Public Key Verfahren

Ein Schlüssel besteht aus einem privaten und einmal öffentlichen Teil. Der **private Schlüssel** wird **NIEMALS** weitergegeben. Der **öffentliche Schlüssel darf beliebig** (auch über unsichere Kanäle) weitergegeben werden.

1. Authentifizierung bei einem Server oder Dienst. Beim Server wird der öffentliche Schlüssel gespeichert. Der private Schlüssel bleibt beim Benutzer.
2. Mit dem privaten Schlüssel können Dateien unterschrieben werden (signiert). Der öffentliche Schlüssel kann zur Validierung (=Überprüfung der Signatur) genutzt werden.
3. Mit einem öffentlichen Schlüssel kann verschlüsselt werden. Der private Schlüssel dient zur Entschlüsselung der Daten.