



# [ClosedTalk]<sup>®</sup>

Secure Voice Communication

[ClosedTalk]<sup>®</sup> is a secure Voice over IP solution that enables talks to be made in total privacy. [ClosedTalk]<sup>®</sup> provides privacy, the confidence in the Identity of your talk partner and all other benefits of a VoIP solution. All data to establish a connection and the actual voice data are transmitted in an encrypted format. Unlike other VoIP solutions, [ClosedTalk]<sup>®</sup> protect the communication through:

- strong encryption technology,
- direct key exchange between the partners, and
- optional trustful authentication by digital certificates

## High Security & Ease of Use

Robust security features are combined with ease of use and optional hardware features. By using the built-in sound system of the computer, [ClosedTalk]<sup>®</sup> users communicate without the need of IP telephones. The solution incorporates top-end security technologies, such as ECC based Diffie-Hellman Key Generation Protocol to provide secure session keys and a strong 256 Bit AES encryption to secure the voice and the management data. Making internet calls using [ClosedTalk]<sup>®</sup> is easy as the caller only need the recipient's email address. [ClosedTalk]<sup>®</sup> does not need the old-fashioned telephone numbers. A gatekeeper service is provided by CE-Infosys to locate the public IP addresses of the communication partners on the Internet. Compared to a telephone communication, [ClosedTalk]<sup>®</sup> provides highest sound quality as you need it to identify the voice of a partner or to listen to music.

Diffie-Hellman  
Key  
Generation  
Protocol

## Management Commitment

The FREE version of [ClosedTalk]<sup>®</sup> will be kept free of charge for all of the future. We will sell hardware enhancements such as [ClosedTalk]<sup>®</sup> Handsets, approved Headsets, [ClosedTalk]<sup>®</sup> USB Handsets, e-Identity<sup>®</sup> Tokens and Smart Cards, digital certificates as well as private Gatekeepers. A [ClosedTalk]<sup>®</sup> version will be included in the CompuSec<sup>®</sup> Pocket. CompuSec<sup>®</sup> Pocket with [ClosedTalk]<sup>®</sup> is chargeable.

We also commit that [ClosedTalk]<sup>®</sup> will be further developed and enhanced with useful functions and features over time. We do not seek to make the most profit in the shortest time, but we want to win with [ClosedTalk]<sup>®</sup> those customers who prefer an independent and trustful security. We guarantee that we will provide fixes and corrections for the product if problems are found by our customers or by ourselves. We further promise that we are committed to an open policy. If security weaknesses should be found, we will inform the community and provide solutions.



## How to Build Trust?

It is not easy for a user to trust an IT product when private information may be send over the public Internet. To support you to build trust in our product, we at CE-Infosys will provide technical details of the security implementation. We will explain how the product works and why you can trust the product. We will publish White Papers explaining concepts and protocols. We will not publish the source code in detail due to our commercial obligations for our investments and skills, but we will answer questions that can help people to understand the security implementation.

