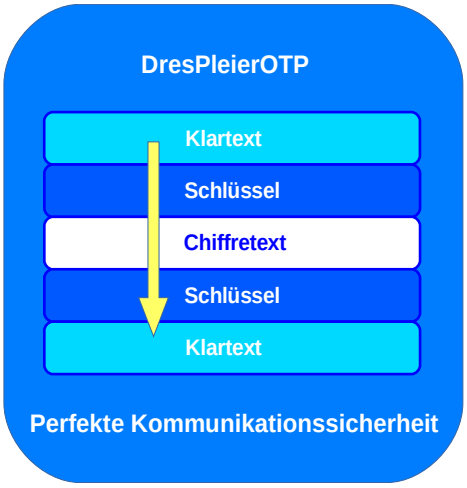
DresPleierOTP - Perfekte Kommunikationssicherheit durch Einmalschlüssel

DresPleier GmbH, 84149 Velden, Deutschland

One-Time-Pad (OTP), deutsch Einmal-Block bzw. Einmalschlüssel, gibt es schon sehr lange und ist dementsprechend genau untersucht. Es wurde 1882 von Frank Miller vorgeschlagen, 1890 durch Gilber Vernam patentiert und ca. 1920 in Deutschland umgesetzt als i-Wurm (individueller Wurm). Die Grundidee ist, Einmalschlüssel, so lange wie die Nachricht und mittels einem echten Zufall erstellt, zu verwenden, um Nachrichten beim Sender zu ver- und beim Empfänger zu entschlüsseln. OTP gilt als informationstheoretisch absolut sicher und unknackbar, auch in der Zukunft nicht, wie ca. 1940 von Claude Shannon bewiesen wurde. Diese Beweisbarkeit ist der große Vorteil und wird in der Wissenschaft als perfekte Sicherheit bezeichnet. Dieser Beweis steht im Gegensatz zu anderen Verfahren, wo man lediglich annimmt, daß diese stark und sicher sind. Zudem ist das Verfahren OTP sehr einfach anzuwenden.



DresPleierOTP ist eine Lösung zur Realisierung einer Verschlüsselung via OTP mit allem, was dazugehört. Für beste Sicherheit wird ein Offline-System genutzt. Dort werden Nachrichten erstellt und verschlüsselt, dann über ein beliebiges Medium zum Empfänger übertragen. Dieser empfängt die geschützte Nachricht, transferiert sie zu seinem Offline-System und entschlüsselt sie dort. Die Schlüssel, das Programm, ein sicheres Nutzungskonzept, ggf. weiteres wie ein Offline-Rechner kommen von der DresPleier GmbH.

Zu OTP werden oft drei Gegenargumente genannt, die nicht wirklich greifen: Erstens OTP sei nicht praktikabel, da man z.B. zum Verschlüsseln einer Festplatte eine weitere Festplatte benötigt. Wird das Verfahren jedoch geeignet genutzt, konkret für den Schutz von Kommunikation, sind die dafür nötigen Schlüsselgrößen gut handhabbar. Zweitens die Schlüsselverteilung wäre zu aufwändig, nicht machbar. Für eine perfekte Kommunikationssicherheit ist jedoch ein passender Aufwand für einen sicheren Schlüsselaustausch akzeptabel. Zudem hängt der Aufwand vom konkreten Nutzerkreis ab. Ist dieser lokal und weniger veränderlich, so ist es problemlos machbar. Die Idee ist, die Schlüssel vorab in Ruhe zu einem gewählten Zeitpunkt sicher zu verteilen, danach jederzeit sicher kommunizieren zu können. Und drittens OTP wäre nicht notwendig, denn es gäbe doch andere, etablierte und starke Verfahren und diese sind noch 20 Jahre lang sicher. Dies ist aber nicht bewiesen, sondern wird nur vermutet, sowohl die aktuelle, als auch die langjährige Unknackbarkeit. Bei OTP dagegen gibt es einen Beweis.

DresPleierOTP ist eine Lösung zum Schutz der Vertraulichkeit der Kommunikation auf höchstem Niveau. Es kann breit genutzt werden von Firmen, Behörden, Privatpersonen, Vereinen, Verbänden usw. und ist insbesondere wertvoll zum Schutz von Geschäftsgeheimnissen und personenbezogenen Daten wie bei Anwälten, Ärzten, Steuerberatern usw. DresPleierOTP wird aus rechtlichen und abrechnungstechnischen Gründen nur innerhalb Deutschland und derzeit aus Sicherheitsgründen nur für Debian-Linux-Systeme angeboten.

Firma: DresPleier GmbH ; **Geschäftsführer:** Dr. Christoph Pleier ; **Sitz und Registergericht:** Landshut HRB 6587 ; **USt-ID:** DE814347435
Anschrift: Vils 8, 84149 Velden ; **Telefon:** 08742/5870894 ; **Telefax:** 03222/4170655 ; **Mail:** info@DresPleier.de ; **Web:** www.DresPleier.de