Comp C-3/37792

Microsoft, Implementation of Commission Decision

Response of Sun Microsystems, Inc. to Commission Art. 18 Request Dated 5 September 2005

Non-Confidential Version

Jeffrey S. Kingston
Morgan, Lewis & Bockius
One Market Plaza
San Francisco, Ca. 94105

1. Please describe in detail how the evaluation took place on-site, and in particular what kind of facilities Microsoft provided and what kind of security measures Microsoft put in place.

Response 1.

The evaluation took place over three days, Aug 29-31, in Redmond, Washington in a Microsoft building. Sun conducted the evaluation with three of its engineers.

Difficulties were encountered obtaining access to all of the evaluation documents. On arrival the first morning, Sun found that the documentation only included protocols within the User and Group Administration ("UGA") category. Microsoft initially took the position that Sun had only requested these materials and not the remainder, based upon communications between the companies wherein Sun had expressed particular interest in Active Directory. Sun had understood these communications differently, and had not anticipated that their focus on Active Directory would be construed as Sun's intention of having its access restricted to only a subset of the WSPP protocols. Once these differing understandings were sorted through, MS did make a version of the omitted materials available to the Sun engineers late in the afternoon on the first day. This version was dated 2004. Later the following day, Microsoft provided another version of the initially missing materials dated July 2005. Sun's ability to review the materials effectively was compromised by both the initial absence of the non-UGA materials and by the provision of what were obsolete and in many cases incomplete 2004 materials. As a result, Sun's review of what it would infer to be the current version of the non-UGA materials was but a single day in length.

There were several security issues which arose. Microsoft initially objected to the Sun employees carrying in a copy of the Annexes to the WSPP protocol agreement directly copied from Microsoft's web site. Those pages contained some brief notations on them. After the first day, Microsoft prohibited those pages from being used in the room. In addition, Microsoft objected to Sun employees using their own blank pads of paper for taking notes, requiring instead that the employees use a few blank pieces of paper which Microsoft offered. After discussion, Microsoft permitted the Sun employees to carry in a note pad on the first day. However, after the first day, Microsoft required that Sun use only paper supplied by Microsoft.

The Sun employees were obliged to remain in the company of a single Microsoft security guard for the entire time that they were inside the Microsoft building. If at any time a Sun employee needed to leave the room in which the evaluation materials were made available, all Sun employees were required to leave the room with him, attended by the Microsoft guard. The guard was within listening distance at all times during the

evaluation process, preventing private conversation among the Sun employees. In addition, Sun employees were not permitted to make any phone calls while in the protocol inspection area.

The materials were presented on three computers, all located in a single room. The protocols were displayed on Windows terminals. Although Sun was not able to determine the model and configuration of the computer upon which the protocol file were installed, when multiple demands were placed upon the system, performance noticeably degraded. One of the computer terminals froze during the course of review. Although Microsoft was called, more than an hour elapsed during which time the computer could not be used.

Evidently for security reasons, the computers were not connected to the internet. Thus, outside reference sources could not be checked during the course of review. Further, although certain links in the documentation to outside sources were included, those links were not operable because of the absence of an outside connection. Inoperable links included those to MSDN. Even though access was provided to a non-internet version of MSDN, many links in the documentation were only to the internet version, and, hence, were not operable.

2. Do you consider that the Technical Documentation examined by Sun provides complete and accurate specifications (see Article 1(1) of the Decision) for the protocols covered by the Decision? Please substantiate your answer.

Response 2

No.

The shortcomings of the documentation can be seen as falling into two general categories: 1. general matters common to the protocols as a group and 2. Specific items related to one or more individual protocols.

General matters. As a general matter, the documentation was not provided in a form conceived to facilitate use for the creation of implementations envisioned by the Decision. The documentation consisted of a large collection of protocol disclosures, which in themselves were individually incomplete, and lacked sufficient overall description tying or associating the operation and interrelationship of groups of protocols together for the provision of particular features or functions of workgroup servers as required by the Decision. In addition, the disclosure concerning the protocols themselves generally shared the following shortcomings.

