

Ziel oder Ende

Liebe Leserinnen, liebe Leser,

zumeist geht es mit der Technik und ihren Anwendungen rasant voran. Als Beispiel dafür gilt die Mondlandung, ein lange gehegtes sportliches Ziel der Menschheit. 1961 kündigte sie Präsident Kennedy für 1970 an. 1969 war es geschafft. Mit viel Geld. Ein damaliger Kritiker rechnete aus, man hätte für das gleiche Geld den Mount Everest zur Hälfte abtragen und nach Amerika verschiffen können. Auf der anderen Seite gibt es Ziele der Technik, die weniger spektakulär sind, großen Nutzen versprechen und dennoch nicht vorankommen.

So z.B. stellte man sich in der zweiten Hälfte der 70er-Jahre das Ziel, die elektronische Kommunikation für den Rechtsgebrauch sicher zu machen. Das erforderte insbesondere ein elektronisches Äquivalent der eigenhändigen Unterschrift. Für diesen Zweck kam man auf die Kryptografie und überlegte sich, wie mit ihr das Problem zu lösen wäre. Die bis dahin bekannten Kryptoverfahren erforderten, dass der Schlüssel geheim bleibt; sie waren also für eine öffentlich verifizierbare Signatur ungeeignet. Der Verifikationsschlüssel musste öffentlich sein. Man suchte und entdeckte asymmetrische Kryptoverfahren, mit einem geheimen Schlüssel zum Signieren und einem öffentlichen zum Verifizieren.¹ 1978 erschien dazu die bahnbrechende Publikation: „A method of obtaining digital signatures and public-key cryptosystems“.²

Das liegt heute mehr als dreißig Jahre zurück. Damals beflügelte es die Phantasie der Fachwelt und löste lebhaft akademische Aktivitäten aus; sehr zum Unmut der eingesessenen Kryptologen – Nachrichtendienste, Sicherheitsdienste, Polizei. Man konnte ja mit dem selben Algorithmus an den Aufpassern vorbei auch subversive Kommunikation verschlüsseln. Doch ließen sich die Normungsorganisationen nicht von ihrer Aufgabe abbringen. 1979/80 nahmen sie die Normung kryptographischer Systeme und deren Anwendungen auf. Bis heute haben sie rund 100 Normen dazu produziert, technische Normen, die den Grund für eine rechtssichere Kommunikation legen. Schritt haltend produzierte der Gesetzgeber das erste Signaturgesetz vom 22. Juni 1997. Europäisches Parlament und Rat erließen daraufhin die Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 13. Dezember 1999. Deutschland folgte der Vorgabe mit dem zweiten Signaturgesetz vom 16. Mai 2001. Am 11. Januar 2005 erschien das Signaturänderungsgesetz und am 26. Februar 2007 das Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz. Dazu kamen die Verordnungen und die Artikel zur Einführung der digitalen Signatur in anderen Gesetzen. So hält seit dreißig Jahren die digitale Signatur Gesetzgeber, Standardisierer, Telekom-Unternehmen und Sicherheitsdienste beschäftigt.

Hat man nun nach so viel Zeit das gesetzte Ziel erreicht? Dazu kann man in der letzten Dezemberausgabe dieser Zeitschrift lesen: „Trotz der wachsenden Bedeutung des Internet für die Kommunikation zwischen Behörden und Unternehmen sind Sicherheit, Vertraulichkeit und Rechtsverbindlichkeit des elektronischen Rechts- und Geschäftsverkehrs nicht gewährleistet.“³ Nicht gewährleistet! So ist es. Zwar bieten sich immer neue Anwendungen der digitalen Unterschrift an, aber mit dem alten Vorhaben ist man nicht am Ziel und auch nicht am Ende; es geht weiter. Und die Moral der Geschichte? Man kann, liebe Leserinnen und Leser, sich das Ziel setzen, den Mond zu betreten, und kann es auch überraschend schnell erreichen. Man kann aber nicht so schnell die Menschen dazu bringen, rechtssicher zu kommunizieren.

Mit freundlichen Grüßen, Ihr



1 W. Diffie, M.E. Hellman: New directions in cryptography, Trans IEEE Inf. Theory IT-22, 1976

2 R.L. Rivest, A. Shamir, L. Adleman, Comm ACM, 1978

3 A. Roßnagel, G.. Hornung, M. Knopp, D. Wilke: De-Mail und Bürgerportale, DuD 12/09