CRYPTIFY CALL

CERTIFIED ENCRYPTION OF VOICE AND MESSAGING

PROTECTING COMMUNICATION SINCE 2013

For most organisations, wiretapping of key individuals would cause severe damage.

Using Cryptify Call is as simple as making an ordinary phone call or sending messages. As it runs on your Smartphone, you always have a secure alternative available that you know how to use.

The security is based on well proven, state-of-the-art cryptography such as MIKEY-SAKKE for key exchange and Advanced Encryption Standard (AES) for media protection.

The solution offers an intuitive, easy-to-use, management system that gives the organisation absolute and exclusive control of all key material in their, so called, Security Domain.

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

UK OFFICIAL

CESG Certified Product

Foundation Grade
VOIPC45465459

NATO RESTRICTED

NCI AGENCY

---

cryptify
Securing Communication

AEP

Ultra ELECTRONICS

VALUES AND BENEFITS

The Cryptify Call solution provides end-to-end encrypted and authenticated voice and messaging communication over existing mobile broadband or Wi-Fi networks.

Being able to utilise 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 organisation to have full control of all security related information, while at the same time being able to share parts of the infrastructure with other organisations.

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.

TECHNICAL SPECIFICATION

- SAKAI-KASAHARA KEY ENCRYPTION IN MULTIMEDIA INTERNET KEYING (MIKEY-SAKKE) IETF RFC 3830, 6508, 6509
- ELLIPTIC CURVE-BASED CERTIFICATELESS SIGNATURES FOR IDENTIFY-BASED ENCRYPTION (ECCSI) IETF RFC 6507
- ADVANCED ENCRYPTION STANDARD GALOIS/COUNTER MODE (AES-GCM) FIPS-197
- SECURE REAL-TIME TRANSPORT PROTOCOL (SRTP) IETF RFC 3711

Ultra ELECTRONICS

making a difference

cryptify
Securing Communication

Ultra Electronics
AEP
419 Bridport Rd,
Greenford,
Middlesex UB6 8UA
Main Switchboard: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com

Cryptify
Södra Torggatan 6,
434 30 Kungsbacka,
Sweden,
Email: info@cryptify.com
www.cryptify.com