DIE ZERTIFIZIERUNGSSTELLE DER BUNDESNOTARKAMMER ALS AKKREDITIERTER ZERTIFIZIERUNGSDIENSTEANBIETER IM PROJEKT BEA

Martin Davies / Cosmina Radu

Senior Consultant, Capgemini Business Technology Public Sector
Potsdamer Platz 5, 10785 Berlin, DE
martin.davies@capgemini.com; https://www.de.capgemini.com/

Consultant, Capgemini Business Technology Public Sector
Potsdamer Platz 5, 10785 Berlin, DE
cosmina.radu@capgemini.com; https://www.de.capgemini.com/

Schlagworte: ***Elektronischer Rechtsverkehr, Bundesnotarkammer, BNotK, Bundesrechtsanwaltskammer, BRAK, Das besondere elektronische Anwaltspostfach, beA***

Abstract: *Die Zertifizierungsstelle der Bundesnotarkammer realisiert als akkreditierter Zertifizierungsdienstanbieter gemäß Signaturgesetz (SigG) die technischen und organisatorischen Voraussetzungen für den Betrieb einer Public Key Infrastructure (PKI). Durch die Bereitstellung und Verwaltung fortgeschrittener und qualifizierter elektronischer Zertifikate unterstützt sie die fortschreitende Entwicklung des Elektronischen Rechtsverkehrs (ERV) in Deutschland, aktuell im Projekt beA der Bundesrechtsanwaltskammer (BRAK).*

1. ERV in Deutschland

Ziel des ERVs ist es, den Beteiligten an gerichtlichen Verfahren die Abgabe verbindlicher Erklärungen in elektronischer Form zu ermöglichen. Im Gegensatz zum web-basierten Elektronischen Rechtsverkehr der österreichischen Justiz ist die Nutzung in Deutschland bisher jedoch nicht verpflichtend vorgeschrieben. Mit dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten wurde in Deutschland 2013 die stufenweise Einführung einer Anwendungspflicht für Rechtsanwälte bis spätestens zum 1. Januar 2022 erlassen.[1] Hierzu bedarf es gesetzlich zulässiger Verfahren, die das bestehende Maß an Integrität und Verbindlichkeit eines handschriftlich unterzeichneten Dokuments auch in seiner digitalen Form sicherstellen und somit ein rechtsverbindliches, elektronisches Handeln ermöglichen. Mit dem SigG und der Signaturverordnung (SigV) hat der deutsche Gesetzgeber hierzu das weltweit anerkannte und genutzte Konzept einer PKI in deutsches Recht umgesetzt.

2. Public Key Infrastructure

Aus technischer Sicht wird die Möglichkeit zur Verschlüsselung und Signatur innerhalb einer PKI durch ein asymmetrisches Kryptosystem realisiert, für das jeder Anwender mit einem Schlüsselpaar ausgestattet wird.[2] Dieses Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel. Während der private

[1] Vgl. Kilian, Matthias/Rimkus, Felix, Der elektronische Rechtsverkehr mit den Gerichten: Besonderes Elektronsiches Anwaltspostfach ante Portas. In: BRAK (Hrsg.), BRAK-Mitteilungen 5/2015, Berlin 2015, S. 217.

[2] Für eine anschauliche Darstellung des verwendeten asymmetrischen Kryptosystems vgl. Goetze, Andreas, Elektronische Signaturen. In: Zertifizierungsstelle der Bundesnotarkammer (Hrsg.), https://zertifizierungsstelle.bnotk.de (aufgerufen am 21. Januar 2016), 2014,

Schlüssel durch den Anwender geheim gehalten werden muss, wird der öffentliche Schlüssel bekanntgegeben. Der Absender nutzt seinen privaten Schlüssel, um Nachrichten zu signieren. Empfänger können die Echtheit der Signatur dann anhand des öffentlichen Schlüssels prüfen. Umgekehrt können Nachrichten an den Empfänger mit dessen öffentlichem Schlüssel verschlüsselt werden, so dass diese nur durch den Empfänger anhand seines privaten Schlüssels entschlüsselt werden können.

