Düsseldorf, den 29. April 2015

Protokoll

der neunundzwanzigsten Sitzung des Ärztlichen Beirates

am Mittwoch, den 29. April 2015

in der Ärztekammer Nordrhein

in Düsseldorf

Vorsitz:	Dr. Christiane Groß, M.A., Dr. Dr. Hans-Jürgen Bickmann
Gast:	Matthias Redders (Ministerium für Gesundheit, Emanzipation, Pflege und Alter)
Anwesend:	s. Teilnehmerliste
Beginn:	17.30 Uhr
Ende:	20.00 Uhr

Hinweis: Aus Gründen der besseren Lesbarkeit wird in diesem Protokoll auf eine geschlechterdifferenzierte Formulierung verzichtet. Es wird ausdrücklich darauf hingewiesen, dass Begriffe wie Arzt, Patient, Mitglied usw. immer auch für die weibliche Form stehen, es sei denn, es wird ausdrücklich auf die männliche oder weibliche Form hingewiesen.

TOP 1 Begrüßung

Frau Dr. Groß begrüßt im Namen der beiden Vorsitzenden die Anwesenden (s. Teilnehmerliste). Insbesondere begrüßt sie die Referenten zum heutigen Thema Herrn Clemens Wanko und Herrn Dr. Georgios Raptis.

In der Tagesordnung muss der TOP 4 „Auswirkungen der eIDAS auf die TI“ entfallen, da Herr Michael Tautenhahn von der gematik den Termin kurzfristig abgesagt hat. Da die gematik auch die Folien des Vortrags nicht zur Verfügung gestellt hat, muss dieser TOP 4 vollständig entfallen. Dr. Groß stellt die abgeänderte Tagesordnung zur Abstimmung. Sie wird ohne Änderung angenommen.

TOP 2 Genehmigung des Protokolls der Sitzung vom 04. März 2015

Dr. Groß ruft als nächsten Tagesordnungspunkt die Genehmigung des Protokolls der letzten Sitzung auf. Da keine schriftlichen Einsprüche vorliegen und auch in der Sitzung keine Beanstandungen angemeldet werden, wird das Protokoll einstimmig ohne Enthaltungen angenommen.

TOP 3 Hat die qualifizierte Signatur nach Signaturgesetz (SigG) mit Inkrafttreten der eIDAS am 01.07.2016 ihr Lebensende erreicht?

Dr. Groß eröffnet diesen TOP mit dem Hinweis, dass die qualifizierte elektronische Signatur (QES) bei den geplanten medizinischen Anwendungen in der Telematikinfrastruktur eine entscheidende Rolle beim Aufbau einer Sicherheits- und Vertrauenskultur spielen sollte. Es. muss damit gerechnet werden, dass mit der neuen europäischen Verordnung das Sicherheits- und Vertrauensniveau unseres Signaturgesetzes gesenkt wird und dieses damit an sein Lebensende angelangt sein wird. Dr. Groß begrüßt noch einmal den Referenten zu diesem Thema, Herrn Clemens Wanko von der Zertifizierungsstelle der TÜV Informationstechnik.

Herr Wanko verrät zu Beginn seines Vortrags seine Einschätzung, dass er die Qualifizierte Signatur und das mit ihr durch das Deutsche Signatur Gesetz (SigG) erreichte Sicherheits- und Vertrauensniveau nicht an seinem Lebensende sieht. Dieses wird er in seinem Vortrag begründen. (Der Vortrag wird dem Protokoll beigefügt.)

Die neue EU-Verordnung Nr. 910/2014 über „elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS) regelt künftig europaweit den Umgang mit elektronischen Signaturen und Identifizierungen von Personen und Unternehmen und Websites. Sie wurde durch den EU-Ratsbeschluss am 23.07.2014 erlassen. Die eIDAS Verordnung löst bis zum 01. Juli 2016 die bislang gültige Signaturrichtlinie der EU ab. Damit wird sie auch das deutsche Signaturgesetz von 2001 ersetzen. Bis Mitte 2016 wird die eIDAS-VO schrittweise umgesetzt werden, wobei eine Reihe von Rahmenumsetzungen bereits erfolgt sind. Offen ist dann die Frage, welche Änderungen zum SigG vorgenommen worden sind.

