Technisches und rechtliches Rezertifizierungs-Gutachten - Kurzgutachten -

"RED Medical"

für:
RED Medical Systems GmbH
Maximilianstr. 16
82319 Starnberg

für das Gütesiegel für IT-Produkte (ULD)

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 – 37 89 05
fax 04822 – 37 89 04
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)

Neustadt 56
24939 Flensburg
tel 0461 – 90 91 356
fax 0461 – 90 91 357
mob 0171 – 20 44 98 1
email sh@hansen-oest.com

Stand: 18.12.2014

A. Einleitung

Die RED Medical Systems GmbH strebt die Rezertifizierung ihres Produktes „RED Medical“ für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) an.

Die Vorlage eines rechtlichen und technischen Gutachtens ist Voraussetzung für die Rezertifizierung des Produktes. Dieses Dokument dient als Gutachten zur Vorlage beim ULD im Zusammenhang mit der Rezertifizierung des Produktes.

Dem Gutachten wird der Anforderungskatalog in der Version 1.2 zugrunde gelegt.

Im nachfolgenden Gutachten wird eine Ergänzung des Produktes bewertet. Im Übrigen wird auf die Beschreibung des Zertifizierungsgegenstandes im Gutachten der Erstzertifizierung (Zertifizierung erfolgte am 11.07.2013) verwiesen. Mit Ausnahme des neuen „Statistikmoduls“ gab es keine Änderungen an dem Produkt.
In rechtlicher Hinsicht trat am 01.01.2014 die neue Datenschutzverordnung (DSVO) des Landes Schleswig-Holstein in Kraft. In dieser gibt es im Vergleich zur DSVO 2009 Änderungen bei der Erstellung der Verfahrensdokumentation (§ 3), bei der Dokumentation der Sicherheitsmaßnahmen (§ 3) (hier insbesondere die Erweiterung bei der Dokumentation des Datenschutzmanagements), bei der Dokumentation des Tests und der Freigabe (§ 5).

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 23.11.2013 bis zum 18.12.2014 statt.

C. Übersicht der Änderungen

Seit der Zertifizierung des Produktes im Juli 2013 haben sich folgende aus Datenschutzsicht relevanten Produktänderungen ergeben:
a) Das Statistikmodul
b) Die Verschlüsselungsbibliotheken
c) Der Connector
d) Das Rechenzentrum

D. Änderungen und Neuerungen des Produktes

a) Statistik-Modul

Die Anwender des Produktes RED Medical sind als Ärzte darauf angewiesen, statistische Auswertungen von Daten vorzunehmen. Hiervon sind folgende Datenarten betroffen:

- Diagnosen
- Gebührenordnungsnummern
- Arzneimittelverordnungen

Erforderlich ist die Auswertung der Daten für das wirtschaftliche Betreiben der Praxis. Im Gegensatz zu vielen anderen Berufsgruppen unterliegen Kassenärzte regulatorischen Einschränkungen. So sind z.B. Arzneimittelverschreibungen budgetiert. Bei einer Überschreitung eines Budgets können die Berufsträger mit Rückforderungsansprüchen konfrontiert werden, die sich auch auf das persönliche Vermögen erstrecken. Auch im Bereich der Erbringung ärztlicher Leistungen erfolgt eine Budgetierung anhand der jeweiligen Gebührenordnungsnummern (GO-Nummern).

In der Quartalsplanung ist es für die Berufsträger zwingend erforderlich, sich einen Überblick darüber verschaffen zu können, wie viele Arzneiverordnungen welchen Typs und welche ärztlichen Leistungen erbracht worden sind, um Regressforderungen verhindern zu können und die Erbringung der weiteren ärztlichen Leistungen zu planen.

Für diese Zwecke bietet RED Medical ein zusätzliches „Statistikmodul" an, das den Anwendern die Möglichkeit bietet, strukturell vordefinierte Auswertungen auszuwählen. Dabei können Auswertungszeiträume und –entitäten festgelegt und die Auswertungsdaten angezeigt und ausgedruckt werden.

