Kurzgutachten

für das IT-Produkt und den IT-basierenden Service

Secure Data Space

1. Name und Version des IT Produkts und IT-basierenden Services:

Secure Data Space in den Varianten

- Secure Data Space Online
- Secure Data Space Dedicated
- Secure Data Space Virtual Appliance.

Version: 3.0

Funktionaler Status: Juni 2015.

Es handelt es sich um ein IT-Produkt und um einen IT-basierenden Service.

2. Hersteller oder Anbieter des IT Produkts und IT-basierenden Services:

SSP Europe GmbH
Maximilianstraße 35a
80539 München, Deutschland
als Hersteller, Anbieter und Provider des IT Produkts und IT-basierenden Services.

Kontakt: Herr Dan Jacob, Head of IT-Security Solutions of SSP Europe GmbH und Dr. Florian Scheurer, IT-Security Consultant of SSP Europe GmbH.

3. Zeitraum der Evaluation:

29.04.2015 bis 09.06.2015

4. EuroPriSe Experten, die das des IT Produkt und den IT-basierenden Services evaluiert haben:

Name der rechtlichen Expertin:	Dr. Irene Karper
Anschrift:	c/o datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen, Deutschland E-Mail: ikarper@datenschutz-cert.de
Name des technischen Experten:	Ralf von Rahden
Anschrift:	c/o datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen, Deutschland E-Mail: rrahden@datenschutz-cert.de

5. Zertifizierungsstelle:

Name:	EuroPriSe Certification Authority
Anschrift:	Joseph-Schumpeter-Allee 25 53227 Bonn Deutschland
E-Mail:	contact@european-privacy-seal.eu

6. Spezifizierung des Evaluationsgegensrtands (ToE):

SDS ist ein webbasierender, virtueller Datenraum (Data Room), in welchem Daten hochgeladen, gespeichert, verwaltet und ausgetauscht werden können. Der SDS ist für den gewerblichen B2B- Einsatz konzipiert. Die online per Webzugang zur Verfügung gestellten Verarbeitungskapazitäten des SDS sind als typische Cloud-Dienstleistung zu klassifizieren. Anwender sind Unternehmen, Organisationen oder öffentliche Stellen.

Anbieter ist die SSP Europe GmbH, welche die Entwicklung, Pflege und den Betrieb des SDS im Auftrag des Anwenders als Software as a Service (SaaS) am Standort München durchführt. Das Vertragskonvolut zwischen der SSP Europe GmbH und dem Anwender entspricht den gesetzlichen Vorgaben der Auftragsdatenverarbeitung. Das Informationsmanagementsystem der SSP Europe GmbH ist gemäß ISO/IEC 27001:2013 zertifiziert.

SDS wird im Unterauftrag der SSP Europe GmbH in einem Rechenzentrum der QSC AG am Standort in Nürnberg betrieben. Der hierzu vorliegende Vertrag wurde im Rahmen des Audits geprüft und entspricht den gesetzlichen Vorgaben der Auftragsdatenverarbeitung. Das Rechenzentrum ist gemäß ISO/IEC 27001:2005 zertifiziert. Die Angemessenheit der technisch-organisatorischen Sicherheitsmaßnahmen wurde darüber hinaus im Rahmen des Audits bewertet.

Diese Aspekte unterstützen die Anforderungen der Datenschutzaufsichtsbehörden zum Cloud Computing[1].

Der SDS ist im Internet unter https://dataspace.ssp-europe.eu erreichbar.

