

GSMK CryptoPhone IP Server System

GSMK CryptoPhone IP Server System

Secure switching system for private CryptoPhone IP networks

SYSTEM OVERVIEW

Concept

The GSMK CryptoPhone IP server system offers the capability to run private, customer-managed CryptoPhone IP networks by providing IP presence and routing services.

GSMK CryptoPhone IP servers exclusively provide private call switching and presence services. They are not involved in the call and message encryption process since communication between GSMK CryptoPhones is always end-to-end encrypted. All voice and message encryption functionality resides exclusively on the users' phones. This ensures that even if a GSMK CryptoPhone IP server is captured by hostile elements, it remains impossible to compromise the security of encrypted communications.

Each CryptoPhone IP server element is scalable to multiple hardware nodes per element.

GSMK CryptoPhone infrastructure elements are implemented in Erlang to achieve true carrier-grade reliability, scalability and redundancy. All system state is held in a distributed database that can be spread over multiple hosts via VPN interconnects to provide maximum reliability, allowing clients to build distributed private, fault-tolerant, non-stop CryptoPhone IP networks. Changes to a running server can be made at runtime without stopping productive operations, so updates do not interrupt communications.

CryptoPhone IP server systems are scalable from small groups to very large corporate and government-wide systems capable of serving hundreds of thousands simultaneous encrypted calls.



Trustworthy Voice & Message Encryption

GSMK CryptoPhone IP servers come with full source code available for independent review. Finally, you can perform an independent assessment to ensure that you can build your private network without any backdoor in the communications infrastructure that you entrust your security to. The GSMK CryptoPhone server system enables you to put the trust where it belongs – in a trustworthy, open and scientific verification process.

GSMK CryptoPhone IP secure phones supported by CryptoPhone IP server technology are based on well-researched algorithms for both encryption and voice processing. They feature the strongest encryption available combined with key lengths that provide peace of mind today and in the future.

Server Elements & Administration

Each GSMK CryptoPhone IP server system consists of two logical elements, which are typically deployed together in one single hardware system.

Presence Server • The Presence Server keeps in regular contact with each GSMK CryptoPhone IP secure phone registered in the private network to ensure reachability regardless of how and where each CryptoPhone connects to the network. In this capacity, the Presence Server functions as the point of contact between individual CryptoPhones. When one CryptoPhone calls another CryptoPhone that is registered with a particular Presence Server, the server checks if the target phone is online and notifies that phone of the incoming call. When the call is picked up, the Presence Server requests a trunk connection at the Trunk Server and hands the trunk information over to both calling and called party.

Trunk Server • The trunk server connects the end-to-end encrypted data streams of two GSMK CryptoPhones, as directed by the Presence Server. Its sole purpose is setting up and maintaining this connection until one of the parties hangs up. Trunks have different types, for messages and for streaming data.

Administration • Administration of a private server infrastructure is straightforward and accomplished via a web-based user interface. Administrators can add and remove users to and from the private network either manually or based on individually configured rule sets. All administrative functions only control access to the private network. By design, GSMK CryptoPhone IP servers exclusively perform call and message routing functions, completely independent from and without any information about the encryption processes performed by the individual phones.

Configurations

- ✓ Deployment options: 19" rack-mounted servers for deployment in data centers 19"/2 ruggedized, MIL-STD- 810F & MIL-STD-461E compliant servers for mobile deployment in extreme environments
- ✓ Backhaul options: High-speed fixed-line Ethernet, satellite and/or terrestrial wireless IP data links for land-mobile and naval applications
- ✓ Scalability options: Available in configurations from redundant stand-alone systems for small groups to distributed, fault-tolerant server configurations for CryptoPhone IP mass

deployments throughout large organizations

- ✓ Configurability: Freely configurable levels of isolation from walled-off private networks to IP PBX integration with virtual extensions

Optional Accessories

- ✓ IP54, MIL-STD-810F and MIL-STD-461E compliant uninterruptible power supplies
- ✓ Shock and vibration absorbing mounts with passive cooling for mobile deployment in heavy vehicles in conjunction with tactical wireless network systems

GSMK - CryptoPhone - IP Server System