ARENIM TECHNOLOGIES

CryptTalk

Maximum communication security

Comprehensive call and SMS encryption
Complex security against interception
Direct end-to-end encryption

Features

- Comprehensive call and instant message encryption
- Secure authentication
- Carrier independent
- Easy to use
- Mobile and desktop versions
- European product
- Outstanding voice quality
- Voice transfer without delay
- No investment, you will pay a license fee
- Customizable solution
- Company integration
- The product is not publicly available
- Independent vendor
- Audited technology
- Legal solution to protect your communication

CryptTalk

CryptTalk is a new generation communication encryption solution, which hinders the interception of users' conversations by applying the most advanced encryption and authentication technologies.

When using CryptTalk, you can be sure that your calls cannot be decrypted - your communication will not be accessible to third parties.

Maximum security

CryptTalk uses the most secure encryption technologies which are recommended by prominent IT security experts and trusted by military services worldwide.

The asymmetric encryption and digital signature for the communication channel combined with the most reliable encryption algorithms guarantees that the encrypted information can be decoded and understood only by the authorized communicating parties.

Even if the communication is intercepted and an attempt is made by 3rd parties to decode it, the data packets cannot be decoded.

No backdoor

CryptTalk is created so that calls cannot be decoded even if the interceptor had access to the source code of the application and has access to the central servers of the service.

Voice data is transmitted directly between the end users, without any intermediary service providers.

Carrier independent

Keys used in CryptTalk as well as the voice transfer between parties are carried out directly, using an encrypted channel. This ensures comprehensive independence from carriers or networks and the encryption cannot be perceived by the network provider.

The service can be used on traditional as well as on mobile internet networks.

Worldwide coverage

CryptTalk provides worldwide service coverage - subscribers with proper internet access can use our services anywhere in the world.

ARENIM TECHNOLOGIES

CryptTalk

"There are no built-in backdoors or universal keys in CryptTalk.

The solution is designed and implemented so that calls cannot be decoded even when the interceptor has the source code of the product.

Calls using CryptTalk are guaranteed to be indecipherable even by the developers of the solution.

In addition to guaranteeing the fact that no calls made with CryptTalk can be decrypted, the software can provide a legal and easy-to-use solution to protect private and business communication."

The CryptTalk Developer Team

Arenim Technologies AB.

Stureplan 4c, 4th floor
11435 Stockholm
Sweden

sales@arenim.com

+46 812 410 590

www.crypttalk.com

Limited and closed distribution

CryptTalk is not available publicly – this increases security. For distribution details please consult your sales contact.

Closed network

The central telephone servers of the service can be deployed in tandem with the company's internal network if requested, or you can use the hosted service provided by CryptTalk. The CryptTalk server environment is strictly guarded and monitored, and it guaranties high availability.

Multiple platform

The solution is currently available for devices running Apple's iOS. If requested the technology can be ported to any desktop or mobile platform.

Why CryptTalk?

- It is guaranteed that calls made by using CryptTalk cannot be decrypted
- Calls are not put through a central server
- The communication cannot be deciphered - even when the interceptor has the source code
- Servers used by the service can be deployed within an isolated corporate environment where it is impossible for vendors to gain access
- Unlimited free worldwide secure encrypted phone calls and instant messages over WiFi and 3G networks without additional per minute costs
- Built on the most secure algorithms
- Does not depend on the network service provider
- Encryption cannot be perceived by the network service provider
- This product is distributed for a closed group of users and not available publicly
- Legal solution to protect private and business communication