EuroPriSe European Privacy Seal

Short Public Report

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

goTRESOR HighSecurePlus “Enterprise” and “on Demand”

2. Manufacturer or vendor of the IT product and provider of the IT-based service:

Company Name:

GOGU Systems GmbH

Address:

Jakob-Klar-Strasse 4
80796 München

Contact Person:

Dr. Emil Gogu

3. Time frame of evaluation:

October 4th 2013 to November 11th 2014

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

Name of the Legal Expert:

Stephan Hansen-Oest

Address of the Legal Expert:

Neustadt 56
24939 Flensburg
Germany
sh@hansen-oest.com

Name of the Technical Expert:

Andreas Bethke

Address of the Technical Expert:

Papenbergallee 34
25548 Kellinghusen
Germany
bethke@europrise.expert

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 ToE is a web based service for a secure file and message exchange. Furthermore the ToE contains a chat-function, a calendar and a resubmission-function. All data, files and messages are stored encrypted using the so called “4-Keys-Technology”.
Within the ToE the owner has the possibility to create access permissions and to grant appropriate permissions for each user.

The ToE includes the following components:

- GoTresor-HighSecurePlus “onDemand” (data hosted on manufacturer’s server)
- GoTresor-HighSecurePlus “Enterprise” (data hosted on manufacturer’s server)
- GoTresor-HighSecurePlus “Enterprise” (data hosted on customer’s server)
- Manufacturer’s web-portal https://www.gotresor.de

The ToE does not include the following components:

- The firewall used in the data center of Hetzner AG
- The processing of customer’s personal data by the manufacturer for contract execution

7. General description of the IT product and IT-based service:
GoTresor-HighSecurePlus is a data-exchange-service which can be used by anyone who wants to share data (files, messages, timetable entries, resubmissions) with other users within a closed user group. The data-exchange-service can be installed on an own server or be used as a web service provided by GOGU Systems - either on a dedicated server managed by GOGU Systems in a German data center or on a dedicated server of the client managed by GOGU Systems. The ToE is both product and a service dependent on which goTRESOR offer is chosen by the customer.

GOGU Systems offers several goTRESOR services/products. They differ in regard to the level of security and included services (e.g. level of encryption, Access-PIN by SMS, white label branding, own domain). All product variants included in the ToE offer the highest level of encryption with the “4-Keys-Technology” by GOGU Systems. All data is encrypted when using the ToE.

The data is stored in a so called “online-locker”. The owner of the online-locker grants rights to the invited users. For each individual user access rights can be assigned by the owner. All data is encrypted by keys, initialized through the owner of an “online-locker”.

Customers of the manufacturer for the edition “enterprise” can decide, if they want to install the service on an own server, or if they want to use a manufacturers server, which is placed in the data center of Hetzner AG in Germany and which is managed by the German company SPIEGLHOF media GmbH.

8. Transnational issues:

   - none -

9. Tools used by the manufacturer of the IT product / provider of the IT-based service:
   - Development Environment:
     - Server OS: Linux Debian, Windows 2003 and 2008
     - XAMP 1.7.3 (PHP 5.3.1, Apache 2.2.14, mySQL 5.1.41)
     - Client OS: Windows 7
     - PHP Designer 2006
     - mySQL Query Browser 1.2.13
     - Ultraedit
     - Eclipse with GIT and SWN
   - Test Environment:
     - Server OS: Linux Debian, Windows 2003 (and higher)
     - Webserver Apache 2.2.14 (and higher)
     - Databasesystem: mySQL 5.1.41 (and higher)
     - Framework: Smarty 2.6 (and higher)
     - PHP 5.2.6 (and higher)
     - Client OS: Windows XP (and higher), Linux (div.), Mac OS X, Android

- Browser: MS IE 7.0 (and higher), Firefox 3.0 (and higher), Safari 3.0 (and higher), Chrome 3.0 (and higher), Opera 8.0 (and higher)

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria November 2011

11. Evaluation results:

Set 1: Overview on fundamental issues

By using the ToE all data are encrypted, so no one, except the owner and user of the ToE who are granted access, is able to access the data. The rights are granted individually. The saved data may contain personal data with high protection requirements.