1. Microsoft has disclosed certain information concerning protocols which are used at a connection between operating systems, but has generally excluded information concerning behaviors and dependencies which lie behind the connection or which determine what information goes out over a connection, when, why, and with what

impact upon other elements of the system. Such behaviors and dependencies must be disclosed in order for interoperability to be achieved. Implementation is effectively prevented by these omissions.

2. The protocols lacked basic descriptions of their construction and theory of operation. It is a matter of general protocol documentation practice that a detailed description of the protocol and its theory of operation is provided. As well, a description of the behaviors of the protocol under all of the conditions of operation as well as all of its inter-dependencies is furnished. Microsoft did not follow industry practice in that it omitted this critical information. It is extremely difficult and in many cases practically impossible to understand detailed documentation of a specification without this explanatory material.

3. It was common for the protocol documentation to assume knowledge and information located in other Microsoft disclosures made outside of WSPP. This other Microsoft disclosed information was not, however, explicitly set forth in WSPP or referred to in the documentation. Such information would need to be known and used in conjunction with the WSPP documentation. As a result, the protocols could not be implemented from information on the face of the documentation as provided. In Sun's view the protocol documentation should be complete within its four corners and neither assume nor require additional Microsoft information residing elsewhere.

4. The documentation in many cases contained express references to non-Microsoft outside sources but did not include those sources within the materials. This impeded the review process and would make implementation more difficult and time consuming.

5. The protocols commonly lacked a complete revision history and commonly lacked detailed information concerning changes between revisions. As well, the materials often lacked information mapping particular protocol revisions, features and elements to particular versions of Microsoft operating systems.

6. There was no indication that Microsoft was providing test suites or other aids to verify that an implementation was complete and accurate. An inability to test effectively is a substantial barrier to creating a commercial implementation.

7. In general, Vista protocols were missing from the documentation. Vista is now in widespread beta release.

Specific Protocols:

1. Active Directory Technical Specification.

   a. Active Directory Technical Specification. Although the materials referred to an "Active Directory Technical Specification", all that was provided was a circular

reference back to itself. No evidence was found of a technical specification as such.

In order to permit an implementation of an Active Directory Domain Controller, Microsoft should have provided a detailed specification of the full functionality of Active Directory including all of its functions, features and externally visible behaviors and dependencies.

b. DRSUAPI – is a network protocol that is used for housekeeping and management operations of the Active Directory on a Domain Controller. There were many shortcomings in its documentation, including the following:

This API uses MS RPC 4.0 and dynamically assigned endpoints as described in the "networking and Directory Services Network Communications Message Queuing" document that was not provided. It should also be noted that in several locations, Microsoft RPC 5.0 was also mentioned and used but not documented.

According to the documents, directory replicas are based on versions; V1, V2 etc. There was no express indication as to the relationship of these versions to versions of AD.

The description in the disclosure indicated that KDCs (Key Distribution Centers) of AD can route replica trafficaround domain controllers that appear to be offline. However, no documentation was provided concerning how this occurs.

The Directory Services (DRSUAPI) protocol uses a set of RPC based operations (24 RPC op numbers were disclosed) that run over and can be utilized over any of the following transports:

1. SMB
2. Windows Sockets
3. HTTP
4. Microsoft Message Queue (MSMQ)
5. SPX

With the exception of SMB, the documentation did not set forth how DRSUAPI uses these transports. Further none of the transports other than SMB were themselves documented. The DRSUAPI documentation described its IDL/RPC interface. It included a one or two line description of each function, and structure definitions of the parameters passed to and received from each function. Each structure definition listed the type of each of its fields, as well as a line of text that described its meaning. The documentation does not describe either the kind of service that would use the various functions or the sequence in which the functions should be called.

The interface documentation included references to such functions as "ReplicaAdd", "ReplicaModify", and "ReplicaRemove". Complete descriptions of these functions were not provided. Nor was information concerning their use, sequence, or other important implementation parameters disclosed.

