Kurzgutachten gemäß der Datenschutzgütesiegelverordnung Schleswig-Holstein für das IT-Produkt „ViViAN, Version 4.0“

im Auftrag der MicroNova AG

datenschutz cert GmbH

30.11.2015

datenschutz cert

Inhaltsverzeichnis

1. Vorbemerkung

Mit diesem Kurzgutachten wird die datenschutzrechtliche Auditierung des IT-Produktes „VIVIAN“ in der Version 4.0 der MicroNova AG im Überblick dokumentiert, mit welcher die Prüfstelle der datenschutz cert GmbH beauftragt wurde.

2. Zeitraum der Prüfung

Die Auditierung erstreckte sich auf den Zeitraum von 02.01.2014 bis 30.11.2015 und beinhaltete eine konzeptionelle Analyse der zur Verfügung gestellten Unterlagen sowie verschiedene Besichtigungen des Testsystems. Darüber hinaus ist der Authentifikationsvorgang praktisch getestet worden.

3. Antragstellerin

Antragstellerin dieses Gutachtens ist die

MicroNova AG
Unterfeldring 17
D-85256 Vierkirchen

als Anbieter und Betreiber des IT-Produktes. Ansprechpartner ist Herr Reindl.

4. Sachverständiger/Prüfstelle

Sachverständige dieses Gutachtens ist die Prüfstelle

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Irene Karper (Recht). Ansprechpartner für diese Auditierung sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

5. Kurzbezeichnung des IT-Produkts

Begutachtet wird das IT-Produkt „VIVIAN“ in der Version 4.0. ViViAN bezeichnet die Virtuelle Vernetzung im Arzt-Netz.

6. Beschreibung des IT-Produkts

ViViAN stellt Daten zur Mit- bzw. Weiterbehandlung z.B. Ärzten, Laboren, Medizintechnikern, Reha-Kliniken oder Physiotherapeuten in einem Gesundheitsnetzwerk zur Verfügung und ermöglicht einen sicheren, schnellen und Hersteller-unabhängigen Datenaustausch der PVS/AIS. Die medizinischen Daten verbleiben dezentral im jeweiligen Ärzte- oder Praxisnetz. Nachfolgend wird der häufigste Anwendungsfall der Vernetzung von Arzt-Praxen beispielhaft dargestellt.

6.1 Wesentliche Funktionen

Der Verbindungsaufbau wird durch den ViViAN-Client initiiert, der auf einem zentralen Rechner (i.d.R. PVS-Server) der Praxis mit Internetanschluss installiert ist.
Installation

Für die Installation ist ein drei-teiliger Authentifizierungsprozess notwendig:

Im ersten Schritt erhält der Anwender einen **Freischaltungsbrief** per Post seitens der MicroNova AG. Dieser Brief enthält die für die Installation notwendigen Identifikationsdaten (Praxis-Name, Betriebsstättennummer - BSNR, Adresse, Telefon, Fax, Object Identifier - OID und Transaktionsnummer - TAN) des Anwenders.

In einem zweiten Schritt wird vom Anwender das **Praxis-Zertifikat** erstellt. Hierfür müssen die Praxis-Daten angegeben werden, welche im Freischaltungsbrief enthalten sind. Für den Start des ViViAN-Clients muss der Anwender sodann ein sicheres Kennwort für die Zertifikate vergeben, welches bei jedem Start abgefragt wird.

In einem dritten Schritt muss vom **Händler** – ein Mitarbeiter der MicroNova AG, der den Anwender bei der Installation begleitet, die Installation mit Hilfe seines Händler-Zertifikats gegenüber dem ViViAN-Server authentisieren und für das Praxis-Zertifikat ein Sign-Request in der ViViAN-PKI stellen. Das Praxis-Zertifikat für den ViViAN-Client wird mit einer Gültigkeit von 36 Monaten ausgestellt. 30 Tage vor Ablauf des Zertifikats erscheint beim Start des ViViAN-Clients ein Hinweis. Mittels der auf dem Freischaltungsbrief vorhandenen TAN kann ein neues Zertifikat ausgestellt werden.

Sollte eine Unterstützung der MicroNova AG erforderlich sein, erfolgt der **Support** mittels Teamviewer. Für diesen Fall muss der Arzt eine Patientenerklärung einholen, die ihn von der Schweigepflicht entbindet. Der Anwender schaltet die Teamviewer-Sitzung frei und kann sie jederzeit beenden. Für die Durchführung der Fernwartung ist es möglich auf Testdaten ohne Personenbezug zurückzugreifen.

Einschreibung und Verwaltung von Patientendaten in ViViAN

Im Rahmen der ersten Einschreibung eines Patienten bei ViViAN als Netzpatient wird ein klar definierter Prozess verwendet, um die notwendigen Informationen zu erfassen. Der Patient wird in ViViAN anhand einer von drei Patienten-IDs identifiziert.

Die **Patienten-IDs** berechnen sich aus Informationen über den Patienten, die in jeder Arzt-Praxis im PVS/AIS verfügbar sind. Zum Schutz dieser Informationen wird mit SHA-256 ein Hash-Wert (Pseudonym) berechnet, so dass am Coordination-Server kein Rückschluss auf die zur Berechnung verwendeten Patientendaten gezogen werden kann. Zur Berechnung der Patienten-IDs können folgende Datensätze in folgender Reihenfolge genutzt werden:

1. die eGK-Nummer (automatisch aus der eGK ausgelesen)
2. die Versicherten-Nummer und das Institutskennzeichen (automatisch aus der Krankenversicherungskarte ausgelesen)
3. Grunddaten des Patienten (Name/Geburtsname, Vorname, Geburtsdatum, Geburtsort)

ViViAN ermittelt immer alle Patienten-IDs, die auf Basis der verfügbaren Daten berechnet werden können, um die Wahrscheinlichkeit der Identifikation zu erhöhen.

Liegt für den Patienten nur die Grunddaten-Patienten-ID vor, ist es möglich, dass bei der Einschreibung Übereinstimmungen im Netz gefunden werden. Dann erfolgt der Hinweis, dass mehrdeutige Grunddaten vorliegen, und es werden weitere Grunddaten passend zum gefundenen Patientennetz aus den anderen

behandelnden Praxen angefordert und angezeigt. Der Anwender vergleicht nun diese Daten und identifiziert den Patienten.

Für die Vernetzung in ViViAN ist eine **Teilnahmeerklärung** des Patienten nötig, die in ViViAN als Notiz hinterlegt wird. Sie enthält eine Information zur Datenverarbeitung und eine Entbindung von der **ärztlichen Schweigepflicht**. Die Aufbewahrung der schriftlichen Erklärung erfolgt in der Praxis; Kopien gehen an das sogenannte „Netzbüro" und an den Patienten. Im Detail unterliegt der Prozess dem Arztnetz und der Prüfung durch dessen Datenschutzbeauftragten.