In einem symmetrischen Kryptosystem müssten sich Sender und Empfänger erst auf einen gemeinsamen und geheimen Schlüssel einigen und diesen im Geheimen austauschen. Für jede Kommunikationsbeziehung würde zudem ein eigener Schlüssel benötigt. Gerade in einem hochgradig vernetzten System wie dem Internet verfügen asymmetrische Kryptosysteme daher über deutliche Vorteile und haben sich z.B. in Form des Protokolls Transport Layer Security (TLS) für die verschlüsselte Datenübertragung zwischen Servern und Clients und in Form des Standards Secure/Multipurpose Internet Mail Extensions (S/MIME) für die Kommunikation per E-Mail weltweit durchgesetzt.

Aus organisatorischer Sicht setzt ein asymmetrisches Kryptosystem jedoch eine Public Key Infrastructure voraus, da der jeweiligen Anwender anhand eines Zertifikats mit seinem öffentlichen Schlüssel zuverlässig verknüpft werden muss.[3] Im ERV hat sich diese zentrale Lösung mit einer akkreditierten Zertifizierungsstelle vor allem vor dem Hintergrund erhöhter Sicherheitsanforderungen gegenüber einem dezentralen «Web of Trust» durchgesetzt.

3. Public Key Infrastructure im ERV Deutschlands

Aus dem resultierenden hohen Sicherheitsniveau der von einer akkreditierten Zertifizierungsstelle ausgestellten Zertifikate folgte in Deutschland gem. Formanpassungsgesetz (FormAnpG) bereits im Jahr 2001 die Gleichstellung der qualifizierten elektronischen Signatur mit der handschriftlichen Unterschrift im Hinblick auf das gesetzlich erforderliche Schriftformerfordernis.[4]

Im ERV basiert die Kommunikation hierbei im Gegensatz zur gewöhnlichen E-Mail auf dem Protokollstandard Online Services Computer Interface (OSCI), der zwischen Absender und Empfänger einen zusätzlichen neutralen Kommunikationspartner, den «Intermediär», vorsieht.[5] Dieser Intermediär nimmt Nachrichten entgegen und stellt sie dem Empfänger bereit. Er ist somit in der Lage, im Streitfall zuverlässig Auskunft über Datum und Zeitpunkt erfolgter Zustellungen zu geben und ergänzt daher das bestehende System der PKI gerade für den Bereich, in dem Absender und Empfänger das Ob und Wann einer Zustellung in Frage stellen könnten. Durch die Teilung einer Nachricht in Nutzungs- und Inhaltsdaten, kann der Intermediär dabei genau die Informationen einsehen, die er für seine Aufgabe benötigt. Die Inhaltsdaten selbst bleiben zu jedem Zeitpunkt zwischen dem Sender und dem Empfänger Ende-zu-Ende verschlüsselt. Sie können nur durch den Empfänger selbst eingesehen werden.

4. Elektronischen Gerichts- und Verwaltungspostfachs (EGVP)

Die hierauf basierende Anwendung des EGVP wird durch die Teilnehmer des ERV genutzt um mit Gerichten und Behörden rechtssicher zu kommunizieren.[6] So nutzen die deutschen Notarinnen und Notare seit 2007

S. 6 ff.

3 Vgl. Hühnlein, Detlef/Korte, Ulrike, Grundlagen der elektronischen Signatur. Recht Technik Anwendung, Bonn 2006, S .46 ff.

4 Vgl. Bernhardt, Wilfried, Die deutsche Justiz im digitalen Zeitalter. Entwicklung und Entwicklungsperspektiven von E-Justice. In: Ewer,Wolfgang et al. (Hrsg.), Neue Juristische Wochenschrift 38/2015, Berlin 2015, S. 2775 f.

5 Vgl. OSCI Leitstelle, OSCI-Transport 1.2, Bremen 2002, S. 8.

6 Vgl. Bacher, Klaus, Der elektronische Rechtsverkehr im Zivilprozess. In: Ewer,Wolfgang et al. (Hrsg.), Neue Juristische Wochenschrift 38/2015, Berlin 2015, S. 2754.

die Möglichkeiten des elektronischen Grundbuchs sowie des elektronischen Handelsregisters. Rechtsanwältinnen und Rechtsanwälte können bereits heute die Antragstellung im elektronischen Mahnverfahren anhand qualifizierter elektronischer Signaturen digital vornehmen.

