End to End Encryption

Author: Old Gocs Berlin, 2016

This is actually the classical method of secure transmission of information between two Partners.

What do you mean, end to end encryption?

Both partners have the same encryption or cipher.
Both partners have key agents.
The key agents are organized in pairs.
That is, a pair of keys means consists of two identical keys.
Each partner receives a copy. The services, the association has naturalized that the Is used to encrypt or encrypt copies. 1 The specimen 2 is replaced by the receiver the encrypted or encrypted message.
To ensure that also the receiving partner can send information, has he about key copies with the number 1 and the receiving partner the copy. 2
Bidirectional information History:
partner 1
partner 2
Key xyz 1 copy ---------- ◊ Key xyz 2 copy
information direction
Key abc 2. copy ⇓ ---------- key abc 1 copy
This is the basic principle of the key organization (key distribution)
One could conclude now, a key pair would be sufficient for a safe Information link.
But this is a serious mistake. They comply with this procedure, the "Deadly Sins Cryptology ".

A key pair may be used only once.
Violations of this type are known from history. (VENONA etc.)
You need a pair of keys for each transmission of information.
Hence the conclusion that you according to the number of information transfers must use the same number of key pairs.

Forum for Information Security [www.gocs.de ... eu ... info .... com.de]

At this used for your information transmission key, of course, certain asked cryptologic requirements.

On the cryptologic requirements will not be discussed at this point.
For additional requirements in the "Forum for Information Security".
At this point, only a simple question of how change partners your keys from?
Should you, because it is so simple, the key means through the same transmission channel as the
To transmit information.

Why do you want then encrypt or scramble your information!
In today's world, the virtual space is needed for many applications and abused.

Thus, the age-old question, how can the key agent gives to the partner sent?

Solutions :
(1) key agents in the same way as the encrypted or scrambled
Received information?
(2) key means are received on another, open carry Tung channel?
(3) key agents through a secure transmission path (courier, diplomatic bag, or other forms) received?
Whichever method would you choose?
The method (1) is likely in the virtual world the most common method to be. Simple - Fast - Free - unsafe because key generation erfolgt.- in the virtual world
a "third party" knows the key and thus the information to be protected
Key generation: insecure
Key Distribution: unsure
compromised keys

The method (2) is characterized in that only the key distribution in the virtual world,
takes place.
Key generation: relatively safe, depending on local conditions
Key Distribution: unsure

Key is compromised.

The method (3) is the most secure version of key distribution. But, in the past that losses recorded. But there was also a case that by an authorized person
Were passed key means to a third party (Case Walker, United States).
Key generation: sure
Key Distribution: safe

Key not compromised.

In addition, there are also other methods, a substantial increase in the Implement key security on the open transmission channels of the virtual world.

The key general

Actually, the key is a sequence of elements. Simple shapes, but also very safe were, Numbers in the range 0 ... 9, or even letters in the range of A .... Z and a ... z. With the

Development of computers has been expanded this range of values from 0 to CHR CHR 255th [CHR =

Character = characters].

What cryptologic quality of key you use has, should not at this point

Be the subject of consideration.