White Paper

11 April 2016

Introduction

This white paper provides a technical description of TextoCrypt's end-to-end encryption features. For a general description of the application, please visit Google Play or www.cyberens.eu/solutions.

TextoCrypt v1.0:

- allows users to exchange short text messages between each other using mobile networks;
- encrypts messages end-to-end for users having installed the application;
- sends messages in the clear to non TextoCrypt users;
- does not replace a standard SMS application;
- does not perform any statistics on what users do;
- does not send any other information in the background either than encrypted Daily Keys;
- does not need any other service or specific server to operate either than a cellular network and the SMS protocol.

This document gives an overview of the cryptographic services that are used in TextoCrypt.

Terms

Asymmetric Key Types

- Identity Key Pair– A one year Curve 255-19 key pair, generated at installation time.

Symmetric Key Types

- Daily Key– A 32-byte value.

Application installation

At installation time, TextoCrypt generates the user Identity Key, and sets its validity to one year. The public part of the Identity Key is stored in a self-signed certificate containing a unique Id, a name, a phone number and an expiration date. The certificate can then be sent by the user only to any other user. At no time does TextoCrypt send a public or private key to a server or any user data.

Sending Short Messages

To communicate with another TextoCrypt user, a user first needs to send her/his certificate to this other user. This is done by TextoCrypt using the SMS protocol under the user's control. The certificate is possibly split into several messages.

Then to communicate securely:

1. The sender selects a recipient in the contact list and types a message.
2. The sender then hits the "send" button.

   Case 1) The recipient has already sent her/his TextoCrypt **certificate**:

   Option a) The **Daily Key** is less than 24 hours old: TextoCrypt encrypts the text and sends the encrypted text message to the recipient;

   Option b) There is no **Daily Key** or the **Daily Key** is more than 24 hours old: TextoCrypt generates a new random Secret Key and sends it encrypted to the recipient using the SMS.

   Case 2) The recipient is not a TextoCrypt user, the text message is sent in the clear.

The encrypted text message (ETM) is converted in a printable string before being sent to prevent non printable characters from being interpreted as control characters or from being stripped out. An ETM uses more than twice as many characters as a text message in the clear because of the extra characters needed for the initialization vector used by the AES and some padding to align the overall payload on a multiple of 16 bytes before encryption.

Receiving Short Messages

Several types of short messages can be received by a user with TextoCrypt: certificates, secret keys, standard text messages (STM). All TextoCrypt generated messages are prefixed with a sequence looking like [xxx…xxx] and are visible in any standard SMS application.

Certificates: are not displayed in any discussion thread.

Secret Keys: are encrypted and wrapped using ECIES and are not displayed in TextoCrypt.

STMs: are decrypted then displayed in a TextoCrypt discussion thread.

With a standard application, a STM will look like [xxx…xxx]ABCDEF0123456789. Information in […] indicates the type of message (certificate, key, STM) and provides a sequence number used to reorder the initial text when the full cryptogram exceeds 160 characters, thus forcing the sending SMS module to split it into several chunks.

Cryptography

TextoCrypt uses the following algorithms and modes:

- The Advanced Encryption Standard (AES) with 256 bit keys in the Cipher Block Chaining (CBC) mode;

- The Password-Based Key Derivation Function version 2 (PBKDF2);
- The Secure Hash Algorithm version 2 (SHA2) with a 256 bit hash size;
- The Elliptic Curve Integrated Encryption Scheme (ECIES) with curve “255-19” with SHA-256 and AES-MAC-128.

The pseudo-random function is provided by the use of /dev/random on Android for all cryptographic variables including initialization vectors. Each secret key is randomly generated and has a cryptoperiod of 24 hours.

Smartphones do not generally provide high computing power compared to standard PCs and key and hash sizes have been selected in order to provide a reasonable user experience on these platforms. The AES key size has been set to 256 and the SHA2 hash size to 256. As text messages usually have a short lifetime, this performance/security trade-off should be acceptable to the vast majority of users.

Messages stored on the smartphone are encrypted with the AES (CBC) using a 256 bit key. **Daily Keys** are stored in an encrypted file protected by a key derived from the user password with PBKDF2.

Verifying Keys

Keys can only be verified “manually”, i.e., by comparing them when two users meet.

In a future version, TextoCrypt will offer the possibility to display a public key in the form a QR code that can be scanned and compared from another TextoCrypt instance.

What is not addressed?

TextoCrypt has been designed to protect text messages using the SMS protocol. There is no TextoCrypt server either on mobile networks or on the Internet. Consequently, signal protection cannot be provided and the now famous “metadata” generated by each network connection (recipient name, address/number, time, duration, etc.) is not encrypted by TextoCrypt.

One-to-many messaging is not supported in version 1.0.

Also, the Multimedia Message Service (MMS) is not supported in version 1.0.

Conclusion

Messages between TextoCrypt users are protected with end-to-end encryption that is deemed strong enough for text messages. Neither third parties nor Cyberens can read text messages encrypted with TextoCrypt. This can only be done by the sender and the recipient.