MAXA-Key-Exchanger (MKE)

Document Revision EN V 1.1

The smart & simple way to achieve
A Secure Key Exchange

Preamble

Throughout history, security and self-protection has always been among everyone's basic requirements and rights. What has changed is society itself - culturally, politically, legally and technically. The vulnerability of today's IT systems to modern attack methods has several similarities to the Cold War with both competing offensive and defensive technologies.

Why do we need a key exchange?

Networking PCs means a much greater danger of illegal access to data. The type of networking is actually irrelevant - every data transfer between sender and receiver means that there will be security weaknesses.

The size of the danger posed to data, along with its administration, means that the only reasonable solution is for users to secure their data themselves. To do so, a secure pass phrase is needed that is based on a symmetrical key.

The problem with symmetrical keys is that both parties need to establish a shared secret or passphrase. That passphrase must not be published or forwarded in any insecure way: by email, instant messaging or phone. In most cases, both parties do not have direct physical contact, and/or they do not have some type of secure channel available to them. MAXA-Key-Exchanger solves this problem in a simple, secure and easy to use way.

The Diffie-Hellman key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other, to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

MAXA-Key-Exchanger creates a shared secret or passphrase (*randomly out of all printable ASCII characters*). This passphrase should be considered as the first step in securely encrypting data before it leaves your PC.

Generate unique passphrases for individuals, clients, and more. Utilizing a key like this with an encryption tool, such as MAXA-Crypt, allows users to be able to send encrypted data, without fear. MAXA-Crypt's default is to use 256 bit encryption with AES (*which is considered as absolutely safe*).

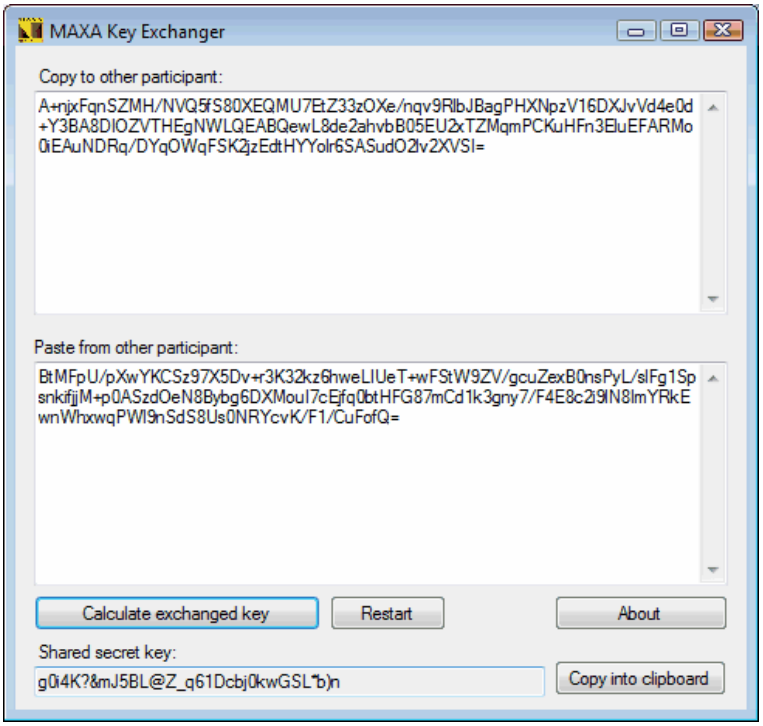
How does the key exchange work?

Both parties must download and run MAXA-Key-Exchanger on each of their computers. MKE randomly generates special numbers[1] which need to be exchanged. Simply copy the block of text and numbers and paste it into an email or instant message. Yes, we know, email is as insecure as it comes, but it is important to understand that this data exchange does not need to be kept confidential. However, you must be certain that you are actually communicating with the person you think you are (e.g. recognize the other person form its voice), and that the numbers are not modified by someone in the middle.

Each person runs the application on their respective machine and sends the data in the first box to the other person.

Once each box is filled, simply press "Calculate" and your passphrase is now completed.

[1] A very large prime number together with one of its primitive roots. The Diffie-Hellman Key exchange is based on the mathematical asymmetry of calculating the discrete logarithm.



Minimum hardware and software requirements for MAXA-Key-Exchanger

Hardware: Pentium II, 266MHz, VGA, keyboard & mouse (*or equivalent*)

Software: Windows Vista, 2008 Server, 7 or newer. Needs Microsoft's ".NET Framework 3.5".

Note:

- Errors & Omissions Excepted
- This paper reflects the technical situation as at May 2009
- MAXA and the text and image references are Registered Trademarks of MAXA Research Int'l, Inc.
- Any other trademarks mentioned are the property of the registered owner.
- MAXA-Key-Exchanger STD is a full version and is considered freeware
- A branded version (*in your company's corporate design*) is available for a small fee

➢ E N D