable access to offline conversations.

- Silently hides on Target Mobile or PC
- Obtains data all activity data
- Untraceable to source
- Evades Virus Signatures
- Can work across any boundaries
- Specialized process to deliver and deploy payload

EVIDENCE ANALYSIS

Advanced tools are made available for all products where law enforcement agencies can assign officers to monitor a specific target. All data is recorded on the user panel and can be managed via the admin panel. User panel enables officers to plot data on a map, listen to recorded conversations, read SMS, Call list and perform searches across dates and time for deeper analysis.

- A control panel is available to analysis uploaded data
- Plot movements on a map
- Gets Calls, Calling activity, SMS, GPS, Photos and more
- Enable separate users to monitor targets
- Complete Admin panel to manage officers
- Can monitor one or hundreds of targets

CRIMINAL INVESTIGATION

In an on-going investigation it is required to get the complete chain removed arrested or removed from the streets. Our applications get all data inside the mobile or PC device such as Contact Book / Address list, Email Contacts, Passwords, Browsing History, Photos, Videos which are not readily available but allowed while monitoring under a warrant. This level of data access will enable an agency to get a list of all associates and their daily movement by means of exact location. Our PC products go ahead and also get Voice Recordings and screen shots apart from keystrokes, shell access, complete file system access and more.

- Ability to track and monitor an individual or group
- Monitor Calls, SMS, and Location remotely
- Software is hidden and tamper-proof
- Data is uploaded over an encrypted channel
- Application works over proxy

	GSM CONTROLLER (LIVE)	GSM CONTROLLER (DELAYED)	ATLAS MONITOR (PC)	ATLAS MONITOR MOBILE
RECOMMENDED DEPLOYMENT	• Undercover Operations • Counter Terrorism	• Criminal Investigations • Undercover Operations	• Undercover Operations • Counter Terrorism • Criminal Investigations	• Undercover Operations • Counter Terrorism • Criminal Investigations • Evidence Analysis
DATA OBTAINED FROM TARGET	• Live Room Conversations • Live Call list, SMS & GPS	• Room & Call Recordings	• Screenshots, Keystrokes • Voice Recording, Shell, Clipboard • Remote File system, App Upgrade • Proxy Support, Kill & install app	• Room & Call Recordings • SMS, Call list, GPS • Photos, Contacts, BBM • Web History
RANGE LIMITATION	Unlimited	Unlimited	Unlimited	Unlimited
DETECTABLE BY PHYSICAL SEARCH	No	No	No	No
DETECTABLE BY ELECTRONIC SWEEP	No	No	No	No
MONITOR TYPE	Real time	15 Minutes delayed	15 Minutes delayed	Live PC Monitor
UNDETECTABLE	Yes	Yes	Yes	Yes
ENCRYPTED TUNNEL UPLOAD	N/A since voice is routed over GSM / CDMA	Yes	Yes	Yes
INDIVIDUAL SIGNATURE	Yes	Yes	Yes	Yes
WEB PANEL	Yes	Yes	Yes	Yes
REMOTE CONTROL	Yes	Yes	Yes	Yes
VISIBLE IN INSTALLED APPS	No	No	No	No
COMPATIBILITY	• Android • Symbian / Nokia	• Android • Blackberry • iOS • Symbian / Nokia	• Windows XP & above • Windows 2000 Server & above • Windows x86 & 64	• Android • Blackberry • iOS • Symbian / Nokia

LONG RANGE (REALTIME) MOBILE MONITOR

Long Range Mobile Controller is an undetectable listening device for Undercover, sting or Live Counter Terrorism Operations. It is installed as software in an existing off-the-shelf Mobile Device and modifies the behavior of the mobile handset as per defined rules.

The Long Range controller software implements the capability to answer an incoming call silently from a pre-defined number. All other activities of the mobile device remain unaltered. This enables a Law Enforcement team to listen into Live Conversations taking place around the device to accurately execute the next steps of any operation.

LONG RANGE (REALTIME) MOBILE MONITOR

Enables real time access to Room & Call conversations, SMS and GPS Location
Internet is not required on the Target Device.

UNDER COVER OPERATIONS

- Arm the operative with Long Range enabled mobile device and listen in from a van or HQ located half way around the world.
- High Voice quality
- Works anywhere with GSM / CDMA Coverage

COUNTER TERRORISM

- Install Long Range software on a Target and monitor all their room conversations.
- Monitor at any time without being detected from any distance.

