Was ist ein symmetrisches Verschlüsselungsverfahren?

Um das Abgreifen der versendeten Nachrichten und Daten durch einen Dritten zu verhindern, werden im Allgemeinen kryptographische Verfahren angewendet.

Bei symmetrischen Verschlüsselungsverfahren gibt es genau einen einzigen

Schlüssel, den so genannten Secret Key. Dieser Schlüssel dient sowohl zur Verschlüsselung der Nachricht als auch zur Entschlüsselung.

D.h. sowohl der Sender, wie auch der Empfänger benötigen denselben Schlüssel. Zu diesem Zweck

müssen beide Parteien vorab diesen Schlüssel vereinbart bzw. ausgetauscht haben.

Beispielsweise per Mail/Telefon oder per Hand. Die größte Problematik der

symmetrischen Verfahren besteht jedoch beim unsicheren Schlüsselaustausch.

Eine verschlüsselte Nachricht kann zwar gefahrlos verschickt werden, nicht aber der Schlüssel.

Deswegen ist es bei der symmetrischen Verschlüsselung sehr wichtig, dass der

Schlüssel auf einem sicheren Übertragungsweg an den Empfänger weitervermittelt wird.

Vorteile:

- Einfaches Schlüsselmanagement, da nur ein Schlüssel für Ent- und Verschlüsselung notwendig ist
- Verschlüsselung beliebig großer Datenmengen ist möglich

Nachteile:

- Unsicherer Schlüsselaustausch
- Der Schlüssel muss geheim gehalten werden und darf nicht in unbefugte Hände gelangen

FTAPI verwendet zur Vermeidung der Nachteile eine Kombination aus symmetrischen und asymmetrischen Verschlüsselungsverfahren.

Weitere Informationen finden Sie hier:
Verschlüsselungsmethoden

zurück