**MEMORANDUM**

Von: [redacted] secunet Security Networks AG

Thema: Review beA-Sicherheitskonzept V1.3 und begleitende Dokumentation

Datum: 18. Oktober 2019

Zum Review vorgelegt wurde die Dokumente

‚Sicherheitskonzept „System zum Betrieb des besonderen elektronischen Anwaltspostfachs" Version 1.3,

„Besonderes Anwaltspostfach beA Kryptokonzept", Version 2.01

„beA-Schlüsselmanagement" Version 1.03

„beA Incident und Security Management Konzept" Version 1.01

Geprüft wurde, ob die Dokumente die Anforderungen an die Sicherheitsdokumentation des beA erfüllen, insbesondere das Sicherheitskonzept einen schlüssigen Nachweis dafür liefert, die Sicherheitsrisiken beim Betrieb des besonderen Anwaltspostfachs (beA) auf ein tolerierbares Maß reduziert zu haben. Im Juli 2019 waren ältere Versionen der Dokumente geprüft und bemängelt worden.

Die nun vorliegenden Dokumente erscheinen ausreichend, um die wesentlichen Sicherheitsmaßnahmen des beA zu erläutern und den gewünschten Nachweis hinreichender Sicherheit der Funktionen des beA zu liefern. Eine weitere Überarbeitung ist nicht notwendig.

## Anmerkungen

Das vorgelegte **Sicherheitskonzept** hat nun die gewünschte Struktur und im jeweiligen Strukturelement die benötigten Informationen. Die spezifischen Sicherheitsmaßnahmen des beA rund um „continuous encryption" wurden ausreichend erläutert. Die spezifischen beA-Bedrohungen für Assets mit hohem Schutzbedarf wurden vollständig behandelt.

Das vorgelegte **Kryptokonzept** entspricht nach Struktur und Inhalt den Vorgaben des BSI (Bundesamt für Sicherheit in der Informationstechnik) über ein solches Konzept. Es ist daher nicht zu beanstanden.

Das **Schlüsselmanagement-Konzept** behandelt alle relevanten Aspekte im Lebenszyklus kryptographischer Schlüssel des beA. Es erscheint auch (ohne tiefere Prüfung, nur auf der Grundlage des im Sicherheitsgutachten des beA erworbenen Wissens um dessen Funktionsweise) das Schlüsselmaterial vollständig zu erfassen.

Das **Incident- und Security-Management-Konzept** stellt dar, dass beim Betrieb des beA Security-Incidents im Rahmen des alllgemeinen Betriebssupports erfasst und die notwendigen Folgemaßnahmen von dort aus veranlasst werden. Es behandelt Security-Incidents generisch und legt keine spezifischen Maßnahmen für spezifische Security-Incidents (wie z.B. Kompromittierung des Schlüsselmaterials der HSM) fest. Eine solche

Vorausplanung wäre zwar wünschenswert, aber das vorgelegte Konzept ist mit der generischen Behandlung ausreichend.

## Empfehlungen

Die Dokumente müssen im Rahmen der Produktpflege bei relevanten Veränderungen des beA fortgeschrieben werden.

Das Kryptokonzept enthält nicht eine vollständige Darstellung aller kryptographischen Operationen, die im beA ablaufen, sondern nur eine summarische Übersicht über Schlüsselmaterial und verwendete kryptographische Algorithmen. Es wird empfohlen, eine Beschreibung der konkreten kryptographischen Operationen (Eingabedatum, verwendetes Verfahren, verwendeter Schlüssel, Ausgabedatum) im Rahmen der Systemdokumentation als Grundlage für die Weiterentwicklung des beA anzufertigen, um einer fehlerhaften Implementierung der Kryptographie vorzubeugen.

Eine Überprüfung der Vollständigkeit des Schlüsselmanagementkonzepts hinsichtlich des aufgeführten Schlüsselmaterials sollte der neue Betreiber 2020 im Rahmen der Fortschreibung und Pflege der Sicherheitsdokumentation durchführen.

Alle geprüften Dokumente enthalten betriebliche Details, deren Kenntnis es einem Angreifer erleichtern könnte, einem Schutzobjekt des beA Schaden zuzufügen. Daher sollten alle diese Dokumente als „vertraulich" eingestuft werden.