

## HÖCHSTE VERTRAULICHKEIT FÜR IHRE MOBILE KOMMUNIKATION

Secure Mobile VME ist eine für Mobiltelefone nach modernsten Standards und höchsten Sicherheitstechnologien konzipierte Verschlüsselungs-Suite für Managed Service Provider. Diese ermöglicht die verschlüsselte Kommunikation von Telefongesprächen, SMS sowie E-Mail und genügt dabei in puncto Sicherheit allerhöchsten militärischen Standards. Als Verschlüsselungsalgorithmus kommt dabei AES mit einer Schlüssellänge von 256 Bit zum Einsatz. Für optimalen Schutz sorgt darüber hinaus eine nach EAL5+ zertifizierte Micro SD-Karte, die im Lieferumfang enthalten ist.

**Bereits wenige Minuten nach der Installation ist Secure Cloud Mobile VME betriebsbereit.**

### WARUM MOBILE KOMMUNIKATION VERSCHLÜSSELN?

Haben Sie jemals über die Mittel und Wege nachgedacht, mit der Ihr Mobiltelefongespräch von einem Gerät zum nächsten übertragen wird und wie viele Abhörmöglichkeiten es gibt? Andere können leicht Ihre gesamte Kommunikation belauschen. Die gewonnenen Informationen lassen sich in vielfacher Weise missbrauchen. Deshalb sollten Sie sich dieses Sicherheitsrisikos stets bewusst sein!

### WIE FUNKTIONIERT SECURE MOBILE VME?

Nach einer zunächst automatisch eingeleiteten sicheren Authentifizierung über den VME-VoIP-Server beim Service Provider erfolgt ein Schlüsselaustausch und es startet die Synchronisierung für die Verschlüsselung des Mobiltelefons. Die Stimme wird dabei durch Secure Mobile VME in Daten umgewandelt, transparent verschlüsselt und in kleine Datenpakete aufgeteilt. Diese Datenpakete werden dann fast in Echtzeit übermittelt, bis sie das andere Mobiltelefon erreichen. Nach Erhalt der sicheren Pakete entschlüsselt das andere Mobiltelefon die Daten und stellt den Originalton auf dem Gerät her.

**„Secure Cloud Mobile VME ist sehr einfach zu verwalten sowie zu benutzen und bietet eine hervorragende Sprachqualität!“**

SECURE  
CLOUD®



### VERSCHLÜSSELT HOCHSICHER TELEFONGESPRÄCHE, SMS, CHAT UND E-MAIL

Telefonpartner können mit Secure Mobile VME ihre Gespräche und andere Datenübertragungen über Telekommunikationsnetzwerke wie WiFi, HSUPA, HSDPA, UMTS, LTE, CDMA, GPRS, EDGE, GSM und Satellit effizient durch sichere Verschlüsselung gegen das Abhören durch Dritte schützen. Der Clou: Secure Mobile VME lässt sich völlig risikolos über beliebige Hotspots nutzen. Steht eine WiFi-Verbindung zur Verfügung, wird diese automatisch genutzt und ansonsten teure Gesprächskosten entfallen völlig.

Secure Mobile VME erfordert vom Mobiltelefonbenutzer keinerlei technische Fähigkeiten. Kodierungsschlüssel sind direkt durch diesen leicht zu konfigurieren und garantieren einen ganzheitlichen Datenschutz. Secure Mobile VME ist ein Top-Level-Produkt, das entwickelt wurde, um u. a. Militär- und Regierungsvorgaben zu genügen.

Die Sicherheitslösung stellt gleich zwei Möglichkeiten bereit, um den während des Gespräches verwendeten Anti-Spionage-Kodierungsschlüssel zu erzeugen: Das 4096-Bit-Diffie-Hellman-Protokoll oder die elliptischen Diffie-Hellman-Kurven.

