

Kurzgutachten

Einhaltung datenschutzrechtlicher Anforderungen
durch das IT-Produkt

- healthCONNECT Version 1 -

der

EOS Health IT-Concept GmbH
Lübeckertordamm 73
20099 Hamburg

erstellt von:

Andreas Bethke

Dipl. Inf. (FH)

Beim Unabhängigen Landeszentrum für
Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-
Produkte (technisch)

Papenbergallee 34

25548 Kellinghusen

tel 04822 – 36 63 000

fax 04822 – 36 63 333

mob 0179 – 321 97 88

email bethke@datenschutz-guetesiegel.sh

Stephan Hansen-Oest

Rechtsanwalt

Beim Unabhängigen Landeszentrum für
Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-
Produkte (rechtlich)

Im Tal 10a

24939 Flensburg

tel 0461 – 900 138 21

fax 0461 – 900 138 22

mob 0171 – 2044981

email sh@hansen-oest.com

Stand: November 2017

Inhaltsverzeichnis

A. Einleitung und Kurzbezeichnung	3
B. Zeitpunkt der Prüfung	3
C. Detaillierte Bezeichnung des Begutachtungsgegenstandes	3
D. Tools, die zur Herstellung des IT-Produktes verwendet wurden.....	5
D. Zweck und Einsatzbereich des Begutachtungsgegenstandes.....	6
E. Datenflusses.....	6
E. Zusammenfassung der Prüfergebnisse	7
H. Beschreibung, wie das Produkt den Datenschutz fördert	10

A. Einleitung und Kurzbezeichnung

In diesem Kurzgutachten werden die Ergebnisse des Zertifizierungsprozesses für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) bezüglich des IT-Produktes „healthCONNECT“ der Firma EOS Health IT-Concept GmbH (im weiteren kurz ITC) zusammengefasst. Die Prüfung erfolgte mit dem Software-Release Version 1.

Für die Begutachtung wird der Anforderungskatalog in der Version 2.0 zugrunde gelegt.

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand in der Zeit vom 16.01.2017 bis 02.11.2017 statt.

C. Detaillierte Bezeichnung des Begutachtungsgegenstandes

Bei healthCONNECT handelt es sich um ein Java-basiertes Softwaremodul, das mittels URLs angesprochen werden kann.

Der Aufbau lässt sich in drei Teile gliedern:

- Konfiguration (Einrichtung der Praxisparameter)
- Web Server (Bündelung d. Datenkommunikation; Verschlüsselung)
- Services (Eigentliche Funktionalität; Geräteanbindung etc.)

Es umfasst also mehrere Funktionen, wovon eine dieser Funktionen ein **Proxy-Server** ist, der sich um die Verschlüsselung von übergebenen Daten kümmert. **Nur diese Funktion ist Gegenstand der Zertifizierung.** Sie kann losgelöst von den anderen Funktionen (wie die Ansteuerung von Druckern und Kartenlesegeräten) eingesetzt werden.

Die interne Architektur von healthCONNECT verdeutlicht die interne Trennung der Funktionen.

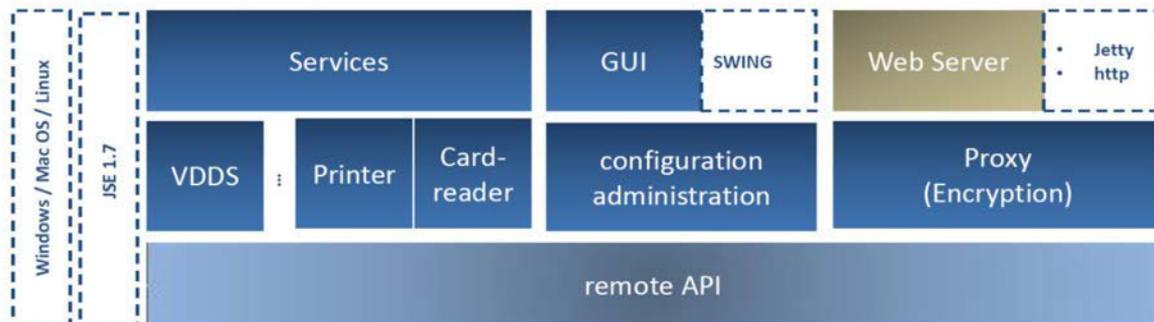


Abbildung 1: Architektur von healthCONNECT

Die Konfigurationsmöglichkeit ist nur insoweit Gegenstand der Zertifizierung und geprüft worden, dass eine Server-Adresse eingetragen wird und der Benutzerschlüssel generiert und sicher verwahrt wird.