Following types of data is collected by the system:

- personal user data (just first-name, last-name and an e-mail-adress is required)
- content of messages
- calendar appointments
- personal data (delegation) within a resubmission
- file-content
- log-data

Set 2: Legitimacy of Data Processing

The processing of personal data by the manufacturer is lawful pursuant to Art. 7 (b) of the Directive 95/46/EC. The manufacturer collects, processes and uses personal data of owners of online lockers in “goTresor” to the amount necessary for the performance of the contract.

Users of the service can invite other users to their online locker. For registering with the service these third party users have to fill in very limited personal data. The manufacturer of the data has no access to this personal data due to encryption of the data.

Session cookies are used by the manufacturer for the performance of the service. The cookie holds the session ID of the user which is used to perform operations requested by the user. The session cookie is necessary to provide the functionality of the service to the user. By disabling cookies the service would not be usable for the user. Furthermore the functionality of the service has been explicitly request by the user. By taking WP 194 of the Art. 29 WP into account these sort of cookies can be exempted from the provision of having consent pursuant to Art. 5 (3) of Directive 2002/58/EC.

Regarding the processing of data by a processor the necessary legal provisions are met. The manufacturer has signed commissioned data processing agreement with the service providers involved in the service. These contracts meet the requirements of Sec. 11 of the German Federal Data Protection Act ("BDSG").

In regard to the data processed by users with the service, the user is the controller of the data processing. Therefore the user has to take care of a legal basis for the processing of personal data. GOGU Systems provides a data protection leaflet for customers that contains information in regard to lawful processing of data using GoTRESOR.

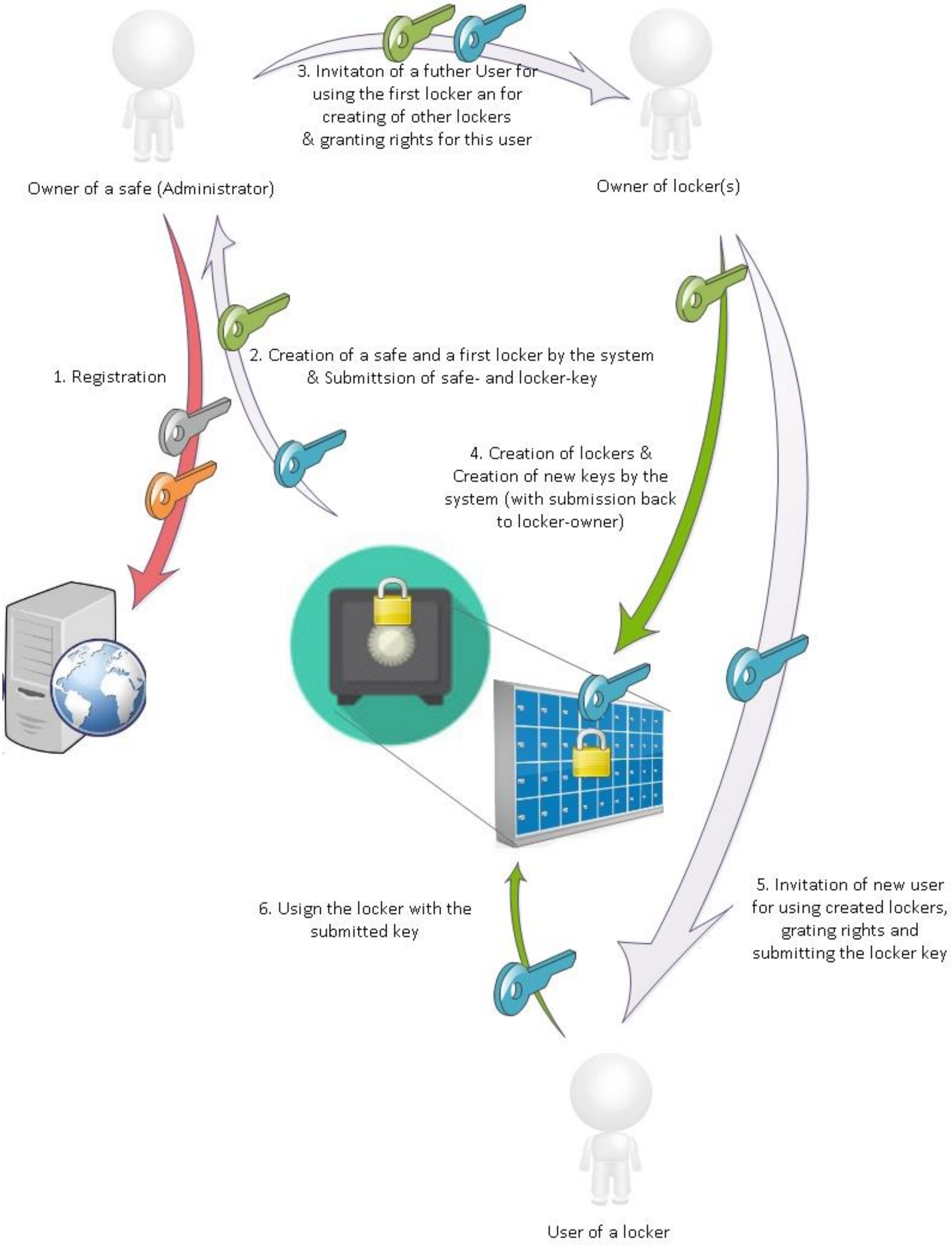
Set 3: Technical-Organisational Measures: Accompanying Measures of Protections for the Data-Subject