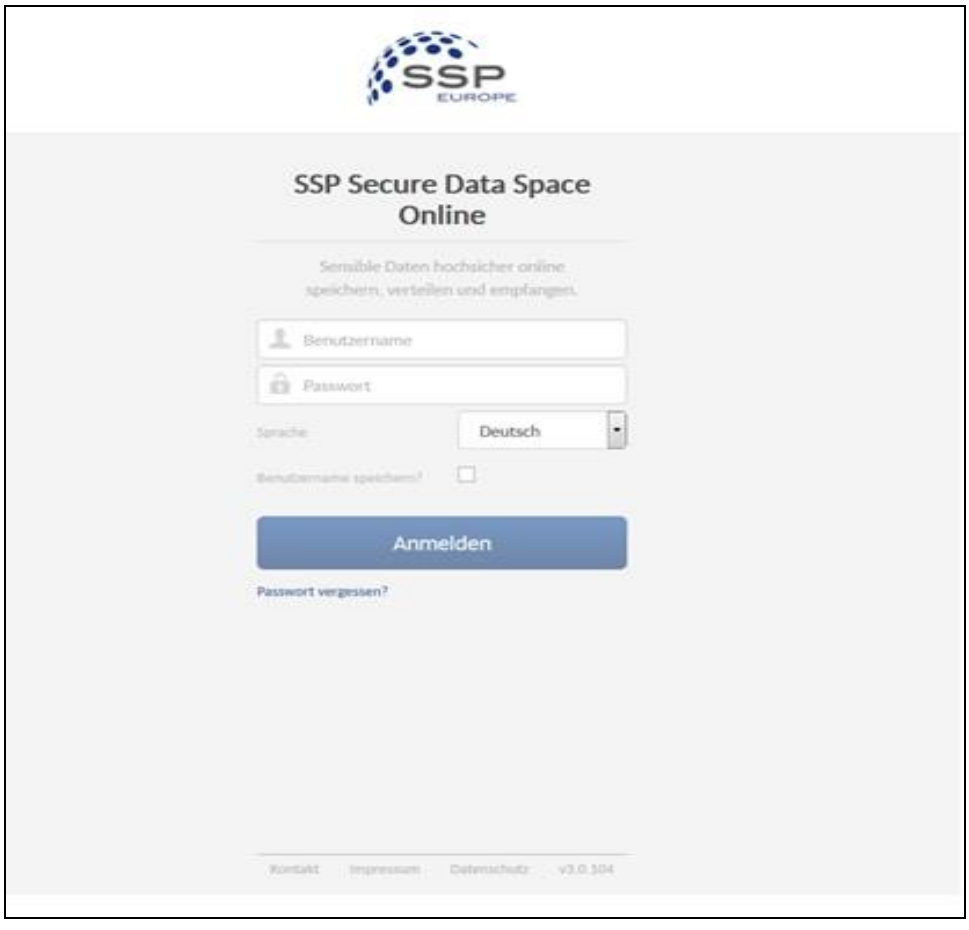


Abbildung 1: Login zum SDS

[1] Z.B. gemäß der „*Orientierungshilfe – Cloud Computing*“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder oder gemäß des Working Paper No. 196 der Artikel-29-Datenschutzgruppe (*„Opinion 05/2012 on Cloud Computing“).*

SDS wird in 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.

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 ein Softwarepaket, das einerseits vom Anwender in seiner eigenen Umgebung installiert und gehostet werden kann, andererseits als SaaS beauftragt werden kann.

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 sind für den Anwender im Benutzerhandbuch transparent dokumentiert. SDS ermöglicht neben den klassischen Funktionen eines Data Rooms (Dateien ablegen, hochladen, sortieren, austauschen, Berechtigungskonzepte erstellen, Daten verschlüsseln usw.) die Klassifizierung von Vertraulichkeits-Stufen beim Upload. 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 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 bietet der SDS Dedicated folgende 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 zum SDS Online und SDS Dedicated bietet die SDS Virtual Appliance:

- 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.

Zum ToE gehören die SDS-Komponenten

- Web-UI
- JSON-REST-API-Schnittstelle

- SDS-Server
- Management Database.

Nicht zum ToE gehören

- Der Einsatz von SDS über Smartphones und Tablets, sowie mobile Apps für SDS
- Die Einsatzumgebung beim Anwender
- die Hardwarebestandteile und das diesbezüglich verwendete Betriebssystem im Rechenzentrum
- die Lizenzierung und Vertriebsprozesse bei der SSP Europe GmbH
- die Unternehmensdarstellung unter http://www.ssp-europe.eu
- weitergehende Serviceleistungen der SSP Europe GmbH.

7. Generelle Beschreibung des IT Produkts und IT-basierenden Services:

Datenarten:

Welche Daten an den SDS übertragen werden, hängt vom Anwender ab; diese können personenbezogen oder -beziehbar sein. Aufgrund der individuellen Anwendung können die Daten nicht abschließend aufgeführt werden. Beispielhaft wurde für die Evaluation 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.

Verschlüsselung:

Die Datenübertragung zwischen Server und Client erfolgt mittels SSL Verbindung und einem zum Evaluationszeitpunkt 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 erst-maliger 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 Daten-bank 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 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 Rescue Key einzurichten. Wird ein neuer Data Room angelegt, so hat der 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 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.

Datenlöschung:

Löschvorgänge werden zwischen der SSP Europe GmbH und dem Anwender vertraglich geregelt. Primärdaten können vom Anwender selbst gelöscht 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 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.

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.

