Kurzgutachten zur Erteilung eines Datenschutzgütesiegels für „Secure Data Space“ gemäß DSGSVO

im Auftrag der SSP Europe GmbH

datenschutz cert GmbH
10.06..2015

Inhaltsverzeichnis

1. Vorbemerkung

Mit diesem Kurzgutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Auditierung des „Secure Data Space“ in der Version 3.0 gemäß der Datenschutzgütesiegelverordnung (DSGSVO) Schleswig-Holsteins[1] zusammengefasst.

2. Zeitraum der Prüfung

Die Begutachtung erfolgte vom 29.04.2015 bis 09.06.2015 und beinhaltete neben der konzeptionellen Analyse der zur Verfügung gestellten Unterlagen die Durchführung von Funktionstests anhand eines Testzugangs für das Nutzerprofil sowie ein Administrationsprofil innerhalb der geschlossenen Nutzergruppe. Hierbei sind u.a. die Verschlüsselungsmechanismen überprüft worden.

3. Antragstellerin

Antragstellerin ist die ist die

SSP Europe GmbH

Maximilianstraße 35a

80539 München, Bundesrepublik Deutschland

als Anbieter des „Secure Data Space“.

Ansprechpartner und Projektverantwortliche sind Herr Dan Jacob, Head of IT-Security Solutions der SSP Europe GmbH sowie Herr Dr. Florian Scheurer, IT-Security Consultant der SSP Europe GmbH.

4. Sachverständiger/Prüfstelle

Sachverständige Prüfstelle ist die

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 Prüfung sind:

Bereich „Recht“:	Bereich „Technik“:
Frau Dr. Irene Karper datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen	Herr Ralf von Rahden datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen.

[1] Landesverordnung über ein Datenschutzgütesiegel v. 30.11.2013, GVOBl. Schl.-H. 2013, S.536ff. Konkretisiert wird die DSGSVO durch den Anforderungskatalog des ULD, der zum Zeitpunkt des Audits in der Version 2 vorlag. Die Kriterien sind abrufbar unter https://www.datenschutzzentrum.de/uploads/guetesiegel/guetesiegel-anforderungskatalog.pdf. Stand dieser und weiterer hier zitierter Webseiten ist März 2015.

5. Kurzbezeichnung des IT-Produkts

Secure Data Space - SDS in der Version 3.0.

6. Beschreibung des IT-Produkts

SDS ist ein webbasierender, virtueller Datenraum, in welchem Daten hochgeladen, gespeichert, verwaltet und ausgetauscht werden können. Die online per Webzugang zur Verfügung gestellten Verarbeitungskapazitäten des SDS sind als typische Cloud-Dienstleistung zu klassifizieren.

SDS wird von der SSP Europe GmbH vertrieben und als *Software as a Service* (SaaS) im Auftrag für den Anwender in Deutschland entwickelt, gepflegt und in einem Rechenzentrum in Deutschland betrieben. Die Auditierung dieser IT-basierenden Services des SDS bezog sich dabei auf den Funktionsstand im Januar 2015.

SDS wird in folgenden drei Varianten angeboten:

--- Secure Data Space Online

--- Secure Data Space Dedicated

--- Secure Data Space Virtual Appliance.

Die Variante *Secure Data Space Online* ist die Standardausführung. Sie wird von der SSP Europe GmbH als SaaS angeboten.

Die Variante *Secure Data Space Dedicated* entspricht der Standardausführung. Allerdings erhält der Anwender die Möglichkeit, den SDS auf seine Bedürfnisse und das Corporate Design zu branden sowie eine Anmeldung über sein Active Directory zu erhalten.

Secure Data Space Virtual Appliance ist dagegen ein Softwarepaket, das einerseits vom Anwender in seiner eigenen Umgebung installiert und gehostet werden kann, andererseits als SaaS beauftragt werden kann.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Keine.

8. Zweck und Einsatzbereich

Der SDS ist für den gewerblichen B2B- Einsatz konzipiert und dient dem Hochladen, Speichern, Verwalten und Austausch von Daten in virtuellen Datenräumen (Data Rooms).

Anwender sind Unternehmen, Organisationen oder öffentliche Stellen. Der SDS kommt dabei im Verantwortungsbereich des lizenzierten Anwenders zum Einsatz, so dass es sich um eine Private-Cloud-Dienstleistung handelt. Der Anwender kann als Lizenznehmer aus den genannten drei Varianten wählen.

Anbieter ist die SSP Europe GmbH, welche die Entwicklung, Pflege und den Betrieb des SDS im Auftrag des Anwenders am Standort München durchführt. Das Informationsmanagementsystem (ISMS) der SSP Europe GmbH ist gemäß ISO/IEC 27001:2013 zertifiziert. Das von den Auditoren eingesehene Zertifikat wurde seitens der DQS GmbH für den Geltungsbereich „*Betrieb und Entwicklung*

der SSP Europe Services und Produkte, Managed Security Services, Betrieb des Backoffices“ für die Standorte Galgenbergstraße 2a in 93053 Regensburg und Maximilianstraße 35a in 80539 München unter der Zertifizierungsnummer 486027 ISMS13 erteilt und ist bis zum 03.03.2017 gültig.

Das Vertragskonvolut zwischen der SSP Europe GmbH und dem Anwender entspricht den gesetzlichen Vorgaben der Auftragsdatenverarbeitung.

SDS wird im Unterauftrag der SSP Europe GmbH in einem Rechenzentrum der QSC AG, Am Tower 5, 90475 Nürnberg am Standort in Nürnberg, Deutschland betrieben. Das Rechenzentrum ist gemäß ISO/IEC 27001:2005 zertifiziert. Das von den Auditoren eingesehene Zertifikat wurde seitens der TÜV Rheinland Cert GmbH für den Geltungsbereich „*IT Dienstleistungen, Housing, Hosting, Rechenzentrumsbetrieb*“ unter der Zertifizierungsnummer 01153120814 erteilt und ist bis zum 21.08.2016 gültig. Die QSC AG ist Subunternehmer der SSP Europe GmbH. Der zwischen den Unternehmen vorliegende Vertrag entspricht den gesetzlichen Vorgaben der Auftragsdatenverarbeitung.

Der SDS ist im Internet unter https://dataspace.ssp-europe.eu erreichbar. Hierbei handelt es sich um das Zugangsportal zum SDS.

