Eine Themenbeilage der
Heise Medien GmbH & Co. KG

I
2015

SICHERHEIT & DATENSCHUTZ

Verschlüsselung, Authentifizierung und Public-Key-Infrastruktur

Access Control:
Was Biometrie heute schon leisten kann

OpenPGP für Unternehmen:
Wie Open Encryption für Firmen funktioniert

E-Mail Security:
Welche Gefahren mit der Post kommen

Smart Grids & Industrie 4.0:
Wann kritische Infrastrukturen sicher sind

Vertrauensnetzwerke:
Wem wir unsere Schlüssel anvertrauen dürfen

Public-Key-Infrastruktur:
Welche Aufgaben eine PKI übernehmen muss

powered by: TeleTrusT Pioneers in IT security. iX

Digitale Souveränität

Liebe Leserinnen und Leser,

sind Sie digital souverän? Können Sie mit jedem Ihrer Geschäftspartner einfach, aber dennoch vertraulich kommunizieren? Sind Ihre täglich zu übermittelnden Daten ausreichend vor fremden Blicken geschützt?

In unserer durchdigitalisierten Gesellschaft sind sensible Daten ein begehrtes Gut und deshalb auch ständigen Gefahren ausgesetzt. Durch Schnüffelaktionen, Cyberkriminalität und allzu oft einfach durch Fehler bei der Absicherung kommen Daten abhanden und können anschließend durch Dritte verwertet werden. Auch der Gesetzgeber nimmt, unter anderem bedingt durch die sich etablierende Meldepflicht sicherheitsrelevanter IT-Vorfälle bei kritischen Infrastrukturen, Einfluss auf die Hoheit über Unternehmensdaten. Obwohl ein effizienter Schutz von Bestands- und Kommunikationsdaten zum Standard gehören sollte, besteht bei vielen Unternehmen, Organisationen und Institutionen noch dringender Nachholbedarf.

All diesen Herausforderungen zum Trotz ist aber digitale Souveränität möglich. Die IT-Sicherheitsbranche in Deutschland ist sehr gut aufgestellt und besitzt durch die starke deutsche Datenschutzgesetzgebung ein Alleinstellungsmerkmal. Die mittelständisch geprägte deutsche IT-Sicherheitswirtschaft gilt mit ihren Lösungen und Dienstleistungen als innovativ und wegweisend. „IT Security made in Germany“ steht wie ein Leuchtturm und strahlt über Deutschland hinaus.

Die vorliegende Beilage „Sicherheit & Datenschutz“ will Ihnen Einblick in ausgewählte Themen der IT-Sicherheit verschaffen, die uns als Bundesverband IT-Sicherheit derzeit beschäftigen. Unsere Artikel zielen dabei auf grundsätzliche Fragen ab, mit denen Sie sich als IT-Verantwortlicher beschäftigen müssen. Neben Alltagsproblemen kleiner und mittelständischer Unternehmen (KMU) mit der Verschlüsselung soll Ihnen das Themenfeld „E-Mail Security“ (S. 14) nähergebracht werden. Damit verbunden stellt sich die Frage, wie „Vertrauensnetzwerke“ (S. 33) dazu ihren Beitrag leisten können.

Außer der technischen Sicherheit spielt insbesondere der verantwortungsbewusste Umgang mit den eingesetzten Verschlüsselungstechnologien eine zentrale Rolle. Hierzu stellen wir Ihnen mit Beiträgen zu den Themen „OpenPGP für Unternehmen“ (S. 8), „Any-to-Any Encryption“ (S. 20) und „Public-Key-Infrastrukturen“ (S. 29) drei Konzepte vor, die Ihnen bei der Realisierung der Verschlüsselung in Ihrem Unternehmen helfen können.