Für die Verwaltung von Verträgen eines Arztnetzes (z.B. Teilnahmeerklärungen der integrierten Versorgung) ist ein „**Netzbüro**" über einen Eintrag im LDAP-Server eingerichtet. Das Netzbüro ist eine virtuelle Stelle des an ViViAN angeschlossenen Arztnetzes. Es wird analog zu einer Arztpraxis von ViViAN integriert. Das Netzbüro kann keine medizinischen Daten eines Patienten einsehen, es verwaltet aber die Patientenverträge und steuert, zwischen welchen Anwendern Daten ausgetauscht werden dürfen. Es verfügt dazu über einen ViViAN-Client und einen VisioDok-Browser sowie über eine Arztnetz-spezifische Vertrags-Datenbank. Von der MicroNova AG wird hierfür ein SFTP-Server betrieben, über den Vertragsformulare abrufbar sind. Das Netzbüro übernimmt die Praxisausschreibung, Netzkündigung, Vertragsausschreibung, Vertragseinschreibung, Deaktivierung und Aktivierung. Die bezüglich des Netzbüros verantwortliche Stelle im Sinne des BDSG ist abhängig von der Unterbringung dieser virtuellen Einheit innerhalb der Organisation des Arztnetzwerkes: Dies kann ein Arzt in einer Praxis sein oder eine eigene Verwaltungseinheit einer größeren Stelle (z.B. Krankenhaus). Nach der Organisation des jeweiligen Arztnetzwerkes richtet sich dann das Hosting des Netzbüros, dessen Kommunikation von einem Client aus mit dem Netzwerk erfolgt.

Patientenstammdaten können nicht direkt manuell in ViViAN angelegt werden. Dadurch sollen Fehlerquellen vermieden werden. Patientenstammdaten werden vielmehr automatisiert aus dem AIS/PVS übernommen. ViViAN verfügt zudem über die Möglichkeit, Daten der Versichertenkarte einzulesen. Die Patientenstammdaten werden in der ViViAN-Patientenkarteikarte hinterlegt und können in VisioDok korrigiert werden. Sofern Unterschiede zu ggf. zuvor in ViViAN erfassten Daten bestehen, werden diese zum Abgleich rot hervorgehoben und können überprüft und ergänzt, berichtigt oder gelöscht werden.

Über ein Symbol im VisoDok-Browser wird angezeigt, ob ein Patient im Ärztenetz eingeschrieben ist (grün) oder nicht (rot) und welche Versorgungsverträge für diesen Patienten gelten.

Ferner ist ein Freitextfeld für vernetzungsrelevante Kommentare vorgesehen. Tooltipps beim Mouse-Over weisen darauf hin, das Feld datensparsam zu nutzen.

