Die Präsidentenkonferenz beschließt die Wiederinbetriebnahme des beA-Systems in zwei Stufen:

Ab dem 4.7.2018 soll die Client Security zum Download und zur Installation bereitgestellt und die Erstregistrierung am beA ermöglicht werden. Voraussetzung hierfür ist, dass secunet bis dahin die Beseitigung der in ihrem Gutachten vom 18.6.2018 unter Ziffern 3.5.4 und 5.4.1 benannten Schwachstellen bestätigt hat, soweit sie sich auf die Client Security beziehen.

Zum 3.9.2018 soll das beA-System freigeschaltet werden. Voraussetzung hierfür ist, dass secunet bis dahin die Beseitigung der Schwachstellen, die in den Ziffern 3.5.3, 3.6.1, 3.6.2, 3.6.3, 3.6.7, 3.6.9, 3.6.10, 3.6.12, 3.6.13, 4.5.1, 4.5.2, 4.5.3, 5.4.1 (soweit der Nachrichtenversand betroffen ist), 5.4.2 des Gutachtens beschrieben sind, bestätigt hat. Die übrigen Schwachstellen der Kategorie B werden im laufenden Betrieb beseitigt.

Die Präsidentenkonferenz beschließt weiter:
1. Die in dem Gutachten unter den Ziffern 5.5.1 und 5.5.3 beschriebenen Schwachstellen der Kategorie B betreffend die Hardware Security Module werden im laufenden Betrieb, voraussichtlich in den ersten Monaten des Jahres 2019, durch technische Maßnahmen beseitigt.
2. Die von secunet im Kapitel 5.7 des Gutachtens geforderte Optimierung der Betriebs- und Sicherheitskonzepte wird spätestens in den ersten Monaten des Jahres 2019 abgeschlossen und von secunet bestätigt.

Die BRAK wird sich gegenüber dem BMJV und gegenüber den Justizministerien der Länder für die Einführung einer mindestens 4-wöchigen Testphase nach Wiederinbetriebnahme des beA-Systems einsetzen.