Einen Schwerpunkt unserer aktuellen Arbeit bilden gegenwärtig auch die Herausforderungen des geplanten IT-Sicherheitsgesetzes und dessen Auswirkungen auf Unternehmen und kritische Infrastrukturen Dies wird in den Beiträgen zum „IT-Sicherheitsgesetz“ (S. 19) und zum Thema „Smart Grids & Industrie 4.0“ (S. 26) differenziert aufbereitet.

Weitere Praxisbeiträge, etwa zur technischen Zukunft der Gesundheitsfürsorge im Artikel „E-Health-Telematik“ (S. 11) sowie zu Anwendungsszenarien biometrischer Verfahren in Verbindung mit dem Thema „Access Control“ (S. 4), runden diese Beilage ab.

Wir möchten Sie mit unseren Beiträgen anregen, sich stärker mit Ihrer IT-Sicherheit zu beschäftigen: Bewahren Sie Ihre digitale Souveränität!

Dr. Holger Mühlbauer
TeleTrusT – Bundesverband IT-Sicherheit e.V. (Geschäftsführer)

Access Control
Biometrie wird alltagstauglich 4

OpenPGP für Unternehmen
Leitfaden für eine effiziente E-Mail-Verschlüsselung 8

E-Health-Telematik
Digitale Vernetzung im Gesundheitswesen 11

E-Mail Security
Rechtssichere und vertrauliche E-Mail-Kommunikation 14

IT-Sicherheitsgesetz
(Un-)Sicherheit im nationalen Alleingang? 19

Any-to-Any Encryption
Verschlüsselt an alle und überall 20

Smart Grids & Industrie 4.0
Kritische Infrastrukturen brauchen schärferen Schutz 26

Public-Key-Infrastrukturen
Nach innen und außen zuverlässig geschützt 29

Vertrauensnetzwerke
Verschlüsselung allein ist nicht alles 33

Digitale Vernetzung im Gesundheitswesen

Der Masterplan für eine zukunftssichere E-Health-Infrastruktur scheint zu stehen

Die Planungen für die elektronische Gesundheitskarte und eine passende telematische Infrastruktur in Deutschland wurden intensiv diskutiert. Der Informationsstand ist aber sogar in Fachkreisen oft dürftig und von Pseudodebatten geprägt. Dabei ist das konzeptionell solide Projekt recht visionär aufgesetzt.

Das gesamte deutsche Gesundheitswesen soll zukünftig mittels einer dedizierten Telematikinfrastruktur (TI) sicher und sektorenübergreifend, etwa zwischen ambulantem und stationärem Bereich, digital vernetzt werden. Elektronik ersetzt Papier. Das ist eine Infrastrukturmaßnahme von einschneidender Bedeutung für jeden Bürger. Diese Kurzübersicht will etwas Transparenz in die Details des Megaprojekts bringen. Dafür lohnt sich zunächst ein Blick auf die vier Kernkomponenten der anvisierten Telematikinfrastruktur: Gesundheitskarten, Heilberufsausweise, Konnektoren und gesicherte Vernetzung.