The ToE uses a cascade of encryption-technologies for data exchanged through the service. When uploading data to the locker on the webserver, the file is sliced to several pieces which are then encrypted with the key of the online locker of the user on the client side. The data is then transmitted to the server using TLS-/SSL-encryption. The encrypted slices of data are constructed to one encrypted file with an encrypted file name on the server again. When downloading data the file is separated to different pieces, too. The separate pieces are then decrypted on the server ("on the fly") and encrypted with the symmetric SSL-key and then transmitted over an SSL-connection. The browser of the user will finally put the pieces of data together to a file. Every safe and every locker within the safe uses a different AES256 key for encryption. The whole transmission of data is encrypted by using the Transport Layer Security (TLS) / Secure Socket Layer (SSL)

Set 4: Data Subject Rights

The users are adequately informed about the privacy policy of the product, which can be viewed on the website. The information is related to the preservation of the rights of the concerning person.

12. Data flow:


3. Invitaton of a futher User for using the first locker an for creating of other lockers & granting rights for this user
Owner of a safe (Administrator)
Owner of locker(s)
1. Registration
2. Creation of a safe and a first locker by the system & Submittsion of safe- and locker-key
4. Creation of lockers & Creation of new keys by the system (with submission back to locker-owner)
6. Usign the locker with the submitted key
5. Invitation of new user for using created lockers, grating rights and submitting the locker key
User of a locker

13. Privacy-enhancing functionalities:
As a very special feature the manufacturer has implemented a mechanism for controllers to verify that the code on the webserver has not been changed (by the manufacturer).

14. Issues demanding special user attention:
- none -

15. Compensation of weaknesses:
- does not apply -

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*excellent*	Due to the fact that all data stored in an "online locker", are encrypted, the principle of data avoidance and data economy is explicitly taken into account.
Transparency	*excellent*	The manufacturer has created a reasonable and above all very clear and understandable documentation of the service. It contains not only the use of product but also details for encryption and for testing of critical program code.
Technical-Organisational Measures	*adequate*	The technical-organisational measures taken by the manufacturer are adequate.
Data Subjects' Rights	*adequate*	The users are adequately informed about the privacy policy of the product, which can be viewed on the website. The information is related to the preservation of the rights of the data subject.

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.

Flensburg, 11.12.2014	Stephan Hansen-Oest	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Kellinghusen, 11.12.2014	Andreas Bethke	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Certification Result

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

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

	EuroPriSe Certification Authority	
Place, Date	Name of Certification Authority	Signature