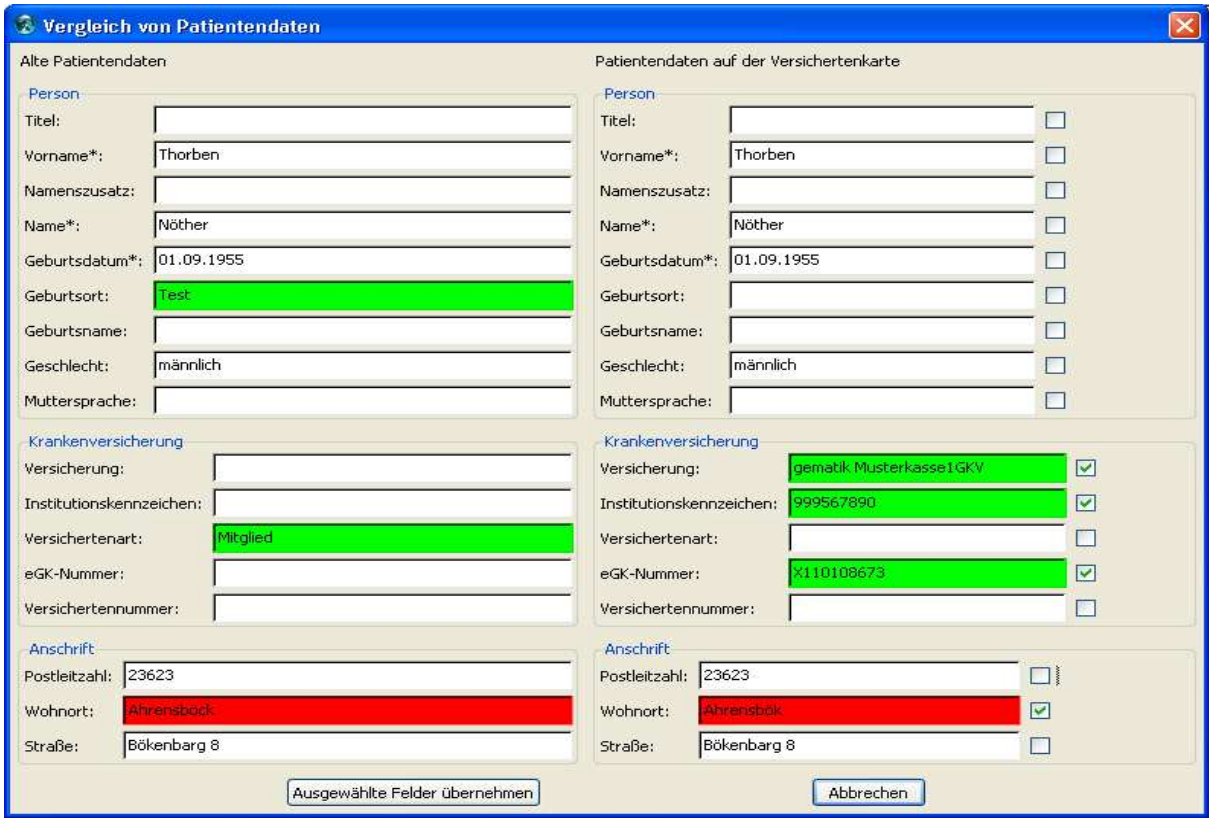

Abbildung 1 Vergleich der Patientenkarte bei Einlesen der Versicherungskarte

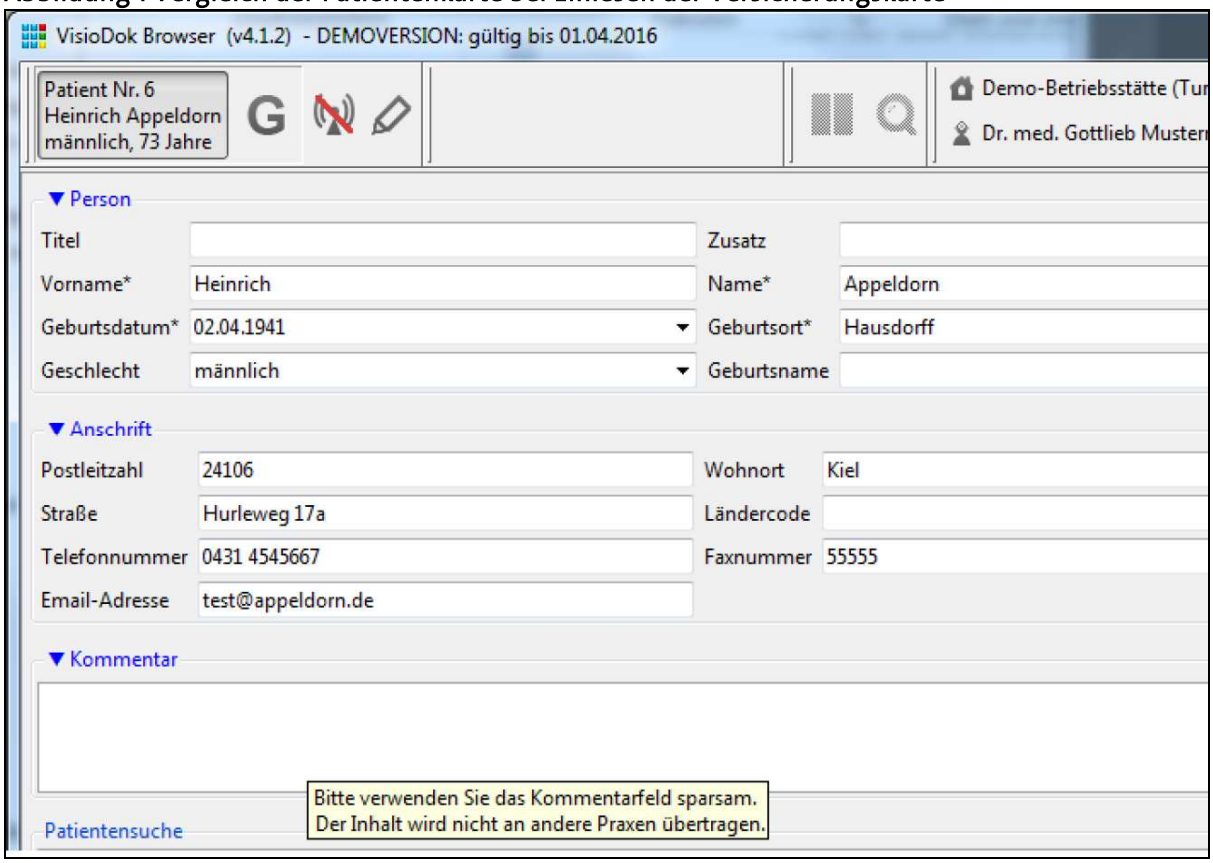

Abbildung 2 Patientendaten mit Tooltipp zur datensparsamen Nutzung

Kündigung der Teilnahme oder Ausschreibung einer Praxis

Der Patient kann die Teilnahme an der Vernetzung bei der Praxis oder im Netzbüro kündigen. Die Praxis/das Netzbüro schickt den Auftrag zur Sperrung des Patientennetzes (identifiziert durch die Patienten-ID) und des Vertrags an den Coordination-Server. Dieser markiert das gesamte Patientennetz als ausgeschrieben. Möchte der Patient nur die Behandlung durch eine bestimmte Praxis ausschließen, ist der Ausschreibungsvorgang derselbe. Aufgrund der gesetzlichen Aufbewahrungsfristen für Patientendaten wird der Datensatz nach Fristablauf gelöscht und mit Kündigung/Ausschreibung zunächst gesperrt, so dass keine Datenübermittlungen mehr stattfinden können. Andere Ärzte, welche eine ausgeschriebene Praxis in die Kommunikation zu den Patientendaten einbeziehen wollen, erhalten einen Hinweis, dass dies aufgrund der Ausschreibung nicht mehr möglich ist.

Versand von Patientendaten

Nachrichten zu einem Patienten (z.B. empfangene Befunde) können über einen Posteingang mittels ViViAN abgerufen werden. Dateien wie Röntgenbilder, Arztbriefe, etc. werden nicht direkt mit den Patientendaten verschickt, sondern nur ein Verweis auf die Datei, der den Speicherort und einen Kommentar des Absenders zur Datei enthält. Optional kann der Arzt auch einen Datum definieren, nach dem die Datei nicht mehr abgerufen werden kann. Der Empfänger fordert den Versand der Datei an, wenn er an der Datei interessiert ist. Damit wird die versendete Datenmenge auf ein Minimum reduziert. Der Versand und die Anzeige von Dateien mit den Erweiterungen bat, cmd, com, exe, msi, pif, reg, scr, vbs wird blockiert.

Werden für einen Patienten neue **Karteikarteneinträge** erfasst, erfolgt eine Übernahme dieser Einträge in die Netzakte von VisioDok. Bei den Karteikarteneinträgen handelt es sich um einzelne Zeilen des Krankenblatts. Diese werden entweder aus dem PVS geladen oder in der Vernetzungssoftware erstellt. Die Karteieinträge können Befunde oder Arztbriefe enthalten. Diese Übernahme kann automatisch oder manuell erfolgen. Ist der Patient in dieser Praxis nicht eingeschrieben, erhalten die übernommenen Einträge den Status „nicht versenden“.

Bei einem eingeschriebenen Patienten werden Versandregeln angewendet, die den Status der Einträge definieren. Es sind folgende Stati möglich: versenden nicht möglich, nicht versenden, verzögert versenden, sofort versenden. Nach erfolgter Übernahme kann der Status manuell angepasst werden. Es sind folgende Änderungen möglich:

--- verzögert versenden -> sofort versenden

--- verzögert versenden -> nicht versenden

--- nicht versenden -> sofort versenden

Ist die Übernahme der Karteikarteneinträge in VisioDok automatisch erfolgt, werden auch die Einträge verzögert verschickt, die durch eine Regel zum sofortigen Versand vorgesehen wären. Die Verzögerungszeit ist konfigurierbar, beträgt aber mindestens 30 Minuten. Der Versand von Patientendaten über ViViAN kann so konfiguriert werden, dass er zeitlich verzögert erfolgt. Bei der zeitlichen Verzögerung wird ein Default-Wert von 60 Minuten verwendet. Im Rahmen der Installation wird dieser Punkt mit der Praxis durchgesprochen und den Wünschen der Praxis für die

Verzögerungszeit entsprochen. Es ist nicht möglich, ein Zeitintervall kleiner als 30 Minuten anzugeben. Durch die Verzögerung zwischen Freigabe eines Datensatzes und dem tatsächlichen Versenden ist es möglich, versehentliche Freigaben rechtzeitig zu stoppen. Die Adressaten sind immer alle Praxen im Patientennetz (außer dem Sender selbst). Die Definition der Filter geschieht in jeder Praxis einzeln, um auf fachgruppenspezifische Regelungen (z.B. Sonderbehandlung von psychologischen Praxen) eingehen zu können. Alle versendeten Einträge werden mit einer Ende-zu-Ende-Verschlüsselung geschützt. Zudem werden die Einträge mit einer elektronischen Signatur des Senders gegen Manipulation geschützt.