Komponenten:

Der SDS umfasst folgende redundant ausgelegte Komponenten:

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

Der Zugriff erfolgt über gängige Webbrowser. SDS kann dabei auch über mobile devices (Smartphones, Tablets) abgerufen werden. **Apps und mobile devices sind kein Bestandteil des ToE.**

Ferner kann SDS über die Schnittstelle WebDAV als Laufwerk eingebunden werden, dann allerdings ohne die clientseitige Verschlüsselung. Der Anwender wird im Datenschutzmerkblatt 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:  450b57f7bf4d334d3fad9361bc5d7c53692e269aa279c7719cd28a31c3da0d6b

forge.min.js
SHA256:  e5cf57d8300753f633b67cf1978464695940dc99941ae6519a2241d080acd4d4

prime.worker.js
SHA256:  1a485ddf5763ad8ea862cf939911a1702712981fe5242e85e60ccf1afff661fe

sdsConfig.js
```

SHA256: 329225526c4758c9423c3e9a7747ea256f28aac9eef0d32f22a68cf557ed5225

sdsCrypto.js

SHA256: c6bf21633b3256130ad9d4a1cea91cbc0c4d0a72b1ba42334e4465da13c26fb3

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

Schnittstellen und Berechtigungskonzept:

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

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 2: Rollenkonzept

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.

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.

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.

Der **Link-Empfänger** und das **Upload Konto** beschreiben Rollen der Nutzer der Downloadlinks bzw. 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.

8. Transnationale Aspekte:

Als webbasiertes System kann SDS weltweit eingesetzt werden. Es wird aktuell von Stellen angewandt, die Ihren Sitz in der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR) oder in Drittstaaten haben. Datenbank und Server befinden sich räumlich in der Bundesrepublik Deutschland und werden im Auftrag des Anwenders durch die SSP Europe GmbH geführt. Alle Komponenten des SDS sowie die dazugehörigen Wartungsleistungen werden innerhalb der Bundesrepublik Deutschland ausgeführt.

9. Tools, die vom Hersteller des IT Produkts und IT-basierenden Services verwendet wurden:

Keine.

10. Ausgabe des EuroPriSe-Kriterienkataloges, der genutzt wurde:

Version aus November 2011.

11. Evaluationsergebnisse:

Der Secure Data Space ist nach Ansicht der Evaluatoren ein tatsächlich sicherer Datenraum, der den Anforderungen des Datenschutzes und der IT-Sicherheit vollumfänglich Rechnung trägt.

Informationen über den SDS sind für Anwender schnell zugänglich, aussagekräftig und bieten weiterführende Hinweise zur optimalen, datenschutzfreundlichen Konfiguration und zu den systemseitig verarbeiteten Daten.