INTERNAL AFFAIRS

- Monitor internal assets to ensure Highest Standards of integrity

How to install?	How does it work?
1 Enter a URL on the target phone.	1 Send SMS to the Target Phone to set the pre-defined number.
2 Click "Yes" to any queries that need permission to install.	2 Place call to the Target Phone.
3 Walk Away from the Target Handset.	3 It will answer in ghost mode & you can monitor all room conversations around the target device.

CERTIFICATION

- Developed using ISO 9001:2008 Management Process

FEATURES

- Answers call silently without indication.
- No Call Logs, Flickers or vibration.
- Default behavior of device is unchanged.
- Undetectable by Metal Detector Undetectable by "pat-down's" or Bug Monitoring Equipment
- Obtains GPS Location when requested via SMS

SPACE REQUIREMENT

- 100 Kb free on device

REQUIREMENTS

- Active SIM Card with SMS Credits

COMPATIBILITY

- Android Devices
- Symbian Devices

LONG RANGE (DELAYED) MOBILE MONITOR

Long Range (Delayed) Mobile Controller is undetectable software for evidence gathering in Law Enforcement Operations. It is installed as software in an existing off-the-shelf Mobile Device and records Room Conversations on the target device and sends it to control room for analysis.

This software is an advanced logger of sorts with the capability to logging Room Conversations and uploading them to a central server. An excellent tool for undercover, terror suspect monitor or mole hunting operation where voice data is imperative for delayed analysis.

Live Data analysis is possible via Long Range (Real Time) Mobile Monitor

LONG RANGE (DELAYED) MOBILE MONITOR

Logs and uploads Voice Conversations, SMS and GPS Location of the target phone every 15 minutes.

UNDER COVER OPERATIONS

- Where real time monitoring is not possible and evidence can be uploaded at end of day or at a defined interval
- Data is stored and displayed on timeline thus providing greater insight into an investigation
- Can record room conversation with GSM / CDMA Coverage. Upload only requires Internet access via Satellite, 3G or Wi-Fi. Hence can be deployed where network coverage is weak.

COUNTER TERRORISM

- Install Long Range software on a Target and monitor all their room conversations.
- Monitor at any time without being detected from any distance.

INTERNAL AFFAIRS

- Monitor multiple internal assets and get all data uploaded at night for deeper analysis.

How to install?	How does it work?
1 Enter a URL on the target phone.	1 Application uploads Recorded room conversations, SMS & GPS to a control room server.
2 Click "Yes" to any queries that need permission to install.	2 All data is encrypted AES 256 and uploaded via HTTPS.
3 Walk Away from the Target Handset.	3 Control Room Server enables detailed viewing per user, plotting on map & viewing data such as Uploaded SMS, Photos from device & Phone-book.

