

MAXA-Key-Exchanger (MKE)

Dokumentrevision DE V 1.1



Die intelligente und simple Art des sicheren Schlüsselaustausches

Vorwort

Der Schutz und die Sicherheit gehört zu den Grundrechten- und Bedürfnissen des Menschen. Daran hat sich in der Geschichte nie etwas geändert. Verändert hat sich allerdings der zugrunde liegende gesellschaftliche Hintergrund durch kulturelle, politische, juristische und technische Anpassung.

Die Verletzlichkeit heutiger Datenverarbeitung durch modernste Methoden, hat eine ähnliche Situation wie im „Kalten Krieg“ geschaffen. Ein Wettrüsten mit geeigneten Mitteln von Angriff und Verteidigung.

Wozu benötigt man einen Schlüsselaustausch?

In Netzwerken zu arbeiten bedeutet einer wesentlich höheren Gefahr, illegalen Angriffen ausgesetzt zu sein. Die Art und Weise der Netzwerkverbindung ist dabei unbedeutend. Jeglicher Datenaustausch zwischen Sender und Empfänger stellt dabei eine Schwachstelle dar.

Um die Gefahr zu reduzieren, liegt es primär in der Verantwortung der beiden Parteien für eine entsprechende Absicherung zu sorgen. Eine Verschlüsselung auf der Basis symmetrischer Verfahren ist hier zu empfehlen.

Eine Eigenheit symmetrischer Schlüssel ist, dass beide Seiten sich auf eine gemeinsame Passphrase (*längeres Passwort*) verständigen müssen. In den meisten Fällen besteht keine unmittelbare Möglichkeit der sicheren Kommunikation (z.B. *direkter physikalischer Kontakt*).

MAXA-Key-Exchanger löst dieses Problem auf elegante Weise, einfach, sicher und schnell auf der Basis des Diffie-Hellman Verfahrens. Hierbei handelt es sich um ein Protokoll, welches den beiden Parteien ermöglicht, ohne besondere Vorkenntnisse einen gemeinsamen sicheren Schlüssel zu erstellen um diesen dann auf einem „unsicheren Kanal“ auszutauschen. Dieser Schlüssel bzw. Passphrase kann dann für die symmetrische Verschlüsselung genutzt werden.

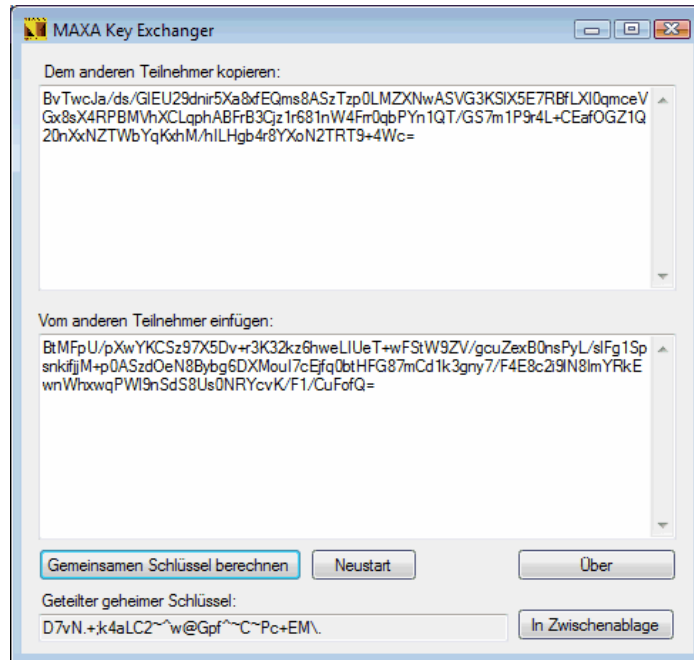
MAXA-Key-Exchanger kreiert eine gemeinsame Passphrase mit einer Verschlüsselungstiefe von 128 Bit (*auf Zufallsbasis aus dem Bereich aller darstellbaren ASCII-Zeichen*). Dies sollte als „erster Schritt“ einer sicheren Datenverschlüsselung betrachtet werden.

Die Erstellung einer „einmaligen und extrem sicheren Passphrase“ kann mit dem Tool MAXA-Crypt oder MAXA-Crypt-Mobile vorgenommen werden. Es erlaubt dem Nutzer auf der Basis von 256 Bit Verschlüsselungstiefe mit AES (*gilt derzeit als absolut sicher*) zu verschlüsseln.

Wie funktioniert der Schlüsselaustausch?

Beide Parteien starten die Applikation MAXA-Key-Exchanger auf ihrem jeweiligen Rechner. MAXA-Key-Exchanger erstellt dabei eine zufällige Zeichenfolge, die zwischen den Parteien ausgetauscht werden muss, indem dieser alphanumerische Block durch Copy & Paste per Email, Sofortnachricht oder sonstigem Medium übertragen wird. Dabei dürfen diese Texte auch über als **nicht abhörsicher eingestufte Übertragungswege** ausgetauscht werden, ohne die Sicherheit des Ergebnisschlüssels zu kompromittieren. Sie müssen jedoch sicherstellen, dass Sie sich tatsächlich direkt mit der gewollten Person austauschen (z.B. erkennen diese an der Stimme), ohne dass eine andere Partei in die Möglichkeit hätte, die übertragenen Zeichenfolgen zu ändern.

Wenn beide Parteien die Textfelder im Programm mit dem übertragenen Inhalt gefüllt haben, muss nur noch die Schaltfläche „Gemeinsamen Schlüssel berechnen“ gedrückt werden und die Passphrase ist erstellt.



Welche Hard- und Softwarevoraussetzung benötigt MAXA-Key-Exchanger?

Minimum Pentium II/266MHz, VGA, Tastatur und Maus oder vergleichbar.
Windows VISTA, Server 2008, 7 oder neuer. Microsoft .NET Framework v3.5, dieses kann
kostenlos von Microsoft heruntergeladen werden.

Hinweis:

- Irrtum und Änderungen vorbehalten.
- Der technische Stand ist Mai 2009
- MAXA und die Wort/Bildmarke sind eingetragene Marken von MAXA Research Int'l Inc.
- Weitere fremd erwähnte Wort/Bildmarken sind eingetragene Marken ihrer rechtmäßigen Eigentümer.
- Eine Branding-Version (*mit Werbehinweis Ihrer Firma*) ist gegen Gebühr möglich.
- MAXA-Key-Exchanger STD (standard) ist eine Vollversion und wird als kostenlose Freeware angeboten

➤ ENDE