RED Medical ist ein Produkt, das im Hinblick auf die datenschutzrechtliche Zulässigkeit darauf basiert, dass personenbezogene Daten im Rechenzentrum ausschließlich verschlüsselt gespeichert werden, so dass Beschäftigte der RED Medical Systems GmbH und Beschäftigte des Rechenzentrums keine Möglichkeit der Kenntnisnahme

von personenbezogenen Daten haben. Auf diese Weise werden auch die rechtlichen Vorgaben der ärztlichen Schweigepflicht i.S.d. § 203 StGB eingehalten.

Da nicht ausgeschlossen werden kann, dass in Einzelfällen auch atomare medizinische Informationen – ggf. unter Hinzuziehung von Zusatzwissen – einen Personenbezug ermöglichen könnten, werden auch diese Daten grundsätzlich nur verschlüsselt gespeichert. Dies betrifft ebenso alle diesbezüglichen Metainformation, aus denen die ursprüngliche Information abgeleitet werden könnte, also zum Beispiel die Punktzahl von Gebührennummern oder der Preis eines Arzneimittels.

Die diesbezügliche Verschlüsselung quantitativer Angaben (hier: Punktzahlen/Preise) erschwert die Durchführung von Analysen für RED Medical entsprechend, da aus bzw. mit den verschlüsselten Daten nicht ohne weiteres die o. g. erforderlichen Analysen durchgeführt werden können.

Der Anbieter der Software hat nun eine Möglichkeit gefunden, die eine Durchführung von Analysen auf Basis von verschlüsselten Daten ermöglicht. Hierbei kommen u.a. auch Methoden aus der homomorphen Kryptographie zur Anwendung.

Die Durchführung von Analysen erfolgt dabei u.A. dadurch, dass für bestimmte medizinische Informationen, die nicht für sich unmittelbar personenbezogen sind, mandanten-spezifische Hashwerte erzeugt werden. Die Besonderheit bei Hashwerten besteht darin, dass diese jeweils für den gleichen Ausgangswert (z.B. ICD-Code: I15.9) immer wieder den gleichen Hashwert ergeben. Das macht es auf der einen Seite dem Softwareanbieter möglich, mit Hashwerten Aggregationen durchzuführen, auf der anderen Seite aber verhindert es wegen der Mandantenspezifität, dass selbst mit Mitteln der quantitativen Analyse aus diesen Daten der Ursprungswert rückermittelt werden kann.

b) Verschlüsselungsbibliotheken

Eine zentrale Rolle im Produkt spielt die clientseitige Verschlüsselung. Bislang kamen für die Verschlüsselung zwei verschiedene Bibiotheken zum Einsatz:

1. Standford JavaScript Crypto Library[1]

[1] http://crypto.stanford.edu/sjcl/

2. CryptoJS[2]
Da für den Anwender nicht nur die Sicherheit des Produktes, sondern auch die Performance zählt, wurden diese beiden Bibliotheken gegen Funktionen der asmcrypto.js[3]. Diese ist gegenüber der Standford-Bibliothek um Faktor 20 schneller und gegenüber der CryptoJS ungefähr um den Faktor 13.
Dabei bleiben die verwendeten Algorythmen (AES, PBDKF2 etc.) vollständig gleich.