CERTIFICATION

- Developed using ISO 9001:2008 Management Process

SPACE REQUIREMENT

- 100 Kb free on device

REQUIREMENTS

- Active SIM Card with 3G Credit

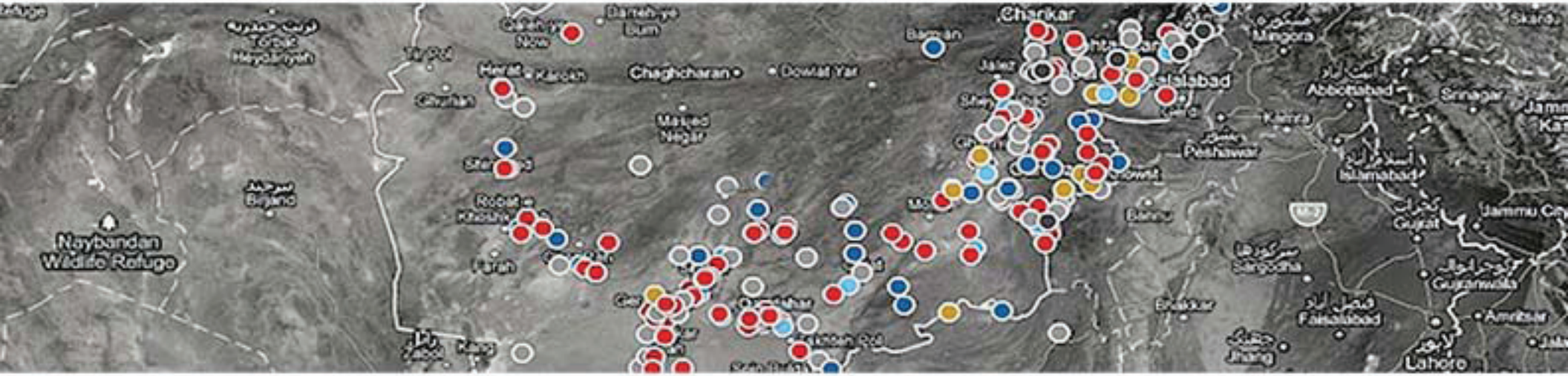
COMPATIBILITY

- Android Devices
- Blackberry Devices
- iPhone / iOS Devixce
- Symbian Devices

ATLAS MONITOR (MOBILE)

AtlasMonitor – Mobile performs extensive data sniffing on a Mobile device and uploads that silently to a Control Server in the background. AtlastMonitor (Mobile) accepts commands silently via HTTP (S) from the server and administers services and uploads as per the instruction set.

AtlasMonitor (Mobile) has two components to its architecture. The first being the Mobile Client that works on Android, Blackberry, iPhone and Symbian; The second being the Control Server which resides behind a secure firewall accessible to the Mobile Client via HTTP.



ATLAS MONITOR (MOBILE)

EVIDENCE GATHERING

- AtlasMonitor (Mobile) enabled detailed evidence to be obtained from the Mobile Device of a suspect with time.
- Nothing escapes the software. All conversations can be recoded even when they suspect is out of network coverage.

INTERNAL AFFAIRS

- Monitor internal assets to ensure Highest Standards

The Mobile Client is able to obtain the following

- Recording of environmental conversations (i.e. room conversations)
- SMS Data of Incoming & Outgoing SMS with Name and Number.
- GPS Location of Handset
- Contact book data (name, phone number and email addresses)
- Photos stored on device
- Call Activity
- BBM (for Blackberry only)
- Web Browsing History

The Control Room Server is able to send commands to initiate data retrieval of the above-mentioned command including the ability to start / stop and kill the application on the device. The application is hidden in all Handsets that is being achieved by means of deploying Mobile Vulnerabilities not available to the public.

How to install?	How does it work?
1 Enter a URL on the target phone.	1 Application uploads Recorded room conversations, SMS & GPS to a control room server.
2 Click "Yes" to any queries that need permission to install.	2 All data is encrypted AES 256 and uploaded via HTTPS.
3 Walk Away from the Target Handset.	3 Control Room Server enables detailed viewing per user, plotting on map & viewing data such as Uploaded SMS, Photos from device & Phone-book.

ATLAS MONITOR (PC)

An advanced PC Monitoring Remote Backdoor that has the capability to intercept all traffic from the Target PC; accept commands from the Control Server and is undetectable by Anti-Virus Scanners (signature and heuristic) and hidden in Windows.

Advanced PC Monitoring software takes advantage of several vulnerabilities to deliver it's payload, run hidden on PC and transfer data using HTTPs bearer.

ATLAS MONITOR (PC)

AtlasMonitor (PC) or Remote Administrator Tool (RAT) has the following backdoor features:

TYPE OF SERVICE

The PC RAT is connecting service with an "always-on" HTTP connection to accept command.