Der Anwender definiert den Anwendungsbereiche und welche **Benutzer** Zugriff auf den SDS, die Data Rooms und die Dateien bekommen. Zugriffsberechtigt können z.B. interne Bereiche oder einzelne Mitarbeiter sein aber auch Stellen außerhalb des Anwenders, wie z.B. anderer Unternehmen. Die Organisationsstruktur kann über die Data Rooms abgebildet werden (z.B. ein Fachbereich oder eine Abteilung). Der SDS stellt hierfür ein detailliert abstufbares Berechtigungskonzept zur Verfügung.

Die Funktionen des SDS in den drei Varianten sind für den Anwender im Benutzerhandbuch transparent dokumentiert und Kern dieses Audits:

Im **SDS** gibt es folgende Grund-Funktionen:

--- Ablaufdatum für Files, Benutzeraccounts und Downloadlinks

--- Kommentarfunktion für Dateien

--- Sortierung nach User, Datum, Typ, Größe, Name.

--- Up- und Downloads als Zip-Archiv

--- Dateiaustausch als öffentliche Downloadlinks/Quicklinks (optional passwortgeschützt, zeitlich limitiert)

--- Verschlüsselte Ablage aller Nutzdaten sowie aller temporären Kennwörter z.B. für Accounts oder Datei-Freigaben; dadurch ist kein Zugriff des Providers auf die Daten des Anwenders möglich

--- Dateien werden nach Upload automatisch vom Anti-Viren-Scanner überprüft (sofern Dateien nicht verschlüsselt sind)**.** Ist eine Datei infiziert, wird der Versuch einer Desinfektion unternommen. Gelingt dies nicht, so wird die Datei auf die Endung „.virus“ umbenannt und der Zugriff wird gesperrt. Durch automatisiertes Löschen in festgelegten Abständen werden diese Dateien endgültig vom System entfernt

--- Zugriff mittels Benutzerkonten über E-Mail-Adresse und Kennwort als Standard

--- Einbindung der Data Rooms in das IT-Netzwerk des Anwenders möglich

--- Einfache Einbindung als Laufwerk (PC, MAC, LINUX)

--- Konfigurierbare, temporäre Upload-Konten für den zeitlich und volumentechnisch beschränkten Zugriff durch Drittbenutzer / Geschäftspartner des Anwenders zum Hochladen von Dateien

--- Sämtliche Events, wie IPs, Zugriffe, Änderungen, Uploads etc. werden optional revisionssicher protokolliert

--- Administration und Dateiaustausch über die Webapplikation (WebGUI)

--- Mehrsprachiges Interface: Deutsch, Englisch, Spanisch (Sprachen sind erweiterbar)

--- Backup kompletter Data Rooms manuell durch Data Room Admins oder Data Space Admins möglich oder automatisiert (über einen sogenannten Backup-Agent)

--- Verschlüsselung von Data Rooms mittels clientseitiger Verschlüsselung.

SDS ermöglicht die Klassifizierung von Vertraulichkeits-Stufen beim Upload in

--- öffentlich

--- nur für interne Nutzung

--- vertraulich und

--- streng vertraulich.

Der Benutzer kann hierzu die Klassifizierung innerhalb seines Data Rooms bei der Verarbeitung der gewünschten Datei auswählen. Die Begrifflichkeiten sind dabei mittels eines Hinweistextes im Mouse-Over erklärt. Die Klassifizierung wird durch den SDS unterstützt, indem der Anwender eine Warnung erhält, sofern er eine als nicht öffentlich eingestufte Datei freigeben will. Ferner kann eine als nicht öffentlich klassifizierte Datei ohne das dazugehörige Kennwort nicht freigegeben werden. Zudem erhält der Benutzer einen Hinweis, sofern andere Zugriffsrechte auf einen Datenraum herrschen, in welchen er eine streng vertrauliche Datei kopieren möchte. Des Weiteren gibt die Dokumentklassifikation dem Data Space Administrator die Möglichkeit, entsprechende Freigaben zu filtern und zu verwalten.

Über einen Upload Account können Benutzer ein zeit- und mengenbegrenztes Upload-Recht auf einen definierten Data Room, einen Subroom oder Ordner für externe oder interne Benutzer gewähren. Dazu werden temporäre Accounts unter einem Aliasnamen angelegt, der als User-Name für den Upload verwendet wird.

Der befugte Zugriff auf Daten, die zum Mandanten im SDS gehören, wird über das Berechtigungskonzept sichergestellt.

Zusätzlich zu den Grundfunktionalitäten des SDS Online bietet der **SDS Dedicated** nachfolgende Besonderheiten:

--- Eine dediziert für den Anbieter bereitgestellte Storage-Umgebung

--- Ein dediziertes Kennwort für die Verschlüsselung der Storage Umgebung

--- Es ist ein Branding der Umgebung nach Vorgaben des Anwenders möglich

--- Es ist eine Active Directory-Anmeldung möglich

--- Der Zugriff aus dem Internet kann über eine beliebige Adresse im Rahmen der Domains des Anwenders über ein vorhandenes oder durch die SSP Europe GmbH zur Verfügung gestelltes SSL Zertifikat erfolgen.

Zusätzlich zu den Grundfunktionalitäten und den zu SDS Dedicated beschriebenen Möglichkeiten, bietet die **SDS Virtual Appliance** nachfolgende Besonderheiten:

--- Nutzung beim Anwender als Inhouse-Lösung möglich

--- Anbindung an den vom Anwender bereitgestellten Storage nach Vorgaben der SSP Europe GmbH

--- Nutzung im Housing Betrieb oder im Data Center des Anwenders.

8.1 Login und Authentisierung

Der Benutzer verbindet sich mittels SSL-gesicherter Verbindung zum Frontend (https://dataspace.ssp-europe.eu) und authentisiert sich mit Benutzername und Passwort.