Werden einer Praxis Karteieinträge zugeschickt, so wird die Echtheit der Daten anhand der Signatur des Senders überprüft und der Empfang der versendenden Praxis bestätigt. Die neuen Karteieinträge werden automatisch in die Karteikarte von ViViAN übernommen. Dadurch wird sichergestellt, dass der Arzt während der Behandlung alle verfügbaren Daten sieht. Neu eingegangene Einträge werden als ungelesen markiert und erscheinen infolgedessen in der Posteingangsansicht. Hier kann der Arzt auswählen, welche der Einträge ins PVS übertragen werden sollen. Diese erscheinen infolgedessen nicht mehr im Posteingang. Der Arzt kann Einträge als gelesen markieren, die nicht ins PVS übertragen werden sollen. Diese Einträge erscheinen infolgedessen nicht mehr im Posteingang, verbleiben aber trotzdem in der Karteikarte von ViViAN.

Änderung von Patientendaten

Eine Änderung von Patientendaten zieht eine Änderung der Patienten-ID nach sich. Die neue Patienten-ID muss im System als äquivalent zur alten Patienten-ID bekannt gemacht werden:

1. Der Patient teilt der Praxis die Änderung der Patientendaten mit (ggf. werden neue Patientendaten automatisch beim Auslesen der eGK oder der KVK oder durch Kommunikation mit dem PVS erkannt).
2. Die Praxis trägt die neuen Patientendaten in die Vernetzungssoftware ein und bestätigt die Änderung.
3. Die Vernetzungssoftware berechnet die neue Patienten-ID (die neue Basis-ID mit der alten Einschreibungs-ID) und schickt diese mit der alten Patienten-ID an den Server.
4. Der Server markiert die alte und die neue Patienten-ID als äquivalent.

Löschung von Patientendaten

Sämtliche Patientendaten in der lokalen Datenbank können händisch gelöscht werden, sofern sie die Mindestaufbewahrungsdauer von 10 Jahren überschritten haben. Der Arzt ist für die Einhaltung von erweiterten Aufbewahrungsfristen verantwortlich. Werden alle Karteikarteneinträge eines Patienten gelöscht, können auch die Grunddaten des Patienten gelöscht werden. Mit dem Button „Weitere Funktionen“ öffnet sich ein Menü, in dem der Anwender „Patientendaten löschen“ kann. Nach der Auswahl von „Patientendaten löschen“ öffnet sich ein neuer Dialog, in dem das Löschen der Daten des aktuellen Patienten parametrisiert werden kann.

Ein Arzt kann auf Wunsch des Patienten bei der MicroNova AG beantragen, dass Pseudonyme gelöscht werden. Ein entsprechendes Formular ist im Anhang der Bedienungsanleitung enthalten. Durch eine Arbeitsanweisung ist bei der MicroNova AG festgelegt, wie bei Eingang eines solchen Antrags vorzugehen ist. Die eigentliche Löschung wird durch ein Script am PKI-Server durchgeführt.

6.2 Komponenten und Schnittstellen

Für die Vernetzung durch ViViAN werden zentrale und dezentrale Komponenten benötigt, welche die Authentizität des Senders und Empfängers sowie die Integrität und Vertraulichkeit der übermittelten Daten sicherstellen. Zu diesem Zweck stellt ViViAN eine Public Key Infrastucture (PKI) bereit. Dafür werden zwei zentrale Komponenten eingesetzt: Ein **CA-Server** zur Ausstellung der Zertifikate und ein **Coordination-Server** zur Verwaltung der Zertifikate und Koordination der Kommunikation. Beide Komponenten werden auch als **ViViAN-Server** bezeichnet.

Als dezentrale Komponente wird beim Anwender ein **ViViAN-Client** installiert, in der Regel auf dem Praxis-Server. Der ViViAN-Client initiiert die Verbindung über das Internet zu den anderen Komponenten des Netzwerkes von ViViAN.

Der **VisioDok-Browser** dient als Benutzeroberfläche für ViViAN. VisioDok ist zugleich ein Dokumentationsverfahren zur Verwaltung von Patientendaten, welches ebenfalls von der MicroNova AG angeboten wird. VisioDok ist nicht Auditgegenstand. Für ViViAN wird lediglich die Benutzeroberfläche von VisioDok genutzt, auch dann, wenn ein anderes Dokumentationssystem genutzt wird. Der VisioDok-Browser ist auf dem Rechner beim Anwender installiert. Hierüber werden Postein- und -ausgang zur Verfügung gestellt, über welche der Daten-Import des PVS/AIS abgewickelt wird. Zudem findet hierüber die Benutzerverwaltung statt.

ViViAN greift über die **Schnittstelle DSSQLAB** auf die Daten des PVS/AIS zu und liest die für den Import freigegebenen Informationen aus. Dabei werden Sender und Empfänger identifiziert und autorisiert. Ferner wird geprüft, ob der Patient Mitglied des Netzwerkes ist und welcher Status oder welche Beschränkungen für den Datensatz vorliegen. Der Anwender kann freigegebene Datensätze anderer vernetzter Anwender aufrufen oder diese für die Vernetzung freigeben.

Der ViViAN-Client baut eine Verbindung zum **Coordination-Server** (LDAP und XMPP) auf. Diese Verbindung wird per TLS abgesichert. Der Server befindet sich **ab 2016** im Rechenzentrum der noris network AG. Er ist ein Linux-Server mit dem Betriebssystem (Cent OS) und stellt die Dienste XMPP über eJabberd und LDAP über OpenLDAP sowie den Socks5-Proxy bereit. Ebenfalls ist hier der PKI-Client zur Erstellung der Praxis-Zertifikate installiert, welcher über XMPP mit Praxen kommuniziert. Hierüber werden die aktuell gültigen Zertifikate der PKI verwaltet. Die Prozesse des LDAP- und XMPP-Servers sowie des PKI-Clients werden durch die **SW ManageEngine** überwacht. Das Monitoring wird im Rahmen des Supports durch die MicroNova AG durchgeführt.

Die Zertifikate für Praxen und Netzteilnehmer werden über den **CA-Server** ausgestellt, welcher im Rechenzentrum der MicroNova AG untergebracht ist. Der CA-Server ist ein Linux-Server. Er erstellt regelmäßig Backups des Coordination Servers. Ferner erledigt er Verwaltungsaufgaben, wie etwa das Einrichten von Anwendern.

