Verband der Beschäftigten des Gewerblichen Rechtsschutzes

Die Kompetenzgewerkschaft im Deutschen Patent- und Markenamt

dbb beamtenbund und tarifunion

Warum eine Signaturkarte mit qualifizierter Signatur inklusive privater Haftungs- und Datenschutzrisiken und keine Karte mit fortgeschrittener Signatur ohne Risiken für den Einzelnen???

Diese Frage stellt sich nachdem die Amtsleitung alle Kolleginnen und Kollegen mit dem ElSA Newsletter 7 aufgefordert hat, eine Signaturkarte mit qualifizierter Signatur zu beantragen.

Jeder Mitarbeiter, der eine Signaturkarte mit einer qualifizierten Signatur verwenden soll, muss einen Vertrag als Privatperson mit der Deutschen Sparkassen Verlag GmbH (S-Trust) abzuschließen. Die qualifizierte Signatur ersetzt dann die eigene Unterschrift (siehe §126a BGB). Neben datenschutzrechtlichen Bedenken sind es vor allem die persönlichen Haftungsrisiken, warum die Einführung und den Gebrauch der qualifizierten Signatur von Beschäftigten im DPMA nicht sinnvoll ist:

- Was passiert bei Verlust und anschließendem Missbrauch der Karte? Hafte ich, wenn das Trustcenter nicht sicher ist, zum Beispiel weil Dritte an die Daten des Trustcenters gekommen sind? Nach den Geschäftsbedingungen haftet das Trustcenter nur begrenzt.
- Bis zu welcher Grenze haftet der Einzelne PERSÖNLICH, insbesondere wenn mit einer verlorenen oder gestohlenen Karte private Verträge wie Kreditverträge, Mietverträge oder Kaufverträge (Autokauf) abgeschlossen werden? Muss der oder die Beschäftigte bei Missbrauch mit eigenem Vermögen einstehen oder muss sie oder er sich für die Begleichung der Geschäfte sogar hoch verschulden?
- Wie kann der Einzelne sicherstellen, dass sämtliche Vertragsbedingungen, die an den Eigentümer der Karte gestellt werden eingehalten werden. Oft kann dies der oder die Beschäftigte nicht sicherstellen (z. B. Sicherheit der Computeranlage oder mangelhafte Aufbewahrungsmöglichkeiten im Büro)?
- Kann ich bei einer Änderung der Vertragsbedingungen den Kartenvertrag kündigen, ohne dass dies Auswirkungen auf meinen Arbeitsplatz hat?

Der VBGR ist nach vorläufiger Klärung des Sachverhaltes der Überzeugung, dass die Verwendung einer Signaturkarte mit qualifizierter Signatur wegen der möglichen negativen Folgen auf die Beschäftigten der Fürsorgepflicht des Dienstherrn nicht gerecht wird, risikobehaftet und unnötig ist.

Alternativ und von der Verordnung vorgeschrieben ist nämlich lediglich die Verwendung einer Karte mit fortgeschrittener Signatur. Der VBGR fordert daher die Amtsleitung auf, den eingeschlagenen Weg zu verlassen und auf die Verwendung einer Signaturkarte mit qualifizierter Signatur zu verzichten. Wir weisen darauf hin, dass laut Bundestagsdrucksache 14/4662 (Seite 19 zu §2 Nummer 6) Zertifikate auch auf juristische Personen ausgestellt werden können.

Geschäftsstelle München

Morassistraße 2
D-80469 München
Telefon 089.2157-8433
Telefax 089.2157-8433
post@vbgr.dbb.de
www.vbgr.dbb.de

Verantwortlich

Franz Gotsis
Telefon 089/2195-4077
Bernd Kessler
Telefon 089/2195-4428
Dr. Volker Jörgens
Telefon 089/2195-2712

München, 12.04.2011

05/11

VBGR aktuell

Informationsdienst des VBGR

Die Position des VBGR zur Einführung der qualifizierten Signaturen für einen großen Teil der Mitarbeiter im DPMA