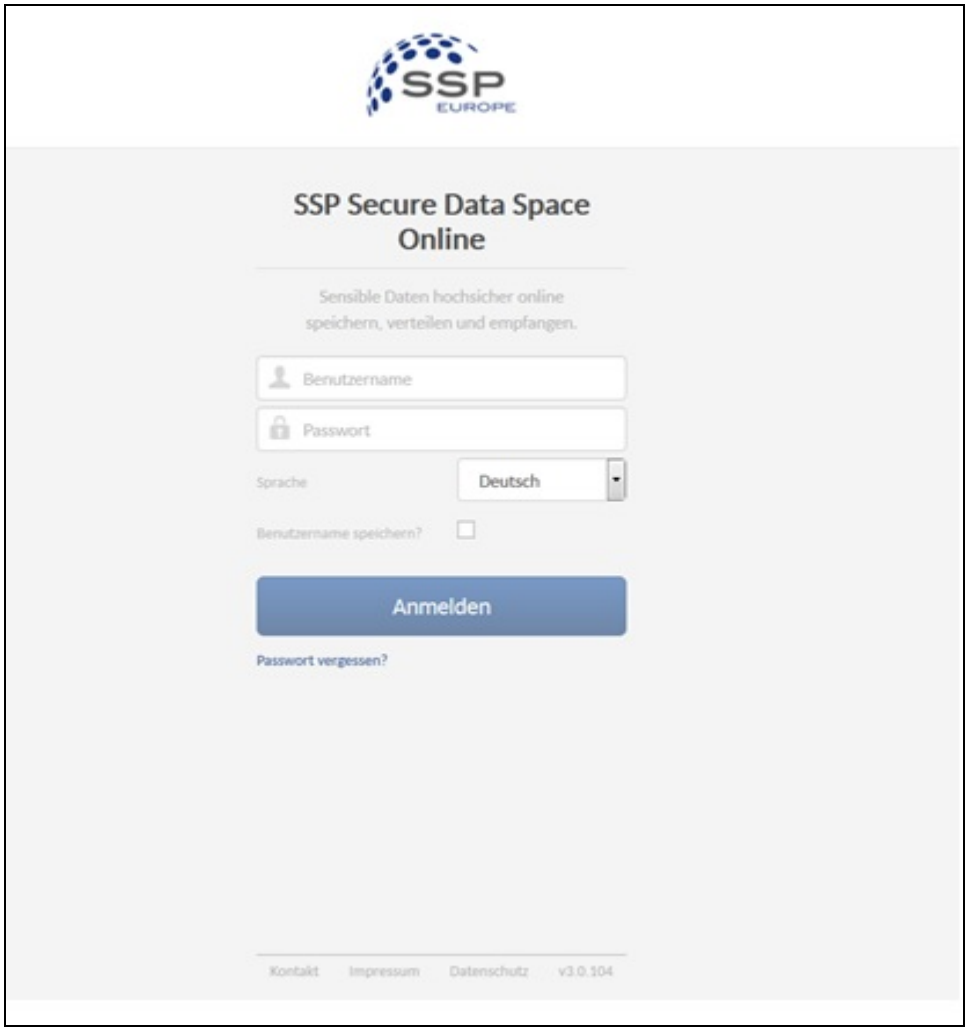

Abbildung 1: Login-Maske - Variante SDS Dedicated

Bei der erstmaligen Anmeldung am SDS muss das Passwort geändert werden. Es muss mindestens 8 Zeichen besitzen und aus Buchstaben und Ziffern bestehen, die automatisiert gegengeprüft werden. Dies ist als Minimalanforderung systemseitig vorgegeben. Der Anwender wird in einem Merkblatt zum Datenschutz darauf hingewiesen, den Passwortschutz zu nutzen. Das Merkblatt ist Vertragsbestandteil und innerhalb des Accounts des SDS abrufbar. Es ist allerdings möglich, dass auf Wunsch der Anwender des SDS Virtual Appliance sowie des SDS Dedicated eine andere Konfiguration der Passwortkonvention implementiert wird.

Bei Falscheingaben des Passwortes wird der Account gesperrt.

Die Benutzernamen werden im Klartext in der Datenbank gespeichert, die Passwörter werden verschlüsselt und als Hash abgelegt. SDS verwendet bcrypt inklusive Salting und behandelt die Authentisierung nach folgendem Konzept:

1. Passwort wird auf der Loginseite eingegeben.
2. Dieses wird über SSL an den Server übertragen.
3. Etwaige SQL Injection/Cross Site Scripting Versuche werden herausgefiltert und protokolliert.
4. Es wird geprüft, ob der Username existiert.
5. Falls nein, erfolgt die Standardmeldung: „Username/Kennwort falsch“ und der Abbruch.
6. Das Passwort wird aus historischen Gründen zuerst mit MD5 gehasht.
7. Anschließend wird der Hashwert um einen individuellen Salt-Wert (mit div. Parametern) sowie einem systemweiten Pepper-Wert (in der Server-Konfiguration hinterlegt) ergänzt und mit SHA-1 gehasht. Dies ist ein Normalisierungsvorgang, da die eigentliche Hashfunktion – bcrypt – maximal 55 Byte Input akzeptiert.
8. Dieser SHA-1-Hash wird um ein bsalt (spezieller Salt-Wert von bcrypt) ergänzt und mit bcrypt sicher gehasht.
9. Dieser bcrypt-Hash wird dann mit dem der Datenbank verglichen.
10. Bei Übereinstimmung wird der User eingeloggt, falls nicht, erfolgt die Standardmeldung: „Username/Kennwort falsch“, Abbruch.

Wird die Standard-Authentisierung verwendet, wird das Passwort mittels bcrypt/Salting in der Datenbank abgelegt. Das Rücksetzen des Passwortes geschieht über die E-Mail-Adresse, an welche ein auf 24h-Gültigkeit begrenzter Link gesendet wird. Hier kann der Benutzer sein Passwort selbst zurücksetzen.

Bei den Varianten SDS Dedicated und SDS Virtual Appliance ist auf Wunsch des Anwenders auch eine Authentifizierung durch die Anbindung an ein Active Directory (AD) möglich. Der Benutzer meldet sich dann mit seinem AD-Benutzernamen und dem -Passwort an. Der Authentisierungsprozess bei Standardinstallation, bei dem sich Benutzer mit den in der Datenbank gespeicherten Login-Daten anmelden können, bleibt ebenfalls möglich. Somit ist sichergestellt, dass auch externe Benutzer, die kein Konto im AD besitzen, den SDS nutzen können. Alternativ kann die Authentisierung auch gegen einen Radius Server per Token erfolgen. Der Benutzer meldet sich mit seinem Benutzernamen, einer PIN und einem durch den Token generierten Einmalpasswort an. Die

Anmeldung mittels der in der Datenbank gespeicherten Login-Daten wird in diesem Fall unterbunden.