Grundsätzlich ist healthCONNECT unabhängig von einer vorgelagerten Software. Es ist so parametrisierbar, dass es sich auch mit einem lokalen Speicher/Datenbankserver verbinden kann. Es muss also keine Verbindung über das Internet aufgebaut werden.

Das Produkt wird über eine lokale URL aufgerufen. Dabei werden Datenfelder übergeben und zu jedem Feld wird die Information übergeben, ob das Feld verschlüsselt werden soll, oder nicht.

Für die Verschlüsselung der Daten kommt ein mehrstufiges Prinzip zum Tragen, das nachfolgend kurz erläutert wird.

Soll ein Datum (z.B. „Nachname“) verschlüsselt werden, wird hierfür zunächst ein für das betreffende Datum individueller, symmetrischer 256-bit Schlüssel generiert, mit welchem das Datum per AES Algorithmus verschlüsselt wird.

Der Einsatz individueller Schlüssel je Datum begegnet den Bedrohungsszenarien, dass ein Angreifer in den Besitz verschlüsselter Daten gelangen und aufgrund von erkannten Mustern einen Schlüssel ermitteln kann und dass ein ihm die Ermittlung des für die Verschlüsselung eines Datums verwendeten Schlüssels gelingt und er somit weitere Daten entschlüsseln kann.

Um auch einem Bedrohungsszenario („Einschleusen von Pseudodaten“) zu begegnen, dass ein Angreifer durch die Möglichkeit definierte Daten mit dem verwendeten Algorithmus zu verschlüsseln und so Kenntnisse über den Schlüssel bekommt, wird der AES Algorithmus im

Cipher Block Chaining (CBC) Betriebsmodus verwendet. Da das Ergebnis der Verschlüsselung von Blöcken dabei abhängig vom vorhergehenden Block ist, haben bei unterschiedlicher Initialisierung gleiche Blöcke unterschiedliche Verschlüsselungsergebnisse.

In einem zweiten Schritt wird der für die AES Verschlüsselung verwendete individuelle Schlüssel selbst mit Hilfe des öffentlichen Teils des asymmetrischen Benutzerschlüssels verschlüsselt. Als Algorithmus kommt hier Curve 25519 zum Einsatz. Im Gegensatz zu z.B. RSA gelten Algorithmen auf Basis von Eliptischen Kurven bei geringerer Schlüssellänge als ebenso sicher und sind deutlich performanter. Curve 25519 ist ein solcher Algorithmus, der zudem in verschiedenen Standards enthalten ist.

Beide Teile werden zusammengefügt und als (verschlüsselter) „Nachname“ an den Server übertragen.

healthCONNECT bzw. der Proxy selbst verarbeitet also keine festen Datenstrukturen, sondern wird entsprechend individuell angesteuert. Alle Klartext-Daten, die ein Kunde verschlüsselt verarbeiten möchte (Adressen, Login-Daten usw.) werden lokal bei dem Kunden erfasst und vor der Speicherung in einer Datenbank verschlüsselt. Somit hat nur er Zugriff auf diese Daten. Der Hersteller des Produkts selbst weiß zu keinem Zeitpunkt, welche Datenarten und Strukturen mit seinem Produkt verarbeitet werden. Der private Teil des Benutzerschlüssels wird niemals übermittelt und dient nur der Entschlüsselung der individuellen AES-Schlüssel, die für jedes Datum erzeugt werden.

D. Tools, die zur Herstellung des IT-Produktes verwendet wurden

Bei der Entwicklung kommen folgende Tools zum Einsatz:

- Eclipse
- Git
- Maven

In der Testumgebung kommen folgende Tools zum Einsatz:

- Microsoft Server 2008/2012/2016
- Microsoft Windows XP, 7, 8.1, 10
- CentOS

D. Zweck und Einsatzbereich des Begutachtungsgegenstandes

Das Produkt ist zum Einsatz in Bereichen vorgesehen, in denen Daten vor der Speicherung in einer Datenbank verschlüsselt werden müssen (besondere Arten personenbezogener Daten) und wo die bisher eingesetzte Software keine Verschlüsselungsmöglichkeit bietet. Dies kann also in jeder öffentlichen Stelle des Landes Schleswig-Holsteins sein.