Die Amtsleitung hat im ELSA Newsletter Nummer 7/2011 angekündigt, dass alle Mitarbeiter, die bisher Dokumente zu unterschreiben hatten, diese Unterschrift in Zukunft als qualifizierte Signatur nach dem Signaturgesetz (SigG) zu leisten haben. Dieses Gesetz sieht vor, dass eine qualifizierte Signatur so realisiert werden muss, dass die Person, die das Dokument signiert, eindeutig identifizierbar sein muss und diese über ein Zertifikat eines Zertifizierungsdiensteanbieters (Trustcenter) überprüfbar sein muss. Hierin liegt der Unterschied zur fortgeschrittenen Signatur (siehe §2 SigG und §5 EAPatV). Die **qualifizierte Signatur** ist nach §126a BGB ein Ersatz der handschriftlichen Unterschrift für jedes Rechtsgeschäft, ob im Internet, gegenüber Behörden oder Banken, etwa zur Beantragung eines Kredits. Diese weit reichenden Einsatzmöglichkeiten sind aber für die elektronische Aktenführung im Rahmen von ELSA nicht nötig und setzen die Mitarbeiter des DPMA erheblichen finanziellen Risiken aus. Sie müssen einen Vertrag als Privatperson mit einer Firma schließen, um ihre dienstlichen Aufgaben weiter erfüllen zu können und setzen damit sich und ihren Familienangehörigen Haftungsrisiken aus, die der einzelne Mitarbeiter weder überblicken noch begrenzen kann. Da aufgrund des §8 SigG Nummer 1, die rückwirkende Sperrung eines Zertifikats nicht möglich ist (auch nicht bei Missbrauch), muss jeder Inhaber einer Signaturkarte bei längerer Abwesenheit (etwa aufgrund einer Urlaubsreise) sicherstellen, dass seine Signaturkarte so sicher verwahrt ist, dass ein Missbrauch ausgeschlossen werden kann. Falls der Computer an dem die Signaturkarte eingesetzt wird, von einem fremden Administrator oder Einbrecher (Hacker) verfälscht wurde und die Sicherheit nicht mehr gegeben ist, so dass die signierten Dokumente für den Benutzer unsichtbar geändert werden können, ist das damit ausgelöste Rechtsgeschäft trotzdem grundsätzlich gültig. Der oder die Karteninhaber/in kann, falls der Urheber des Missbrauchs festgestellt werden kann (was im Regelfall nicht möglich ist), den Schaden nachträglich gegen diesen geltend machen. Hinzu kommt, dass der Benutzer der Karte nicht unmittelbar, wie bei einer Bankkarte durch den Blick in einen schriftlichen oder elektronischen Kontoauszug feststellen kann, dass ein Missbrauch stattgefunden hat. Besonders kritisch ist in diesem Zusammenhang der §19 SigG: Dort ist in Absatz 4 festgelegt, dass die zuständige Behörde (Bundesnetzagentur), qualifizierte Zertifikate sperren kann, wenn die Befürchtung besteht, dass „qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung qualifizierter elektronischer Signaturen oder eine unbemerkte Verfälschung damit signierter Daten zulassen". Der nächste Absatz (5) führt aus, dass die vor der Sperrung ausgestellten qualifizierten Zertifikate und damit die geschlossenen Verträge trotzdem gültig bleiben.

Die von der Amtsleitung zitierte Verordnung über die elektronische Aktenführung bei dem Patentamt, dem Patentgericht und dem Bundesgerichtshof (EAPatV) legt aus gutem Grund in §5 die **fortgeschrittene Signatur** als Herkunftsnachweis für Schriftstücke der Behörden fest. Die qualifizierte Signatur ist für die Verwendung durch Privatpersonen im elektronischen Verkehr mit Ämtern und Firmen vorgesehen, nicht jedoch für den elektronischen Versand durch eine Behörde. Der Unterschied ist, dass Einzelpersonen bei einem Einkauf im Internet oder bei der Beantragung von öffentlichen Leistungen nur mit ihrer Privatadresse über ihren Eintrag bei der Meldebehörde identifizierbar sind, während Behörden aufgrund von Gesetzen oder sonstigen Rechtsvorschriften eindeutig identifiziert werden können. Im Falle von Behörden ist für den Empfänger nicht in erster Linie entscheidend, welcher Mitarbeiter der Behörde das Dokument ausgestellt hat, sondern dass die Behörde an sich der Urheber des Dokuments ist und erst in zweiter Linie der Beschäftigte. Der Grund ist, dass falls eine Bürgerin oder ein Bürger gegen die Bescheide oder Beschlüsse einer Behörde vorgehen will, die Behörde rechtlich belangen muss, nicht aber den Mitarbeiter persönlich.

Forderung des VBGR: Aus der Gesetzesbegründung zum §2 des Signaturgesetz (Bundestagsdrucksache 14/4662) ist auf Seite 19 zum Punkt 6 erläutert, dass Zertifikate (im Gegensatz zu qualifizierten Zertifikaten) auch auf juristische Personen ausgestellt werden können. In Anlehnung daran ist die Unterzeichnung aller Schriftstücke der Behörde DPMA mit einer fortgeschrittenen Signatur auf der Basis eines Zertifikats, das auf die Behörde DPMA ausgestellt ist, ein für das DPMA sinnvolles Verfahren, das damit auch den Vorgaben des §5 EAPatV genügt. Die bereits beschafften Geräte und Signaturkarten könnten weiterverwendet werden und die Zuordnung einer bestimmten Signatur zu einer Person könnte das DPMA intern sicherstellen, auch ohne dass die Beschäftigten Verträge als Privatperson mit einem Zertifizierungsanbieter (Trustcenter) abschließen müssen. Ein derartiges Vorgehen würde die Interessen der Anmelder berücksichtigen, die einen Echtheitsnachweis der erhaltenen Schriftstücke ermöglicht und es würde den Mitarbeitern nicht abverlangen, private Verträge mit Firmen einzugehen und erhebliche Haftungsrisiken in Kauf zu nehmen. Derartige Schriftstücke könnten im Text nach wie vor den Urheber der Dokumente enthalten oder auch fortgeschrittene Signaturen einzelner Mitarbeiter, so dass der Anmelder aus dem Text nach wie vor und zu dem rechtssicher auf den Urheber schließen kann.