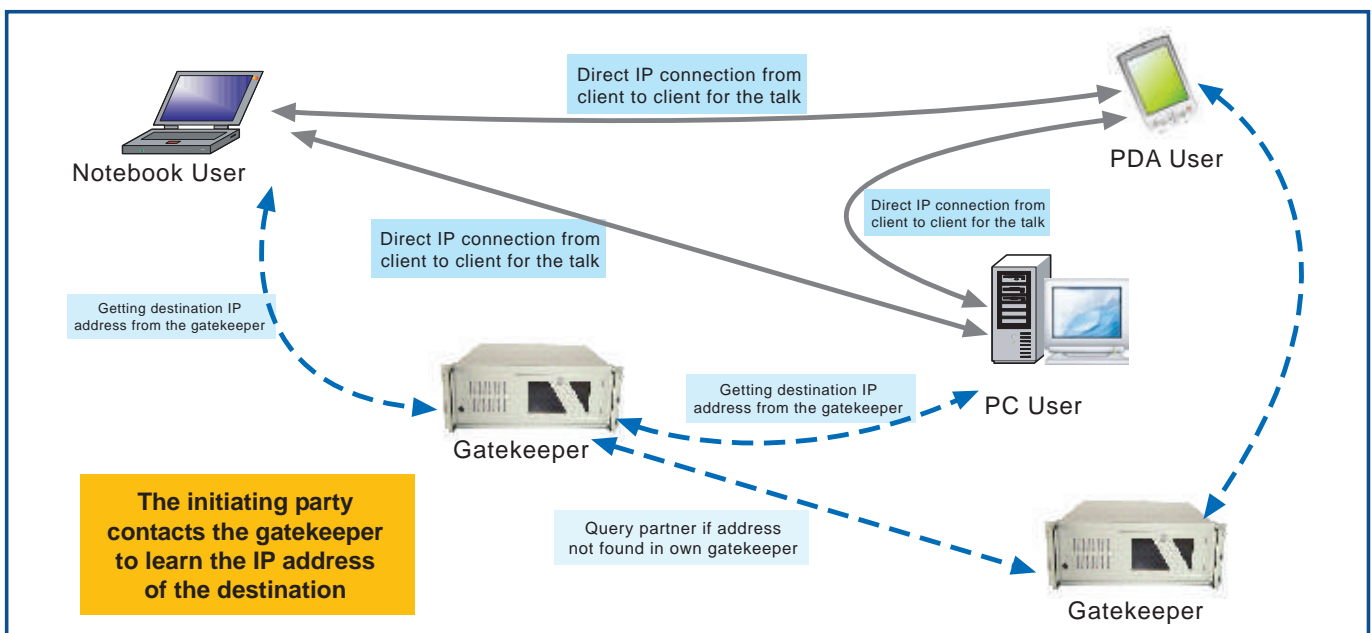


## A First Look At How [ClosedTalk]<sup>®</sup> Works

[ClosedTalk]<sup>®</sup> is for secure communication; therefore a connection to traditional phone systems is not included and not planned. At the gateway to a traditional phone system, the encrypted data would have to be decrypted. At that point, the privacy would be lost. Telephone numbers are not needed if you do not connect to traditional phone systems. The concept of building a connection using the e-mail address is not new, but is very useful because remembering an e-mail address is much easier than a long string of numbers. After the initial registration at the Gatekeeper, the e-mail address is erased in the Gatekeeper. When a [ClosedTalk]<sup>®</sup> Client is switched on, a hash value of the e-mail address is sent to the Gatekeeper together with the IP address of the user. This hashed value cannot be calculated backward into the e-mail address.

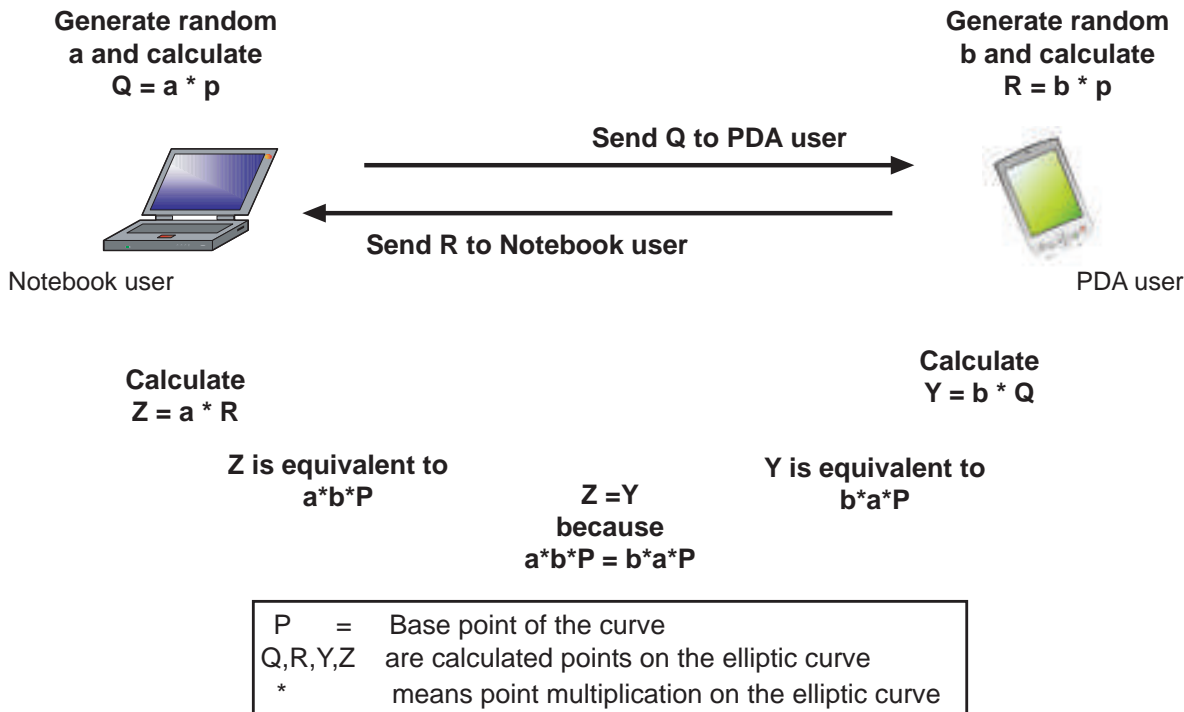
When the caller enters the email address of the communication partner, [ClosedTalk]<sup>®</sup> calculates the hash value of the other party and contacts the Gatekeeper. The Gatekeeper will locate the other party in its table of online clients and provide the IP address of the destination to the caller. A direct IP connection is then established between the two parties.