DYNAMIC PROXY BASED DATA ROUTING

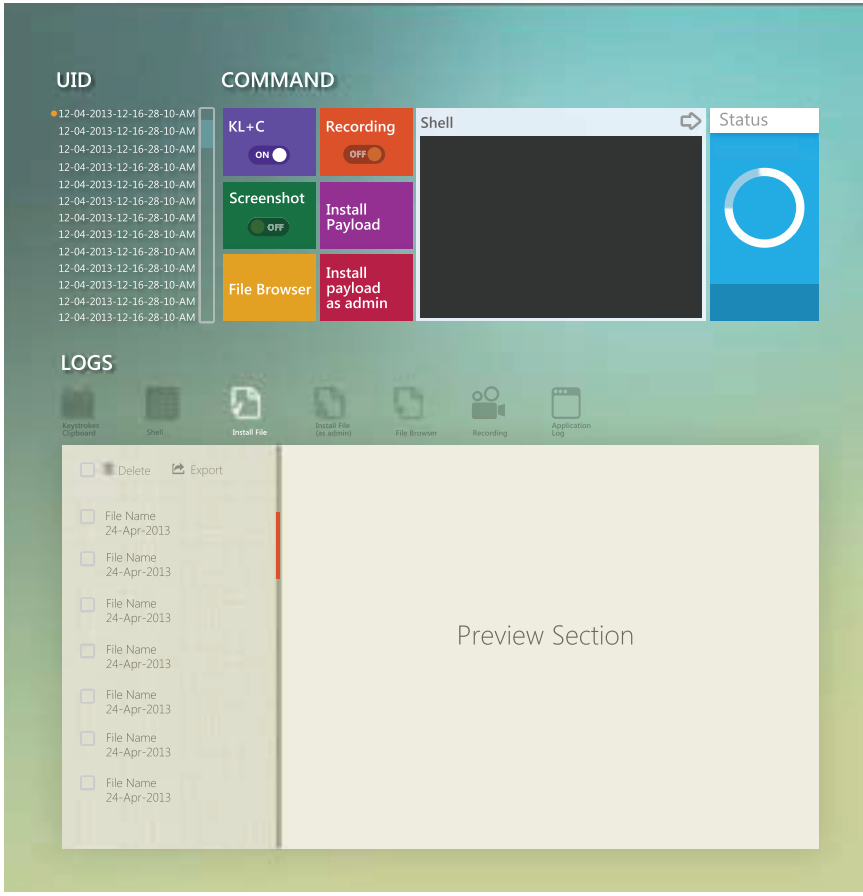
The administrator can setup proxy servers to re-route data from the Target PC or change the command servers via the panel. The application also has the ability to self heal itself incase any of the command servers are down.

HIDDEN STARTUP

The RAT startups on every computer restart without creating an entry in the registry or startup items list.

INSTALL / REMOVE SOFTWARE

Control Panel enables installation or removal of any software via a custom binary that will be silently down-loaded and executed.



ATLAS MONITOR (PC)

REMOTE SHELL ACCESS

Single command and multi-command advanced cached shell access is provided via the connecting service. Full shell commands are available without any restrictions. Shell commands are executed as per the privileges of the currently logged on user.

- Single Command Shell gives the ability to the user to send a single command and obtain a quick response from the Target PC.
- Cached Shell commands give the ability to the user to send multiple commands in one go and receive a comprehensive response. The benefit is decreased data transfer on network thus reducing the risk of altering a Network Administrator.

REMOTE FILE BROWSER

Download files to Target PC: RAT enables any type of documents/files/photo or custom extension files to be downloaded to the target PC at any location.

Upload files from Target PC: RAT enables the Listening post to upload any file(s) from the target PC to the Monitoring Panel.

REMOTE FILE EXTRACTOR

Ability to fetch any file from any folder

REMOTLY INFECT OTHER NETWORK PC

Ability to remotely view network configuration and send file to desired PC

RECORD ROOM CONVERSATIONS

Records Room conversations around the PC and instantly uploads in PCM (lossless) format. The files are zipped to minimze net-

ADDITIONAL FEATURES

- Skype/Yahoo/MSN/Jabber or any other
- App's Chat Logs
- View Installed Apps
- Remotely Install new Apps

ATLAS MONITOR (PC)

SCREENSHOTS

The application takes high-resolution screenshot (PNG format) and uses an internal compression algorithm that compresses the PNG by 95%. This ensures very low data transfer between the PC and Server to ensure any monitoring eyes don't see a lot of network traffic.

CLIPBOARD MONITOR

All clipboard activity is uploaded to the monitoring panel.

KEYBOARD MONITOR

All keys typed on the Target PC are captured silently and uploaded to the Monitoring Panel.

LOW TRAFFIC GENERATION	2 Kb every 21 minutes, if activated
COMMAND PAYLOAD SIZE	5 bytes
COMPATIBILITY	Windows XP, Windows 7 & 8.
DEPLOYMENT BEARER	Internet, USB, Silent attachment exploiting LNK vulnerability or Binary.
SPACE REQUIREMENT	3 Mb of free space on Target Machine
CERTIFICATION	Developed using ISO 9001:2008 Management Process
SECURITY FEATURES	Hidden auto start on boot No pop up during startup or shutdown Cannot be detected by Anti Virus Applications Ability to send & receive responses via proxy Ability for AtlasMonitor to heal itself
COMPATIBILITY	All Windows Platforms

Deployment Process

Since every deployment is done differently several vulnerabilities can be exploited to install the software. These are available as demos and then for purchase as per the customer requirement. Silent and cloaked installation processes are available to the Law Enforcement Agencies.

