

## Projektgruppe: „Digitale Signaturen auf dem Prüfstein der Wissenschaften“

von Christian J. Langenbach, Europäische Akademie Bad Neuenahr-Ahrweiler GmbH

### 1 Einführung

Es ist nicht ungewöhnlich, dass eine technische Entwicklung wie die digitale Signatur auf rechtliche, ökonomische, soziale und kulturelle Hindernisse stoßen. Denn diese technische Entwicklung bringt bei genauer Analyse eine Reihe von Fragen mit sich, beispielsweise: Was sollten digitale Signaturen kosten? Könnte aus dem Übergang von der eigenhändigen Unterschrift zur digitalen Signatur ein Bruch der Rechtskultur folgen? Wie könnte die kryptographische Sicherheit verbessert werden? Wie könnte Vertrauen in digitale Signaturen vermittelt werden? Wie ist mit den Schwierigkeiten bei der Langzeitverfügbarkeit elektronischer gespeicherter Daten umzugehen – jenseits der 30 Jahre des Signaturgesetzes? Könnten digitale Signaturen als technologisches Instrument zur Erweiterung Europas angesehen werden, und welche Folgen würde dies erzeugen?

Diese – und andere – Fragestellungen werden gegenwärtig in dem interdisziplinären, europäischen Projekt *„Digitale Signaturen. Kulturelle Beherrschbarkeit und moralische Verantwortbarkeit“* der Europäischen Akademie bearbeitet. Dies liegt nahe, weil nur interdisziplinäre Sichtweisen geeignet sind, die neue Basistechnologie der digitalen Signatur in ihren kulturell und sozial erkennbaren Konsequenzen umfassend ins Visier zu bekommen. Dabei geht es über fachwissenschaftliches Verfügungswissen hinaus um Orientierungswissen für den Umgang mit den gefundenen Ergebnissen, um so einen Dialog mit Wirtschaft, Kultur, Politik und Gesellschaft unter europäischer Perspektive anzuregen.

### 2 Projekthintergrund

Die bereits heute erkennbaren, aber noch in spezifischer dynamischer Entwicklung befindlichen Trends und Ausprägungen der IT-

Produkte produzieren ihre eigene Verletzlichkeit und Verwundbarkeit – die systeminhärente „Achillesferse“ – gleich mit. Dass dieses sich abzeichnende Real-Szenario unsicherer IT-Produkte in der sich entfaltenden Informationsgesellschaft nicht aus der Luft gegriffen ist, dafür stehen etwa der fehlende Schutz digitalisierten geistigen Eigentums, die neuen Formen der elektronischen Wirtschaftsspionage oder die noch fehlende Rechtsverbindlichkeit des elektronischen Handels.

Letztgenanntes – auch bekannt als E-Commerce – ist ein Schlagwort, das im Zusammenhang mit dem Internet immer häufiger genannt wird. Eines der entscheidenden Merkmale des E-Commerce ist die Nutzung des dezentralen und „unsicheren“ Internets. Dies ist sicherlich mit ein Grund, warum sich die Nutzer beim „online-shoppen“ noch recht verhalten zeigen. Die diversen Anbieter suchen die Schuld zum einen beim Gesetzgeber, doch der hat mit dem Informations- und Kommunikationsdienstegesetz (IUKDG) die rechtliche Grundlage bereits geschaffen. Zum anderen seien die Nutzer viel zu sicherheitsbewusst und hätten unbegründet Vertrauensdefizite. Doch der Nutzer, und das belegen Zahlen, hat ein Interesse daran, ohne Abstriche an dem E-Commerce teilzuhaben. Und hier sollen vor allem die digitalen Signaturverfahren als treibende Kraft wirken, die vielfältigen Angebote des elektronischen Geschäftsverkehrs, auch in Hinblick auf einen gemeinsamen europäischen Binnenmarkt, für die Anwender zu erschließen.

#### 2.1 Digitale Signaturen

Von der technischen Seite her betrachtet stellt eine digitale Signatur eine Art Siegel dar, welches die digitalen Daten signiert, ähnlich der eigenhändigen Unterschrift unter einen Vertrag. Es beruht im Kern auf mathematischen Verfahren, die mit Hilfe kryptographischer Methoden zur Erzeugung einer digitalen Signatur führen. Die Art der Kommunikationsbeziehungen benötigen die Papierform nicht mehr und die Schrift mit den Varianten Handschrift, Maschinenschrift und Druckschrift verliert in dem Prozess des Wandels der Gesellschaftsform an Bedeutung. Die digitale Signatur soll Authentizität und Integrität des digital signierten Dokuments gewährleisten.