Physische Zugangsarten

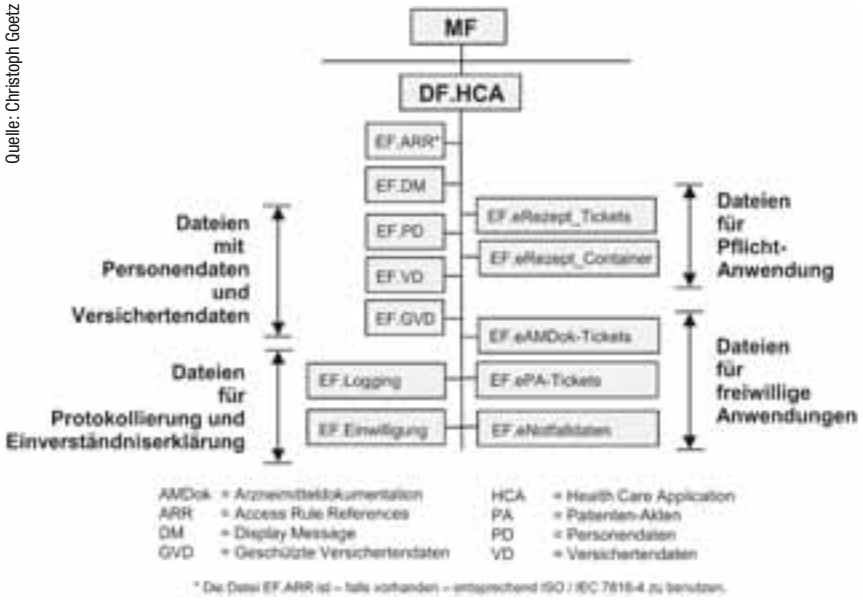
Die neue *elektronische Gesundheitskarte* (eGK) dient für jede gesetzlich versicherte Person in Deutschland als Versicherungsnachweis und gewährt Zugang zu den Leistungen der Gesetzlichen Krankenversicherung (GKV). Physisch ist sie eine Mikroprozessorkarte mit zertifiziertem Kartenbetriebssystem (COS). Sie trägt die Sicherheitsprüfung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf der Stufe „Hoch“ mit Kopier- und Änderungsschutz sowie PIN-Funktionen für die Zugriffe. Das COS unterstützt hochwertige Kryptografie und unterbindet jeden Zugriff auf die im Chip gespeicherten Schlüssel. Beim Rollout enthält sie im Wesentlichen die gleichen Stammdaten wie die bisherige Krankenversichertenkarte (KVK), also Name, Anschrift, Versicherungsverhältnis usw., das Ganze jedoch zweimal (einmal im alten KVK-Stil und einmal in einem gesicherten Container, also vergleichbar einer signierten Datei). Darüber hinaus trägt sie ein Bild des Versicherten und die Braille-Kennzeichnung „eGK“. Die Datenfelder im Chip enthalten Zertifikate mit zwei Schlüsselpaaren: eines für die Anmeldung (also Authentifizierung) und eines für die Ver- und Entschlüsselung. Weitere Container im Chip sind definiert und können später je nach PIN-Freischaltung gelesen, geschrieben oder aktualisiert werden. Zusätzlich enthalten die Karten ein Card Verifiable Certificate zur Abwicklung von Card-to-Card-Mechanismen. Ein CV-Zertifikat kann direkt von einer Chipkarte gelesen und direkt durch eine andere Karte verifiziert werden.

Spezielle *Heilberufsausweise* (HBA) gibt es für die Mitglieder der vier verkammerten Heilberufe, also die Ärzte, Zahnärzte, Apotheker und Psychotherapeuten. Auch sie sind Chip-Karten mit geprüftem und zertifiziertem COS. Sie enthalten mittels Postident und Kammerbestätigung verifizierte Stammdaten und tragen ein Bild des Heilberuflers. Die Datenfelder im Chip enthalten HBA-Attribute, Signaturen und Zertifikate mit drei Schlüsselpaaren: eines für die Anmeldung, eines für die Ver- und Entschlüsselung und ein drittes für die Qualifizierte Elektronische Signatur (QES) nach dem deutschen Signaturgesetz. Auch diese Karten enthalten ein CV-Zertifikat. Sie ersetzen die bisherigen Kammerausweise aus Karton oder in Leporelloform.

