Privacy Audit

Short Public Report Version 1.0d

for the approval of the

ULD Privacy Quality Seal

and the

European Privacy Seal

-Final-

Target of Evaluation (ToE)

Microsoft Software Protection Platform

Short Public Report

2

3 Name and version of the IT product:

Microsoft Software Protection Platform (SPP)

4 Manufacturer of the IT product:

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA

5 Time frame of evaluation:

June 2007 to November 2008

6 EuroPrise and ULD Experts who evaluated the IT product:

Evaluation Body for Privacy / EuroPriSe Expert (Legal)
Marcus Belke, Attorney at Law
Oliver Gönner, Attorney at Law
2B Advice GmbH
Wilhelmstrasse 40-42
53111 Bonn
Germany
marcus.belke@2b-advice.com

Evaluation Body for Privacy / EuroPriSe Expert (Technical)
Stephan Di Nunzio
TÜV Informationstechnik GmbH
Langemarckstrasse 20

45141 Essen
Germany
S.DiNunzio@tuvit.de

7 Certification Body:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98
D-24103 Kiel
Germany

8 Specification of Target of Evaluation (ToE):

Microsoft Software Protection Platform is the name for the summary of the services Activation, Volume License Management and Security Breach Response. The results of the privacy audit are only applicable to Microsoft Software Protection Platform.

The products must be used in the following environment: Operation systems: Windows Vista RTM as well as Windows Vista SP1, Windows Server 2008 RTM.

RTM is the shortcut for Release to Manufacture and describes the first version of the Vista and Windows Server 2008 released.

The main usage scenarios of Software Protection Platform are:
Single License Activation
Activation by Original Equipment Manufacturer (OEM)
Volume License Activation with Key Management Server (KMS)
Volume License Activation with Volume License Activation Management Tool (VAMT)
Windows Genuine Advantage (WGA)
Breach Response Tool (BRT)

The genuine test in general as well as the update mechanism are not part of the ToE. The WGA 1.7 and MU 6.0 components have been evaluated for Windows XP in an earlier privacy

seal process.[1] Only data transmission between Software Protection Platform and these components are checked as well in this evaluation.

9 General description of the Product

Microsoft's Software Protection Platform is a service that provides mechanisms to consumers and institutions that protect them from the risk of counterfeit software and better enables volume license customers to manage their software assets. The overall goal of Software Protection Platform is to bring together new anti-piracy innovations, counterfeit detection practices and tamper resistance. The combination of these processes into a complete platform provides better software protection to programs that use this Software Protection Platform. In the first stage of Software Protection Platform, only Microsoft Windows Vista and Microsoft Windows Server 2008 use the platform to protect the system from software piracy. The main advantage of Software Protection Platform is that in all steps of communication cryptographic methods are used to protect the integrity of communication and systems.

The Software Protection Platform provides two main entry points. The first entry point to Software Protection Platform is the software activation that every product has to perform at least once. Before a Microsoft operating system that uses Software Protection Platform can be fully used, it has to be activated. The second entry point to Software Protection Platform is the validation of the genuine state of software within any download of specially protected software from Microsoft. The genuine test is necessary to access the Microsoft Download Center or Windows Update. These Windows downloads and updates will only be available for genuine Windows systems.

10 Transnational issues

The product Software Protection Platform is offered and used worldwide. All data is stored in a Microsoft Corporation US Datacenter.

11 Tools that were employed to the production of the IT-product

Microsoft Visual Studio .Net Professional 2003 & 2008

Microsoft Office Professional Edition 2003 & 2007

[1] https://www.datenschutzzentrum.de/guetesiegel/kurzgutachten/g070908/g070908-kurzgutachten-microsoft-wga-englisch.pdf

Microsoft Office Visio Professional 2003 & 2007

Microsoft Office Project Professional 2003 & 2007

Microsoft Product Studio 2.10.6729.0

Microsoft Source Depot 3.0

Microsoft FxCop 1.3

Microsoft SQL Server 2000

Warbird 1.1.10

Microsoft Prefast

Microsoft Prefix

Microsoft APTool

Microsoft SQL Server

12 Version of the requirement Catalogue

ULD Requirements Catalogue, Version 1.2 (August 29, 2005)

EuroPriSe Catalogue, Version 0.2 (December 13, 2007)

13 Evaluation Results

The evaluation of Microsoft's Software Protection Platform brought up as an overall result that the processing of personal data is implemented in an excellent way. The different usage scenarios were evaluated in detail:

1. Single License Activation

In general, every Microsoft operating system has to be activated. Systems that do not perform the activation process within a grace period of 30 days are set into a reduced functionality mode in the RTM version of the operating system and set to a notification mode in SP 1 version. Whereas in the reduced functionality mode the usage of the system is limited to core functionality, in notification mode the system is fully usable while only a notification that the software is not activated appears for a short period.