Wanko stellt zu Beginn seines Vortrags einige bisherige Begriffe des SigG den künftigen der eIDAS-VO gegenüber. Dabei wird deutlich, dass sich zwar die Begriffe ändern, aber dieselben Organisationen dahinter stehen. Die „Zertifizierungsdiensteanbieter“ (ZDA) behalten ihren Status bei. Auch die Prüf- und Bestätigungsstellen wird es unter der anderen Bezeichnung Konformitätsbewertungsstelle auch weiterhin geben. Als zuständige nationale Aufsichtsstelle wird neben der Bundesnetzagentur noch das BSI treten. Warum man mehr als eine Stelle bestimmt hat, ist eine offene Frage.

In den folgenden Folien stellt Wanko die Umsetzung der bisher gültigen EU-Vorgabe „Signatur RL 1999/93/EG“ vor, insbesondere ihre Implementierung im Jahre 2001 ins deutsche Recht durch das „Signaturgesetz“ (SigG) und die „Signaturverordnung“ (SigV). Dieses war eine „Umsetzungsdirektive“, die rechtlich wie auch technisch in den Mitgliedstaaten nicht harmonisiert sondern unterschiedlich realisiert wurde, was zu keiner Interoperabilität zwischen den nationalen Systemen führte. Die technischen und administrativen Festlegungen wurden in Deutschland auf Basis anerkannter vertrauenswürdiger Technologien maßgeblich von der „Bundesnetzagentur“ (BNetzA) als zuständiger Behörde sowie der „Arbeitsgemeinschaft anerkannter Bestätigungsstellen“ (AGAB) bestimmt und verantwortet. Wanko erläutert, dass nach dem SigG sowohl angezeigte (6 Stück) sowie akkreditierte (9 Stück) ZDA gibt, die QES und qualifizierte Zeitstempel anbieten. In dieser Mengenübersicht sind auch ZDA enthalten, die ohne einen eigenen technischen Betrieb zugelassen wurden. Eine detaillierte Übersicht über die aktiven ZDA und denen, die ihre Dienste beendet haben oder deren Dienste von der Aufsichtsbehörde untersagt wurde, findet man unter http://www.nrca-ds.de/ .

In den restlichen Folien zur bisherigen Umsetzung erläutert Wanko die Dienste und Produkte, das Sicherheitsniveau und ihre Auflistung in der vertrauenswürdigen nationalen TSL (Trusted Service List) der BNetzA.

Gegenüber der „Richtlinie 1999/93/EG“ ist die neue „eIDAS-VO“ eine „Umsetzungsverordnung“, die zum 01.07.2016 das geltende Signaturrecht aller EU-Mitgliedstaaten vollständig ersetzen wird. Wanko erläutert zunächst in der Folie 15 den strukturellen Aufbau dieser Verordnung. Dieses Legal Framework (Rahmengesetzwerk) der eIDAS VO gliedert sich in Chapter (Kapitel), Section (Abschnitt) und Article (Artikel). In den blau dargestellten Kästchen sind die Textstellen angegeben, in denen die Vorgaben der Verordnung niedergeschrieben sind. In den Artikeln wird auch auf nachgelagerte Rechtsfestlegungen verwiesen, in denen die komplexen technischen Vorgaben auf europäischer Ebene und die spezifischen technischen Rahmenbedingungen der Mitgliedsländer Eingang finden sollen. Deshalb soll die Kommission mit dem Erlass von „Delegated Acts“ (delegierten Rechtsakten) bzw. „Implementing Acts“ (Durchführungsrechtsakten) die von europäischen und internationalen Normungsorganisationen und -einrichtungen — insbesondere dem Europäischen Komitee für Normung (CEN), dem Europäischen Institut für Telekommunikationsnormen (ETSI), der Internationalen Normungsorganisation (ISO) und der Internationalen Fernmeldeunion (ITU) — festgelegten Normen und technischen Spezifikationen gebührend berücksichtigen, damit ein hohes Maß an Sicherheit und Interoperabilität bei der elektronischen Identifizierung und bei den elektronischen Vertrauensdiensten erreicht wird. Bei den delegierten Rechtsakten geht es um die Regelung eines Gegenstandes, während es bei den Durchführungsrechtsakten um 24 Bereiche (davon 20 freiwillige und 4 verpflichtende) geht. Die eIDAS VO mit den delegierten Rechtsakten und den Durchführungsrechtsakten wird über das Vertrauensdienstegesetz in unser nationales Recht umgesetzt und voraussichtlich das SigG ersetzen. Dieses führt hoffentlich zu einer harmonisierten Umsetzung in den Mitgliedsstaaten und zu harmonisierten Anforderungen an die „Vertrauensdiensteanbieter“ (VDA). Von der eIDAS VO sind alle in der EU niedergelassenen Vertrauensdiensteanbieter betroffen, nicht jedoch Vertrauensdienste in geschlossenen Benutzergruppen, sogenannten „Closed User Groups“ (CUG).