Neue Netzstrukturen

Neben den speziellen (Dual-Slot-)E-Health-Kartenterminals, die zum Stecken, Auslesen und zur gegenseitigen Authentifizierung der eGK und HBA zum Einsatz kommen und ebenfalls zum Schreiben und zur Aktualisierung der Gesundheitskarten verwendet werden, ist der *Konnektor* eine der wichtigsten dezentralen Komponenten der TI. Er sitzt

Quelle: Christoph Goetz



Die Elementary Files (EF) der eGK decken alle relevanten Bereiche ab.

zwischen dem Praxis- oder Kliniknetz und dem Wide Area Network der TI. Netzwerktechnisch bildet er das Bindeglied zwischen den Primärsystemen, also Praxis oder Klinik, und den Diensten und Anwendungen der zentralen TI der Leistungserbringer. Er verfügt mittels Security Module Card (SMC) über eine eigene elektronische Identität und funktioniert gleichzeitig als Netz- und Anwendungskonnektor sowie als Signaturanwendungskomponente. Die Anwendungen laufen dabei nach einem serviceorientierten Architekturansatz (SOA) ab. Sie werden lastverteilt und bestimmte Nachrichtentypen werden durch das Ersetzen von personenbezogenen Zertifikaten (durch Rollenzertifikate) anonymisiert.

Konzeptionell und funktionell eng mit dem Konnektor verbunden ist die Architekturentscheidung, grundsätzlich nur *gesicherte Vernetzung* mittels Tunnel, als sogenannte Virtuelle Private Netze (VPNs), zuzulassen. Der Konnektor baut IPsec-Tunnel zu den VPN-Zugangsdiensten auf, die aus den verschiedenen Netzwerken der Leistungserbringer angeboten werden. Das ermöglicht eine dezentrale Nutzung von zentralen und fachanwendungsspezifischen Diensten vieler verschiedener Anbieter sowie die Auswahl von Anwendungsoptionen für die Nutzung eines speziell gehärteten Internetzugangs.

Erweiterte Sicherheitskomponenten

Es gibt aber noch andere wichtige Authentifizierungskomponenten für die geplante TI und noch weitere Akteure. Langfristiges Ziel ist eine gemeinsame, zuverlässige und sichere Vernetzung für das gesamte deutsche Gesundheitswesen mit vergleichbarer Qualität für alle Beteiligten. Anforderungen auf gleicher Augenhöhe sind in der TI des Gesundheitswesens besonders wichtig. Jedes Sicherheitsprinzip würde zusammenbrechen, wenn sich z.B. die Heilberufsangehörigen durch qualifiziertes „Haben und Wissen“ (also Karte und PIN) ausweisen müssten, während sich andere Gesundheitsakteure nur mit Namen und Passwort (also nur „Wissen“) oder einfach ungesichert einklinken könnten. Die Entwickler haben das erkannt, entsprechende Lösungsansätze sind weit fortgeschritten, teilweise schon in Erprobung.

Rein technisch betrachtet werden neben den Heilberufsausweisen, die auf eine individuelle Person ausgestellt sind, auch elektronische Sicherungs- und Identitätsobjektanker für andere Zuschnitte bzw. Kollektive benötigt:

Die *gSMC-KT* (gerätespezifische Security Module Card für Kartenterminals) implementiert durch ein eingebautes Sicherheitsmodul die Identität des E-Health-Kartenterminals. Sie dient der sicheren Kommunikation mit anderen Komponenten der TI (z.B. durch Unterstützung einer Remote-PIN-Eingabe).

Die *gSMC-K* (gerätespezifische Security Module Card für Konnektoren) implementiert, ebenfalls durch ein eingebautes Sicherheitsmodul, die Identität des Konnektors. Auch sie sorgt für eine sichere Kommunikation innerhalb der TI.

Die *SMC-B* (Security Module Card, Type B) dient der Authentisierung und elektronischen Signatur für Organisationen des Gesundheitswesens. Sie ist also nicht auf eine einzelne Person, sondern auf eine ganze Abteilung oder Praxis ausgerichtet.

Das *HSM-B* (Hardware Security Module, Type B) kann die kryptografischen Aufgaben einer SMC-B für große Organisationen des Gesundheitswesens, wie z.B. ganze Krankenhäuser, übernehmen, falls die Performance der einfachen SMC-B nicht ausreicht.