6.3 Verschlüsselungsmechanismen

Die Vertraulichkeit der versendeten Daten und Authentizität von Sender und Empfänger basieren auf der PKI. Diese ist wie folgt aufgebaut. Es gibt eine **Root-CA** und drei mit dem Schlüssel der Root-CA signierte Sub-CAs:

- **Server-CA**. Die ServerCA stellt die Zertifikate für die Server-Dienste XMPP und LDAP aus, um die Kommunikation via TLS zu verschlüsseln.
- **Site-CA**. Die SiteCA stellt die Zertifikate für die Praxen aus, mit denen die Verschlüsselung der Patientendaten zwischen den Praxen erfolgt.
- **Dist-CA**. Die DistCA stellt die Zertifikate für Mitarbeiter von MicroNova aus, die Software ViViAN in den Arztpraxen einrichten.

Die PKI erstellt/signiert X.509-Zertifikate basierend auf RSA-2048 und dem Hashverfahren SHA-256. Die Zertifikate werden mit einer Gültigkeit von 5 Jahren ausgestellt – CA-Zertifikate haben eine Gültigkeit von 20 Jahren. Die gesamte Zertifikatskette wird beim Verbindungsaufbau mit dem LDAP-Server überprüft. Diese Verbindung ist auch Voraussetzung für einen erfolgreichen Verbindungsaufbau mit dem XMPP-Server. Am LDAP-Server wird eine Revokation-Lists für die Site-CA hinterlegt, welche Logins von nicht freigegebenen Praxen sperrt. Es gibt keine clientseitige CRL. Stattdessen werden die gesperrten Zertifikate vom Server gelöscht und können nicht mehr zur Verschlüsselung von Daten verwendet werden. Praxen erhalten ein von der Site-CA ausgestelltes Zertifikat. Die Schlüssel werden zum einen verwendet, um übertragene Daten zu signieren (Integrität und Authentizität des Senders) und zum anderen, um dem Empfänger den symmetrischen Schüssel für die eigentliche Datenübertragung (mit dem öffentlichen Schlüssel verschlüsselt) zuzusenden. Für die Übertragung von Patientendaten kommen Transport- und Datenverschlüsselungen mit angemessen sicheren Mechanismen zum Einsatz.

6.4 Sicherheit der Einsatzumgebung

Es kann vorausgesetzt werden, dass die Einsatzumgebung von ViViAN beim Anwender den gleichen Schutzmechanismen unterliegt, wie sie für das AIS bzw. PVS gelten. Die Sicherheit dieser Umgebung hängt damit von den jeweiligen Anforderungen ab, die der Anwender an seine eigene IT-Landschaft stellt und umsetzt. Diese kann im Rahmen der Auditierung nicht konkretisiert werden. Die MicroNova AG hält allerdings zahlreiche Hinweise und Mindestanforderungen an die IT-sicherheit bei der Nutzung von ViViAN als Sensibilisierung bereit, die den Anwender bei der Umsetzung eines datensicheren und datenschutzkonformen Umgangs mit ViViAN unterstützen.

Die Sicherheit der Einsatzumgebung von Komponenten im Rechenzentrum der **MicroNova AG** wird als angemessen bewertet. Die MicroNova AG ist Entwickler, Hersteller und Vertreiber von ViViAN. Die MicroNova AG stellt auch die Rolle des Händlers, welcher den Anwender bei der Erstellung des Praxis-Zertifikats unterstützt und der zudem den Anwender und sein Personal im Umgang mit ViViAN schult. Zudem bietet sie Firewalladministration, Support-, Monitoring- und Backup-Dienstleistungen in Bezug auf ViViAN an und wird daher als Auftragsdatenverarbeiter gemäß § 11 BDSG tätig. Für Kunden hält die MicroNova AG das Muster „*Vertrag zur Auftragsdatenverarbeitung gemäß § 11 BDSG*“ zur

Verfügung. Am Sitz in Vierkirchen, wo sich das für ViViAN relevante Rechenzentrum befindet, ist das Unternehmen gemäß ISO 9001:2008 durch die TüV Süd Management Service GmbH zertifiziert. Die Umsetzung der technisch-organisatorischen Maßnahmen im Rechenzentrum der MicroNova AG wurden zudem durch einen unabhängigen Sachverständigen geprüft und bestätigt.

Die noris network AG ist als Subunternehmer i.S.d. § 11 BDSG der MicroNova AG tätig für das Hosting der Server-Systeme und dort betriebenen Anwendungen, für die Administration und Support der Server-Systeme, das Monitoring und für die Betreuung der von der MicroNova AG betriebenen Firewall. Zwischen der MicroNova AG und der noris network AG wurde ein „*Auftrag gemäß § 11 BDSG*" abgeschlossen. Zudem verfügt das relevante Rechenzentrum u.a. über Zertifizierungen gemäß ISO/IEC 27001:2005 für den Geltungsbereich „*Lösungen, Produkte und Services in den Bereichen IT-Outsourcing, Cloud Services, Managed Services, Network & Security sowie Rechenzentrumsinfrastrukturen und –betrieb*", ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz auf und ein Zertifikat für das Service-Managementsystem für den Geltungsbereich „*Outsourcing Services, Cloud Services, Managed Services, Network & Security Services, Bereitstellung und Services von Rechenzentren und deren Infrastruktur sowie Betriebsdienstleistungen*" gemäß ISO/IEC 20000-1:2011. Die Umsetzung angemessener technischer und organisatorischer Sicherheitsmaßnahmen der Einsatzumgebung bei der noris network AG wurden demnach umfassend durch unabhängige Sachverständige geprüft und von anerkannten Zertifizierungsstellen bestätigt.

6.5 Datenarten

Folgende **Primärdaten** werden verarbeitet:

Daten des Anwenders:

Name (z.B. Praxisname, Arztname)	Betriebsstättennummer (BSNR)
Anschrift	Lebenslange Arztnummer
Telefon	Fachrichtung (z.B. Hausarzt)
Fax	Kennwort

Bei den Anwenderdaten handelt es sich um geschäftliche Daten, die – soweit sie Rückschlüsse auf eine natürliche Person zulassen – auch dem Schutz des BDSG unterfallen. Zweck der Datenverarbeitung ist die eindeutige Zuordnung der Arzt-Praxis im Ärzte Netz sowie die schnelle Anrufbarkeit der Kontaktdaten für die Kontaktaufnahme im Rahmen einer Behandlung.