Nach der Anmeldung gelangt der Benutzer auf ein Dashboard als Startseite:

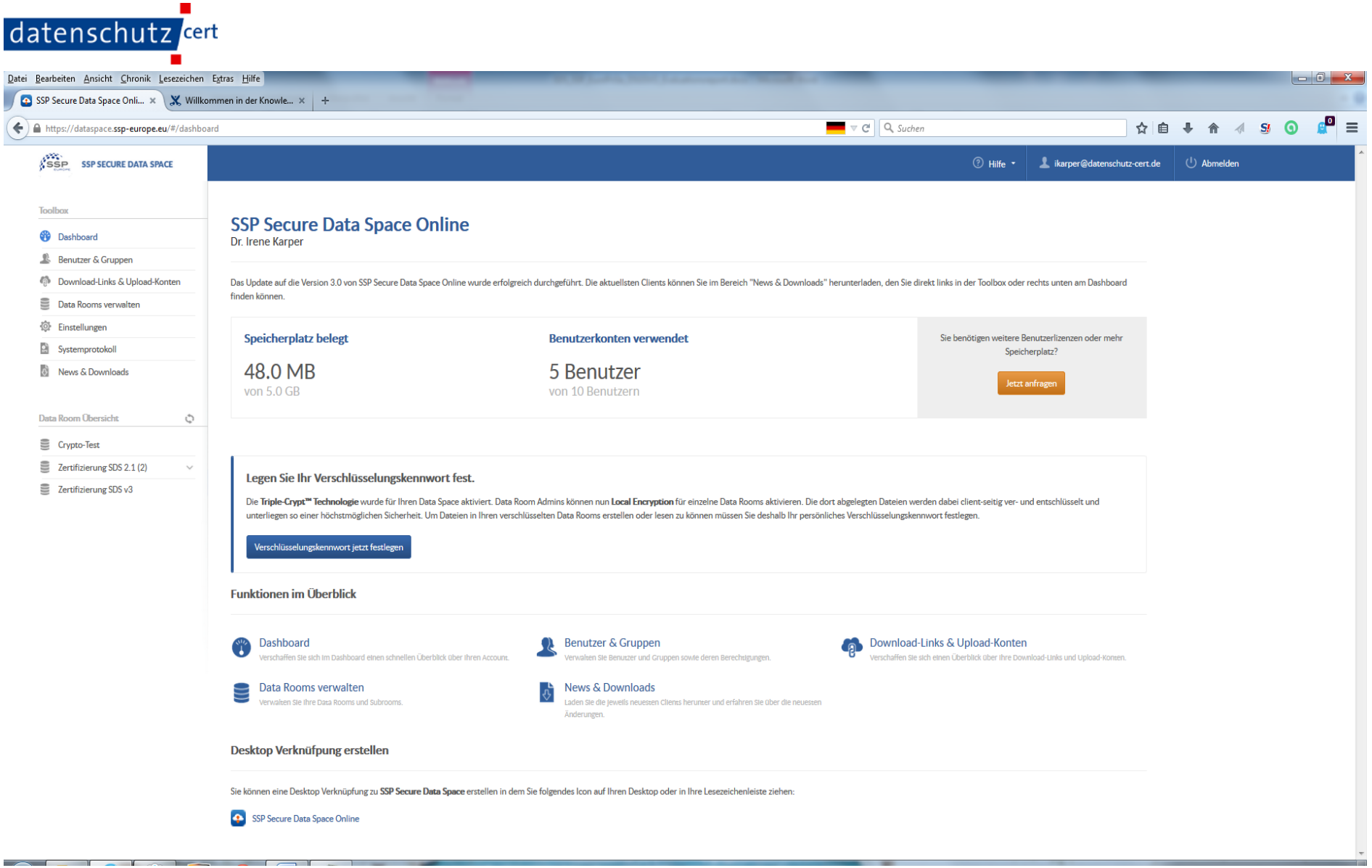

Abbildung 2: Dashboard – hier für Data Space Admins

8.2 Verschlüsselung

Die Datenübertragung zwischen Server und Client erfolgt mittels SSL Verbindung und einem zum Auditzeitpunkt bis 2018 gültigen Zertifikat. Die SSP Europe GmbH bietet auf Wunsch des Anwenders Verschlüsselungsgrade bis zu 256 Bit an, sofern die eingesetzten Webbrowser und Betriebssysteme dies unterstützen.

Die Datenbank selbst ist nicht verschlüsselt. Daten werden aber auf einem LUKS-verschlüsselten Datenträger innerhalb des gesicherten Rechenzentrums gespeichert, so dass hierdurch ein zusätzlicher Diebstahlschutz gewährleistet wird. Optional können Daten vor Übertragung in den Data Room clientseitig verschlüsselt werden. Bei einer Verschlüsselung wird der gesamte Data Room verschlüsselt, was nur im leeren Zustand möglich ist. Jeder Benutzer wird bei erstmaliger Nutzung eines Data Spaces mit aktiviertem „Triple-Crypt“ aufgefordert, ein Verschlüsselungs-Passwort zu wählen, aus dem ein Schlüsselpaar (RSA-2048) generiert wird. Dieses Schlüsselpaar kommt in allen verschlüsselten Data Rooms dieses Data Spaces zum Einsatz. Für jedes Dokument, das nun hier abgelegt wird, wird ein zufälliger symmetrischer Schlüssel (AES256) generiert, mit dem das Dokument unter Verwendung des Galois Counter Mode (GCM) verschlüsselt wird. Dieser symmetrische Schlüssel wird anschließend mit dem öffentlichen Schlüssel aller für diesen Data Room berechtigten Benutzer verschlüsselt und zusammen mit den verschlüsselten Daten in der Datenbank abgelegt. Somit können alle Benutzer, die für einen Data Room Leseberechtigung haben, alle Daten in diesem Data Room lesen, auch wenn diese verschlüsselt sind. Sollen diese nur für einen Benutzer lesbar sein, ist es möglich einzelne Sub-Rooms anzulegen, für die nur einzelne Benutzer Leseberechtigung haben.

Zum Lesen einer verschlüsselten Datei wird der Benutzer aufgefordert, sein Verschlüsselungs-Kennwort einzugeben, womit der private Schlüssel freigegeben wird, um den symmetrischen Schlüssel entschlüsseln und verwenden zu können.

Der Ver- und Entschlüsselungsvorgang wird per JAVA Script oder Java Applet im Browser des SDS-Benutzers am Client durchgeführt. Die Keys werden aus der Datenbank des SDS angefordert und im Speicher des Clients vorgehalten.

Über diese Kombination und dieses Verfahren ist bei durch den SDS Benutzer aktivierten, clientseitigen Verschlüsselung zu keinem Zeitpunkt eine Datei unverschlüsselt auf den SDS Backend-Systemen vorhanden und somit auch durch keinen Administrator der SSP Europe GmbH einsehbar, auch nicht auf dem Transportweg.