c) Connector
Vor dem Hintergrund, dass Plugins zukünftig in den Browsern der beiden Hersteller Google (Chrome[4]) und Mozilla Foundation (FireFox[5]) nicht mehr unterstützt werden, hat sich der Hersteller für den Einsatz einer neue Technologie namens „Connector" entschieden. Dabei handelt es sich um einen kleinen lokalen Server, mit dem der Client via HTTPS kommuniziert. Der „Connector" wird, wie die Plugins auch, von der Webseite des Herstellers heruntergeladen.
Um die Sicherheit gegenüber der alten Plugin-Variante zu erhöhen, wurden zum einen alle bestehenden Sicherheitsfeatures des Plugins übernommen (Überprüfung der Webseite, von der der Aufruf kommt, Authentifizierung gegenüber dem Client, Starten von authentifizierten Systemprozessen, Sicheres Löschen von Dateien und Ordnern) und zudem noch eine Kommunikation via HTTPS und eine Session-Prüfung implementiert. Diese prüft jede vom Browser an den Connector übergebene Session-ID beim Server auf ihre Gültigkeit, bevor der Request beantwortet wird.

In der Folge bedeutet es, dass die Überwachung der Verschlüsselungsmethode, die quasi das Überwachungsinstrument gegenüber dem Hersteller darstellt, nun auch durch den Connector ersetzt wird.
Durch die neue Technologie ergibt sich eine Änderung im Datenfluss. Bislang sah dieser so aus:

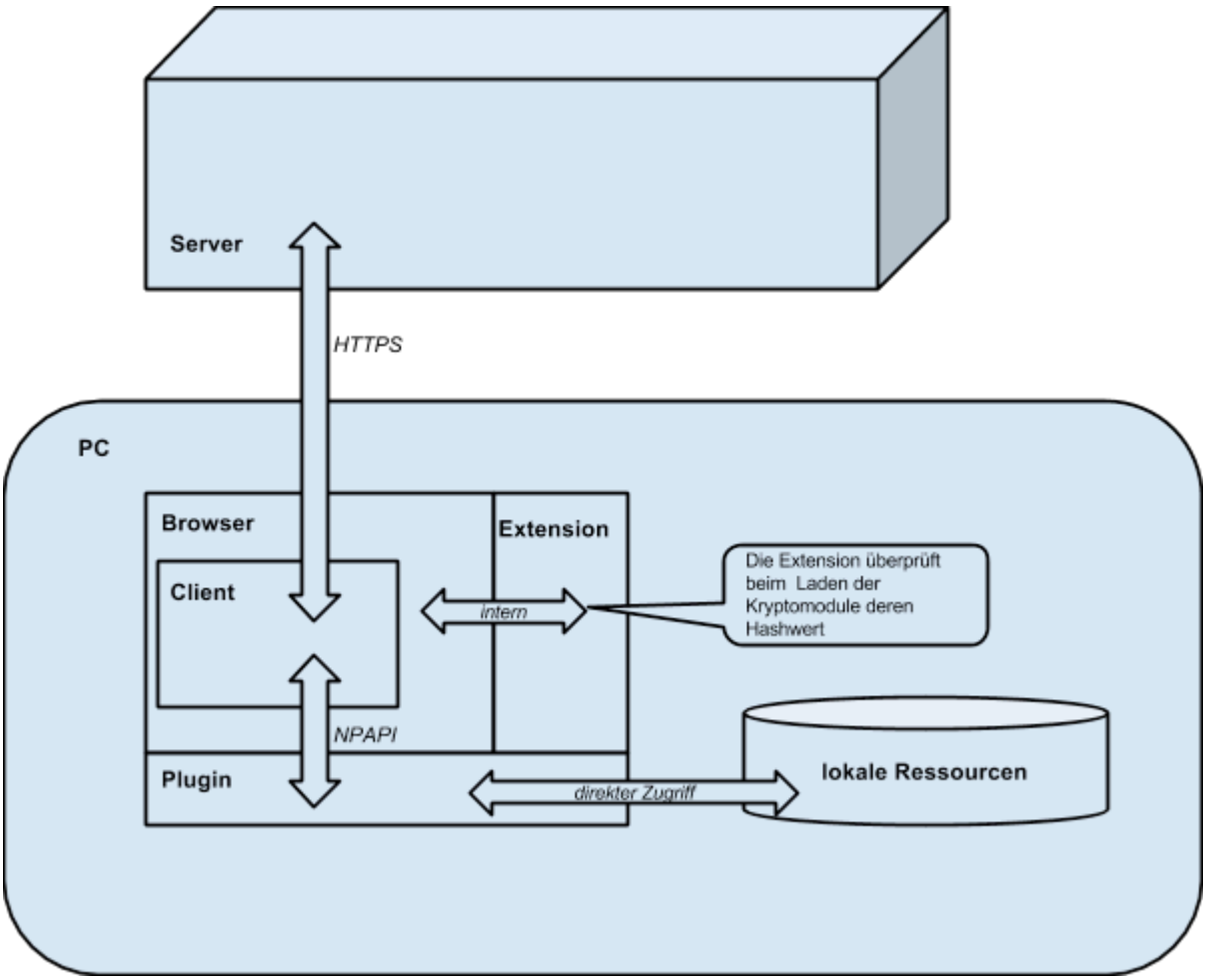
---

[2] http://code.google.com/p/crypto-js

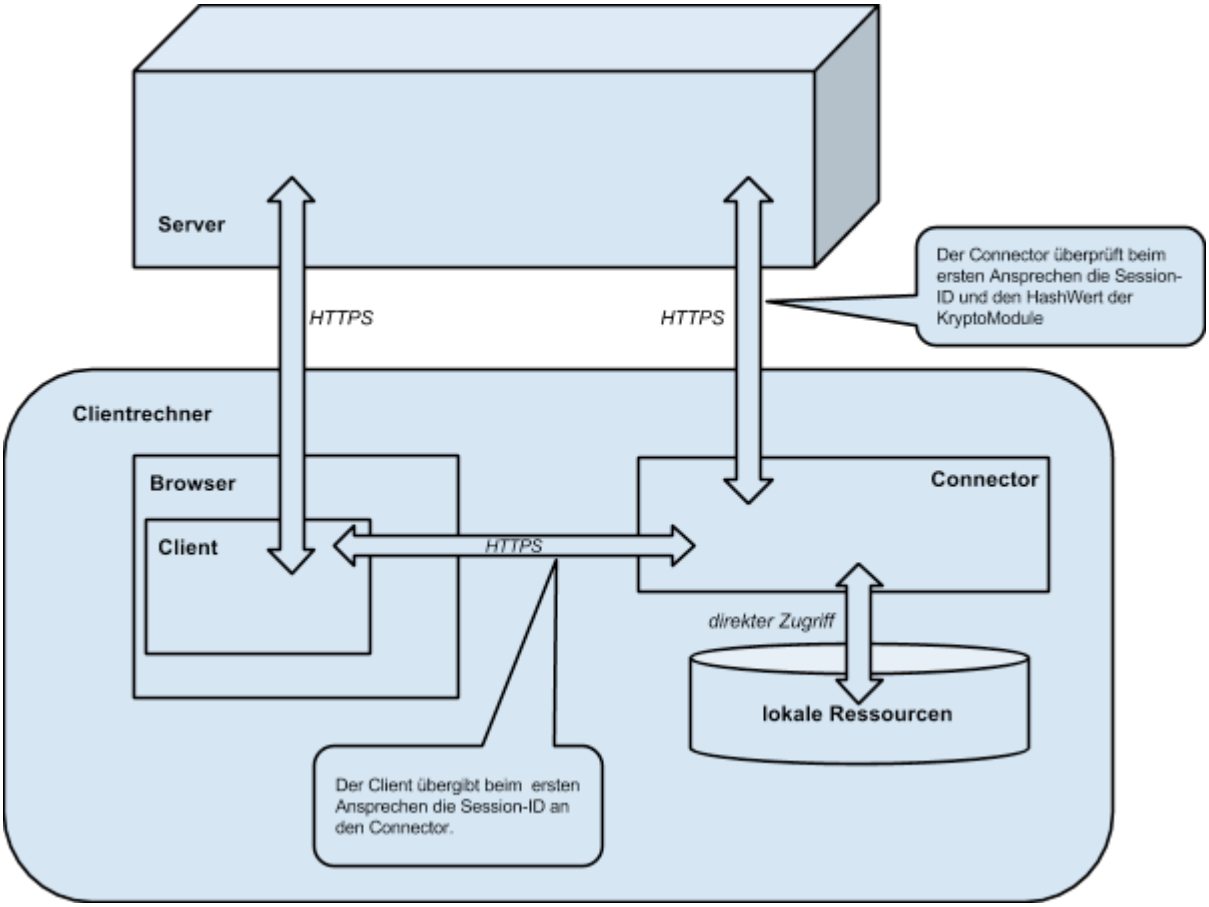
[3] https://github.com/vibornoff/asmcrypto.js

