Feature List

- Secure group communication
- Cross platform
- Contact authorization control
- Suitable for any IP access network
- Presence information
- Call recording with user indication
- Secure voice calls (VoIP)
- Centralized contact, device and user management
- Secure file transfer (videos, pictures, audio messages and documents)

Secure conference calls
Secure Chat / IM
Secure SMS
Link-quality indicator during calls
Auto-destruction of messages
Mute and loudspeaker call features

Citizen Services & Immigration Control
Law Enforcement
Critical Infrastructure Management
Public Administration Services
Information Management
Emergency & Disaster Management
Inter-Agency Collaboration

Prevent Phone Tapping with
Secure Mobile Communications
Overview

The evolution of wireless communications has spread enormously in corporations, enterprises and public institutions. Even military forces, police, emergency and rescue, political and other sensitive sectors have adopted new technologies widely. The benefit is clear; increased mobility, availability of value-added services and higher efficiency in the daily operation of those organizations.

Whilst professionals in different industries need to exchange information anytime and anywhere, it must be ensured that all sensitive data is kept secure and private. This concerns not only the communication traversing uncontrolled networks but also a person's identity, credentials, permissions and rights. The usage of public networks and services for communication, like traditional cellular voice networks, SMS, wireless data, etc. has been proven to be unsecure.

Secure Mobile Communication is a mobile communication solution combining multiple services such as telephony, instant messaging and SMS with sophisticated security mechanisms to protect your organization's sensitive and confidential information. Secure Mobile Communication (SMC) solution transforms public communication networks and standard terminals into highly secure communication channels. Special hardened devices are as well available to meet the strongest security requirements.

Security Architecture

Double layer security for extra protection

- End-to-End encryption
- Fully deployable on customer premises without any third party access
- Scalable and modular architecture
- Key agreement: Ephemeral Diffie-Hellman (EDH)
- Encryption cipher: AES 256
- Hashing algorithm: SHA-2
- Support for Hardware Security Modules (HSM) through a PKCS#11 interface
- Keys are negotiated per call and destroyed afterwards
- Protection against replay attacks and dictionary attacks
- Protection against Man-In-The-Middle (MITM) attacks
- Device authorization control for additional user protection

Benefits

- Protect your organization with a reliable, global, secure network for voice and messaging services
- The solution protects the data in transit end-to-end
- Authentication confidentiality and integrity is supported across different communication domains
- Delivers high voice quality in mobile data networks
- Deployable independently of mobile operators
- Fully integrated into the mobile operating system of the end user devices
- Suitable for a multitude of networks (EDGE, UMTS or Wi-Fi)
- Incorporates an intuitive and friendly user interface
- Helps organizations optimize their communication costs
- Can be hosted completely within the customer's own premises without any third party involvement
- Low user involvement and reduced maintenance costs compared to traditional hardware based solutions
- BYOD strategies are as well fully supported and empowered under this concept