SDS bietet die Möglichkeit für den Notfall Rescue Keys einzurichten. Wenn Triple-Crypt aktiviert wird, hat der Data Space-Admin die Möglichkeit, einen Data Space Rescue Key einzurichten. Wird ein neuer Data Room angelegt, so hat der Data Room-Admin die Möglichkeit zu entscheiden, ob für diesen Data Room der Data Space Rescue Key als Notfallschlüssel verwendet werden soll, ob ein eigener Data Room Rescue Key erzeugt und verwendet werden soll oder ob es keinen Rescue Key für diesen Data Room geben soll.

Die Rescue Keys sind technisch gesehen Schlüsselpaare für asymmetrische Verschlüsselung und unterscheiden sich nicht von den Nutzer-Schlüsselpaaren.

Der private Schlüssel ist über ein langes und komplexes Passwort gesichert, welches von der entsprechenden Rolle (Data Space-Admin oder Data Room-Admin) durch organisatorische Maßnahmen geeignet geschützt wird.

Sämtliche symmetrischen File-Keys eines Data Rooms werden, wenn ein Rescue-Key verwendet wird, mit allen öffentlichen Schlüssel der berechtigten Nutzer und des entsprechenden Rescue-Keys verschlüsselt und in der Datenbank abgelegt.

Bei Verwendung eines Data Space Rescue Keys ist durch das Berechtigungskonzept sichergestellt, dass ein Data Space Admin auch bei Kenntnis des Data Space Rescue Keys nur auf Daten zugreifen kann, die für ihn durch den jeweiligen Data Room Admin freigegeben worden sind.

Die Rescue Keys dienen als Sicherheitsanker, für den Fall, dass alle Benutzer eines Data Rooms ihre Verschlüsselungs-Passwörter vergessen haben. Mit Hilfe des Rescue Keys sind die Daten dann noch entschlüsselbar. Wird kein Rescue-Key verwendet, sind die Daten nicht mehr zu entschlüsseln.

8.3 Datenlöschung

Löschvorgänge werden zwischen der SSP Europe GmbH und dem Anwender vertraglich geregelt. Primärdaten können vom Anwender selbst gelöscht werden oder bereits bei Erstellung mit einem Löschdatum (Ablaufdatum) versehen werden. Im letzteren Fall werden die markierten Dateien nach Ablauf der Löschfrist per cronjob vollständig gelöscht. Zugehörige Sekundärdaten wie Änderungsprotokolle bleiben bis zur Kündigung von SDS durch den Anwender erhalten.

Logdaten, die einer Angriffserkennung dienen, werden, sofern nicht anders beauftragt, nach 7 Tagen gelöscht. Auf Wunsch des Anwenders können Logdaten länger vorgehalten und bereitgestellt werden. Hierfür ist ein gesonderter Auftrag erforderlich. Die übliche Aufbewahrungsfrist beträgt dann in der Regel drei Monate.

Bei Kündigung erhält der Anwender die Möglichkeit, sämtliche Daten per zip-Archiv zu exportieren. Benutzer, die lediglich ein Test-Account nutzen, können ihre Daten jederzeit selbst löschen.

8.4 Audit Log

Über ein Audit Log können Data Space Administratoren Transaktionen suchen, einsehen und nachvollziehen, die mandantenbezogen ausgeführt wurden. Das Audit Log ist systemseitig nicht veränderbar und kann nur gelöscht werden, indem eine Löschung des Mandanten erfolgt.

8.5 Komponenten

Der SDS umfasst folgende redundant ausgelegte Komponenten:

--- VMware-HA Reverse Proxies
--- VMware-HA Applikationsserver
--- VMware-HA Datenbankserver
--- VMware-HA gespiegelte Storageserver.

Der Zugriff auf den SDS erfolgt über gängige Webbrowser.

SDS kann dabei auch über mobile devices (Smartphones, Tablets) abgerufen werden. **Weder Apps noch mobile devices sind Bestandteil des hier untersuchten ToE.**

Ferner kann SDS über die Schnittstelle WebDAV als Laufwerk eingebunden werden, wobei dann die clientseitige Verschlüsselung nicht zur Verfügung steht. Der Anwender wird im Datenschutzmerkblatt daher sensibilisiert, vertrauenswürdige Clients zu nutzen. Insbesondere wird er auf die Wahrung von Berufsgeheimnissen und die mögliche Strafbarkeit bei rechtswidriger Offenbarung hingewiesen.

Für die Clientseitige Verschlüsselung werden JavaScript Dateien und ein Java Applet im Browser ausgeführt, welche über den verschlüsselten TLS-Kanal vom Server an den Browser übertragen werden. Die Integrität dieser Dateien lässt sich an Hand der folgenden Prüfsummen überprüfen.

```
forge.bundle.js
SHA256:
450b57f7bf4d334d3fad9361bc5d7c53692e269aa279c7719cd28a31c3da0
d6b

forge.min.js
SHA256:
e5cf57d8300753f633b67cf1978464695940dc99941ae6519a2241d080acd
4d4

prime.worker.js
SHA256:
1a485ddf5763ad8ea862cf939911a1702712981fe5242e85e60ccf1afff66
1fe

sdsConfig.js
SHA256:
329225526c4758c9423c3e9a7747ea256f28aac9eef0d32f22a68cf557ed5
225

sdsCrypto.js
SHA256:
c6bf21633b3256130ad9d4a1cea91cbc0c4d0a72b1ba42334e4465da13c26
fb3
```

Das Java-Applet (FsHelper_2.1.5.jar) ist darüber hinaus digital signiert.

8.6 Schnittstellen

Der *SDS*-Server bietet eine umfassende JSON-REST-API an, über die sämtliche Funktionalität der Software abgebildet ist. Somit ist Funktionalität und Logik des Programmablaufes aus den Client-Anwendungen in den Server verlagert worden. Diese API stellt inzwischen die einzige Schnittstelle zu jeglichen Anwendungen dar, die an den *SDS* angebunden werden. Somit gelten automatisch für alle Clients

die gleichen Sicherheitsanforderungen und -mechanismen sowie datenschutzrelevanten Komponenten.

Die Clients selbst tragen nur noch diejenige Logik in sich, die sie für die Darstellung der bereitgestellten Informationen auf dem Bildschirm des Benutzers benötigen oder die eine Integration des *SDS* in bestehende Umgebungen, Systeme und Workflows ermöglichen – und natürlich die Funktionalität, die für die client-seitigen kryptographischen Operationen benötigt wird.

Die WebUI – der Standard-Client, auf den Benutzer zurückgreifen können und der einzige Client, der von Hause aus den vollständigen Funktionsumfang bereitstellt – wird ebenfalls in der Umgebung der SSP Europe GmbH gehostet. Allerdings besitzt die WebUI keine server-seitige Logik (wie es bei klassischen Web-Anwendungen z.B. in PHP oder JSP der Fall wäre), sondern führt die gesamte Darstellung der Oberfläche in Form von JavaScript im Browser des Clients aus. Dieser kommuniziert direkt mit der API, um die dafür benötigten Daten zu beziehen.