Patientendaten (besondere personenbezogene Daten):

Titel	Postanschrift
Vor- und Nachname	Postleitzahl
Namenszusatz	Ort
Geburtsdatum	Straße
Geschlecht	Ländercode
Geburtsort	Krankenversicherungsdaten
Geburtsname	Versicherung
Muttersprache	Institutionskennzeichen (IKZ)

Versichertenart (Mitglied)	Patientenstatus (eingeschrieben o. nicht)
Versicherungsnummer	Datum der Einschreibung/Ausschreibung
Elektronische Gesundheitskarten-Nummer (eGK-Nr.)	Verträge des Patienten inkl. Vertragsnummern
Status	Netz des Patienten (= Informationen zu den Praxen des Patientennetzes). Es handelt sich um: Praxisname, Betriebsstättennummer, Anschrift, Telefon- u. Faxnummer
Einlesedatum	Betreuungspraxis: Dies ist i.d.R. der Hausarzt, der den Patienten eingeschrieben hat und Arztbesuche koordiniert. Es ist der Hauptansprechpartner für die Vernetzung.
Gültigkeitsdatum	Betreuungsart
Patienten-OID (= ViViAN-ID): Dies ist ein eindeutiger Schlüssel der einem Patienten (= einer Netzakte) als Identifikationsmerkmal zugewiesen wird.	Patientendokumentation in Form von Karteieinträgen.
AIS/PVS-ID	

Ferner enthält ViViAN Freitextfelder für vernetzungsrelevante Kommentare. Bei der Kommentierung wird der Anwender auf den datensparsamen Umgang sensibilisiert. Sodann können mittels ViViAN auch Dateianhänge mitgeliefert werden, z.B. Dokumente oder Bilddaten mit medizinischen Befunden, Diagnosen.

Zweck der Datenverarbeitung aller genannten Daten ist die Behandlung des Patienten, für die neben den medizinischen Informationen auch die Kontaktdaten sowie Krankenversicherungsdaten vorliegen müssen. Neben dem Namen und der Postanschrift dienen die Angaben über den Geburtsort der eindeutigen Zuordnung des Patienten bei Namensgleichheiten. Die Angabe der Muttersprache dient der Unterstützung der Behandlung bei Patienten, die der deutschen Sprache nicht oder nicht ausreichend mächtig sind.

Als **Sekundärdaten** fallen Logdaten auf den Servern und im ViViAN Client an.

6.6 Komponenten und Schnittstellen

Folgende Komponenten sind Bestandteile und damit Zertifizierungsgegenstand:

- --- ViViAN-Client
- --- VisioDok-Browser (nicht aber das Dokumentationssystem VisioDok)
- --- Coordination-Server
- --- CA-Server
- --- SW ManageEngine
- --- sftp-Server (für Vertragsformulare den Netzbüros).

Nicht auditiert werden folgende Komponenten:

- --- Das PVS/AIS der Anwender

--- Die Vertrags-Datenbanken des Netzbüros; sie ist optionaler Teil des IT-Produktes. Der Betrieb von ViViAN ist auch ohne diese Datenbank möglich.

--- die Einsatzumgebung beim Anwender inklusive eingesetzter Tablets, Apps oder Smartphones. ViViAN ist nicht als „App“ verfügbar.

--- Die Verfahren VisioDok, VisioContract und VisioPush

--- sonstige Dienstleistungen oder IT-Produkte der MicroNova AG.

Der ToE enthält folgende Schnittstelle:

--- DSSQLAB für den Zugriff auf die Daten des PVS/AIS

--- sftp zum Datenbank-Server für die Vertragsformulare

--- TLS für die Kommunikation innerhalb des ViViAN-Netzes

--- ssh für die Administration des Coordination-Servers durch die MicroNova AG.

6.7 Datenschutzrechtliche Vorgaben

Der rechtliche Rahmen zur Entwicklung eines Anforderungsprofils gemäß der Datenschutzgütesiegelverordnung Schleswig-Holstein besteht in dem Landesdatenschutzgesetz Schleswig-Holstein, der Datenschutzverordnung, dem Bundesdatenschutzgesetz sowie den bereichsspezifischen Bestimmungen des Gesundheitswesens. Die Auslegung dieser Rechtsnormen wird konkretisiert durch Rechtsprechung und durch Mitteilungen der Datenschutzaufsichtsbehörden.

Die Pflicht zum ordnungsgemäßen Umgang mit Patientendaten ergibt sich für den Arzt aus einer Vielzahl von bereichsspezifischen Rechtsvorschriften. Dies folgt aus § 10 der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) bzw. den nahezu gleichlautenden landesgesetzlichen Ausprägungen der Berufsordnungen. Wesentlich ist die ärztliche Schweigepflicht. Sie gilt gemäß § 203 StGB in Verbindung mit § 9 MBO-Ä für das gesamte Behandlungsverhältnis, folglich auch gegenüber Dritten außerhalb des Arzt-Patienten-Verhältnisses (z.B. bei Offenbarung von Patientendaten an Ärzte, die nicht an der Behandlung teilhaben).

Eine Ausnahme gilt für Ärzte, die in Gemeinschaftspraxen zusammengeschlossen sind: Da der Patient in diesem Fall den Behandlungsvertrag nicht nur mit seinem behandelnden Arzt schließt, sondern mit der Ärztegemeinschaft, dürfen sich diese untereinander über den Patienten austauschen. Da bei dieser Art des Behandlungsvertrages im Falle der Verhinderung des behandelnden Arztes eine gegenseitige Vertretung vorgesehen ist, ist ein solcher Informationsaustausch zum Wohle des Patienten zwingend erforderlich. Hieraus ergibt sich die Befugnis, auf den Datenbestand in der Gemeinschaftspraxis zuzugreifen, ohne dass damit die ärztliche Schweigepflicht verletzt würde. Gleiches gilt für Stationen in Krankenhäusern, da auch hier die gemeinsame Behandlung von Patienten die Regel ist.

In Praxisgemeinschaften dagegen ist der Austausch von Informationen über Patienten in der Regel nicht zulässig. Praxisgemeinschaften sind lediglich ein wirtschaftlich geprägter Zusammenschluss von Ärzten, der im Wesentlichen dazu dient, gemeinsame Praxisflächen und ggf. weiteres Anlagevermögen gemein-

schaftlich zu nutzen. Den Behandlungsvertrag schließt der Patient in diesem Fall nur mit „seinem“ Arzt, eine Vertretung ist nicht vorgesehen. Aus diesem Grund ist die ärztliche Schweigepflicht zu beachten, sofern nicht Ärzte eine Behandlung ausnahmsweise gemeinschaftlich durchführen oder der Patient sie von der Schweigepflicht entbunden hat. Ebenfalls nicht in den Behandlungsvertrag eingebunden sind sonstige dritte Stellen, welche die technischen Grundlagen für eine Verarbeitung von Patientendaten für den behandelnden Arzt herstellen, wie z.B. ein externes Rechenzentrum.

