Privacy Audit

Short Report Version 1.0a

-FINAL-

Target of Evaluation (ToE)

Windows Genuine Advantage 1.7

Date audit took place

December 2006 to August 2007

Name and address of the applicant

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

Name and addresses of the experts

2B Advice GmbH
2B Secure Evaluation Body for Privacy (Legal)
Head: Marcus Belke, Attorney at Law
Wilhelmstr. 40-42
53111 Bonn
Germany
marcus.belke@2b-advice.com

TÜV Informationstechnik GmbH:
Evaluation Body for Privacy (Technical)
Head: Dr. Silke Keller
Langemarckstrasse 20
45141 Essen
Germany
s.keller@tuvit.de

Short description of the IT Service

Windows Genuine Advantage 1.7

More detailed description of the service

Microsoft Windows Genuine Advantage (WGA 1.7) containing Validation, Notification, Legalization and Counterfeit Replacement.
The results of the privacy audit are only applicable to WGA 1.7. The products must be used in the following environment:

Operation systems: Windows XP Home Edition SP2, Windows XP Professional SP2, Internet Explorer 6.0 and higher.

The user of WGA 1.7 have to assure that the used Computer is protected sufficiently using virus scanning tools and firewalls against malicious code or direct attacks which may be used to harm the privacy functions of the TOE.

Windows Genuine Advantage (WGA) 1.7 is a service to differentiate the genuine Windows experience from the non-genuine experience by reserving some Microsoft services and assets for customers on genuine Windows systems only.

The user of a Windows XP Home Edition SP2 or Windows XP Professional SP2 with Internet Explorer 6.0 and higher will pass through a system genuine check prior to accessing downloads or updates marked as genuine-only. This genuine check performs validation tests of the system against several criteria for license legitimacy. The results of this system validation determine whether or not the user is given access to the marked downloads and, if not, provides appropriate reporting of software piracy.

The WGA gateway 1.7 is being set up and operated by developing several components:

- Validation 1.5
- WGA Notifier Tool 1.7
- Legalization 1.7
- Counterfeit Replacement 2.0

Validation 1.5 is the core service within the ToE. It is designed to detect “any software that has been activated through Microsoft using a Product ID that is now blocked by the company” because it is known to be used fraudulently.

WGA Notifications Tool 1.7 is a tool that will raise awareness of the WGA program and the advantages of genuine Windows. It does so by detecting if the system is genuine, informing the user if their system is not genuine thru several user interfaces and providing legalization assistance as necessary. WGA Notifications Tool makes use of Validator to detect if the system is genuine.

Once a given system has been detected to be non-genuine, Legalization provides a means to legalize the system by offering the user an opportunity to purchase a legal copy and to alter the installation in place in a way that least affects this installation.

Purpose of the **Legalization 1.7** and **Counterfeit Replacement 2.0** process is to help Microsoft customers to replace a non-genuine copy of a Microsoft operating system with a genuine copy. This shall in particular be possible for the customers that received a copy that is not obviously an illegal copy. There are a lot of non-genuine copies being regularly sold to vendors and to end-customers where it is hard to tell whether it is a non-genuine or a genuine copy of a Microsoft product. To not upset those customers and to possibly find out more about the responsible persons behind those copies Microsoft provides genuine Microsoft operating system copies to the customer after he/she has filled in a counterfeit report and named the fraudulent reseller.

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

- Microsoft Visual Studio.Net Professional 2003
- Microsoft Office Professional Edition 2003
- Microsoft Office Visio Professional 2003
- Microsoft Office Project Professional 2003
- Microsoft Product Studio 2.10
- Microsoft Source Depot 3.0
- Microsoft FxCop 1.3
- Microsoft SQL Server 2000
- Warbird 1.1.10
- Product Studio, Version 2.10.6729.0

Purpose and Usage Environment

TÜV Informationstechnik GmbH (TÜViT), Essen – Member of TÜV NORD Group – and 2B Secure - the Evaluation Body for Privacy of 2B Advice GmbH - evaluated by order of Microsoft Inc., Redmond, Microsoft Windows Genuine Advantage 1.7 (WGA) from December 2006 to August 2007. A legal audit of Microsoft's statements, policies and specifications was performed to set the requirements for a technical audit which, in turn, determined that the program's databases and implementation respect privacy concerns. The realization of the evaluation occurred on basis of documents, statements, and technical testing. MS has signed the Safe Harbor agreement for human resources and customer data on 29th of June 2001.

The major goal of Windows Genuine Advantage (WGA) 1.7 is to increase the shipment mix of licensed versus unlicensed Windows XP and Windows Vista. Even though Windows Vista partly uses the WGA 1.7 implementation, it is not part of this evaluation. Since the software

piracy problems lead to more and more revenue loss, Microsoft implements with the Target of Evaluation a service gateway and tools to make it more attractive to customers to use genuine software. Targets for Microsoft are to attract demand for genuine-only registration with an opt-in Windows “bonus” program (i.e. “Photo Story, Scientific Calculator, Security Tools, media player” download), align and launch “Genuine” Windows initiatives with targeting “bonus” content/downloads to campaign themes, enable a value added download experience for product or subscription customers in the Download Center (i.e. “Premium” Downloads):

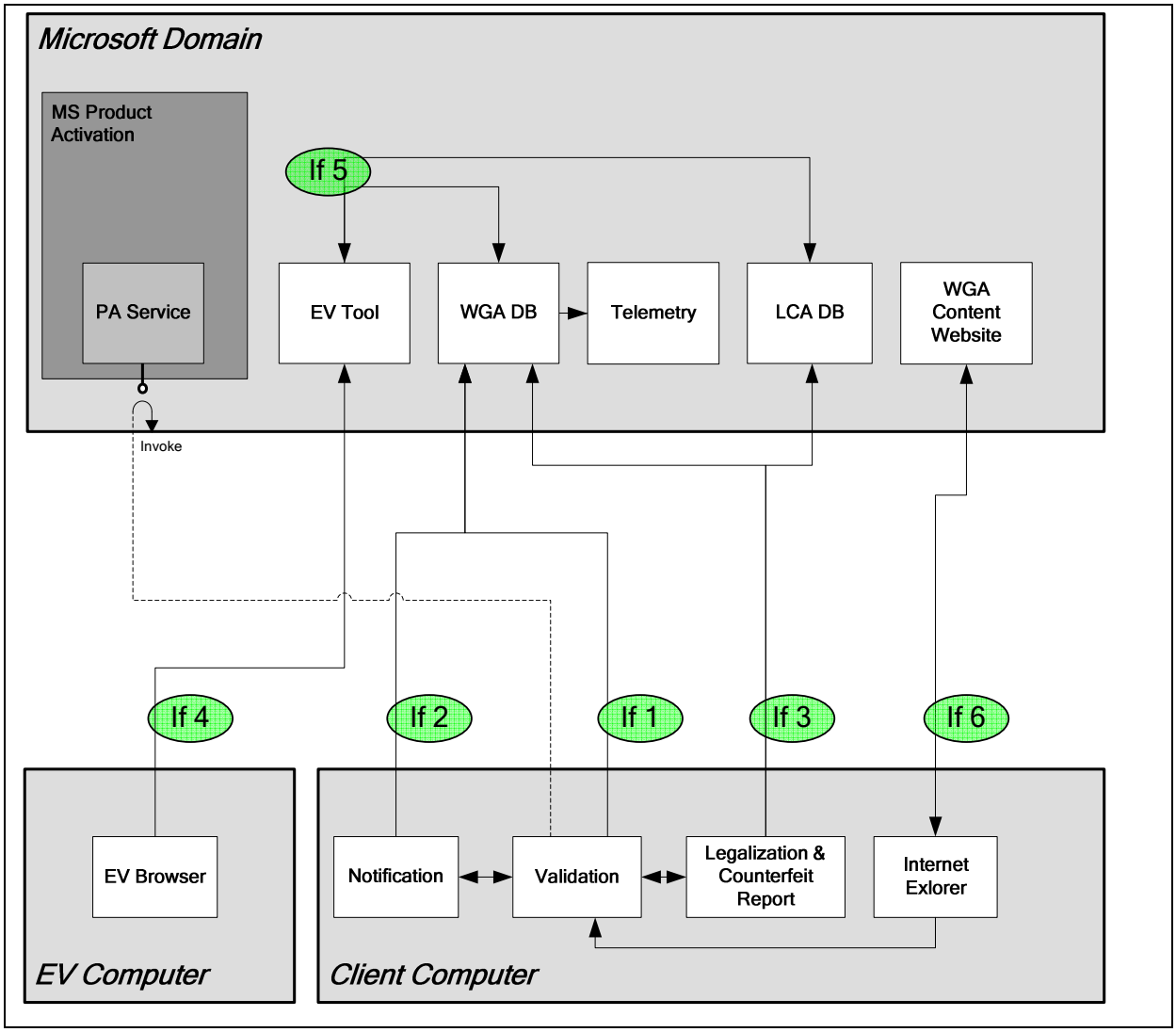
- by getting consumers to demand “genuine” Windows XP (based on awareness of ongoing value)
- creating a customer feedback loop to OEM/SBs driven by consumer awareness of whether their Windows is genuine by reducing available product key inventory that can be pirated (drive activation of SLP PCs) without gathering explicit personal user data.

Therefore, the Software does not aim to enrich the user security or data protection strategy of a valid system. It is primarily a tool to protect Microsoft’s revenues from the products Windows XP and Windows Vista and part of the anti piracy strategy. It does protect users of non-genuine systems, by identifying manipulated and therefore unsafe Windows systems.

Microsoft Windows Advantage Gateway 1.7 may be used on systems that are private, public, in companies or belonging to public authorities as long as the systems have Microsoft Windows XP, Microsoft Windows Vista and Internet Explorer 6.0 installed. But the usage of this software is conditionally to get future software upgrades or additional software from Microsoft, which will be distributed online to customers like private persons, companies or public institutions.

Thus secondarily, it is important for all users of the Microsoft operating systems, whether they are located in authorities, in private companies or at home, that this system can be used within the rules of the privacy laws and without being afraid that data protected by privacy laws is being transferred.

168 **Overall Modeling of the data flow**



169

170

The validation component provides the core functionality by retrieving and processing system information of the client computer as they are: Computer make and model, Version information for the operating system and software using Genuine Advantage, Region and language setting, a unique number assigned to your computer by the tools, Product Key (hashed) and Product ID, BIOS name, revision number, and revision date, Hard drive volume serial number (hashed) and the IP Address.

Only the Product Key, Product ID and Hardware ID are also transmitted from validation to the PA (Product) webservice in order to check the “genuine” state of the system. Although, the Product Activation webservice and the involved data flow were not part of the evaluation, the evaluators have checked on a document basis the data going to the product activation service and the return value.

The validation component sends a data block to the WGA database providing information on the validation performed together with data on the environment the validation was performed in. This data is then analyzed, aggregated and stored in the WGA database. If the system is detected being not genuine, the user will be informed on this circumstance by the WGA Notification Tool.

Legalization and Counterfeit Report are not executed on the client computer but are basically web pages offering the user of the client computer the opportunity to legalize the system by either purchasing a valid copy or by receiving a free copy based on a counterfeit report entered by the user. Within the Counterfeit Report, the user has to give his contact information, contact information of the reseller that sold the software, the circumstances of purchase (e.g. Price, Date and Payment Method). Additionally there is information on the computer system that will be gathered by an automatic process (e.g. Operating System Type and Service Pack Status,…). All data is deleted as soon as there is no reason for storage like providing the genuine replacement software or further prosecution against the reseller.

The IP Address is in general used to communicate with the Microsoft Service. The retention time for this usage of the IP address is seven days.

Besides that the IP Address is used during validation to look up the region where the system is located to identify regions were Non Genuine Copies are used more often. A person cannot be identified since the closest possible resolution would be the city. Only for Volume License Key users, it is used to also determine the domain name looked up in a public databases like RIPE. This means that the domain name resolved from the IP will continue to be stored, but only when it shows up together with to a volume license key. The IP address used within validation is in any case being deleted right after the lookup.

The EV (Evaluation Vendor) browser on the server side is again a web application that allows a well-defined set of users closely related to Microsoft to cross-check Counterfeit Reports by examining either the CDs sent physically by the counterfeit victim with a reference to the Counterfeit Report or a scanned image of the CD sent by mail and stored together with the Counterfeit Report. The EV user has to decide whether the quality of the counterfeit is good enough to grant the Counterfeit Report sender a free copy. Otherwise a rejection letter is created. EV users are not customers but employees of either the Microsoft Corporation or of a third party and only receive pseudonymous data: CRID (Next number), Shortened Guide and the product by mail from the Microsoft Customer without further Access to the Microsoft databases. The only third party running the Evaluation Vendor Tool and that has also access to the MS WGA databases is IP Services Inc. This Vendor has committed itself to the “Standard Privacy Language for Contracts involving a Company Acting as an Agent for Microsoft” that guarantee the necessary level of privacy protection. Further more the contract with the PID Vendors gives them strict rules how to go on with any occasions. The PID Vendor can only process data on the basis of these instructions given by Microsoft and the evaluation vendor process can be regarded as commissioned data processing in the meaning of section 11 BDSG.

Version of the requirement catalogue

Version 1.2

How the product enhances privacy

The product enhances privacy by using anonymized and pseudonymized data in most of the processes. The product uses sophisticated methods to discover and fight software piracy and counterfeit products without the usage of personal data.
At the point where pseudonymized data have to be processed, a great importance is attached to the fact that these pseudonyms cannot be resolved to natural persons and the mass of data used in total cannot be used to identify a user.

Even though much pseudonymous data is used to run the service it is technically insured that it is not possible to identify a natural person. In addition to the technical measures Microsoft implemented organizational measures to secure privacy. Besides the regular Microsoft Privacy and Security Guidelines in place, there are strict WGA team self – obligations that are in place to prevent any attempt of combination of information from other teams within Microsoft. These self-obligations and policies are controlled by an implemented regular auditing process within Microsoft and regard also data economy and data retention times for the use of the counterfeit replacement processes.

A WGA policy prevents the usage of the data by other teams and audit processes in place, run by the Microsoft Privacy Specialists to check on a regular basis that the self-obligations are in place. For WGA Advantage team, the privacy specialists have to additionally demonstrate at least every six month that the Windows Genuine Advantage team:

1. Does not share or merge WGA user's personal or pseudonymous data with other teams in any way that would allow the WGA team or any other team to learn more about a given user.
2. Collects only the information necessary to meet the WGA business needs and limits the use of pseudonymous and private data to what is required by the scope of the WGA services.
3. Abides by all stated retention times, specifically those around the deletion of user's IP addresses and the personal data collected through the Counterfeit Report.

Beside the self obligations, ingenious techniques like one way hash functions are used to protect privacy. In all cases the hash that is created is in a smaller space and represents a significant data loss, ensuring that the hash is irreversible and not completely unique. Identifiers used by WGA are only usable for WGA purpose, because they are exclusively produced by the WGA team.

Summary of the audit results

The TÜV Informationstechnik GmbH (TÜViT), Essen – Member of TÜV NORD Group - and 2B Secure - the Evaluation Body for Privacy of 2B Advice GmbH – evaluated in order of Microsoft Inc., Redmond, the Windows Genuine Advantage Version 1.7 for Microsoft Windows XP in December 2006 to August 2007. A legal audit of Microsoft's statements, policies and specifications was performed to set the requirements for a technical audit which, in turn, determined that the program's databases and implementation respect privacy concerns. The realization of the evaluation occurred on the basis of documents, interviews, statements and technical testing.

MS has signed the Safe Harbor agreement for human resources and customer data on 29th of June 2001.

Within the validation- and notification-part of the ToE, the vast majority of data collected, processed and used do not represent personal data even though a variety of pseudonymous data types are collected, processed, and used. However, no personal data within the sense of section 3 (1) BDSG, are collected, used, and processed, because of the fact that the reference list of these pseudonyms is not accessible to Microsoft. Even the UGUID, a unique number assigned to each user's computer, has to be regarded as pseudonymous because it represents a hash value of the used hardware, which is even for Microsoft not re-engineerable. The combination of all aliased data does not give any hint to a natural person. Sufficient technical and organizational measures are implemented to guarantee that the pseudonyms cannot be uncovered.

In the legalization and counterfeit replacement process, personal data is stored and processed. Due to the demand of separation, the used data is stored in different databases. One database with pseudonymous data is accessible to the evaluation vendors, that have to evaluate the quality of the counterfeit software and the second database, containing personal data of the applicant, is only accessible to Microsoft. An abdication of personal data in the legalization and replacement process is not possible, because on the one hand Microsoft needs personal data from the applicant to ship the genuine replacement and on the other hand they need the applicant as a witness in the process of enforcement and litigation against a fraudulent reseller. Regarding the principle of data reduction and data economy Microsoft erases personal data as soon as the purpose for which the data was stored, is achieved. Due to these justified interests, the collection, storage and usage of personal data is admissible by German data protection law.

With view to employees of the public administration or public officials the collection, processing, usage, storage and transmission of aforementioned data may be considered to be covered either by the permission of sections 13(1) BDSG and 14(1) BDSG in conjunction with section 14(4) and 16 BDSG or by the respective sections of the LDSG of the Länder, e.g. section 11 (1 Alternative 3) LDSG-SH and section 13(2) LDSG-SH as well as sections 16 LDSG-SH. With view to employees of non-public bodies the collection, processing, usage and transmission of aforementioned personal data may be considered to be covered by the permission of section 28 BDSG.

Microsoft has stated that they publish a new privacy statement with changes concerning the counterfeit replacement process and the processing of data in the USA until the 1st of October 2007 at the latest. In total the user is well informed on the processed data.