Secure Mobile VME generiert für jedes Telefongespräch einen anderen Kodierungsschlüssel. Benutzer können dabei auch Kombinationen von Diffie-Hellman- und gemeinsamen Schlüsseln einsetzen. Am Ende eines jeden Gespräches wird der Schlüssel dann automatisch gelöscht.

Die Lizenzierung für Secure Mobile VME erfolgt auf Basis einer mitgelieferten MicroSD-Karte, die in das Mobiltelefon einzusetzen ist.

**LEISTUNGSMERKMALE & FUNKTIONEN**

- Absolut sicherer Abhörschutz für ein- und ausgehende Mobiltelefonate, den Anforderungen von Regierungen und Militär genügend.
- Verschlüsselte Mobilfunk-Kommunikation über den CSDv.110- oder v.32-Kanal (auch bekannt als Daten-/FAX-Kanal).
- Sichere Ende-zu-Ende-Verschlüsselung unter Nutzung des AES Algorithmus mit 256 Bit Schlüssellänge.
- Codeschlüssel generiert mit Diffie-Hellman 4096-Bit oder elliptischen Kurven 571-Bit.
- Sichere, verschlüsselte Speicherung des benutzer-eigenen Kodierungsschlüssels.
- Bidirektionale numerische Identifikation zur Abwehr von Man-in-the-middle-Angriffen.
- Möglichkeit zur Implementierung proprietärer Verschlüsselungsalgorithmen und S-Boxen.
- Kommunikation in Klartext mit anderen Teilnehmern ohne Krypto-Funktion im Mobilfunktelefon.
- Mehrsprachige, einfache und benutzerfreundliche Menüführung.
- Automatische Anruflistenlöschung beim Ausschalten.
- Starke Benutzer-Authentifizierung, Empfangen und Senden von verschlüsselten SMS-Nachrichten.
- Sicheres und verborgenes Speichern von verschlüsselten und unverschlüsselten SMS.
- SMS-Nachrichtenaustausch mit Benutzern auch ohne Verschlüsselung möglich.
- Gezielte Löschung aller Kryptoinformationen auf beiden beteiligten Endgeräten.
- Benachrichtigung bei nicht autorisiertem Wechsel der SIM-Karte im Falle eines Verlusts oder bei Diebstahl.
- Remote administrierbares Schlüssel-Management-System (KMS).
- Möglichkeit zur Einrichtung geschlossener Benutzergruppen sowie Mehrfachgruppenzuordnungen für Benutzer.
- Beliebig skalierbar.
- \*Optional: Eigenes Key-Management

**TECHNISCHE DATEN**

## VERSCHLÜSSELUNGALGORITHMEN

- AES256, ECDH, HMAC, SHA256

## ERWEITERTE SICHERHEIT

- MicroSD-Karte für das Mobiltelefon mit eingebettetem, EAL5+ zugelassenem Smartchip, der die Sicherheitsfunktionen durchführt.
- Zufallsgenerator im Smartchip.

## UNTERSTÜTZTE MOBILTELEFONPLATTFORMEN

- BlackBerry RIM OS5, OS7
- Nokia Symbian
- Android

## NETZWERKE

- UMTS
- LTE
- WiFi

## HARDWAREANFORDERUNGEN VME VOIP-SERVER

- CPU: Intel Xeon i7 W3520
- RAM: 24 GB
- Festplatte: 120 GB SSD/SATA Raid
- Double Source Hot Switch Stromversorgung

## SOFTWAREANFORDERUNGEN VME VOIP-SERVER

- Ubuntu ab V10.04 oder höher
- Alternativ: Debian ab V6.0

## HARDWAREANFORDERUNGEN KME\*

- Notebook oder PC mit internem UMTS-SIM-Slot oder USB-Port für externe USB-UMTS-Modem-Verbindung

## SOFTWAREANFORDERUNGEN KME\*

- Microsoft Windows 7 Professional, englisch



it-securitygroup