

Open Innovation gibt es nicht umsonst

Hochschulpatente und offene Innovationsstrukturen von Unternehmen

VON

DR. REGINA KRATT

IM AUFTRAG DES TECHNOLOGIE-LIZENZ-BÜRO (TLB) DER BADEN-WÜRTTEMBERGISCHEN HOCHSCHULEN GMBH

Universitäten sind für Unternehmen interessante Partner, wenn es um die Nutzung externer Ideen für die eigenen Innovationsprozesse geht. Die Technologie-Lizenz-Büro (TLB) GmbH Karlsruhe managt den Transfer zwischen Wissenschaft und Wirtschaft und wahrt dabei mit geeigneten Vergütungsmodellen die Interessen von Universität und Erfinder. Hierfür bilden Schutzrechte die Basis - auch bei Softwareerfindungen.

Patente als sichere Basis für Geschäftsbeziehungen

Open Innovation bedeutet freier Austausch von Informationen über die Grenzen von Disziplinen, Unternehmen, Instituten und Ländern hinweg mit dem Ziel, gänzlich neue Ideen beziehungsweise Anwendungen zu finden, Neuentwicklungen zu beschleunigen und diese langfristig auf Erfolg auszurichten. Wichtiger Partner ist für Unternehmen, neben Kunden, Zulieferern, Wettbewerbern, mit steigender Tendenz auch die Wissenscommunity, zu denen insbesondere Universitäten oder im IT-Bereich "Open-Source-Gruppen" gehören.

Als Patent- und Verwertungsagentur der baden-württembergischen Universitäten und Hochschulen unterstützt TLB die Universitäten und Hochschulen darin, erfolgrei-

che Partner für technologieorientierte Unternehmen zu sein. Alle Erfindungen, die in das TLB-Portfolio aufgenommen werden, sind auch als Patent angemeldet, denn nur schutzrechtlich abgesicherte Erfindungen sind für Unternehmen wirtschaftlich interessant. Klassischerweise stecken Unternehmen ihre Marktposition gegenüber Wettbewerbern bereits frühzeitig mit Patenten ab und sichern auf diese Weise nachhaltig das Know-how des Unternehmens.

In offenen Innovationsstrukturen schaffen Patente für alle Transferbeteiligten eine klare Verhandlungsbasis und sichern darüber die erforderlichen Investitionen der Nutzer. Sie bedeuten Alleinstellungsmerkmale für Erfinder bzw. Hochschulen sowie Unternehmen und eröffnen dadurch wirksame Lizenzierungsmöglichkeiten.

So wird Wissen wieder zu Geld.

Spezialthema Software:

Eine Extremform von Open Innovation ist Open-Source-Software, deren Quelltext öffentlich zugänglich ist und von Nutzern in "Communities" im Internet konzipiert wird. Tatsächlich ist Open-Source-Software in den meisten Fällen wirklich kostenlos, im erweiterten Verständnis ist das jedoch nicht so (im Sinne von: "free speech, not free beer" - "freie Meinungsäußerung, nicht Freibier"). Derzeit begleitet TLB Ausgründungen, die zwar im Wesentlichen auf Open Source-Lizenzen basieren, dabei aber selbstverständlich ein auf wirtschaftlichen Gewinn ausgerichtetes Geschäftsmodell haben. Auch Kombinationen von Open-Source-Software und Softwarepatenten sind denkbar.

Entgegen vieler Meinungen aus Foren und Zeitungen erteilt das Europäische Patentamt sehr wohl Patente für sogenannte "computerimplementierte Erfindungen", d.h. für solche Erfindungen, die mithilfe eines Computers praktisch umgesetzt werden. Voraussetzung ist jedoch, dass die betreffenden Erfindungen einen technischen Charakter aufweisen. Der Patentschutz erstreckt sich anders als der Urheberrechtsschutz nicht nur auf die konkrete Gestalt (wie den Source Code), sondern ebenfalls auf die zugrunde liegenden erfinderischen Ideen und deren Umsetzung. Daher ist Patentschutz eine sehr effiziente und wirksame Art, Erfindungen auch im Bereich der computerimplementierten Erfindungen abzusichern. Insofern ist es auch nicht verwunderlich, dass die Zahl der Patentanmeldungen im Bereich "Datenverarbeitung" (nach der Internationalen Patentklassifikation die IPC-Klasse G06) im Vergleich zu den europäischen Anmeldezahlen insgesamt überproportional ansteigt. Auch TLB meldete in den letzten Jahren verstärkt

“TLB patentiert und verwertet auch computerimplementierte Erfindungen”

