Was ist Verschlüsselung & Keypairs – Grundlagen verständlich erklärt

Wenn du Dateien mit sensiblen Informationen – zum Beispiel personenbezogene Daten von Minderjährigen – sicher übermitteln oder speichern möchtest, reicht es nicht aus, sie einfach per E-Mail zu versenden oder in einem Ordner abzulegen. Verschlüsselung stellt sicher, dass nur die Person, für die eine Datei bestimmt ist, sie auch lesen kann.

Wie funktioniert Verschlüsselung?

Stell dir einen Briefkasten vor: Jeder kann einen Brief einwerfen – aber nur der Besitzer des Briefkastens hat den Schlüssel, um ihn zu öffnen. Genau so funktioniert asymmetrische Verschlüsselung.

Jede Person hat dabei zwei zusammengehörige Schlüssel:

Public Key (öffentlicher Schlüssel): Dieser Schlüssel kann und soll weitergegeben werden. Wer dir eine verschlüsselte Datei schicken möchte, verwendet deinen Public Key dafür. Mit einem fremden Public Key kann man Dateien verschlüsseln – aber nicht entschlüsseln.

Private Key (privater Schlüssel): Dieser Schlüssel bleibt ausschließlich bei dir und wird niemals weitergegeben. Nur mit dem Private Key kannst du Dateien entschlüsseln, die mit deinem Public Key verschlüsselt wurden.

Warum zwei Schlüssel?

Der entscheidende Vorteil: Du musst niemals einen geheimen Schlüssel übermitteln. Jemand, der dir eine verschlüsselte Datei schicken möchte, braucht nur deinen Public Key – den kannst du bedenkenlos öffentlich teilen. Dein Private Key verlässt dabei niemals dein Gerät.

Was ist GPG?

GPG (GNU Privacy Guard) ist ein weit verbreitetes, freies und etabliertes Programm zur Dateiverschlüsselung auf Basis dieses Verfahrens. Es gilt als sicher, ist gut dokumentiert und wird weltweit von Behörden, Organisationen und Sicherheitsexperten eingesetzt.

In diesem Kapitel verwenden wir GPG mit einer Schlüssellänge von **4096 Bit** – einem besonders hohen Sicherheitsstandard, der angesichts der Sensibilität der verarbeiteten Daten ausdrücklich empfohlen wird.

Wann sollte ich verschlüsseln?

- Bei der Übermittlung personenbezogener Daten – insbesondere von Minderjährigen
- Bei sensiblen organisatorischen Informationen
- Immer dann, wenn eine Datei über unsichere Kanäle wie E-Mail übertragen wird
- Bei der Langzeitarchivierung schützenswerter Daten

> **Wichtig:** Verschlüsselung schützt den Inhalt einer Datei – nicht die Tatsache, dass sie existiert. Sie ersetzt außerdem keine sichere Ablage und kein Zugriffskonzept, sondern ergänzt beides.

Revision #2
Created 2026-03-05 04:16:28 UTC by Christian Weiß
Updated 2026-03-05 04:19:25 UTC by Christian Weiß