Der hierfür notwendige EGVP Client wurde bisher durch die Justiz bereitgestellt und gepflegt. Zum 1. Januar 2016 wurde der bisherige EGVP-Client abgekündigt und zum 1. Oktober 2016 abgeschaltet, denn künftig soll die elektronische Kommunikation der Rechtsanwälte und Notare mit der Justiz über das beA bzw. das besondere Notarpostfach (beN) erfolgen.

5. Das besondere elektronische Anwaltspostfach

Für die Umsetzung der neuen technischen und organisatorischen Anforderungen sieht das Gesetz zur Förderung des ERVs im Bereich der Rechtsanwälte und Rechtsanwältinnen die BRAK vor. Im Rahmen des Projektes beA baut die BRAK Insbesondere einen eigenen Intermediär auf und betreibt diesen, richtet für jeden zugelassenen Rechtsanwalt ein beA ein und stellt die Mittel für die Authentisierung gegenüber dem beA bereit.

Um dem hohen Schutzbedarf des beA angemessen zu entsprechen, wurde der Zugang zum besonderen elektronischen Anwaltspostfachs gemäß §31a der Bundesrechtsanwaltsordnung (BRAO) anhand einer Zwei-Faktor-Authentifizierung abgesichert, also dem Identitätsnachweis mittels der Kombination zweier verschiedener und insbesondere unabhängiger Faktoren.[7] Neben der Kenntnis einer persönlichen Identifizierungsnummer (PIN) als erstem Sicherheitsfaktor, ist der Besitz einer beA-Karte und des hierauf enthaltenen Zertifikates als zweiter Sicherheitsfaktor notwendig, um lesenden Zugriff auf das Postfach zu erhalten. Die BRAK setzt daher voraus, dass alle gegenwärtigen und zukünftigen Anwender mindestens ein fortgeschrittenes elektronisches Zertifikat für den Zugriff auf das Postfach verwenden.

Rechtsanwältinnen und Rechtsanwälte können auf Wunsch zusätzlich ein qualifiziertes elektronisches Zertifikat nach erfolgter Auslieferung der beA-Karte Basis anhand einer Nachladefunktion auf die Karte laden, die dann als beA-Karte Signatur bezeichnet wird. Voraussetzung für die Ausstattung mit einem qualifizierten Zertifikat ist jedoch stets eine eindeutige Identifizierung des Signaturschlüsselinhabers im Rahmen eines Identifizierungsverfahrens gemäß §5 SigG.

6. Die Zertifizierungsstelle der Bundesnotarkammer[8]

Die BNotK verfügte mit der Zertifizierungsstelle der Bundesnotarkammer bereits seit 2001 über die erforderliche und durch TÜVIT geprüfte, hochsichere Infrastruktur. Die Zertifizierungsstelle ist als zertifizierter Dienstanbieter gemäß §15 SigG akkreditiert und gibt als solche bereits fortgeschrittene und qualifizierte elektronische Zertifikate sowie qualifizierte Zeitstempel an Notare, Rechtsanwälte und weitere Antragssteller aus. Die Zertifizierungsstelle übernimmt hierbei eine Vielzahl von Aufgaben. Eingehende Zertifikatsanträge prüft und bewilligt sie, zudem erstellt sie die Zertifikate und beauskunftet bzw. sperrt diese.

Für den sicheren Betrieb der Zertifizierungsstelle sind hierbei – neben baulichen Maßnahmen wie dem Abstrahlschutz und den Zugangsbeschränkungen – auch erhebliche organisatorische und technische Maßnahmen notwendig. Die Umsetzung dieser Maßnahmen wird regelmäßig anhand interner und externer Überprüfungen nachgewiesen. Diesem erhöhten Aufwand steht jedoch ein eindeutiger Nutzen gegenüber, der für die BNotK zu der Entscheidung für den Aufbau einer eigenen Zertifizierungsstelle führte. So stehen für die Kammer

[7] Vgl. Brosch, Christopher/Fiebig, Peggy, beA-sicher Die Sicherheitsarchitektur des beA. In: BRAK (Hrsg.), BRAK Magazin 4/2015, Berlin 2015, S. 11–12.

