Short Public Report

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

IT product: Test Data Migration Server (TDMS), Version 4.0

2. Manufacturer or vendor of the IT product:

Company Name: SAP AG

Address: Dietmar-Hopp-Allee 16,
69190 Walldorf

Web: www.sap.com

Contact Person: Volker von Seggern

3. Time frame of evaluation:

27.02.2011 – 06.09.2012

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: datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen, Deutschland

ikarper@datenschutz-cert.de

Name of the Technical Expert: Ralf von Rahden

Address of the Technical Expert: datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen, Deutschland

rrahden@datenschutz-cert.de

5. Certification Body:

Name: Unabhaengiges Landeszentrum fuer Datenschutz - ULD
Address: Holstenstr. 98
24103 Kiel
Germany
eMail: europrise@datenschutzzentrum.de

6. Specification of Target of Evaluation (ToE):

Target of Evaluation (ToE) is the IT product *Test Data Migration Server (TDMS) in the version 4.0* (short TDMS).

The ToE contains the following components

- TDMS plug-in on the sender system
- TDMS server, consisting of a central system and a control system
- TDMS plug-in on the receiver system

7. General description of the IT product:

Using TDMS, data from SAP systems can be made available for development, testing, quality assurance or training. The data can be reduced to the desired degree and distorted (scrambled) without losing consistency.

7.1 Scope

TDMS allows the processing of data from the respective SAP based system, where the identifiability of persons can completely be prevented (anonymisation) or at least be made more difficult (pseudonymisation) by different rules for the distortion of the data (scrambling), to be selected by the user in each case.

As an exception, it is also possible to define rules without anonymisation, or pseudonymisation. To inform the user about compliance with data protection, a popup with a warning label appears if the user uses no scrambling rules and the data thus will be transferred undistorted. In addition, an information sheet about data protection explains the aspects of data minimization, anonymisation and pseudonymisation to the user.

TDMS generates its own log for each activity. This contains the user name of the user as the only personal data. TDMS passes the log data to the SAP production system without saving it in TDMS, where it is recorded and can be processed for means of revision.

Users are companies or public bodies. Typically TDMS is used to process personal data as created by the SAP module human capital management (HCM) on the basis of info-types, or customer data, such as data saved in the modules customer relationship management (CRM), enterprise resource planning (ERP) and business intelligence (BI).

TDMS, Version 4.0 can be used with the following SAP Basis systems:

- Business Suite:
  - SAP ERP
  - SAP ERP HCM
  - SAP CRM
  - SAP SCM
  - SAP SRM
- Industry Solutions:
  - AFS
  - Banking (Loans and Deposits)
  - Oil & Gas (Downstream)
  - Utilities
  - CRM for Utilities
  - Healthcare
  - DIMP
  - Retail

- SAP NetWeaver BW
- SAP GTS.

7.2 Range of functions of the ToE

The ToE contains the following components

- TDMS plug-in on the sender system
- TDMS server, consisting of a central system and a control system
- TDMS plug-in on the receiver system

The TDMS system landscape consists of a sender system (sender), the TDMS server with the control system (control) and the central system (central) and a receiver system (receiver).

TDMS receives selected real-time data from the sender for development, testing, quality assurance or training. The sender system is always a SAP production system. The selected real-time data can be distorted by TDMS on the SAP production system (scrambling). TDMS offers several mechanisms for this purpose. As a general rule scrambling is applied using TDMS, as this is a major benefit of TDMS. However, it is possible to pass on selected data without distortion to the receiver.

The scrambling mechanisms and settings (used systems, created user accounts, defined roles, permissions) are stored in the control system of the TDMS server. The background processing of data migration is performed in the central system. As a task is triggered, the data is transferred to the receiving system.

Scrambling

The focus of TDMS is the scrambling of data before transfer from the sender system to the receiver system. The user can do this by defining their own rules or - specifically for SAP ERP HCM – use scrambling packages predefined by the manufacturer, and use and customize it for their needs.

Scrambling offers the following options:

- Data values can be randomly changed, assigned fixed values or can be deleted
- Distortion strategies for individual data fields can be inherited by other data fields. In this way, the consistency of the data record is preserved

Whether the use of certain scrambling rules leads to an anonymisation or pseudonymisation in terms of data protection law, is to be determined by the user in every single case.