Weiter erläutert Wanko in den Folien 18 bis 24 die Rahmenbedingungen der eIDAS VO mit einer Auflistung der vorgesehenen Vertrauensdienste und den technischen und organisatorischen Voraussetzungen und die Komformitätstätsprüfungen der Vertrauensdienstanbieter.

Zum Abschluss seines Vortrages kommt Wanko auf die Eingangs gestellte Frage zurück, ob er die Qualifizierte Signatur und das mit ihr durch das Deutsche Signatur Gesetz (SigG) erreichte Sicherheits- und Vertrauensniveau mit Einführung der eIDAS VO nicht an seinem Lebensende sieht. Zum besseren Verständnis seiner Begründung, dass er es nicht an seinem Lebensende angekommen sieht, nutzt Wanko Grafiken, mit denen er sowohl in einer Querschnittsdarstellung als auch in einer Draufsicht den Abdeckungsgrad unserer nationalen Gesetze einerseits und der eIDAS VO andererseits darstellt, indem er sie auf den Regelungsbedarf für Trust Service Provider projiziert. Dabei sieht man, dass das SigG, das DE-Mail-Gesetz und andere nationale Gesetze – jedes Gesetz für seinen Bereich - zusammen diesen Regelungsbedarf abdecken, während die eIDAS VO diesen Regelungsbedarf nicht vollständig abdeckt. Jedoch zeigt die Draufsicht auch, dass die eIDAS VO Bereiche des Regelungsbedarfs bedient, die nicht durch das SigG abgedeckt werden, sondern durch das DE-Mail-Gesetz oder durch andere nationale Gesetze. So kommt er zu dem Schluss, und hier zitiert er Herrn Prof. Dr. Alexander Roßnagel, dass sich im Ergebnis zeigt, dass die eIDAS VO bezogen auf den Regelungsbedarf von Vertrauensdiensten unvollständig und unterkom-

plex ist. Zum Abschluss seines Vortrags spielt Wanko 5 unterschiedliche Fälle zur Umsetzung von eIDAS in Deutschland durch, je nachdem ob

1. das SigG oder auch anderes Recht in Deutschland den gleichen Sachverhalt regelt wie die eIDAS VO, wobei die eIDAS VO den Anwendungsvorrang besitzt.
2. nur deutsches Recht für den Regelungsbedarf und keine eIDAS VO zur Verfügung steht, wobei nur deutsches Recht wie das SigG zur Anwendung kommt.
3. das deutsche Recht die Regelungen der eIDAS VO präzisiert, was zu einer Geltung der europäischen und der deutschen Rechtsebene führt.
4. der Durchführungsrechtsakt in der eIDAS VO offen bleibt, wobei nur das deutsche Recht zur Geltung kommt.
5. Gesetze/Regelungen mit ausschließlich nationaler Bedeutung auf das SigG verweisen, sodass es ausschließlich diesen Regelungsbedarf abdeckt.