Besteht auch nur die Möglichkeit, dass diese dritten Stellen unbefugt Einsicht in die Patientendaten nehmen könnten (beispielsweise durch Auslesen des zur Codierung verwendeten Schlüssels oder durch direkten Zugriff auf die Datenbank), ist - mangels einer gesetzlichen Rechtsgrundlage – grundsätzlich eine Einwilligungserklärung des Betroffenen bzw. eine Schweigepflichtentbindungserklärung in Bezug auf diese konkrete Offenbarung des Patienten erforderlich. Im Zuge der Datenverarbeitung mittels ViViAN, darf das Patientengeheimnis daher weder innerhalb von Praxisgemeinschaften, noch gegenüber externen Personen rechtswidrig offenbart werden, sofern diese Rolle nicht zugleich einem behandelnden Arzt zuzuordnen ist oder sofern keine Entbindung von der Schweigepflicht vorliegt. Die Möglichkeit einer Offenbarung von Patientendaten ist bei folgenden ViViAN-Rollen gegeben:

--- Bei dem für die Erstellung des Praxis-Zertifikates eingesetzten Händler der MicroNova AG

--- Bei dem ggf. über Teamviewer zugeschaltete Support der MicroNova AG

--- Bei Personen des Netzbüros, soweit diese nicht zugleich behandelnde Ärzte sind. Diese können zwar keine medizinischen Patientendaten einsehen aber die Verträge, aus denen sich i.d.R. eine spezifische Erkrankung ergibt.

Um eine rechtswidrige Offenbarung zu verhindern, kommt es daher auf die Rechtsgrundlage des individuellen Behandlungsvertrages zwischen Patient und Arzt in Verbindung mit einer schriftlichen Patientenerklärung an, in welcher der Patient nach vorheriger Aufklärung über die Datenverarbeitungszwecke in die Datenverarbeitung widerruflich einwilligt und den Arzt von seiner Schweigepflicht entbindet. Ein Muster dieser Patientenerklärung ist als Anhang zum Mustervertrag zur Auftragsdatenverarbeitung der MicroNova AG definiert und wird jedem Anwender von ViViAN mit Vertragsschluss ausgehändigt.

Keine Offenbarung liegt vor, wenn Datensätze in pseudonymisierter Form übermittelt und bei dritten Stellen (zwischen)gespeichert werden, sofern die Referenztabelle zur Entpseudonymisierung ausschließlich beim behandelnden Arzt verbleibt[1]. Auch darf die externe Stelle nicht mit dem bei ihr vorhandenen oder beschaffbaren Zusatzwissen eine Zuordnung der Pseudonyme zu Patienten vornehmen können. Verbleibt hingegen eine theoretische Möglichkeit, dass unverschlüsselte Daten unbefugten Dritten zur Einsicht gelangen könnten, kann die Offenbarung allenfalls durch technische, organisatorische und gut dokumentierte Maßnahmen abgeschwächt werden. Für das IT-Produkt ViViAN bedeutet dies, dass

[1] Vgl. ULD „Patientendatenverarbeitung im Auftrag“, abrufbar unter https://www.datenschutzzentrum.de/material/themen/gesund/patdvia.htm .

neben der Patientenerklärung auch Maßnahmen zur Authentizität und Vertraulichkeit der Daten besondere Bedeutung haben, welche hier durch die angewandten Verschlüsselungsmechanismen angemessen umgesetzt sind.

ViViAN kommt im ärztlichen Informationssystem zur Anwendung. Dabei könnte es Teil bzw. Subsystem eines Krankenhausinformationssystems (KIS) sein. Demnach sind die Auslegungshilfen der „*Orientierungshilfe Krankenhausinformations-systeme*“ (OH-KIS) der Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[2] anwendbar. Für ViViAN wurden im Rahmen des Audits die Hersteller-seitigen Vorgaben der OH-KIS betrachtet. Da es lediglich ein Subsystem eines KIS darstellen kann, sind die obligatorischen Regelungen der OH-KIS zudem nur dann als anwendbar, soweit sich diese nicht auf die reine elektronische Patientenakte beziehen. Im Ergebnis werden alle Anforderungen der OH-KIS von ViViAN erfüllt.

Hervorzuheben ist, dass im Rahmen dieses Audits nicht untersucht wurde, ob ViViAN konform zum Medizinproduktegesetz aufgestellt ist.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Folgende Tools wurden für die Entwicklung eingesetzt:

Quellcode-Verwaltung: Subversion	Scripts: Bash, Python, TCL
Java-IDE: Eclipse	Datenbank: SQLite
Build-/Testumgebung: Jenkins	Installation: InstallAnywhere
Java-Compiler: JDK7	Festplattenverschlüsselung TrueCrypt

Folgende Tools werden für den Betrieb eingesetzt:

Smack 3.2.2	SQLite3 3.5.9	XPhoto 1.36
Apache Log4J 1.2.16	tclDES 1.0.0	ICD-10-GM 2013
Unboundid LDAP SDK 2.3.1	Tcllib 1.1	OpenLDAP 2.4
Apache XMLRPC 3.1.3	Tcl SOAP 1.6.7	eJabberD 2.1.11
Apache commons-net 3.2	TclXML 3.2	CentOS 6.7
Freewrap 8.5.10	tkImg 1.4.0.4	OpenSSL 1.0
InnoSetup 5.4.3	Tktable 2.10	TrueCrypt 7.1a
Ffidl 0.6	Trf 2.1.4	
html_library 0.3	Twapi 3.1.17	

8. Zweck und Einsatzbereich

ViViAN ist eine Software zur Vernetzung, mit der Leistungserbringer im Gesundheitswesen Behandlungsdaten austauschen. Es wird eingesetzt, um Daten zur Mit- bzw. Weiterbehandlung den medizinischen Akteuren zur Verfügung zu stellen. ViViAN kann u.a. von Kliniken in öffentlicher Trägerschaft eingesetzt werden und ist daher auditierbar nach DSGSVO.

[2] Z.B. abrufbar unter http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=13016&article_id=95681&_psmand=48..