Sämtliche weitere Schnittstellen, die nicht innerhalb des Scopes der Zertifizierung liegen, werden ebenfalls über die JSON-REST-API realisiert. Dabei wurde für die WebDAV- und SFTP-Schnittstellen ein Proxie entwickelt, die die Kommunikation mit den entsprechenden Clients über das bereitgestellte Protokoll auf die API mappen.

Der Secure Data Space enthält folgende Schnittstellen:

- --- https-Zugriff auf das WebUI
- --- interne MySQL-Datenbankschnittstelle
- --- Java/IO Funktion zum local mount und zur Dateiablage
- --- smtp für Mailversand (Versenden von Links zum Download)
- --- API-Schnittstelle
  - --- sftp-Schnittstelle via API
  - --- WebDav Schnittstelle (zur Einbindung als Laufwerk beim Anwender) via API
  - --- Schnittstelle für Mobile Apps und Drive Letter

8.7 Berechtigung und Rollen

Berechtigungen können entsprechend der Rollen und Funktionen abgestuft und detailliert zugewiesen werden:

ROLLENKONZEPT	DATA SPACE ADMIN Zentrale Adminfunktion	DATA ROOM ADMIN Admin für Data Room	DATA ROOM USER Typischer Benutzer	LINK EMPFÄNGER Temporärer User
Festlegung globaler Systemeinstellungen	+	–	–	–
Globale Benutzerverwaltung	+	–	–	–
Anlegen von neuen Data Rooms und Zuweisung von Data Room Admins	+	–	–	–
Rechteverwaltung innerhalb der Data Rooms	–	+	–	–
Benutzerverwaltung innderhalb der Data Rooms	–	+	–	–
Verschlüsselung von Data Rooms	–	+	–	–
Hochladen, Löschen und Versenden von Dateien	+	+	+	–
Nutzen von Down- und Uploadlinks	+	+	+	+

Abbildung 3: Rollenkonzept

8.7.1 Data Space Admin

Der Data Space Admin besitzt die zentrale Administrationsfunktion des Anwender-Accounts zum SDS mit einem Gesamtüberblick sowie allen Rechte auf die Data Space Rooms und Subrooms sowie die User-/Rechteverwaltung.

8.7.2 Data Room Admin

Der Data Room Admin ist der Administrator des jeweiligen Data Rooms, hat einen Überblick über die Benutzer, vergibt die Benutzerrechte (Upload, Löschen, Data Room Admin), kann Subrooms anlegen und bearbeitet Zuweisungen zu seinen Data Rooms (nicht zugewiesene Benutzer hinzufügen, hinzugefügte Benutzer entfernen). Er kann gleichzeitig in verschiedenen Data Rooms / Subrooms Data Room Admin oder Data Room User sein. Mit der Version 3.0 des SDS hat zudem jeder Data Room Admin nun automatisch die Möglichkeit, mit wenigen Klicks in seinen Räumen die clientseitige Verschlüsselung zu aktivieren.

8.7.3 Data Space User

Der Data Space User ist eine typische Benutzerrolle des Data Room. Dieser kann in seinem Account Dateien hochladen, löschen und Downloadlinks versenden (je nach zugeteilten Rechten). Der Data Space User kann – je nach Anforderung beim Anwender - zugleich die Rolle eines Data Room Admin innehaben.

8.7.4 Link-Empfänger und Upload Konto

Diese Rolle beschreibt die Nutzer der Downloadlinks bzw. die Nutzer des Upload-Kontos, welche keinen eigenen Account bei dem SDS besitzen müssen. Hervorzuheben ist, dass die Links aus einer zufälligen Zeichenkombination bestehen, so dass keine Rückschlüsse anhand der Nummerierung o.Ä. möglich sind.

Neu mit der Version 3.0 des SDS ist, dass die Länge der Freigabelinks vergrößert wurde, um das Risiko des Erratens zu minimieren. Sie erhalten nun anstelle von

10 Stellen (a-z) 32 Stellen (A-Z, a-z, 0-9). Es gibt nunmehr 62^{32} (Größenordnung: 10^{57}) unterschiedliche Links, die darüber hinaus zusätzlich (wie gehabt) mit einem Passwort geschützt werden können.

Weiterhin ist jetzt deutlich einfacher, unterschiedliche Freigabelinks (mit unterschiedlichen Passwörtern und Ablaufdaten) für die gleiche Datei anzulegen. Somit erhalten unterschiedliche Benutzer unterschiedliche Links und müssen nicht das gleiche Passwort erfahren (das sie möglicherweise wiederverwenden).

Die maximale Anzahl an Downloads eines Freigabelinks kann festgelegt werden. Möchte man eine sensible Information teilen, so kann man die maximale Anzahl auf *1* festlegen. Damit werden nach dem ersten Aufruf die Daten wieder unzugänglich. Sollte dem Empfänger der Download nicht ermöglicht werden, so kann man in diesem Fall feststellen, dass die Informationen wohl unberechtigt heruntergeladen wurden und somit als kompromittiert gelten müssen.

8.8 Rechtsgrundlagen der Datenverarbeitung im SDS

Die für den SDS einschlägigen Rahmenvorgaben finden sich in dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H), der Datenschutzverordnung (DSVO)[2] Schleswig-Holstein sowie den Bestimmungen des Bundesdatenschutzgesetz (BDSG) [3] und des Telemediengesetzes[4].

Zudem sind die Auslegungshilfen der Datenschutzaufsichtsbehörden und Rechtsprechung zu beachten. Etwa sind hierzu das Working Paper No. 196 der Artikel-29-Datenschutzgruppe („*Opinion 05/2012 on Cloud Computing*")[5] und die „*Orientierungshilfe – Cloud Computing*" der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[6] zu nennen.

Die Anwendungsbereiche des SDS und deren spezialgesetzliche Grundlagen für den Anwender können weder abschließend aufgeführt noch umfassend geprüft werden. Um dennoch ein vergleichbares datenschutzrechtliches Schutzniveau annehmen zu können, wurde seitens der Auditoren davon ausgegangen, dass mittels des SDS auch besondere personenbezogene Daten verarbeitet werden können. Diese Daten unterliegen einem hohen datenschutzrechtlichen Schutz, der für die Auditierung den Prüfmaßstab bildete. Die Prüfung erfolgte dabei am Beispiel einer Archivierung von Patientendaten, die als Gesundheitsdaten diesem besonderen Schutz unterfallen.