The communication to the Gatekeeper is encrypted using an ECC key generation protocol.

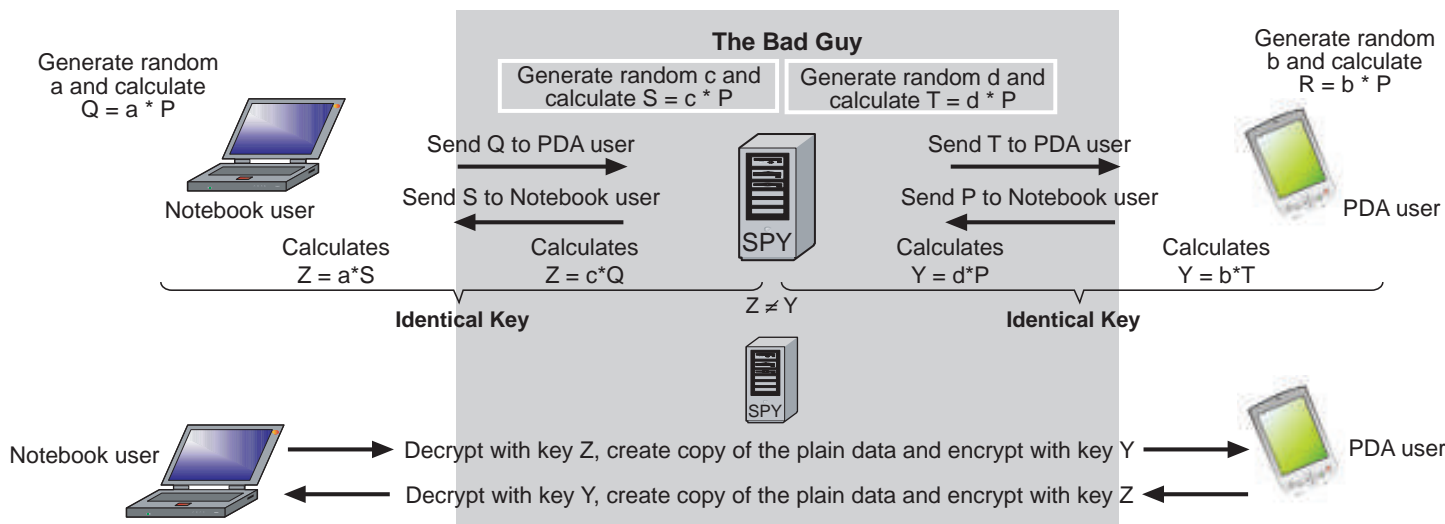


**How [ClosedTalk]<sup>®</sup> Secures the Voice Communication**

Conversations between the [ClosedTalk]<sup>®</sup> users are protected using an ECC based Diffie-Hellman Key Generation Protocol to provide secure session keys and a strong 256 Bit AES encryption to secure the voice data.