If TDMS is used without the distortion of real data (e.g. to create a 1:1 copy of the data), then the system displays a pop up window that requests that the user checks and confirms this situation. Furthermore the user is informed about the relevant privacy laws in an information sheet about data protection ("Notes on data protection and anonymization SAP Test Data Migration Server 4.0 (SAP TDMS 4.0)").

Data reduction

TDMS also allows users to select, for example, only individual company codes or data of specified time periods. This way data can be reduced to the desired degree.

Data transfer

The data transfer is carried out directly from the sender to the receiver via remote function call (RFC). Alternatively, a transfer via an export / import function is possible. In this case the resulting cluster of scrambled data (if scrambling rules have been applied) is exported to a file that can be imported in the receiver system from a mobile disk for example. Since the data then is not protected in the same way, such as using the RFC connections, we recommend that users protect the data for example by using encryption as outlined in chapter 3.11 of the master guide.

It is important to point out that personal data is not in any circumstances stored on the central system or the control system. Instead the user performs a read

access on the sending system and a write access on the receiving system, so the data can be transferred directly from the sender to the receiver. TDMS supports in this sense only the transmission of data.

7.3 Range of functions outside the ToE

Not part of the ToE and therefore not being evaluated are

- The sender and the receiver system if they are not identical to the TDMS server.
- The underlying SAP product line or the SAP system including data collection and data processing
- The environment for the user, as well as a data processing on behalf of the user
- The hardware components of TDMS servers, the operating system and the used database system
- Licensing and sales processes with SAP AG or their customers

8. Transnational issues:

TDMS can used by companies or public authorities with offices within the European Union, the EEA or are used around the world. Database and server are situated in the area of responsibility of the respective user. The relevant frameworks can be found in particular in Directive 95/46/EC[1]. These have been implemented in the EU Member States into national law, such as in the German Bundesdatenschutzgesetz (BDSG)[2]. In addition are the interpretation helps of the art-29 data protection group (Art-29-Datenschutzgruppe), the European courts' rulings/case-law, as well as national requirements of the data protection supervisory authorities such as the to the Federal Republic of Germany applicable Guide "data protection and data security in projects: project and

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ABl.EU L 281 v. 23.11.1995, p. 31ff.

[2] Federal data protection act in the version of the notice of. 14.01.2003 (BGBl. I S. 66), last change by Art. 1 of this law of 14.08.2009 (BGBl. I S. 2814).

production" of the Working Group "Technical and organisational data protection issues" of the Conference of the supervisor of the Federal and State.

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:

The experts use the EuroPriSe criteria catalogue in the version from May 2011 and the EuroPriSe glossary in version 1.0.

11. Evaluation results:

Following significant results have been identified:

11.1 Implementation of legal requirements

The legal basis for the application of TDMS depends on the respective purpose of the data processing and the legislation for the user. TDMS supports this by informing the user by providing an information sheet about data protection to generally review the compliance with applicable law. TDMS also allows a selection, reduction, or the distortion of the transferred data so that the user can choose only such data which comply with the respective basis. If data is anonymised using TDMS, data processing is usually allowed.

Also adequately met are the requirements of transparency, limitations on use and proportionality. In particular the information sheet about data protection as well as additional documentation provided by SAP AG provide an overview of the data processed by means of TDMS for further privacy policy relevant assessment. By these means, tasks of the data protection official are supported.

11.2 Data Minimization

TDMS offers the possibility to use only data that is necessary for a specific task. At the same time, personal data can be anonymised or pseudonymised in an efficient manner. Temporary files are deleted immediately.

Secondary data is provided to the underlying SAP system on the TDMS server. TDMS does not set a retention time for this data. This has to be changed with the next support package to be released before March 2013.

The user is explicitly informed by the information sheet on data protection about the adherence to the principles of data reduction and data minimization when establishing and using TDMS.

11.3 Data security

Permissions can be assigned gradually according to the roles and functions. TDMS is delivered with predefined roles; these can be customized by the user. Hereby TDMS supports the establishment of a very granular authorization and role concept.

TDMS is installed as an extension of an existing SAP base system. It uses the authentication mechanisms of the base system. The users must log on to the system by using one of these systems. Only a user who has been configured with appropriate rights can access TDMS. A password policy to set the password complexity must be set in the base system and depends on the risk analysis of the user for their data.

Overall, TDMS offers a detailed logging functionality, which can and must be configured by the user according to his needs together with the associated permissions.

TDMS implemented connections between sender, central and receiver system via RFC-connections. The RFC-connection can use encryption by means of secure network communication (SNC), i.e. using SSL. When using encrypted RFC connections, the authorization credentials are also encrypted and thus transferred in a protected manner. TDMS itself does not protect the network connections, but supports the use of secure protocols.

Basically no primary data are stored permanently in TDMS. Therefore, there is no need to back up data or to protect against unforeseen loss. For more information about backup and restore the operation guide refers to the general documentation from SAP NetWeaver. TDMS offers no backup functionality.

The operations guide informs the user about possible support. As an internal support desk can be set up or questions/problem messages can be routed through a CA-TDM component directly to SAP. The development process of TDMS follows the PIL (product innovation life cycle). In the PIL are clearly defined test and release procedures, which ensure a careful quality control.

TDMS itself provides no encryption functions. Because TDMS is designed for transmission within the same network, this is also not necessary from point of view of experts.

Using the export functionality, selected and scrambled data can be stored on a mobile disk for transfer. In this case it is pointed out in the master guide, that a proper encryption of the disk is strongly recommended. Furthermore, there is a corresponding reference to the encryption of mobile disks in the information sheet about data protection.

11.4 Data Subjects' Rights

Data Subjects' Rights are supported adequately when the system is set up and used properly. Users are made aware on the implementation of data subjects' rights in the use of TDMS in the fact sheet about data protection. Also the TDMS product documentation and guidance on data protection for certain SAP production systems are provided, which also inform the user about dealing with the rights of persons affected.

12. Data flow:

The data flow can be represented with the following figure::

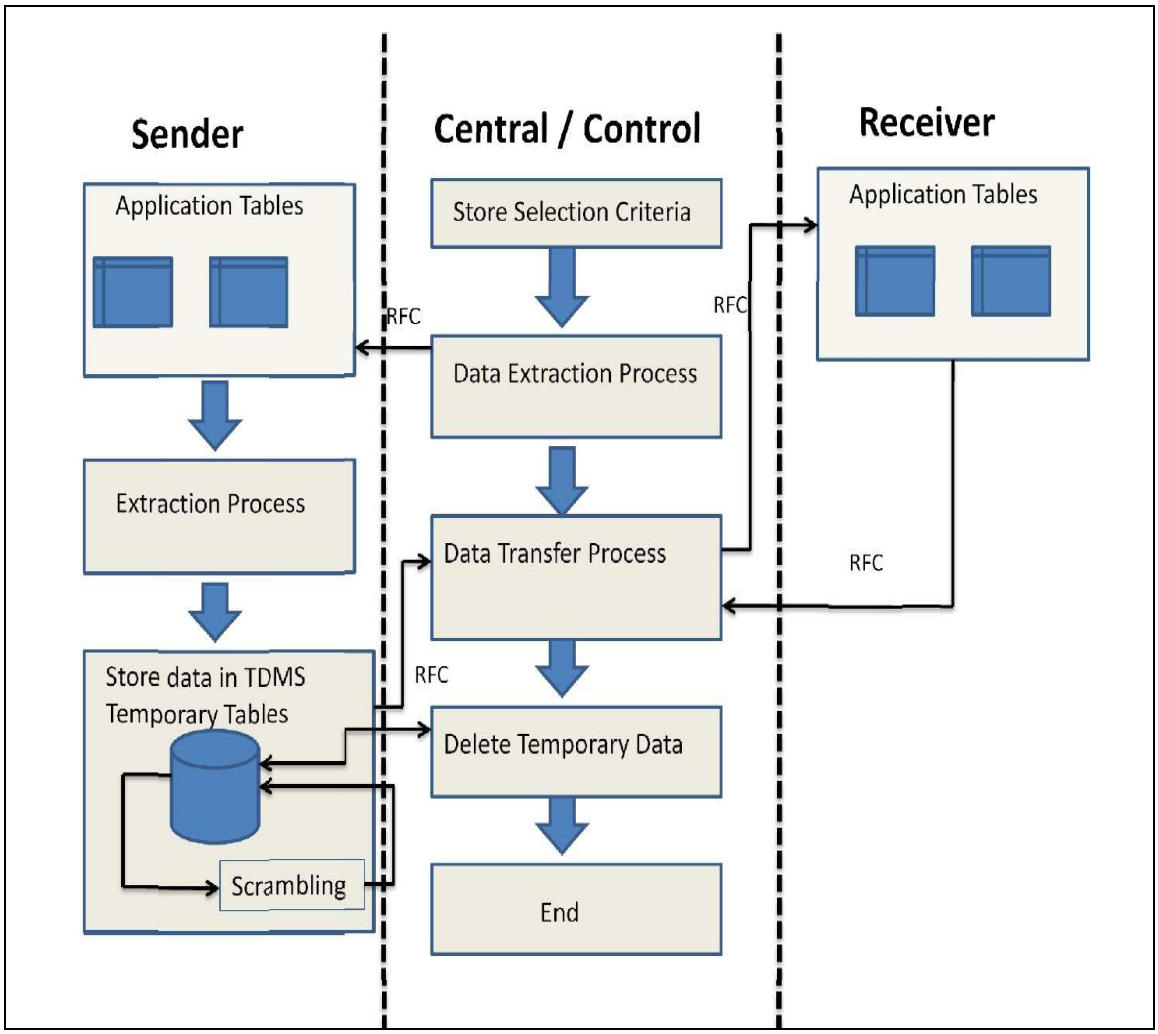

Figure 1: Data flow

13. Privacy-enhancing functionalities:

The product includes the following, enhancing data protection features:

- TDMS offers the ability to create high quality test data from production data, while unnecessary personal data in an optimum manner can be anonymised or pseudonymised.
- Possibilities of data avoidance and data reduction are excellent. The immediate deletion of temporary data on the sending system after the transfer is exemplary.
- Users are pointed out in various ways to the requirements of the processing of personal data, in particular the possibilities and requirements of anonymisation and pseudonymisation. The information summarized in the privacy information sheet on data protection is to be highlighted.
- TDMS has a fine granular role concept. It allows the user to adapt the delivered role templates according to his needs precisely. In this way, limited permissions may be granted exactly on the essential.
- The incident management, as well as test and release procedures are excellent.

14. Issues demanding special user attention:

The privacy-compliant use of TDMS is the responsibility of the user. They must apply the information to the privacy standards provided by the manufacturer and a configuration supporting data protection in each case.

During evaluation the experts found that the log data created by TDMS is provided to the SAP basis system without a predetermined deletion date. The user is not supported in this case by the TOE itself to comply with deletion times. With the next support pack for TDMS SAP implements a maximum age of log data of one year as the default value.

15. Compensation of weaknesses:

There no requirement of the criteria that is evaluated "barely passing". Due to lack of weakness, there is no need for compensation.

16. Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimization	excellent	TDMS offers the possibility to use only the data that is necessary for the processing of each task. At the same time, personal data can be anonymised or pseudonymised in an optimum manner Temporary data is deleted immediately.
Transparency	excellent	The documentation and information to the legal conditions and data protection are informative, current and understandable.
Technical / Organizational Measures	excellent	The role and authorization concept can be configured in an efficient manner. Incident management, test and release procedures as well as the information on data protection with examples for data security are exemplary and promote the implementation of appropriate technical and organizational aspects of the user.
Data Subjects' Rights	adequate	The user is informed appropriately in the information sheet about data protection on the implementation of data subjects' rights in the use of TDMS.

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, 06.09.2012 Dr. Irene Karper LLM.Eur.

Place, Date	Name of Legal Expert	Signature of Legal Expert

Bremen, 06.09.2012 Ralf von Rahden

Place, Date	Name of Technical Expert	Signature of Technical Expert

Certification Result

The above-named IT product passed the EuroPriSe evaluation.

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

Kiel 2012 Unabhängiges Landeszentrum für Datenschutz

Place, Date	Name of Certification Body	Signature