[4] http://blog.chromium.org/2013/09/saying-goodbye-to-our-old-friend-npapi.html

[5] http://thenextweb.com/apps/2013/01/29/mozilla-to-enable-click-to-play-for-all-firefox-plugins-by-default-except-the-latest-flash-version/



Durch den Connector ändert sich der Datenfluss wie folgt:



Eine Speicherung von Daten im Connector selbst findet nicht statt.

d) Neues Rechenzentrum

Der Hersteller hat sich entschlossen, für seine Server ein anderes bzw. ggf. mehrere andere Rechenzentren zu nutzen. Dabei sind zwei Rechenzentren ausgewählt worden:

1. Rechenzentrum der STRATO AG
2. Rechenzentrum der Hetzner Online AG

In beiden Rechenzentren kommen dedizierte Server für die RED Medical Systems GmbH zum Einsatz. Beim Einsatz der Rechenzentrumsanbieter kommen die von den Rechenzentrumsdienstleistern angebotenen Auftragsdatenverarbeitungsverträge zum Einsatz.

Sowohl der Auftragsdatenverarbeitungsvertrag der STRATO AG als auch der Auftragsdatenverarbeitungsvertrag der Hetzner Online AG erfüllen die gesetzlichen Voraussetzungen des § 11 BDSG.

Die von den Rechenzentrum getroffenen technischen und organisatorischen Maßnahmen i.S.d. Anlage zu § 9 Satz 1 BDSG sind durch hinreichende Dokumente und Testate der Anbieter nachgewiesen. Details sind dem Langgutachten zu entnehmen.

E. Datenschutzrechtliche Bewertung

Für die datenschutzrechtliche Bewertung des neuen Statistikmoduls ist entscheidend, ob im Zusammenhang mit den neuen Verarbeitungen an irgendeiner Stelle ein Personenbezug durch RED Medical oder einen Dritten hergestellt werden kann.

Dies ist nach Überzeugung der Gutachter nicht der Fall.

Wenn eine Analyse der Daten auf dem Client des Berufsgeheimnisträgers stattfindet, werden die Daten erst auf dem Client in der Praxis entschlüsselt. Hier besteht für RED Medical keine Möglichkeit zur Herstellung eines Personenbezuges. Da die Analysen zudem nicht auf den Server zurück übertragen werden, ist insoweit auch kein Personenbezug möglich.

Bei der zweiten Variante, der Durchführung von Analysen auf der Basis von anonymisierten Klartextdaten auf dem Server ist entscheiden, ob aus den im Klartext übertragenen Daten noch ein Personenbezug herzustellen ist.

