Short Public Report

Secure Data Space

1. Name and version of the IT product or IT-based service:

Secure Data Space with the following variation

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

Version: 3.0

Functional status: 06/2015.

SDS is both an IT-product and an IT-based service.

2. Manufacturer or vendor of the IT product / Provider of the IT-based service:

SSP Europe GmbH
Maximilianstraße 35a
80539 München, Germany
as vendor and provider of the IT product and IT-based service.

Contact Person: Mr. Dan Jacob, Head of IT-Security Solutions of SSP Europe GmbH and Dr. Florian Scheuer, IT-Security Consultant of SSP Europe GmbH.

3. Time frame of evaluation:

29.04.2015 bis 09.06.2015.

4. EuroPriSe Experts who evaluated the IT product or IT-based service:

Name of the Legal Expert: Dr. Irene Karper
Address of the Legal Expert: c/o datenschutz cert GmbH

	Konsul-Smidt-Str. 88a 28217 Bremen, Germany eMail: ikarper@datenschutz-cert.de
Name of the Technical Expert:	Ralf von Rahden
Address of the Technical Expert:	c/o datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen, Germany eMail: rrahden@datenschutz-cert.de

5. Certification Body:

Name:	EuroPriSe Certification Authority
Address:	Joseph-Schumpeter-Allee 25 53227 Bonn, Germany
eMail:	contact@european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

SDS is a web-based, virtual data room, which can be used for uploads, downloads, storage, manage and transfer of data. SDS is designed for B2B. SDS is a so called Cloud-based service. Users are corporations, organizations or public authorities.

Vendor is the SSP Europe GmbH which performs development, maintenance and operation of SDS by order of the customer as a software as a service (SaaS) at the location Munic, Germany. Contracts between the SSP Europe GmbH and the customer are conform to the legal aspects of data processing by an agent. The information management system of SSP Europe GmbH is certified according to ISO/IEC 27001:2013.

The SDS Service is being hosted in a datacenter of the QSC AG in Nuremberg, Germany. The QSC AG is subcontractor of SSP Europe GmbH and the datacenter is ISO/IEC 27001:2005 certified. As part of the audit the contract between QSC AG and SSP Europe GmbH and the adequacy of the technical-organizational measures of the datacenter have been evaluated.

Those aspects support the requirements of public data protection authorities with regard to Cloud-Computing[1].

SDS is accessible on the website https://dataspace.ssp-europe.eu.

Fig. 1: Login SDS

SDS comes with the following variation:

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

[1] E.g. according to the „*Orientierungshilfe – Cloud Computing*“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder or according to Working Paper No. 196 of Article-29-Group „*Opinion 05/2012 on Cloud Computing“.*

Secure Data Space Online is the basic variation.

Secure Data Space Dedicated corresponds with Secure Data Space Online, but additionally it can be branded by the corporate Identity and Authentication can be realized by using the Active Directory.

Secure Data Space Virtual Appliance provides the same range of functionality as Secure Data Space Dedicated but in addition to that the user has the choice to run SDS in his own IT-environment or as a SAAS hosted by SSP Europe.

The user defines the applications and the access rights. The organizational structure can be mapped onto the data rooms (e.g. a Department or a Division). The SDS provides a graded authorization concept for this.

The functions of the SDS are documented transparently for the user in the user's Guide. SDS allows in addition to the classic functions of data rooms (files drop, upload, sort, replace, manage access rights, encrypt data, and so on) the classification of levels of confidentiality with the upload. The user can select the classification, within its data rooms when processing the file. The concepts are explained using in a mouse-over text. The classification is supported by the SDS, by giving the user a warning, if he wants to share a file that is classified as non-public. In addition, a file classified as a non-public cannot be shared without knowledge of the related password. Also, the user receives a note, if other permissions on a data room reign, in which he would like to copy a strictly confidential file. Furthermore, the document classification gives the administrator the ability to filter and manage relevant shares.

Users can grant a time - and quantity-limited upload right for internal or external users to a defined data room, subroom, or folder. These are temporary accounts - upload accounts – using an alias for the upload.

Authorized access to data belonging to the user in the SDS, is provided by means of the authorization concept.

In the following an overview on the differences of the three variations is given.