In the Single License Activation scenario, the user buys Windows Vista or Windows Server 2008 in a store and installs it on an arbitrary computer system. In this case, he has to activate the system either online or by telephone. In some countries activation can be alternatively performed by cell phone's short messaging service (sms).

Within the online part of Single License Activation, a connection between Microsoft and the user's client machine is established. Microsoft installed a communication layer that is called Software Licensing Service. This layer within Microsoft manages communication with the client machine.

Microsoft's second layer is the database layer behind the communication stage. Client communication is filtered by the communication layer and forwarded to the Database layer called Activation Service Clearinghouse. This layer hosts the databases that are stored forever.

The evaluation showed that on the connection to Microsoft no personal data are transmitted. As a matter of online communication, still the IP address of the machine is transferred. The IP address is only used and stored as long as necessary to answer the request of the client machine.

In addition, the clients' machine name that a user can enter in installation routine is transferred to the communication layer of Software Protection Platform. At the communication layer, information can be recorded for debugging purposes if needed. The recording can only be enabled if a predefined clearance process is performed. The evaluation has shown, that in case of the user giving his computer system a real name related to natural persons, personal data could be transferred to Microsoft. The standard setting of the computer name field is the first entered username with the appendix -Computer. The evaluator advises users not to enter a real person's name in the computer name field. If the user does enter a real name as the machine name personal data will be transferred and possibly stored within Microsoft until the following changes apply:

After a hint within the evaluation process, Microsoft decided to stop recording both IP address and Machine Name by October 17th 2008. The transmission of the Machine Name will be completely stopped by a client update on January 19th 2009. Due to TCP/IP communication needs, the transmission of the IP address cannot be shut off completely, but the data only will be stored as long as necessary to communicate.

Beside this some other non-personal data but unique data like hard- and software checksums as well as the product key are transferred to Microsoft in four communication steps. The unique hardware identifier is built on the client's hardware. This hardware information is used to bind the final license that makes a proper usage possible. The change of too many hardware components makes therefore a reactivation necessary. The hardware identifier is non-personal data for Microsoft. It might be pseudonymous data but it is assured that

Microsoft has no reference to it. The same considerations count for the product key that also is unique and processed by Microsoft. The product key is also used by the WGA 1.7 process. At this point it was checked whether the product key could lead to a re-personalization regarding the fact that in the counterfeit replacement scenario of WGA 1.7 Microsoft has to collect personal data (address of the customer, address of the vendor of the counterfeit product) in combination with the product key of the counterfeit software in order to provide a replacement copy of the product. In any case of WGA 1.7 counterfeit replacement, the product key that is combined to a natural person is a stolen key and is not used any longer due to the fact that the customer sends the counterfeit media to Microsoft within this process. In these scenarios, activation is not possible any longer. The evaluation has shown, that no combination of unique identifiers with personal information (like names) is possible within Software Protection Platform.

Single License Activation is also possible in a phone activation scenario. In this scenario the product generates a nearly unique value of the hardware, which is used by the hotline to generate an activation code. The user has to enter this code in a given form. The product then will be activated. The communication lines in this scenario are telephone and cell phone/SMS. In this scenario less unique data are transferred because the hardware identifier is shortened. In this scenario the problem with the machine name that possibly can hold personal information does not come up. There are no personal or at least pseudonymous data in telephone or short messaging service activation.

User privacy is implemented in an adequate way in the Online Activation and Phone/SMS Activation scenarios.

2. OEM Activation

The activation performed by an Original Equipment Manufacturer is done without any personal data. The system is completely activated before it is sold to the user. No further interaction with Microsoft is necessary. This does not apply if the user changes the hardware sufficiently or the user must recover their machine from a recovery media. In this case, the user has to go through the Single License Activation process. User privacy is implemented in an excellent way in the OEM Activation scenario.

3. Volume License Activation with Key Management Server (KMS)

Volume Licenses are products that can activate a defined number of machines. To support companies and public bodies in activating their machines, Microsoft invented the Key Management Server (KMS). This KMS is a machine hosted within the company or a public body that itself is activated by online or phone activation. The KMS manages the activation

of clients within the internal network. Clients or other internal server activate against this KMS machine that distributes the licenses to the machines. KMS only runs in larger networks with at least 25 client machines or 5 server machines. The machines activated by a KMS have to reactivate within a variable period. Administrators of the KMS can choose the period. The maximum reactivation time is 180 days.

Regarding the fact that no communication of internal machines except the first activation of the machine that hosts the KMS server, has to take place with Microsoft, the impact on users' privacy is minimal. Still within internal communication the complete domain name of a machine is used and stored in the KMS database. This domain name also includes the machine name that once again can hold the name of the user. At this point administrators of the network are advised not to use names of natural persons for machines. This is not a privacy breach of SPP but of network administration within the organization using KMS. The user can check the machine name in the following places: "Computer\Properties" und "Control Panel\System".

User privacy is implemented in an excellent way in the KMS activation scenario.

4. Volume License Activation with Volume License Activation Management Tool (VAMT)

For smaller institutions or laboratory scenarios Microsoft offers a downloadable tool called Volume License Activation Management Tool (VAMT) that has several single modules to suffice the demands. VAMT is a mobile application that can run as a proxy server to forward requests from machines that are not connected to the internet and also to run as harvester and distributor to activate a number of machines in a batch job even in complete offline laboratory or high security scenarios. The VAMT Proxy forwards the requests directly to Microsoft SPP servers. Except the machine name that is not transferred, the unique identifiers are forwarded to Microsoft like in the online activation scenario. In this scenario, the IP address that comes up at Microsoft communication layer is the one of the VAMT proxy machine and not the one from the client machine.

User privacy is implemented in an excellent way in the VAMT Activation scenario.

5. Windows Genuine Advantage (WGA)

Windows Genuine Advantage is a module of Microsoft to protect the system against fraudulent use. Windows Genuine Advantage 1.7 for Windows XP is not part of this evaluation. This was evaluated earlier. Never the less there is an interchange of information between SPP and WGA 1.7. This interchange was checked within this evaluation. A WGA testing is necessary to download special content from Microsoft Download Center. Only genuine systems are allowed to get the advantage of receiving special content form the

Download Center. In the SPP scenario, a license request is sent to the SPP module. This SPP internal module checks the integrity of the system and checks the activation state in the activation database. If the check is performed positively, a temporary WGA License is granted. This license is a cryptographic license with the permission to download special content from Microsoft Download Center. This license itself does not hold any information on the client machine. Communication within SPP to get the license is an interchange of module internal information that was already collected. No new information is transmitted during this process.

This is an excellent way of checking the integrity of a system without the enclosure of machine information even internally.

6. Breach Response Tool (BRT)

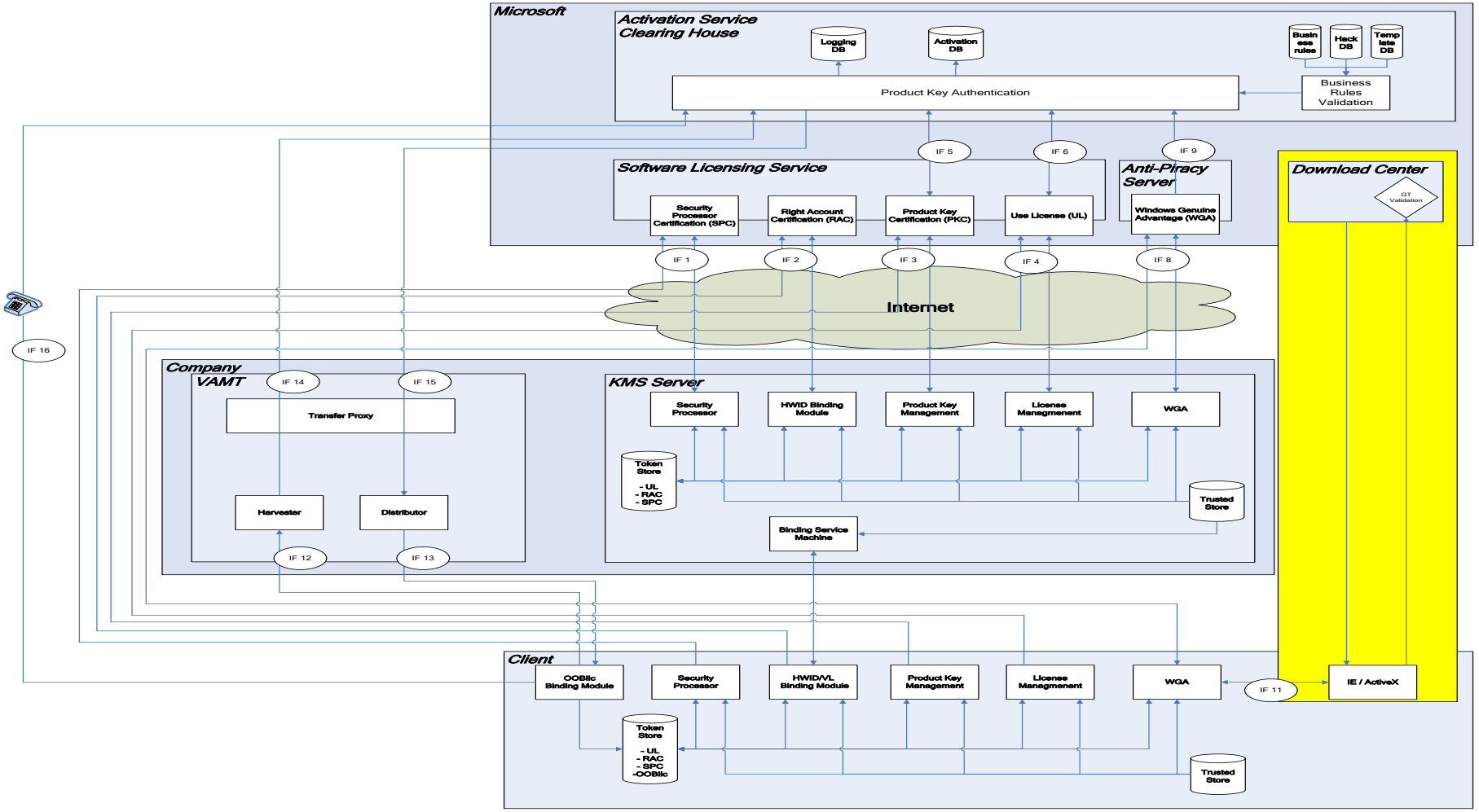
The Breach Response Tool is Microsoft's response on breaches in the security system of SPP. SPP like other products was designed to defend itself against any tamper to deactivate the need of product activation. Software pirates managed to produce exploits that made it possible to use the operating system without activation. These exploits bear the risk of contaminated, unstable systems. To protect the user from these unstable systems, the BRT checks the system against known exploits. The BRT is distributed and triggered by the Windows Update mechanism. In the standard setting the Update Service is deactivated and does not start automatically. If the user decides to automatically install updates at a given time, he is informed, that all updates are installed without further notification. If a user decides to start the Update Service he is informed, that information may be sent to Microsoft. The same information is provided if the user decides to change to automatic updates. In any scenario the user has the option not to install the update that provides BRT.

The user can get additional information on the BRT update by following a link to a connected website. Usually the Microsoft user expects information on the data procession in the Privacy Statement. Today there is no link from the delivered BRT update to the according privacy statement. After a given hint of the evaluator Microsoft decided to add a link from the BRT information page to the relevant privacy statement (http://www.microsoft.com/genuine/downloads/PrivacyInfo.aspx?displaylang=en) by December 1st 2008. This privacy statement will by December 1st 2008 provide additional information on data transmission within BRT. It will be outlined that even if there is no breach still data will be sent by Windows Vista SP 1.

In the RTM mode of Windows Vista, information are only sent, if a breach is found. Vista SP1 always sends information to Microsoft even if the system is untampered. Only in volume license scenarios, this telemetry can be deactivated. The information that will be sent is completely non-personal and is used for statistic purposes.

With view to the fact that the collected data are non-personal, there is no significant impact on the users' privacy. Since only privacy enhancing products should receive a privacy seal, the seal can only be granted under the condition that Microsoft enhances the information given by the BRT update website and the privacy statement until December 1st 2008. This information shall contain a description of BRT and transferred data as well as the fact that telemetry is sent even in unbreached state.

14 Data Flow Model



15 Privacy-enhancing functionalities:

The Software Protection Platform enhances privacy by providing millions of users the possibility

• to validate the activation status of the operating system and ensure a lawful software activation of the operating system for retail and volume license Vista customers,
• to warn users and disable illegal activation tools that have been applied to their Vista operating system and
• to provide users with a possibility to obtain a genuine operating system without the collection of privacy relevant data.

All this is achieved by using smart technologies instead of collecting the user's personal data. This is a leading technology for privacy friendly software activation and copyright protection.

The interaction of local ToE components and Software Protection Platform services uses only pseudonymous, anonymous and non-personal data.

In this way Microsoft as the originator of the Software Protection Platform and the provider of related services respects the privacy of users of the operating systems Windows Vista and helps users to remove illegal activation tools that have been previously installed which carry the inherent risk of privacy breaches of the user data processed on unlawfully activated operating systems.

16 Issues demanding special user attention:

The evaluation has shown, that within the installation process the default setting of the Machine Name is the first chosen username with the appendix –Computer. Regarding privacy concerns, we advice the user to change the Machine Name to a non-personal name. Microsoft has changed the storage procedure to exclude this potential personal information from any database. By January 19th 2009 an update is provided that excludes the machine name from being sent on client side.

A second privacy related hint concerns the so-called Breach Response Tool that is deployed as an important update (KB940510) and triggered by Microsoft Update. This mechanism

checks the system state. With Vista RTM no telemetry is sent to Microsoft but with Vista SP 1 telemetry is sent even if the system is untampered. Still it needs to be mentioned that there are only non – personal data that are sent in telemetry. Sending of telemetry can only be disabled in Volume Activation scenarios. Microsoft adds a link from the website linked to the BRT Update to the privacy statement on http://www.microsoft.com/genuine/downloads/PrivacyInfo.aspx. The privacy statement will provide additional information on data transmission within BRT. It will be outlined that even if there is no breach still data will be sent by Windows Vista SP 1 to Microsoft. This additions will be done by December 1st 2008.

17 Compensation of weakness

There is no privacy weakness within SPP that needs to be compensated.

18 Decision table on relevant requirements:

Privacy Evaluation Requirement	Decision	Remarks
Data Avoidance and Minimisation	excellent	The SPP uses IP addresses for the purpose of communication. Besides that SPP does not use any personal data. The activation is done on the basis of some rare non-personal system identifiers. Even the BRT mechanism only uses system identifiers to find and report the system status.
Transparency	adequate	Microsoft provides well structured privacy information. This information is written in an easy to understand way.

Technical-Organisational Measures	excellent	The technical and organisational measures taken by Microsoft are exemplary. Microsoft has invented a activation mechanism that is based on cryptographical certificates.
Data Subjects' Rights	not applicable	In general there are no personal data that is transmitted to Microsoft therefore, there Microsoft does not have to provide special data subjects' rights.

19 Summary of the audit results

Both legal as well as technical evaluation have shown that the Software Protection Platform implements software product activation in a privacy friendly way. The activation is done without the storage of any personal data. Within the activation process a unique certificate is generated that activates the operating system. This certificate holds the encrypted and signed response of Microsoft Activation Service. The same privacy friendly mechanism is used to perform a WGA testing on the system. Within Volume Activation scenarios, the privacy can be protected by the usage of company internal activation servers. In these cases only the machine that holds the server needs to be activated against Microsoft. All other company internal machines activate against this company internal activation server. No further transmission to Microsoft takes places in these scenarios.

The communication between SPP and WGA to grant a WGA license is also implemented in a privacy friendly way. No personal data or even unique identifiers that make a repersonalization possible are transferred between the two services within Microsoft. The WGA module in SPP generates and signs a download license that is transferred to the WGA service. This license is temporary but does not hold any identifier that encloses any personal information.

The last evaluated scenario, the Breach Response Tool, was implemented into SPP because of some breaches in the security system. With the usage of an exploit that deactivates Microsoft security mechanisms there is also a risk of unexpected crashes of the operating system and privacy breaches of user data. BRT is only performed in a Windows Update process. Users that do not perform updates do not receive BRT. If BRT finds an exploit on the user's system, it leads the user back to a stable system status. Within BRT telemetry is send to Microsoft, but no personal data is transferred to Microsoft.

As an overall assessment, SPP is an efficient License Protection Tool that sufficiently protects Microsoft software against tampering and therefore users of SPP equipped Microsoft software against privacy breaches.

Experts' Statement

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

Bonn, date | Marcus Belke, 2B Advice GmbH | Signature of Legal Expert

Place, date | Stephan Di Nunzio, TüV IT | Signature of Technical Expert

Certification Result

The above-named IT product / IT-based service passed the EuroPriSe and ULD Datenschutz Gütesiegel 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 security.

Kiel, date | Signature