Sehr geehrte Damen und Herren,
Sie haben mich in einem Schreiben vom 1. Juni 2004 eingeladen, eine Stellungnahme abzugeben zur Verordnung ueber Zertifizierungsdienste im Bereich der elektronischen Signatur. Ich bin nicht in der Lage, detailiert Stellung zu nehmen, das Thema interessiert mich aber zentral in der Forschung. Ich sende diese Stellungnahme nur per E-mail. Sollten Sie eine Briefkopie benoetigen, so lassen Sie es mich bitte wissen. Ich habe einen Artikel beigefuegt, der gerade erschienen ist, und der meiner Ansicht nach fuer Ihre Ueberlegungen relevant ist. Er zeigt auf, dass das gaengige Verstaendnis der moeglichen Interpretation digitaler Evidenz (Signaturen, Zertifikate, Zeitstempel, Revokationslisten, etc.) logisch inkonsistent ist und dass ein konsistentes Verstaendnis zu signifikant unterschiedlichen und neuen Erkenntnissen fuehrt. Auch wenn die im Artikel praesentierte Sicht zunaechst provokativ erscheint, nehme ich an, dass diese Einsichten in Ihren Grundzuegen unvermeidbar sind und frueher oder spaeter in praktischen Systemen und auch in der Gesetzgebung miteinbezogen werden. Eine Grundfrage ist, welche Rolle digitale Evidenz innerhalb der gesamten verfuegbaren Evidenz hat, und welche Rolle nach wie vor physikalische Evidenz resp. Aussagen von Beteiligten und moeglichen Zeugen spielen sollen. Es geht hier nicht nur um Detailfragen, sondern um zentrale Kernfragen. Ist z.B. ein Zertifikat der Beweis, dass der zertifizierte Public Key mir gehoert, oder ist letztlich das physikalische Dokument, das ich allenfalls bei der Registrierung unterschreibe und worauf mein Public Key steht, der eigentliche Beweis, dass ich zum Public Key verpflichtet bin. Nimmt man die zweite Sichtweise, dann ist die Rolle des Zertifikates reduziert auf die Aussage der Zertifizierungsinstanz, dass ein solches physikalisches Dokument existiert und im Bedarfsfall vorgelegt werden koennte. Und so gesehen waere das Zertifikat als Evidenz unwichtig resp. irrelevant. Nimmt man die erste Sichtweise, dann koennte man gar nicht argumentieren, dass man nie ein Zertifikat beantragt hat, was sicher nicht wuenschenswert ist. Dies ist nur eine der grundlegenden Fragen, die man sich stellen muss, und die, einmal gestellt, zu ueberraschenden Erkenntnissen fuehrt. Ein meiner Ansicht nach wichtiges Konzept, das im Artikel diskutiert wird, sind sogenannte digitale Deklarationen, d.h. digitale Aufzeichnungen eines Willensaktes, relativ zum relevanten Kontext.
Der Nutzen einer solchen Technologie ist im Artikel diskutiert. Mit besten Gruessen, Ueli Maurer

--
Prof. Ueli Maurer
Department of Computer Science
ETH Zurich
http://www.crypto.ethz.ch/~maurer/