R.A.T Signature

Each customer is provided with a separate build with a different signature and connecting service type. This ensures that no two customers have the same payload.

e96SECURE CALL

e96SecureCall is a easy to use, downloadable application that runs on off-the-shelf on Android™& iPhone® smart-phones and uses AES 265 bit security for protecting sen-sitive Video / Voice calls and SMS against interception.

e96SecureCall uses RTSP to transfer data such as Voice, SMS, Files, Photos, etc. All transfers are realtime via a centrally managed server. This server can be provided at customer premises for self managment.

EASY TO USE

e96SecureCall intuitive user interface makes a secure call as easy as making a normal call:

- To make a call, users simply open the e96SecureCall application by selecting the icon on their phone, and tap a name on your Secure Contact List and press Call (to initiate a secure call) or SMS (to send an encrypted SMS over IP channel)
- e96SecureCall needs to be running on both devices so that both can encrypt/decrypt the voice/video call or SMS at each end to provide security along the entire path between the callers
- It also uses the data channel (IP) rather than voice channel so both devices also need to be connected to the internet using standard data connectivity provided by the service provider
- Government-grade encryption is used to check the identity of each device on the call and then encrypt the call
- The recipient's phone displayes an incoming call alert by means of ring and Incoming Call Display.
- If the call is accepted and the pre-shared key matches then the a normal conversation is conducted until one of the callers hangs up. The caller is notified if the recipient is busy or not online. Video Call only works on front facing camera devices

SECURE MESSAGING ON ANDROID & iPHONE

To counter interception vulnerabilities of standard SMS and IM, e96SecureCall includes a secure messaging feature which brings end-to-end encryption to instant messaging. e96SecureCall's encrypted messaging sends secure messages directly between BlackBerry, Android and iPhone smartphones.

Designed for real-time, short-lived messages, similar to information exchanged via voice calls, e96SecureCall delivers encrypted messages directly when both parties are connected. This avoids the storing and forwarding of messages, which users typically don't want when sending time-sensitive information, preferring instead that the messages be sent immediately and deleted as soon as read. e96SecureCall delivers encrypted voice calls using "Pre-shared" key and symmetric cryptography and its secure messaging uses the same architecture but sends encrypted text data, rather than voice data over IP Channel.

SECURE

In any product, security is only as strong as:

- The strength of the encryption it uses
- The security of the secret keys used to unlock the encryption
- The integrity of the product implementation and the trustworthiness of the supplier

e96SecureCall uses encryption algorithms that are recommended for military and government secure communications and its secret keys never leave the mobile device. The product has been tested by third parties and validated to several government standards including US NIST FIPS 140-2 for its cryptography.

HIGH PERFORMANCE

All communications products that rely on cellular networks are dependent on the strength, availability and reliability of the underlying radio network for their performance. e96SecureCall understands this industry problem and is one of few companies to deliver specific technology solutions for optimizing performance in poor and variable wireless conditions, including its Encrypted Mobile Content Protocol™ and Encrypted Content Delivery Network™.

e96SecureCall automatically switches to the highest quality network that the handset is connected to so that Wi-Fi ™ is selected in preference to cellular networks. Also calls work across changing cellular networks (for example if a 3G connection is degraded by the carrier to an EDGE or GPRS connection) even as the call is in progress. Callers can be on different networks in different countries for example Wi-Fi at one end and GPRS at the other.

EASY TO SET UP

Setting up e96SecureCall on a cell phone is easy:

- Users send a serial number of their phone to e96SecureCall and the secure number they want to use.
- The e96SecureCall software application is then transferred to the user for installation. The easiest transfer method is via a downloadlink contained in an SMS sent by e96SecureCall to the user (if a phone number is given). It can also be sent by email or on a storage device for loading from a PC, or provisioned from a device management application such as BlackBerry Enterprise Server.
- A standard mobile application download procedure is then completed including validation checks by the handset to ensure the authenticity of the e96SecureCall software application.

If the phone is lost or stolen, e96SecureCall can be disabled remotely, instantly.

PRODUCT FEATURES

E96SECURECALL'S TECHNOLOGY

e96SecureCall technology stands apart from the competion since the encryption keys are never passed over the IP Network. Essentially our architecture operates on the lines of a RADIUS server which enables pre-shared keys to be entered on the client devices which ensures that intercepted data cannot be listened into or tampered with. Voice / Video or SMS data is encypted in many layers starting with RC4 and AES 256. The complete process is ISO 27001 and FIP 140 certified.

