TASSTA

# TASSTA

## Security Overview


**SIMPLY PROFESSIONAL**

## Contact

**Novatek DMI Inc**
2211 Rue Metcalfe, Suite 110
Vaudreuil- Dorion QC J7V9H3

**Contact:**
Phone: +1 514 862 6581
Toll Free: +1 844 298 8833

**Web / Email:**
www.tasssta.ca
support@novatekint.com

v 01

END-TO-END ENCRYPTION SECURITY

## Introduction

This document provides an explanation of TASSTA uses general security technics including end-to-end encryption system.

## Security aspects

TASSTA system managing its own security aspects, such as authorization, authentication of user or device and protection of signaling and traffic information. End to end encrypted material to pass between users involved in it.

## Threats

This clause details some of the threats:

- Eavesdropping.
- Traffic analysis.
- Manipulation/insertion.
- Extraction of security information.
- Replay.

## Security measures

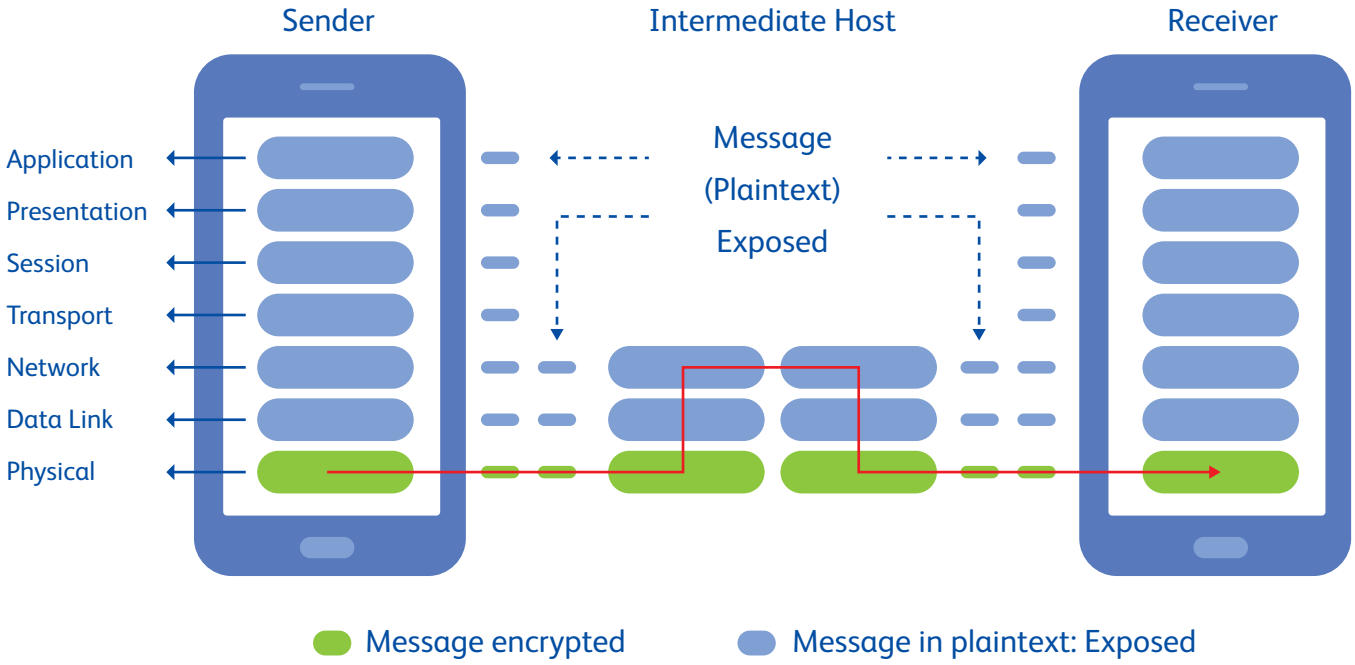
- User authorization.
- User authentication.
- Signaling protection.
- Traffic protection.

## Authentication and Authorization

TASSTA uses authentication is the technique of verifying the identity of a user, process, or device. Confidentiality is defined as keeping data unseen by others through preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

## Transport Layer Encryption

Data is encrypted just before the system places them on the physical communications link and decryption occurs just as the communication arrives at and enters the receiving computer: encryption occurs at layer 1 or 2 of the ISO OSI model.




In TASSTA system communication packets are encrypted once transferred. Based on transport layer TCP or UDP depends on type of it, if tunneled in TCP using the TLS that encrypts the whole signaling and if UDP media it may be applied AES-GCM mode encryption. The AES GCM algorithm implementation is used for traffic encryption.

Server sends a packet to the client with an initial data setup, which contains the cryptographic information for the encryption.