E. Datenfluss

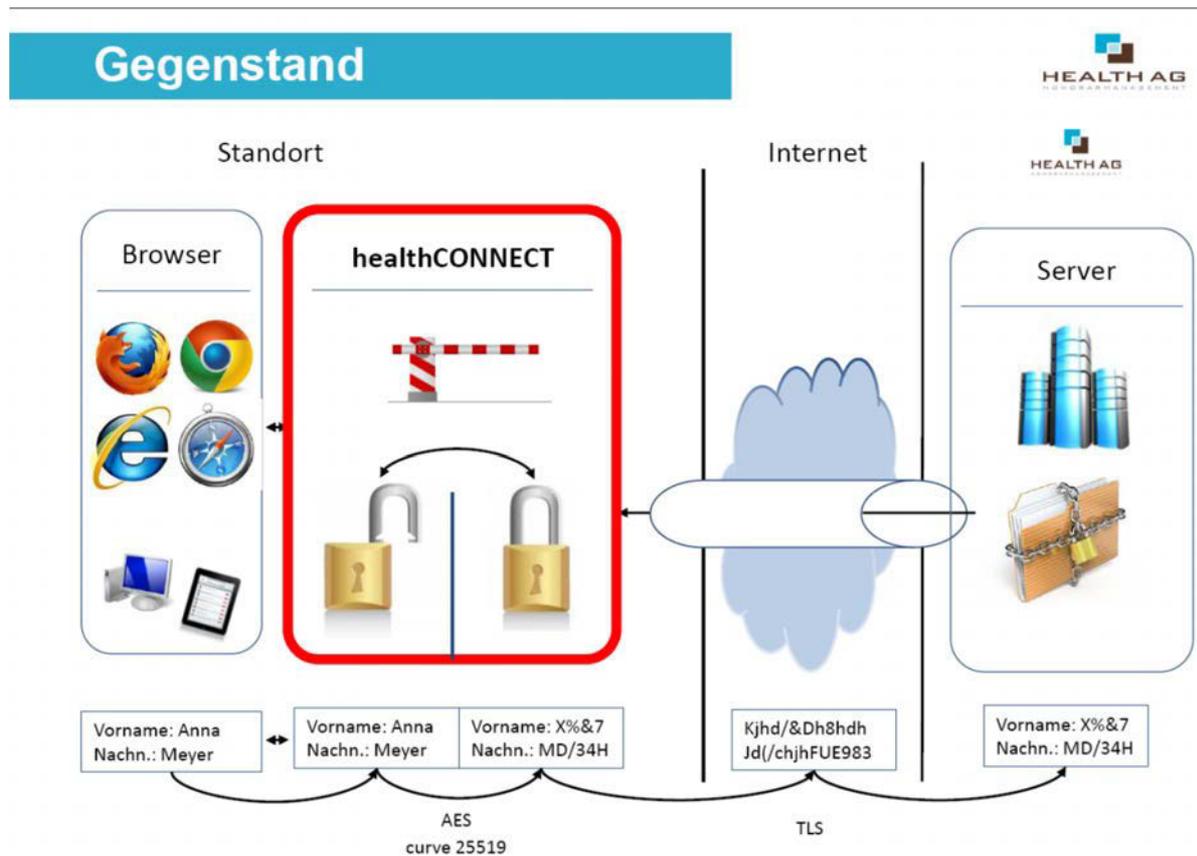


Abbildung 2: Datenfluss und Verschlüsselung von healthCONNECT

E. Zusammenfassung der Prüfergebnisse

healthCONNECT dient der Unterstützung von Datenbankbasierten Softwareprodukten, die sensible oder besondere Daten (wie bspw. Patientendaten, oder Gesundheitsdaten) verarbeiten und die den Anspruch haben diese Daten verschlüsseln zu müssen, es aber selbst nicht leisten können.

Hierfür bietet sich das Produkt als Proxy an, der bei Bedarf einzelne Datenfelder des übergebenen Datenstroms verschlüsselt, bevor die Daten an die Persistenzschicht übergeben werden.

Dabei verfügt das Produkt selbst über keine festen Datenstrukturen.

Die vom übergeordneten Programm übergebenen (und klassifizierten) Daten werden auf dem Server ausschließlich verschlüsselt gespeichert und können nur von dem gleichen Proxy wieder entschlüsselt werden, der den Benutzerschlüssel zum Entschlüsseln der Daten vorhält.

Ein Einsatz des Produktes im Rahmen einer Auftragsdatenverarbeitung ist somit grundsätzlich möglich.

Festzustellen ist, dass ein datenschutzkonformer Einsatz unter Einhaltung der jeweils geltenden Rechtsgrundlagen grundsätzlich möglich ist.

