



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

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



31

32

Short Public Report

33

2

34

3 Name and version of the IT product:

35

Microsoft Software Protection Platform (SPP)

36

37

4 Manufacturer of the IT product:

38

Microsoft Corporation

39

One Microsoft Way

40

Redmond, WA 98052-6399

41

USA

42

43

5 Time frame of evaluation:

44

June 2007 to November 2008

45

46

6 EuroPriSe and ULD Experts who evaluated the IT product:

47

Evaluation Body for Privacy / EuroPriSe Expert (Legal)

48

Marcus Belke, Attorney at Law

49

Oliver Gönner, Attorney at Law

50

2B Advice GmbH

51

Wilhelmstrasse 40-42

52

53111 Bonn

53

Germany

54

marcus.belke@2b-advice.com

55

56

Evaluation Body for Privacy / EuroPriSe Expert (Technical)

57

Stephan Di Nunzio

58

TÜV Informationstechnik GmbH

59

Langemarckstrasse 20

60 45141 Essen
61 Germany
62 S.DiNunzio@tuvit.de

63

64 **7 Certification Body:**

65 **Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein**
66 Holstenstr. 98
67 D-24103 Kiel
68 Germany

69 **8 Specification of Target of Evaluation (ToE):**

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

73

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

76

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

79

80 The main usage scenarios of Software Protection Platform are:

81 Single License Activation

82 Activation by Original Equipment Manufacturer (OEM)

83 Volume License Activation with Key Management Server (KMS)

84 Volume License Activation with Volume License Activation Management Tool (VAMT)

85 Windows Genuine Advantage (WGA)

86 Breach Response Tool (BRT)

87

88 The genuine test in general as well as the update mechanism are not part of the ToE. The

89 WGA 1.7 and MU 6.0 components have been evaluated for Windows XP in an earlier privacy

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

92 **9 General description of the Product**

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

104
105 The Software Protection Platform provides two main entry points. The first entry point to
106 Software Protection Platform is the software activation that every product has to perform at
107 least once. Before a Microsoft operating system that uses Software Protection Platform can
108 be fully used, it has to be activated. The second entry point to Software Protection Platform
109 is the validation of the genuine state of software within any download of specially protected
110 software from Microsoft. The genuine test is necessary to access the Microsoft Download
111 Center or Windows Update. These Windows downloads and updates will only be available for
112 genuine Windows systems.

114 **10 Transnational issues**

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

118 **11 Tools that were employed to the production of the IT-product**

119 Microsoft Visual Studio .Net Professional 2003 & 2008
120 Microsoft Office Professional Edition 2003 & 2007

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

121 Microsoft Office Visio Professional 2003 & 2007
122 Microsoft Office Project Professional 2003 & 2007
123 Microsoft Product Studio 2.10.6729.0
124 Microsoft Source Depot 3.0
125 Microsoft FxCop 1.3
126 Microsoft SQL Server 2000
127 Warbird 1.1.10
128 Microsoft Prefast
129 Microsoft Prefix
130 Microsoft APTool
131 Microsoft SQL Server
132

133 **12 Version of the requirement Catalogue**

134 ULD Requirements Catalogue, Version 1.2 (August 29, 2005)
135 EuroPriSe Catalogue, Version 0.2 (December 13, 2007)
136

137 **13 Evaluation Results**

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

141

142 1. Single License Activation

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

149

150 In the Single License Activation scenario, the user buys Windows Vista or Windows Server
151 2008 in a store and installs it on an arbitrary computer system. In this case, he has to
152 activate the system either online or by telephone. In some countries activation can be
153 alternatively performed by cell phone's short messaging service (sms).

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

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

162
163 The evaluation showed that on the connection to Microsoft no personal data are transmitted.
164 As a matter of online communication, still the IP address of the machine is transferred. The
165 IP address is only used and stored as long as necessary to answer the request of the client
166 machine.

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

177
178 After a hint within the evaluation process, Microsoft decided to stop recording both IP
179 address and Machine Name by October 17th 2008. The transmission of the Machine Name
180 will be completely stopped by a client update on January 19th 2009. Due to TCP/IP
181 communication needs, the transmission of the IP address cannot be shut off completely, but
182 the data only will be stored as long as necessary to communicate.

183
184 Beside this some other non-personal data but unique data like hard- and software checksums
185 as well as the product key are transferred to Microsoft in four communication steps. The
186 unique hardware identifier is built on the client's hardware. This hardware information is
187 used to bind the final license that makes a proper usage possible. The change of too many
188 hardware components makes therefore a reactivation necessary. The hardware identifier is
189 non-personal data for Microsoft. It might be pseudonymous data but it is assured that

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

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

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

212

213 2. OEM Activation

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

220

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

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

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

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

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

241

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

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

254

255 5. Windows Genuine Advantage (WGA)

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

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

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

272

273 6. Breach Response Tool (BRT)

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

286

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

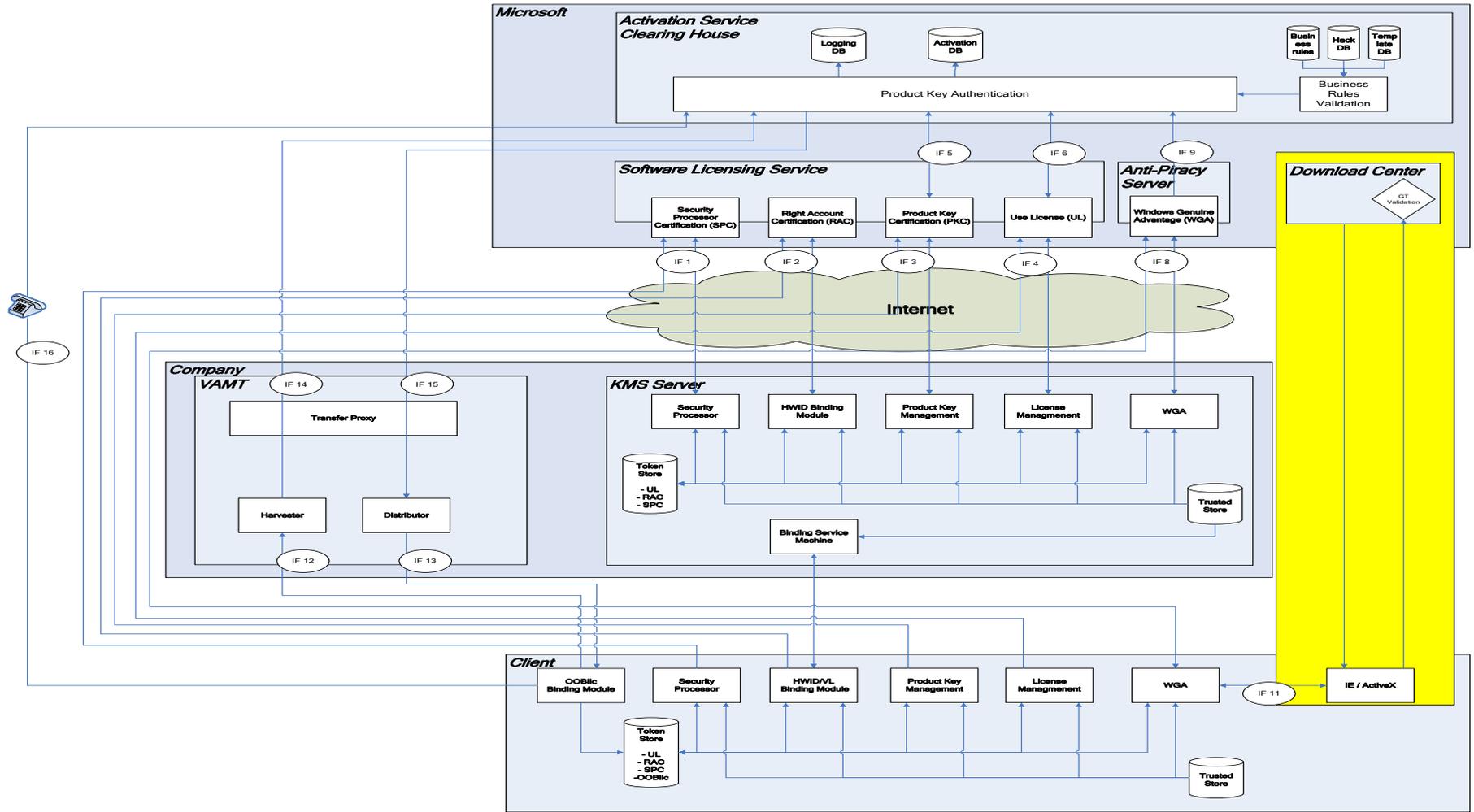
296

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

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

307

308



310
311

312 **15 Privacy-enhancing functionalities:**

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

- 315
- 316 • to validate the activation status of the operating system and ensure a lawful software
 - 317 activation of the operating system for retail and volume license Vista customers,
 - 318 • to warn users and disable illegal activation tools that have been applied to their Vista
 - 319 operating system and
 - 320 • to provide users with a possibility to obtain a genuine operating system
 - 321 without the collection of privacy relevant data.

322

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

325

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

328

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

334
335

336 **16 Issues demanding special user attention:**

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

343

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

346 checks the system state. With Vista RTM no telemetry is sent to Microsoft but with Vista SP
 347 1 telemetry is sent even if the system is untampered. Still it needs to be mentioned that there
 348 are only non – personal data that are sent in telemetry. Sending of telemetry can only be
 349 disabled in Volume Activation scenarios. Microsoft adds a link from the website linked to the
 350 BRT Update to the privacy statement on
 351 <http://www.microsoft.com/genuine/downloads/PrivacyInfo.aspx>. The privacy statement will
 352 provide additional information on data transmission within BRT. It will be outlined that even
 353 if there is no breach still data will be sent by Windows Vista SP 1 to Microsoft. This
 354 additions will be done by December 1st 2008.

356 **17 Compensation of weakness**

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

358

359 **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.

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

360

361 **19 Summary of the audit results**

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

372
373 The communication between SPP and WGA to grant a WGA license is also implemented in a
374 privacy friendly way. No personal data or even unique identifiers that make a
375 repersonalization possible are transferred between the two services within Microsoft. The
376 WGA module in SPP generates and signs a download license that is transferred to the WGA
377 service. This license is temporary but does not hold any identifier that encloses any personal
378 information.

379

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

387

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

391

392