CRYPTOGRAPHY & RANDOM NUMBER GENERATION

e96SecureCall uses standard encryption technologies including:

- Advanced Encryption Standard (AES) for symmetric encryption
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) for key agreement
- Secure Hash Algorithm (SHA) for message digest

In addition, before these algorithms are processed, e96SecureCall uses additional algorithms for added security (double-wrapping). For example, the voice call is first encrypted using RC4-256 bit and then encrypted again using AES-256 bit.

PUBLIC CRYPTOGRAPHY

(2048-bit RSA & ECDSA using curves with 384-bit prime module)
RSA and ECDSA are used for authentication. The key pairs are generated on the phone during the installation and are unique to each phone. A private key is never shared. The Eliptic Curve Dif fie-Hellman (ECDH) and RSA algorithms are used for key exchange. The session key is only valid for one phone call and securely destroyed after use.

HASHING ALGORITHMS

(SHA512)
Industry standard hashing algorithms are used for increased integrity assurance.

SYMMETRIC CRYPTOGRAPHY

(AES & RC4, both 256 bits)
Both encryption algorithms are used at the same time. The data packet is first encrypted with RC4 and the cipher text is then encrypted again with AES in Counter Mode (CTR). Both algorithms are initialized with the exchanged session key.

RANDOM NUMBER GENERATION

A 2048 bit seed pool is generated during the installation and is periodically updated. The initial seed is derived from th e touch input.

CUSTOMIZATION OF E96SECURECALL

Since we are the manufacturers of this product we can white label this and develop custom branding for a corporate or government agency. If required new certification is provided under the required agency name. Preshared keys are generated by the customer which can be changed at any time on the backend server..

Certain handset limitation apply for Video Calls. Contact us for more device compatibility information.

KEY FEATURES

Security	• Strong end-to-end encryption
Simplicity	• Runs on popular smartphones such as Android TM & iPhone® • No specialist equipment required • Intuitive user experience, runs in background & integrates with device phonebook
Performance	• Interoperates across and between leading smartphones and cellular networks • High call quality with low latency • Operates on all data-capable wireless networks International calling in for all GSM networks. • Loseless codec ensures crystal clear audio quality.
Network Support	Any IP-enabled network, e.g. • GSM/CDMA • 2G • 3G • 4G • Satelite • Wi-Fi™

SECURE MESSAGING

e96SecureSMS ensures that SMS are un-crackable by offering a redundant rotating cypher military grade encryption of data. We offer a reward of USD 1,000 to anyone who can intercept and crack this SMS.

e96SecureSMS sends Encrypted SMS from the Native Inbox of the device over the Network provider's SMS Channel. It does not use or route any data over the Internet. In-fact there is no third party server included in the product mix or delivery mechanism.

e96SecureSMS can be used on any network such as GSM / CDMA / Satellite / Closed User Groups or Military Networks.

PRODUCT FEATURES

e96SecureSMS is a secure and innovative messaging application that enables a user to send encrypted SMS to a user from the native Inbox of the device. e96SecureSMS uses AES 256 bit encryption FIPS 140 – 2 Compliant with the initializing vector as a random key generated from device's Meta-data. This key is changed with every SMS thus ensuring adding security.

e96SecureSMS is a 100% secured software solution and does not require expensive gateway and routers to be installed. Simply install the software on two devices and SecureSMS software operates with military grade encryption.

Ideally suited for	How it works
• Covert operations • Interagency operations • Emergency operations • Mission critical communication • Sensitive/private communication • Alerts and notifications	• Open Inbox of your device • Type an Identifier string followed by Body. • Select Recipient(s) and click Send.

APPLICATION SECURITY

- Sends AES 256 bit Encrypted SMS from Default Inbox
- Passcode locked application to access encrypted data
- On device data is encrypted
- FIPS 140 – 2 Compliant
- Rotating Encryption
- No third party server or services are involved

REQUIREMENTS

- Android Device with 4.x above
- Active SIM cards / Network Connec-

APPLICATION FEATURES

- Ability to send encrypted and normal SMS from Default Inbox
- Tight integration with phonebook of device
- Encrypted SMS do not appear in normal Inbox
- Secure SMS can be sent to one or multiple recipients

Mobile monitor