Short Public Report

EuroPriSe European Privacy Seal

for

REISSWOLF f.i.t.

on behalf of

REISSWOLF Systems GmbH
Im Hegen 13
22113 Oststeinbek

Created by

Legal and Technical Expert Ann-Karina Wrede
greeneagle certification GmbH
Innungsstraße 7
21244 Buchholz
www.greeneagle-certification.de

Version 1.2

ISO27001-Audits auf Basis von IT-Grundschutz, IS-Revisionen, Datenschutzprüfungen

greeneagle certification GmbH
Beim Strohhause 17 ▪ 20097 Hamburg
Internet: www.greeneagle-certification.de

Index

1 Name and version of the IT based service

The it based service REISSWOLF f. i. t., a web-based archiving system for data storage and data access in the version 1.5 and with the functions at the time of the audit 30.08.-01.09.2017, was audited.

REISSWOLF f. i. t. serves the purpose of uploading, storing, managing and exchanging data in the sense of a document management system. It is a web application used with an internet browser.

2 Manufacturer or vendor of the IT product

Company Name:
REISSWOLF Systems GmbH

Address:
Im Hegen 13

22113 Oststeinbek

Contact Person:
Mr Axel Pöhlmann

3 Time frame of evaluation

The evaluation of REISSWOLF f. i. t. covered the period from 30 August to 1 September 2017 on site and until 18 May 2018 off-site. It included a structured data protection analysis on the basis of interviews, conducting tests, viewing documentation and on-site inspections.

4 EuroPriSe Experts who evaluated the IT based service

Name of the Legal and Technical Expert:
Ann-Karina Wrede

Address of the Expert:
Beim Strohhause 17
20097 Hamburg
Tel.: 040 790 235 – 291
E-Mail: awrede@greeneagle-certification.de
Web: www.greeneagle-certification.de

5 Certification Authority

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)
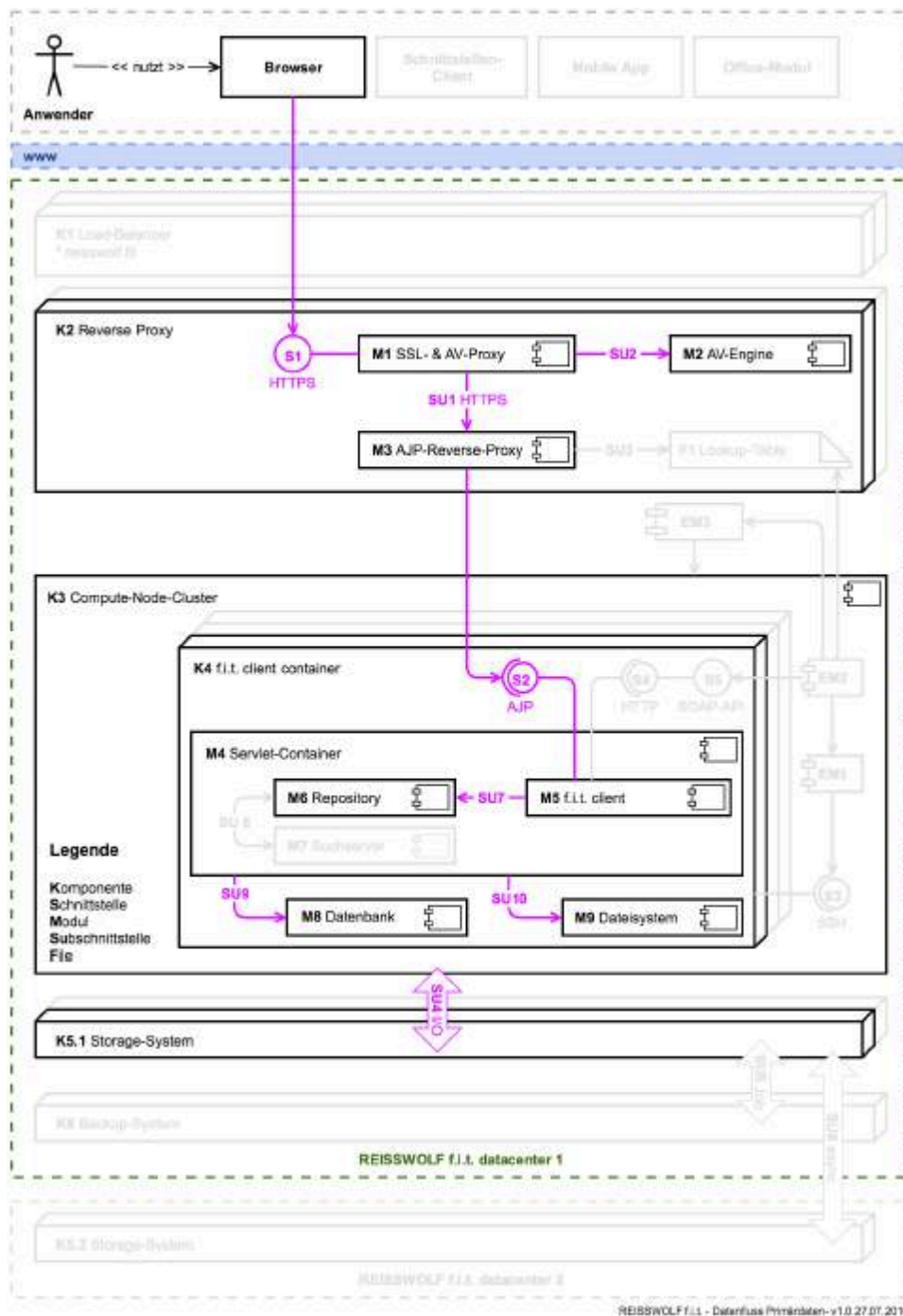
The following components are not part of the evaluation:

- REISSWOLF f.i.t Mobile App
- Office-Modul
- Teamviewer
- REISSWOLF f.i.t. hotfolder
- Other alternative client interfaces

7 General description of the IT based service

REISSWOLF f. i. t. is primarily designed for commercial use and serves the purpose of uploading, storing, managing and exchanging data in the sense of a document management system. Existing documents can be managed and new documents can be added.
REISSWOLF f. i. t. is distributed by REISSWOLF Systems GmbH and operated as Software as a Service (SaaS) in a data center in Germany. REISSWOLF f. i. t. has been developed in Germany and is also maintained in Germany. REISSWOLF f. i. t. is offered and used worldwide. The user needs a personalized user account to start working. REISSWOLF f. i. t. is compatible with the following browsers:

- Microsoft Internet Explorer version 11 or higher (compatibility mode off)
- Mozilla Firefox version 35 or newer
- Google Chrome version 40 or later

The user defines the scope of access rights to folders and documents himself. For example, internal departments or individual employees can have access authorization. Permissions can be defined per folder or document for users or groups. REISSWOLF f. i. t. provides a detailed graduated authorization concept for this purpose. The functions of the REISSWOLF f. i. t. are transparently documented for the user in the user manual. REISSWOLF has no influence on the type of documents uploaded in REISSWOLF f. i. t.. This is the responsibility of the user/customer. However, the user is informed by means of the data protection information in the manual that a consent or declaration of release from confidentiality may be required for the permitted use of REISSWOLF f. i. t. if necessary.
The product is designed for use by companies (Small and medium-sized enterprises), organisations or public authorities, regardless of the country of use.
REISSWOLF f. i. t is used in the area of responsibility of the respective user; i.e., it offers access to an abstracted IT infrastructure within the own organization in an isolated system environment.

8 Transnational issues

REISSWOLF f. i. t. has been developed in Germany and is also maintained in Germany. The product REISSWOLF f. i. t. is offered and used worldwide.

9 Tools used by the manufacturer of the IT based service

Modul	Name	Anbieter	Typ
K1 Load-Balacer			
-	CentOS Linux	CentOS Community	Betriebssystem
-	keepalived		
K2 Reverse Proxy			
-	CentOS Linux	CentOS Community	Betriebssystem
-	Apache HTTP Server	Apache Group	Webserver
K3 Compute-Node-Cluster			
-	Virtuozzo Containers	Virtuozzo	Container Virtualisierung
K4 RW f.i.t client container			

-	Ubuntu Server	Canonical Ltd.	Betriebssystem
-	OpenJDK	Canonical Ltd.	Laufzeitumgebung
M4	Tomcat	Apache Software Foundation	Servlet Container
M8	Percona Server for MySQL	Percona LLC	Datenbank
K5 Storage-System			
-	CentOS Linux	CentOS Community	Betriebssystem
-	NFS		Fileserver
-	DRBD	LINBIT	Datenreplikation
K6 Backup-System			
-	Virtuozzo Containers	Virtuozzo	Betriebssystem
-	prlctl	Virtuozzo	Backup Software

M5 RW f.i.t. client container

Name	Anbieter	Typ
Ehcache	Terracotta, Inc.	Cache
CXF	Apache Software Foundation	Webservice-Framework
Jasypt	jasypt.org	Verschlüsselungs-Framework
Hibernate	Red Hat Community	ORM

10 Edition of EuroPriSe Criteria used for the evaluation

The review was based on the EuroPriSe Criteria of November 2011.

11 Evaluation results

The legal requirements regarding the admissibility of data processing are fulfilled. This relates in particular to compliance with the provisions of Directive 95/46/EC. The requirements for data processing within the framework of contracts for processing by a processor on behalf of the controllerare fulfilled.

When registering and operating REISSWOLF f. i. t., the basic principles of data economy are observed:

A minimum of required data is requested in order to be able to use REISSWOLF f. i. t. With regard to the mandatory information, this only concerns

- E-mail address
- usernames (also pseudonyms)
- First name and surname (also pseudonyms)

The other data can be provided voluntarily by the user:

- Mobile phone number (only mandatory if 2-factor authentication via SMS is selected)
- Secret query and response (only mandatory if 2-factor authentication is selected)

Other business contact details (phone number, Skype for Business/Messenger number) are also optional.

With regard to data security, extensive measures have been taken, which are described in detail in the attached analysis. In particular, the following aspects are to be mentioned here to guarantee data security:

- Graded role and authorization concepts both for REISSWOLF f.i.t. and for the administrators of REISSWOLF.
- In principle, REISSWOLF administrators have no access to the customers' containers and are therefore only possible in exceptional cases (details are given in the detailed expert opinion).
- Encrypted containers, one container per customer. Virtuozzo 7 is used to encrypt the virtual hard disks of containers using dm-crypt and cryptsetup based on AES-256 encryption. The encryption mechanism is separate from the key management.
- Restricted access to the system: The only public interface that allows the customer to use the system is the encrypted communication of the web application via browser using the HTTPS protocol. Integrity and security are regularly checked using Qualys SSL Labs' HTTPS verification tool. The last inspection (11.04.2018) showed an A+ as test result.
- In the event of a deterioration in the result (e.g. due to the availability of new, better procedures or protocol weaknesses that have become known), the management will take the necessary measures on the same business day on which they become known.
- Passwords and access keys are also stored in encrypted form in the respective customer containers. To ensure that only the user and no one else, including no internal system, can know a user's password, they are stored in the database in one-way encryption. The SHA256 process with salt and several passes is used.
- Use of certified data centers via Dogado GmbH:
  - Hostway Deutschland GmbH, Hanover - ISO 27001 based on IT-Grundschutz, BSI-IGZ-0230-2016
  - Level 3 Communications GmbH, Düsseldorf - ISO 27001, 1582475-1
- Comprehensive procedural instructions, process descriptions and work instructions for REISSWOLF employees.

12 Data flow

REISSWOLF f.i.t. - Datenfluss Primärdaten- v1.0 27.07.2016
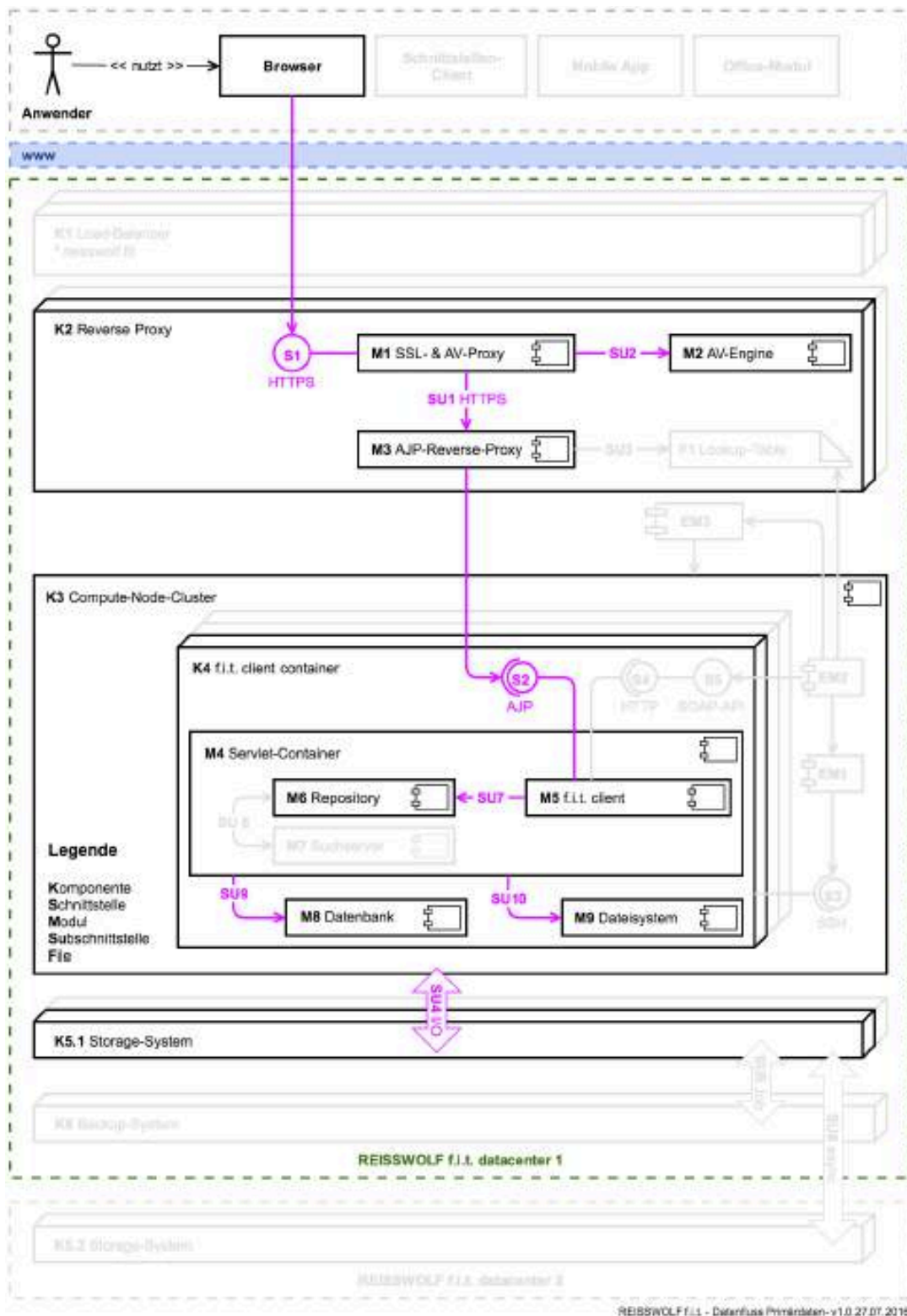
13 Privacy-enhancing functionalities

The IT product enhance privacy in the following way:

- The factory default state of the program contains settings that ensure a high level of security. The user is advised via the user's manual or the administration manual that it is not advisable to deviate from the set default settings.
- REISSWOLF f. i. t. offers a module for two-factor authentication via SMS-TAN, which can prevent unauthorized access even when disclosing user accounts.
- Access policies can be used to restrict system usage to specific times of day and/or IP addresses to reduce the attack vector for third-party access.
- By means of a cross-tab synchronized session countdown, the user is always informed about the actual remaining session time in REISSWOLF f. i. t., even if he works in several browser windows or tabs in parallel.
- Only the user himself can set his password, this also applies to the initial password, which the customer enters when ordering REISSWOLF f. i. t..
- User names can and should be pseudonyms, there is no obligation to provide a clear name.
- The user can change his or her personal data and password at any time.
- The authorization concept of REISSWOLF f. i. t. allows the definition of authorizations for users and/or user groups on individual folder and even file level. You can also disable the inheritance of permissions from folders to subfolders and files and define new permissions.

14 Issues demanding special user attention

There are no issues to which customers / (end) users should pay special attention.

15 Compensation of weaknesses

Not applicable

16 Decision table on relevant requirements

EuroPriSe Requirement	Decision	Remarks
Data Avoidance and Minimisation	adequate	The product makes use of pseudonymisation. Furthermore, only a minimum of required data is requested in order to be able to use REISSWOLF f. i. t.
Transparency	adequate	The documentation and privacy statements are informative, up-to date and understandable. In addition, it is always transparent to the individual user at any

		time which data is processed by him/her in the REISSWOLF f. i. t. at which point.
Technical-Organisational Measures	*adequate*	Encrypted containers, one container per customer, based on AES-256 encryption. Use of certified data centers. Graduated role and authorization concepts.
Data Subjects' Rights	*adequate*	Compliance with the rights of the data subjects concerned is to a large extent the responsibility of the customer. In addition, it is always transparent to the individual user at any time which data of himself/herself is processed by himself/herself in the REISSWOLF f. i. t. at which point.

Experts' Statement

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

Hamburg, 18.06.2018   Ann-Karina Wrede

| Place, Date | Name of Legal and Technical Expert | Signature of Expert |

Certification Result

The above-named 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 |