

# Anleitung zum Austausch verschlüsselter Dokumente

## Inhalt

1.	Ver-und Entschlüsselung mit SigNotar.....	3
2.	Ver-und Entschlüsselung mit anderer Software.....	3

## 1. Ver- und Entschlüsselung mit SigNotar

Die Ver- und Entschlüsselung eines Dokumentes geschieht mit Hilfe zweier unterschiedlicher Schlüssel, die sich beide auf der Signaturkarte befinden. Der öffentliche Schlüssel kann ausgelesen und versendet werden, während der private Schlüssel die Karte nicht verlässt. Um mit einem Kommunikationspartner verschlüsselte Dokumente mit Hilfe von Signaturkarten auszutauschen benötigt der jeweilige Absender den öffentlichen Schlüssel des jeweiligen Empfängers.

Mit seinem nur auf der Signaturkarte vorhandenen privaten Schlüssel kann der Empfänger sodann das Dokument entschlüsseln. Ihren öffentlichen Schlüssel können Sie mit Hilfe von SigNotar speichern und Ihrem Kommunikationspartner sodann übermitteln. Klicken Sie hierzu in Hauptmaske von SigNotar auf die Schaltfläche „Signaturkarten/ Nutzer“ und in der Folgemaske auf die Schaltfläche „Zertifikate auslesen“. Sodann können Sie das angezeigte Verschlüsselungszertifikat, welches den öffentlichen Schlüssel beinhaltet, speichern.

## 2. Ver- und Entschlüsselung mit anderer Software

Sollte Ihnen SigNotar nicht zur Verfügung stehen, können Sie auf das kostenfreie Programm SecCardAdmin zurückgreifen, das Sie unter <https://www.seccommerce.de/de/products/seccardadmin.html> finden.

Für die Ver- und Entschlüsselung von Dokumenten benötigen Sie eine geeignete Software. Hierfür kommt beispielsweise das Programm SecSigner in Betracht, welches auch Bestandteil von SigNotar ist. Die Nutzung der in SigNotar enthaltenen SecSigner-Version ist jedoch nicht für die Verschlüsselung von Dokumenten verwendbar. Um den SecSigner zur Verschlüsselung von Dokumenten zu nutzen, laden Sie sich bitte die kostenlose Downloadversion von der Homepage des Herstellers <http://www.seccommerce.de> herunter und installieren anschließend das Programm. Dokumente können Sie verschlüsseln, indem Sie im Windows-Explorer das Dokument markieren und im Kontextmenü (rechte Maustaste) unter dem Menüpunkt „SecSigner“ den Untermenüpunkt „Daten nur verschlüsseln“ wählen. Anschließend brauchen Sie nur noch den öffentlichen Schlüssel des Empfängers auszuwählen und die nun verschlüsselte Datei an einem geeigneten Ort zu speichern. Diese Datei mit der Endung .pkcs7 übermitteln Sie sodann Ihrem Kommunikationspartner. Eine mit Ihrem öffentlichen Schlüssel verschlüsselte Datei können Sie mit dem SecSigner und Ihrer Signaturkarte durch Doppelklick auf die Datei entschlüsseln. Klicken Sie hierzu in dem sich öffnenden SecSigner zunächst auf die Schaltfläche „Signaturkarte suchen“ und sodann auf „Daten entschlüsseln“. Die entschlüsselte Datei wird automatisch in demselben Ordner gespeichert, in welchem die verschlüsselte Datei abgelegt ist. **Hierbei ist zu beachten, dass für die Entschlüsselungsfunktion nicht die Signatur-PIN, sondern die PIN für die Verschlüsselungs- und Authentisierungsfunktion genutzt werden muss und eine dreimalige Fehleingabe zur Sperrung der Verschlüsselung und Authentisierungsfunktion führt.**