In addition to the basic functionalities of the SDS, SDS Dedicated offers the following features:

--- a dedicated deployed storage environment

--- a dedicated password for encrypting the storage environment,
--- a branding of the environment according to the user's instructions
--- login using the user’s Active Directory
--- SDS can be accessed from the Internet using any address in the context of the customer’s domain. SSP Europe GmbH provides a SSL certificate, if needed.

In addition to the online SDS and SDS Dedicated the SDS Virtual Appliance provides:

--- Using as an in-house solution possible
--- connection to the storage provided by the user according to the SSP Europe GmbH
--- Use in the housing operation or in the data center of the user.

The following SDS components belong to the ToE

--- WebUI
--- JSON_REST_API interface
--- SDS Server
--- management database.

The ToE does not include:

--- The use of SDS on Smartphones and tablets and the mobile apps,
--- The operational environment
--- the hardware components and in this respect the used operating system in the Datacenter
--- licensing and sales processes of SSP Europe GmbH
--- the company presentation http://www.ssp-europe.eu
--- any further services of SSP Europe GmbH.

7. General description of the IT product or IT-based service:

Data:

The data that is transferred into the SDS, depends on the user; This can of course be personal or person-related data. Due to the individual usage, the data can be

not finally listed. It was assumed for the evaluation that it could be health data, so that a high level of data protection had to be implemented.

User data is identified as primary data - in particular the E-Mail address that will be used as login, title and first and last name, which appear in the dashboard.

Log files, which are processed in the system of the SDS as well as the audit log, are classified as secondary data.

Encryption:

The data transfer between the server and client uses a TLS connection. The server-certificate was valid until 2018 at the time of evaluation. The communication is encrypted using keys of length up to 256 bit and at least 128 bit.

The database itself is not encrypted, but the data is stored on LUKS encrypted disks within the secured data center. Optionally, data can be encrypted on the client side prior to transmission to the data room. In this case the encryption is always for the entire data room and has to be performed when the data room is empty. When using an encrypted data space for the first time, every user has to choose an encryption password from which a key pair (RSA-2048) is generated. This key pair is used in all encrypted data rooms of this data space. A random symmetric key (AES256) is generated by using Galois Counter Mode (GCM) for any document that is filed here to encrypt the document. This symmetric key is then encrypted with the public key of all users being eligible for the data room and placed along with the encrypted data in the database. Thus, all users who have a data room read permission can read all data in the data room, even if they are encrypted. If only one user shall have a read permission, it is possible to create an individual sub rooms.

To read an encrypted file, the user is prompted to enter his encryption password with which the private key is released to decrypt and use the symmetric key. The encryption and decryption operation is performed via JAVA script and Java applet in the browser of the SDS user on the client. The keys are requested from the database of the SDS and held in the memory of the client.

Using this client-side-encryption there is no file unencrypted on the SDS back-end systems available and thus no administrator of SSP Europe GmbH can read the data not even in transit.

SDS offers the possibility to establish rescue keys for the case of emergency. If triple-crypt is enabled, the data space admin has the ability to set up a rescue key. When a new data room is created, the admin has the ability to decide whether rescue keys are used for this data room of the data space or not. The rescue keys are key pairs for asymmetric encryption and do not differ from the user key pairs. The private key is protected by a long and complex password, which is protected by the appropriate role (data space admin or data room admin) using suitable organizational measures.

When a rescue-key is used, all symmetric file-keys of data rooms are encrypted with the entire legitimate user and the appropriate rescue public keys, and stored in the database. Using a data space rescue key it is ensured by the authorization concept that a data space Admin can only access data, which have been released by the respective data room admin for him - even with knowledge of the data space rescue key. The rescue keys serve as safety anchor, for the case that all users of a data room have forgotten their encryption passwords. With the help of the rescue keys, the data is then still decodable. If no rescue key is used, the data can no longer be decrypted.

Deletion of data:

Deletions are contractually regulated between the SSP Europe GmbH and the user. Primary data can be deleted by the user himself manually or by setting a deletion date (expiration date) when uploading. In the latter case, the selected files are deleted completely after the deletion deadline via cronjob. Associated secondary data, such as change logs remain up to termination of the contract between SDS and the user.