[8] Vgl. Goetze, Andreas, Elektronische Signaturen. In: Zertifizierungsstelle der Bundesnotarkammer (Hrsg.), https://zertifizierungsstelle.bnotk.de (aufgerufen am 21. Januar 2016), 2014, S. 6 ff.

als berufsständische Vertretung keine kurzfristigen finanziellen Gewinne, sondern die Erreichung langfristiger strategischer Ziele des Berufsstandes im Vordergrund. Gerade im Falle der Notare ist dies ein maximales Sicherheits- und Vertrauensniveau im ERV verbunden mit einem zuverlässigen und dauerhaft verfügbaren Dienst.

7. Zusammenarbeit im Projekt beA

Im Rahmen des Projektes beA verzichtete die BRAK aus Gründen der Zeit- und Kosteneffizienz auf den Aufbau und den Betrieb einer eigenen Zertifizierungsstelle. Stattdessen verständigten sich BRAK und BNotK auf eine verwaltungskörperschaftliche Kooperation und die Nutzung der damit verbundenen Synergieeffekte. Die BNotK unterstützt die BRAK aktuell, indem sie die Bestellungen der Zertifikate für die rund 165.000 Rechtsanwälte und deren Mitarbeiter sowie die der Chipkartenleser über ein eigens entwickeltes Bestellsystem im Internet entgegennimmt und beA-Karten, beA-Signaturkarten, Mitarbeiterkarten und Softwarezertifikate durch ihre Zertifizierungsstelle ausstellt und über den gesamten Lebenszyklus verwaltet.[9]

8. Fazit

Die bewährten technischen und organisatorischen Lösungen der Zertifizierungsstelle werden durch die enge Kooperation der BRAK mit der BNotK genutzt um die gemeinsamen langfristigen Ziele im ERV zeit- und kosteneffizient zu erreichen. Auch wenn diese Aufgabe alle Beteiligten gleichermaßen fordert, scheint diese Mühe mehr als gerechtfertigt, wenn das Ziel erreicht wird, dass 165.000 Rechtsanwälte zukünftig rechtssicher und verbindlich Verfahrenserklärungen gegenüber Gerichten per Mausklick abgeben können.

9. Literatur

Bacher, Klaus, Der elektronische Rechtsverkehr im Zivilprozess. In: Ewer,Wolfgang et al. (Hrsg.), Neue Juristische Wochenschrift 38/2015, Berlin 2015, S. 2753–2759.

Bernhardt, Wilfried, Die deutsche Justiz im digitalen Zeitalter. Entwicklung und Entwicklungsperspektiven von E-Justice. In: Ewer,Wolfgang et al. (Hrsg.), Neue Juristische Wochenschrift 38/2015, Berlin 2015, S. 2775–2779.

Brosch, Christopher/Fiebig, Peggy, beA-sicher Die Sicherheitsarchitektur des beA. In: BRAK (Hrsg.), BRAK Magazin 4/2015, Berlin 2015, S. 10–12.

Fiebig, Peggy, Wie bekomme ich mein beA? In: BRAK (Hrsg.), BRAK Magazin 4/2015, Berlin 2015, S. 13.

Goetze, Andreas, Elektronische Signaturen. In: Zertifizierungsstelle der Bundesnotarkammer (Hrsg.), https://zertifizierungsstelle.bnotk.de (aufgerufen am 21. Januar 2016), 2014.

Hühnlein, Detlef/Korte, Ulrike, Grundlagen der elektronischen Signatur. Recht Technik Anwendung, Bonn 2006, S. 46–62.

Kilian, Matthias/Rimkus, Felix, Der elektronische Rechtsverkehr mit den Gerichten: Besonderes Elektronisches Anwaltspostfach ante Portas. In: BRAK (Hrsg.), BRAK-Mitteilungen 5/2015, Berlin 2015, S. 216–221.

OSCI Leitstelle, OSCI-Transport 1.2, Bremen 2002.

[9] Vgl. Fiebig, Peggy, Wie bekomme ich mein beA? In: BRAK (Hrsg.), BRAK Magazin 4/2015, Berlin 2015, S. 13.