Das ist nach Überzeugung der Sachverständigen nicht der Fall. Denn aus den reduzierten Informationen zur Altersgruppe, zum Kassentyp, zu den ersten zwei Ziffern der PLZ, dem Geschlecht, dem Versicherungsstatus und dem Versicherungsfall lassen sich mit an Sicherheit grenzender Wahrscheinlichkeit keine personenbeziehbaren Informationen ableiten. Durch die zusätzlichen Methoden der verzögerten Speicherung der Daten auf dem Server und der Implementierung von Methoden der k-Anonymität ist ausgeschlossen, dass auch aufgrund kleiner Fallgruppen eine Personenbeziehbarkeit erreicht werden kann. Ein Personenbezug wäre nur denkbar, wenn die Person darüber hinaus Kenntnis von sonstigen Daten aus der Praxis hat. De facto würde eine Personenbeziehbarkeit dann nur für das Praxispersonal denkbar sein. Auch bei Kombination aller Faktoren ist davon auszugehen, dass die potentielle Auswahlgruppe der k-Anonymität genügt.

Der Hersteller hat in seinem Konzept zum Statistikmodul die Generalisierung erläutert. Nach Überzeugung der Sachverständigen ist die Umsetzung hinreichend, um einen Personenbezug zu vermeiden.

Ziel der Verarbeitung im Zusammenhang mit dem Statistikmodul ist stets, dass die Analysebasis der Daten so groß ist, dass die Daten eines Patienten in der Masse der Daten „untergehen". Das wird nach Überzeugung der Sachverständigen durch die in der Beschreibung des Statistikmoduls dargestellten Methoden erreicht.

Auch bei der Analyse auf Basis der Daten von Arzneimitteln und GO-Nummern durch das Aggregieren von Hashwerten ist ein Personenbezug nicht herstellbar. Aus den Hashwerten selbst ist eine Personenbeziehbarkeit nicht herzuleiten. Insbesondere ist auch ausgeschlossen, dass aufgrund von seltenen Diagnosen ein Personenbezug hergeleitet werden kann, denn es gibt wiederum hinreichend viele Diagnosen, die selten vorkommen. Und weder RED Medical noch ein anderer Dritter kann aus den Hashwerten ermitteln, um welche Diagnosen es sich handelt.

Nach alledem ist festzustellen, dass ein Personenbezug durch das Statistikmodul in RED Medical nicht möglich ist.

Die Umstellung der Verschlüsselungsbibliotheken stellt kein Risiko dar, da auch die neue Bibliothek quelloffen ist und die Funktionen per se das gleiche Ergebnis liefern. Die neue Bibliothek tut dies nur wesentlich effizienter.
Der Connector ist aus Sicht des Gutachters eine gute Alternative zum Browser-Plugin. Statt einer DLL gibt es nun eine Applikation, die sich wie ein kleiner lokaler Webserver verhält. Der erreichte Sicherheitsgewinn ist eine Überprüfung einer Session-ID auf ihre Gültigkeit am Server des Herstellers, so dass eine Manipulation eines Zugriffs ausgeschlossen werden kann. Ansonsten verhält sich die neue Komponente hinsichtlich der datenschutzrelevanten Fragen wie sein Vorgänger: D.h. keine separate Speicherung von Daten.

Nach Überzeugung der Sachverständigen handelt es sich um eine aus Sicht des Datenschutzes vorbildliche Umsetzung einer Verarbeitung von Daten, mit der das Verschlüsselungskonzept, das RED Medical zugrunde liegt, weiter umgesetzt bleibt.

Der Wechsel des Hostinganbieters ist in zulässiger Weise möglich. Insoweit bestehen keine Bedenken. Beide Rechenzentrumsanbieter verfügen über ausreichende Sicherheitsmaßnahmen und ermöglichen zudem die Begehung des Rechenzentrums im Einzelfall.

Bei der STRATO AG finden auch regelmäßige ISO 27001 Rezertifizierungen statt. Die aktuelle Zertifizierung gilt bis Anfang 2016.

F. Zusammenfassung

Insgesamt kann festgestellt werden, dass auch mit dem neuen Produkt die Rechtsvorschriften zu Datenschutz und Datensicherheit eingehalten werden.

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

Kellinghusen, den 18.12.2014

Andreas Bethke

Flensburg, den 18.12.2014

Stephan Hansen-Oest