Biodaten Entschlüsselung/Export mit eSignatureOffice

Information

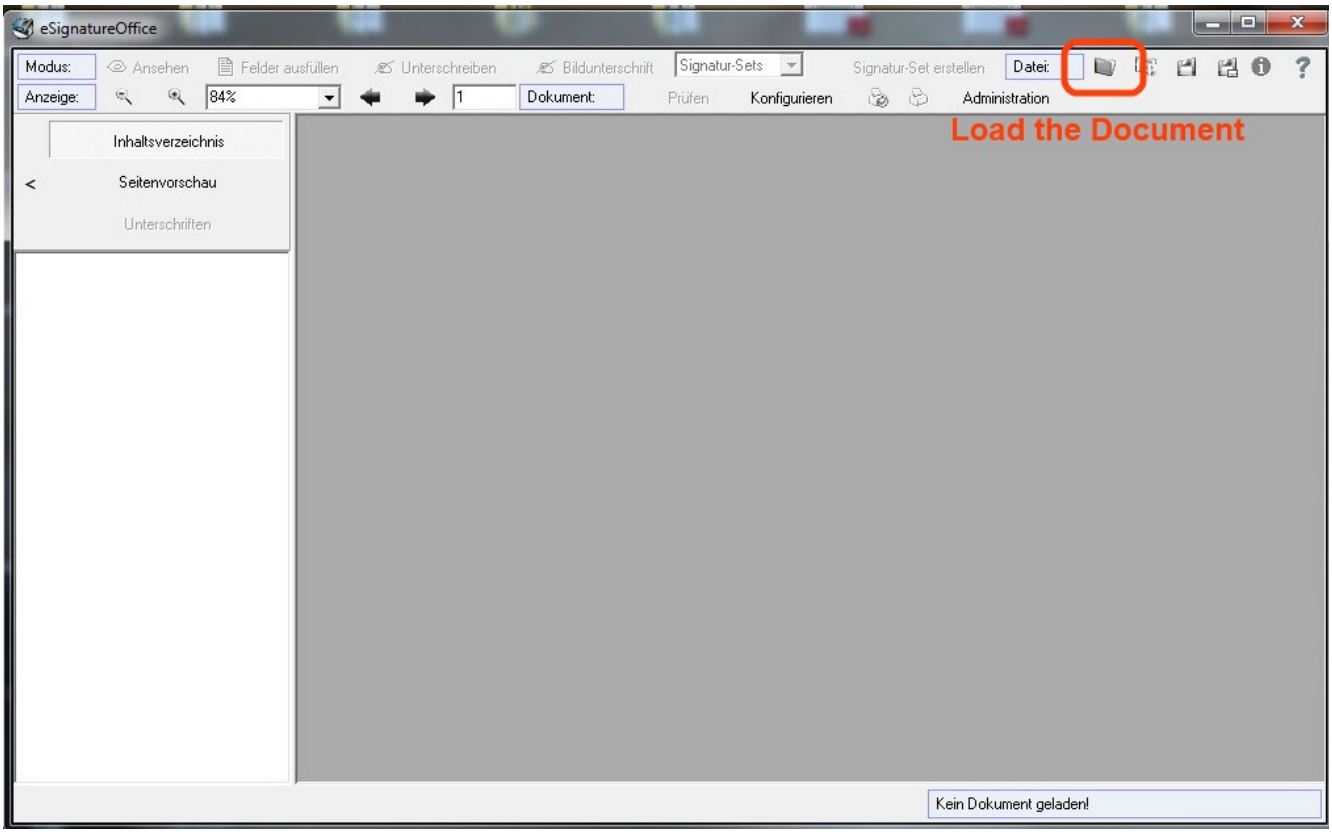
Da es sinnvoll sein kann, nur die Biometrischen Daten einzelner Unterschriften weiterzugeben, zum Beispiel an Schriftsachverständige, gibt es innerhalb von eSignatureOffice entsprechende Funktionen. Man kann zum einen die Unterschrift entschlüsseln und anschließend auch als Textdatei exportieren.

Da die Unterschriften asymmetrisch verschlüsselt sind, benötigt man den privaten Schlüssel, also das Gegenstück des PublicKeys mit dem verschlüsselt worden ist. Dieser Key ist in der Regel sicher bei einen Notar verwahrt, welcher das genau ist lässt sich auch aus dem Dokument auslesen.

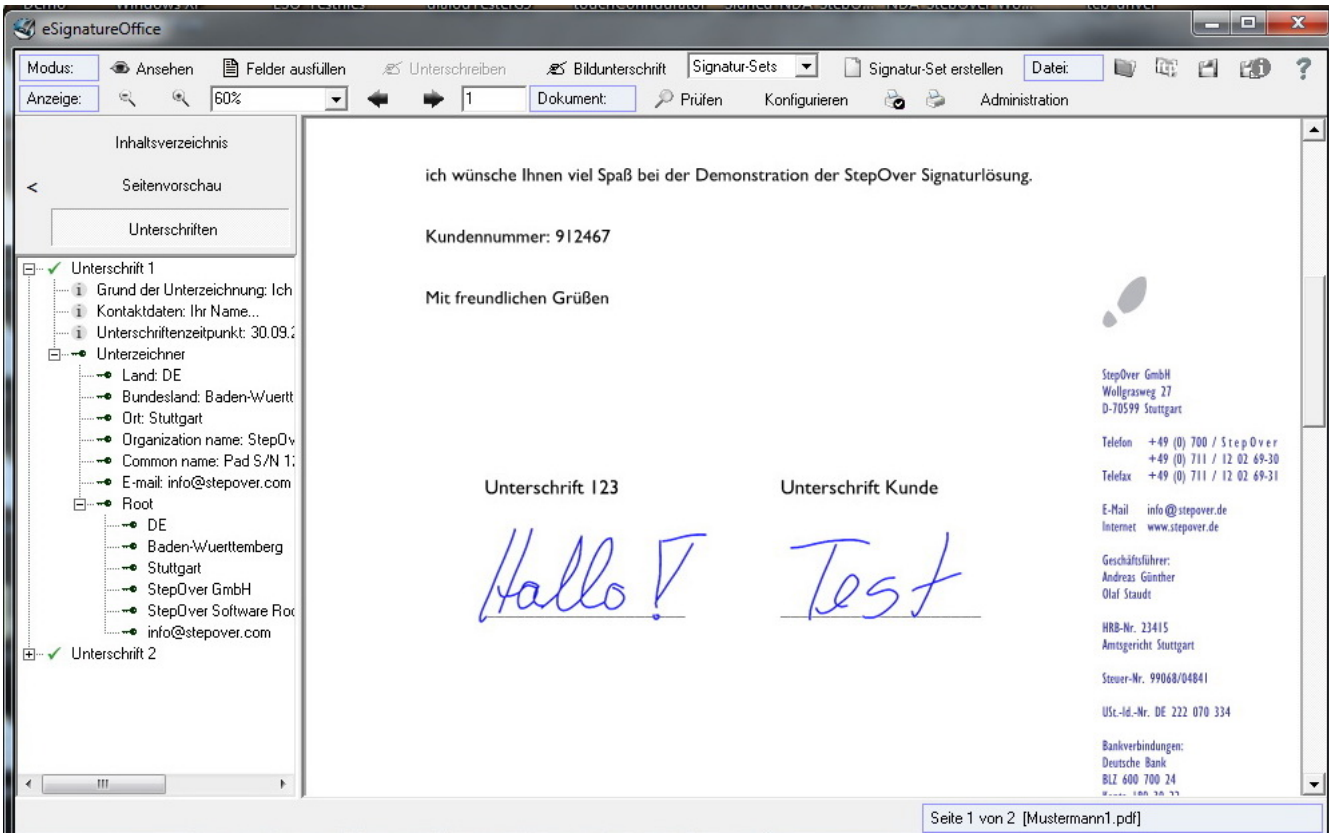
Unterschriften Prüfung mit eSignatureOffice

Dokumentenprüfung ohne den Private Key

Auch ohne dem privaten Schlüssel lassen sich einige nützliche Informationen zu den Unterschriften ermitteln. Starten Sie das eSignatureOffice (SOSigOffice.exe) und laden Sie anschließen das Dokument.

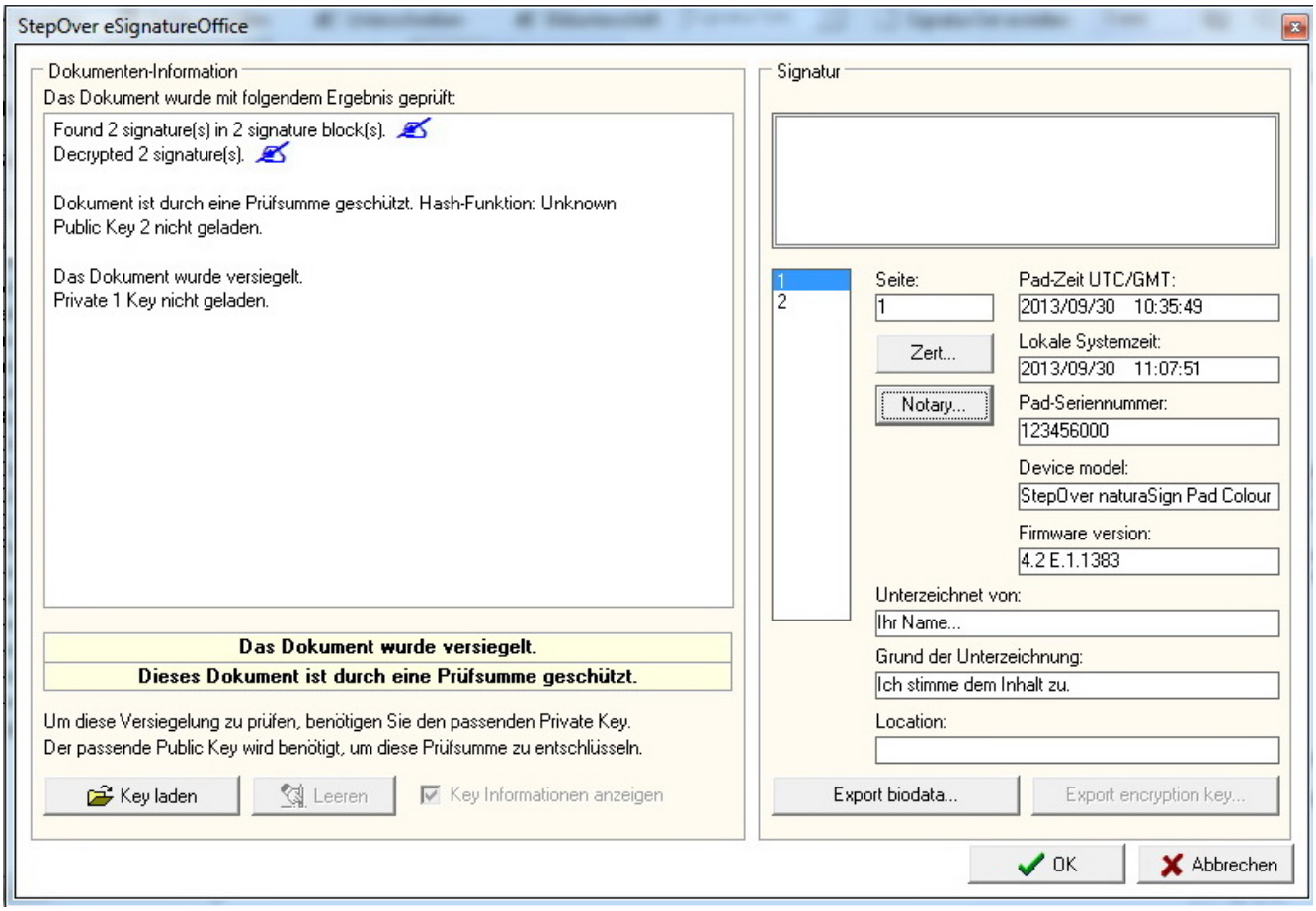


Das eSignatureOffice sollte vorhandene digitale Unterschriften automatisch finden und prüfen. Die Details dazu finden sich in der Seitenleiste unter "Unterschriften". Die Angaben die dort zu sehen sind lassen sich auch mit dem Adobe Reader / Acrobat überprüfen. Diese Prüfung hat noch nichts mit den Biodaten zu tun, es handelt sich nur über die Integritätsprüfung des Dokumentes.

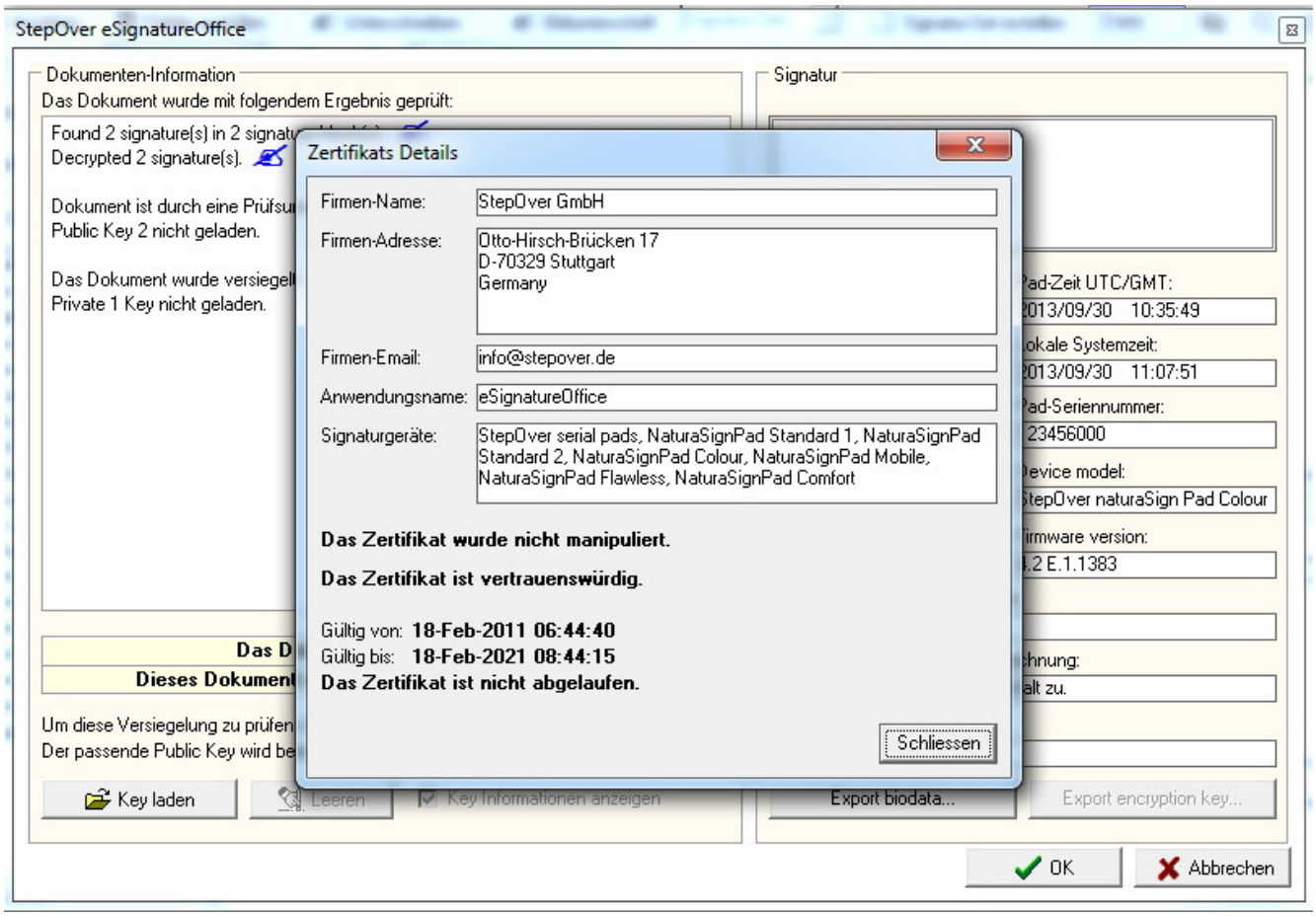


Über den Menü Punkt "Prüfen", kommt man zur Prüfung der Biometrischen Unterschrift. Selbst ohne den Privaten Schlüssel bekommt man einige nützliche Informationen zur Unterschrift:

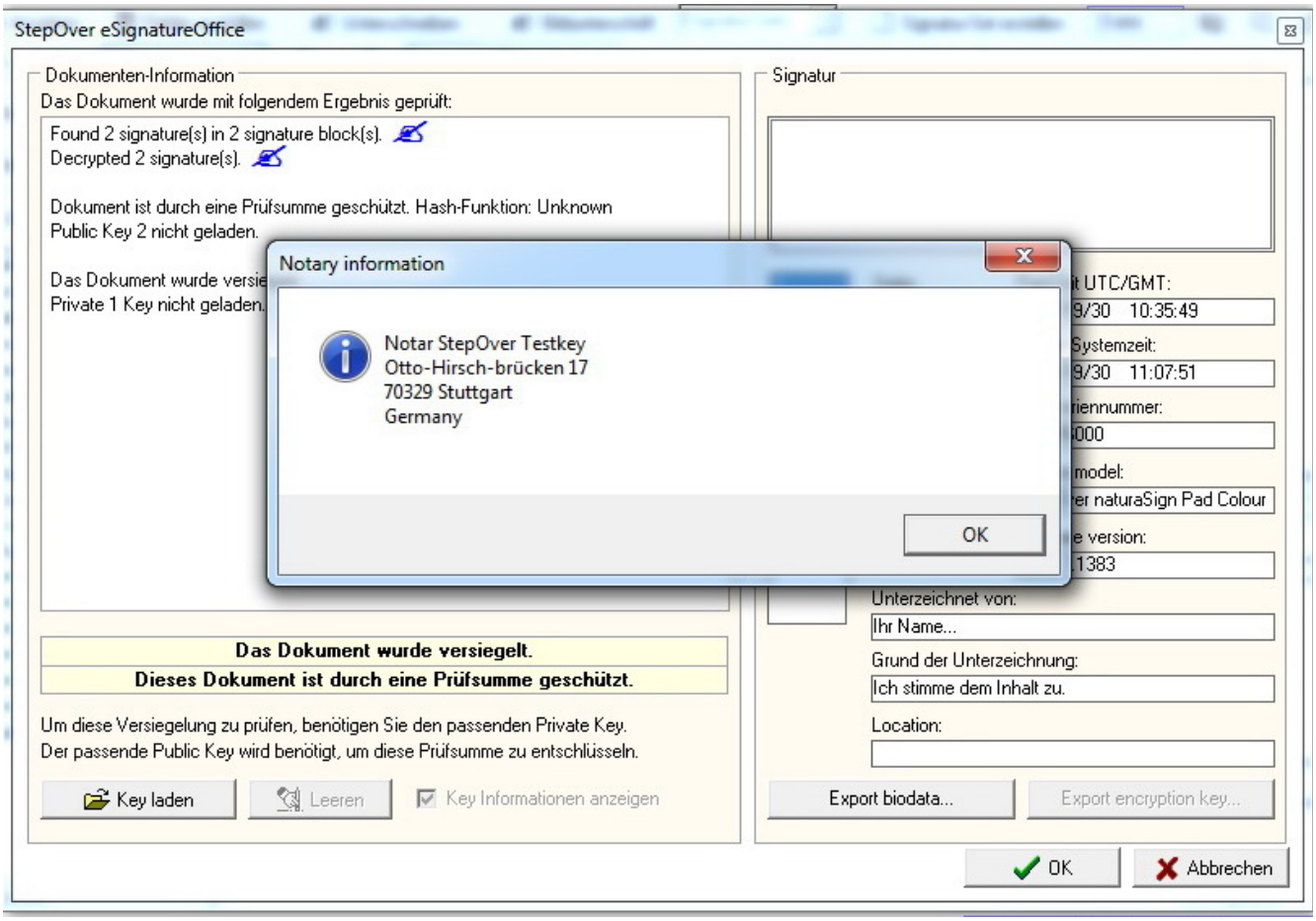
- Datum des Pads (so fern im Pad eine Interne Uhr vorhanden ist)
- Uhrzeit des Computers
- Seriennummer des Unterschriftenpads
- Model Bezeichnung des Unterschriftenpads
- Firmware Version des Unterschriftenpads
- Außerdem Informationen zum Unterzeichner, den Grund und den Ort sofern diese beim Unterschreiben angegeben wurden
- Warnung, daß das Unterschriftenpad mindestens einmal von einer nicht autorisierten Person geöffnet wurde (nur beim ColourPad)



Über die Schaltfläche "Zert..." lässt sich anzeigen welche Anwendung zum Unterschreiben benutzt wurde. Dazu wird das Driver Zertifikat wel ches die Software unseren Treiber übergibt mit in der Unterschrift gespeichert. Damit hat man die Möglichkeit zu erkennen welche Software zum Unterschreiben benutzt wurde.

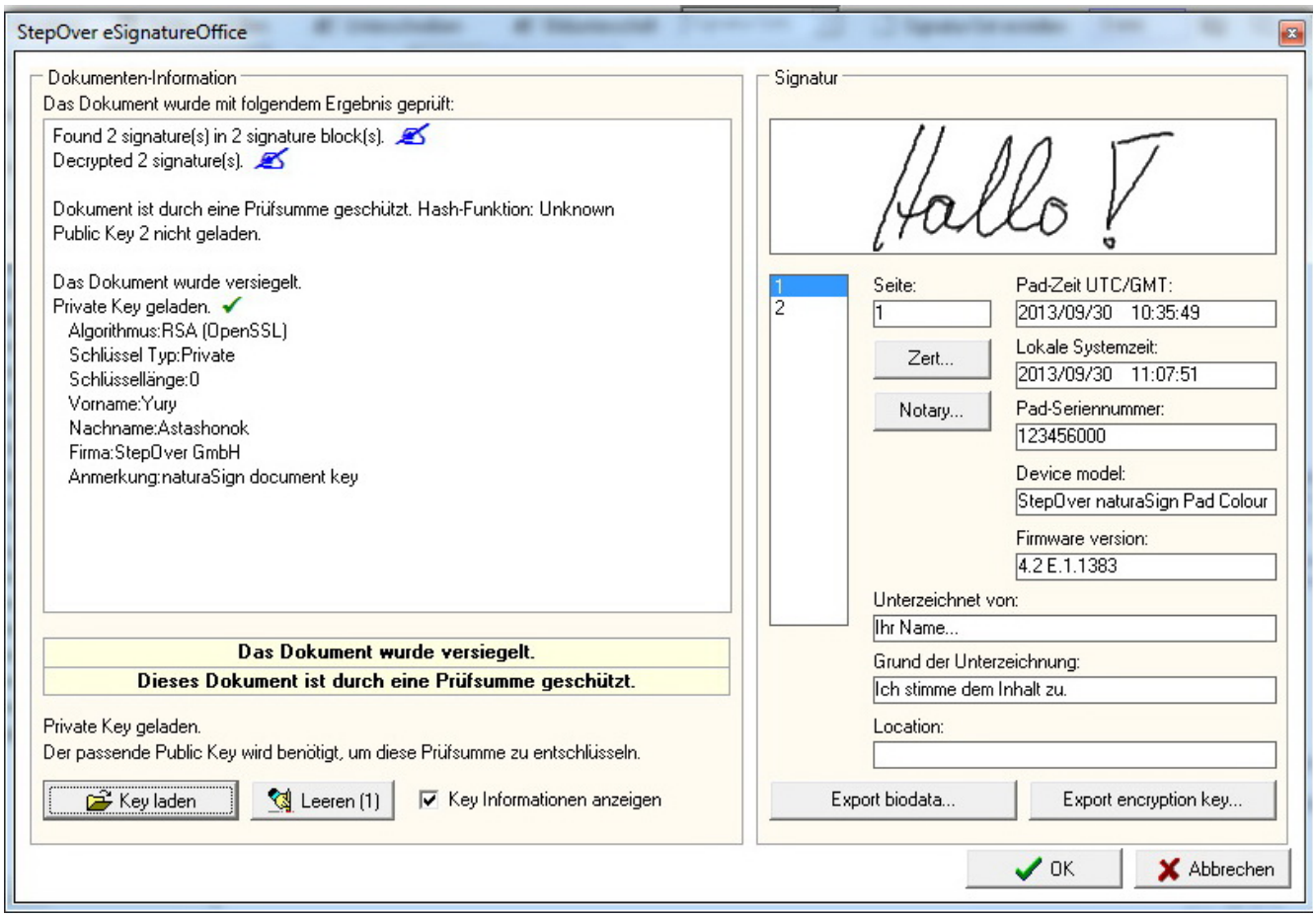


Über die Schaltfläche "Notary..." bekommt man die Information, wer für den privaten Schlüssel zuständig ist. In der Regel ist das die Adresse des Notars welcher das Schlüsselpaar erstellt hatte und den privaten Schlüssel verwahrt.



Biodaten Entschlüsselung

Um die Biodaten zu entschlüsseln, muss man den privaten Schlüssel im SKF über den Button "Key laden..." öffnen. Wenn der Schlüssel korrekt war und die Unterschrift entschlüsselt werden konnte, zeichnet das eSignatureOffice aus den Biometrischen die Unterschrift neu.



Über die Schaltfläche "Export biodata..." kann man sich die Biometrischen Daten als Datei speichern, verwenden Sie am besten die Datei Endung ".dat". Wie die Biometrischen Daten aufgebaut sind finden Sie hier.

Außer den biometrischen Daten kann man auch den "Random Key" exportieren, welcher für die Entschlüsselung notwendig ist. Mit diesen RandomKey und dem Dokument kann die jeweilige Unterschrift auch ohne den Notary Key noch entschlüsselt werden. Natürlich muss dafür auch der PrivateKey vorher geladen sein.