Digitale Signaturen können vielfältig angewendet werden, so etwa

- für die elektronische Steuererklärung;
- für die Rezeptausstellung;
- für Homebanking;
- zwischen Ärzten/Kliniken/Apotheken;
- für Electronic Commerce;
- für den Dokumentenaustausch Bürger/Behörden und Behörden/Behörden;
- zwischen Geschäftspartnern (z.B. bei Verträgen);
- bei der Erstellung elektronischer Ausweise.

## 2.2 *Conclusio: Aspekte der digitalen Signatur*

Vom technischen und gesetzgeberischen Ansatz her ist es durchaus möglich, mit der digitalen Signatur eine bessere Verbindlichkeit im E-Commerce zu erreichen. Darauf aufbauend wird gegenwärtig in verschiedenen Einsatzbereichen von digitalen Signaturen der technisch-organisatorische Aufbau von Trust-Centern, beispielhaft TeleSec und D-Trust, vorangetrieben, so etwa in einigen Kommunen (Media-Kom) und in der Bundesverwaltung (SPHINX). Aber vertrauenswürdige elektronische Kommunikation in globalen Zusammenhängen, und das ist längst nicht mehr neu, entsteht nicht allein durch das Funktionieren der Technik, nicht allein aus dem Recht – also quasi automatisch –, sondern muss als gesellschaftlicher Lernprozess vermittelbar gemacht werden.

Das Projekt der Europäischen Akademie hat sich zum Ziel gesetzt, einige der bis dahin (noch) nicht gestellten oder (noch) nicht beantworteten Fragen in das Zentrum der Überlegungen zu rücken. Angesichts des fundamentalen (kulturellen) „Bruches“ beim Übergang von der eigenhändigen Unterschrift zur digitalen Signatur und der Komplexität der damit verbundenen (technisch-organisatorisch-rechtlichen) Strukturen und Mensch-Technik-Interaktionen müssen Fragen wie Antworten nicht nur in verschiedenen disziplinären „Zugängen“ und „Blickwinkeln“ zur Thematik:

- kulturell-moralische Dimensionen,
- sozial-psychologische Dimension,
- sicherungszwangsgesellschaft,

- rechtliche Dimension,
- technische Dimension,
- ökonomische Dimension,
- gesamteuropäische Dimension

gefunden werden, sondern darüber hinaus auch in einem disziplinübergreifenden Dialog. Wo bei sich angesichts der Globalität eine allein „deutschlandzentrierte“ Sicht verbot und ein „Blick über die Grenzen“ angezeigt war.

## 3 **Projektfortschritt**

Dem Wissenschaftlichen Beirat der Europäischen Akademie wurde im März 1999 ein erstes Projektkonzept vorgelegt. Als Resultat der Begutachtung wurde die Europäische Akademie aufgefordert, das Projekt weiter zu konkretisieren und die vorgesehenen Mitglieder anzusprechen und für das Projekt zu gewinnen. Im September 1999 wertete der Wissenschaftliche Beirat das vorgelegte Arbeitsprogramm der Projektgruppe positiv: „Es handle sich dabei um ein Projekt, das in ausgezeichneter Weise dem wissenschaftlichen Selbstverständnis der Europäischen Akademie entspreche. Das Thema ist sowohl wissenschaftlich hochinteressant als auch gesellschaftlich und politisch aktuell. Die vorgeschlagene interdisziplinäre Vorgehensweise lässt wichtige neue Akzente erwarten.“

Die Berufung der neuen europäisch besetzten Projektgruppe für ein Jahr (Laufzeit Herbst 1999 - Herbst 2000) durch die Europäische Akademie erfolgte mit der konstituierenden Sitzung am 16./17. September 1999. Die Projektgruppe hat in den ersten beiden Sitzungen das Arbeitsgebiet thematisch stärker strukturiert und erste Saattexte zur kulturellen Beherrschbarkeit, zur rechtlichen und technischen Dimension sowie zur Geschichte der Signatur diskutiert. Daneben wurden die Planungen für das Kick-Off-Meeting der Gruppe abgeschlossen. Der interdisziplinäre Diskurs zu den Fragen der „Kulturellen Beherrschbarkeit und moralischen Verantwortbarkeit digitaler Signaturen“ fand am 02./03. Dezember 1999 in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Boppard statt. Neben den Projektgruppenmitgliedern stellten weitere Fachleute die Problembereiche der Digitalen Signaturen mit Vorträgen dar.

Die Vorträge und die Arbeitsgruppen des Kick-Off-Meetings verfolgten an den beiden Tagen etwa 80 Teilnehmer.

Mittlerweile sind die Arbeiten an den Saattexten soweit fortgeschritten, dass ein erster noch grober Entwurf des Memorandums in der Gruppe diskutiert und bearbeitet wird. Der weiterentwickelte Entwurf ist der Ausgangspunkt für Beratungen mit einem ausgewählten Expertengremium. Mitte Juli 2000 werden auf einem von der Projektgruppe organisierten Workshop eine vorerst noch größere Anzahl von Empfehlungen beurteilt. Durch diese vorgutachterliche Beurteilung können Impulse einer breiteren Fachöffentlichkeit in die laufenden Arbeiten Eingang finden.