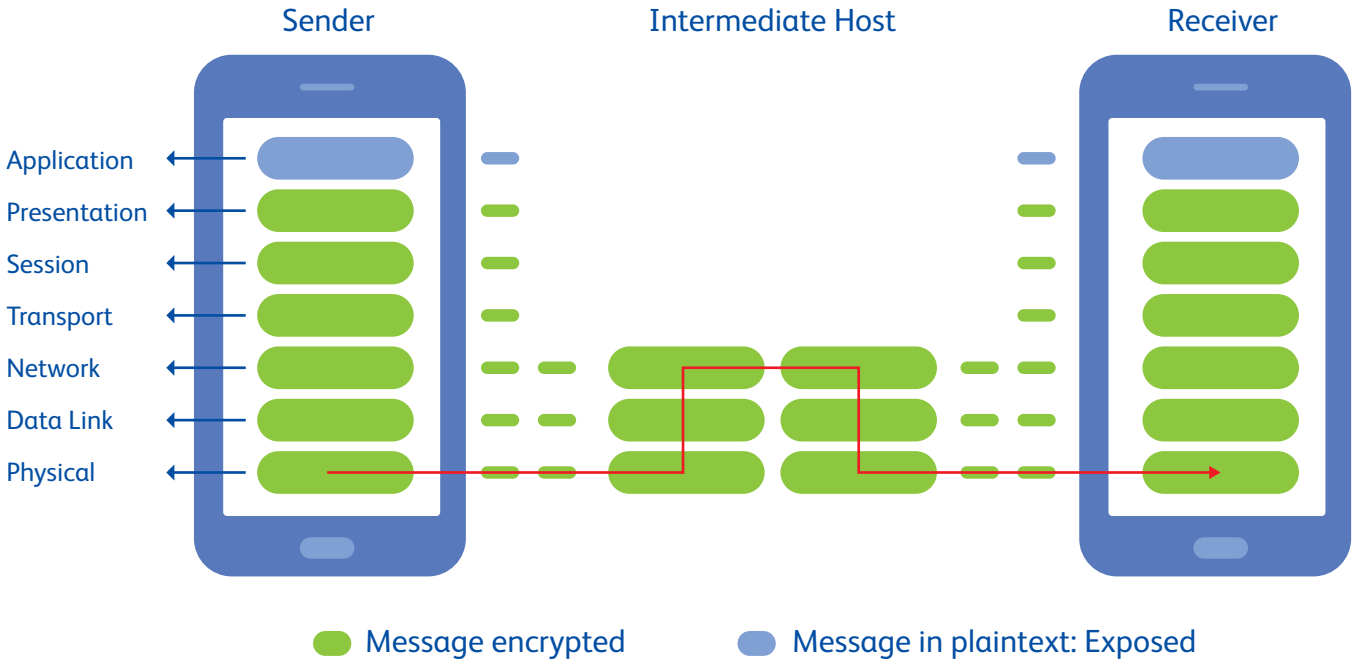
To communicate with another user, a TASSTA client needs to establish an encrypted connection. Once a connection has been established, clients exchange packets that are protected with a TLS using 256-bit AES-SHA. Transport Layer Security (TLS) is a protocol for the encryption of network data.

## E2E Encryption

There are two goals associated with E2EE security:

- The solution does not affect security for any users of either system that are not involved in interworking with the system.
- The solution maintains as high a level of security as possible for users that are involved in interworking communications.

Encryption is performed at the highest level (application layer). E2EE provides security for a message from one end of the transmission to the other. Since encryption precedes all the routing and transmission processing, the message is transmitted in encrypted form throughout the network. The message could go through potentially insecure intermediate nodes. The message is protected against disclosure while in transit.




On top of built-in signaling and voice traffic protection, TASSTA clients offer an additional security mechanism called end-to-end encryption (E2EE).

E2EE prevents potential eavesdroppers from being able to access the encrypted conversation even they are illegally intercepting the communication channel.

The E2EE in TASSTA provides a way of communication where only the communicating users with a right set of user's keys pair (encryption and decryption keys) can hear the voice messages. It is an additional level of protection to ensure that no third parties can intercept the voice data being communicated or stored without having the keys. The TASSTA users need the right key pair to be able to listen to the encrypted E2EE voice messages.

When creating E2EE call it is necessary to use both encryption and decryption keys. Only parties with the correct set of keys are able to listen to voice messages.

A user can also share a key to another user from the user list or from a map.

All E2EE calls can be played back from History only at presence of the appropriate key.

In case of use E2EE, each message is encrypted with the symmetric encryption algorithm (AES128) the secret is shared between two clients is provided by hand entered password code (from this password encryption key is calculated).

The key is generated with SHA1 algorithm from entered Key in dialog; the key is entered manually by the user and the client application is the only system component which is aware of the key; so no service component can decrypt the message.

## SUMMARY

Messages between users are protected with encryption, a voice could be applied for a level of encryption and additionally, the end-to-end-encryption protocol can be used so that third parties and Services cannot consume voice and records if applied and the content can only be decrypted by the trusted recipients, who know agreed keys.

# TASSTA

**SIMPLY PROFESSIONAL**

www.tassta.ca | support@novatekint.com.