Wesentliche Ausprägung des Patientendatenschutzes ist der Grundsatz der ärztlichen Schweigepflicht, welcher eine der ältesten bekannten Datenschutzbestimmungen darstellt[7]. Er ist im deutschen Recht, welches hier

---

[2] Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten
v. 05.12.2014, GVOBl Schl.-H. 2013, S. 554ff.
3 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist.
[4] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 2 Absatz 16 des Gesetzes vom 1. April 2015 (BGBl. I S. 434) geändert worden ist.
[5] Abrufbar unter https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/WP169_CloudComputing.pdf
[6] Vom 09.10.2014, Version 2.0, abrufbar unter https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf .
[7] Zurückgehend auf den Hippokratischen Eid, ca. 400 v. Chr.: „*Was immer ich sehe und höre bei der Behandlung oder außerhalb der Behandlung im Leben der Menschen, so werde ich von dem, das niemals nach draußen ausgeplaudert werden soll, schweigen, indem ich alles Derartige als solches betrachte, das nicht ausgesprochen werden darf*".

beispielhaft geprüft wird, durch § 203 Strafgesetzbuch (StGB)[8] und § 9 der (Muster)-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä)[9] geregelt. Damit zusammenhängend ist zudem ein Beschlagnahmeschutz zu gewähren, wie er sich aus § 97 der Strafprozessordnung (StPO)[10] ergibt.

Soweit das Gesundheitswesen keine spezielleren Regelungen vorsieht, gilt für nicht-öffentliche Stellen ergänzend das BDSG als allgemeineres Gesetz. Für den Einsatz durch öffentliche Stellen Schleswig-Holsteins gilt das LDSG S-H. Die DSVO regelt die Dokumentation automatisierter Verfahren bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 3 Abs. 1 LDSG S-H) sowie deren Tests und die Freigabe dieser Verfahren. Für den SDS kam es daher auf die Prüfung der Dokumentationen, Tests und Freigabeverfahren an.

Hervorzuheben ist, dass die gesetzlichen Vorgaben bei korrekter Anwendung des SDS durch den Anwender eingehalten werden können.

8.9 Identifikation der Datenarten

Welche Daten an den SDS übertragen werden, hängt vom Anwender ab; diese können personenbezogen oder -beziehbar sein, müssen es aber nicht. Aufgrund der individuellen Anwendung können die Daten nicht abschließend aufgeführt werden. Beispielhaft wurde für das Audit allerdings davon ausgegangen, dass es sich um Gesundheitsdaten handelt, so dass ein hohes Datenschutzniveau umgesetzt sein muss. Weiterhin sind Benutzerdaten als Primärdaten anzusehen, insbesondere die E-Mail-Adresse, die als Login verwendet wird sowie Anrede und Vor- und Nachname, welche im Dashboard angezeigt werden.

Neben dem Audit-Log gibt es zudem verschiedene Protokolldateien, die im System des SDS verarbeitet werden. Der Secure Data Space schreibt jede Benutzeraktion in sein Systemlog mit, welches über das Web Frontend eingesehen werden kann. Dieses wird in der SDS Datenbank gespeichert. Am System selbst werden vom Webserver ebenfalls Logdateien angelegt. Hier werden die (auf die weniger signifikante Hälfte reduzierten) IP Adressen der Benutzer und die Zugriffszeit geloggt. Der Application Server legt die Log-Datei „catalina.out“ an. Diese enthält Informationen über den Zustand des Servers und Operationen (durch WebDAV), aber keine personenbezogenen oder personenbeziehbaren Daten. Ferner kann die Protokollierung der vollständigen IP-Adressen in der Datenbank vom Anwender aktiviert werden. Diese Einstellung ist nur in der SDS Dedicated- oder der SDS Virtual Appliance-Version verfügbar. Sollten IP-Adressen so gelogged werden, erkennt der Benutzer dies, indem im Dashboard des SDS nicht nur das Datum seines letzten Logins angezeigt wird, sondern auch die dazugehörige IP-Adresse.

8.10 Einsatzumgebung

[8] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 21. Januar 2015 (BGBl. I S. 10) geändert worden ist.
[9] MBO-Ä 1997 in der Fassung der Beschlüsse des 114. Deutschen Ärztetages 2011 in Kiel. Die MBO-Ä des Landes Schleswig-Holstein ist gleichlautend.
[10] Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 3 des Gesetzes vom 21. Januar 2015 (BGBl. I S. 10) geändert worden ist.

Sofern der SDS Virtual Appliance in einer IT-Systemlandschaft des Anwenders eingesetzt wird, hängt die Sicherheit von den Anforderungen ab, die der Anwender hier umsetzt. Hervorzuheben ist, dass der Anwender im Datenschutzmerkblatt ausreichend sensibilisiert wird, eine sichere Einsatzumgebung herzustellen.

Zur Einsatzumgebung bei der SSP Europe GmbH bzw. des von ihr beauftragten Rechenzentrums gehören ein Backend Server, ein Frontend Server, ein Database Server sowie ein Reverse Proxy System. Standorte, Webseiten und öffentliche Netze der SSP Europe GmbH werden regelmäßig Sicherheitsüberprüfungen bzw. externen Schwachstellenscans unterzogen. Hervorzuheben ist, dass die SSP Europe GmbH im Rahmen ihres gemäß ISO/IEC 27001:2013 zertifizierten ISMS ein Risikomanagement betreibt. Ein Risikomanagementhandbuch sowie eine detaillierte Risikoanalyse wurden seitens der Auditoren eingesehen. Tests des SDS und seiner Komponenten werden in einem Entwicklerhandbuch beschrieben. Für Tests nutzt die SSP Europe GmbH eine separate Testumgebung. Tests werden per Tool dokumentiert.

Mit der Version 3.0 des SDS wurde eine online abrufbare Knowledge-Base eingeführt, die unter der Adresse https://kb.ssp-europe.eu/pages/viewpage.action?pageId=10945501 erreichbar ist. Auf diesem Portal können technische Aspekte des SDS als Online-Hilfe direkt aus dem dahinter eingebundenen Benutzerhandbuch aufgerufen werden. zudem sind hier u.a. Benutzerhandbücher als pdf-Version zur alten und neuen Version des SDS abrufbar.