The documentation referred to an Active Directory service called Knowledge Consistency Checker (KCC). The KCC was essentially undocumented. Sun's information concerning the KCC was obtained from MSDN; this information was not set out in the Evaluation documentation. MSDN describes the administrative tasks performed by the KCC. As very generally described in MSDN, the function of the KCC is to create an efficient replication topology based upon the speed and reliability of the network links between AD sites. The Evaluation documentation includes a few references to the KCC which state that it creates and maintains this topology, but does not describe the KCC algorithms or the DRS calls that it uses. There are DRS functions that return information about domain controllers that might be used by the KCC to create an optimal replication topology. The documentation did mention that a spanning tree algorithm (spanning tree algorithms are generally in the public domain as IEEE standards) is used by the KCC to select routings but did not specify which algorithm is used or how it is used. Essentially all of the particulars of this complex series of operations need to be disclosed in order to implement an interoperable workgroup server and the missing particulars effectively prevent implementation.

AD includes Global Catalog functionality. The documentation contained many references to the Global Catalog but did not set forth an adequate specification of it.

Additional specific deficiencies in DRS documentation include:

- The SMTP messages used for replication are not sufficiently described.
- The compression algorithm "Xpress" is not defined.
- The "DRSBind" function passes a client's DRS_EXTENSIONS parameter, which specifies a system's capabilities such as "compression" and "async". The documentation for DRSBind includes the confusing statement that "only clients that are not domain controllers will make these calls, meaning that the client extensions should be 0".
- SMTP Replication Protocol Extensions

    1. These appear to be based on extensions to the SMTP protocol (IETF RFCs 821 and 2821). No documentation was provided that describes this protocol or its data types. All we know is that it can compress the payload using MS Zip or a third party compression called "Xpress". The DRS documentation includes a reference to a configuration parameter DRS_COMP_ALG_XPRESS, which

implies that the compression algorithm is something, called "Xpress", but does not describe it further.

2. Uses a certificate and private key pair as well as MSZIP to compress the payload.

c. Active Directory Schema

The schema documentation mentions scores of data entry types where the meanings, usages and dependencies are not set forth. Additionally the schema documentation warns that it is "preliminary and subject to change without notice".

2. Advanced Encryption Standard ("AES"). AES is generally in the public domain. No documentation in the Evaluation materials was provided setting forth how Microsoft uses it or whether it has been extended.

3. Passport. The certificate structure is not described.

4. Internet Protocol Security Protocol ("IPSEC"). The documentation noted that the "documentation is subject to change without notice". There were several indications within the documentation that items were for "Internal Use Only" but no information provided concerning the meaning and implications of the statement. Microsoft uses extensions to IETF RFCs; the extensions are not fully described. In addition to not describing fully the changes which Microsoft has made to IPSEC, the documentation omitted to set forth what the changes are for, how they are used and under what conditions they are used. Further, the new parameters are not defined.

5. Net Logon Remote Protocol. This protocol supports the Digest protocol but this was not described. [].

6. Kerberos Interactive Logon Protocol Extensions. Microsoft employs public domain Kerberos, but extends it by including additional data—termed PAC—in fields which the standard version labels as reserved. The documentation concerning the previously undisclosed organization of the PAC data fields has been provided. Even though the organization of the fields is now disclosed, the documentation does not disclose how to formulate or consume the entries in those fields.

7. Microsoft RPC Protocol. There is a general problem with the RPC documentation. RPC can communicate over SMB or TCP/IP. If SMB is used, then Windows identifies RPC endpoints to be used in conjunction with "Named Pipes" and Mailslots. Neither the Named Pipes nor Mailslots were defined in the materials. Also,the materials did not contain the definitions of the RPC endpoints to support them.

8. DFS. Documentation was provided for the NT 4 version of DFS. It should be noted that Microsoft made an earlier disclosure of this now-obsolete version of DFS after the Samba group announced that it had succeeded in reverse engineering it. The current

version of DFS, used by Windows 2000 and above, called the domain version, was incompletely documented. [ ]

9. File Replication Service ("FRS"). The FRS documentation describes "frsapi" and "frsrpc" interfaces. With respect to the frsapi, 11 APIs are described, 4 of which are labeled as obsolete and not adequately disclosed. There is no indication concerning how or if they have been replaced. Moreover, it is necessary that even obsolete replaced APIs must be disclosed for backward compatibility reasons. An older version of an operating system in the network may make these calls, which must be understood. A similar problem existed with respect to the disclosure of the frsrpc apis. In addition, two fields of the frsrpc, "datablob" and "command id," were not defined. Finally there was no description of the AD objects or Registry keys which are used to store FRS configuration data.

10. Windows Update Service. The protocol itself was defined. However the disclosure does not enable implementation. This is because the Update Service requires an Active X control be downloaded and installed in order to instrument the protocol. The information required for this was not provided. In order to run an Active X control the application environment must be supplied.

11. SMB. [].

12. SMB 2. This protocol was not listed in attachments to the WSPP license agreements. It was included, however, in the documentation which was provided to Sun on the second day. There was little description accompanying it except for brief statements that it represents an improvement over SMB in certain enumerated respects and that it is streamlined. The documentation did not describe what the protocol is or how it is used. []

13. Several protocols listed in the WSPP licenses were missing altogether: WS Federated and Windows Management Interactive Protocol.

14. Also missing were items not listed in the WSPP documentation, which Sun considers to be necessary for inclusion in work group servers. These include DLT, MS LDAP, Win32, COM/COM+, .Net Framework, MSMQ Protocol, Extensions to SMTP, Windows Media Streaming Media Protocol, Constrained or Delegated authority protocol, Passport Certificate Structure and DIME.

3. **After scrutiny of the Technical Documentation do you consider that the royalty levels proposed by Microsoft and set out in the Royalty Table annexed to the WSPP Agreements are in conformity with WSPP Pricing Principles, which are also annexed to the WSPP Agreements, in as far as they:**

i. enable implementation of the protocols by a licensee in a commercially practical manner; and

ii. reflect value conferred upon a license 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?

Response 3

A 3 day evaluation process does not allow for a comprehensive evaluation of whether Microsoft has properly applied the pricing principles set forth in the WSPP materials. Sun in the time allocated was not able to review all of the protocols from this perspective. Instead, it concentrated its review upon those protocols labeled "gold" and many of those labeled "silver".

It should be noted that Microsoft did not supply detailed information concerning the factual bases for its royalty claims. In Sun's view, one of the principal reasons for the evaluation is to learn whether any royalty demand can be economically justified. A key component to that analysis is the basis which Microsoft asserts for royalty. According to the royalty principles set forth in the WSPP, Microsoft cannot charge for access, but only innovations which go beyond access by providing improvements over systems known to the industry which provide similar functionality. For every royalty bearing protocol, Microsoft should specify its claims for improvement setting out the specifics of where it has advanced beyond other systems known to it in the industry.

In addition, all relevant intellectual property claims that form a part of the basis for a royalty claim should be disclosed. All Microsoft has done in the WSPP materials is state whether it considers that it has US or European patents relating to a protocol. It does not set out the patent numbers. It should be noted however that it is Sun's interpretation of the pricing agreement that Microsoft has made that the mere existence of intellectual property alone cannot be the justification for royalty. To the extent that the grant of an intellectual property right only relates to access to interoperability with Microsoft products and does not enable a technical improvement beyond what similar systems in the industry provide, a license to that intellectual property right from Microsoft should not be royalty bearing.

Sun also notes that it has previously supplied the Commission with detailed analyses of 5 Microsoft European patents, which Microsoft disclosed to the Commission in earlier filings. It seems to be a reasonable assumption that these are the patents which Microsoft mentions (without identifying patent numbers) in the WSPP documentation. Sun's previous analyses showed that the patents themselves were unlikely to be infringed by an implementation of a work group server and that the inventions taught in the patents did not represent meaningful improvements over other techniques for accomplishing the same functions known in the industry.

Because of the limitations of the Evaluation review process the views expressed below are preliminary.

Gold Protocol: DRSUAPI/SMTP. SMTP is a well known public domain standard transport protocol which Microsoft uses for directory replication over low bandwidth connections. Use of SMTP does not represent any form of innovation by Microsoft. Microsoft couples use of SMTP with compression. Microsoft disclosed two compression systems which it uses: i) MS Zip and ii) Xpress. Neither compression system is unique to Microsoft. Zip is a public domain compression system. Although as noted above, Xpress is not fully defined in the documentation, it appears to be a reference to compression software which is publicly available under license from a company named Intelligent Compression Technology.

The DRSUAPI documentation consisted of a description of 24 RPC functions. The functions provided by these RPC calls are all well known in the industry and provision of this type of functionality in directory software does not represent a unique innovation by Microsoft. The functionalities supported by the calls include: Binding and Unbinding, Replicating, Get/Receive Updates, Add/Delete Replicas, Get Memberships, Add/Delete Directory Servers from the replica, test for Cost of routes etc. Sun was not able to identify a call which provided functionality dissimilar from the functions and features of other directory products known to and available in the industry. As a result, there is no innovative value associated with the disclosure of these RPCs. Disclosure simply provides access to interoperability with Microsoft.

Gold Protocol: DFS. Distributed file systems are not unique to Microsoft. For example the UNIX file system, NFS, is a distributed file system. Indeed, the pioneering work to develop distributed file systems was done by Carnegie Mellon University in their creation of the Andrew File System. Sun did not identify any substantial feature improvements in Microsoft's version of DFS which distinguishes it from the range of features found in other distributed file systems. What is disclosed by Microsoft in the WSPP documentation is an API which creates attributes in AD describing the topology of the distributed files. This is pure access to interoperability with the Microsoft system.

Silver Protocol FRS: What is disclosed in the FRS protocol documentation is the FRS API. File replication, itself, is common to virtually all operating systems. The FRS API is an RPC interface for managing certain aspects of the file replication process. It is used to identify the destination server, obtain parameters from AD, and force an immediate replication between two servers. None of these features of the API are unique to Microsoft. Other file replication systems include features which are substantially similar. What is disclosed are the particular ways these features are called in the Microsoft system, which is pure access to interoperability with the Microsoft system.

There is one additional element described in the documentation which is described as "activating/de-activating between replica sets". The documentation did not adequately describe what this function is for Sun to comment upon it.

Silver Protocol Group Policy: The information disclosed in connection with this protocol consists of the data structures which are employed in the Microsoft system. Group policy systems are not unique to Microsoft; the UNIX operating system and many others provide this functionality. By providing data structure information Microsoft provides only access to interoperability with the Microsoft system.

Silver Protocol Multi-Factor Authentication Certificate Services: There are a total of 4 protocols which are licensed in this silver protocol group. However, two of the protocols, Remote Certificate Map and Windows Client Certificate Services Protocol are licensed elsewhere in WSPP as "bronze protocols". It is reasonable to infer that the two protocols which are not listed as bronze are the two which Microsoft relies upon in setting the silver classification. These are ICert Passage Remote and IKey SvcR Remote Protocol.

ICert Passage Remote is used to read a certificate over the network. The protocol itself simply makes the request to AD to obtain the certificate. This is a pure access/interoperability protocol as it merely provides the proper means to make the request so that AD will understand it.

IKey SvcR Remote Protocol is used as part of the transmission of public key/private key pairs on the network. Under the Microsoft system, a client is able to send such key pairs to AD. The protocol merely provides format for this communication to take place. It, thus, is a pure access/interoperability protocol.

The first "bronze" protocol in this group is Remote Certificate Map. This protocol simply allows for the mapping of a certificate to a user account in AD. Once that is done a user may use a smart card containing a certificate to be authenticated to his or her account. This functionality is well known to the industry and is provided, for example, by Sun's Java card technology. The protocol disclosure provides access/interoperability only.

Sun did not have sufficient time to review the other bronze protocol of the group.