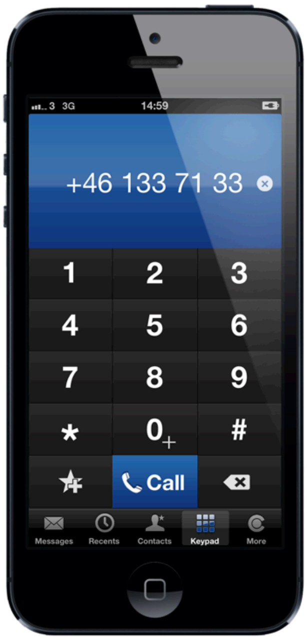
Cryptify Call

voice and messaging encryption for Smartphones

Easy exchange of sensitive information

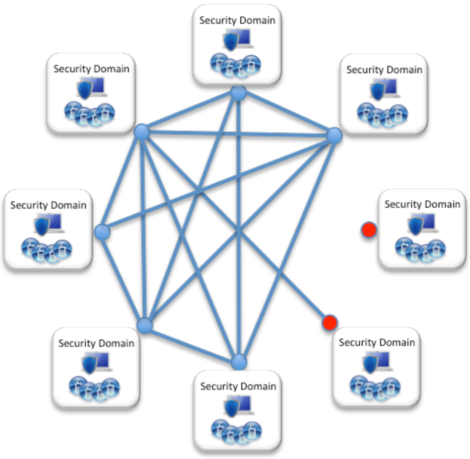
For most organizations wiretapping of key individuals would cause severe damage.

Using Cryptify Call is as simple as making an ordinary phone call / SMS. As it is running on your Smartphone you can be sure to always have a secure alternative available that you know how to use.



The comprehensive security is based on well-proven standard algorithms and protocols such as MIKEY-SAKKE for key exchange and Secure Real-time Transport Protocol (SRTP) with 128-bit Advanced Encryption Standard (AES) for media encryption.

The solution offers an intuitive, easy-to-use, management system that gives the organization absolute and exclusive control of all key material in their, so called, Security Domain. Subject to authorization users can communicate between Security Domains.



Compared with conventional encryption solutions associated with costly and complex IT projects, and in many cases dedicated encryption terminals, Cryptify Call provides a cost effective, assured, solution using standardized communication technology and modern cryptography.

Certified Product

Foundation
VOIPC33470913

Securing Communication

FIPS VALIDATED 140-2 TM

Values and Benefits

The Cryptify Call solution provides end-to-end encryption and authentication communicating over existing mobile broadband or Wi-Fi networks

Being able to utilize Wi-Fi networks in addition to mobile broadband networks does not only provide extra resilience of the service availability, but also a cost efficient alternative when traveling abroad.

The architecture is designed to completely keep security related information apart from other information. This enables each organization to have full control of all security related information, while at the same time being able to share parts of the infrastructure with other organizations.

To enable vendor interoperability Cryptify Call is based on open standards and protocols.

Technology

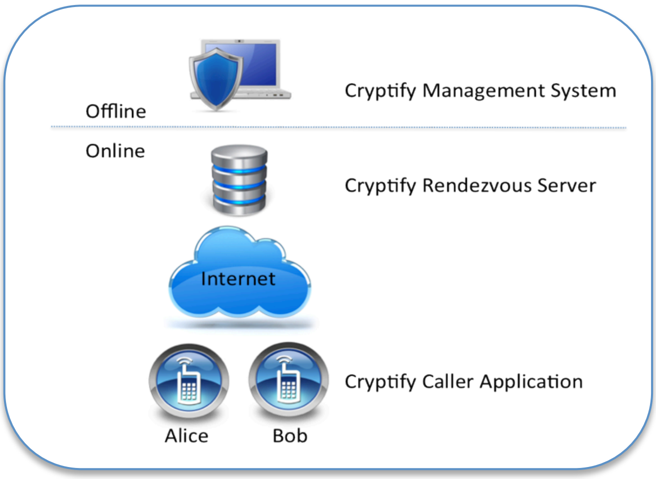
The solution consists of:

- Cryptify Caller Application for Smartphones
- Cryptify Management Server, handling all cryptographic keys for the Security Domain
- Cryptify Rendezvous Server, handling IP telephony functions in the Open Domain for non-sensitive data.

The Cryptify Management Server operates off-line, i.e. is not connected to any network, and hence is completely isolated from Internet threats.

By providing each user with a set of keys, MIKEY-SAKKE algorithms enables an unlimited number of users to create an encrypted and authenticated relation to any user without using any online key server.

The Cryptify Management Server prints an initiation letter to each user containing the users keys. The data is encoded into a QR-code and scanned by the Cryptify Caller Application in order to be armed with the users keys. Once armed, the user can make encrypted calls.


Offline
Cryptify Management System
Online
Cryptify Rendezvous Server
Internet
Cryptify Caller Application
Alice
Bob

Technical Specification

- Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY-SAKKE)
  IETF RFC 3830, 6508, 6509
- Eliptic Curve-based Certificateless Signatures for Identiy-based encryption (ECCSI)
  IETF RFC 6507
- Advanced Encryption Standard Galois/Counter Mode (AES-GCM) 128 bit
  FIPS-197
- Secure Real-time Transport Protocol (SRTP)
  IETF RFC 3711

Securing Communication