secunet

Technische Analyse und Konzeptprüfung des beA

Abschlussgutachten

im Auftrag der

Bundesrechtsanwaltskammer
Körperschaft des öffentlichen Rechts
Littenstraße 9
10179 Berlin

Version: 1.0
Stand: 18.06.2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Management Summary

1.1 Zielsetzung

Die secunet Security Networks AG (secunet) wurde von der Bundesrechtsanwaltskammer (BRAK) beauftragt, die Umsetzung des besonderen elektronischen Anwaltspostfachs (beA) hinsichtlich IT-Sicherheit zu analysieren und zu bewerten.

Ziel der Analyse ist, bereits bekannte technische, organisatorische und konzeptionelle Schwachstellen zu validieren und gegebenenfalls vorhandene neue Schwachstellen zu identifizieren und zu beurteilen.

Im Rahmen der Untersuchungen von Februar bis Ende Mai 2018 wurden neben Penetrationstests ausgewählter beA-Komponenten und Schnittstellen ebenfalls Quelltextanalysen sowie eine konzeptionelle Analyse durchgeführt.

Der Auftrag sieht die Erstellung eines Abschlussgutachtens vor, das mit diesem Dokument an die Bundesrechtsanwaltskammer übergeben wird. Das hier vorliegende Abschlussgutachten bildet den Stand der Untersuchungen zum Stichtag 28.05.2018 ab. Die im Laufe der Analyse erkannten Schwachstellen wurden soweit möglich, bereits vor der Fertigstellung des Gutachtens an den Betreiber kommuniziert. Ein Teil dieser gemeldeten Schwachstellen konnte bereits vor Erstellung dieses Gutachtens behoben und einem erneuten Test (ReTest) durch den Gutachter unterzogen werden. Zum Stichtag ist die Behebung von Schwachstellen durch den Betreiber oder ihr erneuter Test (ReTest) noch nicht abgeschlossen. Der ReTest aller vom Betreiber behobenen Schwachstellen ist beabsichtigt.

Im Rahmen der Analyse wurden die für die Sicherheit wichtigen Komponenten, Schnittstellen, Anwendungsfälle und vorliegenden Dokumente berücksichtigt. Die Bewertung der gefundenen Schwachstellen erfolgt angelehnt an die in dem Fehlermanagementsystem des Betreibers verwendeten Stufen „betriebsverhindernd“, „betriebsbehindernd“ und „sonstige“:

A - Betriebsverhindernde Schwachstelle
Die Behebung vor Wiederinbetriebnahme wird dringend empfohlen.

B - Betriebsbehindernde Schwachstelle
Eine Behebung sobald wie möglich wird empfohlen.

C - Sonstige Schwachstelle
Lediglich unerhebliche Auswirkungen auf den Betrieb sind zu erwarten, eine Behebung wird empfohlen, soweit dies mit verhältnismäßigem (am möglichen Schaden bemessenen) Aufwand möglich ist.

Die Risikobewertung wurde aus technischer Sicht vorgenommen. Dabei gingen die Menge der potentiellen Angreifer, die Komplexität des Angriffs und die Schäden durch einen erfolgreichen Angriff in die Risikobewertung ein. Die mögliche Motivation der Angreifer (ihre Bereitschaft, die erforderlichen Mittel für einen Angriff aufzubringen und die erforderlichen Risiken einzugehen) wurde mangels Schätzbarkeit nur sehr grob berücksichtigt. Sie ist allerdings ein Faktor, der die Eintrittswahrscheinlichkeit eines erfolgreichen Angriffs beeinflusst und bei genauerer Berücksichtigung die Risikobewertung verändern kann. Eine fachliche Sicht (z.B. Bewertung der Bedeutung eines Verlustes von Vertraulichkeit aus juristischer Sicht) von beA-Betreiber und -Anwenderseite kann mögliche Schäden oder ihre Eintrittswahrscheinlichkeit und damit das Risiko ebenfalls anders bewerten. Das Verfahren zur Risikobewertung ist in Kapitel 2 dargestellt.

Die Inhalte und Ergebnisse der Analysen werden in den folgenden Unterabschnitten 1.2 bis 1.4 überblicksweise dargestellt und in den Kapiteln 3 bis 5 ausführlich erläutert.

1.2 Ergebnisse der Penetrationstests

In dem Analysezeitraum konnten zusammenfassend Schwachstellen in den nachfolgenden Ausprägungen identifiziert werden:

- A - Betriebsverhindernd: 4 Schwachstellen 2 behoben
- B - Betriebsbehindernd: 13 Schwachstellen 4 behoben
- C - sonstige Fehler: 19 Schwachstellen 2 behoben

Bei den identifizierten betriebsverhindernden Schwachstellen handelt es sich um die nachfolgend kurz aufgeführten Schwachstellen:

- **Nicht autorisiertes File-Sharing (behoben)**
  Angreifer können die beA-Anwendung als einfachen „Cloud-Dienst“ nutzen um dort beliebige Daten, ggf. auch mit krimineller Absicht, abzulegen und zu einem späteren Zeitpunkt wieder herunterzuladen.

- **Auslesen von Metadaten fremder Nachrichtenanhänge (behoben)**
  Innerhalb der beA-Anwendung angemeldete Angreifer können auf verschlüsselte Anhänge von verschlüsselten Nachrichten Dritter zugreifen. Dadurch wird das Rollenkonzept des beA umgangen und Metadaten können eingesehen werden. Die Verschlüsselung selbst kann dadurch zwar nicht überwunden werden, aber auch die einsehbaren Metadaten können z.B. in den Bezeichnungen für Anhänge sensible Informationen offenbaren.

- **Modifikation von signierten XML-Nachrichten**
  Signaturen können umgangen und so XML-Nachrichten manipuliert werden. Diese Schwachstelle wurde in zwei Schnittstellen gefunden, von denen eine kritisch ist, weil dort Gültigkeitsaussagen zu qualifizierten Signaturen ver-

fälscht werden könnten. Die Ausnutzung ist aber nur Innentätern im beA-Betrieb und Angreifern, die erfolgreich beA-Teilkomponenten unter ihre Kontrolle gebracht haben, möglich.

- **Veraltete Softwareelemente in der beA-Client-Security**
  Es werden Softwareelemente verwendet, die Sicherheitsupdates erfordern.

Des Weiteren konnten durch zeitnahe Meldungen des Gutachters während des Analysezeitraums bereits 8 Schwachstellen durch den Betreiber behoben und durch ReTests als tatsächlich gegenüber der gemeldeten Schwachstelle als geschlossen verifiziert werden. Eine detaillierte Auflistung der gefundene Schwachstellen und der durchgeführten ReTests findet sich in den Detailergebnissen in Abschnitt 3 wieder. Dort werden auch der Analysegegenstand und die Vorgehensweise beschrieben.

1.3 Ergebnisse der Quelltextanalyse

Die beA-Anwendung, beA-Client-Security und die BRAV-Search wurden einer werkzeuggestützten, statischen Quelltextanalyse unterzogen. Für die beA-Client-Security wurde darüber hinaus ein Quelltext-Audit vorgenommen, bei dem die als kritisch identifizierte Teile der beA-Client-Security geprüft und der korrekte Programmablauf nachvollzogen wurde. Quelltext-Analyse und -Audit können Schwachstellen in Software erkennen, die mit Werkzeugen des Penetrationstests nicht entdeckt werden können.

Die statische Quelltext-Analyse hat in der Summe folgende Treffer mit unterschiedlichen Einstufungen erbracht: beA-Client-Security 337 Treffer, beA-Anwendung ca. 1000 Treffer und BRAV-SEARCH 85 Treffer.

Die Anzahl der Treffer an sich erlaubt keinen Rückschluss auf die Quelltext-Qualität. Die Gewichtung der Treffer erstreckt sich von ‚eher' kleineren Unsauberkeiten bis hin zu potentiell gravierend eingestuften Mängeln. Eine Betrachtung wurde nur von den im verwendeten Analysetool höher eingestuften Treffern vorgenommen.

Mit Hilfe der statischen Quelltext-Analyse und des Quelltext-Audits wurden sechs als betriebsverhindernd eingestufte Schwachstellen gefunden. Dies bieten Angreifern potentielle Angriffswege an, die mit bekannten Techniken ausnutzbar sind und dem Angreifer ermöglichen, die Kontrolle über die angegriffenen Systeme zu übernehmen. Diese Schwachstellen wurden in der Zwischenzeit beseitigt. Detailliert beschrieben werden die gefundenen Schwachstellen in Kapitel 4.

Im Rahmen der Quelltext-Analyse (teilweise unterstützt durch die Penetrationstests) wurden auch die vom Chaos Computer Club e. V. (CCC) bemängelten Schwachstellen überprüft, die in der zum Stichtag vorliegenden Fassung von beA-Client-Security und beA-Anwendung fast alle nicht mehr vorhanden sind. Die Unterstützung von aktuellen Betriebssystemen konnte noch nicht bestätigt werden.

1.4 Ergebnisse konzeptionelle Analyse

Gegenstand der konzeptionellen Analyse waren wesentliche Sicherheitsfunktionen des beA, die dem Schutz von Vertraulichkeit und Authentizität der via beA übermittelten Nachrichten dienen.

Es wurde geprüft, ob der erforderliche Schutz der Vertraulichkeit der Nachrichten durch das implementierte Verschlüsselungsverfahren erreicht wird, so dass alle kryptographischen Operationen zum Schutz der Vertraulichkeit von Nachrichten in HSM gekapselt sind und Nachrichten nicht außerhalb der HSM entschlüsselt werden können.

Durchgeführt wurde eine Analyse nach Dokumentenlage, insbesondere durch Auswertung der relevanten Use-Cases (Ablaufbeschreibungen für bestimmte fachliche Vorgänge im beA). Des Weiteren wurden vorgelegte Feinkonzepte (vor allem zum Gesamtsystem, zur HSM-Verwendung und zur beA-Client-Security) analysiert. Die Ergebnisse der Analyse wurden gemeinsam mit dem Betreiber und dem Auftraggeber im Rahmen von Telefonkonferenzen erörtert und verifiziert.

Grundsätzlich ist das dem beA zugrundeliegende Verschlüsselungskonzept geeignet, die Vertraulichkeit der Nachrichten während der Übertragung und Speicherung von Nachrichten durch das beA zu gewährleisten, auch gegenüber dem Betreiber des beA. Nachrichteninhalte liegen unverschlüsselt nur bei den Kommunikationspartnern vor. Die Umverschlüsselung ist in einem HSM gekapselt, schützt daher dort vorübergehend entstehende Schlüsselinformationen in einer besonderen manipulations- und ausspähsicheren Umgebung. Das erkennbare Ziel, die Sicherheit der Nachrichten ausschließlich durch Kryptographie zu schützen, ist aber nicht in vollem Umfang erreicht worden. An einigen Stellen verlässt sich das beA in seiner dem Gutachten zugrunde liegenden Realisierung auf organisatorisch-physikalischen Schutz wichtiger Systemkomponenten (HSM-Schlüssel, SAFE BRAK), was bei voller Ausnutzung der kryptographischen Möglichkeiten, die das Konzept und die eingesetzte Technik bieten, nicht notwendig wäre.

Durch die Analyse konnten aus technischer Sicht zwei betriebsverhindernde, drei betriebsbehindernde und zwei sonstige Schwachstellen identifiziert werden, die ein Angreifer ausnutzen kann, um sich trotz des kryptographischen Schutzes unbefugten Zugang zu Nachrichten zu verschaffen.

Allen Schwachstellen ist gemeinsam, dass das HSM keinen oder keinen ausreichenden Schutz vor diesen Angriffen bietet, d.h. Nachrichten bei erfolgreichem Angriff auch außerhalb des HSM entschlüsselt oder dem HSM Leseberechtigungen vorgetäuscht werden können. Fast allen konzeptionellen Schwachstellen ist allerdings auch gemeinsam, dass sie nur durch oder mit Hilfe von Innentätern, darunter auch Personen mit besonderer Vertrauensstellung, durchgeführt werden können, die dabei physikalisch-organisatorische Schutzmaßnahmen unterlaufen müssen. Außentäter können sich in die Position eines Innentäters bringen, wenn es ihnen gelingt, durch Ausnutzung von Schwachstellen der Serverkomponenten in diese einzudringen und die Kontrolle über sie zu übernehmen. Nur in einem Fall, einer

Täuschung eines beA-Anwenders mittels einer irreführenden EGVP-Adresse, ist auch ein Angriff durch einen Außentäter denkbar, der dafür die beA-Anwendung nicht angreifen muss. Die Ausnutzbarkeit der Schwachstellen ist in der Regel aufgrund des eingeschränkten Täterkreises und einer angenommenen geringen Motivation und besseren Überwachbarkeit von Innentätern gering. Die konzeptionellen Schwachstellen erhalten ihre Bedeutung in der Regel durch ihr hohes (teilweise sehr hohes) Schadenspotential.

Betriebsverhindernd bewertet ist, dass Verschlüsselungszertifikate in der beA-Client-Security vor dem Versand von Nachrichten nicht geprüft werden. Dadurch verlieren die Zertifikate ihre Schutzwirkung, die beA-Client-Security kann durch gefälschte Zertifikate leicht getäuscht werden, und versendet dann Nachrichten lesbar für einen Angreifer. Betriebsverhindernd bewertet wird auch, dass die Integrität des Javascript-Codes, mit dem die beA-Client-Security gesteuert wird, nicht gewährleistet ist. Es besteht die Gefahr, dass durch böswillig manipulierten Javascript-Code bei allen beA-Anwendern Nachrichten im Klartext an einen Angreifer ausgeleitet werden.

Für die Details der konzeptionellen Schwachstellen wird auf die Analyse in Kapitel 5 verwiesen. Im Rahmen der Gutachtenerstellung wurden vom Betreiber für alle beschriebenen Schwachstellen Lösungsvorschläge unterbreitet und teilweise aus Gutachtersicht bewertet. Alle Schwachstellen erscheinen grundsätzlich behebbar, allerdings mit unterschiedlichem Aufwand.

Die betrachteten Signatur- und Signaturprüffunktionen des beA wurden ebenfalls untersucht. In diesem Bereich wurde keine konzeptionelle Schwachstelle gefunden. Auch die Authentisierungsfunktionen für den Zugriff auf ein Postfach und die Verwaltung der Administrations- und Leserechte sind angemessen konzipiert.

Die vom Betreiber vorgelegte Dokumentation zum Nachweis des sicheren IT-Betriebs des beA belegt einen geregelten, auch den Aspekt IT-Sicherheit beachtenden Betrieb. Grundlage ist ein ISO-27001-zertifiziertes Informationssicherheitsmanagement. Erkennbar adressiert wird auch der besondere Schutzbedarf des beA. Es fehlt aber für das beA ein geschlossenes Sicherheitskonzept mit Begleitdokumenten, das basierend auf einer Bedrohungs- und Risikoanalyse einen Nachweis darüber führt, dass allen Risiken für die hoch schutzbedürftigen Daten und IT-Systeme des beA in ausreichendem Maße entgegengewirkt wird. Dadurch war es nicht möglich, sich von der physikalisch-organisatorischen Sicherheit des beA und der vollständigen Abwehr aller nicht tragbaren Risiken zu überzeugen. Es wird empfohlen, ein Sicherheitskonzept und Begleitdokumente nach üblichem Muster zu erstellen, die die fehlenden Teile enthalten und vorhandene Informationen über Sicherheitsmaßnahmen bündeln, um sowohl den Vollständigkeitsnachweis über die Abwehr aller Risiken zu führen als auch eine Grundlage für ein Sicherheits-Audit bereitzustellen. Außerdem sollte ein unabhängiger Auditor den sicheren Betrieb des beA regelmäßig überprüfen. Dies kann als ergänzendes Audit zum bereits regelmäßigen stattfindenden ISO-27001-Audit geschehen.

1.5 Resümee und Empfehlung

Im Rahmen der Penetrationstests wurden insgesamt 36 Schwachstellen gefunden. Davon wurden vier Schwachstellen als betriebsverhindernd und 13 als betriebsbehindernd klassifiziert. Von diesen konnten zum Stichtag zwei betriebsverhindernde und vier betriebsbehindernde Schwachstellen nach Bearbeitung durch den Betreiber erneut getestet und als geschlossen festgestellt werden.

Im Rahmen der Quellcodeanalysen wurden insgesamt zehn Schwachstellen gefunden. Davon wurden sechs Schwachstellen als betriebsverhindernd und vier als betriebsbehindernd klassifiziert. Bis zum Stichtag konnten alle betriebsverhindernden Schwachstellen nach Behandlung durch den Betreiber erneut getestet und als geschlossen festgestellt werden.

Die konzeptionelle Analyse hat zwei betriebsverhindernde, drei betriebsbehindernde und zwei sonstige Schwachstellen aufgezeigt. Besonders problematisch sind hier der unsichere Umgang mit Verschlüsselungszertifikaten in der beA-Client-Security sowie die Verwendung von Javascript zur Steuerung der beA-Client-Security. Es wurde auch Verbesserungsbedarf bei der Dokumentation und der Kontrolle des sicheren Betriebs erkannt.

Grundsätzlich ist das beA ein geeignetes System zur vertraulichen Kommunikation im elektronischen Rechtsverkehr. Das Verschlüsselungskonzept bietet technisch gesehen einen hinreichenden Schutz für die Vertraulichkeit der vom beA übermittelten Nachrichten. Nicht tragbare Risiken, die noch bestehen, können beseitigt werden und sind teilweise auch schon beseitigt worden. Die erneute Inbetriebnahme ist bei Beachtung der folgenden Empfehlungen aus sicherheitstechnischer Sicht möglich.

Für die noch nicht behobenen betriebsverhindernden Schwachstellen wird empfohlen, die beA-Anwendung erst nach deren vollständiger Beseitigung wieder in Betrieb zu nehmen. Darüber hinaus empfehlen wir ebenfalls, die als „betriebsbehindernd“ eingestuften Schwachstellen baldmöglichst zu beheben.

Für den nachhaltig sicheren Betrieb des beA wird empfohlen, ein Sicherheitskonzept, ein Kryptokonzept und ein Konzept für die Behandlung von Sicherheitsvorfällen in üblicher Form und Inhalt zu erstellen, bzw. vorhandene relevante Dokumente hier per Verweis einzubetten und auf der Grundlage dieser Dokumente ein regelmäßiges Audit des ordnungsgemäßen Betriebs durchzuführen. Dies kann in Ergänzung des regelmäßigen ISO-27001-Audits des Betreibers im gleichen Rhythmus geschehen.

1.6 Abgrenzung

Bei der Lektüre und Nutzung dieses Gutachtens sind folgende Hinweise zu berücksichtigen:

- Bei allen durchgeführten Tests handelt es sich um stichprobenartige Überprüfungen, in denen versucht wird, mit einem vertretbaren Aufwand möglichst viele Schwachstellen innerhalb des Betrachtungsbereichs zu identifizieren.
- Die vorliegenden Ergebnisse müssen stichtagsbezogen beziehungsweise bezogen auf einen speziellen Versionsstand aufgefasst werden und enthalten keine Aussagen über die Sicherheit der zukünftigen technischen und organisatorischen Anpassungen bzw. Lösungen.
- Im Rahmen der Analysen wurde lediglich der wesentliche Teil der für das beA-System erforderlichen technischen Komponenten, Schnittstellen oder Anwendungsfälle betrachtet. Es kann somit nicht vollständig ausgeschlossen werden, dass in anderen Teilen weitere nicht erkannte Schwachstellen vorhanden sind. Es kann auch nicht völlig ausgeschlossen werden, dass bereits behobene Schwachstellen in zukünftigen Versionen erneut auftreten oder in zukünftigen Versionen neue Schwachstellen implementiert werden. Zu berücksichtigen ist auch, dass die konzeptionelle Analyse sich auf die Sicherheitsziele „Vertraulichkeit“ und „Authentizität“ konzentriert hat und somit insbesondere eine Betrachtung der „Verfügbarkeit“ nur dort erfolgte, wo eine gefundene Schwachstelle diese unmittelbar bedroht. Innerhalb der technischen Analysen standen die beA-Client-Security, die beA-Anwendung und externe Schnittstellen im Fokus.
- Die vorgelegten grundlegenden Konzepte zur IT-Sicherheit (Sicherheitskonzept, Kryptokonzept etc.) ermöglichten keine abschließende Einschätzung der technisch-organisatorischen Sicherheit des beA. Das Ausnutzen einzelner identifizierter Schwachstellen kann eventuell durch geeignete technische und organisatorische Maßnahmen – seitens des Auftraggebers oder des Betreibers – deutlich erschwert oder sogar vereitelt werden. Umgekehrt können aber auch Schäden durch fehlende bzw. ungeeignete technische und/oder organisatorische Maßnahmen entstehen, die erst bei einer Vollständigkeitsprüfung, wie sie im Rahmen der Erstellung eines geschlossenen Sicherheitskonzeptes durchzuführen wäre, auffallen. Ein solches Sicherheitskonzept liegt nicht vor. Es war nicht Gutachterauftrag, ein solches Konzept auf der Basis der vorgelegten Informationen und Dokumente zu erstellen.
- Darüber hinaus war es erforderlich, Annahmen zu treffen und Abgrenzungen des Betrachtungsgegenstandes vorzunehmen, damit der Aufwand insgesamt vertretbar blieb. So wurde angenommen, dass der Anwaltsrechner eine sichere Einsatzumgebung für den Einsatz der beA-Client-Security darstellt und frei von Schadsoftware ist. Die Absicherung des Anwaltsrechners sowie der Einsatzumgebung war dementsprechend nicht Gegenstand der Untersuchung.

- Eine Analyse, ob das beA-System alle rechtlichen und über die Sicherheit hinausgehenden funktionalen Anforderungen erfüllt, war nicht Gegenstand der Betrachtung.
- Es ist möglich, dass einzelne identifizierte Schwachstellen von Dritten nachvollzogen und ausgenutzt werden können, auch wenn sie bereits behoben wurden, z. B. bei nicht erfolgter Deinstallation älterer Versionen der beA-Client-Security. Außerdem könnten durch die Darstellung von detaillierten technischen Informationen Rechte Dritter verletzt werden, z.B. durch Angabe von Quellcode, oder schützenswerte Informationen aufgedeckt werden, wie z.B. IP-Adressen. Aus diesem Grund werden die Schwachstellen in diesem, zur Veröffentlichung vorgesehenen Gutachten, ohne Angabe von detaillierten technischen Informationen dargestellt. Die detaillierten technischen und inhaltlichen Informationen zu den einzelnen Schwachstellen werden zu deren gezielter Behebung laufend an den Auftraggeber übermittelt.

2 Verfahren zur Schwachstellenbewertung

In diesem Kapitel wird beschrieben, wie gefundene Schwachstellen in den folgenden Kapiteln dargestellt werden und auf welche Art und Weise sie in Risikostufen eingeordnet worden sind.

2.1 Darstellungsform

Bei der Beschreibung und Bewertung der identifizierten Schwachstellen wurde die folgende Darstellungsform gewählt.

{S1} Schwachstellenbeschreibung
Beschreibung der Schwachstelle

{R1} Risikobewertung: ***Einstufung in Risikokategorie (A, B, C)***

Ausnutzbarkeit der Schwachstelle:

Bewertung der Ausnutzbarkeit gemäß Kriterien, die noch erläutert werden

Bewertung Ausnutzbarkeit: ***hoch, mittel oder niedrig***

Bewertung der Bedrohung:

Beschreibung des Schadens eines Angriffs auf diese Schwachstelle im Erfolgsfall, Einstufung des Schadensausmaß in den drei Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit gemäß Kriterien, die noch erläutert werden

Bedrohung Integrität: ***hoch, mittel oder niedrig***
Bedrohung Verfügbarkeit: ***hoch, mittel oder niedrig***
Bedrohung Vertraulichkeit: ***hoch, mittel oder niedrig***

{M1} *Maßnahmenempfehlung, Darstellung, auf welche Weise die Schwachstelle beseitigt werden könnte*

Die Beschreibung der identifizierten Schwachstellen setzt sich aus den drei Komponenten Schwachstelle {S}, Risiko {R} und Maßnahme {M} mit einer zugehörigen eindeutigen Nummer zusammen.

Die Schwachstellen der Kategorie **C-Sonstige Schwachstelle**haben geringe Auswirkung auf die Schutzziele und eine Behebung erscheint nicht zeitkritisch. Aufgrund der damit zusammenhängenden geringeren Relevanz für die Sicherheit des beA-

Systems, wurden diese in übersichtlicher tabellarischer Form aufgelistet. In der Tabelle sind zusätzlich die Ergebnisse der einstufungsrelevanten Bewertungen hinsichtlich Ausnutzbarkeit und Bedrohungen zu finden.

Tabelle 1: Darstellungsform C-Schwachstellen

Legende: h=hoch; m=mittel; n=niedrig; J=Ja		Bedrohung				
Kurzbeschreibung	Komponente	Ausnutzbarkeit	Vertraulichkeit	Integrität	Verfügbarkeit	Schwachstelle behoben
Die REST-API des Wikis ist öffentlich erreichbar und stellt teilweise sensible Informationen bereit, die für den Anwendungszweck des Wikis nicht benötigt werden.	Webportal XWIKI	m	n	n	n	-

2.2 Schwachstelle

Der Bereich **Schwachstelle** beschreibt die identifizierte Schwachstelle. Zusätzliche Erläuterungen zum Verständnis der Schwachstelle finden sich in der Regel in einem der strukturierten Bewertung vorangestellten Fließtext. Zusätzlich werden (falls verfügbar und relevant) zu den identifizierten Schwachstellen die zugehörigen Common Vulnerabilities and Exposure (CVE) IDs aufgeführt. Bei CVE handelt es sich um einen Industriestandard, der eine einheitliche Namenskonvention für Sicherheitslücken und andere Schwachstellen in Computersystemen bereitstellt. Mehrfachbenennungen gleicher Gefahren werden um eine laufende Nummer (z. B. CVE-2006-3086) ergänzt, um eine eindeutige Identifizierung der Schwachstellen zu gewährleisten. Dadurch ist ein reibungsloser Informationsaustausch zwischen den verschiedenen Datenbanken einzelner Hersteller möglich. Basierend auf den CVE-IDs können auf der Web-Seite http://cvedetails.com/ weiterführende Informationen zu der Schwachstelle nachgelesen werden.

2.3 Risikobewertung

Der Bereich **Risikobewertung** stellt das geschätzte Risiko dar, welches durch das Vorhandensein der Schwachstelle hervorgerufen wird. Zur Einschätzung des Risikos werden zum einen die Ausnutzbarkeit der Schwachstelle sowie die Bedrohung (die im Erfolgsfall des Angriffs eintretenden Schäden) bewertet.

2.3.1 Ausnutzbarkeit

Nach kurzen Erläuterungen zur Ausnutzbarkeit der Schwachstelle wird diese in die Klassen **hoch**, **mittel** und **niedrig** eingestuft.

Beispiele für ausgewählte Fragestellungen, anhand derer die Einstufung der Ausnutzbarkeit erfolgt, sowie diesbezügliche Kriterien für eine Einstufung sind in der folgenden Tabelle dargestellt.

Tabelle 2: Beispielkriterien zur Bestimmung der Ausnutzbarkeit

	Beispiele für Kriterien zur Bestimmung der Ausnutzbarkeit		
Fragestellung (Auswahl)	**hoch**	**mittel**	**niedrig**
Auf welchem Wege kann ein Angriff durchgeführt werden?	Der Angriff ist durch direkten Zugriff aus dem Internet möglich. Er erfordert kein Spezialwissen.	Ein berechtigter Zugriff auf den lokalen Rechner des Anwalts oder Server ist erforderlich.	Die Schwachstelle kann nur durch Innentäter ausgenutzt werden.
Wie komplex ist die Durchführung des Angriffs?	Die Ausnutzung ist mit geringem technischem und zeitlichem Aufwand möglich. Für die Ausnutzung der Schwachstelle ist geringer Fachverstand erforderlich. Informationen zum Nutzen der Schwachstelle sind frei verfügbar.	Es müssen nur wenige Sicherheitsmaßnahmen überwunden werden. Die Schwachstelle lässt sich mit verhältnismäßigen Mitteln Ausnutzen.	Für die Ausnutzung der Schwachstelle müssen vorab verschiedene Sicherheitsmaßnahmen überwunden werden. Das Ausnutzen der Schwachstelle ist nur mit unverhältnismäßig hohem Aufwand möglich.
Welche Rechte sind für den Angriff erforderlich?	Der Angriff ist nicht durch eine Rechteprüfung behindert.	Für die Ausnutzung der Schwachstelle sind Zugriffsberechtigungen erforderlich.	Es sind administrative Berechtigungen erforderlich.
Sind bei einen Angriff Nutzerinteraktionen erforderlich?	Der Angriff kann ohne Mitwirkung eine Nutzers oder Administrators durchgeführt werden.	Für den Angriff ist ein aktives Handeln des Nutzers erforderlich (Eingaben, Mausklick etc.).	Der Zugriff ist nur im 4-Augenprinzip möglich

2.3.2 Bedrohung

Im Bereich Bedrohung werden die im Erfolgsfall des Angriffs eintretenden Schäden allgemein bewertet. Die Bewertung erfolgt dabei für die Schutzziele **Integrität** (können Daten unberechtigt verändert werden), die **Verfügbarkeit** (kann die Erreichbarkeit eines Systems / Dienstes eingeschränkt werden) und die **Vertraulichkeit** (kann ein Unberechtigter auf die Daten lesend zugreifen). Pro Kategorie werden die Klassen **hoch**, **mittel** und **niedrig** unterschieden, die angeben, wie kritisch der jeweilige Schaden eingeschätzt wird.

Einen besonderen Stellenwert bei der Betrachtung hat die Vertraulichkeit der Nachrichteninhalte und sonstiger sensibler Informationen zu Mandatsinhalten. Dies ist insbesondere auf die möglichen sensiblen Nachrichteninhalte in Verbindung mit der erforderlichen anwaltlichen Verschwiegenheitspflicht zurückzuführen.

In die Beurteilung der Bedrohungen für die Integrität wurde ebenso das Schutzziel Authentizität (die Echtheit, Zuverlässigkeit und Glaubwürdigkeit einer Mitteilung, ein vertrauenswürdiger Identitätsnachweis) einbezogen. In die Bewertung der Integrität fließt ebenfalls die Bedrohung einer Übernahme der Kontrolle einer beA-Teilkomponente durch einen Angreifer ein (Störung der Systemintegrität).

Exemplarische Kriterien zur Einstufung der Bedrohung des jeweiligen Schutzziels in die Kategorien „hoch“, „mittel“ und „niedrig“ werden in den nachfolgenden Tabellen dargelegt.

Tabelle 3: Einstufung Vertraulichkeit

Einstufung zum Schutzziel	Beispiele für Bedrohungen
Vertraulichkeit hoch	■ Unberechtigte können Einblick in den Klartext von Nachrichten nehmen. Der Angreifer kann frei wählen, welche Nachrichten er lesen kann. ■ Sensible schützenswerte Informationen können unberechtigt gelesen werden (Inhalte der Nachrichtenanhänge im Klartext, Metadaten mit vertraulichen Inhalten) ■ Administrative/technische Informationen (Passwörter), die einen gezielten Angriff direkt ermöglichen, liegen unberechtigt vor
Vertraulichkeit mittel	■ Unberechtigte können Einblick in den Klartext von Nachrichten nehmen. Bei der Auswahl der Nachrichten ist der Angreifer auf maximal ein Postfach eines beA-Anwenders beschränkt. ■ Metadaten zu Nachrichtenanhängen, die Rückschlüsse auf die sensiblen Nachrichteninhalte ermöglichen können unberechtigt gelesen werden
Vertraulichkeit niedrig	■ Metadaten/Informationen/Fehlermeldungen oder sonstige Systeminformationen mit geringem Informationsgehalt zum Auffinden oder Ausnutzen von Schwachstellen sind betroffen.

Tabelle 4: Einstufung Integrität

Einstufung zum Schutzziel	Beispiele für Bedrohungen
Integrität hoch	■ Der Angreifer kann die komplette Kontrolle über eine beA-Systemkomponente übernehmen. ■ Der Urheber einer Nachricht kann beliebig verfälscht werden ■ Die Gültigkeitsinformation über qualifizierte Signaturen kann verfälscht werden. ■ Wichtige Sicherheitsfunktionen können deaktiviert werden, zum Beispiel können signierte Daten verfälscht werden.
Integrität mittel	■ Daten können nur im eingeschränkten Maße geändert werden. ■ Der Angreifer kann mit der Identität eines Anderen in der beA-Anwendung agieren ■ Eine teilweise Übernahme zentraler Komponenten oder Systeme erscheint möglich. Ein unberechtigter Einblick in vertrauliche Informationen oder ein Ausfall des beA-Systems scheint jedoch nicht möglich. ■ Der Anwender kann Funktionen nutzen oder missbrauchen, zu denen er nicht berechtigt ist.
Integrität niedrig	■ Integrität ist nicht betroffen oder die Änderungen haben keine oder kaum Konsequenzen für den Betrieb auf dem Zielsystem. ■ Es enstehen keine unmittelbaren Konsequenzen für andere Systemkomponenten. ■ Ein System stellt kein attraktives Angriffsziel dar, da der mögliche Gewinn aus einer Integritätsstörung gering oder gar nicht erkennbar ist.

Tabelle 5: Einstufung Verfügbarkeit

Einstufung zum Schutzziel	Beispiele für Bedrohungen
Verfügbarkeit hoch	■ Das beA-System steht vollumfänglich nicht zur Verfügung (Komplettausfall des primären Dienstes). ■ Allen Teilnehmern ist es vorübergehend nicht möglich, Nachrichten entgegenzunehmen oder zu versenden.
Verfügbarkeit mittel	■ Einzelnen Teilnehmern ist es vorübergehend nicht möglich, Nachrichten entgegenzunehmen oder zu verwenden. ■ Es bestehen alternative Kommunikationswege bzw. Alternativen zur Erlangung von Informationen.
Verfügbarkeit niedrig	■ Nur eine einzelne Komponente oder Teilfunktion des beA ist betroffen. Die grundlegenden Funktionalitäten zum Empfang und Versand von Nachrichten sind jedoch nicht beeinträchtigt.

2.3.3 Bestimmung des Risikos

Das Risiko wird aus der Ausnutzbarkeit und der Bedrohung abgeleitet. Das Risiko kategorisiert den statistischen Erwartungswert für eintretende Schäden, der sich gemäß den Regeln der Statistik aus dem Produkt der Eintrittswahrscheinlichkeit eines Schadens und dem Umfang dieses Schadens bestimmt. Die Eintrittswahrscheinlichkeit ist durch den Faktor Ausnutzbarkeit, der Umfang des Schadens durch den Faktor Bedrohung bewertet. Das sich daraus ergebende Risiko wird in drei Risikostufen eingeordnet:

A-Betriebsverhindernde Schwachstelle
Die Behebung vor Wiederinbetriebnahme wird dringend empfohlen.

B-Betriebsbehindernde Schwachstelle
Eine Behebung sobald wie möglich wird empfohlen.

C-Sonstige Schwachstelle
Lediglich unerhebliche Auswirkungen auf den Betrieb sind zu erwarten, eine Behebung wird empfohlen, soweit dies mit verhältnismäßigem (am möglichen Schaden bemessenen) Aufwand möglich ist.

Die Begrifflichkeiten entsprechen der Kategorisierung von Systemfehlern im Fehlerbehandlungsprozess des beA. Mit der Einordnung von Schwachstellen in die Risikostufen ist eine Priorisierung ihrer Behebung verbunden, die dem Ausmaß des Risikos entspricht.

Die Einstufung des Risikos anhand der Bewertung für Ausnutzbarkeit und Bedrohung in betriebsverhindernd, betriebsbehindernd und sonstiges leitet sich aus der nachfolgenden Grafik ab. Der Einstufung liegen Erfahrungswerte des Gutachters sowie eine vergleichbare Einstufung aus dem Standard 200-3 Risikomanagement des BSI (Version 1.0, S. 27) zugrunde. Dabei wurden Risiken für die Vertraulichkeit und Integrität als bedeutsamer angesehen, da hier unmittelbar und ohne nachträgliche Abhilfe die Kommunikation der beA-Anwender betroffen ist, während bei einer Einschränkung der Verfügbarkeit alternative Kommunikationswege und Möglichkeiten der Abhilfe (z.B. Wiedereinsetzung in den vorherigen Stand) zur Verfügung stehen.

Tabelle 6: Bewertung des Risikos

	Ausnutzbarkeit hoch	Ausnutzbarkeit mittel	Ausnutzbarkeit niedrig
Bedrohung der Schutzziele			
Vertraulichkeit hoch	A	A	B
Vertraulichkeit mittel	A	B	C
Vertraulichkeit niedrig	B	C	C
Integrität hoch	A	A	B
Integrität mittel	A	B	C
Integrität niedrig	B	C	C
Verfügbarkeit hoch	A	B	C
Verfügbarkeit mittel	B	C	C
Verfügbarkeit niedrig	C	C	C

Dieses Bewertungsschema wurde spezifisch für die Begutachtung des beA entwickelt. Streng genommen ist die Bestimmung des Risikos über Ausnutzbarkeit und Schaden durch einen erfolgreichen Angriff unvollständig, weil sie die Eintrittswahrscheinlichkeit nur zum Teil berücksichtigt. Die Eintrittswahrscheinlichkeit wird durch die Komplexität des Angriffs, Größe des potentiellen Angreiferkreises (alle, nur beA-Nutzer oder Innentäter) und Motivation der Angreifer (Bereitschaft, die erforderlichen Mittel aufzuwenden und Risiken einzugehen, um einen Angriff durchzuführen) bestimmt. Das beschriebene Bewertungsschema berücksichtigt die Komplexität des Angriffs und die Größe des potentiellen Angreiferkreises und fasst diese im Faktor Ausnutzbarkeit zusammen. Die Motivation der Angreifer wird nur sehr grob berücksichtigt, in dem die Ausnutzbarkeit für Innentäter deutlich niedriger eingeordnet wird, als sie es rein technisch gesehen ist, weil sie im Kontext des beA eine schwer schätzbare Größe ist. Sie hängt beim beA ganz wesentlich davon ab, welchen Nutzen für sich selbst potentielle Angreifer z.B. aus der Einsichtnahme in vertrauliche Nachrichten im elektronischen Rechtsverkehr ziehen können. Darüber liegen keine Erfahrungswerte vor.

2.4 Maßnahme

Der Bereich **Maßnahme** beschreibt Maßnahmen, die getroffen werden könnten, um die Schwachstelle zu beseitigen. Die Maßnahmen stellen lediglich mögliche Lösungen dar, und sollen belegen, dass die Schwachstelle beseitigt werden kann. Die Notwendigkeit und Priorität der Schwachstellenbehebung hängt aber nur von der bereits beschriebenen Risikoeinstufung ab.

2.5 Angaben zum Status der Schwachstellenbehebung

Der Status zur Schwachstelle beschreibt den aktuellen Stand, ob die Schwachstelle bereits gutachterlich verifiziert behoben wurde). Dabei gelten die nachfolgenden Definitionen:

- „-“

  Eine Bearbeitung der Schwachstelle durch den Betreiber liegt nicht vor oder es wurde noch kein erneuter Test durch den Gutachter (ReTest) zur Schwachstelle durchgeführt.

- verifiziert: Schwachstelle behoben

  Die bemängelte Schwachstelle konnte nicht mehr nachgewiesen werden bzw. es wurden aus Sicht des Gutachters adäquate Sicherheitsmaßnahmen ergriffen. Die Schwachstelle wird somit zum Stichtag als vollständig behoben angesehen.

- verifiziert: Schwachstelle nicht behoben

  Bei der Überprüfung, ob die ursprüngliche erkannte Schwachstelle beseitigt wurde, wurde die Schwachstelle erneut vorgefunden bzw. die vorgenommenen Verbesserungen wurden als nicht ausreichend eingestuft.

3 Detailergebnisse der Penetrationstests

In den nachfolgenden Abschnitten wird nun zunächst der genaue Analysegegenstand des Gutachtens beschrieben. Dazu wird die gesamte Systemumgebung im beA-Kontext erläutert und die dazugehörigen Schnittstellen kurz beschrieben. In dem Kapitel „Rahmenbedingungen und Abgrenzung“ werden sowohl allgemeine, im Rahmen von Penetrationstests als auch spezifische Abgrenzungen in Bezug auf den beA-Kontext vorgenommen.

Nach dem Kapitel zur Methodik und Vorgehensweise, in dem die allgemeine Vorgehensweise bezüglich der Penetrationstests beschrieben wird, werden in einer Übersichtstabelle alle Schwachstellen der Kategorien A und B aufgeführt.

Diese Schwachstellen werden anschließend in dem Detailkapitel erläutert und bezogen auf das definierte Verfahren zur Schwachstellenbewertung beschrieben. Die als Kategorie C eingestuften Schwachstellen werden abschließend zusammengefasst in einer kompakten Tabelle aufgeführt.

3.1 Beschreibung des Analysegegenstandes

Das besondere elektronische Anwaltspostfach, kurz beA, ist ein über das Internet erreichbarer Systemverbund, der einen Austausch von gesicherten Nachrichten zwischen registrierten Benutzern.

Um den Dienst zum Senden und Empfangen gesicherter Nachrichten nutzen zu können, werden sowohl eine lokale Java-Anwendung, ein Webbrowser sowie eine beA-Karte mit dazugehöriger PIN benötigt.

Wie in Abbildung 1 dargestellt, besteht das beA-Zentralsystem aus verschiedenen Komponenten bzw. Bereichen. So interagiert der Benutzer entweder mit der beA-Client-Security oder mit einer Kanzleisoftware. Weiterhin gibt es den, in der Grafik im oberen Bereich abgebildeten Bereich der Kammern, sowie rechts den Bereich der mit dem beA interagierenden Justizsysteme.

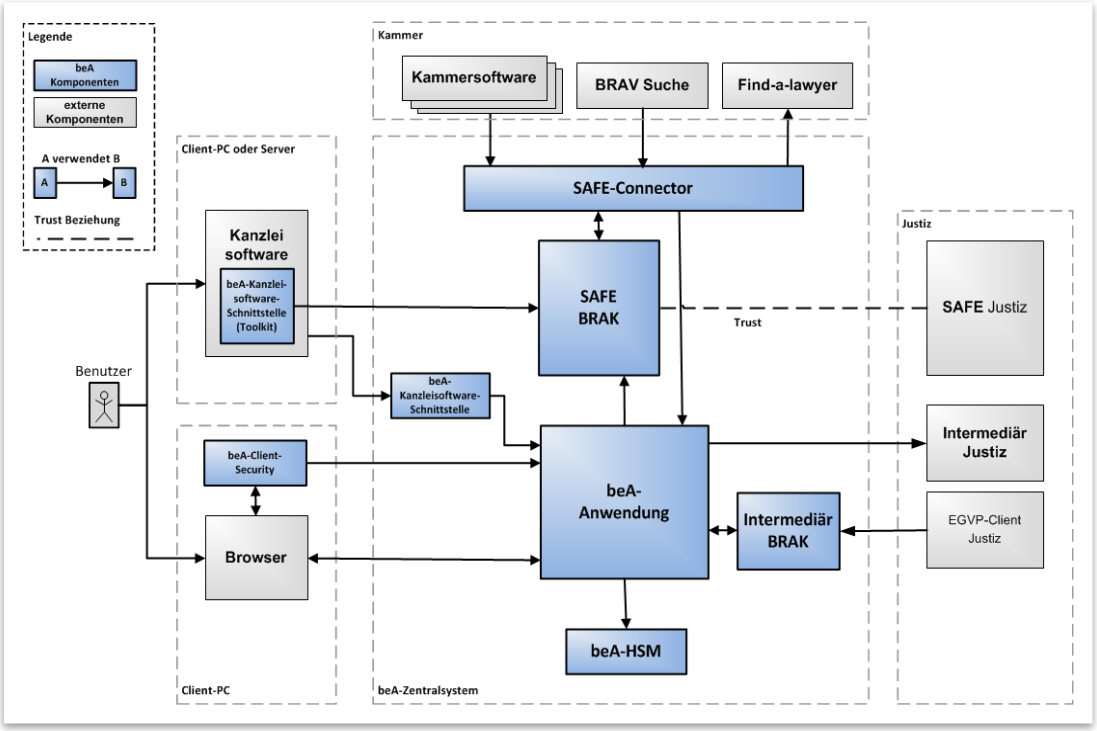

Abbildung 1: Externe Architektur des beA-Zentralsystem

Zur Übersicht werden nun sowohl externen Schnittstellen als auch die allgemeinen relevanten Komponenten kurz erläutert.

beA-Client-Security

Die beA-Client-Security ist eine Anwendung, die als lokale Java-Anwendung auf einem Benutzersystem installiert wird. Sie besteht aus dem Nachrichtenformatmodul, dem Governikus-Signer und dem Krypto-Modul. Die Anwendung kommuniziert über HTTPS mit den Servern der beA-Anwendung. Auf dem lokalen Rechner stellt sie einen Secure-Websocket Dienst bereit. Die Anwendung kommuniziert mit einer Benutzer-Smartcard über das PC/SC Protokoll. Die Kommunikation zwischen verschiedenen Modulen der beA-Client-Security findet über Java-native Schnittstellen statt.

beA-Anwendung

Die beA-Anwendung ist eine Webanwendung. Der Dienst wird in einem JBoss-Applikationsserver betrieben und unterstützt den Download der beA-Client-Security, die Verwaltung von Postfächern, Benutzern und Nachrichten und das Aktualisierungsverfahren der beA-Client-Security. Die beA-Anwendung ist die eigentliche Benutzeroberfläche. Der Browser kommuniziert mit der beA-Anwendung über HTTPS. Der Austausch von Daten erfolgt entweder mit allgemeinen GET- und POST-, oder mit JSON-formatierten REST-Anfragen. Innerhalb der Webapplikation kommunizieren Javascript-Module mit der beA-Client-Security über den lokalen Websocket.

Webservice Kanzleisoftware

Bei dem System handelt es sich um einen Webservice zur Nutzung des beA-Postfaches. Der Dienst benötigt ein gültiges Client-Zertifikat. Der Dienst kann verwendet werden, um die Funktionalitäten der beA-Client-Security in einer eigenständigen Anwendung zu implementieren.

Webservice Kanzlei ⇔ SAFE BRAK

Bei dem System handelt es sich um einen SAML-Webservice zur Nutzung des beA-Postfaches. Für die Anbindung von Kanzleisoftwareprodukten wird eine Webservice-Schnittstelle zur Verfügung gestellt. Dieser Webservice ist mittels einer HTTPS-Client-Authentisierung abgesichert und kann somit nur von freigegebener Kanzleisoftware angesprochen werden. Die benötigten Funktionen der beA-Anwendung für die Nutzung durch die Kanzleisoftware werden über diese Schnittstelle bereitgestellt. Der Service erwartet eine korrekt formulierte Nachricht, da er sonst ausschließlich mit Fehlernachrichten antwortet

SAFE Justiz ⇔ SAFE BRAK

Die SAFE BRAK stellt einen Webservice für die SAFE Justiz zur Verfügung. Über diesen angebotenen Dienst können Informationen zu Identitäten aus einer Identitätsdatenbank innerhalb der SAFE BRAK gesucht werden.

Webservice OSCI ⇔ Intermediär BRAK

Der Intermediär BRAK wird für die Anbindung des besonderen Anwaltspostfachs beA an die EGVP/OSCI-Infrastruktur der Justiz genutzt. Der Webservice dient zur kryptographisch abgesicherten Kommunikation zwischen der Justiz und der BRAK. Hierbei kommt OSCI als Protokoll zum Einsatz.

Kammersoftware

Bei dem System handelt es sich um einen User-Provisioning-Mechanismus, der durch einen HTTP-Upload von CSV-Dateien realisiert wird. Der Dienst verlangt ein Client-Zertifikat. Der Untersuchungsgegenstand umfasste auch den zugehörigen Webservice

Webportal BRAV-Suche

Bei dem System handelt es sich um eine webbasierte Suchfunktion für Rechtsanwältinnen und Rechtsanwälte. Die Suchmaske ist nicht von einer vorherigen Anmeldung oder sonstiger Authentisierung gegenüber dem System abhängig sind.

Webservice Find a Lawyer

Bei dem System handelt es sich um einen Webservice zum Suchen von Anwälten in einer Datenbank des SAFE BRAK über den SAFE-Connector. Der Service verlangt ein Clientzertifikat.

Kanzleisoftware / beA-Client-Security ⇔ Webservice OSCP Relay

Bei dem System handelt es sich um einen Webservice mit OCSP Relay Funktionalität. Der Webservice dient zur Statusüberprüfung von Zertifikaten und zum Extrahieren von Zertifikatinformationen. Der Service ist ohne Authentifizierung nutzbar.

Webservice BNoTK Postfach ⇔ beaPostfach

Bei dem System handelt es sich um einen Webservice zum Abruf der öffentlichen Verschlüsselungszertifikate von Postfächern der Postfacherstellung. Für den Aufruf der Schnittstelle wird von der beA-Anwendung unter Einbindung der HSM ein Zertifikatsrequest erstellt und zusammen mit der SAFE-ID des Postfachs an die Schnittstelle übermittelt. Die Schnittstelle liefert anschließend asynchron das signierte Verschlüsselungszertifikat zurück. Der Service verlangt ein Clientzertifikat.

Webservice BNoTK Antragsportal ⇔ beA

Bei dem System handelt es sich um einen Webservice zur Versorgung des Kartenanbieters mit Adressdaten. Diese Daten werden zur Erstellung der beA-Karte verwendet. Der Kartenanbieter fragt bei der beA-Anwendung Daten mittels SAFE-ID an, welche dann Adressdaten von SAFE BRAK anfordert und diese an den Kartenanbieter zurücksendet. Der Service verlangt ein gültiges Clientzertifikat.

Webportal XWIKI

Bei dem System handelt es sich um ein Webportal zur Bereitstellung von statischen Informationsseiten bzw. Anleitungen rund um die Verwendung des beA für die beA-Benutzer.

Übersicht der externen Schnittstellen im beA

In Tabelle 7 sind die während der Analysen geprüften Software-Versionen der beA-Komponenten aufgeführt. Die hier aufgeführten externen Schnittstellen spiegeln den Gutachtergegenstand im Bereich der Penetrationstest wieder. Dabei wird die Kommunikationsrichtung als Kommunikationspartner aufgeführt.

Tabelle 7: Externe Schnittstellen und analysierte Versionen im beA

Kommunikationspartner A	Kommunikationspartner B	Analysierte Versionen
-	beA-Client-Security	v3.1.3.6 v3.1.3.7 (ReTests)
Browser	beA-Anwendung	v2.0.10 v2.1.X v2.1.1 (ReTests)
Kanzleisoftware	beA-Kanzleisoftware-Schnittstelle	v2.1.X (v2.1.1 (ReTests)

Kommunikationspartner A	Kommunikationspartner B	Analysierte Versionen
Kanzleisoftware	SAFE BRAK	v2.1.X (v2.1.1 (ReTests)
SAFE Justiz	SAFE BRAK	v2.1.X (v2.1.1 (ReTests)
OSCI-Empfang	Intermediär BRAK	v2.1.X v2.1.1 (ReTests)
Kammersoftware	SAFE-Connector	v2.1.X v2.1.1 (ReTests)
Browser	BRAV-Suche	v2.1.X v2.1.1 (ReTests) v2.1.1.1 (ReTests)
Browser	Find-a-lawyer	v2.1.X v2.1.1 (ReTests)
Kanzleisoftware / beA-Client-Security	OCSP Relay Service	v2.1.X v2.1.1 (ReTests)
BNotK Postfach-Zertifikatservice	beA Postfach-zertifikatschnittstelle	v2.1.X v2.1.1 (ReTests)
BNotK Antragsportal	beA Adressdatenschnittstelle	v2.1.X v2.1.1 (ReTests)
Browser	beA Xwiki	v2.1.X v2.1.1 (ReTests)

3.2 Rahmenbedingungen und Abgrenzung

Ein Penetrationstest muss immer als Betrachtung zu einem Stichtag aufgefasst werden. Die zu diesem Zeitpunkt bekannten Schwachstellen und Angriffstechniken werden genutzt. Aussagen über die Zukunft lassen sich jedoch nicht treffen. Demzufolge kann ein System, bei dem keine Schwachstelle gefunden wurde, bereits kurze Zeit später durch eine neu entdeckte Schwachstelle oder neue Angriffsverfahren angreifbar werden. Auch Änderungen von Systemeinstellungen in dessen Kontext der Prüfgegenstand läuft, können positive oder negative Auswirkungen auf die Systemsicherheit haben

3.3 Methodik und Vorgehensweise

Ausgangspunkt für die Festlegung des für die Penetrationstest relevanten Prüfgegenstände ist die Perspektive, einem aus dem Internet agierender Angreifer (Greybox-Ansatz). Weitere Angriffsszenarien werden durch die durchgeführten Quelltext-Analysen und die konzeptionelle Analyse ergänzt (Whitebox-Ansatz). Zu dem genannten Ausgangspunkt gehören auch Angreifer, welche einen einfachen Zugang zum beA-System mittels valider beA-Karte und dazugehöriger PIN besitzen. Der

Analysegegenstand ergibt sich somit primär aus den im Internet verfügbaren externen Schnittstellen des gesamten beA-Systems.

