Secure Endpoints - Mobile

Cybersecurity

PhoneCrypt M100

▼ PhoneCrypt M100

ST Engineering

KeyCrypt C10

microSD HC

8GB

Secure Communication

PhoneCrypt solution suite is a dedicated Secure Voice over IP (VoIP) and Instant Messaging (IM) solution to ensure complete privacy for voice and IM communication for enterprise professional and organization. It comprises of front-end client solution and backend VoIP/IM system to provide a complete secure communication over IP network. It is designed with the true end-to-end encryption and rich features for secure voice call and instant messaging.
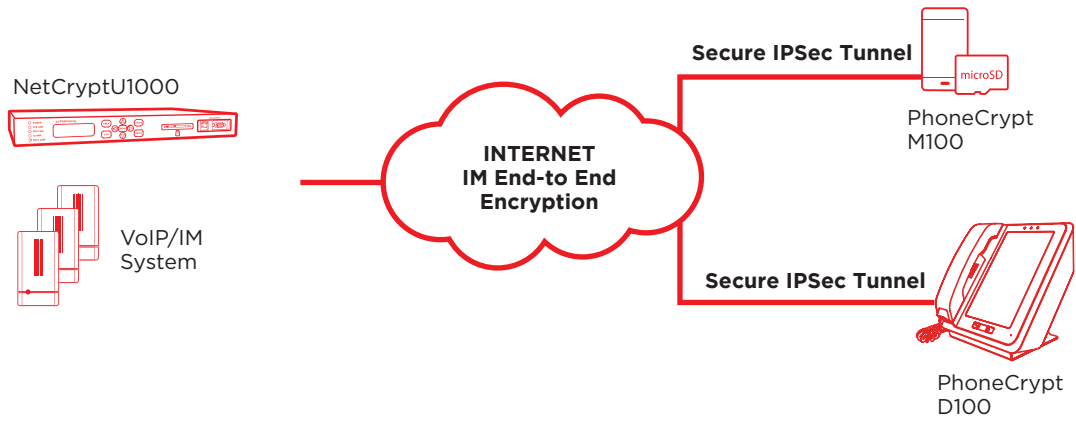
PhoneCrypt M100: a Secure VoIP/IM Android application with secret credentials store in a cryptographic MicroSD card. It is designed for mobile user with Android smartphone and it connects to backend secure VoIP/IM system through 3G/4G/Wifi connection.

Both the Phonecrypt D100 and M100 will be connected to the secure backend VoIP/IM system which comprises of NetCrypt U1000 IP encryptor and PhoneCrypt server.

Key Features

• End to end secure voice conversation and instant messaging between the clients through the backend PhoneCrypt system

• Layer 3 IPSec security providing maximum security

• AES algorithm for data confidentiality, Secure Hash Algorithm (SHA) as well as Internet Key Exchange (IKE) protocols for integrity protection and user authentication

• Excellent voice quality

• Easy installation and supporting dynamic IP addressing

• Plug-and-play unit provides greater convenience for travellers

• Back-end system also comprised of encrypted storage system for contacts. It protects confidential data against unauthorized access

ST Engineering

Deployment Use Cases

NetCryptU1000

VoIP/IM System

INTERNET
IM End-to End Encryption

Secure IPSec Tunnel

PhoneCrypt M100

microSD

Secure IPSec Tunnel

PhoneCrypt D100

Specifications

Supported Platform	Android 9 and above with internal microSD slot
Network Features & Protocols	IP Security/Encapsulating Security Protocol Support Layer 3 encryption capability IP Compression QoS support Traffic flow confidentiality
Authentication	RSA Public Key Signature (up to 2048 bit)
Key Management	Support Internet Key exchange (IKE v2) DH supports up to 8192 bit Supports ECDH (up to P-521 bit)
Encryption Algorithm/Modes	AES-CBC (256 bit)
Hash Algorithm	HMAC-SHA1 HMAC-SHA2 (256, 384, 512 bit)
Security Features	FIPS 140-2 certified cryptographic MicroSD card for key storage

www.stengg.com/cybersecurity
cybersecurity@stengg.com