White Paper

Notarielle Erzeugung und Aufbewahrung eines privaten Biometrie-Schlüssels

Version: 1.1
Datum: 14.08.2020

signotec GmbH
Am Gierath 20 b
D-40885 Ratingen

+49 (2102) 53575-10
+49 (2102) 53575-39
info@signotec.de
www.signotec.com

Inhaltsverzeichnis

1. Vorwort

Mit den Lösungen von signotec können Sie fortgeschrittene elektronische Signaturen gemäß der EU-eIDAS-Verordnung erzeugen. Um die gesetzlichen Anforderungen an eine solche zu erfüllen, werden biometrische Daten der Unterschrift erfasst und verschlüsselt im Dokument hinterlegt. Diese Verschlüsselung findet auf dem aktuellen Stand der Technik durch ein RSA-Verfahren mit Schlüssellängen von bis zu 4.096 Bit statt. Bestenfalls sogar direkt im sicheren Speicher des signotec Unterschriftenpads.

Um eine solche asymmetrische Verschlüsselung durchführen zu können, wird ein Schlüsselpaar benötigt. Ein solches besteht aus einem öffentlichen Teil, welcher die Daten verschlüsselt sowie einem privaten Teil, welcher die Daten bei Bedarf wieder entschlüsseln kann. Die Schlüssel werden oftmals in Form eines Zertifikats verwendet und aufbewahrt.

Die ganzheitliche Beweiskraft ist demnach unter anderem auch davon abhängig, wie viele Personen Zugriff auf den privaten Schlüssel haben und wie wahrscheinlich eine nachträgliche Manipulation ist. Daher ist es besonders wichtig, den privaten Schlüssel sicher aufzubewahren und (z. B.) Zugriffe einzuschränken und zu protokollieren.

Die sicherste Lösung für die Schlüsselaufbewahrung ist dabei die Hinterlegung bei einem Notar, welcher die Obhut des Schlüssels mit höchster Vertrauensstellung im Rahmen seiner unabhängigen Tätigkeiten übernimmt. Einen solchen durch einen Notar erzeugten und aufbewahrten Schlüssel bietet signotec zur Nutzung an, insofern Sie nicht die Möglichkeiten einer sicheren Aufbewahrung in Ihrem Unternehmen haben.

2. Notarielles Schlüsselpaar

2.1. Auswahl des Notars

Das von signotec angebotene Schlüsselpaar wurde in Zusammenarbeit mit einem erfahrenen Notar erzeugt. Neben der Zulassung und langjährigen Tätigkeit als Notar hat dieser auch Erfahrung auf dem Gebiet der elektronischen Signaturen und war mehrere Jahre Mitglied der Geschäftsführung der Bundesnotarkammer.

2.2. Erzeugung des Schlüsselpaars

Das Schlüsselpaar wurde unter Anwesenheit von signotec im Notariat durch den Notar erzeugt. Für die Erstellung gibt es eine offizielle Urkundenrolle mit einem Tatsachenprotokoll, in welcher der Hergang detailliert beschrieben wurde. Es lässt sich somit nachvollziehen, wann und unter welchen Voraussetzungen die Schlüssel erzeugt wurden.

Die wichtigsten Fakten zur Erzeugung:

- Die Schlüssel wurden vom Notar persönlich auf seinem System erzeugt.
- Für die Generierung der Schlüssel hat der Notar eine eigene CA erstellt.
- Den privaten Schlüssel sowie verwendete Passwörter kennt nur der Notar.
- Es wurde ein PC verwendet, welcher vollständig offline war.
- Die verwendeten Softwareprodukte und erzeugten Daten wurden von dem PC entfernt, bevor er wieder online genommen wurde.

Das Schlüsselpaar wird vom Notar redundant gemäß einer detaillierten Verwahrungsanweisung aufbewahrt. Der unbefugte Zugriff wird unter Berücksichtigung gängiger Datensicherheitsaspekte verhindert. Die Aufbewahrung wurde von signotec für 10 Jahre mit Optionen zur Verlängerung beauftragt und im Voraus bezahlt.

Nach Erzeugung wurde der öffentliche Schlüssel durch signotec u. a. in Form eines Public-Key-Zertifikats in Empfang genommen.

Die Funktionsweise des Schlüssels inkl. dem Verfahren zur Entschlüsselung wurde noch vor Ort durch signotec und den Notar erfolgreich getestet.

2.3. Eckdaten des Schlüssels

Das erzeugte Schlüsselpaar weist die folgenden allgemeinen Eigenschaften auf:

Antragsteller:	signotec GmbH Biometric Encryption
Seriennummer:	5D2C6349D87E2CA5
Aussteller:	Notar Marius Klingler
Schlüssellänge:	4.096 Bit

Die ganzheitlichen Informationen können direkt dem Zertifikat selbst entnommen werden.

2.4. Prüfsumme des Zertifikats

Das Zertifikat wird als *.CRT-Datei bereitgestellt. Die Integrität des Zertifikats kann mithilfe der folgenden SHA-256 Prüfsumme überprüft werden.

07343010F27355084DE73E8C1466AD3A042FEF8D6A2EBDE9EF7887FDFAE95B20

2.5. Erneuerung des Schlüsselpaars

Der Schlüssel wurde für hohe Sicherheitsanforderungen mit einer Schlüssellänge von 4.096 Bit erstellt. Es ist derzeit nicht zu erwarten, dass der Schlüssel in naher Zukunft als unsicher anzusehen ist und erneuert werden muss. Insofern sich die Bedingungen (z. B. durch technischen Fortschritt) ändern sollten, plant signotec die Erzeugung und Verteilung eines neuen Schlüsselpaars, um die Datensicherheit weiterhin zu gewährleisten.

3. Nutzung des Schlüssels

Der öffentliche Schlüssel wird von signotec kostenfrei zur Verfügung gestellt. Je nach Produkt ist dieser Teil des Lieferumfangs. Alternativ kann dieser direkt bei signotec oder autorisierten Partnern angefragt oder einfach heruntergeladen werden.

Um mit dem Schlüssel die Unterschriften verschlüsseln zu können, wird dieser in der Software konfiguriert oder bestenfalls direkt in das signotec Unterschriftenpad geladen. Dies kann auf Anfrage auch direkt in der Produktion geschehen.

Wie ein Sie ein individuelles Zertifikat in Ihrer Software konfigurieren, können Sie dem jeweiligen Handbuch entnehmen.

4. Entschlüsselung im Streitfall

Sollte es zu einem Streitfall kommen und gerichtlich ein Unterschriftenvergleich verlangt werden, so kann die Entschlüsselung nur durch den Notar erfolgen. Um die Daten zu entschlüsseln, müssen Sie sich mit den Dokumenten und der gerichtlichen Anordnung an signotec oder unter Vorlage einer Vollmacht direkt an den Notar wenden. Dieser wird die Unterschriften aus dem Dokument extrahieren, protokollieren und Ihnen bzw. dem vom Gericht beauftragten Gutachter auf geeignete Art und Weise zur Verfügung stellen. Die Entschlüsselung von Unterschriften sowie die notarielle Protokollierung kann beim Notar beauftragt werden.

5. Fazit

Die Erzeugung und Aufbewahrung der zur Verschlüsselung der Unterschrift notwendigen Schlüssel bei einem Notar stellen die höchste Vertrauensstellung für ein solches Verfahren dar, denn es ist ausgeschlossen, dass der private Schlüssel zur Manipulation der Unterschrift oder des Dokuments verwendet werden konnte. In einem Gerichtsverfahren können Sie somit die Sicherheit und Vertraulichkeit der Erzeugung, Aufbewahrung und auch der Entschlüsselung der Unterschriften lückenlos beweisen.

Insofern Sie selbst nicht die Möglichkeit zur sicheren Erstellung und Aufbewahrung von Schlüsseln (z. B. innerhalb einer eigenen CA) haben, so ist die Hinterlegung bei einem Notar sehr zu empfehlen. Der von signotec bereitgestellte Schlüssel hilft Ihnen dabei, Ihre Sicherheitsanforderungen auch mit geringem Eigenaufwand zu erfüllen.