Zugangskontrolle für freie Heilberufe

Ein anderer Blickwinkel richtet sich auf jene Heilberufsgruppen, die nicht in Kammern organisiert sind, aber ebenfalls Zugriff auf die TI des Gesundheitswesens benötigen bzw. darüber angesprochen werden müssen. Für sie wurde ein für Deutschland ganz neues elektronisches Gesundheitsberuferegister (eGBR) gegründet. Es übernimmt die sichere Identifizierung der Antragsstellenden für elektronische Heilberufs- oder Berufsausweise (eHBA/eBA) und überprüft die Berufserlaubnisse in Zusammenarbeit mit den zuständigen Länderbehörden.

Mehr als 30 verschiedene Gruppierungen sind gegenwärtig im eGBR vertreten, darunter der Arbeitgeber- und BerufsVerband Privater Pflege e.V. (ABVP), der Bund freiberuflicher Hebammen Deutschlands e.V. (BfHD), die Bundesinnung der Hörgeräteakustiker (BIHA), der Bundesinnungsverband für Orthopädie-Technik (BIV-OT) und der Bundesverband für Ergotherapeuten in Deutschland e.V. (BED).

Schutz persönlicher Daten

Die Vertrauenswürdigkeit jeder TI hängt in starkem Maße davon ab, wie wirksam und konsequent geplante Sicherheitsmaßnahmen konkret umgesetzt werden. Für das deutsche Gesundheitswesen ist der Sicherstellungsauftrag nach dem Zwei-Schlüssel-Prinzip formuliert und auf der Basis von eGKs und HBAs gewissermaßen in Silizium verankert. Die Technik hat entsprechend robuste Mechanismen für die gegenseitige Authentifizierung umgesetzt.

Das Zwei-Schlüssel-Prinzip zwischen den beiden Karten stellt sicher, dass der Zugriff auf medizinische Daten der eGK immer den gleichzei-

tigen Einsatz der eGK und eines HBA erfordert. Erst wenn die eGK durch eine erfolgreiche Card-to-Card-Authentisierung festgestellt hat, dass sie sich einem gültigen HBA im erhöhten Sicherheitszustand (also nach PIN-Eingabe) gegenübersieht und auch der Versicherte seine PIN eingegeben hat, ist der Zugriff auf die medizinischen Datencontainer oder die Nutzung des geheimen Schlüsselmaterials auf der eGK möglich.

Auf ausdrücklichen Wunsch des Versicherten können über die obligaten Stammdaten hinaus medizinische Informationen freiwillig in den Containern verschlüsselt und PIN-geschützt auf der Karte gespeichert werden. Wegen des begrenzten sicheren Speichers der Karten steht dafür nur ein bestimmter Anteil des Datenvolumens zur Verfügung. Entsprechende Kartenmechanismen (Containermodelle) gibt es schon, doch die Sachdiskussion über konkrete Anwendungen ist noch nicht abgeschlossen. Geplant sind verschiedene Datencontainer, z.B. zur Prüfung der Arzneimitteltherapiesicherheit, ein elektronisches Patientenfach oder eine elektronische Patientenquittung. Bei großen Datenvolumen, etwa für elektronische Patientenakten oder CT-Bilder, wären aber auch indirekte Verweise nach dem Pointer-Schlüssel-Prinzip möglich. In jedem Fall bleibt der Versicherte immer Herr über diese Daten. Er kann sie seinem Arzt zur Verfügung stellen oder eben nicht, sie verstecken oder jederzeit löschen lassen. Implementiert und beweisbar gesichert wird dies immer über das Zwei-Schlüssel-Prinzip.

Sonderfall: Freiwillige Notfallregelungen

Von dieser eisernen Regel gibt es zwei Ausnahmen. Genau genommen handelt es sich um zwei voneinander unabhängige, aber auch vollkommen freiwillige Anwendungen mit einer gleichgelagerten Herausforderung für deren Nutzung: Zum einen geht es um das Erstellen und Pflegen eines Notfalldatensatzes (NFD) und zum anderen um das Anlegen eines Datensatzes Persönliche Erklärungen (DPE).