#### 4 Projekterwartungen

Die Herausbildung und Entwicklung vertrauenswürdiger elektronischer Kommunikation bedarf des interdisziplinären Prozesses. Technik allein stellt kein Vertrauen her, und Recht allein bietet keinen realen Schutz für eine vertrauenswürdige elektronische Kommunikation. Deshalb bedarf die Weiterentwicklung des Vertrauens in eine neuartige Sicherheitsinfrastruktur eines gesellschaftlichen Lernprozesses. Die Forschungsergebnisse der interdisziplinären Projektgruppe der Europäischen Akademie zur kulturellen Beherrschbarkeit und moralischen Verantwortbarkeit digitaler Signaturen sollen die perspektivische Beurteilung der Möglichkeitsräume, in denen sich vorgenannte wissenschaftlich-technische Entwicklungen vollziehen, erlauben. In diesem Sinne richtet sich die Europäische Akademie mit ihren Ergebnissen vorrangig an wissenschafts- und technikpolitisch relevante Instanzen, besonders im nationalen und europäischen Bereich. Die Resultate der Arbeit der Projektgruppe werden Empfehlungscharakter haben und in Form eines Memorandums zusammengefasst. Die Resultate sollen den komplexen vielschichtigen Vertrauensbildungsprozess durch die verschiedenen gesellschaftlichen Akteure forcieren.

#### 5 Mitglieder der Projektgruppe

Vorsitz: *Dr. rer. pol. Otto Ulrich*, Referat Technikfolgen-Abschätzung, Bundesamt für

Sicherheit in der Informationstechnik (BSI), Bonn

*Professor Dr. sc. phil. Gerhard Banse*, Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Forschungszentrum Karlsruhe – Technik und Umwelt

*Dr. jur. Helmut Bäumler*, Landesbeauftragter für den Datenschutz Schleswig-Holstein, Kiel

*Professor Dr. jur. Jos Dumortier*, Interdisciplinary Centre for Law and Information Technology (IRCI), K.U. Leuven (B)

*Dr. jur. Riccardo Genghini*, Studio Notarile Genghini, Mailand (I)

*Professor Dr. phil. habil. Andrzej Kiepas*, Institut für Philosophie, Schlesische Universität Katowice (PL)

*Professor Dr. jur. Bernd Lutterbeck*, Institut für Angewandte Informatik, Technische Universität Berlin

*Dr. phil. Petr Machleidt*, Zentrum für Wissenschafts-, Technik- und Gesellschaftsstudien (CSTSS) beim Institut für Philosophie, Akademie der Wissenschaften der Tschechischen Republik, Prag (CZ)

*Professor Dr. rer. nat. Andreas Pfitzmann*, Institut für Theoretische Informatik, Technische Universität Dresden

*Professor Dr. phil. Georg Rudinger*, Psychologisches Institut, Abt. Methodenlehre, Diagnostik & EDV, Universität Bonn

*Professor Dr. sc. pol. Reinhard Voßbein*, Unternehmens- und Informations-Management Consultants Dr. Voßbein Unternehmensberatung (UIMC), Wuppertal

#### Veröffentlichungen

*Langenbach, C.J.*, 1999: Didaktik im Spannungsfeld zwischen NetUse und IT-Sicherheit. In: BSI (Hrsg.): Zur Didaktik der IT-Sicherheit. Interdisziplinärer Diskurs zu querschnittlichen Fragen der IT-Sicherheit. SecuMedia Verlag, Ingelheim

*Langenbach, C.J.*, 1999: Elektronische Unterschrift. Verliert der Bürger seine Identität?. Akademie-Brief Nr. 15, Europäische Akademie Bad Neuenahr-Ahrweiler

*Ulrich, O.*, 1999: Protection Profile – ein industriepolitischer Ansatz zur Förderung des „neuen Datenschutzes“. Graue Reihe Nr. 17, Europäische Akademie Bad Neuenahr-Ahrweiler

*Banse, G.; Langenbach, C.J.; Ulrich, O.*, 1999: Digitale Signaturen im Weitblick. KES 99/5, SecuMedia Verlag, Ingelheim, S. 85-87

**Kontakt**

Dr.-Ing. Christian J. Langenbach (Projektleiter)  
Europäische Akademie zur Erforschung von Folgen  
wissenschaftlich-technischer Entwicklungen Bad  
Neuenahr-Ahrweiler GmbH  
Wilhelmstr. 56, D-53474 Bad Neuenahr-Ahrweiler  
Tel.: + 49 (0) 26 41 97 33 11  
Fax: + 49 (0) 26 41 97 33 20  
E-Mail: [christian.langenbach@dlr.de](mailto:christian.langenbach@dlr.de)

« »