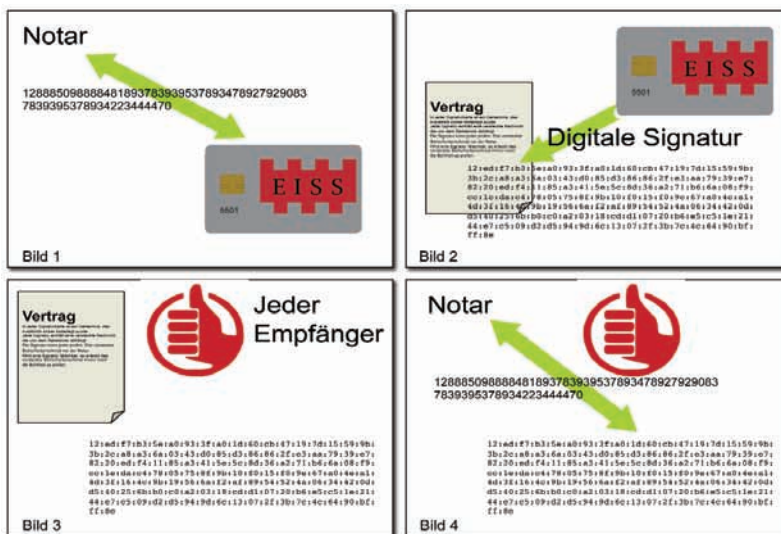
computerimplementierte Erfindungen zum Patent an.

Versteckte Sicherheit in Digitalen Signaturen

Wer Kaufverträge, Banktransaktionen und Rechnungen über das Internet abwickeln will, muss die zugehörigen elektronischen Dokumente auch sicher signieren können. Die Sicherheit, die heutige Systeme gegen Hackerangriffe bieten, kann in ein paar Jahren aufgrund von höherer Rechnerkapazität, zum Beispiel auch durch das Thema Cloud-Computing, längst überholt sein. Am Europäischen Institut für Systemsicherheit (EISS) des KIT wurde unter der Leitung von Prof. Dr. Jörn Müller-Quade ein Verfahren entwickelt, das die Sicherheit digitaler Sig-

KIT entwickelte Verfahren erstmals eine vereinfachte und effiziente Möglichkeit eine Signatur zu überprüfen. Der große Vorteil besteht darin, dass - im Unterschied zu Fail-Stop Signaturen - das neue System für die weit verbreiteten Signaturverfahren einsetzbar ist, wie beispielsweise für das von der Bundesnetzagentur zugelassene RSA-Verfahren. Kern der Erfindung ist ein zweiter beim Notar hinterlegter Schlüssel, der clever und unsichtbar in jede Signatur mit einfließt.

Durch die Unterschriftenfunktion von Signaturkarten kann ein elektronisches Dokument signiert und die Identität der Person, die das Dokument versandt hat, nachgewie-



▲ Neues Verfahren bei Signaturkarten

naturen auf lange Sicht gewährleistet.

Mit einer digitalen Signatur wird zu einer beliebigen Nachricht ein "Zahlenschlüssel" berechnet, mit dem die Urheberschaft des Senders vom Empfänger geprüft werden kann. Anders als bei den derzeit verwendeten Verfahren ist es wünschenswert, dass eine digitale Signatur über ein zusätzliches Sicherheitsmerkmal verfügt, damit die Signatur, sobald ihre Sicherheit in Frage gestellt wird, als gültig identifizierbar sein bzw. als Fälschung erkannt werden können.

Bei den bisher in der Forschung vorgeschlagenen sogenannten Fail-Stop Signaturen wird für ein solches Nachweisverfahren eine spezielle Art von Signaturen verwendet, die für eine breite Anwendung zu aufwendig ist. Hingegen ermöglicht das am

sen werden. Bei dem neuen Verfahren ist in jeder Signaturkarte neben dem zum Signieren notwendigen Geheimnis ein zweites Geheimnis enthalten, das zusätzlich bei einer sicheren Instanz, etwa einem Notar, hinterlegt ist (Bild 1). Beim Erzeugen der digitalen Signatur, zum Beispiel für einen Vertrag, wird dieser zweite Schlüssel in der Unterschrift versteckt (Bild 2). Der Clou des Verfahrens liegt darin, dass die Funktionsweise der digitalen Signatur dadurch nicht beeinträchtigt wird und die Identität der Signatur sich nach wie vor von jedem Empfänger mit dem öffentlichen Schlüssel prüfen lässt (Bild 3). Kommen Zweifel an der Echtheit der Signatur auf, kann ein Notar die Echtheit die Signatur über den zweiten Schlüssel prüfen (Bild 4). ■