Die Allmachtsphantasien für die Umsetzung des digital identifizierbaren

Bürgers in der EU,

ohne demokratisch-parlamentarische Prozesse und ohne Bürgerbeteiligung,

beschleunigt umgesetzt über die Zwänge im neuen Gesundheitssystem,

der Telematikinfrastruktur

Das Gesundheitsministerium plant nun den Konnektor und das bei den Ärzten unbeliebte Versichertenstammdatenmanagement 2023 abzuschaffen, Patienten und Ärzte sollen sich dann über ihre **digitale Identität** identifizieren.

Siehe

https://www.aend.de/download/26a2d794c7

Was steckt dahinter?

Zunächst einmal ermöglichen die Pläne Einsparung für Hardware wie den Konnektor, die Kartenlesegeräte und die Chipkarten, die dann je nach Lösungsszenario nicht mehr benötigt werden.

Das bisher bekannte Authentifizierungsverfahren, im Zusammenspiel mit der elektronischen Gesundheitskarte, dem Heilberufsausweis und dem Konnektor, finden dann in dieser Form nicht mehr statt.

Die Lösung dafür ist die **digitale Identität!** Die digitale Identität, ein eher allgemeiner Begriff, ist hier vielmehr gleichzusetzen mit den seit Jahren andauernden Bemühungen der europäischen Union eine einmalige und unverwechselbare digitale Identität zu schaffen, die unsere analoge Identität ablöst. Da dann unsere Identität und die damit verbundenen persönlichen Angaben wie z.B. Name und Adresse permanent über dieses neue elektronische Verfahren aktualisiert und mit den Krankenkassen im Hintergrund automatisch abgeglichen werden können, erübrigt sich das Versicherten-Stammdaten-Management und die notwendige Aktualisierung und Abspeicherung dieser Daten direkt auf den Chipkarten, wie der eGK und dem HBA.

Siehe z.B.

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html

Damit Sie verstehen können was hier passiert sollten Sie die zwei Begriffe PKI und die Zertifikatsverkettung und Ihre Wirkungsweise grob nachvollziehen können. Bitte berücksichtigen Sie, dass meine nachfolgenden Ausführungen nur dem Zweck dienen soll Ihnen diese komplexe Sachverhalte in ungefährer Weise nahe zu bringen.

PKI und die Zertifikatsverkettung, siehe

https://de.wikipedia.org/wiki/Public-Key-Infrastruktur
https://de.wikipedia.org/wiki/Digitales_Zertifikat

Eine recht einfache Erklärung was PKI und Zertifikate sind:

https://www.computerweekly.com/de/definition/PKI-Public-Key-Infrastruktur

Ein Zertifikat ist eine Datei, z.B. mit der Endung *.asc die einen mathematisch verschlüsselten Wert enthält, dessen Berechnung von einem Masterzertifikat abhängig ist. Die Existenz dieses Zertifikates ersetzt sozusagen die eGK-Chipkarte und kann auch theoretisch Ihren Personalausweis, der ja noch als Chipkarte verbreitet ist, ersetzen.

Das Zertifikat und die Software, mit der Sie dann ihre elektronische-digitale Identität nachweisen, benötigt eine Online-Verbindung zu einem Mastersystem in einem europäischen Rechenzentrum in dem die Masterzertifikate liegen und die kryptographischen Berechnungen durchgeführt werden.

Es besteht in dieser Hinsicht eine Zertifikatsverbindung und Abprüfung, unter Umständen sehr viele Zertikate, die eine Kommunikationskette bilden.

Das Masterzertifikat liegt in einem hochgesicherten Rechenzentrum und steht in Verbindung mit dem Zertifikat, was Ihnen zugeteilt wurde und mit dem Endgerät verknüpft sein muss was Sie gerade benutzen, also ein Smartphone, ein Tablet oder der Microchip unter Ihrer Haut, falls Sie sich schon dafür entschieden haben, was ich sehr bedauern würde.

Das Betriebssystem Linux und freie Software, die zur Verfügung steht, ermöglicht übrigens jedem der das Know how hat eine eigene Public-Key Infrastruktur (CA) mit selbst signierten Zertifikaten aufzubauen! Mit Linux ist es es möglich eigene kryptographische Schlüssel zu generieren.

Schon einigemale haben staatliche Stellen versucht diese Fähigkeiten dem freien Betriebssystem Linux wegzunehmen.

Nun entstammt aber die digitale Identität des Gesundheitsministers, samt der europäischen Pläne, nicht diesem freien Ansatz in eigener Selbstbestimmung.

Die von mir geschilderte Systematik der Nutzung der Zertifikate steht noch mit weiteren Merkmalen und Komponenten in Verbindung, wie einer global einmaligen Versichertennummer oder auch der eindeutigen Ident-Nummer ** Ihres Smart-Phones.