Daraus kann man abschließend zusammenfassen, dass die Verordnung das deutsche Recht nicht außer Kraft setzt, sondern nur Anwendungsvorrang genießt. Deshalb gelten mitgliedschaftliche Bestimmungen weiter, finden aber nur insoweit Anwendung, als sie den Bestimmungen der Verordnung nicht widersprechen. Jedoch wird es nach wie vor offene Punkte geben, wie Archivierungsfristen und Haftungsregelungen, die zwischen den Mitgliedstaaten harmonisiert werden müssen.

Die VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 **über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG** finden Sie im Internet unter:

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.DEU

Dr. Groß bedankt sich bei Herrn Wanko für seinen Vortrag und schlägt vor, den Vortrag von Herrn Dr. Raptis sofort anzuschließen und die Fragen des Auditoriums zu beiden Vorträgen wegen ihrer inhaltlichen Nähe nach diesem zweiten Vortrag zu stellen.

TOP 5 Auswirkungen der europäischen Signaturverordnung (eIDAS) auf die Heilberufsausweise und die medizinische Versorgung in Praxis und Klinik

Dr. Groß begrüßt Herrn Dr. Georgios Raptis von der Bundesärztekammer, der in seinem Vortrag der Frage annehmen wird, was sich mit der Umsetzung der eIDAS VO in deutsches Recht beim elektronischen Heilberufsausweis (eHBA) und bei den Signaturverfahren nach dem bisherigen Beratungsstand der technischen Spezifikationen ändern wird. (Der Vortrag wird dem Protokoll beigefügt.)

Herr Dr. Raptis erläutert, dass die EU-Kommission die europäischen Standardisierungsorganisationen beauftragt hat, technische Rahmenbedingungen zusammen mit den Mitgliedsstaaten zu erarbeiten, damit ein hohes Maß an Sicherheit und Interoperabilität bei der elektronischen Identifizierung und dem Signaturverfahren im Rahmen der Umsetzung der eIDAS VO erreicht wird. Mit dem Mandat m/460 hat die EU-Kommission den Auftrag (an die ETSI) erteilt, technische Standards zu erarbeiten, um Interoperabilität beim Einsatz elektronischer Signaturen auf europäischer Ebene zu verwirklichen. Die Kommission wird in naher Zukunft diese technischen Spezifikationen unter eIDAS als Durchführungsrechtsakte erlassen. Dr. Raptis nimmt an, dass die veröffentlichten Entwürfe stabil bleiben und den Kern der techni-

schen Spezifikationen unter eIDAS bilden. Deshalb ist es Aufgabe der Experten der BÄK, der Bundesnetzagentur, des BSI u. a., diese Entwürfe zu analysieren und im Falle von Defiziten, diese zu kommentieren. So ist nach dem aktuellen Stand der technischen Rahmenbedingungen eine Zertifizierung der Signatursoftware nicht mehr erforderlich, sodass eine solche Zulassung für die „Signaturanwendungskomponente“ (SAK) im Konnektor der TI auch nicht mehr notwendig ist. Da die deutschen Ärzte für ihre QES ein Attributzertifikat als berufsständischen Nachweis benötigen, das im Mandat M/60 von der ETSI nicht standardisiert wurde, wird dieses von der BÄK mit den anderen beteiligten deutschen Organisationen entsprechend beanstandet.

Dr. Raptis sieht keine substantiellen Änderungen bei der Beantragung und Herausgabe von eArztausweisen unter der eIDAS VO, auch wenn die BÄK heute fordert, dass nur akkreditierte „Zertifizierungsdiensteanbieter“ (ZDA) eArztausweise erstellen sollen, was unter der eIDAS nicht erforderlich ist.