Der Anwender des SDS steht hierbei in der Verantwortung, die datenschutzrechtlichen Anforderungen zu beachten und beim Hochladen, Speichern, Nutzen oder Weiterleiten von Daten mittels des SDS umzusetzen. Die datenschutzrechtlichen Anforderungen können je nach Anwender und dessen Aufgabenumfeld variieren. Der SDS unterstützt ihn bei der Einhaltung dieser durch Hinweise und Empfehlungen. Unter Beachtung dieser Hinweise bestehen keine Bedenken, dass der Secure Data Space datenschutzgerecht eingesetzt werden kann.

Technisch-organisatorische Sicherheitsmaßnahmen bei der SSP Europe GmbH und ihrem Dienstleister sind sorgfältig und angemessen umgesetzt und werden regelmäßig kontrolliert. Sie sind durch die gültigen Zertifizierungen der relevanten Systeme und Prozesse von unabhängiger dritter Stelle verifiziert. Betriebliche Vorgaben regeln die Anwendung von Sicherheitsmaßnahmen und den Umgang mit möglichen Abweichungen.

Es werden aktuelle Verschlüsselungsmechanismen eingesetzt, um die Vertraulichkeit der Daten im SDS zu gewährleisten. Insbesondere die Möglichkeit der clientseitigen Verschlüsselung bietet dem Anwender die Möglichkeit, das Lesen von Daten durch Unbefugte auszuschließen. Weder die SSP Europe GmbH noch deren Dienstleister können Daten, die der Anwender in seinem SDS vorhält, lesen. Strenge Anforderungen an den Schutz von Patientendaten oder anderen besonderen personenbezogenen Daten werden dadurch erfüllt. Die verwendeten Algorithmen entsprechen dem aktuellen Stand der Technik. Die Vertraulichkeit und Zweckbindung der Daten wird zudem durch ein Berechtigungskonzept sichergestellt, das die Vergabe sehr differenzierter Zugriffsrechte ermöglicht.

Logdaten und Systemprotokolle sind datensparsam und gleichwohl effektiv zum Schutz der Systeme eingerichtet. Bei optionalen Erweiterungen wird der

verantwortliche Anwender des SDS auf die datenschutzrechtlichen Vorgaben sensibilisiert, insbesondere durch das genannte Datenschutzmerkblatt.

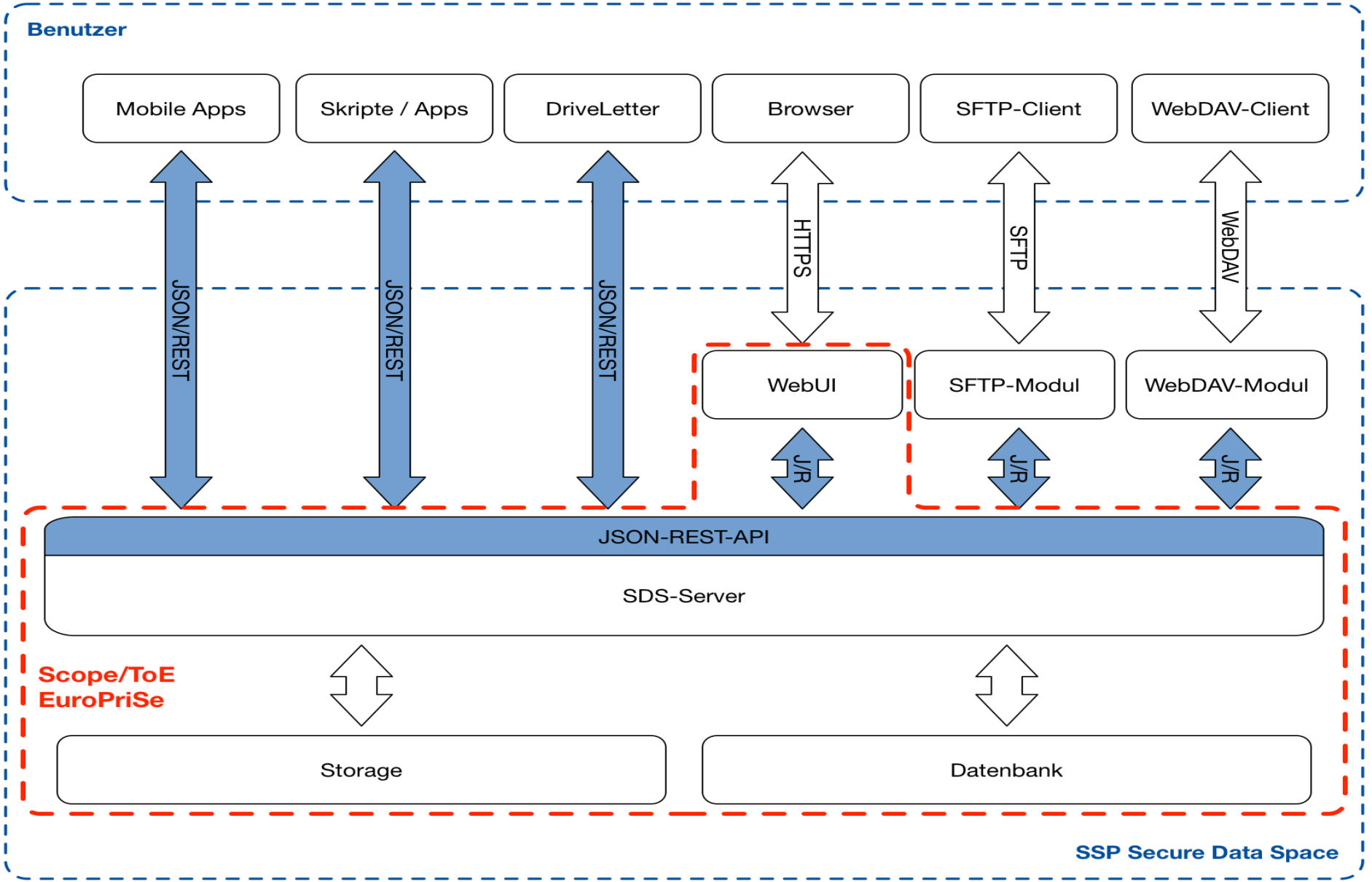
Umfassende Monitorings, Spamfilter und Recoverymechanismen sichern die Verfügbarkeit der Daten im SDS.

Zudem sind die Webseiten per https verschlüsselt und damit vor unbefugtem Auslesen der Kommunikation während der Datenübertragung geschützt. Da über die für den SDS relevanten Webseiten ein Session-Cookies gesetzt wird, ist das Recht auf Information tangiert. Der Besucher der Webseiten wird in dieser Datenschutzerklärung über den Gebrauch des Cookies informiert. Die IP-Adresse des anfragenden Rechners wird nicht personenbeziehbar erfasst.

Hervorzuheben ist, dass die Rechte des Betroffenen grundsätzlich gegenüber dem Anwender geltend zu machen sind, welcher personenbezogene Daten im SDS auf eigene Verantwortung verarbeitet. Der Anwender wird mit den ihm u.a. im Account zur Verfügung stehenden Informationen angemessen auf die Einhaltung der Betroffenenrechte sensibilisiert.

Die SSP Europe GmbH hat ferner einen betrieblichen Datenschutzbeauftragten bestellt, der als Ansprechpartner in Datenschutz-Angelegenheiten fungiert und den Anwender oder auch Betroffene bei Anfragen zum Datenschutz bei SDS unterstützen kann.