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
Komplex 1:		
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit	adäquat	
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)	vorbildlich	
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)	adäquat	
1.4 Datenschutz-Schutzziel: Intervenierbarkeit	vorbildlich	
1.5 Anpassung des IT-Produkts	adäquat	
1.6 Privacy by Default	adäquat	
1.7 Sonstige Anforderungen	entfällt	
Komplex 2:		
2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten	adäquat	
2.1.2 Einwilligung des Betroffenen	adäquat	
2.1.3.1 Vorschriften über die Datenerhebung	entfällt	

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
2.1.3.2 Vorschriften über die Übermittlung	adäquat	
2.1.3.3 Löschung nach Wegfall des Erfordernisses	entfällt	
2.2.1 Zweckbindung und Zweckänderung	adäquat	
2.2.2 Erleichterung der Umsetzung des Trennungsgebotes	adäquat	
2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG)		Siehe Komplex 3
2.3 Datenverarbeitung im Auftrag	adäquat	-
2.4.1 gemeinsame Verfahren/Abrufverfahren	entfällt	-
2.4.2 Trennung der Verantwortlichkeiten	entfällt	-
2.4.3 Veröffentlichungen im Internet	entfällt	
2.4.4 Weitere besondere technische Verfahren	entfällt	
2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	entfällt	
Komplex 3:		
3.1.1. Physikalische Sicherung	entfällt	
3.1.2 Authentisierung	adäquat	
3.1.3 Autorisierung	adäquat	
3.1.4 Protokollierung	adäquat	
3.1.5 Verschlüsselung und Signatur	vorbildlich	
3.1.6 Pseudonymisieren	entfällt	
3.1.7 Anonymisieren	entfällt	
3.2.1.1 Verfügbarkeit	adäquat	
3.2.1.2 Integrität	adäquat	
3.2.1.3 Vertraulichkeit	adäquat	
3.2.1.4 Nicht-Verkettbarkeit	vorbildlich	
3.2.1.5 Transparenz	adäquat	
3.2.1.6 Intervenierbarkeit	vorbildlich	
3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	adäquat	
3.2.1.8 Test und Freigabe	adäquat	
3.2.2 Erleichterung der Vorabkontrolle	adäquat	
3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses	adäquat	
3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	adäquat	

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten	adäquat	
3.3.1 Verschlüsselung	vorbildlich	
3.3.2 Anonymisierung oder Pseudonymisierung	adäquat	
3.3.3.1 Mobile Datenverarbeitungssysteme	entfällt	
3.3.3.2 Video-Überwachung und –Aufzeichnung	entfällt	
3.3.3.3 Automatisierte Einzelentscheidungen	entfällt	
3.3.3.4 Veröffentlichungen im Internet	entfällt	
3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	adäquat	
3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	entfällt	
3.6 Sonstige Anforderungen	entfällt	
Komplex 4:		Im Hinblick auf den konkreten Zertifizierungsgegenstand sind die Kriterien aus Komplex 4 nicht anwendbar
4.1 Aufklärung und Benachrichtigung	entfällt	
4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	entfällt	
4.3 Auskunft	entfällt	
4.4.1 Berichtigung	entfällt	
4.4.2 Vollständige Löschung	entfällt	
4.4.3 Sperrung	entfällt	
4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	entfällt	
4.3.5 Gegendarstellung	entfällt	
4.5 Sonstige Anforderungen	entfällt	

Insgesamt kann festgestellt werden, dass das Produkt healthCONNECT die Voraussetzungen für den Erhalt eines Gütesiegels für IT Produkte erfüllt. Beim Einsatz des Produktes durch öffentliche Stellen des Landes Schleswig-Holstein können alle datenschutzrechtlichen Vorschriften eingehalten werden.

H. Beschreibung, wie das Produkt den Datenschutz fördert

Durch die konsequente Umsetzung einer Verschlüsselungstechnologie wird es für die einsetzende Stelle möglich eine Ende-zu-Ende-Verschlüsselung zu gewährleisten, auch wenn ein bereits eingesetztes Softwareprodukt, das sensible Daten verarbeitet, eine Verschlüsselung selbst nicht leisten kann. Dabei verzichtet healthCONNECT auf ein konkretes Mapping und somit auf das Wissen, welche Datenfelder mit ihm verarbeitet werden. Rückschlüsse auf Inhalte sind somit ebenfalls nicht möglich. Das Schlüsselmanagement gewährleistet, dass Schlüssel die einsetzende Stelle nicht verlassen müssen und auch sonst niemand Kenntnis von diesen haben muss. Auch findet keine Protokollierung von Datensätzen statt, so dass der Grundsatz der Datenvermeidung und Datensparsamkeit eingehalten wird.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 24.11.2017

Flensburg, den 24.11.2017



Andreas Bethke

Dipl. Inf. (FH)

Beim Unabhängigen Landeszentrum für
Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (technisch)



Stephan Hansen-Oest

Rechtsanwalt

Beim Unabhängigen Landeszentrum für
Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (rechtlich)