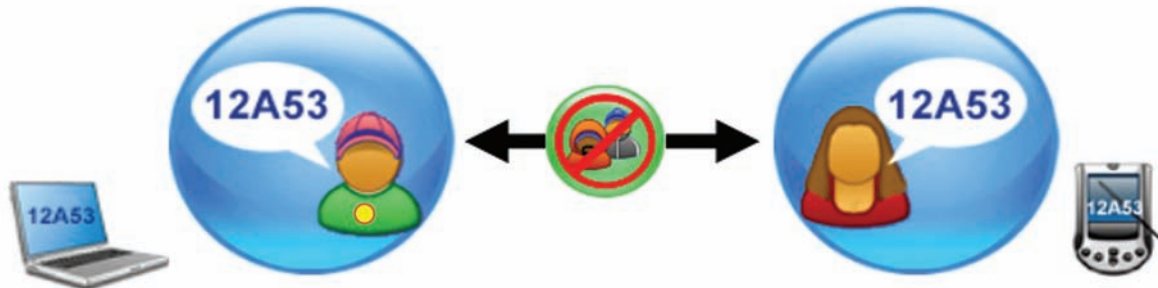


It is known that traditional VoIP communications can be easily intercepted. Interceptions happen when conversations fall vulnerable to a third-party's eavesdropping. Key exchange and voice content are intercepted, opened for retrieval, and sent back to the destination almost undetected. This form of interception is commonly known as the 'man in the middle' attack. The diagram shows how a 'man in the middle attack' works during the session key generation.



Whenever 'The Bad Guy' has its own keys shared with both the unsuspecting communication partners, the automatic decryption of their voice channel will be very easy and cannot be detected!

[ClosedTalk]® exposes such attacks by calculating a hash value of the generated session key and displays some byte of it as security code on both the callers' screens. This security code is like a checksum of the session keys. If an attack does take place, this 'checksum' will be different on both end-points of the communication as seen on the users' screens. The users can exchange these codes verbally to verify with each other. So long as the security codes are identical, there is no interception of the voice data.



**[ClosedTalk]® Total Solution**

The [ClosedTalk]® software is provided free as part of the FREE CompuSec® security suite. It is also included in all chargeable version of CompuSec® solutions. [ClosedTalk]® users can enhance their communication productivity further by opting for a total solution which includes easy-to-use handsets, private gatekeeper for business users and certificate support for a larger user base.



[ClosedTalk]® Handsets



[VoiceGate]® for companies

**System Requirements**

- Pentium 3 PC Notebook or Workstation
- Windows Vista, Windows XP and Windows 2000
- 20 MB Hard Disk Free Space
- Built-in Sound Card
- Network Connection
- Broadband Connection Speed of 45kbps (Upload and Download)



**CE-Infosys GmbH**  
 Am Kümmerling 45  
 D-55294 Bodenheim  
 Germany  
 Tel.: +49 (0) 6135 / 77 0  
 Fax: +49 (0) 6135 / 77 77  
 de.sales@ce-infosys.com

**CE-Infosys Pte Ltd**  
 31 International Business Park  
 #04-03A Creative Resource  
 Singapore 609921  
 Tel.: +65 6899 9392  
 Fax: +65 6899 9373  
 sg.sales@ce-infosys.com

**CE-Infosys FZ-LLC**  
 Dubai Internet City  
 Thuraya 2 Building Office 1007  
 PO Box 500434 Dubai U.A.E  
 Tel.: +971 4 369 7578  
 Fax: +971 4 369 7579  
 ae.sales@ce-infosys.com

CompuSec, e-Identity, [ClosedTalk] & [VoiceGate] are registered trademarks of CE-Infosys Pte Ltd in Singapore.

Reseller: