MICROSOFT WORK GROUP SERVER PROTOCOL PROGRAM
LICENSE AGREEMENT
(NO PATENTS)
FOR DEVELOPMENT AND PRODUCT DISTRIBUTION

This **Microsoft Work Group Server Protocol Program License Agreement (No Patents) for Development and Product Distribution** (the "**Agreement**") is entered into between Microsoft Corporation, a Washington corporation, with offices at One Microsoft Way, Redmond, Washington 98052-6399 U.S.A. ("**Microsoft**"), and the person(s) or company(ies) identified as Licensees below, all of whom are jointly and severally liable under this Agreement ("**Licensee**"), effective as of the date it has been signed on behalf of all parties (the "**Effective Date**").

Licensee Full Legal Name: **Protocol Freedom Information Foundation**
~~(parent)~~
Type of Legal Entity (corporation, company, partnership, sole proprietorship or other): **Non-profit Corporation**
State/Province Organized: **Delaware**
Street Address: **1995 Broadway**
City, State (or equivalent), Country and Postal Code: **New York, New York 10027 U.S.A.**
~~DUNS #:~~
Licensee Contact Name: **Ms. Rachel Wiener**
Phone Number: **212-461-1904**
email: **rachel@softwarefreedom.org**
~~Fax Number:~~
~~***[Licensee may execute the agreement on behalf of its wholly-owned subsidiaries]***~~
~~***[add the following for each licensee affiliate also licensed under this agreement]***~~
~~Licensee Full Legal Name: (subsidiary)~~
~~Type of Legal Entity (corporation, partnership, sole proprietorship or other):~~
~~State/Province Organized:~~
~~Licensee Legal Advisor Contact Information, if any:~~
~~Legal Advisor Name:~~
~~Legal Advisor Contact Phone Number:~~
~~Legal Advisor Contact Fax Number:~~
~~Licensee Support Phone Number:~~
~~Licensee Support Website:~~

Table of Exhibits

Exhibit A	Licensed Protocols
Exhibit B	Program Entry Requirements (applicable as of the Effective Date)
Appendix 1	WSPP Pricing Principles and Available Protocols
Appendix 2	Protocol Technical Documentation Specifications
Appendix 3	Third Party IP Claims (as of the Effective Date)
Appendix 4	European Union and United States Patents and Patent Applications

1. Definitions. Capitalized terms used in this Agreement are defined in this **Section 1** or elsewhere in this Agreement.

1.1 "**Commission**" means the Commission of the European Communities.

1.2 "**Confidential Information**" has the meaning set forth in **Section 5.1**.

1.3 "**Decision**" means the Commission of the European Communities Decision dated March 24, 2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792-Microsoft-Decision).

1.4 “**Distribute**” or “**Distribution**” means licensing (including the right to modify and redistribute source code versions of ~~Licensed Server~~ Implementations), distributing, providing online access to, importing or otherwise making available in any manner to a third party.

1.5 “**Licensed Protocols**” means the WSPP Protocols listed in **Exhibit A**.

1.6 “**Microsoft Licensed Intellectual Property**” means the following intellectual property in the WSPP Protocols or WSPP Documentation that Microsoft owns or has the right to sublicense without a fee: (a) know-how, industrial secrets, trade secrets and confidential information embodied in the WSPP Protocols or disclosed by the WSPP Documentation; and (b) copyrights in the WSPP Documentation, and, to the extent necessary for Licensee to exercise its rights under the scope of the license granted in **Section 2.1** of this Agreement, in the WSPP Protocols. For purposes of clarification, Microsoft Licensed Intellectual Property does not include any rights under Microsoft patents or patent applications. Microsoft acknowledges that by signing this Agreement, Licensee is not waiving its right to contest the validity of any of Microsoft’s patents, know-how, industrial secrets, trade secrets and confidential information embodied in the WSPP Protocols and disclosed by the WSPP Documentation, or copyrights.

1.7 “**Program Entry Requirements**” means the WSPP program entry requirements posted on the WSPP Website from time to time.

1.8 “**Protocol**” means a set of rules of interconnection and interaction between various instances of Windows Server Operating Systems and Windows Client Operating Systems running on different computers in a Windows Work Group Network.

1.9 “**Service Pack**” means updates that Microsoft makes commercially available as a “service pack” to a Windows Client Operating System or a Windows Server Operating System, under the applicable end user license agreement for such product.

1.10 “**Subject Patent Claims**” means those claims of Microsoft-owned or Microsoft-controlled patents that are contained in a patent or patent application that: (a) is listed in Appendix 4; (b) issues from any of the pending patent applications listed in Appendix 4; (c) issues from an application with a priority date that is after the Effective Date, provided Microsoft has provided Licensee with an updated version of Appendix 4 that contains such patent application no later than 45 days after the date such patent application has been filed; (d) is added to Appendix 4 following an update to the WSPP Documentation that causes such patent or patent application to read upon the WSPP Documentation, provided Microsoft has provided Licensee with an updated version of Appendix 4 that contains such patent or patent application no later than 45 days after the date the updated WSPP Documentation is made available to Licensee; (e) issues from any continuation, continuation-in-part, or divisional that has priority based upon any of the patents described in (a), (b), (c), or (d) above; or (f) is a re-issue, renewal, substitution, re examination or extension of any of the patents described in (a), (b), (c), (d), or (e) above. Microsoft typically publishes patent applications within eighteen (18) months after the date of the application. In addition, upon Licensee’s request at any time after notice under (c) or (d) is provided to Licensee (or, with respect to the applications listed in Appendix 4 as of the Effective Date, then upon Licensee’s request any time after the Effective Date), Microsoft will promptly provide Licensee with a copy of any unpublished application identified in such notice, together with the citation list to prior art cited in such application or its counterparts. Subject Patent Claims also do not include any claims (1) to any underlying or enabling technology that may be used or needed to make or use an Implementation, or (2) to any implementation of specifications or technologies that are merely referred to in the body of the WSPP Documentation.

1.11~~1.10~~ “**Trustee**” means a trustee appointed by the Commission pursuant to the Decision and the Commission Decision of 28.7.2005 (C (2005) 2988 final) .

1.12~~1.11~~ “**Update**” means any critical fix or recommended modification to, or updated component for, a Windows Client Operating System or a Windows Server Operating System, that Microsoft develops and makes commercially generally available (e.g., through its website or any other general distribution means) for the product to which the update applies~~, (e.g., Windows Update or successor site),~~ under the applicable end user license agreement for such product.

1.13~~1.12~~ “**Windows Client Operating Systems**” means the software marketed, distributed and licensed by Microsoft as Windows 98, Windows 98 Second Edition, Windows Millennium Edition, Windows NT Workstation 4.0, Windows 2000 Professional, Windows XP Professional, Windows XP Home, or Windows Vista, including updates (which include, without limitation, security patches) and upgrades (both described in **Section 3.2(a)**) thereto, or their successors (including updates and upgrades thereto) for use on personal computers. "Windows Client Operating Systems" do not include Windows XP Embedded or its successors, Windows CE or its successors, or any other operating system designed for use with non-PC devices such as gaming consoles, television set-top boxes, mobile telephones and personal digital assistants.

1.14~~1.13~~ "**Windows Server Operating Systems**" means the software marketed, distributed and licensed by Microsoft as Windows NT Server 4.0, Windows 2000 Server Standard Edition, Windows Server 2003 Standard Edition, and Windows Server 2008, including updates (which include, without limitation, security patches) and upgrades (both described in **Section 3.2(a)**) thereto, or their successors (including updates and upgrades thereto).

1.15~~1.14~~ "**Windows Work Group Network**" means any group of (i) personal computers connected to a network and on each of which a Windows Client Operating System is installed and (ii) Windows Work Group Servers, linked together via a computer network. "**Windows Work Group Server**" means a computer connected to a network and on which a Windows Server Operating System is installed.

1.16~~1.15~~ **"WSPP"** means the Microsoft Work Group Server Protocol Program licensing program made available by Microsoft and described at the WSPP Website.

1.17~~1.16~~ "**WSPP Development Agreement**" means a then current version of a Microsoft protocol license agreement for development and product distribution entered into by Microsoft and a licensee under the WSPP.

1.18~~1.17~~ "**WSPP Development Licensee**" means another licensee under a WSPP Development Agreement, who has satisfied applicable Program Entry Requirements.

1.19~~1.18~~ "**WSPP Documentation**" means the specifications for the WSPP Protocols, including updates and corrections per **Sections 3.2 and 3.3(a)**, provided by Microsoft pursuant to Article 5 of the Decision and under this Agreement (and absent a specific reference to WSPP IDL Documentation, includes WSPP IDL Documentation).

1.20~~1.19~~ "**WSPP IDL Documentation**" means the Interface Definition Language (IDL) specifications for the WSPP IDLs.

1.21~~1.20~~ "**WSPP IDLs**" means the file & print and user & group administration IDLs associated with certain WSPP Protocols. WSPP Protocols with which WSPP IDLs are associated as of the Effective Date are identified in **Table A-2** of **Appendix 1**.

1.22~~1.21~~ **"WSPP Protocols"** means the file & print and user & group administration Protocols disclosed by Microsoft pursuant to Article 5 of the Decision and that are available for license under the WSPP (and absent a specific reference to WSPP IDLs, includes WSPP IDLs). The WSPP Protocols as of the Effective Date are listed in **Appendix 1**, and include updates and corrections per **Sections 3.2 and 3.3(a)** of this Agreement.

1.23~~1.22~~ "**WSPP Website**" means the website located at

http://www.microsoft.com/mscorp/legal/eudecision or successor site.

2. License Grant; ~~Licensed Server~~ Implementations; License Clarifications; No Microsoft Statements; No Other Rights; Discussion of Licensing Terms; Notification Regarding Other Licenses

2.1 License Grant.

(a) General. Effective upon Licensee's fulfillment of all Program Entry Requirements, Microsoft hereby grants to Licensee a world-wide, non-exclusive, personal license under the Microsoft Licensed Intellectual Property to make copies of the WSPP Documentation and to receive and use the Confidential

Information in order to develop, make, use, and Distribute ~~Licensed Server~~ Implementations (as defined below), subject to all provisions of this Agreement.

(b) Subcontracting. Licensee may contract with a third party to develop, consistent with all of the terms of this Agreement, ~~Licensed Server~~ Implementations on Licensee's behalf (**“Subcontractor”**) provided that any such contract must contain terms requiring any and all third party Subcontractors to comply with obligations no less restrictive than the applicable terms of this Agreement, including but not limited to **Sections 2 and 5** of this Agreement. Further, nothing in this Agreement shall preclude any such third party Subcontractor from performing similar development work for any other WSPP Development Licensee, pursuant to their WSPP Development Agreement.

2.2 “~~“**Licensed Server**~~ **Implementation(s)**” means only those portion(s) of ~~individual copies of~~ software developed by or for Licensee or derived therefrom that implement the Licensed Protocols.

2.3 License Clarifications. Except as provided in **Sections 2.1(b)** and **5.2(b)**, the ~~The~~ licenses granted to Licensee in this Agreement do not include any right to modify or Distribute the WSPP Documentation (or to modify or Distribute WSPP IDL Documentation), except that Licensee may annotate those copies of the WSPP Documentation made available by Microsoft to Licensee under this Agreement, for the purpose of Licensee’s development activities under the license granted in **Section 2.1(a)**. Confidential~~**2.1(a)(i)**.~~ Information (other than Confidential Information~~information~~ included in source code) obtained from~~contained in~~ the WSPP Documentation may not be Distributed in any manner other than as part of an ~~Licensed Server~~ Implementation.

2.4 No Microsoft Statements. This Agreement does not authorize Licensee to make any claim, representation, warranty (whether express, implied or statutory), or other statement on behalf of Microsoft, including any statement that:

(a) Creates or purports to create any support or other obligations on the part of Microsoft, with respect to the ~~Licensed Server~~ Implementation or otherwise;

(b) Allows any recovery of damages by any third party directly from Microsoft under any theory of liability for any matter related to the ~~Licensed Server~~ Implementation; or

(c) States or suggests that Microsoft is responsible for, or had any part in, selecting or providing the ~~Licensed Server~~ Implementation.

2.5 No Other Rights. Except as expressly provided in this Agreement, no other rights are granted under this Agreement by implication or estoppel or otherwise.

2.6 Discussion of Licensing Terms; Notification and Opportunity Regarding Other Licenses. Microsoft acknowledges that this Agreement must be reasonable and non-discriminatory under the terms of the Decision. In the event that Licensee believes any term in this Agreement is unreasonable, Licensee may advise Microsoft of the issue and the reasons why Licensee believes the term or terms are unreasonable. Microsoft agrees to work with Licensee in good faith to appropriately resolve the issue in a reasonable and timely manner, i.e. within 60 days after Microsoft received notice from Licensee. In the event that Microsoft and Licensee are unable to achieve agreement on such terms after good faith efforts, Microsoft is willing to submit the matter for review by the Trustee. If any other WSPP Development Licensee enters into a WSPP Development Agreement for the same or substantively equivalent (in terms of grouping, value, technical complexity, etc.) Licensed Protocols ~~with the same WSPP Documentation under the same Microsoft Licensed Intellectual Property~~ as licensed by Licensee under this Agreement (such WSPP Development Agreement, an **“Other License”**), and the License Fee (as defined below) and/or other terms of that Other License are more advantageous to that other WSPP Development Licensee than the terms of this Agreement, Microsoft will notify Licensee and Licensee will have the opportunity to enter into the same agreement as that Other License. Licensee will also have the opportunity to receive a refund (if applicable) of the License Fee already paid by Licensee under this Agreement, that reflects the same License Fee adjustment as received by the licensee under that Other License.

3. Deliverables; Updates; Support; Comments and Suggestions

3.1 WSPP Documentation – Delivery.

(a) General. Microsoft will provide Licensee with access to WSPP Documentation for the Licensed Protocols via a security-protected online site or other reasonable method determined by Microsoft from time to time as described in this **Section 3.1** and **Section 3.2.**

(b) Licensee's Selection of Protocol Documentation.

(i) Once Licensee has initially fulfilled generally applicable Program Entry Requirements, Microsoft will provide Licensee with access to the WSPP Documentation for the Licensed Protocols initially selected by Licensee and listed on **Exhibit A**. Upon fulfillment of all applicable Program Entry Requirements, the WSPP Protocols chosen by Licensee will become "Licensed Protocols" under this Agreement. Program Entry Requirements applicable to Licensee's initial choices of Licensed Protocols as of the Effective Date are listed on **Exhibit B**, and once Licensee has fulfilled those Program Entry Requirements, Licensee will not be required to re-fulfill them, even if they subsequently change. At Licensee's request, Microsoft will also provide up to three printed, personalized volumes of such WSPP Documentation to Licensee. In light of Licensee's access also to an online version of the WSPP Documentation, updated volumes will be provided annually.

(ii) If applicable, within 10 days of receipt of a written request from Licensee, Microsoft will also provide Licensee with access to WSPP Documentation for any other WSPP Protocols subsequently selected by Licensee. Microsoft will send Licensee an updated **Exhibit A,** and any additional WSPP Protocols listed on that updated exhibit will also become a "Licensed Protocol" under this Agreement.

3.2 WSPP Documentation – Updates.

(a) General. Microsoft will make updated WSPP Documentation for modified and new WSPP Protocols (that are added to WSPP after Microsoft initially provides WSPP Documentation to Licensee under **Section 3.1**) available for license by Licensee under this Agreement:

(i) if applicable, upon release of the First Beta for the relevant Service Pack to the relevant product, or new version of that product, that includes the modified or new WSPP Protocol (documentation provided in such instance, a "**Preliminary Documentation Update**"), or

(ii) if no such First Beta is released, then at least 15 days before the :

(A) commercial release of the Service Pack to the relevant product (i.e., Windows Client Operating System or Windows Server Operating System), or new version of that product, that includes the modified or new WSPP Protocol, or

(B) the day on which the final version of any other Update is released.~~posted to the Microsoft website for the product to which the update applies (e.g., Windows Update site or successor website).~~

"**First Beta**" means the first public beta testing version of the Service Pack or new version of the relevant Windows operating system product made available by Microsoft via an MSDN (Microsoft Developers Network) subscription offering or of which 150,000 or more copies are distributed.

Licensee will be given automatic access to the WSPP Documentation for any Licensed Protocol modifications made available under this **Section 3.2**, for no additional charge beyond the License Fee. ~~**3.2**.~~ Licensee will be given access to the WSPP Documentation for any other WSPP Protocol modifications or any new WSPP Protocols pursuant to the process described in **Section 3.1(b)(ii)**, for no additional charge beyond the License Fee.~~**3.1(b)(ii)**.~~

(b) Preliminary Documentation Updates. When a Preliminary Documentation Update is made available to Licensee, Microsoft will also make the WSPP Documentation for the commercially released~~Commercially Released~~ version of the relevant Service Pack or new product version (such documentation, a "**Final Documentation Update**") available to Licensee within 15 days after the relevant date production is authorized for the manufacture of copies of software for commercial availability. THE ~~CORRECTION ASSISTANCE AND~~ WARRANTY PROVISIONS OF **SECTIONS 3.3(a) AND 6.3** DO NOT APPLY TO PRELIMINARY DOCUMENTATION UPDATES, BUT DO APPLY TO FINAL DOCUMENTATION UPDATES. ~~Once Final Documentation Update(s) are made available, all Licensee~~

~~rights to use relevant Preliminary Documentation Update(s) automatically terminate.~~ SINCE THE FIRST BETA CODE, FEATURES AND/OR FUNCTIONALITY MAY BE SIGNIFICANTLY DIFFERENT FROM THE CODE, FEATURES AND/OR FUNCTIONALITY OF THE COMMERCIALLY RELEASED VERSION, LICENSEE IS ADVISED THAT THERE ARE RISKS IN ANY RELIANCE ON PRELIMINARY DOCUMENTATION UPDATES, AND TO THE EXTENT THAT LICENSEE INCURS ADDITIONAL DEVELOPMENT OR ANY OTHER COSTS AS A RESULT OF SUCH RELIANCE, IT DOES SO AT ITS OWN RISK.

(c) Availability. Once a protocol becomes a WSPP Protocol under the WSPP, Microsoft will continue to make WSPP Documentation for that protocol available during the Term. Subject to the foregoing, nothing in this Agreement requires Microsoft to (i) deliver any WSPP Documentation for any modified or new protocol other than as provided in this **Section 3.2** or (ii) continue to implement any WSPP Protocol in any Windows Client Operating System or Windows Server Operating System. However, Microsoft will provide notice to Licensee in the relevant portion of the WSPP Documentation of WSPP Protocols that remain available for license but which are no longer used by Microsoft in Windows Client and Server Operating Systems, generally in accordance with the timeframe in **Section 3.2(a)(i)**.

3.3 Support.

(a) Correction Assistance. Microsoft (either itself or through a third party) will (i) specifically acknowledge (i.e., beyond an auto-generated email) any Licensee requests for correction assistance regarding any inaccuracies or omissions in the WSPP Documentation within 24 hours of such request, and (ii) correct within a reasonable time any confirmed inaccuracies or omissions that prevent the WSPP Documentation from complying with the warranty in **Section 6.3** (“**Correction Assistance**”) (including any documents, information or protocols that Licensee believes should be included in the WSPP Documentation). Microsoft and Licensee will coordinate on communications to ensure that Licensee has access to Correction Assistance, and that Correction Assistance (and, at License’s option, the technical support under Section 3.3(b)) will provide the primary vehicle to address both issues within the WSPP Documentation and items that Licensee believes should be included in the WSPP Documentation (as well as any Licensee-suggested improvements to the WSPP Documentation), including a mechanism to enable Licensee to report issues and to ensure that Licensee can track issues to resolution.~~.~~ Correction Assistance does not include development or delivery of any software (including any computer program or code, any product related bug fixes, workarounds, patches, beta fixes or beta builds), or any resolution to implementation issues.

(b) Additional Technical Support. Licensee may, at its option, obtain free and unlimited managed technical support regarding Microsoft’s WSPP Documentation and Windows operating systems products, ~~at levels up to and including an on-site Technical Account Manager,~~ by entering into a WSPP Licensed Protocol Support Addendum (a form of which is posted on the WSPP Website). Microsoft technical support personnel will have access to internal Microsoft technical resources such as its product engineering organization, and Windows operating system products source code as needed. Such technical support may include (i) information about WSPP Protocols or WSPP Documentation; (ii) information about Windows operating systems products publicly or programmatically available to Microsoft’s customers or ISVs (independent software vendors), other than source code; and/or (iii) assistance with debugging and verifying actual operation of WSPP Protocols between Windows Server and Windows Client Operating Systems products. Such technical support will not include (A) Licensee access to source code of Windows operating systems or other Microsoft products, other than by entering into a WSPP Source Code License Addendum (a form of which is posted on the WSPP Website); (B) any writing by Microsoft support personnel of source code for ~~Licensed Server~~ Implementations; or (C) any assistance regarding Licensee implementations of any underlying server functionality (as contrasted with the WSPP Protocols). Any information and assistance provided in connection with support described in this **Section 3.3(b)** concerning the behavior, meaning or interdependencies of Microsoft’s products or protocol implementations is provided for reference only and Licensee does not obtain any additional license rights under this Agreement as a result of any disclosure contemplated by this **Section 3.3(b)**.

(c) Third Party IP Rights and Claims.

(i) Rights. Although Microsoft warranty and notice obligations regarding Third Party IP Claims (as defined below) are provided in **Sections 3.3(c)(ii), 6.2,** and ~~**Section**~~ **6.4**, it is also possible that third parties may have intellectual property rights in the WSPP Protocols of which Microsoft is unaware or under which it is not free to sublicense. ~~sublicense, and accordingly,~~ Licensee acknowledges that no such intellectual property~~it may be required to obtain additional license~~ rights are licensed~~from third parties in order to implement the WSPP Protocols~~ under~~ the licenses granted in~~ this Agreement.

(ii) Claims. If the Microsoft Law and Corporate Affairs Department receives in its possession during the Term a Third Party IP Claim in which Microsoft is an IP Defendant, Microsoft will provide Licensee with written notice identifying that Third Party IP Claim. Also, if Licensee receives in its possession during the Term a Third Party IP Claim in which Licensee is an IP Defendant, Licensee may provide Microsoft with written notice identifying that Third Party IP Claim. "**Third Party IP Claim(s)**" means, with respect to the entity (either Microsoft or Licensee) who is named as a defendant or against whom a claim is made (the "**IP Defendant**") (i) litigation in which the IP Defendant is named as a defendant and served with process or (ii) a written threat of litigation against the IP Defendant that a third party or its authorized agent sends to the IP Defendant, and the IP Defendant and the IP Defendant's internal legal department (to the extent the IP Defendant has one) receives in its possession, which alleges that a WSPP Protocol (or its implementation in a Windows Client Operating System or a Windows Server Operating System) or the WSPP Documentation infringes that third party's own intellectual property rights for which Licensee is licensed under Section 2.1(a), with specificity and in sufficient detail for the IP Defendant to identify (A) the allegedly infringing WSPP Protocol (or its implementation in a Windows Client Operating System or a Windows Server Operating System) or WSPP Documentation, (B) the allegedly infringed intellectual property and (C) the legal and technical basis of the allegation.

(d) Other. Except for the Microsoft obligations expressly described in **Sections 3.3(a), (b) and (c)**, as between Microsoft and Licensee, Licensee is solely responsible for all support issues relating to ~~Licensed Server~~ Implementations.

3.4 Comments and Suggestions. Microsoft invites Licensee's comments and suggestions on the WSPP Documentation and other items or information provided by Microsoft under this Agreement ("**Comments and Suggestions**"). If Licensee voluntarily provides (in connection with correction assistance or otherwise) any Comments and Suggestions relating to the WSPP Documentation or matters contained therein, Microsoft may, in connection with Microsoft products and services, use, disclose or otherwise commercialize in any manner, any of those Comments and Suggestions without obligation or restriction based on intellectual property rights or otherwise except that the foregoing does not permit the Comments or Suggestions to be licensed by Microsoft on a standalone basis.

4. License Fee and Payments.

4.1 License Fee. Licensee will pay Microsoft a one-time license fee of 10,000 Euros ("**License Fee**").

4.2 Payments.

(a) Payment Terms and Instructions. Licensee will pay an invoice issued by Microsoft (or its Payment Agent) for the Licensee Fee within 30 days of receipt of the invoice. Payment will be made to the Payment Agent (i.e. payments will be made out to the Payment Agent), to the following account or address (or alternate Payment Agent, account or address upon reasonable notice from Microsoft):

Payment Agent: Microsoft Corporation

For all Wire Transfers:
Bank of America
1401 Elm Street
Dallas, Texas 75202 USA

Account # 3750891058
ABA # 0260-0959-3
SWIFT# BOFAUS3N
Attn: Microsoft Corporation

For Approved checks sent via courier (FedEx, UPS, Airborne, etc.):
Bank of America
Attn: Microsoft Corporation #100430

6000 Feldwood Road
College Park, GA 30349-3652

For Approved checks sent via National Mail:
Microsoft Corporation
P. O. BOX 100430
Atlanta, GA 30384-0430
*(Please remit **one week prior** to invoice due date if paying by check. Licensee is responsible for mailing & courier fees.)*

(b) Manner of Payment. The License Fee is payable in Euros. All references in this Agreement to "€" refer to Euros. The License Fee is non-refundable except as provided in **Section 9.2(c)**.

(c) Taxes. This **Section 4.2(c)** governs the treatment of all taxes arising as a result of or in connection with this Agreement, notwithstanding any other provision of this Agreement.

(i) Licensee is responsible for the billing, collecting and remitting of sales, use, value added, and other comparable taxes due with respect to the collection of any revenues by Licensee, or any portion thereof. Microsoft is not liable for any taxes (including any penalties or interest thereon), that Licensee is legally obligated to pay and that are incurred by Licensee in connection with this Agreement or any Licensee revenues or related to the licensing or other Distribution of any ~~Licensed Server~~ Implementation, and Licensee takes full responsibility for all such taxes. Licensee is not liable for any income taxes that Microsoft is legally obligated to pay with respect to any amounts paid to Microsoft by Licensee under this Agreement.

(ii) The License Fee excludes any taxes, duties, levies, fees, excises or tariffs imposed on any of Licensee's activities in connection with this Agreement. Licensee will pay to Microsoft (pursuant to **Section 4.2(a)**) any applicable taxes that are owed by Licensee solely as a result of entering into this Agreement and which are permitted to be collected from Licensee by Microsoft under applicable law, except to the extent Licensee provides to Microsoft a valid exemption certificate for such taxes. Licensee agrees to indemnify, defend and hold Microsoft harmless from any ~~taxes (including without limitation~~ sales, ~~or~~ use or similar taxes payable~~paid~~ by Licensee ~~to Microsoft)~~ or claims, causes of action, costs (including without limitation reasonable attorneys' fees) and any other liabilities of any nature whatsoever related to such taxes.

(iii) If, after a determination by a tax authority outside the U.S., any taxes are required to be withheld on payments made by Licensee to Microsoft, Licensee may deduct such taxes from the amount owed Microsoft and pay them to the appropriate taxing authority; provided however, that Licensee will promptly secure and deliver to Microsoft (through its Payment Agent) an official receipt for any such taxes withheld or other documents necessary to enable Microsoft to claim a U.S. Foreign Tax Credit. Licensee will make certain that any taxes withheld are minimized to the extent possible under applicable law.

5. Confidentiality

5.1 Definition of Confidential Information. Microsoft asserts that it has invested significant effort and expense in developing the WSPP Protocols and WSPP Documentation (although Microsoft acknowledges that by signing this Agreement, Licensee is not (i) necessarily agreeing with the foregoing assertion or (ii) waiving its right to contest it). The WSPP Documentation, and all non-public information disclosed to Licensee in connection with Correction Assistance per **Section 3.3(a)**, are Microsoft's **"Confidential Information."** The terms of this Agreement are not Confidential Information of either party, except for the specific Licensed Protocols selected by Licensee, which are Confidential Information of Licensee. Each party disclosing its Confidential Information to the other party under this Agreement is the "**Disclosing Party**", and the party receiving such Confidential Information is the "**Receiving Party**."

5.2 Use and Disclosure of Confidential Information.

(a) General. Each Receiving Party will: (a) subject to **Sections 5.5 and 5.6,~~5.4,~~** retain ~~in confidence the~~ Confidential Information provided by~~of~~ the Disclosing Party in confidence;~~;~~ (b) make no use of that~~the~~ Confidential Information ~~of the Disclosing Party~~ except as permitted under this Agreement;

and (c) protect that Confidential Information~~ of the Disclosing Party~~ by using reasonable measures sufficient to maintain the confidentiality of such Confidential Information.

(b) Permitted Recipients. Except as otherwise expressly authorized in **Sections 5.5 or 5.6**, the Receiving Party may disclose Confidential Information of the Disclosing Party~~ to its employees, temporary personnel or independent contractors or other persons authorized by Licensee~~ only on a "need to know basis" and under a suitable written non-disclosure agreement that does not permit disclosure or use except as permitted under this Agreement. Without limiting the foregoing, Licensee may make the WSPP Documentation available to other WSPP Development Licensees in connection with communications described in Section 5.6(b). ~~,~~

5.3 [Reserved]

~~5.3 Specific Procedures. Without limiting the generality of its obligations as a Receiving Party under **Section 5.2**: (a) Licensee will preserve, abide by and not circumvent or attempt to circumvent any technological mechanism (such as digital rights management technology or password protection) designed to restrict access to or limit copying of the WSPP Documentation and that is included in or applied to the WSPP Documentation made available by Microsoft, and (b) Licensee will not place or save the electronic file containing the WSPP Documentation on any computer system that is accessible via the Internet, except via a secure encrypted "virtual private network" connection to Licensee's internal network system that is limited to authenticated use by persons otherwise authorized to have access to Confidential Information under **Section 5.2**.~~

5.4 Exclusions. Neither party's Confidential Information includes information which: (a) is in or subsequently enters the public domain or is or subsequently becomes known to the Receiving Party from a source other than the Disclosing Party, without imposition of a confidentiality obligation on the Receiving Party, and provided that entry into the public domain or disclosure does not result from any violation of laws or breach by the Receiving Party of an obligation of confidentiality owed ~~directly or indirectly~~ with respect to the information;~~ or~~ (b) was independently developed by the Receiving Party without reference to any Confidential Information of the Disclosing Party in any form; or (c) becomes publicly known or enters into the public domain through an independent analysis of the source code as given in Section 5.6(a).~~form.~~

5.5 Independent Development/Residuals. The terms of confidentiality under this Agreement shall not be construed to limit either the Disclosing Party or the Receiving Party's right to independently develop or acquire products without use of the other party's Confidential Information. Further, the Receiving Party shall be free to use for any purpose the residuals resulting from access to or work with the Confidential Information of the Disclosing Party, provided that, during the period such individual is accessing the WSPP Documentation and for a period of three months following the individual's last access to the WSPP Documentation, the individual~~Receiving Party~~ shall not disclose such residuals~~Confidential Information~~ except as otherwise expressly permitted pursuant to the terms of this Agreement. The term "residuals" means information in intangible form, which is retained in unaided memory by persons authorized by the Receiving Party who have had access to the Disclosing Party's Confidential Information per the provisions of **Section 5.2** (such persons, "**Authorized Persons**"), including ideas, concepts, know-how or techniques contained in such Confidential Information. An Authorized Person's memory will be considered to be unaided if such Authorized Person has not intentionally memorized the Confidential Information for the purpose of retaining and subsequently using or disclosing it. The Receiving Party shall not have any obligation to limit or restrict the assignment of Authorized Persons or to pay royalties for any work resulting from the use of residuals. However, this **Section 5.5** shall not be deemed to grant to the Receiving Party a license under the Disclosing Party's copyrights or patents.

5.6 Permitted Disclosures.

(a) To the extent that Microsoft Confidential Information is embodied in and disclosed by source code (including comments to source code in line with standard industry practice) versions of ~~Licensed Server~~ Implementations, Licensee may disclose such Confidential Information as part of a distribution of such source code. For further clarification of standard industry practice, the parties intend that the standard will be the commenting and/or commit messages reasonably required from the perspective of good software engineering practices. Without limiting the sources of such standards, the kinds of practice that would typically be sources for those standards would include those described in Writing Clean Code (Steve Maguire) and Code Complete (Steve McConnell), as well as those used generally in the published source code from Samba.org as of the date of this Agreement.

(b) Microsoft will also establish a mechanism (for example a secure mailing list) that enables Licensee to communicate with other WSPP licensees and Microsoft about the WSPP Documentation, and such communications may include discussion of the content of the WSPP Documentation among WSPP licensees. In connection with development of Implementations and with Microsoft Plugfests and similar events held for WSPP Documentation, Licensee may also communicate with other WSPP licensees about the WSPP Documentation.

(c) Sections 5.6(a) and 5.6(b) do ~~The foregoing does~~ not authorize Licensee to publish the WSPP Documentation in any manner (including in connection with or as part of ~~Licensed Server~~ Implementation source code) or to disclose Microsoft Confidential Information in any other manner than publication of ~~Licensed Server~~ Implementation source code or works derived from it.

(d)~~(b)~~ The Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order, provided the Receiving Party (i) gives the Disclosing Party reasonable notice prior to such disclosure to allow the Disclosing Party a reasonable opportunity to seek a protective order or equivalent, or (ii) obtains written assurance from the applicable judicial or governmental entity affording the Confidential Information the highest level of protection afforded under applicable law or regulation, provided that (except with respect to governmental orders) in no event may such level of protection be less than is reasonably necessary to maintain the confidentiality of such Confidential Information.

(e)~~(c)~~ Subject to **Section 5.6(d)~~.5.6(b)~~,** the Receiving Party may also disclose Confidential Information in connection with the Microsoft Work Group Server Protocol Program or Microsoft's compliance with the Decision, to the Commission, to the Trustee, or, in connection with judicial enforcement of this agreement, to the High Court of Chancery as set forth in Section 10.7.~~ or to the Trustee.~~

(f)~~(d)~~ Confidential Information disclosed under ~~this~~ **Section 5.6(b), (c) and (e)** remains Confidential Information under this Agreement.

5.7 Publicity. Nothing in this Agreement prohibits Licensee from disclosing the fact that it has entered into this Agreement and that it has implemented WSPP Protocol(s) in ~~Licensed Server~~ Implementation(s), as long as Licensee does not use any Microsoft logo in so doing. However, Microsoft will not, without Licensee's approval, issue any press releases or similar communications during the Term regarding the fact that Licensee has entered into this Agreement, unless such fact has already been made public by someone other than Microsoft.

5.8 Acknowledgement about Implementation Details. The parties acknowledge that constraints in the protocols specified in the WSPP Documentation may require a level of similarity in some source code elements of Implementations, in comparison to the content of the WSPP Documentation, and that Licensee may choose to use the same names for protocol elements in the Implementations as Microsoft uses in the WSPP Documentation. These similarities should not be interpreted in and of themselves as evidence of a breach of the confidentiality provisions in this Section 5, nor will Microsoft assert any claim of copyright infringement on the basis of such similarities.

6. Warranties, Limitations of Liability, Exclusive Remedies and Sole Liability.

6.1 General.

~~(a)~~ Each party warrants that (i) the person executing this Agreement on behalf of such party has all necessary power and authority to do so, and that upon such signature this Agreement is a legal, valid and binding obligation enforceable against such party, and (ii) that it is entering into this Agreement in good faith.

~~(b) Licensee further warrants that, as of the Effective Date and throughout the Term: Licensee has not: (i) created or Distributed a computer virus with malicious intent; or (ii) engaged in repeated willful violations, or knowing and material contribution or inducement to repeated willful violations by third~~

~~parties, of intellectual property rights or of laws or regulations prohibiting circumvention of technology measures that control access to, or the ability to copy, software or other copyrighted digital content.~~

6.2 Additional Microsoft Warranties.

(a) ~~Copyright Infringement.~~ Microsoft further warrants that the WSPP Protocols and the WSPP Documentation do not infringe any copyright of any third party.

(b) Microsoft further warrants that it will not assert any patent claims other than Subject Patent Claims against Licensee or any third party for developing, making, using or Distributing any Implementation. Microsoft further acknowledges that the inclusion of the Subject Patent Claims in this Agreement does not imply that Licensee's Implementation(s) infringe the Subject Patent Claims, and Microsoft acknowledges that Licensee is not waiving its right to contest the validity or applicability of any of Microsoft's patents. Any assignment or other transfer by Microsoft or its related companies of Microsoft's patent claims subject to this paragraph 6.2(b) will be subject to Microsoft's obligations under this Agreement.

6.3 Documentation and Licensing Terms. Microsoft further represents and warrants and undertakes that

(a) the WSPP Documentation is complete and accurate as required by Article 5 of the Decision read in conjunction with Article 1 of the Decision;

(b) the WSPP Documentation conforms to the Protocol Technical Documentation Specifications listed in Appendix 2;

(c) the WSPP Documentation is and will be kept updated on an ongoing basis and in a timely manner as required by Article 5 of the Decision read in conjunction with Article 1 of the Decision;

(d) the WSPP Documentation provided by Microsoft under this Agreement will be provided in an organized manner and in a format suitable for analysis and interpretation by software engineers reasonably skilled in the art of server software protocols and familiar with (although not necessarily specialized in) Windows Server Operating Systems developer technologies;

(e) in offering the terms and conditions under this Agreement to Licensee (including, without limitation, the financial provisions, warranties and any restrictions imposed on Licensee hereunder in relation to its right to access and use the WSPP Documentation), Microsoft complies and shall continue to comply with the requirement under Article 5 of the Decision that it must allow undertakings to use the Interoperability Information (as defined in Article 1 of the Decision) on terms which are reasonable and non-discriminatory. If at any time Microsoft grants any Third Party license fees, terms and conditions that may be deemed to be more advantageous, Microsoft will give prompt notice to Licensee and provide the necessary information to determine compliance with this representation and warranty.

6.4 Third Party Claims. Microsoft further warrants that as of the Effective Date, to the best of its knowledge, it does not have any Third Party IP Claims (defined in **Section 3.3(c)(ii)**) other than as may be set forth in **Appendix 3** to this Agreement.

6.5 **LIMITATIONS OF LIABILITY**. EXCEPT AS PROVIDED IN **SECTIONS 6.1-6.4** AND WITH REGARD TO THE IMPLIED WARRANTY OF TITLE AS TO ANY GOODS PROVIDED TO LICENSEE, TO THE MAXIMUM EXTENT PERMITTED BY LAW, EACH PARTY EXCLUDES ALL CONDITIONS, WARRANTIES AND OTHER TERMS WHICH MIGHT HAVE EFFECT BETWEEN THE PARTIES OR BE IMPLIED OR INCORPORATED INTO THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, IN RELATION TO (i) THE WSPP DOCUMENTATION, (ii) PRELIMINARY DOCUMENTATION UPDATES, (iii) CORRECTION ASSISTANCE, (iv) COMMENTS AND SUGGESTIONS, AND (v) ALL INTELLECTUAL PROPERTY IN ANY OF THE FOREGOING (INCLUDING, WITHOUT LIMITATION, THE MICROSOFT LICENSED INTELLECTUAL PROPERTY) (COLLECTIVELY, THE "**MATERIALS**"), WHETHER BY STATUTE, COMMON LAW OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, THE IMPLIED CONDITIONS, WARRANTIES AND OTHER TERMS AS TO SATISFACTORY QUALITY, FITNESS FOR PURPOSE AND THE USE OF REASONABLE SKILL AND CARE. EXCEPT AS PROVIDED IN **SECTION 6.2(A) OR 6.4** AND WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, MICROSOFT MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND THAT (i) THE

MATERIALS DO NOT INFRINGE THE INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY OR (ii) ANY ~~LICENSED SERVER~~ IMPLEMENTATION WILL NOT INFRINGE ANY INTELLECTUAL PROPERTY RIGHT OF ANY THIRD PARTY.

6.6 **EXCLUSIVE REMEDIES AND SOLE LIABILITY.** BOTH PARTIES AGREE THAT LICENSEE'S SOLE AND EXCLUSIVE REMEDY AND MICROSOFT'S SOLE LIABILITY IN CONNECTION WITH ANY CLAIM RELATED TO:

(a) A VIOLATION OR BREACH OF THE WARRANTY IN **SECTION 6.2(A)** IS A CLAIM FOR INDEMNIFICATION FROM THIRD PARTY CLAIMS UNDER **SECTION 7.1(a)** (SUBJECT TO THE TERMS AND LIMITATIONS SET FORTH IN **SECTION 7**), AND THAT LICENSEE IS NOT ENTITLED TO BRING ANY CLAIM FOR DAMAGES AGAINST MICROSOFT BASED ON ANY ALLEGED OR ACTUAL VIOLATION OR BREACH OF THE WARRANTY IN **SECTION 6.2(A);~~6.2;~~**

(b) **SECTION 6.4** (INCLUDING WITHOUT LIMITATION ANY BREACH THEREOF) IS FOR LICENSEE TO TERMINATE THIS AGREEMENT WITH RESPECT TO ALL WSPP PROTOCOLS THAT ARE THE SUBJECT OF THE RELEVANT THIRD PARTY IP CLAIM AND, FOLLOWING SUCH TERMINATION, TO PURSUE A CLAIM FOR DAMAGES AGAINST MICROSOFT BASED ON A VIOLATION OR BREACH OF THE WARRANTY IN **SECTION 6.4**, PROVIDED THAT SUCH DAMAGES WILL NOT IN ANY EVENT EXCEED (REGARDLESS OF THE LEGAL THEORY UPON WHICH ANY CLAIM FOR SUCH DAMAGES IS BASED) THE AMOUNT OF THE LICENSE FEE PAID BY LICENSEE TO MICROSOFT HEREUNDER, AND TO THE EXTENT APPLICABLE, TO OBTAIN INDEMNIFICATION AND DEFENSE BY MICROSOFT WITH RESPECT TO THIRD PARTY IP CLAIMS UNDER **SECTION 7.1(b)** SUBJECT TO THE TERMS AND LIMITATIONS SET FORTH IN **SECTION 7**; AND

NOTHING IN THIS **SECTION 6.6** IS INTENDED TO LIMIT THE REMEDIES AVAILABLE TO MICROSOFT WITH RESPECT TO MISREPRESENTATIONS BY LICENSEE OR OTHER BREACHES OF **SECTION 6.1**. NOTHING IN THIS AGREEMENT SHALL EXCLUDE MICROSOFT'S LIABILITY FOR DEATH OR PERSONAL INJURY ARISING FROM NEGLIGENCE.

7. Indemnification.

7.1 General. Subject to **Sections 7.2** and **7.3**, Microsoft agrees at its expense and Licensee's request to indemnify and hold harmless Licensee and Licensee's subsidiaries, directors, officers, and employees ("**Indemnified Parties**"), from and against amounts awarded by (or in an award enforceable by) a court of competent jurisdiction or agreed to in a settlement pursuant to **Section 7.3** below ("**Indemnified Damages**") as a result of:

(a) third party claims, demands or actions based on allegations which, if true, would constitute a breach of Microsoft's warranty in **Section** 6.2(a),~~6.2,~~ and/or

(b) third party claims, demands or actions based on allegations which, if true, would constitute a breach of Microsoft's warranty in **Section 6.4** ("**7.1(b) Covered Claims**"; along with the claims referenced in **Section 7.1(a)**, "**Covered Claims**").

7.2 7.1(b) Claims. Subject to **Section 7.3**, Microsoft also agrees at its expense to defend the Indemnified Parties against 7.1(b) Covered Claims, and the costs of such defense are not capped; provided, however, that such defense obligation, and Microsoft's obligation to indemnify and hold the Indemnified Parties harmless under **Section 7.1(b)**, excludes Licensee's reverse engineered products or products created by Licensee prior to the Effective Date.

7.3 Condition and Procedures. Microsoft's obligation to indemnify, hold harmless and defend the Indemnified Parties under **Section 7.1 and 7.2** is conditioned on Licensee's providing Microsoft with reasonably prompt notice in writing of any Covered Claim, and tendering control of the defense of such Covered Claim to Microsoft. Microsoft will not settle any Covered Claim except with prior written permission of Licensee, which permission Licensee will not unreasonably withhold. Notwithstanding Licensee's tender of control of defense to Microsoft under this **Section 7.3**, Licensee may also participate at its own expense in such defense, provided that control over defense strategy decisions remains with Microsoft subject only to the express provisions of this **Section 7.3** regarding settlement approvals.

7.4 Additional Claims. Microsoft agrees at its expense and Licensee's request to defend Licensee in a lawsuit, and pay the amount of any adverse final judgment (or settlement to which Microsoft agrees in advance in writing) from such lawsuit, for any third party claim(s) that a Licensed Protocol implemented and Distributed in an~~ Licensed Server~~ Implementation in accordance with **Section 2** and the other provisions of this Agreement, infringes third party patent Necessary Claims that were not known to Microsoft as of the Effective Date (such third party claims, "**Additional Claim(s)**"); provided that:

(a) Licensee promptly notifies Microsoft in writing of the Additional Claim, in sufficient detail to identify (i) the allegedly infringing Licensed Protocol, (ii) the allegedly infringed patent Necessary Claims and (iii) the legal and technical basis of the allegation,

(b) Microsoft controls the defense and/or settlement of the Additional Claim,

(c) Licensee provides Microsoft with reasonable assistance (at Microsoft's expense) in the defense of the Additional Claim,

(d) Microsoft's obligations to defend and pay any Additional Claim shall be limited to Additional Claims wherein the Licensed Protocol alone, without combination or modification, constitutes direct or contributory infringement of such Additional Claim, and

(e) if the lawsuit identified above includes any claim, other than Additional Claim(s), that the ~~Licensed Server~~ Implementation containing the allegedly infringing Licensed Protocol(s) infringes any third party intellectual property rights ("**Other Claims**"), Licensee reimburses Microsoft for any and all attorney's fees and costs incurred by Microsoft in defending against Other Claims, provided that Licensee controls the defense and/or settlement of those Other Claims.

Notwithstanding each party's control of defense of Additional Claims and Other Claims under this **Section 7.4**, the other party may also participate at its own expense in such defense, provided that control over defense strategy decisions with respect to (i) Additional Claims remains with Microsoft and (ii) Other Claims remains with Licensee. Microsoft will have no obligations under this **Section 7.4** for any Additional Claim based on (A) Licensee's manufacture, use or Distribution of software containing an allegedly infringing Licensed Protocol more than 20 days after Microsoft has provided Licensee with at least 20 days written notice that (1) Microsoft (at its option) will stop such activity or (2) Microsoft (at its option) will modify the allegedly infringing Licensed Protocol and provide that modified Licensed Protocol to Licensee for license under this Agreement in lieu of the allegedly infringing Licensed Protocol at or prior to the end of such notice period, or (B) on Licensee's reverse engineered products or products created by Licensee prior to the Effective Date. Microsoft's liability under this **Section 7.4** will not exceed, in the aggregate, the License Fee; however, this limitation does not apply to any fees and expenses of attorneys incurred by Microsoft in defending Additional Claim(s).

8. LIMITATIONS OF REMEDIES & LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY IS LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL LOSSES OR SPECIAL DAMAGES WHATSOEVER, OR FOR LOSS OF PROFITS, ANTICIPATED SAVINGS, BUSINESS OPPORTUNITY OR GOODWILL OR LOSS OF DATA, ARISING OUT OF OR IN ANY WAY CONNECTED TO THE USE OF OR INABILITY TO USE THE WSPP DOCUMENTATION OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, WHETHER ARISING OUT OF NEGLIGENCE OR OTHERWISE. THE FOREGOING EXCLUSION APPLIES EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE AND EVEN IF ANY AVAILABLE REMEDY FAILS OF ITS ESSENTIAL PURPOSE, BUT DOES NOT APPLY TO (I) BREACH OF **SECTION 5** (CONFIDENTIALITY)~~, **SECTION 6.1(B)** (CERTAIN LICENSEE WARRANTIES),~~ OR **SECTION 6.3** (DOCUMENTATION AND LICENSING TERMS) ((II) INDEMNIFIED DAMAGES, OR (III) ANY INFRINGEMENT OR MISAPPROPRIATION OF EITHER PARTY'S INTELLECTUAL PROPERTY RIGHTS. NOTHING IN THIS AGREEMENT EXCLUDES MICROSOFT'S LIABILITY FOR DEATH OR PERSONAL INJURY ARISING FROM NEGLIGENCE.

9. Term & Termination.

9.1 Term.

(a) Initial Term. The initial term of this Agreement commences on the Effective Date and remains in effect until the date that is five years from the Effective Date, unless and until this Agreement is earlier terminated in accordance with **Section 9.2** ("**Initial Term**").

(b) Term Extensions. Unless the Agreement has been terminated prior to expiration, Licensee may extend the term of this Agreement for successive terms of five years ("**Extensions**") by giving written notice to Microsoft during the period beginning 60 days prior and ending on the expiration date of the Initial Term or then-current Extension. The Initial Term, together with any Extensions, constitutes the "**Term**" of this Agreement. To account for the availability of new technology or other developments, Microsoft reserves the right to make any Extension subject to Licensee's agreement to new or revised terms, including the License Fee amount set forth in Section 4.1,~~royalty terms,~~ provided any such terms are consistent with the Decision and the WSPP Pricing Principles set forth in **Appendix 1**. Microsoft may terminate Licensee's right to obtain Extensions by giving written notice to Licensee if Microsoft receives permission from the Commission of the European Communities to do so. Following delivery of such notice, the Agreement will expire on the date that is the later of (i) the last day of the Initial Term or then-current Extension (if applicable); or (ii) three years following the date of such notice.

9.2 Termination.

(a) By Licensee Without Cause. Licensee may terminate this Agreement at any time, in its sole discretion and without cause, by providing written notice to Microsoft and complying with **Section 9.3(a)**.

(b) By Microsoft for Cause. Microsoft may terminate this Agreement: (i) immediately upon written notice at any time, if Licensee is in material breach of **Section 5** of this Agreement; (ii) upon written notice at any time if Licensee is in material breach of any warranty, term or condition of this Agreement and fails to remedy that breach (if such breach is capable of being remedied) within 60 days after written notice thereof; or (iii) upon written notice at any time if Licensee has received three or more written termination notices under the preceding clause (ii) within the previous 12-month period based on an actual material breach of a material warranty, term, or condition of this Agreement, even if those previous material breaches have been cured. Any material breach has to first be established by a court of competent jurisdiction.

(c) Termination for Non-Satisfaction of Program Entry Requirements. If Licensee has not satisfied all applicable Program Entry Requirements within 90 days after the Effective Date, Microsoft has the right to immediately terminate this Agreement upon written notice to Licensee, and in the event of such termination, Microsoft will promptly refund to Licensee any of the License Fee that Licensee has paid before such termination. Licensee's failure to satisfy any Program Entry Requirements is not, in and of itself, a material breach of this Agreement.

(d) Termination as to Licensee Subsidiaries; Survival. Notwithstanding any other provision of this Agreement: (i) this Agreement will terminate immediately (without notice or opportunity to cure) with respect to any party identified as a Licensee subsidiary on the first page of this Agreement, at such time as such subsidiary ceases to be a wholly-owned subsidiary of the party identified as the Licensee parent on the first page of this Agreement, and (ii) upon such termination, such subsidiary will no longer be entitled to exercise any rights under this Agreement, but all obligations and liabilities of such subsidiary accruing before the termination date will survive such termination; provided that any subsidiary so terminated may (after meeting applicable then-current Program Entry Requirements) enter into a new agreement on its own behalf either: (i) on the then-current terms of the WSPP Development Agreement, or (ii) for a period of 30 days after such termination, on the same terms as this Agreement (rather than the then-current terms of the WSPP Development Agreement) and for a term concurrent with this Agreement.

9.3 Effect of Expiration or Termination; Survival.

(a) Termination - General. Upon any expiration or termination of this Agreement: (i) unless Licensee elects to exercise its ~~or (if applicable) Licensee's~~ rights under Sections 9.3(b) or ~~**(c)**: (i) except as provided in Section~~ 9.3(c) below, and with the exception of what is otherwise specifically permitted under this Agreement, including, without limitation, under **Sections 5.4** (Exclusions), **5.5** (Independent Development/Residuals), and **5.6** (Permitted Disclosures), Licensee ~~Licensee~~ will ~~immediately (A)~~ cease all use of and direct reference to ~~and use of~~ the WSPP Documentation and will return ~~activities (including but not limited to~~ all hard~~production and all Distribution of Licensed Server Implementations) with respect to the WSPP Protocols and/or Microsoft Licensed Intellectual Property and (B) if Licensee has received any~~ copies of the WSPP Documentation in its~~from Microsoft, return to Microsoft all such WSPP Documentation copies (including any portion thereof) in Licensee's~~ possession to Microsoft;~~or under its control and if requested by Microsoft, provide a declaration signed by a Licensee officer attesting that all such copies have been returned to Microsoft,~~ and (ii) the following will survive such termination: **Sections 3.2(b)** (Preliminary Documentation Updates), solely as to the warranty and liability exclusions therein; **3.4** (Comments and Suggestions); **4.2(c)** (Taxes); **5** (Confidentiality);~~ (License Fee and Payment), **5** (Confidentiality),~~ **6-8** (Warranties, Limitations of Liability, Exclusive Remedies and Sole Liability; Indemnification; Limitations of Remedies & Liability);~~Liability),~~ and **10** (Miscellaneous);~~(Miscellaneous),~~ as well as **Sections 9.1-9.2, 9.4** and this **Section 9.3.~~9.3(a).~~**

(b) Expiration of Agreement (Without Earlier Termination). If this Agreement has not been earlier terminated, then upon expiration of the full Term of this Agreement and unless Licensee elects to return and cease reference to the WSPP Documentation as described in Section 9.3(a) above:~~:~~ (i) subject to the express license scope and other terms and conditions referenced in **Sections 2 and 5**, the rights granted Licensee under **Section 2.1(a)** will survive, and Licensee may retain in its possession and continue to use the WSPP Documentation made available to it by Microsoft during the Term solely to exercise such rights; and (ii) the following will also survive such expiration: **Sections 3.2(b)** (Preliminary Documentation Updates), solely as to the warranty and liability exclusions therein; **3.4** (Comments and Suggestions); **4.2(c)** (Taxes); **5** (Confidentiality), including without limitation 5.5 (Independent Development/Residuals);~~ (License Fee and Payment); **5** (Confidentiality);~~ **6-8** (Warranties, Limitations of Liability, Exclusive Remedies and Sole Liability; Indemnification; Limitations of Remedies & Liability); and **10** (Miscellaneous); and this **Section 9** (Termination).

(c) Support for Licensee Products Following Termination. Subject to the express license scope and other terms and conditions referenced in **Sections 2 and 5** and unless Licensee elects to return and cease reference to the WSPP Documentation as described in Section 9.3(a) above,~~,~~ upon any termination of this Agreement other than under Section 9.2(a), Licensee may retain in its possession and continue to use the WSPP Documentation made available to it by Microsoft during the Term solely for purposes of providing technical support and maintenance services for versions of ~~Licensed Server~~ Implementations commercially released or released for production use~~Commercially Released~~ prior to such termination ("**Existing WSPP Implementations**"), including Distribution of bug fixes and patches for such Existing WSPP Implementations. The following provisions of this Agreement will also survive as applicable to such technical support and maintenance activities: **Sections 3.2(b)** (Preliminary Documentation Updates), solely as to the warranty and liability exclusions therein; **3.4** (Comments and Suggestions); **4(c)** (Taxes);~~ (License Fee and Payment);~~ **5** (Confidentiality); **6-8** (Warranties, Limitations of Liability, Exclusive Remedies and Sole Liability; Indemnification; Limitations of Remedies & Liability); and **10** (Miscellaneous); and this **Section 9** (Termination).

(d) Ongoing Rights Following Expiration or Termination. ~~(d)~~ Expiration or Termination of this Agreement do not affect the rights of recipients of source code versions of Existing WSPP~~Licensed Server~~ Implementations to copy, distribute and modify source code versions of Existing WSPP~~Licensed Server~~ Implementations. Such expiration or termination also does not affect the rights of Licensee to copy, distribute and modify source code versions of Existing WSPP Implementations, without reference to the WSPP Documentation, and subject to **Section 5** (Confidentiality), including without limitation **Section 5.5** (Independent Development/Residuals).

9.4 Remedies Not Exclusive. The rights and remedies set forth in this **Section 9** are cumulative and are not exclusive of any rights or remedies available at law or in equity, subject only to the express waivers and limitations of liability set forth in this Agreement.

10. Miscellaneous.

10.1 No Partnership, Joint Venture or Franchise. Neither this Agreement, nor any terms or conditions contained herein, create a partnership, joint venture or agency relationship or grant a franchise as defined in the Washington Franchise Investment Protection Act, RCW 10.100, as amended, 16 CFR Section 436.2(a), or any other similar laws in other jurisdictions.

10.2 Export Laws and Regulations. Products and technical information of Microsoft are subject to U.S. export jurisdiction and other applicable national or international laws and regulations, and the licenses and deliveries of technical information and data contemplated herein may be prohibited by such laws and regulations. Licensee agrees to comply with all such export control~~applicable international and national~~ laws. For additional information, see http://www.microsoft.com/exporting/.

10.3 Actions on Behalf of the Parties. Microsoft and Licensee are each liable for, and will be deemed for all purposes of this Agreement to have done or failed to do, any act or omission of their respective officers, employees, temporary personnel, or independent contractors related to acts or omissions in connection with this Agreement.

10.4 Notices. All notices and requests in connection with this Agreement are deemed given on the day they are received either by messenger, delivery service, or in the United States of America mails, postage prepaid, certified or registered, return receipt requested, and addressed to Licensee using the contact information indicated on the first page of this Agreement, to Microsoft using the contact information below, or to either party at such other address as the party to receive the notice or request so designates per this notice provision:

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399 U.S.A.
Attention: General Manager, Competition Law Compliance Team
Phone: (425) 882-8080
Fax: (425) 706-7329
Copy to: Law & Corporate Affairs
Fax: (425) 706-7409

10.5 Licensee Contests and Complaints.

(a) Microsoft acknowledges that by signing this Agreement, Licensee is not waiving its right to contest the validity of any of Microsoft's patents, know-how, industrial secrets, trade secrets and confidential information embodied in the WSPP Protocols and disclosed by the WSPP Documentation, or copyrights, and without prejudice to the provisions of **Section 9.2**, Microsoft will not withhold WSPP Documentation from Licensee or terminate this Agreement on the basis of such a contest by Licensee.

(b) Nothing in this Agreement will prevent Licensee from complaining to the Commission of the European Communities with respect to~~that terms and conditions of~~ this Agreement or~~do not comply with~~ the Decision. Without prejudice to the provisions of **Section 9.2**, Microsoft will not withhold WSPP Documentation from Licensee or terminate this Agreement on the basis of such a complaint by Licensee.

(c) This Agreement neither takes away from nor adds (except as expressly stated in this Agreement) to any rights a licensee might have under Articles 81 or 82 EC or equivalent provisions of national competition laws.

10.6 Injunctive and Equitable Relief, Liquidated Damages.

(a) Microsoft acknowledges and agrees that (i) monetary damages will not be a sufficient remedy for Microsoft's breach of its obligations under **Section 5**, and (ii) such unauthorized disclosure, use or exercise of rights will cause Licensee immediate, severe and irreparable injury. Accordingly, notwithstanding the provisions of **Section 10.7**, Microsoft acknowledges that Licensee will be entitled in such circumstances, without waiving or prejudicing any other rights or remedies, to such injunctive or equitable relief as a court of competent jurisdiction may grant.

(b) The Parties acknowledge and agree that in case of Microsoft's breach of Article 5 of the Decision or the representations, warranties, or undertakings in **Section 6.3**, (i) monetary damages will not be a sufficient remedy; (ii) in any event, the injured party will be entitled to such injunctive or equitable relief as a court of competent jurisdiction may grant, without waiving or prejudicing any other rights or remedies. In the event of any breach by Microsoft of any of the provisions of Sections 6.3(a), (b), (c) or (d) of this Agreement, where as a result of such breach (and as long as it continues) Licensee is unable effectively to use the WSPP Documentation as contemplated in Article 5 of the Decision for a software development project the planning or actual execution of which is duly substantiated, Microsoft shall pay Licensee liquidated damages in the amount of One Hundred Thirty-Five Thousand Euros (135,000)~~[*to be determined by Parties based on an estimation of actual damages, but at least €135.000*~~] per day for each day in which such breach continues. The parties acknowledge that the foregoing amount reflects their assessment of the damages which Licensee is likely to incur as a result of such breach including by reason of expected delays in developing products and launching products on the market.

(c) Licensee acknowledges and agrees that (i) monetary damages will not be a sufficient remedy for Licensee's breach of its obligations under **Section 5**, or for use of the WSPP Documentation or exercise of rights in the Microsoft Licensed Intellectual Property other than as authorized by **Sections 2** and **5** of this Agreement, and (ii) such unauthorized disclosure, use or exercise of rights will cause Microsoft immediate, severe and irreparable injury. Accordingly, notwithstanding the provisions of **Section 10.7**, Licensee acknowledges that Microsoft will be entitled in such circumstances, without waiving or prejudicing any other rights or remedies, to such injunctive or equitable relief as a court of competent jurisdiction may grant.

10.7 Governing Law; Jurisdiction; Attorneys' Fees. This Agreement shall be governed by and construed in accordance with English law. Each party hereby submits to the exclusive jurisdiction of the Chancery Division of the High Court of England and Wales in London. Process may be served on either party in the manner authorized by applicable law or court rule. In any formal action or suit to enforce any right or remedy under this Agreement or to interpret any provision of this Agreement, the prevailing party is entitled to recover its costs, including reasonable attorneys' fees, costs and other expenses. The Parties acknowledge and agree that any formal action or suit to enforce any right or remedy under this Agreement or to interpret any provision of this Agreement constitutes an issue relating to the application of Article 82 of the Treaty within the meaning of Article 15 of Regulation 1/2003.

10.8 Assignment.

(a) The party identified as the Licensee parent on the first page of this Agreement may assign this Agreement on satisfaction of the following conditions precedent: (i) such Licensee and the proposed assignee have executed and delivered an Assignment and Assumption Agreement in a form acceptable to Microsoft (a sample of which is available on the WSPP Website), which agreement provides for the assignment of all of Licensee's rights and obligations under this Agreement to the proposed assignee; and (ii) the proposed assignee has satisfied all applicable Program Entry Requirements. Upon fulfillment of (i) and (ii) Microsoft will promptly sign the Assignment and Assumption Agreement and return an executed copy to Licensee and the proposed assignee.

(b) Microsoft may terminate this Agreement immediately upon written notice if the party identified as the Licensee parent on the first page of this Agreement assigns or otherwise transfers, whether by operation of contract, law or otherwise, fifty percent (50%) or more of such Licensee's assets, excluding this Agreement, in a single transaction or series of transactions, unless either (i) the entity to which such Licensee proposes to make such assignment or transfer first enters into a Guarantee Agreement in the form posted on the WSPP Website from time to time, or (ii) such Licensee and Microsoft expressly agree otherwise in writing.

(c) Notwithstanding any other provision of this Agreement, any party identified as a Licensee subsidiary on the first page of this Agreement does not have the right to, and will not, assign this Agreement (or its rights or obligations hereunder) in whole or in part.

(d) Any attempted assignment in violation of **Section 10.8(a), (b) or (c)** is null and void and has no force or effect.

10.9 Construction. This Agreement shall be constructed and applied in light of the operative part of the Decision and statement of reasons for it. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, other than **Sections 2.1, 2.2, 2.3, -2.5** (License Grant; ~~Licensed Server~~ Implementations; License Clarifications; No Other Rights), **5** (Confidentiality**),** **6.5** (Limitations of Liability), **6.6** (Exclusive Remedies and Sole Liability), **8** (Limitations of Remedies & Liability), or **10.8** (Assignment), to be unenforceable, the rest will remain in effect. If any of the foregoing provisions or any portion thereof are held by a court of competent jurisdiction to be unenforceable, this Agreement terminates immediately.

10.10 Third Parties Rights. Other than Section 6.2(b), a~~A~~ person who is not a party to this Agreement is not a beneficiary of the rights granted to Licensee under this Agreement, and has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement in contract.

10.11 Entire Agreement. This Agreement does not constitute an offer by Microsoft and is not effective unless and until this Agreement is signed by duly authorized representatives of both parties. This Agreement may be executed in counterparts, each of which shall be an original and all of which together shall constitute one and the same instrument. This Agreement (including its Exhibits and Appendices) constitutes the entire agreement between the parties with respect to its subject matter and supersedes all prior and contemporaneous communications, agreements, arrangements and understandings between the parties in connection with this Agreement and on such subject matter. Except as provided in **Section 3.1(b)(ii)** (regarding updates to **Exhibit A**), no modifications of this Agreement are effective unless contained in a subsequent written agreement that expressly references this Agreement and its intent to modify its terms, and is signed by duly authorized representatives of Licensee and Microsoft.

IN WITNESS WHEREOF, the parties, through their duly authorized representatives, have entered into this Agreement, to be effective on the Effective Date.

PROTOCOL FREEDOM INFORMATION FOUNDATION~~[LICENSEE NAME]~~ ~~*(parent)*~~

MICROSOFT CORPORATION

______________________________ ______________________________

By (Sign) By (Sign)

______________________________ ______________________________

Name (Print) Name (Print)

______________________________ ______________________________

Title Title

______________________________ ______________________________

Date Date

~~***[Add signature block(s) for each licensee affiliate also licensed under this agreement, if applicable]***~~

EXHIBIT A
Licensed Protocols

(~~(Exhibit A lists WSPP Protocols selected by Licensee.~~ This Exhibit will~~may~~ be updated for additions~~amended from time~~ to ~~time by~~ the WSPP program and (b) any additions as a result~~addition~~ of ~~WSPP Protocols at~~ the Correction Assistance.~~request of the Licensee.~~)

All WSPP
~~[Specific~~ Protocols listed in Appendix 1, Table A-1~~TBD]~~

EXHIBIT B

Program Entry Requirements (applicable as of the Effective Date)

(Version posted to web site October 2007)

Microsoft Work Group and Server Protocol Program: Entry Requirements

Microsoft Work Group Server Protocol Program (WSPP) licensees must sign a license agreement and must meet the following program entry requirements before the agreement becomes effective.

	Section		
Agreement Type	A: Business Status Confirmation	B: General Eligibility	C: Required Payments
4-Day Evaluation Agreement	**X**	**X**	
45-Day Evaluation Agreement	**X**	**X**	**X**
WSPP "All IP" Development Agreement	**X**	**X**	**X**
WSPP "No Patents" Development Agreement	**X**	**X**	**X**
WSPP "Patent Only" Development Agreement	**X**	**X**	**X**
WSPP "IDL Only" Development Agreement	**X**	**X**	**X**

Section A: Business Status Confirmation

A-1. Provide documentation of the legal status of the entity signing the license agreement:

- If the entity is a corporation or limited liability company, you must provide a certificate of good standing from the jurisdiction in which the organization is legally established, dated no earlier than seven days prior to the date you sign the applicable License Agreement.
- If the entity is a partnership or other business entity other than a corporation or limited liability company, you must provide the most recently available issue of a document equivalent to a certificate of good standing.
- If you are an individual or a sole proprietor operating under a business name, you must provide a copy of the applicable business name registration showing both the business name and individual owner.
- **If you are signing as an individual not operating under a business name, you must provide a copy of a government-issued proof of identity, such as a driver's license, that shows a current address.**

Section B: General Eligibility

B-1. Provide your DUNS Number or the equivalent if a DUNS Number is not available in your country. (The D&B "D-U-N-S" Number is a unique nine-digit identification sequence assigned by the D&B Corporation. It is recognized as a global business identification standard and is used by many global, industry, and trade associations as well as commercial companies and governmental agencies. Any business or individual can obtain a DUNS Number from D&B for no charge. For more information, see www.dnb.com.)

B-2. You are not eligible for a license under the Microsoft Work Group Server Protocol Program if:

- A previous Microsoft Work Group Server Protocol Program agreement has been terminated by Microsoft for material breach by you (or a Participating Subsidiary).
- Microsoft has given you written notice of breach of any Microsoft Work Group Server Protocol Program agreement established by a court of competent jurisdiction and the breach has not been cured.

B-3. You are not eligible if providing you (or any Participating Subsidiary) with any licensed data or documentation would be restricted or prohibited by the law of the United States or any other jurisdiction, including export and trade laws (such as U.S. Export Administration Regulations, and end-user, end-use, and destination restrictions). The products, data, and documentation licensed under the Program are subject to United States export jurisdiction.

Section C: Required Payments

C-1. An evaluation fee of €1,000 is required for a 45-day evaluation. The evaluation fee is nonrefundable but is 100 percent applicable toward the prepaid royalties required for a WSPP Development Agreement.

C-2. For each separate WSPP Development Agreement, a license fee (for technical documentation) of €10,000 ~~and a prepaid royalty payment (for patent licenses) of €5,000~~ is required. These amounts are nonrefundable unless your participation in the Microsoft Work Group Server Protocol Program is terminated because you do not complete other Program Entry Requirements.

Additional Notes

These program entry requirements may be revised periodically. However, a potential licensee can elect to qualify under the previous requirements for up to 60 days after revised requirements are posted.

APPENDIX 1
WSPP Pricing Principles and Available Protocols

This Appendix includes the Pricing Principles supporting development of the remuneration under this Agreement, together with a list and description of all protocols currently available for licensing. Microsoft also will discuss with potential licensees the possibility of adding incremental technology or intellectual property rights to those within the WSPP, on commercially reasonable license terms outside of WSPP.

Pricing Principles

Microsoft believes that, with the licensing program it has established and the additional flexibility it is prepared to offer, it will be able to reach an appropriate license with any undertaking that has a good-faith interest in taking a license in accordance with the Decision. However, in the event that Microsoft and a potential licensee are unable to achieve agreement on pricing after good faith efforts, Microsoft is willing to submit the matter for review by the Trustee. In addressing the matter in question, the Trustee shall utilize the following framework for determining appropriate pricing:

The remuneration proposed and/or established by Microsoft is appropriate if it:

i. enables implementation of the protocols by a licensee in a commercially practicable manner; *and*

ii. reflects value conferred upon a licensee to the exclusion of the strategic value stemming from Microsoft's market power in the client PC operating system market or in the work group server operating system market.

The Trustee should recognize that the effectiveness of the Decision in accordance with Article 82 may be hampered if royalties are excessive. In this regard, the Trustee should consider as a cap on the appropriate royalty level the likely non-strategic incremental income to the licensee that will result from implementation of the specifications.

With regard to part (ii), the Trustee shall consider, in particular:

- whether the protocols described in the specifications are Microsoft's own creations (as opposed to Microsoft's implementation of a publicly available standard, such as IETF RFCs, W3C standards or other comparables);
- whether these creations by Microsoft constitute innovation; and,
- a market valuation of technologies deemed comparable, excluding the strategic value that stems from the dominance of any such technologies.

The Trustee may consider other factors that he or she deems appropriate and which are consistent with the Decision, as confirmed by the Commission, drawing upon standard valuation techniques.

Additional information with respect to Microsoft's commitment on licensing scenarios is provided below.

WSPP Protocols

The WSPP Protocols are the versions of the following protocols as implemented in Windows Server Operating Systems and used to provide File and Print Server or User and Group Administration Server services (as the case may be) in accordance with this Agreement**,** to a Windows Client Operating System or Windows Server Operating System running on another computer in a Windows Work Group Network, or to obtain such services from a Windows Server Operating System running on another computer in a Windows Work Group Network.

Appendix 1 lists the WSPP Protocols grouped by functionality based upon Microsoft's implementations of the WSPP Protocols (**Table A-1**) and describes in detail each WSPP Protocol (**Table A-2**). Other reasonable functional categories may be developed at the request of Licensee**.**

The WSPP Protocols are grouped (and may be licensed) in three basic ways:

1. All WSPP Protocols

2. WSPP Protocols for a specific task: A task is a collection of protocols used to implement a specific but fairly broad system function. There are three tasks that are part of WSPP. Each task may be licensed individually and includes protocols from all the protocol groups under it.

    a. File/Print
    b. User and Group Administration
    c. General Networking

3. WSPP Protocols for a defined Scenario: A Scenario is a more limited set of functions that is part of a specific task. The Scenarios that may be licensed individually are as follows:

    a. File/Print
        i. Base File Services
        ii. Distributed File System (DFS) + File Replication Service (FRS)
        iii. Print Remote Procedure Call
        iv. Internet File Print
        v. Advanced File Services

    b. User and Group Administration
        i. Base Authentication and Authorization
        ii. Domain Services Interaction
        iii. Multi-Factor Authentication & Certificate Services
        iv. Group Policy
        v. Systems and System Health Management
        vi. Directory & Global Catalog Replication
        vii. Kerberos Group Membership
        viii. Windows Remote Registry Services
        ix. Windows Event Logging
        x. Network Time Services
        xi. Network Connection Management
        xii. MSDN Protocols
        xiii. Remote Procedure Calls
        xiv. Network Access Protection
        xv. Windows Security Health Validator
        xvi. NAP Extensions for DHCP
        xvii. Rights Management

    c. All Client-Server Protocols

    d. Networking Transport

    e. One-time Flat Fee Protocols

Table A-1

List of WSPP Protocols

1. The table does not include listings for recently added new WSPP Protocols for the Standard Edition of Windows Server 2008.
2. **Bold** indicates protocols **new** to Windows Server 2008
3. *Italics* indicate protocols *modified* for Windows Server 2008
4. ~~An asterisk indicates that the protocol is a Restricted Protocol.~~

Protocol Information	**Technical Documentation Title**	**IDL**
I. File/Print Task		
A. Base File Services Scenario		
1. Common Interface File System (CIFS) Browser Protocol	[MS-BRWS]: Common Internet File System (CIFS) Browser Protocol Specification	
2. Disk Management Remote Protocol	[MS-DMRP]: Disk Management Remote Protocol Specification	Y
3. Distributed Link Tracking: Central Manager Protocol	[MS-DLTM]: Distributed Link Tracking: Central Manager Protocol Specification	Y
4. Distributed Link Tracking: Central Store Protocol	[MS-DLTCS]: Distributed Link Tracking Central Store Protocol Specification	
5. Distributed Link Tracking: Workstation Protocol	[MS-DLTW]: Distributed Link Tracking: Workstation Protocol Specification	Y
6. Encrypting File System Remote Protocol	[MS-EFSR]: Encrypting File System Remote (EFSRPC) Protocol Specification	Y
7. FrontPage Server Extensions Remote Protocol	[MS-FPSE]: FrontPage Server Extensions Remote Protocol Specification	
8. Microsoft Content Indexing Services Protocol	[MS-MCIS]: Content Indexing Services Protocol Specification	
9. Remote Administration Protocol	[MS-RAP]: Remote Administration Protocol Specification	
10. Remote Mailslot Protocol	[MS-MAIL]: Remote Mailslot Protocol Specification	
11. Removable Storage Manager (RSM) Remote Protocol	[MS-RSMP]: Removable Storage Manager (RSM) Remote Protocol Specification	Y
12. Server Message Block (SMB) Version 1.0 Protocol	[MS-FSCC]: File System Control Codes [MS-SMB]: Server Message Block (SMB) Protocol Specification	
13. Server Service Remote Protocol	[MS-SRVS]: Server Service Remote Protocol Specification	Y
14. Virtual Disk Service (VDS) Protocol	[MS-VDS]: Virtual Disk Service (VDS) Protocol Specification	Y
15. Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions	[MS-WDV]: Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions	

Protocol Information	**Technical Documentation Title**	**IDL**
16. Web Distributed Authoring and Versioning (WebDAV) Protocol: Microsoft Extensions	[MS-WDVRN]: World Wide Distributed Authoring and Versioning (WebDAV) Noroot Depth Protocol Specification [MS-WDVRV]: World Wide Distributed Authoring and Versioning (WebDAV) MS-Author-Via Protocol Specification	
17. Web Distributed Authoring and Versioning (WebDAV) Protocol: Server Extensions	[MS-WDVRN]: World Wide Distributed Authoring and Versioning (WebDAV) Noroot Depth Protocol Specification [MS-WDVRV]: World Wide Distributed Authoring and Versioning (WebDAV) MS-Author-Via Protocol Specification	
18. Windows Search Protocol	[MS-WSP]: Windows Search Protocol Specification	
19. WS-Management Protocol Version 2.0 Extensions	[MS-WSMV]: Web Services Management Protocol Extensions for Windows Vista	
B. DFS (Distributed File Service) + FRS (File Replication Service) Scenario		
1. Distributed File System (DFS): Namespace Management Protocol	[MS-DFSN]: Distributed File System (DFS): Namespace Management Protocol Specification	Y
2. Distributed File System (DFS): Namespace Referral Protocol	[MS-DFSC]: Distributed File System (DFS): Referral Protocol Specification	
3. File Replication Service (FRS) Protocol	[MS-BKUP]: Microsoft NT Backup File Structure Specification [MS-FRS1]: File Replication Service Protocol Specification	Y
C. Print RPC Scenario		
1. Enhanced Metafile (EMF) Format: Plus Extensions (EMF+)	[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions Specification	
2. Enhanced Metafile (EMF) Spool Format	[MS-EMFSPOOL]: Enhanced Metafile Spool Format Specification	
3. Print System Asynchronous Notification Protocol	[MS-PAN]: Print System Asynchronous Notification Protocol Specification	Y
4. Print System Asynchronous Remote Protocol	[MS-PAR]: Print System Asynchronous Remote Protocol Specification	Y
5. Print System Remote Protocol	[MS-RPRN]: Print System Remote Protocol Specification	Y
D. Internet File and Print Scenario		
1. Web Point and Print Protocol	[MS-WPRN]: Web Point-and-Print Protocol Specification	
E. Advanced File Services Scenario		
1. Common Interface File System (CIFS) Browser Protocol	[MS-BRWS]: Common Internet File System (CIFS) Browser Protocol Specification	
2. Disk Management Remote Protocol	[MS-DMRP]: Disk Management Remote Protocol Specification	Y

Protocol Information	**Technical Documentation Title**	**IDL**
3. Distributed File System: Replication (DFS-R) Protocol	[MS-BKUP]: Microsoft NT Backup File Structure Specification [MS-FRS2]: SD Microsoft Distributed File System Replication Protocol Specification	**Y**
4. Distributed File System: Replication Helper Protocol (DFS-R Helper)	[MS-DFSRH]: DFS Replication Helper Protocol Specification	**Y**
5. Distributed Link Tracking: Central Manager Protocol	[MS-DLTM]: Distributed Link Tracking: Central Manager Protocol Specification	Y
6. Distributed Link Tracking: Central Store Protocol	[MS-DLTCS]: Distributed Link Tracking Central Store Protocol Specification	
7. Distributed Link Tracking: Workstation Protocol	[MS-DLTW]: Distributed Link Tracking: Workstation Protocol Specification	Y
8. Encrypting File System Remote Protocol	[MS-EFSR]: Encrypting File System Remote (EFSRPC) Protocol Specification	Y
9. FrontPage Server Extensions Remote Protocol	[MS-FPSE]: FrontPage Server Extensions Remote Protocol Specification	
10. Microsoft Content Indexing Services Protocol	[MS-MCIS]: Content Indexing Services Protocol Specification	
11. Peer Name Resolution Protocol (PNRP) Version 4.0	[MS-PNRP]: Peer Name Resolution Protocol (PNRP) Version 4.0 Specification	
12. Remote Administration Protocol	[MS-RAP]: Remote Administration Protocol Specification	
13. Remote Differential Compression (RDC) Protocol	[MS-RDC]: Remote Differential Compression Protocol Specification	
14. Remote Mailslot Protocol	[MS-MAIL]: Remote Mailslot Protocol Specification	
15. Removable Storage Manager (RSM) Remote Protocol	[MS-RSMP]: Removable Storage Manager (RSM) Remote Protocol Specification	Y
16. Server Message Block (SMB) Version 1.0 Protocol	[MS-FSCC]: File System Control Codes [MS-SMB]: Server Message Block (SMB) Protocol Specification	
17. Server Message Block (SMB) Version 2.0 Protocol	[MS-SMB2]: Server Message Block (SMB) Version 2.0 Protocol Specification	
18. Server Service Remote Protocol	[MS-SRVS]: Server Service Remote Protocol Specification	Y
19. Virtual Disk Service (VDS) Protocol	[MS-VDS]: Virtual Disk Service (VDS) Protocol Specification	Y
20. Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions	[MS-WDV]: Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions	
21. Web Distributed Authoring and Versioning (WebDAV) Protocol: Microsoft Extensions	[MS-WDVRN]: World Wide Distributed Authoring and Versioning (WebDAV) Noroot Depth Protocol Specification [MS-WDVRV]: World Wide Distributed Authoring and Versioning (WebDAV) MS-Author-Via Protocol Specification	

Protocol Information	**Technical Documentation Title**	**IDL**
22. Web Distributed Authoring and Versioning (WebDAV) Protocol: Server Extensions	[MS-WDVRN]: World Wide Distributed Authoring and Versioning (WebDAV) Noroot Depth Protocol Specification [MS-WDVRV]: World Wide Distributed Authoring and Versioning (WebDAV) MS-Author-Via Protocol Specification	
23. Windows Search Protocol	[MS-WSP]: Windows Search Protocol Specification	
24. WS-Management Protocol Version 2.0 Extensions	[MS-WSMV]: Web Services Management Protocol Extensions for Windows Vista	
II. User & Group Administration Task		
A. Base Authentication and Authorization Scenario		
1. Authentication Protocol Domain Support	[MS-APDS]: Authentication Protocol Domain Support Specification	
2. _BackupKey Remote Protocol_*	[MS-BKRP]: BackupKey Remote Protocol Specification	Y
3. Digest Access Authentication: Microsoft Extensions	[MS-DPSP]: Digest Protocol Extensions	
4. Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) Protocol Extension	[MS-GSSA]: Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) Protocol Extension	
5. _Kerberos Network Authentication Service (v5) Extensions_*	[MS-KILE]: Kerberos Protocol Extensions	
6. Kerberos Network Authentication Service (v5) Service for User (S4U) Extension	[MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol Specification	
7. _Local Security Authority (Domain Policy) Remote Protocol_*	[MS-LSAD]: Local Security Authority (Domain Policy) Remote Protocol Specification	Y
8. Local Security Authority (Translation Methods) Remote Protocol	[MS-LSAT]: Local Security Authority (Translation Methods) Remote Protocol Specification	Y
9. _Netlogon Remote Protocol_*	[MS-NRPC]: Netlogon Remote Protocol Specification	Y
10. _NetLogon Remote Protocol: Challenge Handshake Authentication Protocol (CHAP)/ EAP-MD5 SubAuthentication Extension_*	[MS-APDS]: Authentication Protocol Domain Support Specification	
11. NT LAN Manager (NTLM) Authentication Protocol	[MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol Specification	
12. NTLM Over HTTP Protocol	[MS-NTHT]: NTLM Over HTTP Protocol Specification	
13. Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol: Microsoft Extensions	[MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol Specification	
14. _Security Account Manager (SAM) Remote Protocol (Client-to-Server)_*	[MS-SAMR]: Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)	Y

Protocol Information	**Technical Documentation Title**	**IDL**
15. *Security Account Manager (SAM) Remote Protocol (Server-to-Server)**	[MS-SAMS]: Security Account Manager (SAM) Remote Protocol Specification (Server-to-Server)	
16. *Simple and Protected Generic Security Service Application Program Interface Negotiation Mechanism (SPNEGO) Protocol Extensions*	[MS-SPNG]: Simple and Protected Generic Security Service Application Program Interface Negotiation Mechanism (SPNEGO) Protocol Extensions	
17. *Web Browser Federated Sign-On Protocol*	[MS-MWBF]: Microsoft Web Browser Federated Sign-On Protocol Specification	
18. *Web Browser Federated Sign-On Protocol Extensions*	[MS-MWBE]: Microsoft Web Browser Federated Sign-On Protocol Extensions	
B. Domain Services Interaction Scenario		
1. *Active Directory Technical Specification**	[MS-ADA1]: Active Directory Schema Attributes A-L [MS-ADA2]: Active Directory Schema Attributes M [MS-ADA3]: Active Directory Schema Attributes N-Z [MS-ADLS]: Active Directory Lightweight Directory Services Schema [MS-ADSC]: Active Directory Schema Classes [MS-ADTS]: Active Directory Technical Specification	
2. *Authentication Protocol Domain Support*	[MS-APDS]: Authentication Protocol Domain Support Specification	
3. *BackupKey Remote Protocol**	[MS-BKRP]: BackupKey Remote Protocol Specification	Y
4. *Kerberos Network Authentication Service (v5) Extensions**	[MS-KILE]: Kerberos Protocol Extensions	
5. *Local Security Authority (Domain Policy) Remote Protocol**	[MS-LSAD]: Local Security Authority (Domain Policy) Remote Protocol Specification	Y
6. Local Security Authority (Translation Methods) Remote Protocol	[MS-LSAT]: Local Security Authority (Translation Methods) Remote Protocol Specification	Y
7. *Netlogon Remote Protocol**	[MS-NRPC]: Netlogon Remote Protocol Specification	Y
8. Privilege Attribute Certificate (PAC) Data Structure	[MS-PAC]: Privilege Attribute Certificate Data Structure	
9. *Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol*	[MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol Specification	
10. Remote Certificate Mapping Protocol*	[MS-RCMP]: Remote Certificate Mapping Protocol Specification	
11. *Security Account Manager (SAM) Remote Protocol (Client-to-Server)**	[MS-SAMR]: Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)	Y
12. *Security Account Manager (SAM) Remote Protocol (Server-to-Server)**	[MS-SAMS]: Security Account Manager (SAM) Remote Protocol Specification (Server-to-Server)	
13. *Windows Client Certificate Enrollment Protocol**	[MS-WCCE]: Windows Client Certificate Enrollment Protocol Specification	Y

Protocol Information	Technical Documentation Title	IDL
C. Multi-Factor Authentication & Certificate Services Scenario		
1. Certificate Services Remote Administration Protocol*	[MS-CSRA]: Certificate Services Remote Administration Protocol Specification	Y
2. Certificate Templates	[MS-CRTD]: Certificate Templates Structure Specification	
3. Remote Certificate Mapping Protocol*	[MS-RCMP]: Remote Certificate Mapping Protocol Specification	
4. *Windows Client Certificate Enrollment Protocol**	[MS-WCCE]: Windows Client Certificate Enrollment Protocol Specification	Y
D. Group Policy Scenario		
1. Group Policy: Folder Redirection Protocol Extension	[MS-GPFR]: Group Policy: Folder Redirection Protocol Extension	
2. Group Policy: Core Protocol	[MS-GPOL]: Group Policy: Core Protocol Specification	
3. Group Policy: Deployed Printer Connections Extension	[MS-GPDPC]: Group Policy: Deployed Printer Connections Extension	
4. Group Policy: Host Security Configuration	[MS-GPSB]: Group Policy: Security Protocol Extension	
5. Group Policy: Internet Explorer Maintenance Extension	[MS-GPIE]: Group Policy: Internet Explorer Maintenance Extension	
6. Group Policy: IP Security (IPSec) Protocol Extension	[MS-GPIPSEC]: Group Policy: IP Security (IPSec) Protocol Extension	
7. Group Policy: Preferences Extension	[MS-GPPREF]: Group Policy: Preferences Extension Data Structure	
8. Group Policy: Registry Extension Encoding	[MS-GPREG]: Group Policy: Registry Extension Encoding	
9. Group Policy: Scripts Extension Encoding	[MS-GPSCR]: Group Policy: Scripts Extension Encoding	
10. Group Policy: Software Installation Protocol Extension	[MS-GPSI]: Group Policy: Software Installation Protocol Extension	
11. Group Policy: Wireless/Wired Protocol Extension	[MS-GPWL]: Group Policy: Wireless/Wired Protocol Extension	
E. Systems and Systems Health Management Scenario		
1. Background Intelligent Transfer Service (BITS) Peer-Caching: Content Retrieval	[MS-BPCR]: Background Intelligent Transfer Service (BITS) Peer-Caching: Content Retrieval Protocol Specification	
2. Background Intelligent Transfer Service (BITS) Peer-Caching: Peer	[MS-BPAU]: Background Intelligent Transfer Service (BITS) Peer-Caching: Peer Authentication Protocol Specification	**Y**
3. Background Intelligent Transfer Service (BITS) Peer-Caching: Peer Discovery	[MS-BPDP]: Background Intelligent Transfer Service (BITS) Peer-Caching: Peer Discovery Protocol Specification	

Protocol Information	Technical Documentation Title	IDL
4. *Directory Services Setup Remote Protocol**	[MS-DSSP]: Directory Services Setup Remote Protocol Specification	Y
5. *Disk Management Remote Protocol*	[MS-DMRP]: Disk Management Remote Protocol Specification	Y
6. *InitShutdown Protocol*	[MS-RSP]: Remote Shutdown Protocol Specification	Y
7. *Removable Storage Manager (RSM) Remote Protocol*	[MS-RSMP]: Removable Storage Manager (RSM) Remote Protocol Specification	Y
8. *Server Service Remote Protocol*	[MS-SRVS]: Server Service Remote Protocol Specification	Y
9. Service Control Manager Remote Protocol	[MS-SCMR]: Service Control Manager Remote Protocol Specification	Y
10. *Task Scheduler Remoting Protocol*	[MS-TSCH]: AT Service Remote Protocol Specification	Y
11. Windows Management Instrumentation Encoding Version 1.0 Protocol	[MS-WMIO]: Windows Management Instrumentation Encoding Version 1.0 Protocol Specification	
12. Windows Management Instrumentation Remote Protocol	[MS-WMI]: Windows Management Instrumentation Remote Protocol Specification [MS-WMIO]: Windows Management Instrumentation Encoding Version 1.0 Protocol Specification	Y
13. WS-Management Protocol Extensions	[MS-WSMAN]: Web Services Management Protocol Extensions for Windows Server 2003	
14. WS-Management Version 2.0 Protocol Extensions	[MS-WSMV]: Web Services Management Protocol Extensions for Windows Vista	
F. Directory & Global Catalog Replication Scenario		
1. *Directory Replication Service (DRS) Remote Protocol**	[MS-DRSR]: Directory Replication Service (DRS) Remote Protocol Specification	Y
2. SMTP Replication Protocol Extensions	[MS-SRPL]: Directory Replication Service (DRS) Protocol Extensions for SMTP	
G. Kerberos Group Membership Scenario		
1. *Kerberos Network Authentication Service (v5) Extensions**	[MS-KILE]: Kerberos Protocol Extensions	
2. *Kerberos Network Authentication Service (v5) Service for User (S4U) Extension*	[MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol Specification	
3. *Privilege Attribute Certificate (PAC) Data Structure*	[MS-PAC]: Privilege Attribute Certificate Data Structure	
H. Windows Remote Registry Services		
1. Windows Remote Registry Protocol	[MS-RRP]: Windows Remote Registry Protocol Specification	Y
I. Windows Event Logging Scenario		

Protocol Information	**Technical Documentation Title**	**IDL**
1. Eventlog Remoting Protocol Version 1.0	[MS-EVEN]: Eventlog Remote Protocol Specification	Y
2. Eventlog Remoting Protocol Version 6.0	**[MS-EVEN6]: Eventlog Remote Protocol Version 6.0 Specification**	**Y**
J. Network Time Services		
1. Network Time Protocol (NTP) Authentication Extensions	[MS-SNTP]: Network Time Protocol (NTP) Authentication Extensions	
2. W32Time Remote Protocol	[MS-W32T]: W32Time Remote Protocol Specification	Y
K. Network Connection Management		
1. Workstation Service Remote Protocol (WKSSVC)	[MS-WKST]: Workstation Service Remote Protocol Specification	Y
L. MSDN Protocols		
1. See MSDN Website		Y
M. Remote Procedure Calls (RPC) Scenario		
1. ExtendedError Remote Data Structure	[MS-EERR]: ExtendedError Remote Data Structure	Y
2. Remote Procedure Call Location Services Protocol Extensions	[MS-RPCL]: Remote Procedure Call Location Services Extensions	Y
3. Remote Procedure Call Over HTTP Protocol	[MS-RPCH]: Remote Procedure Call Over HTTP Protocol Specification	
4. Remote Procedure Call Protocol Extensions	[MS-RPCE]: Remote Procedure Call Protocol Extensions	Y
N. Network Access Protection (NAP) Scenario		
1. Health Certificate Enrollment Protocol	[MS-HCEP]: Health Certificate Enrollment Protocol Specification	**Y**
2. Network Access Protection Statement of Health	[MS-SOH]: Statement of Health for Network Access Protection (NAP) Protocol Specification	
3. Remote Access Dial In User Service (RADIUS): Network Access Protection (NAP) Attributes	[MS-RNAP]: Vendor-Specific RADIUS Attributes for Network Access Protection (NAP) Protocol Specification	
O. Windows Security Health Validator		
1. Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol	[MS-WSH]: Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol Specification	
P. Network Access Protection (NAP) Extensions for DHCP		
1. Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP)	[MS-DHCPN]: Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP)	

Protocol Information	**Technical Documentation Title**	**IDL**
R. Rights Management Services		
1. **Rights Management Server (RMS): Client-Server Protocol***	[MS-RMPR]: Rights Management Services (RMS): Client-to-Server Protocol Specification	
2. **Rights Management Server (RMS): Server-Server Protocol***	[MS-RMPRS]: Rights Management Services (RMS): Server-to-Server Protocol Specification	
III. Networking Transport		
1. Authenticated Internet Protocol	[MS-AIPS]: Authenticated Internet Protocol Specification	
2. Distributed Component Object Model (DCOM) Remote Protocols	[MS-DCOM]: Distributed Component Object Model (DCOM) Remote Protocol Specification	Y
3. Dynamic Host Configuration Protocol (DHCP) Extensions	[MS-DHCPE]: Dynamic Host Configuration Protocol (DHCP) Extensions	
4. Extensible Authentication Protocol Method for Microsoft Challenge	[MS-CHAP]: Extensible Authentication Protocol Method for Microsoft Challenge Handshake Authentication Protocol (CHAP) Specification	
5. ICertPassage Remote Protocol	[MS-ICPR]: ICertPassage Remote Protocol Specification	Y
6. Internet Key Exchange (IKE) Protocol Extensions	[MS-IKEE]: Internet Key Exchange Protocol Extensions	
7. IPv4 over IEEE 1394 Protocol Extensions	[MS-V4OF]: IPv4 Over IEEE 1394 Protocol Extensions	
8. Key Service Remote (IkeySvcR) Protocol	[MS-IKEY]: Key Service Remote (IKeySvcR) Protocol Specification	Y
9. Messenger Service Messaging Protocol	[MS-MSRP]: Messenger Service Remote Protocol Specification	Y
10. Messenger Service Name Management Protocol	[MS-MSRP]: Messenger Service Remote Protocol Specification	Y
11. Microsoft Protected Extensible Authentication Protocol (PEAP)	[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP) Specification	
12. OLE Automation Protocol	[MS-OAUT]: OLE Automation Protocol Specification	Y
13. Remote Data Services (RDS) Transport Protocol	[MS-ADTG]: Remote Data Services (RDS) Transport Protocol Specification	
14. Server-Side Include (SSI) 1.4 Protocol	[MS-PASS]: Passport Server Side Include (SSI) Version 1.4 Protocol Specification	
15. Teredo Extensions	[MS-TERE]: Teredo Extensions	
16. User Name Mapping (UNM) Protocol	[MS-UNMP]: User Name Mapping Protocol Specification	Y
17. Windows Internet Naming Service (WINS) Replication and Autodiscovery Protocol	[MS-WINSRA]: Windows Internet Naming Service (WINS) Replication and Autodiscovery Protocol Specification	
18. Windows Server Update Services: Client-Server Protocol	[MS-WUSP]: Windows Update Services: Client-Server Protocol Specification	

Protocol Information	Technical Documentation Title	IDL
19. Windows Server Update Services: Server-Server Protocol	[MS-WSUSSS]: Windows Update Services: Server-Server Protocol Specification	

Table A-2
Description of WSPP Protocols

(**Note:** The table does not include listings for recently added new WSPP Protocols for the Standard Edition of Windows Server 2008.)

Protocol	**Description**
I. File and Print Protocol Groups	
A. Base File Server Protocols: Protocols used to provide basic file service operations to other Windows client and server computers on a network.	
1. Common Interface File System (CIFS) Browser Protocol	Enables interaction with the Browser service, which creates and maintains a view of resources available on a network.
2. Disk Management Remote Protocol	Enables remote management of disks on a computer running Windows 2000, Microsoft Windows XP, or Microsoft Windows Server 2003.
3. Distributed Link Tracking: Central Manager Protocol	Used to determine the new location of a file that has moved, whether the file has moved within a computer or between computers in a network.
4. Distributed Link Tracking: Central Store Protocol	Used to determine the new location of a file that has moved, whether the file has moved within a computer or between computers in a network.
5. Distributed Link Tracking: Workstation Protocol	Used to determine the new location of a file that has moved, whether the file has moved within a computer or between computers in a network.
6. Encrypting File System Remote Protocol	Performs remote Encrypting File System (EFS) operations. Methods are provided to handle read, write, and retrieval operations between a client and server.
7. FrontPage Server Extensions Remote Protocol	Allows client access to server resources and resource properties.
8. Microsoft Content Indexing Services Protocol	Provides methods of querying and managing Microsoft Content Indexing Services parameters using a named pipe.
9. Remote Administration Protocol	Provides a mechanism to enable clients to browse services on the network that are advertised through this protocol. Example services are print and file shares.
10. Remote Mailslot Protocol	Enables a simple, unreliable, unidirectional Inter-Process Communication (IPC) between a client and server.
11. Removable Storage Manager (RSM) Remote Protocol	Enables data management client applications to access removable media in automated libraries, including calling for media to be moved from storage slots to drives on Windows 2000 and Windows XP
12. Server Message Block (SMB) Version 1.0 Protocol	Allows client systems to request file and print services from server systems over a network.
13. Server Service Remote Protocol	Provides the ability to manage file and print serving resources, and responds to requests made by other computers for shared resources on the local computer.

Protocol	Description
14. Virtual Disk Service (VDS) Protocol	Provides a mechanism for remote configuration of disks, partitions, volumes and iSCSI initiators on a server. Through the VDS Protocol, a client can change the configuration of disks into partitions, partitions into volumes, and volumes into file systems. The protocol also enables clients to obtain notifications of changes to these storage objects.
15. Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions	Allows client access to server resources and resource properties.
16. Web Distributed Authoring and Versioning (WebDAV) Protocol: Microsoft Extensions	Allows client access to server resources and resource properties.
17. Web Distributed Authoring and Versioning (WebDAV) Protocol: Server Extensions	Allows client access to server resources and resource properties.
18. Windows Search Protocol	Sends and receives search queries between a client process and the Windows Search service on a local or remote machine.
19. WS-Management Protocol Version 2.0 Extensions	Contains the Microsoft profile of WS-Management 1.0 included in Microsoft Windows Vista. Also includes definitions for interoperating with the WS-Management profile for Microsoft Windows Server 2003 R2.
B. Distributed File System (DFS) + File Replication Service (FRS) Server Protocols: Protocols used between Windows servers to administer the management of files located on multiple connected computers accessed using a single namespace. Protocols used between Windows servers for automatic replication of files to across multiple connected servers.	
1. Distributed File System (DFS): Namespace Management Protocol	Used to create and administer DFS Namespaces, which enable creation of a virtual contiguous file system namespace to unify disparate file server namespaces.
2. Distributed File System (DFS): Namespace Referral Protocol	Used by the filesystem component of Windows to resolve domain names. Optionally it can traverse the namespace to find a reparse point (i.e. leaf) to provide an additional level of indirection.
3. File Replication Service (FRS) Protocol	Replicates files among servers on the network on servers running Windows Server 2003 and Windows 2000 Server.
C. Print Remote Procedure Call Protocols: Protocols used to provide print services to other Windows clients and servers on a network.	
1. Enhanced Metafile (EMF) Format: Plus Extensions (EMF+)	Defines an extension to the Enhanced Metafile Format (EMF) for sending Windows Extended Graphics Device Interface (GDI+) commands and objects to devices, such as displays and printers, that support the drawing of images, graphics, and text.
2. Enhanced Metafile (EMF) Spool Format	This file format is used by the spooler protocol. It includes information such as an EMF file per printed page, printing settings in the DEVMODE structure, and other information like font embedding and injected Postscript commands.
3. Print System Asynchronous Notification Protocol	Used by clients to receive print status notifications from a print server and send any server-requested responses to those notifications back to the server.

Protocol	Description
4. Print System Asynchronous Remote Protocol	Print System Asynchronous Remote Protocol is an asynchronous RPC-based protocol used by a print client to send print jobs to a print server and direct their processing, and to add or remove print queues or perform other print system management functions.
5. Print System Remote Protocol	Remotely manages the print spooler on a server, allowing administration of the printer, job, driver, language monitor, port monitor, and print processor.
D. Internet Print Protocols: Protocols used to provide printing and print job management to Windows clients and servers over the Internet.	
1. Web Point-and-Print Protocol	Allows a worldwide distribution of printer driver software using standard HTTP packets.
E. Advanced File Services Protocols: Protocols used to provide advanced file service operations to other Windows client and server computers on a network	
1. Common Interface File System (CIFS) Browser Protocol	Enables interaction with the Browser service, which creates and maintains a view of resources available on a network.
2. Disk Management Remote Protocol	Enables remote management of disks on a computer running Windows 2000, Microsoft Windows XP, or Microsoft Windows Server 2003.
3. Distributed File System (DFS): Replication Protocol	Replicates files among servers on the network on servers running Windows Server 2003 R2 and later.
4. Distributed File System (DFS): Replication Helper Protocol	A DCOM protocol that consists of interfaces for changing, modifying, and deleting configuration objects in Active Directory by using the server account, and an interface for monitoring DFS replication on the computer and collecting various statistics about the DFS replication operation.
5. Distributed Link Tracking: Central Manager Protocol	Used to determine the new location of a file that has moved, whether the file has moved within a computer or between computers in a network.
6. Distributed Link Tracking: Central Store Protocol	Used to determine the new location of a file that has moved, whether the file has moved within a computer or between computers in a network.
7. Distributed Link Tracking: Workstation Protocol	Used to determine the new location of a file that has moved, whether the file has moved within a computer or between computers in a network.
8. Encrypting File System Remote Protocol	Performs remote Encrypting File System (EFS) operations. Methods are provided to handle read, write, and retrieval operations between a client and server.
9. FrontPage Server Extensions Remote Protocol	Allows client access to server resources and resource properties.
10. Microsoft Content Indexing Services Protocol	Provides methods of querying and managing Microsoft Content Indexing Services parameters using a named pipe.
11. Peer Name Resolution Protocol (PNRP) Version 4.0	Provides peer-to-peer name resolution services by referring requests among active peers in the PNRP cloud.
12. Remote Administration Protocol	Provides a mechanism to enable clients to browse services on the network that are advertised through this protocol. Example services are print and file shares.

Protocol	Description
13. Remote Differential Compression (RDC) Protocol	Enables synchronization of files with a remote source by using compression techniques to minimize the amount of data sent between a client and server.
14. Remote Mailslot Protocol	Enables a simple, unreliable, unidirectional Inter-Process Communication (IPC) between a client and server.
15. Removable Storage Manager (RSM) Remote Protocol	Enables data management client applications to access removable media in automated libraries, including calling for media to be moved from storage slots to drives on Windows 2000 and Windows XP
16. Server Message Block (SMB) Version 1.0 Protocol	Allows client systems to request file and print services from server systems over a network.
17. Server Message Block (SMB) Version 2.0 Protocol	Allows Windows Vista client systems to request advanced file and print services from server systems over a network.
18. Server Service Remote Protocol	Provides the ability to manage file and print serving resources, and responds to requests made by other computers for shared resources on the local computer.
19. Virtual Disk Service (VDS) Protocol	Provides a mechanism for remote configuration of disks, partitions, volumes and iSCSI initiators on a server. Through the VDS Protocol, a client can change the configuration of disks into partitions, partitions into volumes, and volumes into file systems. The protocol also enables clients to obtain notifications of changes to these storage objects.
20. Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions	Allows client access to server resources and resource properties.
21. Web Distributed Authoring and Versioning (WebDAV) Protocol: Microsoft Extensions	Allows client access to server resources and resource properties.
22. Web Distributed Authoring and Versioning (WebDAV) Protocol: Server Extensions	Allows client access to server resources and resource properties.
23. Windows Search Protocol	Sends and receives search queries between a client process and the Windows Search service on a local or remote machine.
24. WS-Management Protocol Version 2.0 Extensions	Contains the Microsoft profile of WS-Management 1.0 included in Microsoft Windows Vista. Also includes definitions for interoperating with the WS-Management profile for Microsoft Windows Server 2003 R2.
II. User & Group Administration Protocol Groups	
A. Base Authentication / Authorization Server Protocols: Protocols used to provide standard authentication and authorization services for Windows clients and servers.	
1. Authentication Protocol Domain Support	Specifies the profiles of multiple authentication protocols required to produce a conformant implementation of a domain controller and a domain-joined client or server machine.
2. BackupKey Remote Protocol	Provides methods for communicating master key backup information between the client computer and the domain controller (DC)
3. Digest Access Authentication: Microsoft Extensions	Performs authentication between a client and a server, based on a user name and a password.

Protocol	**Description**
4. Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) Protocol Extension	Includes changes to the TSIG protocol used when generating the signature on the final response in the TKEY negotiation.
5. Kerberos Network Authentication Service (v5) Extensions	Extends the Kerberos V5 specification with support for interactive user logon.
6. Kerberos Network Authentication Service (v5) Service for User (S4U) Extension	Provides mechanisms for an application service to obtain a Kerberos Service Ticket on behalf of a user, allowing the application to perform functions on behalf of the user.
7. Local Security Authority (Domain Policy) Remote Protocol	Provides access to the domain policy implementation of Local Security Authority (LSA), a protected subsystem of the Microsoft Windows 2000 and later operating systems that performs policy checking and name lookup on the DC.
8. Local Security Authority (Translation Methods) Remote Protocol	Provides access to the translation methods of Local Security Authority (LSA), a protected subsystem of Windows 2000 and later operating systems that performs policy checking and name lookup on the DC.
9. Netlogon Remote Protocol	Provides the complete set of remote procedure call (RPC) methods for Netlogon transactions between client members and DCs.
10. NetLogon Remote Protocol: Challenge Handshake Authentication Protocol (CHAP)/ EAP-MD5 SubAuthentication Extension	Defines an extension to the Net Logon Remote Protocol that allows a Network Policy Server to remotely validate CHAP or EAP-MD5 authentication to Active Directory.
11. NT LAN Manager (NTLM) Authentication Protocol	Allows user account information to be stored either locally on each server or on authentication servers. It is required for network authentication with versions of Windows NT earlier than Windows 2000, and with stand-alone systems.
12. NTLM Over HTTP Protocol	Describes use of the NTLM authentication protocol over HTTP to authenticate Windows clients to servers.
13. Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol: Microsoft Extensions	Describes certain extensions to the RFC4556 standard.
14. Security Account Manager (SAM) Remote Protocol (Client-to-Server)	Performs remote Service Account Manager (SAM) operations, such as user account management and manipulation.
15. Security Account Manager (SAM) Remote Protocol (Server-to-Server)	Provides the server-to-server implementation of the Security Account Manager Remote protocol.
16. Simple and Protected Generic Security Service Application Program Interface Negotiation Mechanism (SPNEGO) Protocol Extensions	Describes extensions that process certain SPNEGO message fields differently from the standard specification, including the NegTokenInit and universal receiver fields.

Protocol	Description
17. Web Browser Federated Sign-On Protocol	Consists of a profile of, and set of extensions to, the WS-Federation protocol for Web Browser federation. The protocol defines a subset of usage patterns for interoperability and the extensions defined are subsumed by the new WS-Federation specification.
18. Web Browser Federated Sign-On Protocol Extensions	Extends the base Web Browser Federation Sign-On Protocol to enable passing of SIDs and to allow marshalling of messages in limited buffer-size environments. This protocol uses HTTP forms and query strings and works with any Web browser.
B. Domain Services Interaction Server Protocols: Protocols used to enable member servers of Windows domains to securely provide pass-through authentication to Windows clients and servers seeking to access a service or application (such as a file server).	
1. Active Directory Technical Specification	Describes the functionality of Active Directory including the basic state model and the schema.
2. Authentication Protocol Domain Support	Specifies the profiles of multiple authentication protocols required to produce a conformant implementation of a domain controller and a domain-joined client or server machine.
3. BackupKey Remote Protocol	Provides methods for communicating master key backup information between the client computer and the domain controller (DC).
4. Kerberos Network Authentication Service (v5) Extensions	Extends the Kerberos V5 specification with support for interactive user logon.
5. Local Security Authority (Domain Policy) Remote Protocol	Provides access to the domain policy implementation of Local Security Authority (LSA), a protected subsystem of the Microsoft Windows 2000 and later operating systems that performs policy checking and name lookup on the DC.
6. Local Security Authority (Translation Methods) Remote Protocol	Provides access to the translation methods of Local Security Authority (LSA), a protected subsystem of Windows 2000 and later operating systems that performs policy checking and name lookup on the DC.
7. Netlogon Remote Protocol	Provides the complete set of remote procedure call (RPC) methods for Netlogon transactions between client members and DCs.
8. Privilege Attribute Certificate (PAC) Data Structure	Data structure for authorization information including group memberships, additional credential information, profile and policy information, and supporting security metadata.
9. Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol: Microsoft Extensions	Describes certain extensions to the RFC4556 standard.
10. Remote Certificate Mapping Protocol	Sends a remote request to map a client security certificate to an Active Directory account.
11. Security Account Manager (SAM) Remote Protocol (Client-to-Server)	Performs remote Service Account Manager (SAM) operations, such as user account management and manipulation.
12. Security Account Manager (SAM) Remote Protocol (Server-to-Server)	Provides the server-to-server implementation of the Security Account Manager Remote protocol.

Protocol	Description
13. Windows Client Certificate Services Protocol	Comprises the user client and administrative client interfaces implemented on a Microsoft Certificate Authority service.
C. Multi-Factor Authentication & Certificate Server Protocols: Protocols used to enable strong authentication methods and simplified public key infrastructure deployment to Windows clients and servers.	
1. Certificate Services Remote Administration Protocol	Consists of a set of DCOM interfaces that allow administrative tools to configure the state and policy of a Certificate Authority (CA) on a server.
2. Certificate Templates	Data structures that can be fetched via LDAP from a corporate database. They carry policy information that controls the behavior of a corporate certificate server.
3. Remote Certificate Mapping Protocol	Sends a remote request to map a client security certificate to an Active Directory account.
4. Windows Client Certificate Services Protocol	Comprises the user client and administrative client interfaces implemented on a Microsoft Certificate Authority service.
D. Group Policy Server Protocols: Protocols used to enable machine and user policy and configuration management to Windows clients and servers.	
1. Windows Group Policy Protocols	The Windows Group Policy protocols enable the management of configuration and other policies for all machines and users in a domain. By processing the policies at machine startup and user logon, pre-defined settings can be applied to security, software installation, scripts, folder redirection, and Microsoft Internet Explorer options.
E. Systems & Systems Health Management Server Protocols: Protocols used to enable centralized systems management and configuration for Windows clients and servers.	
1. Background Intelligent Transfer Service (BITS) Peer-Caching: Content Retrieval	Used to achieve load-balancing by allowing Windows systems to receive software packages from other clients in the same vicinity or subnet. Also ensures that machines are authenticated before they can receive a package from a peer.
2. Background Intelligent Transfer Service (BITS) Peer-Caching: Peer	Used to achieve load-balancing by allowing Windows systems to receive software packages from other clients in the same vicinity or subnet. Also ensures that machines are authenticated before they can receive a package from a peer.
3. Background Intelligent Transfer Service (BITS) Peer-Caching: Peer Discover	Used to achieve load-balancing by allowing Windows systems to receive software packages from other clients in the same vicinity or subnet. Also ensures that machines are authenticated before they can receive a package from a peer.
4. Directory Services Setup Remote Protocol	Includes an interface that retrieves DC information and performs limited administrative operations.
5. Disk Management Remote Protocol	Enables remote management of disks on a computer running Windows 2000, Microsoft Windows XP, or Microsoft Windows Server 2003.
6. InitShutdown Protocol	Used by Winlogon to remotely shut down a system.
7. Removable Storage Manager Remote Protocol	Allows client access to server resources and resource properties.
8. Server Service Remote Protocol	Allows client access to server resources and resource properties.

Protocol	Description
9. Service Control Manager Remote Protocol	Enables remote calls to Service Control Manager to administer services (start, stop, enumerate and set properties).
10. Task Scheduler Remoting Protocol	Provides methods to register and configure a task and to enquire about the status of running tasks on a remote machine.
11. Windows Management Instrumentation (WMI) Encoding Version 1.0 Protocol	Consists of the binary encoding for WMI objects (CIM objects defined by DMTF) used in the custom marshaling portion of the Windows Management Instrumentation Remoting protocol.
12. Windows Management Instrumentation (WMI) Remote Protocol	Extends the DMTF Common Information Model (CIM) to represent management objects in enterprise environments. Numerous interfaces provide methods to enable interaction and management capabilities between providers and clients.
13. WS-Management Protocol Extensions	Contains the Microsoft profile of WS-Management for Windows Server 2003 R2.
14. WS-Management Protocol Version 2.0 Extensions	Contains the Microsoft profile of WS-Management 1.0 included in Microsoft Windows Vista.
F. Directory & Global Catalog Replication Server Protocols: Protocols used between instances of Windows Active Directory domain controller servers to enable providing a single distributed directory and authentication service.	
1. Directory Replication Service (DRS) Remote Protocol	The Directory Replication Service (drsuapi) remote procedure call (RPC) protocol is a network protocol for performing housekeeping and management operations for Active Directory.
2. SMTP Replication Protocol Extensions	Provide the nonreplicated data formats needed to conduct Active Directory replication when using a Simple Mail Transport Protocol (SMTP) replication daemon hosted on a DC.
G. Kerberos Group Membership Protocols: Describes the structure of the Windows 2000-specific group membership authorization data carried in the field of a Kerberos ticket for use by servers in performing access control.	
1. Kerberos Network Authentication Service (v5) Extensions	Extends the Kerberos V5 specification with support for interactive user logon.
2. Kerberos Network Authentication Service (v5) Service for User (S4U) Extension	Provides mechanisms for an application service to obtain a Kerberos Service Ticket on behalf of a user, allowing the application to perform functions on behalf of the user.
3. Privilege Attribute Certificate (PAC) Data Structure	Data structure for authorization information including group memberships, additional credential information, profile and policy information, and supporting security metadata.
H. Windows Remote Registry Services: Protocol for monitoring and modifying registry information and remote system shutdown.	
1. Windows Remote Registry Protocol	Enables a client to modify registry information and to initiate and terminate a system shutdown from a remote source.
I. Windows Event Logging: Protocol for tracking of events that occur as part of a distributed application.	

Protocol	**Description**
1. Eventlog Remoting Protocol Version 1.0	Provides a way to track events that occur on computers functioning as part of a distributed application. It exposes methods for manipulating event logs and their associated data.
2. Eventlog Remoting Protocol Version 6.0	Provides a way to track events that occur on computers functioning as part of a distributed application. It exposes methods for manipulating event logs and their associated data.
J. Network Time Services: Protocols for managing time synchronization between multiple computers on a network.	
1. Network Time Protocol (NTP) Authentication Extensions	The Network Time Protocol (NTP) is used to synchronize computer clocks on the Internet (for more information, see RFC 1305 at www.ietf.org). Microsoft extensions enable digital packet signing.
2. W32Time Remote Protocol	Provides for a domain-time synchronization authority using the methods that define the W32Time interface. It provides a way to configure and read a time server.
K. Network Connection Management: Protocol for transport and configuration of the network redirector to manage network connections with other computers.	
1. Workstation Service Remote Protocol	Manages transport and configuration aspects for the network redirector. The WKSSVC interface provides methods for managing network connections with other computers.
L. MSDN Protocols	
See MSDN Website	
M. Remote Procedure Calls: Foundation protocols for use of Microsoft Remote Procedure Call (RPC) interfaces between computers on a network	
1. ExtendedError Remote Data Structure	Data structure that supports the passing of error information to client applications.
2. Remote Procedure Call Location Services Protocol Extensions	Used by client processes to discover specific RPC services on host systems.
3. Remote Procedure Call over HTTP	Enables RPC/HTTP clients to access and make remote calls to an RPC server. For example, a company could create a Web application that can receive customer information from an RPC server.
4. Remote Procedure Call Protocol Extensions	Establishes communication between the client and server using interprocess communication (IPC) mechanisms.
N. Network Access Protection Protocols: Protocols used to protect network from access by computers that do not meet system health and configuration requirements.	
1. Health Certificate Enrollment Protocol	Allows a network endpoint to obtain digital certificates that are conditionally issued based on the compliance of that endpoint to security policy defined for the network.
2. Network Access Protection Statement of Health	Defines the Statement of Health (SoH) and Statement of Health Response (SoHR) structures, which carry information relating to patch management, configuration for anti-virus products, firewall settings and similar security/system health measures.

Protocol	Description
3. Remote Access Dial-In User Service (RADIUS): Network Access Protection (NAP) Attributes	RADIUS Vendor Specific Attributes implemented in Windows to authenticate and authorize connection requests and configure the level of network access based on validation of system health and configuration requirements.
O. Windows Security Health Validator Protocols: Protocols used to make network quarantine decisions based on the client security health state and a defined network access policy.	
1. Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV)	Specifies the messaging between the WSHA and WSHV used to make network quarantine decisions based on the client security health state and a defined network access policy. .
P. Network Access Protection (NAP) Extensions for DHCP: Protocols used to protect network from access by computers that do not meet system health and configuration requirements.	
1. Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection	Defines the extensions to the DHCP protocol through which the client can convey its health state to the DHCP server, and for the server to convey the client's NAP state and health remediation information to the client.
Q. Rights Management Services: Protocols used to provide rights management services.	
1. Rights Management Services (RMS): Client-Server Protocol	Used by rights-management-aware applications to exchange documents with rights management protections.
2. Rights Management Services (RMS): Server-Server Protocol	Used by servers to discover URL's corresponding to specific RMS protocol endpoints.
III. Networking Transport Task Protocols	
1. Authenticated Internet Protocol	Provides Internet Key Exchange (IKE) based privacy and authentication services at the IP layer. It covers IKE for use with NAT-Traversal, 2048-bit MODP Diffie-Hellman encryption, fast failover, fragmentation support, denial-of-service, and UDP-ESP.
2. Distributed Component Object Model (DCOM) Remote Protocols	Enables a client object to call the methods of a remote COM object over a network. DCOM also monitors connection integrity between server objects and clients. It is designed for use across multiple network transport protocols, including Internet protocols such as HTTP.
3. Dynamic Host Configuration Protocol (DHCP) Extensions	Defines the Microsoft versions of the Classless Static Route (CSR) option, the option for Encoding Long Options, Disable NetBIOS option, Default Route Metric option, and the Release DHCP Lease on Shutdown option.
4. Extensible Authentication Protocol Method for Microsoft Challenge	Allows mutual authentication between an authenticator and a peer that is seeking authentication.
5. ICertPassage Remote Protocol	Provides an interface to the Certificate authority for submitting a PKCS #10 request and receiving a certificate in a PKCS #7 response.
6. Internet Key Exchange (IKE) Protocol Extensions	Extends the IETF IKE standard to support fragmentation of IKE messages, and support CGA (Crytographically Generated Address) certificates that communicate additional information about authenticated peers. The information can then be used in authorization decisions.

Protocol	Description
7. IPv4 over IEEE 1394 Protocol Extensions	Represents a Microsoft extension to the IEEE 1394 protocol that handles a special non-IPv4 packet.
8. Key Service Remote (IkeySvcR) Protocol	Allows administrators of a local machine to import public\private key pairs in PKCS #12 data structure format. It provides an IKeySvcR interface for installing Personal Information Exchange (PFX) BLOBs on the server.
9. Messenger Service Messaging Protocol	This protocol provides methods to send text messages to be displayed to the human operator of a remote computer. That operator is identified by a NETBIOS name. The protocol includes messages to maintain the NETBIOS names it uses.
10. Messenger Service Name Management Protocol	This protocol provides methods to send text messages to be displayed to the human operator of a remote computer. That operator is identified by a NETBIOS name. The protocol includes messages to maintain the NETBIOS names it uses.
11. Microsoft Protected Extensible Authentication Protocol (PEAP)	Allows protection of the Protected Extensible Authentication Protocol (PEAP).
12. Remote Data Services (RDS) Transport Protocol	Used for the transfer of tabular data between systems. It is especially suited for the flow of tabular data, in both directions, between client and server over the HTTP or DCOM protocols. It is used by ActiveX Data Object (ADO) methods.
13. Server-Side Include (SSI) 1.4 Protocol	Carries Passport authentication information during an exchange between the server and a client that is requesting access to a uniform resource locator (URL). Passport enables interaction between a Passport logon (PP-Login) server, a Passport Program Manager (PPM), and a Passport-aware client.
14. Teredo Extensions	Describes extensions to the Teredo protocol specified in RFC 4380 that allow the Teredo protocol to work behind symmetric NATs, and allow communicating peers to detect that they are behind the same NAT.
15. User Name Mapping (UNM) Protocol	Maps Windows domain user and group account names to POSIX user and group identifiers.
16. Windows Internet Naming Service (WINS) Replication and Autodiscovery Protocol	Provides a distributed database for registering and querying dynamic mappings of NetBIOS names for computers and groups used on the network.
17. Windows Server Update Services: Client-Server Protocol	Enables a computer running Microsoft Windows to communicate with the Windows Update service and the Microsoft Software Update Services (SUS) server component.
18. Windows Server Update Services: Server-Server Protocol	Enables a computer running Microsoft Windows to communicate with the Windows Update service and the Microsoft Software Update Services (SUS) server component.
One-time Flat Fee (Uniform Pricing) Protocols	
1. CIFS Browser Protocol	Enables interaction with the Browser service, which creates and maintains a view of resources available on a network.
2. Directory Services Setup Remote Protocol	Includes an interface that retrieves DC information and performs limited administrative operations.
3. Disk Management Remote Protocol	Enables remote management of disks on a computer running Windows 2000, Microsoft® Windows® XP, or Microsoft® Windows Server™ 2003.

Protocol	Description
4. Key Service Remote (IKeySvcR) Remote Protocol	Allows administrators of a local machine to import public\private key pairs in PKCS #12 data structure format. It provides an IKeySvcR interface for installing Personal Information Exchange (PFX) BLOBs on the server.
5. Extensible Authentication Protocol Method for Microsoft Challenge	Allows mutual authentication between an authenticator and a peer that is seeking authentication.
6. Network Time Protocol (NTP) Authentication Extensions	The Network Time Protocol (NTP) is used to synchronize computer clocks on the Internet (for more information, see RFC 1305 at www.ietf.org). Microsoft extensions enable digital packet signing.
7. Server Service Remote Protocol	Provides the ability to manage file and print serving resources, and responds to requests made by other computers for shared resources on the local computer.
8. SMTP Replication Protocol Extensions	Provide the nonreplicated data formats needed to conduct Active Directory replication when using a Simple Mail Transport Protocol (SMTP) replication daemon hosted on a DC.
9. User Name Mapping (UNM) Protocol	Maps Windows domain user and group account names to POSIX user and group identifiers.
10. W32Time Remote Protocol	Provides for a domain-time synchronization authority using the methods that define the W32Time interface. It provides a way to configure and read a time server.
11. Windows Management Instrumentation (WMI) Remote Protocol	Extends the DMTF Common Information Model (CIM) to represent management objects in enterprise environments. Numerous interfaces provide methods to enable interaction and management capabilities between providers and clients.
One-time Flat Fee (Variable Pricing) Protocols	
1. Microsoft Content Indexing Services Protocol	Provides methods of querying and managing Microsoft Content Indexing Services parameters using a named pipe.
2. Local Security Authority (Translation Methods) Remote Protocol	Provides access to the translation methods of Local Security Authority (LSA), a protected subsystem of Windows 2000 and later operating systems that performs policy checking and name lookup on the DC.
3. Security Account Manager Remote Protocol	Performs remote Service Account Manager (SAM) operations, such as user account management and manipulation.
4. Security Account Manager Remote Protocol (Server-to-Server)	Provides the server-to-server implementation of the Security Account Manager Remote protocol.
5. Workstation Service Remote Protocol	Manages transport and configuration aspects for the network redirector. The WKSSVC interface provides methods for managing network connections with other computers.
6. Messenger Service Messaging Protocol	This protocol provides methods to send text messages to be displayed to the human operator of a remote computer. That operator is identified by a NETBIOS name. The protocol includes messages to maintain the NETBIOS names it uses.
7. Messenger Service Name Management Remote Protocol	Provides methods to send text messages to be displayed to the human operator of a remote computer. That operator is identified by a NETBIOS name. The protocol includes messages to maintain the NETBIOS names it uses.

Protocol	Description
8. Distributed Component Object Model (DCOM) Remote Protocols	Enables a client object to call the methods of a remote COM object over a network. DCOM also monitors connection integrity between server objects and clients. It is designed for use across multiple network transport protocols, including Internet protocols such as HTTP.
9. Remote Data Services (RDS) Transport Protocol	Used for the transfer of tabular data between systems. It is especially suited for the flow of tabular data, in both directions, between client and server over the HTTP or DCOM protocols. It is used by ActiveX Data Object (ADO) methods.
10. Server Message Block (SMB) Version 1.0 Protocol	Allows client systems to request file and print services from server systems over a network.

APPENDIX 2
Protocol Technical Documentation Specifications

Please see specifications located at:: http://www.microsoft.com/about/legal/intellectualproperty/protocols/wspp/templatespecs.mspx

APPENDIX 3

Third Party IP Claims
(as of the Effective Date)

Microsoft has received a Third Party IP Claim (as defined in Section 3.3(c)(ii) of this Agreement) with respect to the protocols listed below. This notice does not constitute an admission by Microsoft that such Third Party IP Claim has any merit.

The following protocols are the subject of a Third Party IP Claim under the following patents: U.S. Patent Nos. 7,188,180, 6,502,135, and/or 6,839,759.

1. Peer Name Resolution Protocol (PNRP) Version 4.0
2. Group Policy: IP Security (IPSec) Protocol Extension
3. Remote Procedure Call (RPC) over HTTP Protocol

APPENDIX 4

European Union and United States Patents and Patent Applications for Workgroup Server Protocol Program Protocols

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
A. Base File Services Scenario				
1. Common Interface File System (CIFS) Browser Protocol				
2. Disk Management Remote Protocol				
3. Distributed Link Tracking: Central Manager Protocol	6,449,615			
4. Distributed Link Tracking: Central Store Protocol				
5. Distributed Link Tracking: Workstation Protocol				
6. Encrypting File System Remote Protocol		10/351,683		
7. FrontPage Server Extensions Remote Protocol				
8. Microsoft Content Indexing Services Protocol				
9. Remote Administration Protocol				
10. Remote Mailslot Protocol				
11. Removable Storage Manager (RSM) Remote Protocol				
12. Server Message Block (SMB) Version 1.0 Protocol	5,261,051	10/021,392 2006-0026165-A1	#0438571	Pub. #1619600
13. Server Service Remote Protocol				
14. Virtual Disk Service (VDS) Protocol				
15. Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions				
16. Web Distributed Authoring and Versioning (WebDAV) Protocol: Microsoft Extensions	6,557,040 6,581,099 6,658,476	2007-0050512-A1		
17. Web Distributed Authoring and Versioning (WebDAV) Protocol: Server Extensions	6,557,040 6,581,099 6,658,476	2007-0050512-A1		
18. Windows Search Protocol				

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
19. WS-Management Protocol Version 2.0 Extensions		2007-0118642-A1 2007-0192503-A1 2007-0192773-A1 2007-0192502-A1 2007-0192496 A1		
B. DFS (Distributed File Service) + FRS (File Replication Service) Scenario				
1. Distributed File System (DFS): Namespace Management Protocol				
2. Distributed File System (DFS): Namespace Referral Protocol	5,701,462 5,842,214	2006-0085428-A1	#0661652	Pub. #1643393
3. File Replication Service (FRS) Protocol	5,588,147 5,649,194	2006-0136484-A1		
C. Print RPC Scenario				
1. Enhanced Metafile (EMF) Format: Plus Extensions (EMF+)				
2. Enhanced Metafile (EMF) Spool Format				
3. Print System Asynchronous Notification Protocol				
4. Print System Asynchronous Remote Protocol				
5. Print System Remote Protocol	5,699,495 5,845,058	2004-0193678-A1 2005-0179936-A1		Pub. #1564635
D. Internet File and Print Scenario				
1. Web Point and Print Protocol	6,094,679			
E. Advanced File Services Scenario				
1. Common Interface File System (CIFS) Browser Protocol				
2. Disk Management Remote Protocol				
3. Distributed File System: Replication (DFS-R) Protocol				

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
4. Distributed File System: Replication Helper Protocol (DFS-R Helper)		2005-0015413-A1 2004-0186916-A1 2005-0235043-A1 2006-0047855-A1 2006-0085561-A1 2007-0268516-A1		Pub. #1587007 Pub. #1641219
5. Distributed Link Tracking: Central Manager Protocol	6,449,615			
6. Distributed Link Tracking: Central Store Protocol				
7. Distributed Link Tracking: Workstation Protocol				
8. Encrypting File System Remote Protocol		10/351,683		
9. FrontPage Server Extensions Remote Protocol				
10. Microsoft Content Indexing Services Protocol				
11. Peer Name Resolution Protocol (PNRP) Version 4.0		2006-0239197-A1 2006-0179139-A1 2007-0168512-A1 2005-0004916-A1		
12. Remote Administration Protocol				
13. Remote Differential Compression (RDC) Protocol				
14. Remote Mailslot Protocol				
15. Removable Storage Manager (RSM) Remote Protocol				
16. Server Message Block (SMB) Version 1.0 Protocol	5,261,051	10/021,392 2006-0026165-A1	#0438571	Pub. #1619600
17. Server Message Block (SMB) Version 2.0 Protocol		2006-0271697-A1 2006-0271692-A1		Ser. #05111885.9 Ser. #05111729.9
18. Server Service Remote Protocol				
19. Virtual Disk Service (VDS) Protocol				

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
20. Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions				
21. Web Distributed Authoring and Versioning (WebDAV) Protocol: Microsoft Extensions	6,557,040 6,581,099 6,658,476	2007-0050512-A1		
22. Web Distributed Authoring and Versioning (WebDAV) Protocol: Server Extensions	6,557,040 6,581,099 6,658,476	2007-0050512-A1		
23. Windows Search Protocol				
24. WS-Management Protocol Version 2.0 Extensions		2007-0118642-A1 2007-0192503-A1 2007-0192773-A1 2007-0192502-A1 2007-0192496 A1		
II. User & Group Administration Task				
A. Base Authentication and Authorization Scenario				
1. Authentication Protocol Domain Support	6,427,209			
2. BackupKey Remote Protocol	6,044,155			
3. Digest Access Authentication: Microsoft Extensions				
4. Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) Protocol Extension				
5. Kerberos Network Authentication Service (v5) Extensions	6,401,211 6,427,209			
6. Kerberos Network Authentication Service (v5) Service for User (S4U) Extension		2003-0018913-A1		Pub. #1271882 Pub. #1619856
7. Local Security Authority (Domain Policy) Remote Protocol				
8. Local Security Authority (Translation Methods) Remote Protocol				
9. Netlogon Remote Protocol				
10. NetLogon Remote Protocol: Challenge Handshake Authentication Protocol (CHAP)/EAP-MD5 SubAuthentication Extension	6,427,209			
11. NT LAN Manager (NTLM) Authentication Protocol	6,427,209			

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
12. NTLM Over HTTP Protocol				
13. Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol: Microsoft Extensions				
14. Security Account Manager (SAM) Remote Protocol (Client-to-Server)				
15. Security Account Manager (SAM) Remote Protocol (Server-to-Server)				
16. Simple and Protected Generic Security Service Application Program Interface Negotiation Mechanism (SPNEGO) Protocol Extensions				
17. Web Browser Federated Sign-On Protocol		2005-0223217-A1 2006-0112422-A1		
18. Web Browser Federated Sign-On Protocol Extensions		2005-0223217-A1 2006-0112422-A1		
B. Domain Services Interaction Scenario				
1. Active Directory Technical Specification				
2. Authentication Protocol Domain Support	6,427,209			
3. BackupKey Remote Protocol	6,044,155			
4. Kerberos Network Authentication Service (v5) Extensions	6,401,211 6,427,209			
5. Local Security Authority (Domain Policy) Remote Protocol				
6. Local Security Authority (Translation Methods) Remote Protocol				
7. Netlogon Remote Protocol				
8. Privilege Attribute Certificate (PAC) Data Structure	6,427,209			
9. Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol				
10. Remote Certificate Mapping Protocol	6,427,209			
11. Security Account Manager (SAM) Remote Protocol (Client-to-Server)				
12. Security Account Manager (SAM) Remote Protocol (Server-to-Server)				
13. Windows Client Certificate Enrollment Protocol				

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
C. Multi-Factor Authentication & Certificate Services Scenario				
1. Certificate Services Remote Administration Protocol				
2. Certificate Templates				
3. Remote Certificate Mapping Protocol	6,427,209			
4. Windows Client Certificate Enrollment Protocol				
D. Group Policy Scenario				
1. Group Policy: Folder Redirection Protocol Extension				
2. Group Policy: Core Protocol	6,389,589 6,950,818			
3. Group Policy: Deployed Printer Connections Extension				
4. Group Policy: Host Security Configuration				
5. Group Policy: Internet Explorer Maintenance Extension				
6. Group Policy: IP Security (IPSec) Protocol Extension				
7. Group Policy: Preferences Extension				
8. Group Policy: Registry Extension Encoding				
9. Group Policy: Scripts Extension Encoding				
10. Group Policy: Software Installation Protocol Extension				
11. Group Policy: Wireless/Wired Protocol Extension				
E. Systems and Systems Health Management Scenario				
1. Background Intelligent Transfer Service (BITS) Peer-Caching: Content Retrieval				
2. Background Intelligent Transfer Service (BITS) Peer-Caching: Peer				
3. Background Intelligent Transfer Service (BITS) Peer-Caching: Peer Discovery				
4. Directory Services Setup Remote Protocol				
5. Disk Management Remote Protocol				
6. InitShutdown Protocol				
7. Removable Storage Manager (RSM) Remote Protocol				

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
8. Server Service Remote Protocol				
9. Service Control Manager Remote Protocol				
10. Task Scheduler Remoting Protocol				
11. Windows Management Instrumentation Encoding Version 1.0 Protocol				
12. Windows Management Instrumentation Remote Protocol				
13. WS-Management Protocol Extensions		2007-0118642-A1 2007-0192503-A1 2007-0192773-A1 2007-0192502-A1 2007-0192496 A1		
14. WS-Management Version 2.0 Protocol Extensions		2007-0118642-A1 2007-0192503-A1 2007-0192773-A1 2007-0192502-A1 2007-0192496 A1		
F. Directory & Global Catalog Replication Scenario				
1. Directory Replication Service (DRS) Remote Protocol	5,768,519 5,832,225 5,968,121 6,324,571 6,446,077 6,457,053 6,643,670 6,879,564	10/029,426 2006-0168120-A1 2006-0184589-A1 2006-0200831-A1	#1004193	
2. SMTP Replication Protocol Extensions				
G. Kerberos Group Membership Scenario				
1. Kerberos Network Authentication Service (v5) Extensions	6,401,211 6,427,209			
2. Kerberos Network Authentication Service (v5) Service for User (S4U) Extension		2003-0018913-A1		Pub. #1271882 Pub. #1619856
3. Privilege Attribute Certificate (PAC) Data Structure	6,427,209			

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
H. Windows Remote Registry Services				
1. Windows Remote Registry Protocol		09/665,214 2005-0114300-A1		
I. Windows Event Logging Scenario				
1. Eventlog Remoting Protocol Version 1.0	6,931,405			Pub. #1355232
2. Eventlog Remoting Protocol Version 6.0				
J. Network Time Services				
1. Network Time Protocol (NTP) Authentication Extensions				
2. W32Time Remote Protocol				
K. Network Connection Management				
1. Workstation Service Remote Protocol (WKSSVC)				
L. Remote Procedure Calls (RPC) Scenario				
1. ExtendedError Remote Data Structure				
2. Remote Procedure Call Location Services Protocol Extensions	6,202,089			
3. Remote Procedure Call Over HTTP Protocol		2003-0225889-A1		
4. Remote Procedure Call Protocol Extensions				
M. Network Access Protection (NAP) Scenario				
1. Health Certificate Enrollment Protocol		2005-0267954-A1 2007-0100850-A1 2007-0143392-A1 11/395,559		Pub. #1648137
2. Network Access Protection Statement of Health				
3. Remote Access Dial In User Service (RADIUS): Network Access Protection (NAP) Attributes				
N. Windows Security Health Validator				
1. Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol		2007-0143392-A1		
O. Network Access Protection (NAP) Extensions for DHCP				

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
1. Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP)		2005-0267954 A1		
P. Rights Management Services				
1. Rights Management Server (RMS): Client-Server Protocol		2004-0158709-A1		
2. Rights Management Server (RMS): Server-Server Protocol		2004-0168061-A1 2004-0158709-A1		
III. Networking Transport				
1. Authenticated Internet Protocol				
2. Distributed Component Object Model (DCOM) Remote Protocols	5,724,588 5,881,230 6,208,952 6,820,267		#0669020	
3. Dynamic Host Configuration Protocol (DHCP) Extensions				
4. Extensible Authentication Protocol Method for Microsoft Challenge				
5. ICertPassage Remote Protocol				
6. Internet Key Exchange (IKE) Protocol Extensions		2003-0142823-A1 2005-0108531-A1		Pub. #1333635
7. IPv4 over IEEE 1394 Protocol Extensions				
8. Key Service Remote (IkeySvcR) Protocol				
9. Messenger Service Messaging Protocol				
10. Messenger Service Name Management Protocol				
11. Microsoft Protected Extensible Authentication Protocol (PEAP)		2003-0226017-A1 2007-0101409-A1		
12. OLE Automation Protocol				
13. Remote Data Services (RDS) Transport Protocol	5,974,416			
14. Server-Side Include (SSI) 1.4 Protocol		10/099,403		

Protocol Name	United States		European Union	
	Patents	Applications	Patents	Applications
I. File/Print Task				
15. Teredo Extensions		11/731,337 11/724,495 11/786,989 2006-0182100-A1		
16. User Name Mapping (UNM) Protocol				
17. Windows Internet Naming Service (WINS) Replication and Autodiscovery Protocol				
18. Windows Server Update Services: Client-Server Protocol		2005-0132348-A1 2005-0132349-A1		Pub. #1579301 App. # 04757283.9
19. Windows Server Update Services: Server-Server Protocol				