Der Penetrationstest wurde nach folgendem Ablauf durchgeführt:

- Einarbeitung des Analysten in die Dokumentenbasis
- Einrichtung der Analyseumgebung
- Durchführung der Analysen (einschließlich der Verifikation der Behebung bereits auf andere Weise bekanntgewordener Schwachstellen)
- Dokumentation, Auswertung und Kommunikation von Analyseergebnissen
- Überprüfung behobener Schwachstellen

Zunächst wurde die mögliche Angriffsfläche der Anwendung und ihre Kommunikationskanäle evaluiert. Hierbei wurde das Angreifermodell „externer Angreifer“ zugrunde gelegt, welches lokalen Zugriff auf ein beA-Client-Security-System, sowie mögliche Schadsoftware bzw. konkreter von Angreifern eingerichtete Hintertüren auf dem System ausschließt. Ein „externer Angreifer“ kann hier sowohl ein aus dem Internet agierender Angreifer als auch ein im beA-System registrierter Benutzer sein.

Auf Basis des zugrunde gelegten Angreifermodells wurden insbesondere die TLS-geschützten Kommunikationskanäle zur beA-Anwendung, sowie der Zugriff auf den lokalen Websocket über den Client-Browser als mögliche Angriffsflächen identifiziert. Die Überprüfung eines möglichen Zugriffs bzw. die Manipulation lokaler Kommunikation, wurde auf die Steuerungsmöglichkeiten der Websocket-Schnittstelle fokussiert. Diese muss primär über den Client-Browser als Schnittstelle für externe Kommunikation zur beA-Anwendung ansprechbar sein. Der Browser fungiert in dieser Architektur sowohl für die Bedienung der Web-Anwendung durch den Benutzer, als auch für die Steuerung der beA-Client-Security.

In dem nächsten Schritt der Penetrationstests wurden ergänzend zum beA-Kernsystem, wie es sich für Benutzer des beA darstellt, weitere externe Schnittstellen und Portale untersucht, die für den technischen Betrieb der Infrastruktur eingerichtet sind. Hierzu zählen unter anderem: verschiedene Webservices (SOAP und REST), ein Client für Datenexporte (Kammersoftware), sowie Webportale für die Bereitstellung von Hilfeseiten oder die Suche im Bundesrechtsanwalts-Verzeichnis (BRAV).

Die Webportale und Webservices wurden hierbei angelehnt an den OWASP-Standard auf Schwachstellen hin untersucht, wobei erneut hauptsächlich das Angreifermodell „externer Angreifer“ zugrunde gelegt wurde. Ein „externer Angreifer“ kann hier sowohl ein aus dem Internet agierender Angreifer als auch ein im beA-System registrierter Benutzer sein. Bei der Analyse wurde sowohl das technische, als auch das logische Missbrauchspotenzial der jeweiligen Schnittstellen bzw. Dienste geprüft.

3.4 Übersicht der Schwachstellen

In der nachfolgenden Tabelle werden alle Schwachstellen zum Bereich der Penetrationstests vorab dargestellt. Die A und B Schwachstellen, werden in den nachfolgenden Bereichen detailliert beschreiben. Die Tabelle benennt sowohl die jeweils betroffene Komponente als auch den Behebungsstatus der Schwachstelle zum Stichtag des Abschluss der Analyse. Die Spalte „Einstufung“ benennt die Einstufung des mit der Schwachstelle verbundenen Risikos gemäß Beschreibung in Kapitel 2.

Tabelle 8: Schwachstellenübersicht Penetrationstests

Komponenten	Schwachstellen	Einstufung	behoben
beA-Anwendung	Nicht autorisiertes File-Sharing	A	J
beA-Anwendung	Auslesen von Metadaten dritter Nachrichten	A	J
Kanzleisoftware / beA-Client-Security ⇔ Webservice OSCP Relay	Modifikation von signierten Nachrichten	A	-
beA-Client-Security	Veraltete Softwareelementen	A	-
beA-Anwendung	Veraltete Javascript-Bibliotheken in der beA-Anwendung	B	-
Kammersoftware Webservice	Überschreiben von Dateien	B	-
beA-Anwendung	SessionID als GET Parameter in der URL	B	-
beA-Anwendung	Transportverschlüsselung der beA-Anwendung Client-TLS-Renegotiation	B	J
beA-Client-Security	Transportverschlüsselung der beA-Client-Security: Client-TLS-Renegotiation	B	J
beA-Client-Security	Transportverschlüsselung der beA-Client-Security: Logjam	B	J
beA-Anwendung	Detaillierte Fehlermeldungen der Webapplikationsfirewall	B	
beA-Anwendung	Schwache Lock-Out-Mechanismen in der beA-Anwendung	B	J
beA-Anwendung	Qualität der genutzten Session-Cookies	B	-
beA-Anwendung	Automatisches Ausführen und öffnen von Dateien	B	-
Webservice OSCI ⇔ Intermediär BRAK	Modifikation von signierten XML-Nachrichten	B	-
beA-Client-Security	Innerhalb den Logdateien stehen Informationen zur REST Schnittstelle der beA-Anwendung	B	-
Kammersoftware	Nicht konsistente Zertifikatsprüfung	B	-

Komponenten	Schwachstellen	Ein-stu-fung	behoben
Webportal XWIKI	Die REST-API des Wikis ist öffentlich erreichbar und stellt teilweise sensible Informationen bereit, die für den Anwendungszweck des Wikis nicht benötigt werden.	C	
Webportal XWIKI	Das Portal ist anfällig für eine Reflected-XSS-Schwachstelle, die jedoch nicht ohne weiteres auszunutzen ist.	C	
Webportal BRAV-Suche	Das Webportal hat eine XSS-Schwachstelle.	C	
Webservice Kanzlei-SAFE BRAK	Der Webservice gibt Fehlerbezeichnungen mit Paketnamen und Stack-trace an den Client weiter, wodurch Rückschlüsse auf die Architek-tur möglich sind.	C	
beA-Client-Security	In den Logdateien der lokal installierten beA-Client-Security des Benutzers findet sich die Session-ID der Anwendung.	C	
beA-Anwendung	Die Analyse des Datenverkehrs ergab, dass in einem Großteil der betrachteten Seiten mit vertraulichen Inhalten der Browser-Cache nicht deaktiviert wird.	C	
beA-Anwendung	Die Passwort-Policy für den Mitarbeiterlogin ist nicht ausreichend, da kein Brute-Force Schutz vorhanden ist.	C	J
beA-Anwendung	Das Passwortfeld auf der Anmeldeseite „Registrierung beA Benutzer“ begrenzt die Eingabe eines Passwortes auf 8 Zeichen.	C	J
beA-Anwendung	An mehreren Stellen innerhalb der Web-Applikation können Fehlermeldungen ausgelöst werden.	C	
Webservice Attribute-Service VAS => SAFE BRAK	Der Webservice gibt Fehlerbezeichnungen aus Java an den Client weiter, die Rückschlüsse auf die Architektur zulassen.	C	
RAK Client	Passphrasen werden im Klartext gespeichert.	C	
Kammersoftware Endpunkte	Der Webserver gibt per HTTP-Server-Header seine genaue Version preis.	C	
Webservice Find a Lawyer	Der Webservice gibt im Response-Header die Server-Software und -Versionsnummer über das Server-Response-Header-Feld bekannt.	C	
Find a Lawyer	Der Webservice gibt Fehlerbezeichnungen aus Java an den Client weiter, die Rückschlüsse auf die Architektur zu lassen.	C	
Webservice BNotK Postfach-beA-Postfach	Der Webservice gibt im Response-Header Server Software und Versions-nummer bekannt über das Server-Response-Header-Feld.	C	

Komponenten	Schwachstellen	Ein-stu-fung	behoben
Webservice BNoTK Postfach-beA-Postfach	Der Webservice gibt Fehlerbezeichnungen aus Java an den Client weiter, die Rückschlüsse auf die Architektur zu lassen.	C	
Xwiki	Der Webserver gibt auf Fehlerseiten seine genaue Version und Stack-Traces preis.	C	
Xwiki	Es konnte eine Benutzerlogin-Maske öffentlich abgerufen werden, die durch einen Angreifer ausgenutzt werden könnte und keinen Schutz vor Brute-Force-Angriffen oder lokaler Pass-wort-Speicherung bietet.	C	
Xwiki	Auf dem Server konnten Stack-Trace-Meldungen hervorgerufen werden, die ggf. für weitere Angriffe genutzt werden könnten.	C	

3.5 Beschreibung der A-Schwachstellen

In dem nachfolgenden Kapitel werden alle im Bereich der Penetrationstests identifizierten Schwachstellen der Kategorie A der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit des Zielsystems beschrieben. Jede Schwachstelle wird in einem Unterkapitel aufgeführt und die dazugehörige technische Komponente benannt. Die Methodik und Vorgehensweise der Schwachstellenbeschreibung, der Definition der Risikobewertung, der Ausnutzbarkeit der Schwachstelle sowie zur Einstufung der Bedrohungen wurden in Kapitel 2 erläutert.

3.5.1 Nicht autorisiertes File-Sharing

Untersuchungsobjekt	beA-Client-Security und beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle behoben

{S1} Ein im beA-Kontext genutzter Mechanismus kann für nicht autorisierten Austausch von Daten missbraucht werden. Daten können nicht autorisiert auf dem beA-Anwendungsserver abgespeichert und zu einem späteren Zeitpunkt wieder abgerufen werden.

{R1} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle
Um den betroffenen Mechanismus auszunutzen ist folgender Ablauf nötig:

1. Beliebige Anfrage an den Server schicken um SessionID zu erhalten
2. Ticket auf dem Server erstellen

2.1 Mit SessionID Daten auf den Server schicken
2.2 Rückgabe: TicketID
3. Abruf der Daten mittels TicketID

Die Schwachstelle kann aus dem Internet ohne Kenntnis gültiger Zugangsdaten zur beA-Anwendung ausgenutzt werden. Entsprechend hoch ist die Ausnutzbarkeit.

Ausnutzbarkeit: **hoch**

Bewertung der Bedrohung
Der nicht autorisierte Datenaustausch kann eine Vielzahl an Bedrohungen auslösen. Ein Angreifer kann beispielsweise beliebige Daten hochladen und den Server zur Ablage und Verteilung von legalen oder illegalen Inhalten als einfachen Cloud-Dienst nutzen. Die Bedrohung der Integrität ist hoch. Auch ein Upload von Daten mit großem Speicherbedarf wäre denkbar, um die Serverressourcen auszulasten und so die Verfügbarkeit beeinträchtigen.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **niedrig**

{M1} In einer ersten Maßnahme sollte diese Funktion nur authentifizierten Benutzern bereitgestellt werden. Weiterhin sollte das Abspeichern von Daten auch zeitlich begrenzt werden, um die Angriffsfläche bzw. das Missbrauchspotential zu minimieren.

3.5.2 Auslesen von Metadaten fremder Nachrichtenanhängen

Untersuchungsobjekt	beA-Client-Security und beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle behoben

Es konnte festgestellt werden, dass authentifizierte Benutzer über die beA-Client-Security potenziell auf die Metadaten der Anhänge von versendeten Nachrichten anderer Benutzer zugreifen können. Metadaten in diesem Sinne sind bezogen auf eine verschlüsselte Nachricht, die im beA-Kontext versendet wurde. Diese beschreiben beispielsweise Eigenschaften, welche dem Anhang zugrunde liegen. Als Metadaten in diesem Kontext konnten folgende Informationen identifiziert werden (Einsatzzweck der einzelnen Daten spekulativ):

- „*reference*“: [realer Dateiname im Klartext wie z.B. 2011000000-VR16000-12345678_1.pdf oder Klage.pdf]
- „*alias*“: [Entspricht der in der beA-Anwendung im Browser hinterlegte Bezeichnung des Anhangs. Dieser kann Fließtext wie „falsche Zeugenaussage Person X“ sein]
- „*type*“: ATTACHMENT oder STRUKTURDATENSATZ [Zweck zum aktuellen Zeitpunkt nicht bekannt]

- „*data*“: [nicht lesbarer Inhalt, mit hoher Wahrscheinlichkeit tatsächlicher verschlüsselter Anhang]
- „*key*“: [variable längere Zeichenfolge]
- „*sizeKB*“: 1 [Größe des Anhangs in KB]
- „*hashValue*“: [Hash-Wert zur Überprüfung der Integrität]
- „*sizeEncryptedKB*“: null [Zweck zum aktuellen Zeitpunkt nicht bekannt]


{"reference":"test.txt","alias":"Dieser Anhang sollte von Nachname2 erreichbar sein!","type":"ATTACHMENT","data":"y+3HcTwAGYBPYMY66cwTmBCStoPo4xNcvltpKNhT0+g=","key":"DUQqjbS2d7elH4XgRk1u0Ws3sRJhw05OZQqbU5dRvFhhB1B49J UzBpjQhEWYQRMLFyyY1rKiCShtwFvDoU/VB5xGBx1gOOx1dfHjtFj /aStwLNcQEvrHbVth1NnKZFrJWLv8Xcex4jP0EoB4hJu46KnmGPaRx5SdC+Glev32hFfcdBIX376STZBRNWppSt9EpOPV3NIcfRiQdcP5GsANDKonF+Cq9pflDvheI6gLSaoSD1v2b a3oPUUG4uIZdEJ/Sxqujk7g3PpeySzygKRGKrY/kDt7UiTRex4O/vXVooj /rNq7c5Oxk5O5sugj93kDv93cbLjz3MdUzA+XBHbLNQ==","sizeKB":1,"hashValue":"qtwZVcAw9yPp2J7Z1Ia07vWw0caUW+Dda3s0DUKSjsk=","sizeEncryptedKB":nul l}

Abbildung 2: Anhang test.txt


{"reference":"xjustiz_nachricht.xml","alias":null,"type":"STRUKTURDATENSATZ","data":"+A+wMlT/xtysTvXeU1PkFrRHhL0z9+V0kHJQF84zmhVuo5X /iGXJuuumYsyqKI7A4B7SmiSbtmZ3AJKuiFyERxxqNSBhzpkHT4nWv /VjLaI0izX56UNcfTCcalXludMgiL4X35umw0IIbBnvlmpjiYELUz6aHch8Po1e7gy7VtSzyAcbJg+zE+WhNRAmmQ8AAcJC+5onk/4vBOSaVsAzjZd6 /HyVZ7nz3GlIShhICFFILf3c23JIYiWq2Rr6FFwyv7QjFxrX1/T7gkh6UfgULTyvGHpP1Ykdi7k+xDhB+/Cc4c06LFfXzYsAced4lHQRYPO+80Li3J10iz/Jjqz609us /sLw78DlgrO6TZtl88yMt+OljjwcikSBm0gBCup2wNs3bPpKCe+CWvS8bXJz5wNcWAMFxAoD3k+ShqwsTXA37orrOjzuhcA+EzHYkh4qW40oULSI1GwBEFU4h2dMBTDcrJPzGdiRlQKTbTDGsKIAWWnB MxxCu0lLoO/5BHlpzK1gg7v8C3BIgncU8ct7+D2BV09JRm3Mr6WPojyvbp6X3juQWW6DCXS8yee2BbCcS5cr0SQao/LIQxHJkbRpu1hGgcs3SVtiIp2yiIgBpmvb8Q+f4tYLk1pdwUZsOpxz99g0Jau /7uwyomGpqUlufpgf98+sKfJQ1kSFYmW8VnfavmJSc9RSrucceVavaPYRvN9vXmpDcz8SeBzU00MQQr6XYxy+ZGLcqDzUvFDBNEE0Shyw2b1Y2Gt0lIR979t0GKXzoyrmxMvaOBiBQ58ln8LiD0wy1j5 86abuu0cclXDvrViaZe5W5S1sk0sah+cifLlxmBZwcoiXLrTJWhsgPnqR2fFx2wc2wCNi1//3a302+TUMkVDLTUSRWCoPRYGd9I3 /XaZlzFLoRGujwfA22ORaWxtFnlDdPHJLDD8YZAKmoc6go6YmX3AlPGNjBWIGnMKuM3f8utV/MxpVyXB+g+JxQFcE+dSvabbEfVL04RzbWLHUfuzbqCALZerF/LYnATXQtuBwVUdydpXh6iuuk /lWoeoNejMnlAHL9hbKAUh4GrFq+WAXouip8PfbQUJUKOHSWwlp2KumKfda/7bwusiQFUdWk6oVrnYqld5P+k4tlkX014vNECMKjEa0YXpK2kNilu80tA4Y7eK /iFGQ5af2YsMp2hzbYKbpQc7uHisFB98JZuz8c3hKXA0KZfjkh1CrqKEPJFwPDvPKewQfFEnN93VVYd9MyiE5LTnWlgZMKwrnxVp /XvQf27WSYrH20bk0PN49uwFHFYNzK1YOON5dQLVTiWi1SHXTs2OcXuy+/fOUC/qonteBiGugVZyfDKAo/CAJQP2rruqdxtTWhBlWsoO3lVJ5QEmpXWpX+T /kDm9xbyBf1nUAfrvF5i0iO6M+YFVeQtDk1diORx47KVoavUIW5gYJjbWeSgjthwWv0bKcYehW9G9w7NywdRoAhxtPnVuOD4JgTzP0S7rlo1H1Fh8qYeULBEYsEe7Ep2InvgGAr6CdP3A1OvGaPO5A0H /7tZZ9KuYy2tfkAZIQGuFRwY /DSinAFhxGEybeOlSqghS13+T0GRWUrBS9eewRDYPzJ91DWALqndo9Aw8T5tr72KB6imfudJoB9ImuOP6FBv8Zt772TbylhirLC+3xSxTARUYPXb5cVrhofshLucSdKnEbHON6Foj0qfxBauLqtcmZaY izM+boHLBkI+sIyvYyiIgzfdkeGXLHu7jIXX1ZSaPMcFjsRYKeWZZyeiKDBld9nwM2lh3nBB2sBoKiTIODbcSLotRoSkzJIOwl61kwsf04aAr+Xo /39JQsv66MUtgBw390RQVBxUp8KZ9mxfXpZi27msh9+35VEMCY3F0US8Sh6OlwM24G1HMdpXCxgQhqqX0CD0xLoTaER5Uz06QJWM3gSgVhQgUVmrUUTp30a6IlYBeEzcijOn019uKtE05EAFCMCGJrSB nv6/+MxYOcOOzJI8hhI25R9E6NNgoDZnva5BDMZMHufFoa9cOQQYuAzUFoeHTIM2vUrpSmeOyaHI /fTS9ltrBYRRwcGUXWpEMr7JOHYbClyGRikun0K6DCkRXWzVwFXVB3MggSYToACdLYBnzRWAoJBUJU2iJHQr413ZcERO345xuq3N2dSv/EW1bsykT065MnWwWW6OUmnrrrYU8M9Alx /heCP2nKDP9qRqqGZtQSrGSRckzXsoYg5rLV6xVOQe14rk4ycDGRrwbG0k3nYfcsh5RbAFCGTgpgmuS0zyzmvCRHiQd1hXGWPA6cQa /vETnhbKELkcrp1SH42UvF+8YIVB5B+RSZdWQ54ixfBBh0k75YIUmRZONdcx4C95/MuzOxNN/QVSmRq3cn99Bm+QGJGrMMfJr8ZdeZHs8ojvCJWbNK24bavvFcA0gq2tdDMk1uJzYmfmbsM /S6B4yU4qLhci9YOQUxtgItv97fdSh+Oqq0BNbhyKK6VQ5Pc/sblIUMZRqL0tfhKppo2uTxIkBbdwyLcCn936Vf9BKsyUoLLHrcQxxwkoUVVfJCPnF5inTrAzTu /i0PFaF8+SoqRg2BJJNm28gnwDelrERfuHgy2llH/gnTOHf68YE3v53XcoTJx6wRA83L5i8JD2ft21Q+aeogyvlrCv69HznHse8l /gDDwEeWIiRrbJXhFX7L+XlRUT3CEpCZ9Cobx+M7sZ54S9rYE6NpTJeWBzIxiJKVWGjNIX1ohuIWZ680aNFBdhv3REa858ARShUdaIKJtu36KtD4g/IHubUoaPH /W1urqSKzsMFbH7R28EWS8AK8MfOh7CsES2/c1iAkoK0CBUEi4z/Yx4NUfvub1EgTi70GKxD8AvayOoom3StPC3r3YZiPXMxGYd7S8elhGl5CzC8lORgTezOYXpE /crqdO9F5rAFNfdJlBCBj4YZQuMNxum3DG /gx/EL4xKy+5+gtPrIlGGgEjk1iBvgXdAD4195oYSdF3nnpfkHX2IIQ7layW6ZcYnmzsS4LTB+bUT2VxSeo2nsYT3B55ul16BLsF+8zQPCaJcQ5zGqotST+xBFfHN4YXd6VPCwB /Mp/24Qt5HAPjuhTCs8rOKmAr3YAdsyfC48ARmBtrkfSt+mGGLEuIiHTfM4KrFSgTnAKXLi5ejsYeH3ljG8L8+pb3xGQRSl19D9j0TJxF2dQhd0x3TT28j3ONUkVnVBPgKmEYi /OqDA2HCB8MN2SukLEh8KBh2KeAC3l2FK3zjOpG478NqRsFSlropzl2wuN4CS84lHZT7k4teuxSZ24+YfEdmgOeAx6tpPQZV6eGePgzcjVU8F8aXn7iKQTBMwLoKyyPqWdJSbF/M6CmZqv /eObEgBkMOJ2U0M4KqTs+JKg5AUVU47RrbT0R+JJ9UYMZc6p8qvDjro+9Ou/hQglFLQR0UVhAcsFaOUwlsiVGLO5pQ6Gv/elqlM7K67VzxqC2rZ /pau4qwYeZSYDLUcf+Xv4yrfK93FUqbOM7ML3kiIHt1DTl6G6aDX2+dhv0T2LiGi5zz9u3YcjKsDdQXea0koMCtGY0rYNjiGBw26zUJdKP8p5a+SDJqj8D0Dr0IEp /RCmKXggzhS5rhLUcXgQ4cc+E0n4Oq/De4j0jNU=","key":"JceLyypSBnXRyj5bW3v+GUbsByrgtbOOQpRYRPjw7q0yrjLEDr /W5+a7BvWyeryh8SabbZsOdaGnLXbbn+Yb1xVKYTBf5Kb3PTEUfIQ96DBJGCG9OH5JFiEMOw2avMXnXY3ma0kzh2gCWYSyP4xwBmLysN7QpLUjPsW /Ik327IXk0aXBBxJcbS73+5XBjl6pIkhX+kFtpi6R1TlnCMEfOCoF00MSPe7tRv3xNDle1Xb+JfoRMn/DTmqX114SPc9 /Rg95OYrm4mxA19I9Kp9+yFEK9UnK2HT9t5AJer1UOcxisi7CV3nZcVOmEiTeJ/Jc2UC /g8n/vwOKGT8h00i0lQ==","sizeKB":3,"hashValue":"tp8tKq46NX66qqcYq032Js2jztPOxZibvUOf4u9rTXk=","sizeEncryptedKB":null}

Abbildung 3: Anhang xjustiz_nachrict.xml

Wie in Abbildung 2 und Abbildung 3 zu sehen ist, können die genannten Metadaten lesbar im Browser eingesehen werden. Dabei gelten nun die folgenden Rahmenbedingen:

- Angreifer muss in der beA-Anwendung angemeldet sein
- /<Nachrichten_ID>/ muss erraten werden
- /<Dateiname>/ muss erraten werden

{S2} Innerhalb der beA-Anwendung ist es angemeldeten Angreifern möglich, auf die Metadaten von Nachrichtenanhängen anderer Benutzer zuzugreifen. Der Angreifer kann somit seinen eigenen Nutzerkontext innerhalb der beA-Anwendung erweitern.

{R2} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle
Ein in der beA-Anwendung angemeldeter Angreifer kann hier mittels automatisierter Skripte über Nacht bzw. über mehrere Tage versuchen die numerischen IDs der Anhänge und der Dateinamen zu erraten und so bei Erfolg auf die aufgeführten Metadaten zugreifen. Die Ausnutzbarkeit ist hier hoch definiert, da Schwachstelle einfach auszunutzen ist und eine sehr hohe Nutzerzahl potenziell Zugriff auf diese Schwachstelle hat.

Ausnutzbarkeit: **hoch**

Bewertung der Bedrohung
Ein Angreifer kann die Metadaten der Anhänge von fremden Nachrichtenanhängen abrufen. Er kann diese Informationen für weitere Angriffe missbrauchen. Die Vertraulichkeit des verschlüsselten Anhangs selbst ist durch die genannte Schwachstelle nicht bedroht.

Bedrohung Integrität: **mittel**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **niedrig**

{M2} Benutzer sollten, trotz der Verschlüsselung der konkreten Nachrichten- bzw. Dateiinhalte, nur auf Anhänge und dazu gehörige Informationen zugreifen können, die ihrem Konto zugeordnet sind. Es sollte geprüft werden, warum das implementierte Nutzer- und Rollenkonzept an dieser Stelle einen Zugriff nicht verhindert.

3.5.3 Modifikation von signierten Nachrichten

Untersuchungsobjekt	Webservice OSCP Relay => KSW
Schwachstellenstatus	-

{S3} Bei der Verwendung von signierten XML-Nachrichten sind keine Vorsichtsmaßnahmen getroffen worden, um den Inhalt der signierten XML-Nachricht gegen Modifikation zu schützen. Die vorgesehene Signaturprüfung kann umgangen werden, in dem man dem signierten Datenblock einen weiteren mit identischem Namen hinzufügt, der dann der Modifikation offen steht. Dieser Angriff wird Signature-Wrapping genannt.

{R3} Risikobewertung: **A-Betriebsverhindernd**

Der Angriff steht nur einem Innentäter oder erfolgreich eingedrungenen Außentäter zur Verfügung, der Zugriff auf den Übertragungsweg zwischen beA-Anwendung und OCSP-Relay hat. Ist der Zugriff vorhanden, ist die Durchführung des Angriffs einfach.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:
Signierte Nachrichten des OCSP-Relays, die Gültigkeitsauskunft über qualifizierte Signaturzertifikate geben, können unter Ausnutzung der Schwachstelle verfälscht werden mit der Folge, dass der Prüfbericht über eine Nachricht beim Empfänger falsch Auskunft über den Status einer qualifizierten Signatur gibt. Die Bedrohung der Integrität ist daher hoch.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **niedrig**

{M3} Die Referenz des signierten Elements sollte die Lokalität mit abdecken. Z.B. realisierbar mittels einer absoluten XPath-Expression.

3.5.4 Veraltete Softwareelemente

Untersuchungsobjekt	beA-Client-Security
Schwachstellenstatus	-

In der auf dem Computer installierten beA-Client-Security gibt es eine Funktion zum Anzeigen der installierten Third-Party-Bibliotheken. Unter dieser Funktion wird eine größere Liste von Softwarekomponenten aufgeführt. Die folgenden Third-Party-Bibliotheken sind installiert aber nicht aktuell (zum Zeitpunkt der Analyse):

- Apache Commons Code
  Installiert: 1.10
- Apache Commons Compress
  Installiert: 1.4.1
- Apache Commons IO
  Installiert: 2.4
- Apache Commons Lang
  Installiert: 3.0
- Apache Fontbox
  Installiert 2.0.5
- Apache PDFBox
  Installiert: 2.0.5
- Apache Jackson
  Installiert: 2.9.3
- GlassFish Community
  Installiert: 3.1.0
- Apache Log4J
  Installiert: 2.10.0

- Jetty Websocket
  Installiert: 9.4.8
- Apache XML Security
  Installiert: 2.1.0

{S4} Verwendete Softwarebibliotheken bzw. Softwareelemente sind veraltet und enthalten öffentlich bekannte Sicherheitslücken .

{R4} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle
Im Allgemeinen identifizieren und veröffentlichen Softwarehersteller oder auch Sicherheitsforscher regelmäßig Schwachstellen zu verschiedenen Softwareprodukten. Je nach Art der Veröffentlichung, wird auch bereits der Angriffscode zum Ausnutzen der Schwachstelle mitgeliefert.

An jeder Stelle, an der die Softwareelemente genutzt werden und der Angreifer Zugriff hat, kann er versuchen diese anzugreifen. Nicht alle aufgeführten Softwareelemente haben sicherheitsrelevante Updates. Fehlen allerdings sicherheitsrelevante Updates wie für Apache Jackson, kann ein Angreifer diese ausnutzen.

Angriffe können entweder beim Besuchen von Webseiten über einen Browser oder wenn der Angreifer sich bereits eingeschränkt auf dem Benutzersystem befindet durchgeführt werden. .

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung
Bei einem erfolgreichen Angriff kann der Angreifer das System des beA-Nutzers eingeschränkt kompromittieren.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **mittel**

{M4} Alle Softwareelemente für die sicherheitsrelevante Updates verfügbar sind, sollten aktualisiert werden.

3.6 Beschreibung der B-Schwachstellen

In dem nachfolgenden Kapitel werden alle im Bereich der Penetrationstest identifizierten Schwachstellen der Kategorie B der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit des Zielsystems beschrieben. Jede Schwachstelle wird in einem Unterkapitel aufgeführt und die dazugehörige technische Komponente benannt. Die Methodik und Vorgehensweise der Schwachstellenbeschreibung, der Definition der Risikobewertung, der Ausnutzbarkeit der Schwachstelle sowie zur Einstufung der Bedrohungen wurden in Kapitel 2 aufgeführt

3.6.1 Veraltete Javascript-Bibliotheken in der beA-Anwendung

Untersuchungsobjekt	beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle nicht behoben

{S5} Die beA-Anwendung verwendet veraltete Javascript-Bibliotheken (jQuery und Bootstrap) mit bekannten Schwachstellen. Der Angriff zielt auf die Benutzer der beA-Anwendung ab und betrifft nicht die Sicherheit der beA-Anwendung selbst. Zum Zeitpunkt der Analyse konnten die nachfolgenden veralteten Versionen identifiziert werden

JQuery 1.11.3
Bootstrap 3.3.2
.

{R5} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Je nach Einbindung der Javascript-Bibliotheken können erfolgreiche Angriffe durchgeführt werden. Können die Schwachstellen der veralteten Software-Komponenten tatsächlich ausgenutzt werden, kann ein Angreifer beispielsweise einen manipulierten Link auf die bea-brak.de Webseite erstellen und diesen per Nachricht an einen Nutzer der bea-brak.de Seite oder an beliebige andere Nutzer schicken. Klickt der Nutzer auf den manipulierten Link, so wird ihm eine manipulierte Webseite unter der Domain bea-brak.de angezeigt. Auszug zur JQuery Schwachstelle der genannten Version: CVE-2015-9251

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung
Ein Angreifer könnte die Schwachstellen dieser Versionen ausnutzen, um unerwünschte Skripte auf dem Rechner eines Opfers auszuführen. So kann unter der vertrauenswürdigen beA-Domäne Angriffscode hinterlegt werden. Phishing Angriffe können durchgeführt werden.

Bedrohung Integrität: **mittel**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **niedrig**

{M5} Die genannten Software-Bibliotheken sollten aktualisiert werden.

3.6.2 Überschreiben von Dateien

Untersuchungsobjekt	Client der Regionalen Anwaltskammern (Kammersoftware)
Schwachstellenstatus	-

Sowohl der Upload als auch der Download von CSV-Dateien an dem zugehörigen Webservice des RAK-Client ist anfällig für sog. Path-Traversal Angriffe. Bei diesen Angriffen wird die Funktionalität zum Ablegen von Dateien missbraucht. So kann bei einem Download der Speicherort der Datei von einem Angreifer festgelegt werden. Bei einem Upload der CSV-Datei schien es während der Analyse auch serverseitig möglich, den Speicherort zu manipulieren. Dies konnte während der Analyse allerdings nicht final verifiziert werden.

{S6} Sowohl der Upload als auch der Download von CSV-Dateien an dem zugehörigen Webservice des Kammersoftware ist anfällig für Path-Traversal Angriffe. .

{R6} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Clientseitig: Kann sich ein Angreifer per Man-In-The-Middle in die Kommunikation einschalten, so kann er eingeschränkt Daten innerhalb des Client-Dateisystems schreiben und so weitere Angriffe auf den Client durchführen.

Serverseitig: Der Angreifer benötigt den Kammersoftware, welcher nur den regionalen Anwaltskammern vorbehalten ist sowie ein dazugehöriges Client-Zertifikat. Ist der (nicht verifizierte) Path-Traversal serverseitig erfolgreich, so kann der Angreifer das Zielsystem massiv manipulieren.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung
Clientseitig: Bei einem erfolgreichen Angriff kann der Angreifer versuchen das Clientsystem zu kompromittieren, um so Kontrolle über das Clientsystem zu erhalten und weitere Angriffe durchzuführen.

Serverseitig: Bei einem erfolgreichen Angriff kann der Angreifer den betroffenen Server kompromittieren, Daten überschreiben oder möglicherweise eingeschränkte Kontrolle über das Zielsystem erhalten.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **niedrig**

{M6} Die Content-ID sollte keinen Pfadwechsel erlauben und auf die Kammer des Clients beschränkt werden. Das serverseitige erfolgreiche Ausnutzen der Schwachstelle wurde nicht verifiziert, sollte aber trotzdem in jedem Falle überprüft werden

3.6.3 Session-ID als GET Parameter in der URL

Untersuchungsobjekt	beA-Client-Security und beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle nicht behoben

{S7} Innerhalb des normalen Nutzungsverlaufs der beA-Client-Security mit der beA-Anwendung wird die Session-ID als GET-Argument innerhalb der URL an die beA-Anwendung übermittelt.

{R7} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Angreifer könnten durch Auslesen der Sitzungsinformationen, z.B. aus dem Log eines Webproxys mit TLS-Interception oder aus lokalen Debug-Logdaten, eingeschränkt die Identität des betroffenen Benutzers in der beA-Anwendung übernehmen.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung
Durch erfolgreiches Auslesen der Sitzungsinformationen kann die betroffene Identität eingeschränkt von dem Angreifer angenommen werden. Alle Mechanismen innerhalb der beA-Anwendung, welche ohne die beA-Karte nutzbar sind, können von dem Angreifer durchgeführt werden. Die Bedrohung der Integrität ist hoch, da der Angreifer wie genannt eingeschränkt mit der Identität des betroffenen Nutzers agieren kann und beispielsweise Nachrichten verschicken kann. Die Verfügbarkeit der beA-Anwendung kann dadurch gestört werden, dass eine aktive Sitzung von dem Angreifer übernommen und somit die allgemeine Prozessintegrität gestört wird.
Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **niedrig**

{M7} Die Exposition der Sitzungsinformationen sollte möglichst gering sein, um Session-Hijacking zu verhindern. Die Sitzungsinformationen sollten nicht als Teil der URLs übertragen werden.

3.6.4 Transportverschlüsselung der beA-Anwendung: Client-TLS-Renegotiation

Untersuchungsobjekt	beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle behoben

Verfahren zur Verschlüsselung von Inhalten veralten und müssen an neue Gegebenheiten angepasst werden. Es wurde geprüft, ob in der Kommunikationsverbindung von dem Browser zur beA-Anwendung aktuelle Algorithmen verwendet werden und ob sonstige Schwachstellen vorhanden sind. Die hier betrachtete

Transportverschlüsselung hat nichts mit der Verschlüsselung oder Kryptographie der im beA-Kontext verschlüsselt übertragenen Nachrichten oder Anhänge zu tun.

{S8} Der beA-Anwendungsserver bietet Client-TLS-Renegotiation an.

{R8} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Um den Angriff durchzuführen muss der Angreifer sich zwischen die Kommunikationspartner schalten können. Dies kann er beispielsweise, wenn er bereits auf einem dritten Weg (eingeschränkt) Zugriff auf den Benutzer-Client des Anwenders hat. Ein weiteres Szenario wäre ein Man-In-The-Middle Angriff innerhalb eines öffentlich zugänglichen WLAN.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung
Durch einen erfolgreichen Man-In-The-Middle Angriff und somit das Auslesen der Sitzungsinformationen kann die betroffene Identität eingeschränkt von dem Angreifer angenommen werden. Alle Mechanismen innerhalb der beA-Anwendung, welche ohne die beA-Karte nutzbar sind, können von dem Angreifer durchgeführt werden. Die Bedrohung der Integrität ist hoch, da der Angreifer wie genannt eingeschränkt mit der Identität des betroffenen Nutzers agieren und beispielsweise Nachrichten verschicken kann. Die Verfügbarkeit der beA-Anwendung kann überdies gestört werden, da eine aktive Sitzung von dem Angreifer übernommen wird. Die allgemeine Prozessintegrität wird somit gestört.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **niedrig**

{M8} Die Konfiguration „secure client-initiated regenotiation“ sollte auf dem Server deaktiviert werden.

3.6.5 Transportverschlüsselung der beA-Client-Security: Client-TLS-Renegotiation

Untersuchungsobjekt	beA-Client-Security
Schwachstellenstatus	verifiziert: Schwachstelle behoben

Es wurde geprüft, ob in der Kommunikationsverbindung von dem Browser zur beA-Client-Security aktuelle Algorithmen verwendet werden und ob sonstige Schwachstellen vorhanden sind. Die hier betrachtete Transportverschlüsselung hat nichts mit der Verschlüsselung oder Kryptographie der im beA-Kontext verschlüsselt übertragenen Nachrichten oder Anhänge zu tun.

{S9} Die beA-Client-Security bietet Client-TLS-Renegotiation an.

{R9} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Um den Angriff durchzuführen muss der Angreifer sich zwischen die Kommunikationspartner schalten können. Dies kann er beispielsweise, wenn er bereits auf einem dritten Weg (eingeschränkt) Zugriff auf den Benutzer-Client des Anwenders hat.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung
Durch einen erfolgreichen Man-In-The-Middle Angriff und somit das Auslesen der Sitzungsinformationen kann die betroffene Identität eingeschränkt von dem Angreifer angenommen werden. Alle Mechanismen innerhalb der beA-Anwendung, welche ohne die beA-Karte nutzbar sind, können von dem Angreifer durchgeführt werden. Die Bedrohung der Integrität ist hoch, da der Angreifer wie genannt eingeschränkt mit der Identität des betroffenen Nutzers agieren und beispielsweise Nachrichten verschicken kann. Die Verfügbarkeit der beA-Anwendung kann überdies gestört werden, da eine aktive Sitzung von dem Angreifer übernommen wird. Die allgemeine Prozessintegrität wird somit gestört.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **niedrig**

{M9} Die Konfiguration „secure client-initiated regenotiation“ sollte auf dem Server deaktiviert werden.

3.6.6 Transportverschlüsselung der beA-Client-Security: Logjam

Untersuchungsobjekt	beA-Client-Security
Schwachstellenstatus	verifiziert: Schwachstelle behoben

Verfahren zur Verschlüsselung von Inhalten veralten und müssen an neue Gegebenheiten angepasst werden. Es wurde geprüft, ob in der Kommunikationsverbindung von dem Browser zur beA-Client-Security aktuelle Algorithmen verwendet werden und ob sonstige Schwachstellen vorhanden sind. Die hier betrachtete Transportverschlüsselung hat nichts mit der Verschlüsselung oder Kryptographie der im beA-Kontext verschlüsselt übertragenen Nachrichten oder Anhänge zu tun.

{S10} Der verwendete lokale Webserver der beA-Client-Security ist für den Logjam-Angriff anfällig.

{R10} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Um den Angriff durchzuführen zu können muss der Angreifer sich zwischen die Kommunikationsverbindung schalten können. Dies kann er beispielsweise, wenn er bereits auf einem dritten Weg (eingeschränkt) Zugriff auf den Benutzer-Client des Anwenders hat. Siehe dazu auch: https://weakdh.org/

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung
Durch einen erfolgreichen Man-In-The-Middle Angriff und somit das Auslesen der Sitzungsinformationen kann die betroffene Identität eingeschränkt von dem Angreifer angenommen werden. Alle Mechanismen innerhalb der beA-Anwendung, welche ohne die beA-Karte nutzbar sind, können von dem Angreifer durchgeführt werden. Die Bedrohung der Integrität ist hoch, da der Angreifer wie genannt eingeschränkt mit der Identität des betroffenen Nutzers agieren kann und beispielsweise Nachrichten verschicken kann. Die Verfügbarkeit der beA-Anwendung kann auch gestört werden, da eine aktive Sitzung von dem Angreifer übernommen wird. Die allgemeine Prozessintegrität wird somit gestört.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **niedrig**

{M10} Die unsicheren cipher suites sollten auf dem Server deaktiviert werden.

3.6.7 Detaillierte Fehlermeldungen der Webapplikationsfirewall

Untersuchungsobjekt	beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle nicht behoben

Eine Webapplikationsfirewall (kurz WAF) versucht bei Anfragen an Webanwendungen verdächtige Inhalte von Angreifern zu erkennen und zu blockieren. So sollen typische Angriffe auf Webanwendungen erkannt und abgewehrt werden. Die beA-Anwendung nutzt auch eine solche Technologie.

{S11} Die WAF zeigt den Hersteller, die genaue Version der WAF sowie detaillierte Fehlermeldungen an.

{R11} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Werden bekannte Angriffsmuster an den Server gesendet, werden diese

von der Webapplikationsfirewall erkannt und blockiert. Die entsprechende Fehlermeldung wird angezeigt.

Ausnutzbarkeit: **hoch**

Bewertung der Bedrohung
Wird eine Fehlermeldung der WAF an den Angreifer zurückgegeben, kann dieser seinen gerade durchgeführten Angriff weiter detaillieren. Da die Fehlermeldung den genauen Aufruf des Angreifers und die Stelle, die die WAF als gefährlich einstuft, zurückgibt, kann der Angreifer gezielt versuchen die WAF zu umgehen und seinen ursprünglichen Angriff erfolgreich durchführen.

Die Analyse wurde auf der Testumgebung des beA durchgeführt. Zu Test, Entwicklungs- und Debugzwecken ist es üblich, diese Detailtiefe von Fehlermeldungen anzuzeigen. Wird die serverseitige Konfiguration der WAF auf der Produktionsumgebung oder auf weiteren dritten Systemumgebungen allerdings nicht angepasst, kann diese Schwachstelle erfolgreich ausgenutzt werden

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **niedrig**

{M11} Die angezeigten Fehlerseiten sollten keinen Hinweis auf den Inhalt von Fehlermeldungen der Webapplikationsfirewall enthalten.

3.6.8 Schwache Lock-Out-Mechanismen in der beA-Anwendung

Untersuchungsobjekt	beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle behoben

{S12} Account Lock-Out-Mechanismen werden vornehmlich gegen Brute-Force-Angriffe auf Benutzerpasswörter eingesetzt. Die beA-Anwendung setzt keinen Lock-Out-Mechanismus für die Anmeldung eines Mitarbeiters ein.

{R12} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Ein Angreifer kann automatisiert versuchen Benutzer-Passwörter zu erraten. Hierfür können gängige Angriffstools verwendet werden: Beispielsweise einzelne frei im Internet verfügbare Tools oder auch ein Botnetz.

Ausnutzbarkeit: **hoch**

Bewertung der Bedrohung
Der hier betroffene Zugang wird einmalig und initial für einen bestimmten Anwendungsfall genutzt, wenn sich neue Benutzer registrieren. Da

in jedem Fall für eine vollständige Anmeldung an der beA-Anwendung die Zwei-Faktor Authentisierung genutzt werden muss, kann ein Angreifer selbst bei einer erfolgreich Nutzername/Passwort Kombination kaum etwas mit diesem Zugang anfangen. Entsprechend niedrig sind die Bedrohungen eingestuft.

Bedrohung Integrität:	**niedrig**
Bedrohung Verfügbarkeit:	**niedrig**
Bedrohung Vertraulichkeit:	**niedrig**

{M12} Es sollte ein Lock-Out-Mechanismus implementiert werden, der Benutzer-Accounts nach einer definierten Anzahl von fehlgeschlagenen Login-Versuchen temporär sperrt. Alternativ kann auch ein Captcha in den Login-Prozess integriert werden.

3.6.9 Qualität der genutzten Session-Cookies

Untersuchungsobjekt	beA-Anwendung
Schwachstellenstatus	verifiziert: Schwachstelle nicht behoben

Session-IDs sind nach der beA-Karte und der dazugehörigen PIN das zentrale Authentisierungsmerkmal bei der Benutzung eines Webportals. Entsprechend sicher müssen die Initiierung und der Transport von Session-IDs realisiert werden.

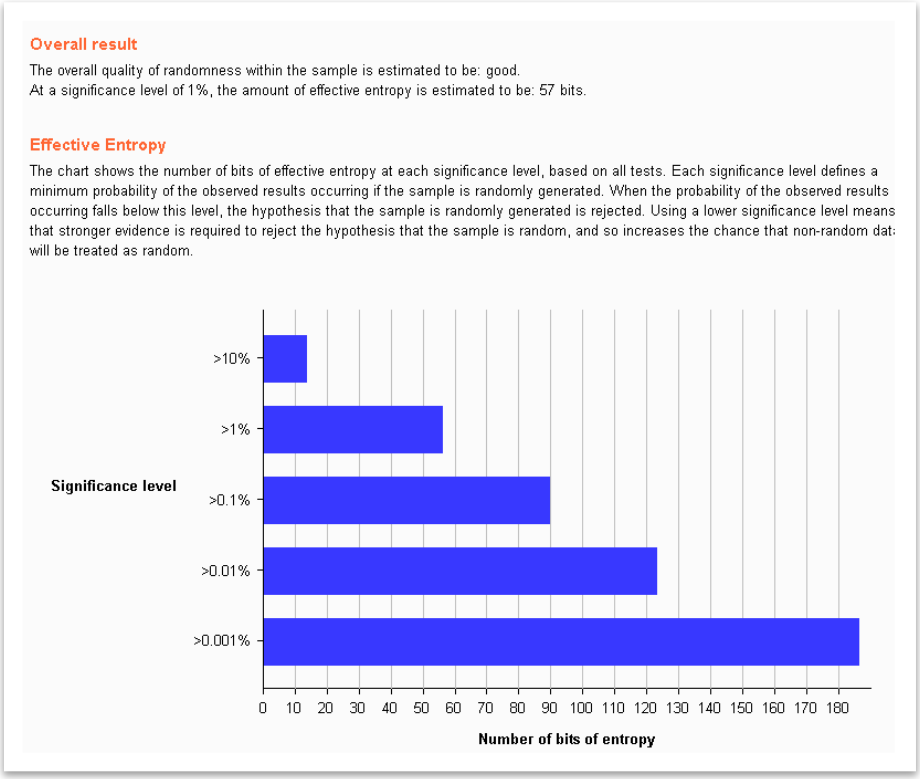

Abbildung 4: Session-Cookie-Entropie, Quelle: Burp Suite Professional

{S13} Die statistische Qualität der SessionID ist gut, aber nicht optimal. (ca. 57 Bit Entropie bei 1% Signifikanz)

{R13} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Ein Angreifer kann automatisiert versuchen entsprechende Session-Cookies zu erraten. Hierfür können gängige Tools verwendet werden: Beispielsweise einzelne frei im Internet verfügbare Tools oder auch ein Botnetz genutzt werden, um möglichst schnell viele Sessions und somit Zugänge zu erraten. Die Erfolgswahrscheinlichkeit ist allerdings auch bei der genannten Entropie sehr gering.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung
Kann ein Angreifer die Sitzungsinformationen erraten, kann die betroffene Sitzung und somit die betroffene Identität eingeschränkt von dem Angreifer angenommen werden. Alle Mechanismen innerhalb der beA-Anwendung, welche ohne die beA-Karte nutzbar sind, können von dem Angreifer durchgeführt werden. Die Bedrohung der Integrität ist hoch, da der Angreifer eingeschränkt mit der Identität des betroffenen Nutzers agieren und beispielsweise Nachrichten verschicken kann. Die Verfügbarkeit der beA-Anwendung kann auch gestört werden, da eine aktive Sitzung von dem Angreifer übernommen wird. Die allgemeine Prozessintegrität wird somit gestört.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **mittel**
Bedrohung Vertraulichkeit: **niedrig**

{M13} Das Generieren der Session sollte mit kryptographischen Zufallszahlengeneratoren durchgeführt und in Bezug auf die Entropie geprüft werden. Eine effektive Entropie von mindestens 64 Bit bei 1% Signifikanz wird empfohlen. Eine exzellente Entropie sollte bei 128 Bit sein.

3.6.10 Automatisches Ausführen und Öffnen von Dateien

Untersuchungsobjekt	beA-Anwendung
Schwachstellenstatus	-

Benutzer, die in der beA-Anwendung angemeldet sind, können empfangene Nachrichten mit Anhängen betrachten. Die beA-Anwendung besitzt dafür eine „Anhang anzeigen“- sowie eine separate „Speichern“-Funktion.

{S14} Anhänge werden basierend auf den Dateiendungen auf dem Benutzersystem ausgeführt.

{R14} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle
Eine manipulierte Datei wird auf dem Angreifer-System erstellt und dann an den Ziel-Empfänger versendet. Für das Erstellen solcher manipulierten Dateien kann auf bekannte Frameworks in der Security-Szene zurückgegriffen werden. Entsprechend einfach ist die Erstellung solcher Dateien. Es wird allerdings davon ausgegangen, dass unbekannte Dateitypen zumindest Misstrauen beim Empfänger auslösen sollten und nicht einfach geöffnet werden.

Die Schwachstelle wird ausgenutzt, wenn der betroffene Benutzer auf „Anzeigen“ des Anhangs klickt.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung
Trotz der Ablehnung der beA-Anwendung von exe-, com-, bat-, cmd- und lnk-Dateien kann ein Angreifer diese Schwachstelle ausnutzen, um einen Angriff auf das Benutzersystem des Datei-Empfängers durchzuführen.

Bei Word-, sowie Excel-Dateien oder Bildern kann davon ausgegangen werden, dass der Benutzer der beA-Anwendung Kenntnis hat, was er hiermit öffnet. Bei einem ps1 oder sonstigem Script-Dokumenten eher nicht. Natürlich kann auch nach dem Abspeichern eine potenziell manipulierte Datei Schaden anrichten. Hier ist sich der Benutzer allerdings bewusst, dass er eine aus dem Internet erhaltene Datei auch tatsächlich auf seinem eigenen System öffnet bzw. ausführt. Dies gilt sowohl für MacOS, Linux und Windows spezifische Dateien. Wird eine manipulierte Datei erfolgreich ausgeführt, kann der Angreifer das Benutzersystem kompromittieren und Kontrolle über dieses erhalten.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **hoch**

{M14} Es existieren viele weitere Dateiendungen mit Potenzial für Angreifer. Das Nachrichtenformat-Modul sollte keine Datei automatisch vom Internet auf dem lokalen Rechner ausführen. Es wird empfohlen eine Whitelist für „vertrauenswürdigen“ Inhalt zu erstellen. Diese könnte beispielsweise Dateitypen wie docx, xlsx, pdf, txt, und csv enthalten. Eine abgestimmte Whitelist könnte ca. 80% der versendeten Anhänge freigeben und für die restlichen 20% müsste dann die Speichern-Funktion verwendet werden. Eine Blacklist ist aufgrund der Vielfältigkeit von Linux, Windows und MacOS nicht zielführend. So gibt es diverse weitere ausführbare Dateitypen, die der Endanwender nicht einschätzen kann (z.B. ps1, ps1xml, ps2, ps2xml, psc1, psc2, msi, sh…).

3.6.11 Modifikation von signierten XML-Nachrichten

Untersuchungsobjekt	Webservice OSCI ⇔Intermediär BRAK
Schwachstellenstatus	-

{S15} Bei der Verwendung von signierten XML-Nachrichten sind keine Vorsichtsmaßnahmen getroffen worden, um den Inhalt der signierten Nachricht der XML-Nachricht gegen Modifikation zu schützen.

{R15} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle:

Der Angriff steht nur einem Innentäter oder erfolgreich eingedrungenen Außentäter zur Verfügung, der Zugriff auf den Übertragungsweg zwischen Webservice-OSCI und Intermediär BRAK hat. Ist der Zugriff vorhanden, ist die Durchführung des Angriffs einfach.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung .
Der Angriff erlaubt, die Container-Signatur einer OSCI-Nachricht zu umgehen, um den Nutzdatenteil der OSCI-Nachricht zu manipulieren. Betroffen ist der Nachrichtenaustausch zwischen beA und EGVP. Es können so z.B. Anhänge entfernt werden. Es besteht eine mittlere Bedrohung der Nachrichtenintegrität. Die Nachrichteninhalte können mit diesem Angriff nicht eingesehen werden, weil sie verschlüsselt bleiben.

Bedrohung Integrität: **mittel**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **niedrig**

{M15} Die Referenz des signierten Elements sollte die Lokalität mit abdecken. Z.B. realisierbar mittels einer absoluten XPath-Expression.

3.6.12 Logdaten: Detaillierte Struktur der REST-Endpunkte

Untersuchungsobjekt	beA-Client-Security
Schwachstellenstatus	verifiziert: Schwachstelle nicht behoben

Die beA-Client-Security speichert in ihrem Nutzungskontext je nach Einstellung des Log-Levels Daten und Informationen in den lokalen Logdateien auf dem Dateisystem des Benutzers.

{S16} Innerhalb den Logdateien stehen Informationen, welche sensible Inhalte darstellen und einem Angreifer im Allgemeinen seine Angriffe erleichtern. Beispielsweise werden detaillierte REST-Endpunkte in der beA-

Anwendung mit konkreten Sitzungsinformationen oder Parametern abgespeichert.

{R16} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle;
Ein Angreifer mit lokal installierter bea-Client-Security kann die Logdateien auf seinem eigenen persönlichen Betriebssystem einsehen.

Ausnutzbarkeit: **hoch**

Bewertung der Bedrohung;
Durch den Informationsgewinn über die REST-Endpunkte innerhalb der beA-Anwendung sowie auch über die Schnittstellen, welche bestimmte und konkrete Parameter erwarten, kann ein Angreifer gezielter die beA-Anwendung angreifen oder auch neue Angriffsvektoren identifizieren. Über diesen Weg konnten im Rahmen der Analyse weitere Schwachstellen identifiziert werden.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **niedrig**

{M16} Die Logs sollten auf Produktiv-Installationen keine detaillierten Hinweise über die Anwendung geben.

3.6.13 Nicht konsistente Zertifikatsprüfung

Untersuchungsobjekt	Kammersoftware
Schwachstellenstatus	-

{S17} Der Client prüft den Common Name (CN) des Zertifikats nicht. Dadurch wird jedes Zertifikat akzeptiert, welches durch eine Certificate Authority (CA) aus dem Keystore ausgestellt wurde. Da wenige CAs den Großteil der HTTPS Verbindungen des Internets absichern, ist es wichtig die Details der Zertifikate zu prüfen. Insbesondere der CN muss geprüft werden um verschiedene Webseiten voneinander zu unterscheiden

{R17} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle;
Eine Nutzerinteraktion des betroffenen Nutzers ist nicht nötig. Die Kammersoftware läuft wie gewohnt und baut regelmäßig eine Netzwerkverbindung auf. Der Angreifer braucht keine Berechtigungen innerhalb des beA-Systems, muss aber Zugriff auf den Datenverkehr haben, um den Angriff durchführen zu können. Dies kann an einer beliebigen Stelle zwischen Kammersoftware und dem beA-Endpunkt erfolgen, beispielsweise im lokalen Netz der Kammersoftware (unsichere Konfiguration des Firmennetzwerkes oder offenes WLAN), im Internet (Manipulation von DNS oder Routing, Massen Überwachung an Internetknoten wie dem DE-CIX) oder

innerhalb des beA-Netzwerkes (siehe Kammersoftware). Lokaler Zugriff ist auf das Betriebssystem des Clients ist nicht nötig.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung;
Ein Angreifer der für seine eigene Domain von einer im Keystore enthaltenen CA ein Zertifikat erhalten hat, kann sich der Kammersoftware gegenüber als beA ausgeben. Dadurch kann dieser eine verschlüsselte Verbindung anstelle des beA annehmen.

Bedrohung Integrität: **mittel**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **niedrig**

{M17} Der Client sollte die Zertifikate der Gegenstelle vollständig prüfen.

3.7 Auflistung der C-Schwachstellen

In dem nachfolgenden Kapitel werden nun alle im Bereich der Penetrationstests identifizierten Schwachstellen der Kategorie C aufgelistet und in verkürzter Form dargestellt.

Tabelle 9: Pentest C-Schwachstellen

Legende: h=hoch; m=mittel; n=niedrig; J=Ja		Bedrohung				
Kurzbeschreibung	Komponente	Ausnutzbarkeit	Vertraulichkeit	Integrität	Verfügbarkeit	Schwachstelle behoben
Die REST-API des Wikis ist öffentlich erreichbar und stellt teilweise sensible Informationen bereit, die für den Anwendungszweck des Wikis nicht benötigt werden.	Webportal XWIKI	m	n	n	n	-
Das Portal ist anfällig für eine Reflected-XSS-Schwachstelle, die jedoch nicht ohne Weiteres auszunutzen ist.	Webportal XWIKI	n	n	n	m	-
Das Webportal hat eine XSS-Schwachstelle.	Webportal BRAV-Suche	n	n	m	n	-
Der Webservice gibt Fehlerbezeichnungen mit Paketnamen und Stack-trace an den Client weiter, wodurch Rückschlüsse auf die Architektur möglich sind.	Webservice Kanzlei-SAFE BRAK	m	n	n	n	-
In den Logdateien der lokal installierten beA-Client-Security des Benutzers findet sich die Session-ID der Anwendung.	beA-Client-Security	m	n	n	n	-
Die Analyse des Datenverkehrs ergab, dass auf einem Großteil der betrachteten Seiten mit vertraulichen Inhalten der Browser-Cache nicht deaktiviert wird.	beA-Anwendung	n	n	n	n	-
Die Passwort-Policy für den Mitarbeiterlogin ist nicht ausreichend, da kein Brute-Force Schutz vorhanden ist.	beA-Anwendung	m	n	n	n	J
Das Passwortfeld auf der Anmeldeseite „Registrierung beA Benutzer“ begrenzt die Eingabe eines Passwortes auf 8 Zeichen.	beA-Anwendung	m	n	n	n	J
An mehreren Stellen innerhalb der Web-Applikation können Fehlermeldungen ausgelöst werden.	beA-Anwendung	m	n	n	n	-
Der Webservice gibt Fehlerbezeichnungen aus Java an den Client weiter, die Rückschlüsse auf die Architektur zulassen.	Webservice Attribute-Service VAS => SAFE BRAK	m	n	n	n	-
Passphrasen werden im Klartext gespeichert.	Kammersoftware	m	n	n	n	-
Der Webserver gibt per HTTP-Server-Header seine genaue Version preis.	Kammersoftware Endpunkte	m	n	n	n	-
Der Webservice gibt im Response-Header die Server-	Webservice	m	n	n	n	-

Legende: h=hoch; m=mittel; n=niedrig; J=Ja		Bedrohung				
Kurzbeschreibung	Komponente	Ausnutzbarkeit	Vertraulichkeit	Integrität	Verfügbarkeit	Schwachstelle behoben
Software und -Versionsnummer über das Server-Response-Header-Feld bekannt.	Find a Lawyer					
Der Webservice gibt Fehlerbezeichnungen aus Java an den Client weiter, die Rückschlüsse auf die Architektur zu lassen.	Find a Lawyer	m	n	n	n	-
Der Webservice gibt im Response-Header Server Software und Versions-nummer bekannt über das Server-Response-Header-Feld.	Webservice BNotK Post-fach-beA-Postfach	m	n	n	n	-
Der Webservice gibt Fehlerbezeichnungen aus Java an den Client weiter, die Rückschlüsse auf die Architektur zu lassen.	Webservice BNoTK Postfach-beA-Postfach	m	n	n	n	-
Der Webserver gibt auf Fehlerseiten seine genaue Version und Stack-Traces preis.	Xwiki	m	n	n	n	-
Es konnte eine Benutzerlogin-Maske öffentlich abgerufen werden, die durch einen Angreifer ausgenutzt werden könnte und keinen Schutz vor Brute-Force-Angriffen oder lokaler Passwort-Speicherung bietet.	Xwiki	m	n	n	n	-
Auf dem Server konnten Stack-Trace-Meldungen hervorgerufen werden, die ggf. für weitere Angriffe genutzt werden könnten.	Xwiki	m	n	n	n	-

4 Quelltextanalysen

4.1 Beschreibung des Analysegegenstandes

Im Rahmen der Analyse wurden die beA-Client-Security, die beA-Anwendung sowie die BRAV-Search betrachtet. Die Analysen wurden als Whitebox-Test durchgeführt, das heißt, der Auftraggeber hat den relevanten Source-Code und die Dokumentation in unterschiedlichen Versionen bereitgestellt. Die zur Verfügung gestellten Sourcen wurden zum einen in Form von lauffähigen Java-Projekten (Client-Security) und zum Teil in Form von *.jar, *.war oder *.ear Dateien ausgeliefert.

Die beA-Client-Security in Version 3.1.3.6 wurde einer statischen Quelltextanalyse unterzogen. Der Quelltext-Audit sowie die erneuten Tests der zuvor gemeldeten Schwachstellen erfolgten auf Basis der Version 3.1.3.7.

Die beA-Anwendung wurde einer statischen Quelltextanalysen unterzogen. Untersucht wurde die Version 2.0.10 sowie die Version 2.1.0. Für die Überprüfung der als behobenen gemeldeter Schwachstellen wurde die Version 2.1.1 genutzt.

Bibliotheken, die während der Laufzeit vom Application-Server (JBoss EAP) zur Verfügung gestellt werden, konnten nicht betrachtet werden und sind somit nicht Bestandteil des Reviews. Dabei handelt es sich nicht nur um JEE-Bibliotheken, sondern auch um Bibliotheken wie die Verschlüsselungsbibliothek BouncyCastle oder die JSF-Implementierung Primefaces.

Die BRAV-Search wurde in der Version 1.2.0 einer statischen Quelltextanalyse unterzogen.

4.2 Methodik und Vorgehensweise

Angewandt wurden werkzeuggestützte statische Quelltextanalysen und ein Quelltext-Audit.

Werkzeuggestützte Quelltextanalysen überprüfen den gesamten Java-Quelltext anhand eines vordefinierten Regelwerks. Dieses Regelwerk wurde von der Open-Source-Gemeinde erstellt und wird regelmäßig erweitert und gepflegt. Abhängig vom eingesetzten Regelwerk und Werkzeug werden Treffer in unterschiedliche Kategorien eingeordnet. Die Treffer können unsauberen Code bis hin zu schwerwiegenden Schwachstellen umfassen. Nicht jeder Treffer ist zwingend eine Schwachstelle, der eine Bedrohung der IT-Sicherheit darstellt. Die Beurteilung, ob ein Treffer eine Schwachstelle ist, muss durch ein Code Review erfolgen. Konzeptionelle Fehler in der Software-Architektur oder dem Programmablauf können in der Regel über dieses Verfahren nicht identifiziert werden. Die Anzahl der Treffer und ihre Einstufung ist nur ein schwacher Indikator für Code-Qualität.

Beim Quelltext-Audit wird im Gegensatz zur statischen Quelltext-Analyse der logische und korrekte Programmablauf überprüft. Werkzeug-Unterstützung, bis auf den Einsatz einer Programmierumgebung, ist nicht vorhanden. Der logische und korrekte Programmablauf wird anhand des geprüften Use-Cases und des zugehörigen Feinkonzeptes belegt. Logische und software-architektonische Unzulänglichkeiten können erkannt werden. Alle Schwachstellen, die nicht den logischen Ablauf oder die Softwarearchitektur betreffen, werden nicht näher betrachtet.

Nach Absprache mit dem Auftraggeber wurde der Quelltext der beA-Client-Security, BRAV-Search und der beA-Anwendung mittels statischer Quelltextanalyse und einem in Umfang und Tiefe begrenzten Quelltext-Audit für die beA-Client-Security auf Schwachstellen überprüft.

Bibliotheken wurden auf Basis ihres Versionsstandes nur anhand öffentlich bekannter Schwachstellen geprüft sowie ihre Verwendung begutachtet.

Beim manuellen Audit der beA-Client-Security wurde bedingt durch den Umfang des Quellcodes der Komponenten das Audit auf folgende Funktionsbereiche eingeschränkt;

- die beA-Client-Security bzgl. Verbindungsaufbau zur beA-Anwendung
- Deserialisierung JSON Objekte am Websocket
- Deserialisierung von XML Dateien

Ausgewählt wurden diese Bereiche wegen ihrer möglichen Bedrohung für die Integrität des Anwalts-PC und anhand von Erfahrungswerten.

4.3 Übersicht der Schwachstellen

Tabelle 10: Schwachstellenübersicht Quelltextanalysen

Komponente	Schwachstelle	Einstufung	behoben
beA-Anwendung	Mögliche Ausführung von Schadcode (XML)	A	J
beA-Anwendung	Java-Abhängigkeiten mit bekannten Schwachstellen	A	J
beA-Client-Security	Mögliche Ausführung von Schadcode (JSON)	A	J
beA-Client-Security	Mögliche Ausführung von Schadcode (XML)	A	J
beA-Client-Security	Verwendete Bibliotheken	A	J
BRAV-Suche	Verwendete Bibliotheken	A	J
beA-Anwendung	beA-Anwendung: SQL-Injection	B	-
beA-Anwendung	Initialisierungs-Vector (IV)	B	-
beA-Anwendung	Unsicheres Auffüllen von Daten bei Verschlüsselung	B	-

beA-Client-Security	TLS-Zertifikate-Validierung	B	J
beA-Client-Security	Unfertiger bzw. System-spezifischer Quelltext	C	-
beA-Anwendung	Verwundbarkeit über unsichere XML-Deserialisierung	C	-
beA-Client-Security	Möglicherweise unsicherer Quelltext - fest vergebene Namen für temporäre Dateien	C	-

4.4 Beschreibung der A-Schwachstellen

4.4.1 beA-Anwendung - Mögliche Ausführung von Schadcode (XML)

Untersuchungsobjekt	Statische Quelltext-Analyse beA-Anwendung
Schwachstellenbehebung	verifiziert, behoben

Das Deserialisieren von XML-Dateien ist potentiell immer eine Gefahr. Einem Angreifer wäre es möglich, über ein manipuliertes XML das System des Anwenders zu kompromittieren. Die XML Spezifikation erlaubt den Download und das Ausführen von externen (z.B. aus dem Internet) Programmen. Hat der Entwickler diesen Sachverhalt während der Entwicklung nicht berücksichtigt, ist es einem Angreifer potentiell möglich, beim Laden einer manipulierten XML-Datei die beA-Anwendung zu übernehmen.

Hier ist es die beA-Anwendung, die XML-Objekte deserialisiert und von einem authentisierten Nutzer dazu gebracht werden kann, Schadcode auf dem Server der beA-Anwendung auszuführen. Dies stellt eine hohe Bedrohung der Integrität der beA-Anwendung dar, was sich mittelbar auch auf die Vertraulichkeit von Nachrichten auswirken kann, die unmittelbar allerdings aufgrund ihrer durch die HSM gesicherten Verschlüsselung nicht aufgedeckt werden können. Wenn der Angreifer aber in die Verteilung von Postfachschlüsseln an Absender oder die Beantragung von Postfachzertifikaten bei der BNotK eingreifen kann, besteht in Verbindung mit der in Abschnitt 5.4.2 oder der in Abschnitt 5.5.1 beschriebenen Schwachstelle die Gefahr, dass er Nachrichten mitliest. Es können außerdem unmittelbar Kommunikationsbeziehungen aufgeklärt werden (Partner, Zeitpunkte). Die Bedrohung für die Systemintegrität und –verfügbarkeit ist hoch, die für die Vertraulichkeit der Nachrichten unmittelbar niedrig (in Verbindung mit den oben referenzierten Schwachstellen wäre sie allerdings **hoch**. Die Ausnutzbarkeit wird als leicht eingeschätzt.

{S18} Die beA-Anwendung ist potentiell verwundbar gegenüber XML-Java-Objekt-Deserialisierung. Durch nicht ausreichend konfigurierte Java-Bibliotheken zum Deserialisieren von XML-Dateien ist es einem Angreifer potentiell möglich, den Server der beA-Anwendung zu übernehmen.

{R18} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle:
Die Ausnutzung ist durch jeden beA-Anwender möglich und benötigt nur allgemein bekannte Techniken. Die Ausnutzbarkeit ist daher hoch.

Ausnutzbarkeit: **hoch**

Bewertung der Bedrohung:

Der Angreifer kann den Server der beA-Anwendung übernehmen und dort die Integrität der Nachrichtenverarbeitung beeinträchtigen, mittelbar

unter Ausnutzung weiterer Schwachstellen auf Nachrichteninhalte zugreifen. Das Schadenspotential wird für die Integrität und Verfügbarkeit als hoch, für die Vertraulichkeit niedrig bewertet.

Bedrohung Integrität:	**hoch**
Bedrohung Verfügbarkeit:	**hoch**
Bedrohung Vertraulichkeit:	**niedrig**

Die Kombination aus hoher Bedrohung der Integrität und hoher Ausnutzbarkeit führt zu einer Bewertung der Schwachstelle als betriebsverhindernd.

{M18} Korrekte Konfiguration der XML Bibliotheken

Diese Schwachstelle wurde zwischenzeitlich geschlossen. Die Überprüfung der betroffenen Quelltext-Zeilen hat ergeben, dass die eingesetzten Bibliotheken so konfiguriert werden, dass die beschriebenen Schwachstellen der XML-Objekt Deserialisierung so nicht erneut auftreten können.

4.4.2 Java-Abhängigkeiten mit bekannten Schwachstellen

Untersuchungsobjekt	Statische Quelltext-Analyse beA-Anwendung
Schwachstellenbehebung	verifiziert, behoben

Verwendung veralteter Drittbibliotheken bzw. Verwendung von Drittbibliotheken mit bekannten Schwachstellen. Drittbibliotheken, die zur Laufzeit vom Application Server zur Verfügung gestellt werden, konnten nicht geprüft werden.

Die untersuchten Komponenten der beA-Anwendung verwenden einige Java-basierte Abhängigkeiten, die zum Teil sehr veraltet sind und bekannte Schwachstellen aufweisen. Diese sind im Einzelnen:

- not-yet-commons-ssl-0.3.9.jar
  - CVE-2014-3604 – Cryptographic Issues - CVSS Score 6.8
- xercesImpl-2.9.1.redhat-6.jar
  - CVE-2012-0881 – Denial of Service - CVSS Score 7.8
- commons-httpclient-3.1.jar
  - CVE-2014-3577 – Cryptographic Issues – CVSS Score 5.8
- log4j-1.2.17.jar
  - CVE-2017-5645 - Deserialization of Untrusted Data – CVSS Score 7.5
- webservices-rt-2.3.jar
  - CVE-2013-2566 - Cryptographic Issues – CVSS Score 4.3
- bcmail-jdk16-1.46.jar

› Letzte Aktualisierung 23-Febr-2011 → Fortführung als bcmail-jdk15on-159.jar

Die Ausnutzbarkeit der Schwachstellen dieser Bibliotheken kann im Rahmen einer statischen Quellcodeanalyse nicht abschließend bewertet werden. Sie kann je nach Schwachstelle und Art der Verwendung der Bibliotheken leicht, mittel oder schwer sein. Für die Risikobewertung wurde eine mittlere Ausnutzbarkeit angenommen. Der potentielle Schaden reicht von einer betriebsverhindernden Störung der beA-Anwendung durch Überlastung oder Absturz einer beA-Anwendungskomponente über ein Aufbrechen von TLS-Verbindungen bis zur Ausführung von Schadcode auf dem beA-Server, also zum vollständigen Verlust der Systemintegrität.

Neben diesen Bibliotheken, die direkt den gelieferten Paketen entnommen werden konnten, gibt es noch die Bibliotheken, die der Application-Server zur Laufzeit zur Verfügung stellt. Diese waren nicht Bestandteil des Untersuchungsgegenstandes und müssen vom Betrieb auf Aktualität geprüft und in Rücksprache mit dem Hersteller der beA-Anwendung aktualisiert werden.

{S19} Für einige verwendete Java-Abhängigkeiten existieren bekannte Schwachstellen.

{R19} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle:

Die Ausnutzbarkeit kann nicht abschließend bewertet werden, sie kann auch je nach Bibliothek und Schwachstelle unterschiedlich sein. Für die Risikoabschätzung wurde eine mittlere Ausnutzbarkeit angenommen.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Ein Angreifer könnte eine veröffentlichte Schwachstelle ausnutzen, um die Integrität oder Verfügbarkeit und/oder Vertraulichkeit zu beeinträchtigen. Besonders die Schwachstellen bzgl. der SSL/TLS Verbindungen (CVE-2014-3604, CVE-2014-3577, CVE-2013-2566) können ein erhöhtes Risiko darstellen. Die Bedrohung für die System-Integrität und –Verfügbarkeit wird hoch, für die Vertraulichkeit von Nachrichten mittel eingeschätzt.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **mittel**

Die Kombination aus mittlerer Ausnutzbarkeit und hohem Schadenspotential führt zu einer Einschätzung der Schwachstelle als betriebsverhindernd.

{M19} Die Java-Abhängigkeiten sollten aktualisiert werden.

Diese Schwachstelle wurde zwischenzeitlich geschlossen. Die genannten Bibliotheken wurden durch aktuelle Versionen ersetzt, für die keine bekannten Schwachstellen mehr vorliegen.

4.4.3 Mögliche Ausführung von Schadcode in der beA-Client-Security (JSON)

Untersuchungsobjekt	Quelltext-Audit beA-Client-Security
Schwachstelle behoben	verifiziert, behoben

Die Serialisierung von Java-Objekten wird an diversen Stellen im Code durchgeführt. Eingesetzt wird hierfür die Bibliothek jackson-core-2.9.3.jar.

Für diese sind derzeit folgende CVE gelistet:

- CVE-2017-17485 (Score 7,5)
- CVE-2018-7489 (Score 7,5)
- CVE-2018-5968 (Score 5.1)

Alle CVEs benennen eine Schwachstelle dieser Bibliothek bei der Verarbeitung eingehender JSON-Objekte. Mit speziell für einen Angriff auf diese Schwachstelle zusammengestellten JSON-Objekten kann ein Angreifer die beA-Client-Security dazu bringen, vom Angreifer vorgegebenen Code auszuführen. Das kann in der Übernahme der Kontrolle der Client-Rechner, auf dem die beA-Client-Security läuft, resultieren. Hiermit ist auch die Vertraulichkeit aller vom angegriffenen Rechner versendeten und empfangenen Nachrichten kompromittiert. Weiterer Schaden für die Nutzer des Rechners muss befürchtet werden. Der Angriff kann ohne wesentlichen Mehraufwand gegen alle beA-Anwender ausgeführt werden. Das Schadenspotential ist daher hoch. Um den Angriff auszuführen, müssen manipulierte JSON-Daten an die Websocket-Schnittstelle der beA-Client-Security gesendet werden. Die Ausnutzbarkeit ist daher leicht.

Als Reaktion auf die vom Chaos Computer Club gefundene Schwachstelle der allgemeinen Ansprechbarkeit der Websocket-Schnittstelle der beA-Client-Security wertet diese nun den sogenannten „Origin-Header“ einer JSON-Objekt-Nachricht aus. Diese gibt Auskunft über den Versender der Nachricht und ist schwer manipulierbar, was einen allgemeinen Zugriff auf diese Schnittstelle erschwert (vergleiche Abschnitt 4.7.2). Der Angreifer muss nun gegenüber der beA-Client-Security als die beA-Anwendung auftreten, was insbesondere erfordert, im Browser in die TLS-Verbindung zwischen beA-Anwendung und Websocket eindringen zu können. Die Ausnutzbarkeit der Schwachstelle wurde durch die beschriebene Maßnahme deutlich reduziert.

Durch die Aktualisierung der verwendeten Bibliothek ist die verwendete Version durch die bekannten Angriffe nicht mehr verwundbar, und damit wurde die Schwachstelle beseitigt. Die Aktualisierung der Bibliothek wurde verifiziert.

{S20} Die beA-Client-Security ist potentiell verwundbar gegenüber JSON Java-Objekt-Deserialisierung.

{R20} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle:

Die Ausnutzbarkeit in der vom Chaos Computer Club untersuchten Version war hoch, da es keinen Zugriffschutz auf die gefährdete Schnittstelle gegeben hat. Durch die Einführung der Überprüfung des Origin-Headers, ist diese Schwachstelle noch als mittel einzustufen.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Ein Angreifer könnte das System eines Anwenders übernehmen. Ein gleichzeitiger Angriff auf alle Client-Systeme ist möglich. Die Übernahme von Rechnern der beA-Anwender bedroht unmittelbar die von diesen Rechnern versendeten und empfangenen Nachrichten, sowie weitere Assets wie bspw. die von den Anwendern verwendeten Schlüssel, und kann darüber hinaus noch zu weiterem erheblichen Schaden führen.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **hoch**

Die Kombination aus mittlerer Ausnutzbarkeit und hohem Schadenspotential führt zu einer Bewertung als betriebsverhindernde Schwachstelle.

{M20} Die verwendete Bibliothek muss durch eine aktuellere nicht verwundbare Version ersetzt werden.

Die schwachstellenbehaftete-Bibliothek wurde im Laufe des Projektverlaufes durch eine aktuellere Version (2.9.5) ersetzt. Für diese sind derzeit keine Schwachstellen (CVE) bekannt.

4.4.4 Mögliche Ausführung von Schadcode in der beA-Client-Security (XML)

Untersuchungsobjekt	Quelltext-Audit beA-Client-Security
Schwachstellenbehebung	verifiziert, behoben

Das Deserialisieren von XML-Dateien ist potentiell immer eine Gefahr. Einem Angreifer wäre es möglich, über ein manipuliertes XML das System des Anwenders zu kompromittieren. Die XML-Spezifikation erlaubt den Download und das Ausführen

von externen (z.B. aus dem Internet) Programmen. Hat der Entwickler diesen Sachverhalt während der Entwicklung nicht berücksichtigt, ist es einem Angreifer potentiell möglich, beim Laden einer manipulierten XML-Datei das System des Anwenders zu übernehmen.

Auch die beA-Client-Security nimmt XML-Nachrichten entgegen. Im Quelltext fehlen aber die notwendigen Vorsichtsmaßnahmen bei der Verarbeitung. Daher ist auch die beA-Client-Security wie die beA-Anwendung durch manipulierte XML-Dateien angreifbar (vgl. Abschnitt 4.4.1) und führt dann Code des Angreifers aus. Hoch bedroht sind unmittelbar die System-Integrität und –Verfügbarkeit des IT-Systems des beA-Anwenders sowie die Vertraulichkeit der auf diesem System versendeten und empfangene Nachrichten, da sie auf dem IT-System des Anwenders im Klartext vorliegen. Die Ausnutzbarkeit verlangt das Eindringen in TLS-Verbindungen und mittlerweile die Manipulation des Origin-Headers und wird daher als mittel bewertet.

In der letzten untersuchten Version der beA-Client-Security wurde die Schwachstelle durch geeignete Konfiguration der XML-Verarbeitung geschlossen. Der geänderte Quellcode wurde verifiziert.

{S21} Die beA-Client-Security ist potentiell verwundbar gegenüber XML-Java-Objekt-Deserialisierung. Durch nicht ausreichend konfigurierte Java-Bibliotheken zur Deserialisierung von XML-Dateien ist es einem Angreifer potentiell möglich, das System des Anwenders zu übernehmen. Es werden ausschließlich XML-Dateien von der beA-Anwendung entgegen genommen.

{R21} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle:

Die Ausnutzbarkeit ist mittel, da die beA-Client-Security den Origin-Header einer XML-Nachricht auswertet.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Ein Angreifer könnte an alle Clients modifizierte XML-Dateien schicken und damit die Rechner des Anwenders übernehmen, mit unmittelbaren Folgen für die Vertraulichkeit der Nachrichten sowie weitere hohe Gefährdungen für die Anwender. Das Schadenspotential ist hoch.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **hoch**

Die Kombination aus mittlerer Ausnutzbarkeit und hohem Schadenspotential ergibt eine Bewertung als betriebsverhindernde Schwachstelle.

{M21} Korrekte Konfiguration der XML Bibliotheken

Diese Schwachstelle wurde zwischenzeitlich geschlossen. Die Überprüfung der betroffenen Quelltext-Zeilen hat ergeben, dass die eingesetzten Bibliotheken so konfi-

guriert werden, dass die beschriebenen Schwachstellen der XML-Objekt-Deserialisierung so nicht erneut auftreten können.

4.4.5 Verwendete Bibliotheken der beA-Client-Security

Untersuchungsobjekt	Quelltext-Audit beA-Client-Security
Schwachstellenbehebung	verifiziert, behoben

Eine Überprüfung der verwendeten Bibliotheken hat für folgende Java-Bibliotheken Schwachstellen ergeben:

Tabelle 11: Bibliotheken mit Schwachstellen (beA-Client-Security)

Dependency	Highest Severity	CVE Count	CPE Confidence
jackson-databind-2.9.3.jar	High	3	Highest

- jackson-databind-2.9.3.jar
  - CVE-2017-17485
  - CVE-2018-5968
  - CVE-2018-7489

Die genannten Schwachstellen erlauben einen Angriff mit manipulierten JSON-Daten, sogenannten JSON-Gadgets, der zur Übernahme des Rechners, auf dem die beA-Client-Security läuft, führen kann. Für die Vorgehensweise des Angreifers, die Ausnutzbarkeit und das Schadenspotential gilt das in Abschnitt 4.4.3 Gesagte. Die Ausnutzbarkeit ist mittel, das Schadenspotential hoch.

{S22} Durch den Einsatz einer mit Mängeln behafteten-Bibliothek besteht das Risiko für das Anwender-System, von einem Angreifer übernommen zu werden.

{R22} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle:

Die Ausnutzbarkeit war hoch in der vom Chaos Computer Club untersuchten Version, da es keinen Zugriffschutz für die gefährdete Schnittstelle gegeben hat, und ist noch mittel nach der eingeführten Auswertung des Origin-Headers.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Ein Angreifer könnte das System eines Anwenders übernehmen. Ein gleichzeitiger Angriff auf alle Client-Systeme ist möglich. Die Übernahme von Rechnern der beA-Anwender bedroht unmittelbar die von diesen Rechnern versendeten und empfangenen Nachrichten, sowie weitere Assets wie bspw. die von den Anwendern verwendeten Schlüssel, und kann darüber hinaus noch zu weiterem erheblichen Schaden führen.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **hoch**

{M22} Aktualisieren der eingesetzten Bibliotheken.

In der beA-Client-Security Version 3.1.3.7 wurde die Jackson-databind-Bibliothek aktualisiert. Derzeit wird die Version 2.9.5 eingesetzt. Für die die Jackson-databind-Bibliothek 2.9.5 sind derzeit keine CVE gemeldet. Mit dem Einsatz dieser Version ist die gemeldete Schwachstelle behoben.

4.4.6 Verwendete Bibliotheken in der BRAV-Suche

Untersuchungsobjekt	Statische Quelltext-Analyse BRAV-Suche
Schwachstellenbehebung	verifiziert, behoben

Eine Überprüfung der von dem BRAV-Suche-Service verwendeten Bibliotheken hat für folgende Java-Bibliotheken bekannte Schwachstellen gezeigt:

Tabelle 12: Bibliotheken mit Schwachstellen (BRAV-Suche)

Dependency	Highest Severity	CVE Count	CPE Confidence
primefaces-5.3.jar	High	1	Highest
commons-collections-3.2.1.jar	High	2	Highest
xstream-1.4.9.jar	Medium	1	Highest
xercesImpl-2.8.0.jar	High	1	Low

- primefaces-5.3.jar
  - CVE-2017-1000486
- commons-collections-3.2.1.jar
  - CVE-2015-6420
  - CVE-2017-15708
- xstream-1.4.9.jar
  - CVE-2017-7957
- xercesImpl-2.8.0.jar
  - CVE-2012-0881

Die Schwachstellen dieser Bibliotheken erlauben entweder die Ausführung von Code auf dem angegriffenen System oder Betriebsstörungen durch Absturz von Programmkomponenten oder Überlastung des Systems.

{S23} Durch den Einsatz einer mit Mängeln behafteten Bibliothek besteht das Risiko für das Anwender-System, von einem Angreifer übernommen zu werden.

{R23} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle:

Die statische Quelltextanalyse kann nicht abschließend die Ausnutzbarkeit bestimmen. Die Ausnutzbarkeit kann auch je nach Bibliothek und Schwachstelle unterschiedlich sein. Angriffe sind durch Außentäter möglich. Die Ausnutzbarkeit wird zum Zweck der Risikobewertung als mittel eingeschätzt.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Der Angriff ermöglicht die betriebsverhindernde Störung oder die Übernahme des BRAV-Suche-Servers durch den Angreifer. Die Bedrohung für die Systemintegrität und die –Verfügbarkeit wird als hoch eingeschätzt. Vertrauliche Nachrichten sind nicht unmittelbar gefährdet.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **niedrig**

Die Kombination aus hoher Bedrohung für Integrität und mittlerer Ausnutzbarkeit ergibt eine Bewertung der Schwachstelle als betriebsverhindernd.

{M23} Aktualisieren der eingesetzten Bibliotheken.

Die genannten Bibliotheken wurden entfernt bzw. aktualisiert.

- PrimeFaces wurde aktualisiert (6.2.3)
- Commons collections wird nicht mehr verwendet
- XStream wurde aktualisiert auf Version 1.4.10
- XercesImpl wird nicht mehr verwendet

Für die aktualisierten Bibliotheken PrimFaces und XStream sind keine CVE gemeldet. Mit dem Einsatz der genannten Bibliotheken und Version und dem Entfernen der Commons collections und der XercesImpl-Bibliothek ist die gemeldete Schwachstelle behoben.

4.5 Beschreibung der B-Schwachstellen

4.5.1 beA-Anwendung: SQL-Injection

Untersuchungsobjekt	Statische Quelltext-Analyse beA-Anwendung
Schwachstellenbehebung	-

In der beA-Anwendung werden an verschiedenen Stellen Eingabeparameter in Datenbank-Befehle (SQL) eingebaut und ausgeführt. Ein authentifizierter Angreifer könnte durch geeignet gewählte Eingaben eigene SQL-Befehle an das Datenbank-

Backend absetzen und so Zugriff auf sensitive Informationen erhalten, diese verändern oder den Datenbankserver komplett übernehmen. Im Rahmen der Analyse konnte nicht evaluiert werden, inwiefern die Schwachstellen tatsächlich ausnutzbar sind, da hierfür ein Quelltext-Audit notwendig wäre (siehe Abschnitt 4.2).

Diese Schwachstelle konnte an acht Stellen im Quelltext nachgewiesen werden.

{S24} Die beA-Anwendung ist potentiell verwundbar gegenüber mehreren SQL-Injection-Schwachstellen.

{R24} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle:

Die Ausnutzbarkeit einer solchen Schwachstelle ist im Allgemeinen mittel. Die Schwierigkeit besteht darin, herauszufinden, welche Eingaben dazu führen, dass gewünschter SQL-Code ausgeführt wird. Beim beA ist die Schwachstelle aber nur beA-Anwendern zugänglich. Da auch kein konkreter Nachweis der Verwundbarkeit gefunden wurde, wird die Ausnutzbarkeit niedrig eingeschätzt.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung:

Mit einem Angriff ist es möglich zunächst die Datenbank und im Anschluss den gesamten Server zu übernehmen. Dadurch kann der Angreifer die Datenbank auslesen und verändern, was mittelbar auch die Vertraulichkeit von Nachrichten bedrohen kann, sofern eine Manipulation von Daten im SAFE BRAK gelingt (hierfür ist dann aber noch die Schwachstelle auszunutzen, dass der beA-Client Postfachzertifikate, die im Safe gespeichert sind, nicht überprüft, siehe Abschnitt 5.4.2). Im Rahmen der Analyse konnte nicht evaluiert werden, inwiefern die Schwachstellen tatsächlich ausnutzbar sind, da hierfür ein Quelltext-Audit notwendig wäre.

Bedrohung Integrität: **hoch**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **mittel**

Die Kombination hoher Bedrohung der Integrität mit niedriger Ausnutzbarkeit ergibt eine Bewertung der Schwachstelle als betriebsbehindernd.

{M24} Es sollte verifiziert werden, dass alle SQL-Statements vor ihrem Einsatz korrekt maskiert werden.

Von Entwickler-Seite wurde zugesichert, dass, bedingt durch die Software-Architektur, die Maskierung an vorgelagerten Stellen stattfindet. Eine Überprüfung der Aussage konnte aufgrund des Quelltext-Umfangs nicht durchgeführt werden.

4.5.2 Initialisierungs-Vector (IV)

Untersuchungsobjekt	Statische Quelltext-Analyse beA-Anwendung
Schwachstellenbehebung	-

Die Befunde der statischen Quelltext-Analyse der beA-Anwendung waren:

- `de/brak/bea/application/services/hsmmock/AESHandler.java:23`
  The use of java.util.Random is predictable [Scary(7), Normal confidence]
- `de/brak/bea/application/services/hsmmock/AESHandler.java:23`
  The use of java.util.Random is predictable [Scary(7), Normal confidence]
- `de/brak/bea/application/services/hsmmock/AESHandler.java:54`
  The initialization vector (IV) is not properly generated [Scary(7), Normal confidence]
- `de/brak/bea/application/services/hsm/util/HSMUtil.java:33`
  The use of java.util.Random is predictable [Scary(7), Normal confidence]
- `de/brak/bea/application/services/hsm/util/HSMUtil.java:83`
  The initialization vector (IV) is not properly generated [Scary(7), Normal confidence]

Die betroffenen Quelltext-Zeilen sind bspw.:

```
private Random random = new Random();
byte[] usedIV = createRandomIV();
cipher.init(Cipher.ENCRYPT_MODE, spec, new
IvParameterSpec(usedIV));
```

Die Verwendung von java.util.Random in Zusammenhang mit kryptographischen Funktionen ist ein schwerwiegendes Problem, da schwache Zufallszahlen eine Vielzahl von Angriffen ermöglichen, die schlussendlich die Sicherheit der kryptographischen Funktionen aushebeln.

Bei der Verschlüsselung sollte der JCE-Provider einen zufälligen Initialisierungsvektor generieren. Eingriffe sind hier nicht erforderlich. Die Qualität lässt sich nur verbessern, wenn man einen qualitativ hochwertigen Zufallszahlengenerator übergibt (z.B. HSM-Provider)

Die einzige Stelle, wo die Klasse „AESHandler.java“ nach bisheriger Analyse aufgerufen wird, ist das Package „de.brak.bea.application.services.hsmmock“. Mit hoher Wahrscheinlichkeit handelt es sich um Test Code, der in der Produktion durch HSM-Aufrufe ersetzt wird – was die Gefahr eines Angriffs relativiert. Auch bei der Klasse HSMUtil handelt es sich augenscheinlich um Test-Code, der nur unter bestimmten konfigurativen Bedingungen zum Einsatz kommt. Ohne zusätzliche Maßnahmen, insbesondere die Verwendung anderer Postfachzertifikate, würde eine Aktivierung dieses Codes dazu führen, dass das beA Nachrichten überhaupt nicht mehr umverschlüsseln kann.

Der Umstand, dass hier vermutlich Test-Code vorliegt, macht eine Bewertung der Schwachstelle schwierig. Die Ausnutzbarkeit von Test-Code ist abhängig von den Umständen, unter denen er aktiv wird, kann aber für die Zwecke der Risikobewer-

tung als niedrig eingestuft werden, da zusätzlich die Ausnutzung nur Innentätern offen steht. Die Gefährdung der Vertraulichkeit von Nachrichten ist aber bei Verwendung dieses Codes hoch. Bedroht sind die in der Datenbank abgelegten verschlüsselten Nachrichtenschlüssel, die aufgrund dieser Schwachstelle nicht ausreichend kryptographisch gesichert wären.

{S25} Schwächung der Kryptographie durch die unsichere Generierung von Initialisierungsvektoren

{R25} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle:

Niedrig, da vermutlich erst nach Aktivierung von Testcode zugänglich. Weiterhin ist die Ausnutzung nur Innentätern zugänglich, die Zugang zu den verschlüsselten Nachrichtenschlüsseln und -inhalten haben.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung:
Mit einem erfolgreichen Angriff können Nachrichtenschlüssel und damit Nachrichteninhalte aufgedeckt werden.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **hoch**

Die Kombination aus niedriger Ausnutzbarkeit und hoher Bedrohung der Vertraulichkeit ergibt eine Bewertung der Schwachstelle als betriebsbehindernd.

{M25} Nicht angemeldete Benutzer sollten keine Tickets auf dem Server erstellen können.

4.5.3 Unsicheres Auffüllen von Daten bei Verschlüsselung

Untersuchungsobjekt	Statische Quelltext-Analyse beA-Anwendung
Schwachstellenbehebung	-

Im Quelltext wurden Stellen gefunden, an denen im Zusammenhang mit Verschlüsselungsoperationen unsichere Padding-Algorithmen (gemäß BSI-Vorgaben) verwendet werden. Das gefährdet die Vertraulichkeit der so verschlüsselten Daten, die dann ggf. ohne Kenntnis geheimer Schlüssel entschlüsselt werden können. Die Ausnutzbarkeit ist niedrig, die Bedrohung der Vertraulichkeit allerdings hoch.

{S26} Es werden unsichere Padding-Algorithmen verwendet, die Angriffe auf damit verschlüsselten Daten erlauben.

{R26} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle:

Die Ausnutzbarkeit wird niedrig bewertet, da die betroffenen Kryptodaten nur Innentätern zugänglich sind und die Schwachstelle nicht zuverlässig das Entschlüsseln der Daten erlaubt.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung:

Ein erfolgreicher Angriff kann zur Offenlegung von Nachrichteninhalten führen. Hier sind potentiell alle im beA gespeicherten Nachrichten betroffen. Die Bedrohung der Vertraulichkeit ist daher hoch.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **hoch**

Die Kombination aus niedriger Ausnutzbarkeit und hoher Bedrohung der Vertraulichkeit ergibt eine Bewertung der Schwachstelle als betriebsbehindernd.

{M26} Unsichere Padding-Verfahren durch zurzeit als sicher geltende Verfahren ersetzen.

4.5.4 TLS-Zertifikate-Validierung

Untersuchungsobjekt	Quelltext-Audit beA-Client-Security
Schwachstellenbehebung	verifiziert, behoben

Für den SAML-Verbindungsaufbau wird ein vom Server nachgeladenes TLS-Zertifikat ohne weitere Überprüfung zur Nutzung freigegeben. Es agiert dann in der beA-Client-Security als Vertrauensanker für die Verifizierung weiterer TLS-Zertifikate. Auf diese Weise kann ein Angreifer die beA-Client-Security von Anwendern über die Identität der Server, mit denen die beA-Client-Security kommuniziert, täuschen. Er kann damit auch TLS-Verbindungen zwischen beA-Client-Security und beA-Anwendung aufbrechen. Dadurch erhält er Zugriff auf Metadaten der Kommunikation, aber noch nicht auf Nachrichteninhalte. Er kann in Benutzersitzungen eindringen und im Namen dieser Benutzer Nachrichten verschicken. Die Bedrohung für die Integrität ist daher mittel. Er kann auch die Nutzung des beA für alle Anwender gleichzeitig unterbinden. Die Bedrohung für die Verfügbarkeit ist daher hoch. Die Vertraulichkeit von Nachrichten ist nicht unmittelbar betroffen.

Der Angreifer muss ein Innentäter oder ein bereits über eine andere Schwachstelle in die beA-Anwendung eingedrungener Außentäter sein. Die vorzunehmende Mani-

pulation hat jedoch geringen Umfang. Die Ausnutzbarkeit wird daher als mittel eingestuft.

Diese Funktionalität ist laut Entwickler als Testcode im beA-System und nicht für den produktiven Einsatz gedacht. Eine Überprüfung der beA-Client-Security in diesem Punkt am laufenden System zeigte, dass zwar der Code für die Annahme des Zertifikats in der beA-Client-Security vorhanden ist, von der beA-Anwendung aber kein Zertifikat übermittelt wird. In der für die Verifizierung der Schwachstellenbehebung zur Verfügung gestellten Version der beA-Client-Security war dieser Testcode entfernt und die Schwachstelle damit behoben.

{S27} Nicht angemeldete Benutzer können beliebigen Text auf dem Server hochladen.

{R27} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle:
Ein Innentäter oder ein bereits durch eine andere Schwachstelle eingedrungener Außentäter kann den Angriff durchführen. Die Ausnutzbarkeit wird daher als mittel eingestuft.

Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Es kann in Benutzersitzungen eingedrungen und dann im Namen eines Benutzers Nachrichten versendet werden. Es ist auch möglich die gesamte Nutzung des beA-Systems zu unterbinden. Metadaten können eingesehen werden.

Bedrohung Integrität: **mittel**
Bedrohung Verfügbarkeit: **hoch**
Bedrohung Vertraulichkeit: **niedrig**

Die Kombination aus hoher Bedrohung der Verfügbarkeit, mittlerer Bedrohung der Integrität und mittlerer Ausnutzbarkeit ergibt eine Bewertung der Schwachstelle als betriebsbehindernd.

{M27} Die Möglichkeit, beim Verbindungsaufbau TLS-Zertifikate vom beA-Server nachzuladen, sollte entfernt werden.

Die Möglichkeit, TLS Zertifikate beim Verbindungsaufbau vom beA-Server nachzuladen und anschließend zu verwenden, wurde entfernt. Eine erneute Prüfung des entsprechenden Quellcode-Teils hat das bestätigt.

4.6 Auflistung der C-Schwachstellen

In der nachfolgenden Tabelle werden alle im Bereich der Quelltextanalyse identifizierten Schwachstellen der Kategorie C aufgelistet.

Tabelle 13: Quelltext C-Schwachstellen

Legende: h=hoch; m=mittel; n=niedrig; J=Ja		Bedrohung				
Kurzbeschreibung	Komponente	Ausnutzbarkeit	Vertraulichkeit	Integrität	Verfügbarkeit	Schwachstelle behoben
Unfertiger bzw. System-spezifischer Quelltext Die beA-Client-Security konstruiert an einer Stelle einen Dateinamen in einer Art und Weise, die nur unter dem Betriebssystem Windows funktioniert. Dies kann zu unerwartetem Verhalten auf anderen Betriebssystemen führen.	beA-Client-Security	m	n	n	m	-
Verwundbarkeit über unsichere XML-Deserialisierung. Würde Systemkontrollübernahme durch Innentäter erlauben. Das Schadenspotential wurde herabgestuft, da der betroffene Code augenscheinlich nicht aufgerufen wird.	OCSP-Relay	n	m	m	m	-
Möglicherweise unsicherer Quelltext - fest vergebene Namen für temporäre Dateien. Durch fest vergebene Namen für temporäre Dateien im Quelltext ist es einem Angreifer potentiell möglich, die Anwendung zu kompromittieren. Vor dem Ausnutzen muss aber das System des Anwenders über einen anderen Weg kompromittiert worden sein. Wurde als niedriges Risiko eingestuft, da dem Angreifer in der benötigten Position bessere Angriffsmöglichkeiten zur Verfügung stehen.	beA-Client-Security	n	n	n	n	-

4.7 Durch den CCC gemeldete Schwachstellen

Der Chaos-Computer-Club Darmstadt meldete am 20.12.2017 sechs Schwachstellen der beA-Anwendung an das BSI.

4.7.1 CCC 1: SSL-Zertifikat für bealocalhost.de kompromittiert

Überprüfung: Quelltext-Audit

Diese Schwachstelle wurde in der untersuchten Version der beA-Client-Security behoben.

4.7.2 CCC 2: beA-Client-Security startet unsicheren Webserver und Websocket

Überprüfung: Quelltext-Audit

Bemängelt wurde der ungeschützte Zugriff beliebiger Websites auf die Websocket-Schnittstelle der beA-Client-Security. Die Absicherung der WebSocket-Schnittstelle erfolgt nun mittels Überprüfung des Origin-Headers der Web-Sessions, der die Herkunft des Zugriffs ausweist und der vor böswilliger Manipulation besonders geschützt ist. Es werden nur Zugriffe durch die beA-Anwendung zugelassen. Das Setzen des Origin-Headers durch den Zugreifer in böswilliger Absicht scheint derzeit nicht möglich und ist dann wahrscheinlich auch nicht trivial. Sollte dies in der Zukunft z.B. durch einen Browser-Bug möglich sein, wäre diese Schutzmaßnahme gebrochen. Dann sollte eine auf kryptographische Verfahren gestützte Variante eingesetzt werden.

4.7.3 CCC 3: beA-Client-Security nimmt serialisierte Java-Objekte via Websocket entgegen und führt sie aus

Überprüfung: Quelltext-Audit

Diese Schwachstelle besteht nicht mehr. Durch die Aktualisierung der Bibliothek wurden die zuvor gemeldeten Schwachstellen bei der Deserialisierung behoben.

Durch die Überprüfung des Origin-Headers wurde zusätzlich eine neue Schutzebene eingezogen, so dass nicht mehr alle Daten, die an die beA-Client-Security über das WebSocket gesendet werden, deserialisiert werden.

4.7.4 CCC 4: Unterstützte Betriebssysteme sind veraltet

Einer der benannten Mängel bezeichnete die Betriebssystemversionen, die das beA unterstützt, als veraltet. Funktionstests für aktuelle Betriebssysteme wurden nicht durchgeführt. Es wird empfohlen, in Zukunft das beA-System auf aktuellen Betriebssystemen zu testen und freizugeben.

4.7.5 CCC 5: Client besteht aus stark veralteten Paketen (zum Teil aus 2011/2013)

Durch Einsatz aktueller Bibliotheken besteht diese Schwachstelle nicht mehr.

4.7.6 CCC 6: XSS-Schwachstelle in der beA-Webanwendung

Überprüfung: Nachweis durch Pentesting

Diese Schwachstelle ist in der aktuellen Version der beA-Anwendung behoben.

5 Konzeptionelle Analyse

5.1 Beschreibung des Analysegegenstandes

5.1.1 Form des Analysegegenstands und Betrachtungsweise

Der untersuchte Analysegegenstand war die Konzeptdokumentation des beA in seinem zum Stichtag aktuellen, vom Betreiber vorgelegten Stand. Sie bestand aus Use-Case-Beschreibungen, Feinkonzepten zum Gesamt-System und wichtigen Teilkomponenten, sowie Sicherheitsdokumentation.

Außerdem wurde die vorgelegte Sicherheitsdokumentation begutachtet.

Betrachtet wurden wesentliche Sicherheitsfunktionen des beA, die der Sicherung der **Vertraulichkeit** und **Authentizität** der via beA übermittelten Nachrichten dienen. Die benötigte Flexibilität beim Lesezugriff auf Empfängerseite erfordert eine Umverschlüsselung der Nachrichten, die einen Schwerpunkt der Analyse bildet. Ebenfalls betrachtet wurde die Zuverlässigkeit der Authentisierung bei der Anmeldung am beA-System, die auch für die Vertraulichkeit von Nachrichten und Metadaten Bedeutung hat. Schließlich wurde betrachtet, wie zuverlässig ein Empfänger den Urheber einer Nachricht erkennen kann.

Im Fokus der Analyse stand daher der kritische Pfad der Nachrichtenübertragung:

- Erstellen der verschlüsselten Nachricht durch einen Absender
- Versand und Ablage der verschlüsselten Nachricht im beA-Postfach
- Abruf von Nachrichten aus dem beA-Postfach durch berechtigte Leser
- Relevante Verwaltungsfunktionen: Verzeichnis möglicher Empfänger, Management von Administrations- und Leseberechtigungen, Einrichtung und Deaktivierung von Postfächern, Management von Zertifikaten und Schlüsseln.

5.1.2 Inhaltliche Beschreibung des Analysegegenstands

Im Folgenden werden Beschreibungen der Use-Cases zum besseren Verständnis der späteren Ausführungen wiedergegeben[1]:

[1] Die Beschreibungen basieren auf der Präsentation „Ende-zu-Ende Verschlüsselung im besonderen elektronischen Anwaltspostfach (beA)“, welche unter https://www.rak-berlin.de/download/pdf_beA_bisEnde2018/HSM_Atos.pdf verfügbar ist

Postfach einrichten

Beim Anlegen eines Postfachs wird ein asymmetrisches Schlüsselpaar generiert und mit dem symmetrischen Postfachschlüssel verschlüsselt in der Datenbank abgelegt. Für dieses Schlüsselpaar wird ein Zertifikatsrequest vom HSM signiert, das resultierende Zertifikat wird auch im SAFE BRAK abgelegt.

Anschließend kann das Postfach durch den Eigentümer in Besitz genommen werden.

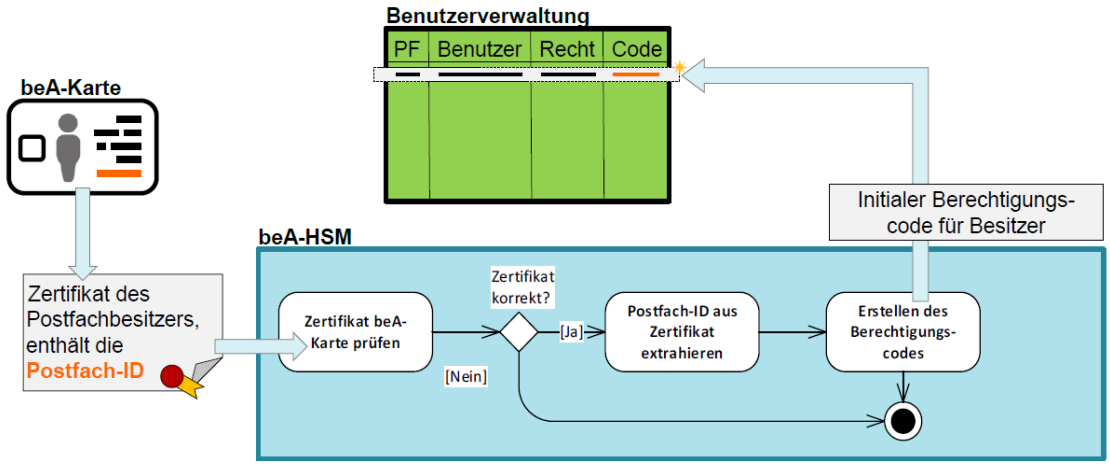

Abbildung 5: Postfach einrichten

Zur Erstellung des initialen Berechtigungscodes (Rechtevergabecode) eines Postfaches wird das Authentifizierungszertifikat der beA-Karte benötigt, welches die Postfach-ID enthält. Dazu wird eine Zertifikatskette übergeben, die unter Zuhilfenahme eines im HSM installierten Trust-Anchors (Root-Zertifikat) validiert wird. Durch die Einbettung der Postfach-ID in dem für den Postfachbesitzer ausgestellten Zertifikat erfolgt eine eineindeutige Zuordnung zum Postfach in der Rechteverwaltung. Mittels dieser speziell für das Postfach erstellten Karte wird sichergestellt, dass ausschließlich der berechtigte Benutzer (= Postfachbesitzer) Zugriff auf das Postfach erlangt.

Management von Administrations- und Leserechten

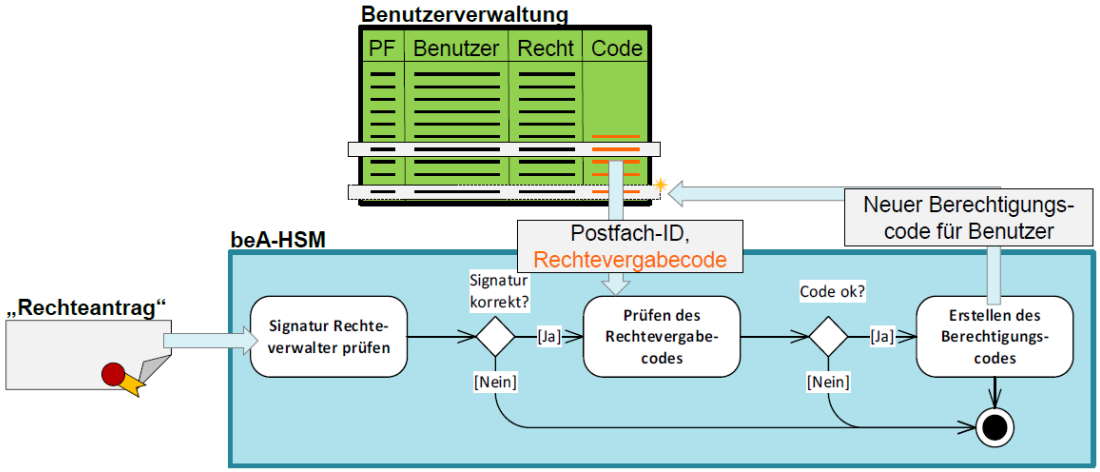

Abbildung 6: Management von Administrations- und Leserechten

Berechtigungscodes werden nur durch das HSM erzeugt. Nur Benutzer, für die in der Benutzerverwaltung ein Berechtigungscode zur Vergabe von Rechten (Rechtevergabecode) vorliegt, können vom HSM neue Berechtigungscodes für andere Benutzer erstellen lassen. Beim Rechteantrag handelt es sich um ein durch den Rechteverwalter signiertes Datenobjekt, welches den öffentlichen Schlüssel des zu Berechtigenden (bei Gewährung von Nachrichtenzugriff der öffentliche Schlüssel des Verschlüsselungszertifikats und bei Gewährung von Rechteverwaltung der des Authentifizierungszertifikats) und das gewünschte Recht (Zugriff oder Rechteverwaltung) enthält.

Zertifikatsmanagement

Die meisten Zertifikate innerhalb der beA-Anwendung werden durch die Bundesnotarkammer ausgestellt. Dies umfasst u. A. die Zertifikate für die HSM, für die Postfächer sowie für die Nutzer von beA-Karten. In den HSM sind die notwendigen Root-Zertifikate der Bundesnotarkammer als Trust-Anchors (Vertrauensanker) hinterlegt. Die Postfach- sowie Nutzerzertifikate werden mittels SAFE-Server verwaltet.

Versand von Nachrichten

Der Versand von Nachrichten spielt sich im Großen und Ganzen auf dem Client des Benutzers ab. Dazu wird ein symmetrischer Schlüssel gebildet, mit dem die Nachricht und eventuelle Anhänge verschlüsselt werden. Dieser symmetrische Schlüssel wird dann mit Hilfe der Zertifikate der Empfänger der Nachricht mit den zugehörigen öffentlichen Schlüsseln (Postfachschlüssel, nicht Anwaltsschlüssel) verschlüsselt (sowie zusätzlich mit dem öffentlichen Schlüssel des eigenen Postfachs, um die gesendeten Nachrichten später einsehen zu können). Anschließend wird die Nachricht zur Ablage in den entsprechenden Postfächern an die beA-Anwendung übertragen.

Ablage von Nachrichten im beA

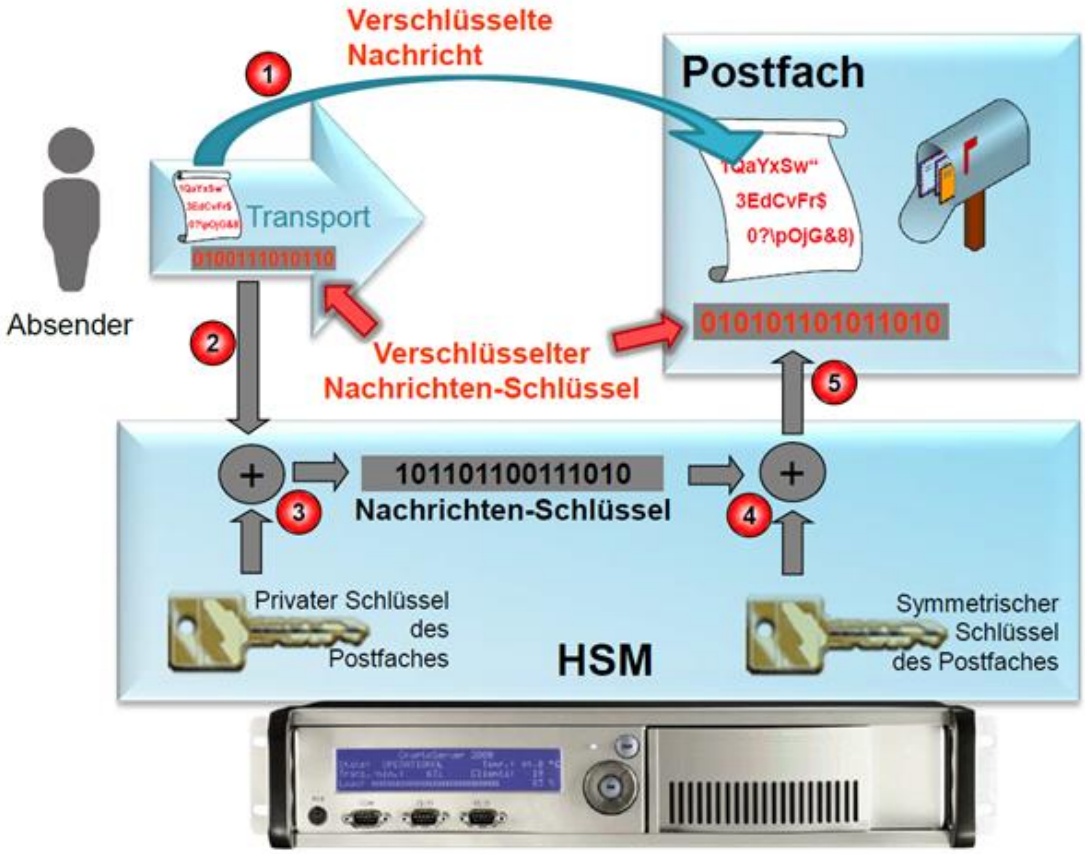

Abbildung 7: Ablage von Nachrichten im beA

Ablauf der Ablage einer empfangenen Nachricht im Postfach:

1. Ein verschlüsselter Nachrichtencontent wird ohne Veränderung im Postfach gespeichert.

2. Der zugehörige mit dem öffentlichen Postfachschlüssel verschlüsselte Nachrichtenschlüssel wird an das HSM zur Umverschlüsselung übergeben.

3. Entschlüsselung des mit dem öffentlichen Postfachschlüssel verschlüsselten Nachrichtenschlüssels mittels privaten Postfachschlüssels.

4. Verschlüsselung des Nachrichtenschlüssels mit dem symmetrischen Schlüssel des Postfaches.

5. Speicherung des mit dem symmetrischen Schlüssel des Postfaches verschlüsselten Nachrichtenschlüssels im Postfach.

Der symmetrische Postfachschlüssel wird auch zur Ver- und Entschlüsselung der im Postfach abgelegten verschlüsselten Betreffzeilen (werden vom Client beim ersten Lesen an die beA-Anwendung verschlüsselt zurückgeschickt) verwendet.

Abruf von Nachrichten

Bevor ein angemeldeter Benutzer Nachrichten abrufen kann, muss ein temporärer Kommunikationsschlüssel durch das HSM erstellt und dem Benutzer mitgeteilt werden.

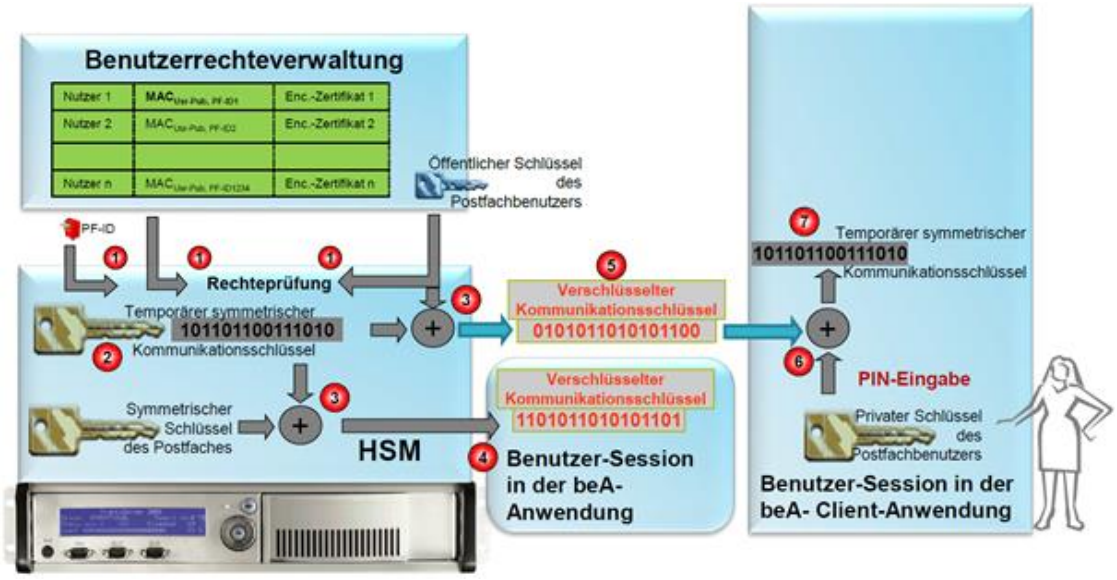

Abbildung 8: Abruf von Nachrichten (Teil 1)

Ablauf der Erstellung eines symmetrischen Kommunikationsschlüssels, der Speicherung, der Übertragung und der Entschlüsselung auf dem Client:

1. Prüfung der Berechtigung der Nachrichtenentschlüsselung eines bestimmten Postfaches für einen Benutzers des beA durch ein HSM.

2. Nach der Anmeldung eines Benutzers am System wird beim ersten Zugriff auf ein Postfach ein temporärer symmetrischer Kommunikationsschlüssel (AES-256) im HSM gebildet.

3. Dieser Kommunikationsschlüssel wird zum einen mit dem öffentlichen Postfach-Schlüssel des Benutzers und zum anderen mit dem symmetrischen Postfachschlüssel (für jedes PF, auf welches der Benutzer Zugriffsrechte hat) im HSM verschlüsselt.

4. Zwischenspeicherung der beiden verschlüsselten Kommunikationsschlüssel in der Benutzer-Session der beA-Anwendung.

5. Aufbau einer TLS-Verbindung und Übertragung des mit dem öffentlichen Schlüssel des autorisierten Benutzers verschlüsselten Kommunikationsschlüssels an den Client des Benutzers.

6. Entschlüsselung des Kommunikationsschlüssels mit dem privaten Postfach-Schlüssel des Benutzers beim Benutzer.

7. Zwischenspeicherung des entschlüsselten Kommunikationsschlüssels in der Client-Session beim Benutzer.

Anschließend kann der Client Nachrichten vom Postfach abholen.

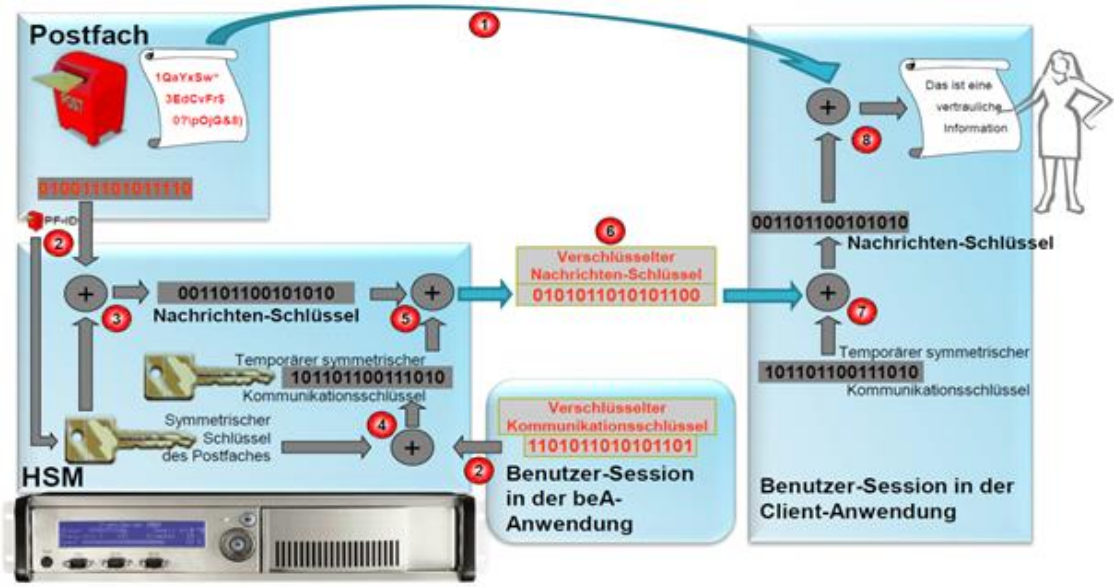

Abbildung 9: Abruf von Nachrichten (Teil 2)

Ablauf der Abholung einer Nachricht aus dem Postfach und Entschlüsselung auf dem Client mit dem temporären symmetrischen Kommunikationsschlüssel:

1. Ein verschlüsselter Nachrichtencontent wird ohne Veränderung aus dem Postfach an den Client übertragen.

   Die Schritte 2-4 werden innerhalb der HSM durchgeführt. Als Resultat wird nur das Ergebnis aus Schritt 4 zurückgegeben.

2. Entschlüsselung des mit dem symmetrischen Postfachschlüssel verschlüsselten Nachrichtenschlüssels innerhalb des HSM.

3. Entschlüsselung des mit dem symmetrischen Postfachschlüssel verschlüsselten Kommunikationsschlüssels innerhalb des HSM.

4. Verschlüsselung des Nachrichtenschlüssels mit dem symmetrischen Kommunikationsschlüssel innerhalb des HSM. Nur das Resultat dieser Verschlüsselung wird vom HSM wieder an die beA-Anwendung zurückgegeben.

5. Übertragung des mit dem symmetrischen Kommunikationsschlüssel verschlüsselten Nachrichtenschlüssels an den Client.

6. Entschlüsselung des Nachrichtenschlüssels beim Client mit dem Kommunikationsschlüssel.

7. Entschlüsselung der Nachricht beim Client mit dem Nachrichtenschlüssel.

Management der HSM-Schlüssel

Die gesamte kryptographische Sicherung der Vertraulichkeit der Nachrichten im beA-System basiert auf der Geheimhaltung eines Satzes von Arbeitsschlüsseln, sogenannter Master-Schlüssel, die in den HSM gespeichert sind und dort verwendet werden, um Nachrichtenschlüssel oder private Postfachschlüssel zu ver- und entschlüsseln, was auch für die Umverschlüsselung genutzt wird.

Insbesondere werden Nachrichtenschlüssel (siehe Ablage von Nachrichten, Schritt 4) mit einen symmetrischen Schlüssel des Postfachs verschlüsselt im beA-System in einer Datenbank gespeichert. Dieser symmetrische Postfachschlüssel wird unter Verwendung der Postfach-ID aus einem Master-Schlüssel gebildet, der in den HSM gespeichert ist. Die Kenntnis dieses Master-Schlüssels erlaubt die Entschlüsselung aller im BeA-System gespeicherten Nachrichten, da die Postfach-IDs selbst nicht geheim sind. Auf seiner Vertraulichkeit basiert die Vertraulichkeit jeder Nachricht im beA.

Es gibt weiterhin Master-Schlüssel für die Erstellung von Berechtigungscodes und für die verschlüsselte Speicherung der privaten Postfachschlüssel außerhalb des HSM, sowie Master-Schlüssel, die beim Abruf von Nachrichten Verwendung finden.

Diese Master-Schlüssel wurden vom Betreiber des beA in einem abgesicherten Rechenzentrum erzeugt, mit einem sogenannten Key Encryption Key (KEK) verschlüsselt, sodann der Key Encryption Key und die verschlüsselten Master-Schlüssel an den Auftraggeber übergeben, die diese seither verwahrt. Der Auftraggeber stellt den KEK sowie die Master-Schlüssel in Schlüsselzeremonien (abgesicherten Verfahren zur Eingabe oder Erzeugung von Schlüsseln) zur Verfügung, wenn ein HSM an einem beA-Systemstandort mit diesen Schlüsseln in Betrieb genommen werden soll.

Die Sicherheit des KEK wird durch Schlüsselteilung, physikalisch getrennte Verwahrung und physikalisch auf spezifische Mitarbeiter des Auftraggebers, die sogenannten Key Custodians, beschränkten Zugriff geschützt. Die beiden Teile des KEK, die nur zusammen die Entschlüsselung und das Einspielen der Master-Schlüssel in ein HSM erlauben, sind auf Papier in versiegelten Briefumschlägen in Safes verwahrt.

Zu jeder Art von Master-Schlüssel sind 100 Varianten erzeugt und gespeichert, von denen aber jeweils immer nur eine von allen HSMs verwendet wird. Die Master-Schlüssel werden im Jahresrhythmus gewechselt, indem eine neue Variante gewählt wird.

5.2 Methodik und Vorgehensweise

Durchgeführt wurde eine Analyse nach Dokumentenlage, insbesondere der Beschreibungen der Use-Cases des kritischen Pfades:

- Postfach einrichten
- Management von Rechten
- Zertifikatsmanagement

- Versand von Nachrichten
- Ablage von Nachrichten im beA
- Abruf von Nachrichten
- Management der HSM-Schlüssel

Die Use-Case-Beschreibungen lagen als Ablaufbeschreibungen mit Auslöser, Vor- und Nachbedingungen sowie als Ablaufdiagramme vor.

Des Weiteren wurden das Feinkonzept HSM und andere Feinkonzepte analysiert, wo Informationen über Sicherheitseigenschaften der Use-Cases gefunden wurden, die sich nicht aus der beschriebenen Prozesslogik selbst ergeben.

Die durch die Use-Cases beschriebenen logischen Prozessabläufe wurden einer Bedrohungsanalyse unterworfen, wie sie für die Erstellung von Sicherheitskonzepten für Objekte mit hohem Schutzbedarf üblich ist. Als Schwachstellen wurden Angriffsmöglichkeiten bezeichnet, die nicht dem Schutzzweck entsprechend hinreichend durch die Prozesslogik oder die in den Dokumenten erkennbaren Sicherheitsmaßnahmen abgewehrt werden. Die Darstellung der Schwachstellen und die Risikobewertung erfolgte dann nach dem in Kapitel 2 erläuterten Verfahren.

Die vorgelegte Sicherheitsdokumentation wurde hinsichtlich der Frage beurteilt, ob sie eine vollständige Abwehr aller nicht tragbaren Sicherheitsrisiken nachweisen kann.

5.3 Übersicht der Schwachstellen

Tabelle 14: Schwachstellenübersicht Konzeptanalyse

Schwachstelle	Einstufung	behoben
Verwendung von Javascript beim beA_Client	A	-
Client prüft Postfachzertifikate nicht	A	-
BNotK kann Ursprung der Zertifikatsanträge aus HSM nicht erkennen	B	-
EGVP-Bürger-Verzeichniseinträge im SAFE können irreführend sein	B	-
HSM-Schlüssel existieren außerhalb des HSM	B	-
Berechtigungs-MACs können nicht sicher widerrufen werden	C	-
Die Postfach-ID wird bei der Beantragung einer Berechtigung nicht mitsigniert.	C	-

5.4 Beschreibung der A-Schwachstellen

Im Folgenden werden die im Konzept des beA vorgefundenen Schwachstellen beschrieben, die aufgrund hoher Ausnutzbarkeit und/oder hoher Bedrohung ein betriebsverhinderndes Risiko darstellen und vor Wiederinbetriebnahme des beA beseitigt werden sollten.

5.4.1 Verwendung von Javascript beim beA_Client

Der beA-Client-Security besteht aus mehreren Teilen. Ein Teil wird als Javascript-Code vom beA-Server ausgeliefert, welcher im Browser des Nutzers ausgeführt wird. Dieser Teil steuert die beA-Client-Security, welche für Verschlüsselung, Entschlüsselung und Authentisierung zuständig ist.

Ein Innentäter kann diesen Code mit der Absicht modifizieren, Nachrichten beim Versenden unverschlüsselt in eine beliebige Richtung zu versenden.

Bei Verwendung von Javascript gibt es keinen Mechanismus, der sicherstellt, dass es sich um den vorgesehenen (unmanipulierten) Code handelt. Ob der Code auf dem beA-Server manipuliert wurde, ist durch den Client nicht erkennbar. Die beA-Client-Security kann auch von manipulierten Javascript-Programmen angesprochen und verwendet werden (z.B. zur Anmeldung am Portal). Alle eingegebenen oder angezeigten Daten können jedoch kompromittiert sein und z.B. zusätzlich an den Angreifer gesendet werden. Mittels böswillig modifizierten Javascript-Codes können alle beA-Nutzer auf einmal angegriffen werden. Es ist dann möglich, alle versendeten Nachrichten im Klartext auszuleiten.

{S28} Der Javascript-Code liegt auf dem beA-Webserver gegen Veränderung ungesichert vor.

{R28} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit der Schwachstelle:

Der Javascript-Code kann durch einen Innentäter mit Schreibrecht auf dem beA-Frontend leicht, von einem Außentäter unter Ausnutzung einer ggf. noch vorhandenen Schwachstelle, über die er sich unberechtigt Zugang zum Frontend verschafft, ausgenutzt werden. Sobald ein schreibender Zugriff auf die Javascript-Seiten besteht, ist die Fortsetzung des Angriffs trivial. Da sowohl Innentäter als auch Außentäter nicht ausgeschlossen werden können, wird die Ausnutzbarkeit als mittel bewertet.

Bewertung der Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Ein erfolgreicher Angreifer kann mit einem Angriff alle vom Beginn des Angriffs an versendeten Nachrichten aller beA-Nutzer einsehen. Aufgrund

des potentiellen Zugriffs auf alle Postfächer wird die Bedrohung der Vertraulichkeit als hoch eingestuft.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **hoch**

Die Kombination aus hoher Bedrohung und mittlerer Ausnutzbarkeit ergibt die Bewertung als betriebsverhindernde Schwachstelle.

{M28} Das ausgelieferte Javascript muss regelmäßig in kurzen Abständen von einem separaten System auf Unversehrtheit, z.B. durch Checksummen, geprüft werden.