Die nachfolgende Abbildung illustriert Komponenten und Datenfluss:

9. Modellierung des Datenflusses

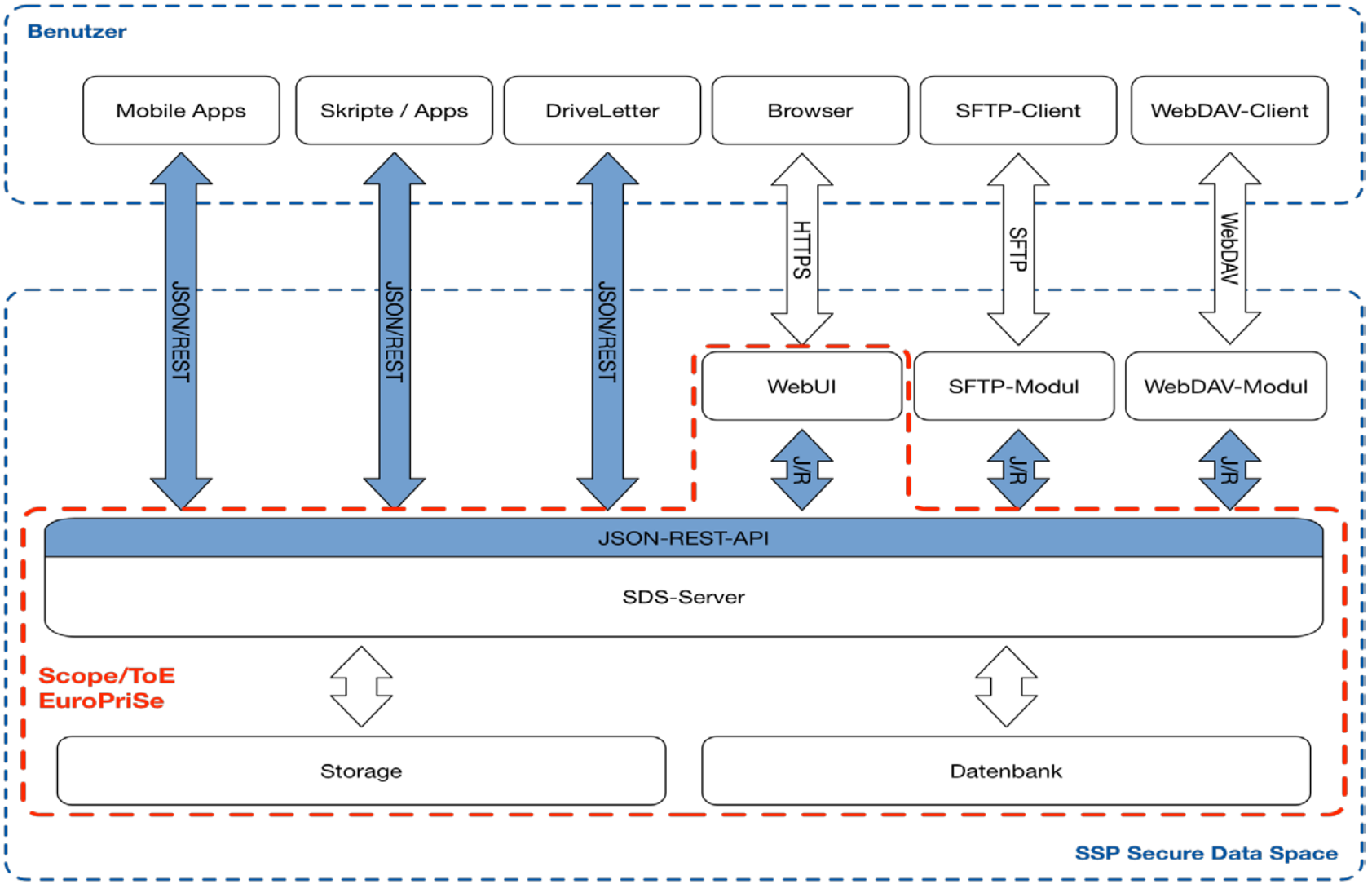

Abbildung 4: Datenfluss

10. Version des Anforderungskatalogs

Version 2

11. Zusammenfassung der Prüfergebnisse

Die Prüfergebnisse im Einzelnen werden wie folgt zusammengefasst:

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

A23 Sonstige Anforderungen	**nicht anwendbar**
Anforderungsprofil für Profildaten (B) nach DSGSVO	**Bewertung DSGSVO**
B1 Datenvermeidung und Datensparsamkeit	**angemessen**
B2 Zweckbindung	**angemessen**
B3 Nicht-Verkettbarkeit	**angemessen**
B4 Transparenz	**vorbildlich**
B5 Rechtsgrundlagen	**angemessen**
B6 Zweckbindung	**angemessen**
B7 Aufbewahrungsfristen	**angemessen**
B8 Physikalische Sicherung	**angemessen**
B9 Zugriffsschutz	**angemessen**
B10 Ermittlung / Sichtbarkeit der Protokolldaten	**angemessen**
B11 Technische Umsetzung der Speicherfristen	**angemessen**
B12 Unzulässige Verkettung	**angemessen**
B13 Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	**angemessen**
B14 Selektive Löschung von Einzeldaten, Beauskunftung, Berichtigung, Sperrung, Einwand	**angemessen**

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

SDS enthält folgende, den Datenschutz fördernde Funktionen:

Die Vertraulichkeit der Daten wird durch ein Berechtigungskonzept sichergestellt, das die Vergabe sehr differenzierter Zugriffsrechte ermöglicht.

SDS bietet dem Benutzer mit der clientseitigen Verschlüsselung die Möglichkeit, Daten absolut vertraulich per SDS zu speichern.

Durch die Vermeidung schwacher Algorithmen bei der Verwendung von TLS für die Kommunikationsverschlüsselung, wird ein hohes Maß an Vertraulichkeit erreicht.

Organisatorische und technische Maßnahmen, die der Auftragnehmer zur Datensicherheit und zum Datenschutz trifft, gehen über die gesetzlichen

Anforderungen hinaus. Der Auftragnehmer sensibilisiert den Anwender in vorbildlicher Weise auf die Einhaltung des Datenschutzes, u.a. durch ein Datenschutzmerkblatt. Das Rechenzentrum weist ein hohes Maß an physikalischer Sicherheit aus und ist zertifiziert.

13. Votum der Auditoren

Der Secure Data Space in den Varianten Secure Data Space Onlinel, Secure Data Space Dedicated und Secure Data Space Virtual Appliance in der Version 3.0 setzt die Anforderungen gemäß DSGSVO angemessen um. Die Auditoren haben daher der Zertifizierungsstelle die Gütesiegelvergabe empfohlen.

Bremen, 10.06.2015

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

Ralf von Rahden
datenschutz cert GmbH