Log data, which serve as an attack detection, are deleted after 7 days, unless otherwise instructed. At the user's request log data can be deployed longer. Therefore, a separate contract is required. The normal retention period is then usually three months. Upon termination, the user gets the option to export all data by zip archive. Users who use only a test account can delete their data at any time.

Audit Log:

Data space administrators can look for, view and understand transactions carried out by users in his data space with the help of the audit log.

The audit log cannot be changed and can only be deleted by deletion of the client.

Components:

SDS has the following components, redundantly laid out:

--- VMware-HA Reverse Proxies
--- VMware-HA application server
--- VMware-HA data base server
--- VMware-HA mirrored storage server.

It can be accessed via standard Web browsers. SDS can also be accessed through mobile devices (smartphones, tablets). Apps and mobile devices are not part of the ToE.

In addition, SDS can be integrated as a drive via the WebDAV interface, but then without the client-side encryption. There is a leaflet with privacy instructions (privacy leaflet) in which the user is made aware, only to use trustworthy clients. In particular, it undeceives the user about a possible criminal liability for unlawful disclosure with respect to professional secrecy. The client-side encryption is performed by JavaScript files and a Java applet in the browser, which are transmitted through the encrypted TLS channel from the server to the browser. The integrity of these files can be verified using the following checksums.

```
forge.bundle.js
SHA256:  450b57f7bf4d334d3fad9361bc5d7c53692e269aa279c7719cd28a31c3da0d6b

forge.min.js
SHA256:  e5cf57d8300753f633b67cf1978464695940dc99941ae6519a2241d080acd4d4

prime.worker.js
SHA256:  1a485ddf5763ad8ea862cf939911a1702712981fe5242e85e60ccf1afff661fe

sdsConfig.js
SHA256:  329225526c4758c9423c3e9a7747ea256f28aac9eef0d32f22a68cf557ed5225

sdsCrypto.js
SHA256: c6bf21633b3256130ad9d4a1cea91cbc0c4d0a72b1ba42334e4465da13c26fb3
```

Possible changes to the checksums by updating these files will be published in the future on the EuroPriSe website.

The Java-Applet (FsHelper_2.1.5.jar) is also digitally signed.

Interfaces and authorization concept:

The SDS server now has a JSON-REST-API that builds functionality of software. Functionality and logic of data proceeding has changed from clients to server side. This API is now the only gateway to applications, implemented in the SDS. Therefore all clients have the same security and data protection measures.

Clients now have only logical functions which are necessary for picturing information on screens, integration of SDS in systems and workflows and for encryption.

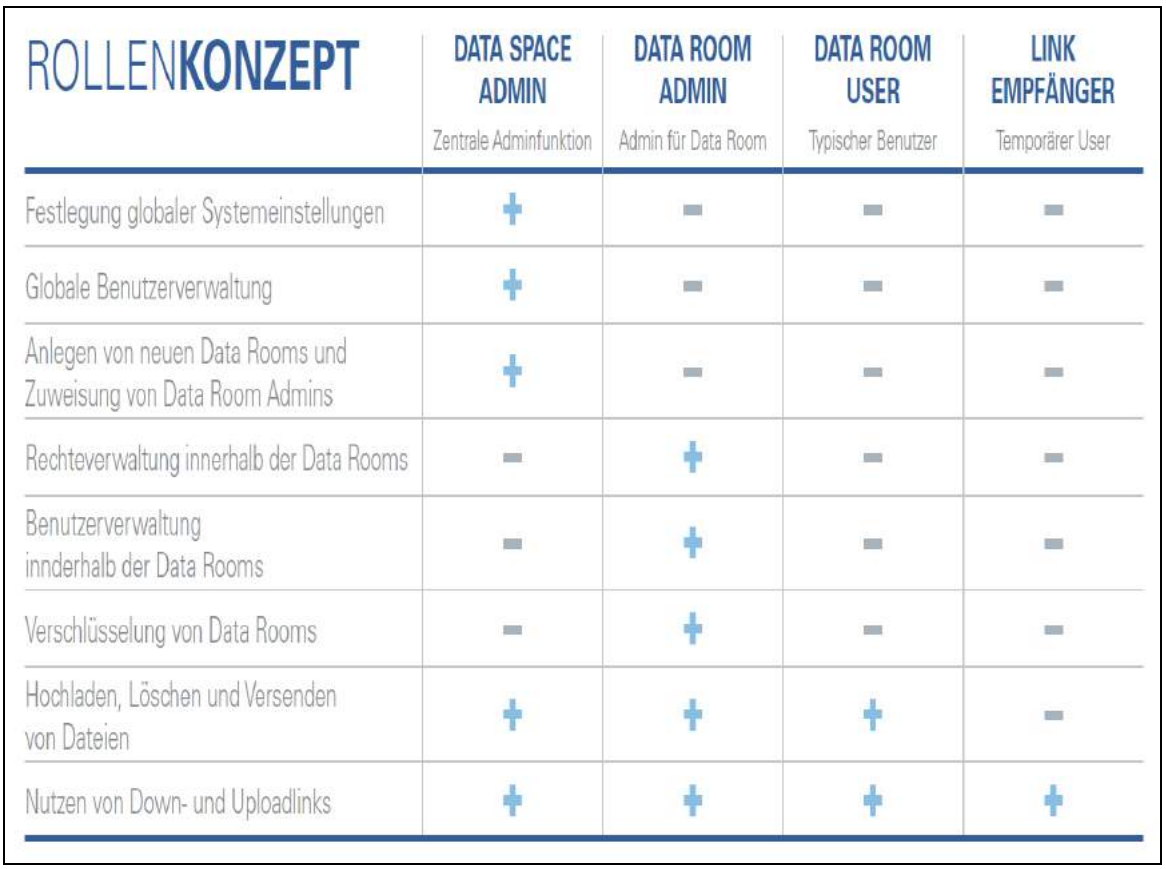
Standard client is a WebUI. This client gives the full functional standard and is hosted in the data center of SSP Europe Ltd. This WebUI has no server side logic (as known by classic web applications PHP or JSP) but it runs the surface by JavaScript within the web browser of the client. To get this information, the client communicates directly with the API.

All further gateways, that are not part of the target of evaluation and certification, were also operated by the JSON_REST_API. For WebDAV and SFTP gateway a proxy was implemented to map communication of clients and API, using the provided protocol.

Secure Data Space has the following interfaces:

- --- https-access over WebIU
- --- internal MySQL data base gateway
- --- Java/IO function for local mount and data-storage
- --- smtp for eMailing (mailing link for download function)
- --- API gateway
    - --- sftp gateway via API
    - --- WebDav gateway (for implementation of hardware) via API
    - --- Gateway for mobile devices and Drive Letter
    - --- Webservice-interface.

Permissions can be assigned gradually according to the roles and functions:



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	+	+	+	+

Fig. 2: Authorization concept (German)

The **data space admin** is the customer's administration role for the user and rights management.

The **data room admin** is the administrator of the respective data rooms. He has an overview of the user, the user rights (upload, delete, data room admin), he can create subrooms and can edit assignments of unassigned users to his data rooms (add, remove added users). He can be data room admin and data room user at the same time in different data rooms / subrooms. Version 3.0 of SDS now gives the data room admin the possibility to activate client side encryption easily by one click.

The **data space user** is a typical user role in the data room. He can upload and delete files or send download links (depending on the assigned rights). The data space user can also have the role of a data room admin.

The **link receiver** and the **upload account** describe roles of users of download links, which don't need to have an own account at the SDS. It must be highlighted,

that the links consist of a random string of characters, not allowing any conclusions based on the numbering or similar.

8. Transnational issues:

Since SDS is a web-based application it can be used worldwide. Organisations deploy SDS at their branches within the EU, the EEA or worldwide.

System and servers of SDS are located in a high security data centre within the Federal Republic of Germany.

9. Tools, used by the manufacturer of the IT product / provider of the IT-based service:

None.

10. Edition of EuroPriSe Criteria used for the evaluation:

Version 11/2011.

11. Evaluation results:

Secure Data Space is – in the opinion of the EuroPriSe expert´s –a save data room which fulfills the requirements of data protection and IT-security.

Information on SDS is easily accessible, significant and gives further hints to usage and configuration of the SDS in an optimal and privacy-friendly way.

The user of the SDS is responsible to observe the data protection requirements and to put to use when uploading, storing, or forwarding of data by means of the SDS. The data protection requirements may vary depending on the user and the task environment. The SDS supports him in compliance by instructions and recommendations. In accordance with these instructions, there is no concern that the secure data space can be used meeting the requirements of data protection.

Technical and organizational security measures at the SSP Europe GmbH and their service providers are carefully and appropriately implemented and regularly checked. They are verified by the valid certifications of the relevant systems and processes by an independent third body. Operational guidelines govern the application of security measures and the handling of possible deviations.

Strong encryption mechanisms are used to ensure the confidentiality of the data in the SDS. In particular, the possibility of the client-side encryption offers the user the possibility to exclude the reading of data by unauthorized persons. The SSP Europe GmbH nor its service providers can read data that is kept encrypted by the user in its SDS. This meets the strict requirements concerning the protection of patient data or other specific personal information. The algorithms used correspond to the current state of the art. The confidentiality and purpose of data is also ensured by the authorization concept, which allows setting differentiated access rights.

Log data and system protocols are used data-minimizing but also effectively to protect the relevant systems. The user is sensitized to privacy measures by using optional add-ons, in particular by the data protection information sheet (privacy leaflet).

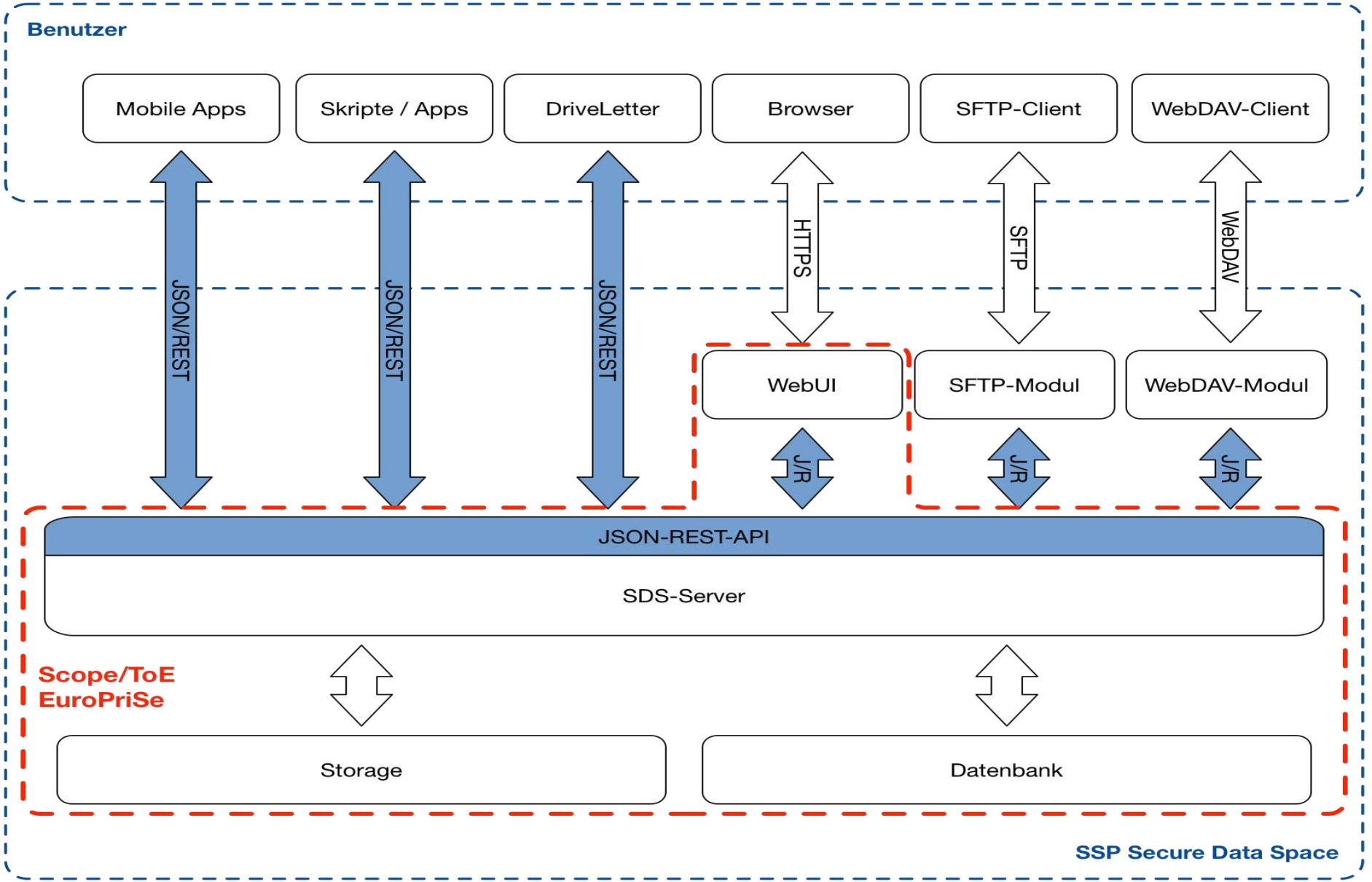
Comprehensive monitoring, SPAM filter and recovery measures assure the availability of data within the SDS.

Websites are encrypted by https. The transport of data while using web-forms is protected. The visitor of the website is informed about the use of cookies (session-cookies are used) in the privacy statement. The IP-address is anonymized.

It is to stress out that the rights of data subjects must be claimed against the customer which processes data on his own liability. The customer has been sensitized by documents and further information about data protection, available at the customers SDS account.

SSP Europe GmbH has a privacy protection officer who is to be contacted for privacy aspects. He supports both, customers and data subjects regarding their data protection rights.

12. Data flow:


Benutzer
Mobile Apps
Skripte / Apps
DriveLetter
Browser
SFTP-Client
WebDAV-Client
JSON/REST
JSON/REST
JSON/REST
HTTPS
SFTP
WebDAV
WebUI
SFTP-Modul
WebDAV-Modul
J/R
J/R
J/R
JSON-REST-API
SDS-Server
Scope/ToE
EuroPriSe
Storage
Datenbank
SSP Secure Data Space

13. Privacy-enhancing functionalities:

SDS has the following privacy enhancing functionalities:

--- An authorization concept, which allows the use of differentiated access rights, ensures the confidentiality of the data.

--- SDS provides the user with the ability to save data absolutely confidentially by SDS by using client-side encryption.

--- Avoiding weak algorithms with the use of TLS for encrypted communication, achieves a high degree of confidentiality.

--- Organizational and technical measures affecting data security and privacy go beyond the legal requirements: SSP Europe GmbH sensitizes the user in an exemplary way on compliance with data protection, including through a data protection leaflet. The data center, in which the components of SDS are located, shows a high degree of physical security and is certified.

14. Issues demanding special user attention:

The evaluation did not rate any of the issues as “additional safeguards needed”. Nevertheless the privacy compliant use of SDS lies within the responsibility of the user. He must adopt the given information by the developer about privacy standards and privacy enhancing configuration of SDS.

15. Compensation of weaknesses:

Since SDS does not pass any requirement with the grade “barely passing”, there is no need to compensate a shortcoming.

16. Decision table on relevant requirements:

EuroPriSe *Requirement*	***Decision***	***Remarks***
Data Avoidance and Minimization	*adequate*	The user of the SDS controls the data storage itself. He is adequately sensitized on the adherence to the principles of data minimization and prevention.
Transparency	*adequate*	Product documentation, privacy statement and the data protection instructions are informative, up-to-date and transparent and provide good guidance in the implementation of the SDS.
Technical-Organisational Measures	*adequate*	Technical and organizational security measures at the SSP Europe GmbH and their service providers are carefully and appropriately implemented and

		checked regularly. They are verified by the valid certifications of the relevant systems and processes by an independent third body. Operational guidelines govern the application of security measures and the handling of possible deviations.
Data Subjects' Rights	*adequate*	The user is appropriately sensitized on the compliance with the rights of the person concerned including the information that is available to him within his account. The SSP Europe GmbH has appointed also a corporate privacy officer, who acts as contact person in privacy matters and inquiries about privacy concerning SDS.

Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Bremen, 2015-06-10 Dr. Irene Karper LLM.Eur.

Place, date	Name of Legal Expert	Signature of Legal Expert

Bremen, 2015-06-10 Ralf von Rahden

Place, date	Name of Technical Expert	Signature of Technical Expert

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