Deswegen macht es Sinn im Rahmen dieser groben Skizzierung das Verfahren der digitalen Idenität und der Abprüfung so darzustellen:

Digitale Identität = Globale Personen Identitätsnummer, inkl. der numerischen Teilmenge der Versicherten-ID + trusted components (z.B. biometrische Merkmale)

+ Endgerät, inkl. der Software oder Portalanwendung, die die digitale Identität überprüft

Die gemeinsame Einsicht in die ePA, die elektronische Patientenakte, würde dann erfolgen, wenn beide Partner, der Arzt und Patient sich per digitaler Identität authentifiziert haben und die Authentifizierungs- und Datenverarbeitungsprozesse ohne Fehler durchgelaufen sind.

Die Frage welche Endgeräte hier dann benutzt werden betrifft eine derzeit offene Situation, da die neuen technischen Lösungen nicht ein an bestimmtes Endgerät gebunden sind.

Wie gesagt das Verfahren könnte mit dem Smartphone oder dem Tablet mit der entsprechenden App oder direkt integriert in die Arztsoftware abgewickelt werden.

Jetzt erstmal durchatmen, denn was passiert hier gerade in enormer Geschwindigkeit?

Das BMG und der Gesundheitsminister versuchen die exponentiell verlaufende Technikentwicklung, in ihrem rasenden Fortschritt, in die praktischen Abläufe des deutschen Gesundheitssystems zu pressen. Das war vorbereitet über die erkennbare Philosophie der Vereinnahmung eines dezentral und vielfältigen Gesundheitssystems über das verkrampfte Schema der sogenannten Primärsysteme und Leistungserbringer.

Wohl oder übel wahr, Menschen und Leistungen wurden so zu Erbringern und primären Datenlieferanten-Systemen. Alleine diese erste Erzwingung des Schemas, in der langen Reihe folgender Zwangsmaßnahmen, ohne intensive Beteiligung der bürgerlichen Gesellschaft, hätte nicht passieren dürfen.

Nicht nur, dass die Philosophie und Ethik der Telematikinfrastruktur die Niedergangsphase des freien, selbstbestimmten und physisch lebendigen und analogen Menschen unterstützt und beschleunigt soll jetzt auch noch über die geschaffene Zwangskultur des neuen deutschen Gesundheitssystems die digitale Identitätskopie von uns im Industrie 4.0 Konsortium und in den europäischen Staatsgebilden verankert werden.

Das ist das Ende einer freien und selbstbestimmten Existenz, eines Lebens was sich anonym und unbeobachtet entfalten und bewegen kann.

Wie oft gesagt: All dies entspringt nicht aus einem deutschen oder auch europäischen Demokratie und Parlamentsprozess, oder aus einer breiten gesellschaftlichen Mitnahme und Diskussion und erst recht nicht aus einem entschleunigten und gründlichen Denkprozess, der die Grundlagen für Gestaltung und Überprüfung bildet.

Viele der beteiligten Technik- und IT-Unternehmen, die mit an der Telematikinfrastruktur gewerkelt haben, wie z.B. der Chipkartenhersteller Giesecke & Devrient oder die Thales Group arbeiten intensiv an der schönen neuen Welt,

siehe (bitte Links selbst kopieren) >>

https://www.gi-de.com/de/mobile-security/industries/unternehmen/identitaets-und-zugriffsmanagement

https://www.vesta-gematik.de/standard/formhandler/324/gemSpec_Autorisierung_V1_0_0.pdf

Die Rolle der Device-ID (IMEI) Auswertung in neueren Verfahren zur Identifizierung eines mobilen Endgerätes in einem digitalen-zellulärenMobilfunknetz >>

https://www.epo.org/law-practice/case-law-appeals/recent/t132032du1.html

Indoor-Tracking >>
https://www.fokus.fraunhofer.de/go/indoor-navigation

In meinem Artikel ePA, DMS, SNOMED-CT und ePA-DMS beschreibe ich mit der Systematik zusammenhängende Unsicherheitsfaktoren durch die Anmeldung am ePA-System mit mobilen Geräten (Smartphone, Tablet) auf Basis der im Gerät gebildetenDevice-ID (IMEI)

http://www.rdlenkewitz.eu/html/pdf/epa_snomed.pdf

Der Weg ist also bereitet für die allumfassende und permanente Kontrolle des Menschen und dagegen müssen wir uns entschieden zur Wehr setzen in dem wir die Menschen aufklären und zum Nachdenken anregen.

Den Allmachtsphantasien für die Umsetzung des digital identifizierbaren Bürgers in der EU, ohne vorherige demokratisch-parlamentarische Prozesse und ohne Bürgerbeteiligung, verankert in der Telematikinfrastruktur des neuen Deutschen Gesundheitssystems, für die staatliche Produktion und Verwertung unserer persönlichsten und sensibelsten Daten, muss ein Ende bereitet werden.

Sonntag, 1.11.2020

Rolf D. Lenkewitz 87769 Oberrieden
0163170 68 09

www.rdlenkewitz.eu

http://www.rdlenkewitz.eu/DSGVO/dsgvo.html