Zudem sollten die Nutzer darauf sensibilisiert werden, darauf zu achten, dass sich der beA-Server mit einem korrekten TLS-Zertifikat ausweist.

Erwägenswert ist das Angebot eines elektronisch signierten „Fat Clients“, also ein vollständiges, lokal installierbares beA-Client-Security-Programm, welches keinen Code mehr von einem Server nachlädt und dessen Integrität kryptographisch gesichert ist. Ebenfalls zu erwägen ist eine Offenlegung der Schnittstellen zwischen beA-Client-Security und -Server, was die Entwicklung von Open-Source-Implementierungen für den beA-Client-Security ermöglichen würde.

Anmerkung: Kanzleisoftware, die nur die REST-API des beA-Servers verwendet, ist nicht betroffen.

5.4.2 Client prüft Postfachzertifikate nicht

Beim Versenden von Nachrichten wird der öffentliche Schlüssel aus dem Postfachzertifikat des vorgesehenen Empfängers verwendet. Die öffentlichen Schlüssel von Postfächern liegen im SAFE BRAK in von der BNotK zertifizierter Form vor.

Der Client geht aber davon aus, dass die von der beA-Anwendung aus dem SAFE BRAK gelieferten Daten korrekt sind und prüft daher weder die Signatur der BNotK unter einem beA-Postfachzertifikat, noch seinen Sperrstatus. Dies ermöglicht es einem Innentäter, der berechtigten Zugang zu den SAFE-Verzeichnisdaten hat, oder einem Angreifer, der sich via Internet unter Ausnutzung von Sicherheitslücken in der beA-Anwendung schreibenden Zugriff auf das Verzeichnis verschafft hat, ein falsches Postfachzertifikat für eine beliebige SAFE_ID einzuspielen, wobei er dabei einen öffentlichen Schlüssel im Zertifikat verwenden wird, für den er den privaten Schlüssel besitzt (Schlüssel und Zertifikate lassen sich sehr einfach mit allgemein bekannten Mitteln erzeugen). Da der Client das Postfachzertifikat nicht prüft, ist es dabei unerheblich, dass es sich um ein offensichtlich falsches, weil nicht von der BNotK signiertes, beA-Postfachzertifikat handelt. Der Angreifer kann auf diese Weise die an die entsprechende SAFE_ID adressierten Nachrichten mitlesen. Dies kann er zudem unbemerkt tun, weil er die Nachrichten nach dem Lesen in für das Postfach korrekter Weise umverschlüsseln und an das beA weiterleiten kann. Er

kann dabei eine beliebige Menge von Postfächern auf einmal erfolgreich angreifen. Der Verzicht auf die Prüfung der Postfachzertifikate in der beA-Client-Security führt dazu, dass die Sicherheitsfunktion der von der BNotK ausgestellten Postfach-Zertifikate vollständig ohne Wirkung bleibt.

Die Verwendung gesperrter beA-Postfachzertifikate ist allerdings hinreichend wirksam erschwert, da der zugehörige private Schlüssel innerhalb eines beA-HSM erzeugt wurde und nur verschlüsselt außerhalb des HSM existiert. Die Möglichkeit, dass ein Angreifer ein ordnungsgemäß ausgestelltes beA-Postfachzertifikat einschließlich des zugehörigen privaten Schlüssels besitzt, besteht nur, wenn auf die Behebung der Schwachstelle 5.5.1 verzichtet wird. Vorbehaltlich einer Behebung der dort genannten Schwachstelle ist eine Prüfung des Sperrstatus der Postfachzertifikate bei der BNotK nicht notwendig.

{S29} Der Client prüft Postfachzertifikate vor dem Versenden von Nachrichten nicht.

{R29} Risikobewertung: **A-Betriebsverhindernd**

Ausnutzbarkeit:

Für die Ausnutzung der Schwachstelle benötigt ein Angreifer nur Schreibzugriff auf den SAFE BRAK. Hierfür kommen neben einem Innentäter auch Außentäter in Frage, die den SAFE BRAK oder eine andere Komponente des beA-Systems erfolgreich übernommen haben. Einem Angreifer stehen mehrere Angriffspunkte zur Auswahl, die Schwachstelle auszunutzen, Angriff auf den SAFE BRAK, dessen Datenbank oder das System, das die Postfach-Zertifikate an den SAFE BRAK liefert. Daher wird die Ausnutzbarkeit als mittel bewertet.

Bewertung der Ausnutzbarkeit: **mittel**

Bewertung der Bedrohung:

Innentäter oder erfolgreiche Angreifer auf den SAFE BRAK könnten die ausgelieferten Zertifikate und zugehörigen Informationen unbemerkt durch eigene ersetzen und so umfassend Nachrichten mitlesen.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **hoch**

Die Kombination aus mittlerer Ausnutzbarkeit und hoher Bedrohung ergibt die Bewertung als betriebsverhindernde Schwachstelle.

{M29} Die beA-Client-Security muss das beA-Postfachzertifikat prüfen (elektronische Unterschrift der BNotK). Auf die fehlende Prüfbarkeit von EGVP-Zertifikaten und die damit verbundenen Risiken muss der Versender hingewiesen werden. Eine Prüfung des Sperrstatus von Postfachzertifikaten, die die BNotK ausgestellt hat, erscheint nicht notwendig, da eine Reihe anderer Mechanismen eine Wiederverwendung eines kompromittierten Postfach-Schlüssels erschweren und eine Kompromittierung eines beA-

Postfachzertifikats nur unter Ausnutzung der Schwachstelle 5.5.1 möglich erscheint. Eine Aufdeckung privater Postfachschlüssel im beA erscheint nur möglich unter Ausnutzung der Schwachstelle 5.5.3, ist dann aber nicht mehr notwendig, weil im dort beschriebenen Fall die Nachrichten dem Angreifer schon ohne Kompromittierung privater Postfachschlüssel zugänglich sind.

5.5 Beschreibung der B-Schwachstellen

5.5.1 BNotK kann Ursprung der Zertifikatsanträge aus HSM nicht erkennen

Die zentrale beA-Anwendung beantragt automatisiert Zertifikate für die Postfächer bei der BNotK. Dazu wird ein elektronischer Zertifikatsantrag benutzt, der den öffentlichen Postfachschlüssel enthält und mit dem privaten Postfachschlüssel signiert wird.

Die BNotK kann allerdings nicht feststellen, ob ein Zertifikatsantrag tatsächlich – wie vorgesehen – in dem HSM signiert wurde und sich auf Schlüssel bezieht, die in dem HSM erzeugt wurden, da eine Authentisierung des HSM im Zertifikatsantrag nicht enthalten ist.

Ein Innentäter oder ein erfolgreicher Angreifer der beA-Anwendung kann also auch Zertifikatsanträge mit eigenen Schlüsseln erstellen und an die BNotK zur Zertifikatsausstellung senden. Das von der BNotK daraufhin erstellte Zertifikat kann der Angreifer dann zusammen mit den eigenen Schlüsseln für weitere Angriffe nutzen. Hier sind verschiedene Szenarien denkbar, z.B.:

1. Der Angreifer manipuliert die beA-Anwendung in der Weise, dass diese bei Postfächern, welche mit Schlüsseln des Angreifers angelegt wurden, eigene Krypto-Routinen des Angreifers verwendet anstelle des HSM. Somit kann der Angreifer im Namen des eigentlichen Postfachbesitzers agieren, also sowohl Nachrichten lesen als auch erstellen, ohne dass dies dem eigentlichen Postfachbesitzer oder den Administratoren unmittelbar auffällt. Selbst die Datenbankinhalte wären völlig unauffällig, da die Chiffrate als solche nicht als außerhalb des HSM erstellt erkannt werden können. Der Angreifer muss natürlich zusehen, dass die Manipulation der beA-Anwendung möglichst (lange) nicht auffällt.

2. Der Angreifer kann gezielt einem potentiellen Absender das erstellte Zertifikat unterschieben, um dann die versendeten Nachrichten abzufangen. Um nicht aufzufallen, kann er dann das echte Zertifikat des Empfängers verwenden, um die Nachricht weiterzuleiten.

{S30} Zertifikatsanträge für Postfachschlüssel enthalten keine Authentisierung der signierenden HSM

{R30} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle:

Der Angreifer benötigt Zugriff auf die Schnittstelle, über die die BNotK Zertifizierungsanträge für Postfachschlüssel entgegennimmt und ausgibt, und Zugriff auf den SAFE BRAK, um das erschlichene Zertifikat Versendern von Nachrichten anzubieten. Dies ist unmittelbar nur einem Innentäter oder einem erfolgreichen Angreifer möglich, der über geeignete Zugriffs-Rechte auf zwei Teilkomponenten des beA verfügt (SAFE BRAK und Schnittstelle zur BNotK).

Bewertung Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung:

Innentäter oder erfolgreiche Angreifer können neue oder bestehende einzelne Postfächer unbemerkt unter ihrer Kontrolle halten und Inhalte mitlesen oder verändern. Sie können einen erfolgreichen Angriff gegen jedes beliebige Postfach ohne nennenswerten Mehraufwand wiederholen und somit, solange der Angriff läuft, potentiell Zugriff auf den Inhalt aller eingehenden Nachrichten bekommen. Das Schadenspotential ist somit deutlich höher als bei einem Angriff auf ein Postfach bei einem beA-Anwender über dessen IT-Infrastruktur. Bereits vor dem Angriff vorhandene Nachrichten sind nicht gefährdet.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **hoch**

Die Einstufung des Risikos als betriebsbehindernd ergibt auch aus der Kombination geringer Ausnutzbarkeit mit einem hohen Schadenspotential.

{M30} Es wird empfohlen, dafür zu sorgen, dass die BNotK erkennen kann, dass der Zertifikatsantrag im HSM signiert wurde und Schlüssel enthält, die im HSM erzeugt wurden. Dies ist technisch z.B. durch eine elektronische Gerätesignatur realisierbar.

5.5.2 EGVP-Bürger-Verzeichniseinträge im SAFE können irreführend sein

Damit auch Bürger mit den Nutzern des beA kommunizieren können, sind diese in der beA-Client-Security adressierbar. Die SAFE-Einträge, die der Bürger mit dem EGVP anlegen kann, werden allerdings bei der Einrichtung nicht geprüft, weshalb hier Phantasiedaten angegeben sein können.

Dabei kann der Bürger auch Bezeichnungen wählen, die mit Institutionen oder anderen Personen assoziiert werden. Es gibt einen Schutz dagegen, dass Bürger für sich selbst Bezeichnungen als Gerichte wählen, sie können sich aber bspw. für einen Anwalt ausgeben. Die frei gewählten Bezeichnungen werden bei einer entspre-

chenden Suche im Client angezeigt, ohne dass ihr Ursprung (Rolle EGVP-Bürger) direkt erkennbar ist. Dies könnte zum Versand vertraulicher Informationen an den falschen Adressaten führen.

Die Kommunikation von beA-Nutzern mit EGVP-Nutzern hat allgemein aufgrund mangelnder Authentifizierung für Bürger und ungeeigneter Verschlüsselungszertifikate (Verwendung nicht prüfbarer Zertifikate) nicht das Sicherheitsniveau der Vertraulichkeit von Nachrichten, das vom beA angestrebt wird. Im EGVP wird der Vertraulichkeit von Nachrichten nicht die gleiche Bedeutung.

{S31} In der Rolle EGVP-Bürger können beliebige ungeprüfte Verzeichniseinträge in SAFE vorgenommen werden, z.B. auch auf den Namen eines Anwalts oder eines anderen Bürgers. Dies kann Versender irreführen und sie dazu bringen, Nachrichten falsch zu adressieren.

{R31} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit der Schwachstelle:

Für Angreifer ist eine Registrierung unter wirksam irreführenden Namen im EGVP leicht möglich. Der Angriff kann durch jedermann erfolgen und benötigt kaum Aufwand und keine Überwindung einer Sicherheitsmaßnahme. Es ist nicht klar, in wie weit sich beA-Nutzer der Gefahr der Irreführung durch EGVP-Nutzer bewusst sind. Für die Bewertung wird angenommen, dass dieses Bewusstsein teilweise vorhanden ist, was den Kreis der angreifbaren beA-Nutzer einschränkt (auf die, die sich der Gefahr der Irreführung nicht bewusst sind). Durch diese Annahme wird die Einstufung der Ausnutzbarkeit ein von „hoch“ auf „mittel“ gesenkt.

Bewertung der Ausnutzbarkeit: **Mittel**

Bewertung der Bedrohung:

Angreifer können Zugang zu Nachrichten von beA-Nutzern an andere Anwälte und Mandanten erhalten, wenn die beA-Nutzer die Irreführung nicht erkennen. Dabei können eine Vielzahl von Kommunikationsbeziehungen angegriffen werden. Der Zugang ist allerdings nicht umfassend auf alle Nachrichten des beA oder auf ein ganzes beA-Postfach, weshalb die Bedrohung für die Vertraulichkeit als mittel bewertet wird.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **mittel**

Die Kombination aus mittlerer Ausnutzbarkeit und mittlerer Bedrohung der Vertraulichkeit ergibt die Bewertung als betriebsbehindernde Schwachstelle.

{M31} In der beA-Client-Security sollte klar erkennbar sein, ob es sich bei einem Adressaten um einen authentisierten Nutzer handelt oder nicht. Auf jeden Fall sollte erkennbar sein, wenn der Adressat die Rolle EGVP-Bürger hat (Warnung vor ungeprüften Angaben).

5.5.3 HSM-Schlüssel existieren außerhalb des HSM

Das HSM verwendet zur verschlüsselten Ablage und zur Umverschlüsselung Arbeitsschlüssel. Die Arbeitsschlüssel liegen auch außerhalb des HSM als verschlüsselte Dateien vor, die mit ebenfalls außerhalb des HSM vorliegenden Key Encryption Keys entschlüsselt werden können.

Elementar geht es um die Sicherheit der verschlüsselten Arbeitsschlüssel (Master-Key-Sets) für die verschiedenen Zwecke des HSM und der Schlüssel (Key Encryption Keys, KEKs), mit denen die Arbeitsschlüssel verschlüsselt sind, sowie die Verwahrung der mit den KEKs verschlüsselten Master-Key-Sets. Wer sich in den Besitz dieses Schlüsselmaterials bringt, kann die im beA-System gespeicherten Nachrichten auch ohne HSM entschlüsseln, unverzüglich und umfassend, d.h. jede Nachricht kann davon betroffen sein.

Die Arbeitsschlüssel sowie die Schlüssel, mit denen sie entschlüsselt werden können, sind vom Betreiber des beA erzeugt worden, an den Auftraggeber übergeben worden und seither in seinem Besitz. Sie sind dort mit organisatorischen Maßnahmen gesichert, die teilweise dokumentiert, teilweise mündlich beschrieben wurden (Verwahrung des KEK in zwei Teilen, mit getrenntem Zugriff auf jeden Teil durch einen Key Custodian, Ablage in versiegelten Umschlägen in Safes). Der Zugriff ist dadurch stark erschwert, aber nicht unmöglich.

Der Missbrauch dieser Schlüssel kann auf zwei Arten geschehen: die Key Custodians des Auftraggebers und ein Helfer beim Betreiber des beA führen den verschlüsselten Nachrichtenbestand und die Schlüssel zusammen und sind dann in der Lage, die Nachrichten zu entschlüsseln. Oder es wurde unberechtigt beim Betreiber des beA nach der Erzeugung der Schlüssel vor der Übergabe an den Auftraggeber an einer Stelle eine Kopie erstellt. Dann kann das Personal des Betreibers alleine die Nachrichten entschlüsseln.

Vor diesem Hintergrund besteht zudem die Möglichkeit, dass der Auftraggeber im Rahmen von Beschlagnahmen von Postfächern gezwungen werden könnte, Nachrichten offenzulegen. Damit sind rechtliche Fragen verbunden, die im Rahmen dieses Gutachtens nicht beantwortet werden können. Daher wurde diese Möglichkeit auch nicht in die Bewertung der Ausnutzbarkeit einbezogen.

Die Verwahrung der Schlüssel außerhalb der HSM dient der Inbetriebnahme neuer HSM. Diese Praxis ist nicht unüblich und findet z.B. im Bankwesen oft Anwendung. Damit sie für das beA geeignet ist, ist es erforderlich, dass die beA-Anwender als potentiell vom Bruch der Vertraulichkeit Bedrohte dem Auftraggeber und dem Betreiber des beA ausreichend vertrauen. Ob dies der Fall ist, kann im Rahmen dieses Gutachtens nicht beurteilt werden. Ist ausreichendes Vertrauen vorhanden, kann die hier aus technischer Sicht (Möglichkeit und Umfang des Schadens) als betriebsbehindernd riskant bewertete Praxis fortgesetzt werden.

{S32} Alle HSM-Schlüssel existieren auch außerhalb des HSM.

{R32} Risikobewertung: **B-Betriebsbehindernd**

Ausnutzbarkeit:

Der Angriff ist nur durch bestimmte Innentäter durchführbar, die dabei eine Vertrauensstellung haben müssen, die sie missbrauchen. Die Ausnutzbarkeit ist daher niedrig.

Bewertung der Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung:

Der Angriff erlaubt die umfassende Aufdeckung des Inhalts aller in beA-Postfächern gespeicherten Nachrichten. Die Bedrohung wird daher als hoch eingeschätzt.

Bedrohung Integrität: **niedrig**
Bedrohung Verfügbarkeit: **niedrig**
Bedrohung Vertraulichkeit: **hoch**

Die Kombination aus niedriger Ausnutzbarkeit und hoher Bedrohung ergibt eine Bewertung der Schwachstelle als betriebsbehindernd.

{M32} Die HSMs sollen die Arbeitsschlüssel selbst erzeugen, und nur in verschlüsselter Form zur Übertragung auf andere HSMs herausgeben (Key-Wrapping).
Alle HSM-Schlüssel sollten nur innerhalb speziell gesicherter Hardware (HSM, Chipkarte) gespeichert werden.

5.6 Auflistung der C-Schwachstellen

Es wurden zwei Schwachstellen mit der Risikobewertung C gefunden.

Tabelle 15: Konzept C-Schwachstellen

Kurzbeschreibung	Bedrohung				
Legende: h=hoch; m=mittel; n=niedrig; J=Ja	Ausnutzbarkeit	Vertraulichkeit	Integrität	Verfügbarkeit	Schwachstelle behoben
Berechtigungs-MACs können nicht sicher widerrufen werden, sondern nur durch Entfernung aus der Berechtigungsdaten-bank deaktiviert werden. Ein Wiedereinspielen bleibt möglich, was ehemals berechtigten Lesern eines Postfachs wieder unberechtigt Zugriff auf dieses Postfach verschaffen könnte.	n	m	m	n	-
Die Postfach-ID wird bei der Beantragung einer Berechtigung nicht mitsigniert. Der Antrag kann daher für andere Postfächer, die der Antragsteller administrieren darf, missbraucht werden und dadurch Berechtigungen schaffen, die nicht beabsichtigt sind.	n	m	m	n	-

5.7 Anmerkungen zu Betriebs- und Sicherheitskonzepten

Das beA-System ist seinem Wesen nach eine IT-Sicherheitslösung. Für den sicheren Betrieb einer solchen Lösung bedarf es eines verbindlichen Sicherheitsregelwerkes mit mindestens folgenden für die IT-Sicherheit wesentlichen Konzepten:

- Sicherheitskonzept
  - Systemmodellierung
  - Schutzbedarfsanalyse
  - Bedrohungsanalyse
  - Risikoanalyse
  - Beschreibung der Sicherheitsmaßnahmen
  - Vollständigkeitsprüfung und Restrisikoanalyse
- Kryptokonzept
  - Welche Algorithmen und Betriebsmodi werden wo verwendet?
  - Welche Schlüsselparameter werden verwendet?
  - etc.
- Schlüsselmanagementkonzept (ggf. als Bestandteil des Kryptokonzepts)
  - Wie werden Schlüssel erzeugt?
  - Wie werden Schlüssel verwahrt und verwaltet?
  - Wie werden Schlüssel sicher ausgetauscht?
  - Wie werden Schlüssel gelöscht?
  - etc.
- Incident- und Security-Managementkonzept

Für das Gutachten wurden Konzepte seitens des Betreibers bereitgestellt, angepasst bzw. neu erstellt. Dieser Prozess ist jedoch zum Zeitpunkt der Erstellung des vorliegenden Berichts noch nicht abgeschlossen, so dass hier noch Handlungsbedarf besteht. Im Folgenden wird daher der aktuelle Stand dargestellt, so wie er für die konzeptionelle Analyse zur Verfügung stand.

In Bezug auf die notwendigen Bestandteile eines Sicherheitskonzeptes liegt eine nachvollziehbare und vollständige Schutzbedarfsanalyse vor. Grundsätzlich erfolgt der Betrieb des beA in einer ISO-27001-zertifizierten Infrastruktur, so dass grundlegende Elemente des sicheren Betriebs vorhanden sind. Des Weiteren werden in

verschiedenen Dokumenten umfangreiche und für das beA spezifische physikalisch-organisatorische Schutzmaßnahmen beschrieben. Die IT-Komponenten der beA-Umgebungen befinden sich in zwei baulich getrennten Rechenzentren, die unabhängig voneinander betrieben werden. Es sind detaillierte Angaben zur physikalisch-organisatorischen Sicherheit der Rechenzentren beschrieben. Sicherheitsmaßnahmen für Rechenzentren gemäß einer vorgegebenen Policy sind einzuhalten. Der Auftraggeber hat das Recht, nach Anmeldung die Rechenzentren und IT-Komponenten zu prüfen und Auditberichte einzusehen.

Es fehlt allerdings eine dokumentierte Analyse der möglichen Bedrohungen der schutzbedürftigen Assets, eine Risikobewertung sowie eine geschlossene Darstellung der den Risiken entgegenwirkenden Sicherheitsmaßnahmen. Damit liegt noch kein Vollständigkeitsnachweis darüber vor, dass jedem nicht tragbaren Risiko ausreichend mit Sicherheitsmaßnahmen begegnet wird.

Die grundsätzlichen kryptographischen Schritte im Umgang mit Nachrichten konnten anhand der vorgelegten Feinkonzepte und des Kryptokonzeptes nachvollzogen werden. Angaben über die verwendeten Algorithmen und ihre Parametrisierung wurden zum Teil nur summarisch gemacht. Vermisst wurde eine genaue Darstellung der kryptographischen Operationen auf die verschiedenen Datenelemente mit Kryptoschutzbedarf. Daher war es nicht immer möglich, die vom beA ausgeführten kryptographischen Operationen im Detail nachzuvollziehen und sich von der Geschlossenheit und kryptographischen Robustheit des Schutzes der Nachrichten zu überzeugen.

Angaben zum Schlüsselmanagement (Erzeugung, Verwendung, Wechsel, Vernichtung) verteilten sich auf eine Vielzahl von Dokumenten, ohne dabei in der Summe vollständig zu sein.

Zum Incident- und Securitymanagement wurde ein Dokument vorgelegt, das allgemein Verantwortlichkeiten und Rollen, aber keine spezifischen Sicherheitsvorfälle für die beA-Anwendung aufzählt und die Reaktionsweise für das Auftreten festlegt. Es wird der Einsatz eines Tools des Betreibers zur Auswertung von Logmeldungen durch ein Call-Center angeführt, aber nicht beschrieben, um welche Art von Logmeldungen der beA-Anwendung es sich handelt. Damit ist nicht einschätzbar, welche Bedeutung das Tool im Rahmen des Incident-Managements für die beA-Anwendung hat.

Weiterhin wird auf ein Tool zur Untersuchung der IT-Landschaft des beA-Zentralsystems durch externes und internes Scannen auf bekannte Schwachstellen hingewiesen, das sich in der Einführung befindet. Diese Anwendung ist eine zu begrüßende Sicherheitsmaßnahme.

Zwischen dem Auftraggeber und dem Betreiber ist kein spezifisches Information Security Management vereinbart. Augenscheinlich werden Sicherheitsvorfälle im Rahmen eines allgemeinen, dem Auftraggeber und dem Betreiber zugänglichen Ticketsystems bearbeitet, dessen eigentlicher Zweck die Identifizierung und Beseitigung von Betriebsstörungen des beA ist. Sicherheitsvorfälle haben aber einen

anderen Charakter, so dass die Gefahr besteht, dass sie im Rahmen der allgemeinen Incident-Behandlung zu niedrig priorisiert werden.

Es erwies sich als zu schwierig, aus den vorgelegten Dokumenten das Rollenkonzept zu ermitteln, das z.B. sicherstellt, dass an sicherheitskritischen Komponenten nur im 4-Augen-Prinzip gearbeitet werden kann. Im Rahmen der Neuorganisation der Sicherheitsdokumentation mit Erstellung eines bündelnden Sicherheitskonzeptes muss darauf geachtet werden, dass für die in der Schutzbedarfsanalyse identifizierten oder daraus abgeleitet hoch schutzbedürftigen IT-System-Komponenten die angewendeten organisatorisch-physikalischen Sicherheitsmaßnahmen leicht zu finden sind.

Grundsätzlich offenbaren die vorliegenden Dokumente einen geregelten IT-Betrieb, der auch den Aspekt IT-Sicherheit behandelt. Die Dokumentation erlaubt aber keine Prüfung, ob allen nicht tragbaren Risiken auch mit hinreichenden Sicherheitsmaßnahmen begegnet wurde. Es wird empfohlen, ein Sicherheitskonzept nach dem üblichen Muster zu erstellen, das die aufgezählten Elemente und für jedes Sicherheitsrisiko einen klaren Verweis auf beschriebene Sicherheitsmaßnahmen in anderen Dokumenten enthält. In einer dabei zu erstellenden Restrisikoanalyse können sich ggf. Schutzlücken ergeben, die dann zu bewerten und zu schließen wären.

Wichtig erscheint auch, dass auf der Basis einer nachvollziehbaren Sicherheitskonzeption ein unabhängiger Auditor sich regelmäßig vom sicheren Betrieb des beA überzeugt. Dieses Audit kann sich dort, wo anwendbar, auf das regelmäßige ISO-27001-Audit stützen und auch dessen Rhythmus folgen.

Außerdem ist ein nachhaltiger Patchmanagement-Prozess zu betreiben, der verwendete Bibliotheken nach Bekanntwerden von Schwachstellen baldmöglichst aktualisiert.

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen, Deutschland