12. Datenflussmodel:



13. Datenschutz-fördernde Funktionen:

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, in welchem sich die Komponenten von SDS befinden, weist ein hohes Maß an physikalischer Sicherheit aus und ist zertifiziert.

14. Aspekte, die spezielle Aufmerksamkeit des Benutzers erfordern:

Im Rahmen der Evaluation wurde nicht festgestellt, dass Aspekte des SDS eine spezielle Aufmerksamkeit des Benutzers erfordern. Der Benutzer ist allgemein verpflichtet, einen datenschutzgerechten Umgang mit Daten im SDS umzusetzen. Ihm werden angemessene Handlungsempfehlungen seitens des SDS gegeben (z.B. das Datenschutzmerkblatt), um dies zu verwirklichen.

15. Kompensation von Schwachstellen:

Da der SDS keine Bewertung mit „gerade bestanden“ erhielt, ist die Kompensation von Schwachstellen nicht relevant.

16. Bewertungstabelle der wesentlichen Anforderungen:

EuroPriSe Anforderung	Entscheidung	Bemerkung
Datenvermeidung und Datensparsamkeit	adäquat	Der Anwender des SDS steuert die Datenhaltung selbst. Er wird auf die Einhaltung der Grundsätze der Datensparsamkeit und -vermeidung angemessen sensibilisiert.

Transparenz	adäquat	Produktdokumentationen und Datenschutzerklärungen sowie das Datenschutzmerkblatt sind informativ, aktuell und transparent und bieten gute Handlungshilfen bei der Anwendung des SDS
Technisch-organisatorische Maßnahmen	adäquat	Technisch-organisatorische Sicherheitsmaßnahmen bei der SSP Europe GmbH und ihrem Dienstleister sind sorgfältig und angemessen umgesetzt und werden regelmäßig kontrolliert. Sie sind durch die gültigen Zertifizierungen der relevanten Systeme und Prozesse von unabhängiger dritter Stelle verifiziert. Betriebliche Vorgaben regeln die Anwendung von Sicherheitsmaßnahmen und den Umgang mit möglichen Abweichungen.
Betroffenenrechte	adäquat	Der Anwender wird mit den ihm u.a. im Account zur Verfügung stehenden Informationen angemessen auf die Einhaltung der Betroffenenrechte sensibilisiert. Die SSP Europe GmbH hat ferner einen betrieblichen Datenschutzbeauftragten bestellt, der als Ansprechpartner in Datenschutz-Angelegenheiten fungiert und den Anwender oder auch Betroffene bei Anfragen zum Datenschutz bei SDS unterstützen kann.

Bestätigung der Experten

Wir bestätigen, dass das oben genannte IT-Produkt und der IT-basierende Service anhand der EuroPriSe Kriterien, Regeln und Prinzipien evaluiert wurde und dass die Feststellungen, wie oben beschrieben, das Ergebnis der Evaluation darstellen.

Bremen, den 10.06.2015

Dr. Irene Karper LLM.Eur.

Ort, Datum	Name der rechtlichen Expertin	Unterschrift der rechtlichen Expertin

Bremen, den 10.06.2015

Ralf von Rahden

Ort, Datum	Name des technischen Experten	Unterschrift des technischen Experten

Certification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Place, Date	Name of Certification Authority	Signature