9. Modellierung des Datenflusses

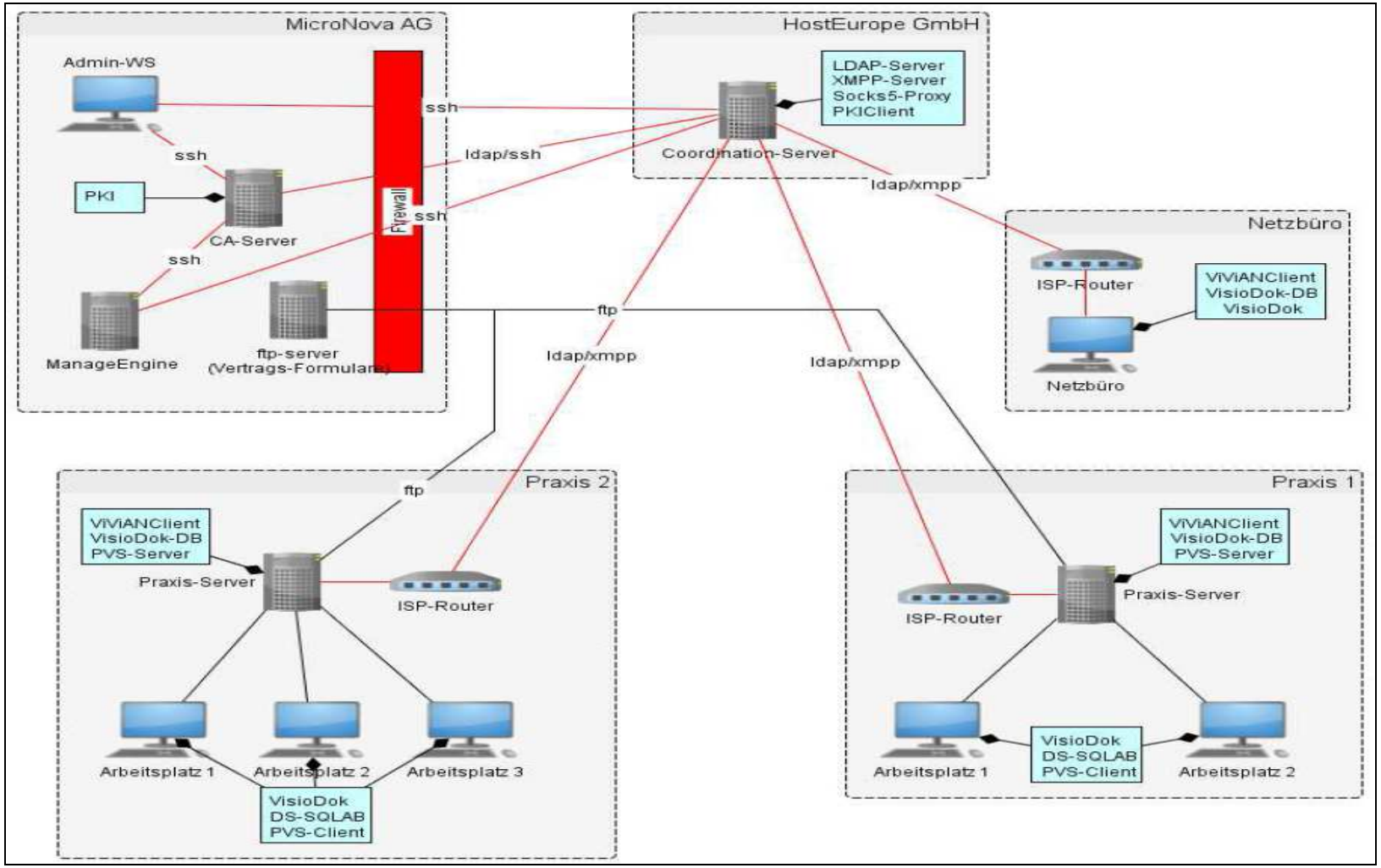

Abbildung 3 Datenfluss (rote Linien = verschlüsselte Kommunikation, „Host Europe GmbH“ ist 2016 durch Noris Network zu ersetzen

10. Version des Anforderungskatalogs als Prüfungsgrundlage

Version 2.

11. Zusammenfassung der Prüfergebnisse

Die Prüfergebnisse im Einzelnen werden wie folgt zusammengefasst:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart A (Primärdaten):		
A1	Verfügbarkeit, Integrität, Vertraulichkeit	Angemessen umgesetzt
A2	Nicht-Verkettbarkeit	Angemessen umgesetzt
A3	Transparenz	Angemessen umgesetzt
A4	Intervenierbarkeit	Angemessen umgesetzt
A5	Anpassung des IT-Produkts	Vorbildlich umgesetzt
A6	Privacy by Default	Angemessen umgesetzt
A7	Sonstige Anforderungen	Angemessen umgesetzt
A8	Zulässigkeit der Datenverarbeitung	Angemessen umgesetzt
A9	Einhaltung allg. Datenschutzgrundsätze	Angemessen umgesetzt
A10	Datenverarbeitung im Auftrag	Angemessen umgesetzt
A11	Besondere technische Verfahren	Nicht anwendbar
A12	Sonstige Anforderungen	Angemessen umgesetzt
A13	Einzelne technisch-organisatorische Maßnahmen	Vorbildlich umgesetzt
A14	Allgemeine Pflichten	Angemessen umgesetzt
A15	Spezifische Pflichten	Angemessen umgesetzt
A16	Pflichten nach DSVO	Angemessen umgesetzt
A17	Betrieb der Auftragsdatenverarbeitung	Angemessen umgesetzt
A18	Sonstige Anforderungen	Nicht anwendbar
A19	Aufklärung und Benachrichtigung	Angemessen umgesetzt
A20	Benachrichtigung bei unrechtmäßiger Kenntniserlangung	Angemessen umgesetzt
A21	Auskunft	Angemessen umgesetzt
A22	Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	Angemessen umgesetzt
A23	Sonstige Anforderungen	Angemessen umgesetzt

Datenart B (Sekundärdaten):		
B1	Datenvermeidung und Datensparsamkeit	Angemessen umgesetzt
B2	Zweckbindung	Angemessen umgesetzt
B3	Nicht-Verkettbarkeit	Angemessen umgesetzt
B4	Transparenz	Angemessen umgesetzt
B5	Rechtsgrundlagen	Angemessen umgesetzt
B6	Zweckbindung	Angemessen umgesetzt
B7	Aufbewahrungsfristen	Angemessen umgesetzt
B8	Physikalische Sicherung	Angemessen umgesetzt
B9	Zugriffsschutz	Angemessen umgesetzt
B10	Ermittlung / Sichtbarkeit der Protokolldaten	Angemessen umgesetzt
B11	Technische Umsetzung der Speicherfristen	Angemessen umgesetzt
B12	Unzulässige Verkettung	Angemessen umgesetzt
B13	Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	Angemessen umgesetzt
B14	Selektive Löschung von Einzeldaten, Beauskunftung, Berichtigung, Sperrung, Einwand	Angemessen umgesetzt
Förderung des Datenschutzes:		
Das IT-Produkt fördert den Datenschutz insgesamt auf angemessene Weise		

12. Beschreibung, wie das IT-Produkt den Datenschutz fördert

ViViAN, Version 4.0, fördert den Datenschutz auf vielfältige Weise:

--- ViViAN wird in einem nach ISO 27001 zertifizierten Rechenzentrum gehostet

--- Es werden Patientendaten nur mit einer Ende-zu-Ende-Verschlüsselung zwischen behandelnden Arztpraxen ausgetauscht.

--- Über die für ViViAN aufgebaute PKI wird die Authentizität der Kommunikationspartner in vorbildlicher Weise sichergestellt.

13. Votum der Auditoren

ViViAN, Version 4.0, setzt insgesamt die Anforderungen an den Datenschutz angemessen um.

Bremen, den 30.11.2015.

Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH