Grenzüberschreitende E-Identität

Am 17. September 2014 ist die eIDAS-Verordnung der EU in Kraft getreten. Diese Verordnung und weitere E-Government-Themen waren Schwerpunkte beim A-Trust-Infoday am 29. Oktober 2014 in Wien.

Eine Basis für den digitalen Binnenmarkt ist, dass darauf vertraut werden kann, dass der jeweilige Geschäftspartner in der EU derjenige ist, als der er sich ausgibt, und dass dies nachgeprüft werden kann. Bisher existieren hierfür nur nationale Regelungen, die auf der Signatur-RL 1999/93/EG (Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen) aufbauen. Auf der Grundlage dieser RL wurden in Österreich das mit 1. Jänner 2000 in Kraft getretene Signaturgesetz (SigG; BGBl I 1999/190) und die darauf aufbauende Signaturverordnung (SigV) erlassen. Durch das E-Government-Gesetz (E-GovG, BGBl I 2004/10) wurde unter anderem die Funktion „Bürgerkarte" geschaffen, die für das E-Government bereits auf den verschiedensten Rechtsgebieten zum Nachweis der Identität von Bedeutung ist.

Mit der „Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der RL 1999/93/EG" gibt es eine einheitliche Regelung für den EU-Binnenmarkt.

Die Verordnung (nicht amtliche Abkürzung: eIDAS-VO) wurde am 28. August 2014 im Amtsblatt der Europäischen Union verlautbart und ist am 20. Tag darauf in Kraft getreten. Um eine einheitliche Vollziehung zu gewährleisten, wurde anstelle einer zunächst in staatliches Recht umzusetzenden Richtlinie die Rechtsform einer unmittelbar verbindlichen Verordnung gewählt.

Die Verordnung bezweckt, das Vertrauen in elektronische Transaktionen im Binnenmarkt dadurch zu stärken, dass eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlicher Verwaltung geschaffen wird.

Die Rechtssicherheit elektronischer Identifizierungsmittel soll durch gegenseitige Anerkennung der Systeme gestärkt werden, damit die Vorteile des Binnenmarktes ausgeschöpft werden können. Geregelt wird die Anerkennung nationaler elektronischer Identifizierungssysteme gegenüber öffentlichen Stellen, wenn eine elektronische Identifizierung erforderlich ist (Art. 6). So kann ein sich ausweisender Spanier in Österreich auf elektronischem Weg ein Gewerbe anmelden. Das jeweilige nationale elektronische Identifizierungssystem muss der Kommission mitgeteilt (notifiziert) werden (Art. 9), die das Vorliegen der Anforderungen des Art. 7 nachprüft. Die Kommission veröffentlicht eine Liste der notifizierten elektronischen Identifizierungssysteme im Amtsblatt der EU. Der notifizierende Mitgliedstaat hat sicherzustellen, dass eine Online-Authentifizierung zur Verfügung steht, durch die die Personenidentifizierungsdaten bestätigt werden können (Art. 7 lit. f).

Manfred Matzka: „Es muss möglich sein, mit *einer* Registrierung Zugang zu allen Online-Anwendungen zu erhalten."

Peter Kustor: „Österreichische Lösungen wie Handy-Signatur und Bürgerkarte hätten „Export"-Potenzial."

Verschiedene Sicherheitsniveaus. Der Privatsektor soll ermutigt werden, freiwillig elektronische Identifizierungsmittel im Rahmen eines notifizierten Systems zu Identifizierungszwecken zu verwenden (Erwägungsgrund 17). Es wird keine zentrale „EU-eID" vergeben oder eine zentrale Datenbank eingerichtet. Die nationalen elektronischen Identifizierungssysteme müssen interoperabel sein (Art. 12).

Es wird zwischen den Sicherheitsniveaus „niedrig", substanziell" und „hoch" unterschieden (Art. 8), die durch Durchführungs-Rechtsakte noch zu definieren sind. Das Niveau „niedrig" kann von öffentlichen Stellen anerkannt werden. Bei den beiden anderen Niveaus ist diese Anerkennung verpflichtend (Art. 6 und 8). Bei Sicherheitsverletzungen ist die Authentifizierung auszusetzen und die Kommission sowie die anderen Mitgliedstaaten sind zu unterrichten (Art. 10). Der notifizierende Mitgliedstaat haftet für Schäden, die durch Fehler in seinem elektronischen Identifizierungssystem entstehen (Art. 11).

Vertrauensdiensteanbieter. Kapitel III der Verordnung betrifft Vertrauensdiensteanbieter. Das sind elektronische Dienste, die in der Regel gegen Entgelt elektronische Signaturen, Siegel oder Zeitstempel erstellen, prüfen oder validieren. Sie werden von einer nationalen Aufsichtsstelle überwacht. Jeder Mitgliedstaat veröffentlicht Vertrauenslisten, in denen qualifizierte Vertrauensdiensteanbieter erfasst sind. In

FOTOS: KURT HICKISCH

A-TRUST

Zertifizierungsdienst

Die *A-Trust GmbH* mit dem Sitz in Wien ist derzeit der einzige akkreditierte Zertifizierungsdiensteanbieter in Österreich. *A-Trust* stellt elektronische Bestätigungen (Zertifikate) darüber aus, dass jemand derjenige ist, als welcher er sich im Internet ausgibt, und zwar mit einem zusätzlichen, sekundengenauen Zeitstempel. Die Server stehen in einem Hochsicherheitsraum in Wien. Auslagerungen von Daten in die Cloud oder zu anderen Diensten finden nicht statt.

Sich bei *A-Trust* registrieren zu lassen, kostet nichts. Es werden überdies kostenlos in einem durch Passwort geschützten Speicherbereich 2 GB Speicherplatz zur Verfügung gestellt („Handy-Signatur-Konto"). Der „E-Tresor" mit größerer Speicherkapazität ist für den kommerziellen Bereich gedacht.

www.a-trust.at

diesem Kapitel sind einheitliche Regelungen für elektronische Signaturen, Siegel, Zeitstempel sowie Dienste für die Zustellung elektronischer Einschreiben angeführt. Die am 17. September 2014 in Kraft getretene Verordnung gilt ab 1. Juli 2016. Mit gleichem Tag wird die Signatur-RL aufgehoben.

A-Trust-Infoday. Bei dem vom Zertifizierungsdiensteanbieter *A-Trust GmbH (www.a-trust.at)* am 29. Oktober 2014 in Wien veranstalteten Informationstag war ein großer Teil der Vorträge und der beiden Podiumsdiskussionen der durch die eIDAS-VO geschaffenen Situation gewidmet – aus rechtlicher Sicht und im Hinblick auf die praktische Umsetzung. Die Veranstaltung wurde von rund 270 Teilnehmern besucht.

Österreich sei im E-Government gut aufgestellt, sagte Sektionschef Dr. Manfred Matzka (Bundeskanzleramt) und wies auf das am 1. November 2014 in Kraft getretene Personenstandsregister hin. Angesichts der rasanten technischen Entwicklung bezeichnete er die Zeitspanne für die Umsetzung der Richtlinie als zu lange. Man hätte sich, statt auf Interoperabilität der Systeme abzustellen, eher auf die Schaffung eines einheitlichen Systems konzentrieren sollen. Die Wirtschaft hätte verpflichtend eingebunden werden sollen.

So müsse man sich im Online-Handel, bei Banken und Versicherungen weiterhin mit jeweils neuen User-IDs und neuen Passwörtern abfinden, anstatt mit dem gesicherten Nachweis seiner Identität über die Funktion „Bürgerkarte". Auf diesem Konzept aufbauend, könnten sich intelligente Identitätslösungen entwickeln. „Es muss doch möglich sein, mit *einer* Registrierung Zugang zu allen Online-Anwendungen zu erhalten", betonte Matzka.

Mag. Peter Kustor, Leiter der Abteilung I/11 des BKA, schilderte den Werdegang der Verordnung und deren Vorgängerprojekt *STORK („Secure IdenTity acrOss boRders linKed"; www.eid-stork.eu)*. Da einige Staaten eigene Lösungen entwickelt hätten, habe man auf Interoperabilität der Systeme abstellen müssen. Die scheidende EU-Kommissarin Neelie Kroes regte in einen Brief an den nunmehrigen EU-Kommissionspräsidenten Jean-Claude Juncker an, den Weg der Digitalisierung der Kommission fortzuführen.

Bürgerkarte: Instrument zum sicheren Nachweis der Identität eines Menschen im elektronischen Rechtsverkehr.

Kroes unterfertigte dieses Schreiben elektronisch mit ihrer österreichischen Signatur von *A-Trust*. Die österreichischen Lösungen wie Handy-Signatur und Bürgerkarte hätten „Export"-Potenzial, betonte Kustor.

Für die Verhandlung der Durchführungsrechtsakte werde noch ein beträchtlicher Aufwand erforderlich sein. Ferner seien umfangreiche Anpassungen des innerstaatlichen Rechtsrahmens notwendig, insbesondere hinsichtlich SigG und SigV, E-GovG und der hiezu ergangenen Verordnungen, ebenso im ZustellG und ZustV.

Cyber-Kriminalität. Mag. Rudolf Unterköfler, Leiter der Abteilung II-BK-7 (Wirtschaftskriminalität) im Bundeskriminalamt, wies darauf hin, dass 40 Prozent der weltweit drei Milliarden Internetnutzer keine aktuelle Schutzsoftware verwenden. Täglich werden 1,5 Millionen Menschen Opfer von Cyber-Kriminalität. Die weltweite Schadenssumme wird auf 400 Milliarden Euro jährlich geschätzt. In der EU wurden von Jänner bis März 2014 125.000 Phishing-Angriffe registriert, hauptsächlich aus den ehemaligen GUS-Staaten. In den USA wurden in den letzten zwölf Monaten 500 Millionen Finanzdaten gestohlen.

In Österreich wurden im Jahr 2013 11.199 Fälle von Cybercrime registriert (+ 8,6 %), davon entfallen 7.670 Fälle auf Internet-Betrug (+ 15,9 %). Cybercrime werde begünstigt vom hohen Grad an Anonymität und das weltweite Netz mit seinen Verzweigungsmöglichkeiten, erläuterte Unterköfer. Unterschiedliche Rechtssysteme, geringe Kontrollmöglichkeiten, das Fehlen einer zentralen Steuerung und von Verantwortlichen begünstigten die Internet- Kriminalität, wenngleich das Netz aus dem heutigen Leben nicht mehr wegzudenken sei. Von UNO, EU und den Nationalstaaten würden Strategien zum Schutz der kritischen Infrastrukturen entwickelt.

Bei den zur Identifizierung und Authentifizierung im elektronischen Rechtsverkehr eingerichteten sicheren Systemen seien erste Missbrauchsfälle bekannt geworden, die allerdings eher auf menschliches Fehlverhalten zurückzuführen seien. Bei dem in Österreich etablierten System der Bürgerkarte sei noch kein Missbrauch polizeilich bekannt geworden. Unterköfler wies in diesem Zusammenhang auf die Wichtigkeit der Überprüfung der zum Nachweis der Identität vorgelegten Dokumente hin. „Für falsche oder gefälschte Dokumente dieser Art hat sich ein eigener Markt entwickelt."

Bürgerkarte. Als Instrument zum sicheren Nachweis der Identität eines Menschen im elektronischen Rechtsverkehr wurde in Österreich die Funktion „Bürgerkarte" geschaffen. Spezielle Smartcards wie die E-Card, sowie Dienst- oder Mitarbeiter-Ausweise und Handys *(www.handy-signatur.at)* kön-

FOTO: KURT HICKISCH

Rudolf Unterköfler: „Unterschiedliche Rechtssysteme und geringe Kontrollmöglichkeiten begünstigten Internet-Kriminalität.“

Michael Butz: „Wir werden bis Jahresende 2015 eine Million Handy-Signaturen freigeschaltet haben.“

nen über einen qualifizierten Zertifizierungsdiensteanbieter (in Österreich die *A-Trust GmbH)* mit dieser Funktion ausgestattet (freigeschaltet) werden. Der Betreffende muss seine Identität nachweisen. Das kann auf verschiedene Arten erfolgen. Für den Einsatz einer Smartcard ist ein Kartenleser erforderlich. Sie empfiehlt sich, wenn häufig personalisierte Dienste in Anspruch genommen werden.

Der Identitätsnachweis über die Handy-Signatur benötigt kein Zusatzgerät. Man erhält über SMS eine TAN, mit der man sich dann als identifizierter Benutzer über Computer und Internet einloggen und rechtsgültig Anträge stellen oder persönliche Daten (Versicherungszeiten, Pensionskonto) abfragen kann. Das breite Feld, das die Verwaltung für Online-Amtswege zur Verfügung stellt, ist unter anderem über *www.buergerkarte.at/anwendungen-handy.html* abrufbar.

Laut Michael Butz, MSc, Geschäftsführer der *A-Trust,* waren im November 2014 ca. 420.000 Handy-Signaturen freigeschaltet. Mit den Karten sind es mehr als 600.000 Signaturen. Monatlich kommen 20.000 bis 25.000 Freischaltungen dazu. „Bis Jahresende 2015 werden wir eine Million Handy-Signaturen erreichen“, sagte Butz.

Jedem Inhaber einer Signatur stellt *A-Trust* kostenlos einen geschützten Speicher von 2 GB zur Verfügung, der über ein persönliches Passwort zugänglich ist und in dem beispielsweise Dokumente, Rechnungen oder Arztbefunde abgelegt werden können. Geschäftskunden wird gegen Entgelt die *A-Trust*-Signaturbox mit erweitertem Funktions- und Speicherumfang zur Verfügung gestellt. *Kurt Hickisch*

Fotos: Kurt Hickisch