In seinem Vortrag führt Dr. Raptis weitere Unterschiede in der PKI und den Zertifikatsprüfungsverfahren zwischen Status-quo im Sig G und der eIDAS VO auf, wie die Ersetzung der Wurzelinstanz (Root) im SigG durch eine „Trust-service Status List“ (TSL). Letztere Vertrauenshierarchie wird in der TI der gematik bei den nicht qualifizierten Zertifikaten aber schon eingesetzt. Ein weiteren Unterschied zwischen der kommenden eIDAS VO und dem SigG sieht Dr. Raptis im Gültigkeitsmodell, also dem Verfahren, mit ein Anwender oder Dienst überprüft, ob ein Zertifikat noch gültig ist oder nicht. Er präferiert das bei uns genutzte Kettenmodell gegenüber dem Schalen- oder PKIX-Modell der ETSI-Standards und hofft, dass unser Gültigkeitsmodell auch dort anerkannt werden wird. Ebenfalls beanstandet Dr. Raptis in diesem Zusammenhang der Gültigkeitsprüfung, dass man entsprechend dem ETSI-Standard gezwungen ist, Zeitstempel zu verwenden, was aufwendiger ist und zu Problemen führt, wenn man Anwendungen nutzt und nicht mit der TI verbunden ist, um Zeitstempel nutzen zu können. Zum weiteren hält Dr. Raptis den Zeitraum für die Nachprüfbarkeit von Daten bei qualifizierten Vertrauensdiensteanbietern nach der eIDAS VO für nicht akzeptabel.

Positiv ist nach Ansicht von Dr. Raptis anzumerken, dass die neu hinzugekommenen Vertrauensdienste der eIDAS VO, wie „Validierungsdienst“ oder „Bewahrungsdienst“, die bei den komplexen Prozessen der Signaturvalidierung oder der Langzeitnutzung von Signaturen z. B. bei der Archivierung von Dokumenten, dem Anwender das Leben einfacher machen können. Jedoch sind hierbei die Besonderheiten beim Umgang mit medizinischen Dokumenten zu berücksichtigen.

Dr. Raptis zeigt auf seiner abschließenden Folie die Bereiche, in denen die BÄK an der eIDAS VO mitarbeitet und zusammenfassend die Themen, die er auch im Vortrag vorgetragen hat, bei denen Anpassungsbedarf besteht.

Mit einem Dank an Herrn Dr. Raptis eröffnet Dr. Groß die Diskussion.

Es wird gefragt, ob auch die Zahnärzte auf der Bundesebene in den Arbeitsprozess zur eIDAS VO eingebunden seien. Dr. Raptis erläutert, dass die BÄK von ärztlicher Seite diese Arbeit koordiniert und alle über eIDAS informiert, die eHBA nutzen. Des Weiteren ist auch die gematik in diesen Arbeitsprozess eingebunden, die die Anforderungen an den eHBA festlegt, sodass alles koordiniert ist.

Auf die Frage, ob die elektronische Fernsignatur in der eIDAS VO berücksichtigt werde, antwortet Dr. Raptis, dass der Schlüssel dabei bei einem Diensteanbieter aufbewahrt werden

müsse, was technisch zwar möglich sei, aber er noch nicht gesehen habe. Im Gesundheitswesen ist ein solches Verfahren noch nicht gewünscht.

Auf die Frage, ob es unter eIDAS die Möglichkeit der Anhebung einer minderwertigen Signatur auf ein qualifiziertes Niveau gibt, weist Dr. Raptis darauf hin, dass ihm das nicht bekannt sei.

Wenn heute bei uns ein Zertifizierungsdiensteanbieter seinen Betrieb vollkommen einstellt, garantiert die Bundesnetzagentur dass die gesetzlichen Anforderungen erfüllt bleiben. Auf die Frage, ob dieses Verfahren auch unter der eIDAS VO vorgesehen ist, weist Herr Wanko darauf hin, dass ein entsprechendes Verfahren unter der eIDAS VO noch nicht bekannt ist.

TOP 6 Diskussion / Verschiedenes

Angesichts der fortgeschrittenen Zeit gibt es keine weiteren Diskussionspunkte, sodass Dr. Groß nur noch die nächsten Termine bekannt gibt:

- Die Vorbesprechung zum nächsten Ärztlichen Beirat ist am Mittwoch den **20. März 2015** um 20:00 Uhr in der Ärztekammer Nordrhein in Düsseldorf, wo das Thema für die nächste Sitzung festgelegt wird.
- Die nächste Sitzung des Ärztlichen Beirats ist am Mittwoch den **24. Juni 2015 um 15:00 Uhr** in der Ärztekammer Düsseldorf.