Der NFD beinhaltet Informationen aus der Vorgeschichte des Patienten, die einem behandelnden Arzt zur Abwendung eines ungünstigen Krankheitsverlaufs möglichst schnell und strukturiert zugänglich sein müssen (z.B. Herzschrittmacherdaten, Informationen zu Nierenersatztherapie oder Allergien usw.). Der NFD ist etwa dann wichtig, wenn ein Patient in die Notaufnahme kommt.

Der DPE ist ein eigenständiger Datensatz unabhängig vom NFD. Er enthält Hinweise auf von Willenserklärungen des Patienten zum Behandlungsverlauf oder zur Organ- und Gewebespende. Dabei sind nicht die persönlichen Erklärungen selbst hinterlegt, sondern nur ein Querverweis auf den Ort, an dem sie aufbewahrt werden.

Bei jenen Versicherten, die diese Anwendungen nutzen möchten, sind beide Datensätze getrennt voneinander auf der eGK abgelegt. Für die Anlage dieser freiwilligen Daten ist eine schriftliche Einwilligung erforderlich. Der Name des Arztes, bei dem die Einwilligung hinterlegt ist, wird in der eGK dokumentiert. Der Versicherte kann seine Einwilligungen jederzeit widerrufen. Durch das Löschen von NFD und/oder DPE wird dann auch die jeweilige Dokumentation der Einwilligung von der eGK entfernt.

Lässt der eGK-Inhaber NFD und/oder DPE als freiwillige Anwendung in seine Karte aufnehmen, gilt für den Zugriff auf diese Datenblöcke ein Sonderfall, da die Mitwirkung des Versicherten im akuten Bedarfsfall ja nicht immer möglich ist. Die beiden Datensätze werden zugriffsgeschützt, jedoch nicht verschlüsselt auf der eGK gespeichert. Wären die Daten verschlüsselt auf der eGK hinterlegt, so würde die Nutzung immer die Eingabe der PIN des Versicherten erfordern. Dies wäre jedoch unvereinbar mit dem Sinn und Zweck der Anwendungen.

Technisch läuft dieser Mechanismus übrigens über das Bit 18 der Flag-Liste im CV-Zertifikat des Heilberufsausweises. Es ist nur bei Ausweisen von Ärzten und deren medizinischen Mitarbeitern sowie bei Rettungsassistenten gesetzt. Die eGK gestattet den Zugriff auf die beiden Anwendungen (und nur auf diese) in Anwesenheit eines HBA mit diesem Flag auch ohne die PIN-Eingabe des Patienten. Die technische Durchsetzung des Zugriffsschutzes erfolgt dabei direkt über das Kartenbetriebssystem der eGK, das den Zugriff erst nach Authentifizierung und Verifizierung des HBA freigibt.

Fazit

Insgesamt ist die Einführung der Vernetzung im deutschen Gesundheitswesen eine Infrastrukturmaßnahme von erheblicher Größe und Komplexität. Allein schon die Eckdaten machen das deutlich: Im Vollausbau ergibt sich durch die Nutzerzahlen von ca. 70 Mio. Versicherten, von über 200.000 Leistungserbringern, von annähernd noch einmal so vielen Institutionen und von einigen weiteren Hunderttausend technischen Komponenten mit einem oder mehreren Zertifikaten eine Verzeichnisinfrastruktur von bisher kaum gekannter Größe. Ungeduld mit der Lösung der nationalen Herausforderungen hieße jedoch ein Kapitulieren vor dieser großen und wichtigen Gesellschaftsaufgabe. Und das hätte Nachteile für jeden von uns – wenn wir einmal selbst gesundheitliche Hilfe in Anspruch nehmen müssen.

Dr. Christoph F-J Goetz
Leiter Gesundheitstelematik
Kassenärztliche Vereinigung Bayerns