[MS-HGRP]:
HomeGroup Protocol Specification

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Copyright © 2011 Microsoft Corporation.

Revision Summary

Date	Revision History	Revision Class	Comments
03/12/2010	1.0	Major	First Release.
04/23/2010	1.0.1	Editorial	Revised and edited the technical content.
06/04/2010	2.0	Major	Updated and revised the technical content.
07/16/2010	3.0	Major	Significantly changed the technical content.
08/27/2010	4.0	Major	Significantly changed the technical content.
10/08/2010	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	5.0	Major	Significantly changed the technical content.
01/07/2011	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	5.0	No change	No changes to the meaning, language, or formatting of the technical content.

Copyright © 2011 Microsoft Corporation.

Contents

Copyright © 2011 Microsoft Corporation.

Copyright © 2011 Microsoft Corporation.

1 Introduction

This document specifies the HomeGroup Protocol, which is used to create a trust relationship that facilitates the advertising and publishing of content between machines via a peer-to-peer (P2P) infrastructure.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

Advanced Encryption Standard (AES)
globally unique identifier (GUID)
Internet Protocol version 6 (IPv6)
little-endian
network access server (NAS)
salt
service set identifier (SSID)

The following terms are specific to this document:

homegroup: A group of one or more computers that are **AES** joined together through the HomeGroup Protocol and which are able to share resources (files, printers, and so on) with each other.

MAC address: An address provided by the network interface vendor to uniquely identify the device on the network, as specified in [IEEE802.3].

peer-to-peer (P2P): An Internet-based networking option in which two or more computers connect directly to each other in order to communicate.

PeerGroup: A group of one or more machines connected through the [MS-PPSEC] protocol.

Rivest-Shamir-Adleman (RSA): A system for public key cryptography. **RSA** is specified in [PKCS1] and [RFC3447].

SHA-256 hash: The value computed from the hashing function described in [FIPS180-3].

Web services on devices (WSD): Web Services on Devices. A function discovery protocol used to communicate certain **HomeGroup** messages, notably the HomeGroup Invitation (section 2.2.1.1) and the Shared Printer (section 2.2.1.2). This is specified in [DPWS].

wireless access point (WAP): A wireless **network access server (NAS)** implementing 802.11.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We

Copyright © 2011 Microsoft Corporation.

will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[DPWS] Chans, S., Conti, D., Schlimmer, J., et al., "Devices Profile for Web Services", February 2006, http://specs.xmlsoap.org/ws/2006/02/devprof/devicesprofile.pdf

[FIPS180-3] Federal Information Processing Standards Publication, "Secure Hash Standard (SHS)", FIPS PUB 180-3, October 2008, http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

[FIPS186] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 186-3: Digital Signature Standard (DSS)", June 2009, http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

[FIPS197] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES)", November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[IEEE802.3] Institute of Electrical and Electronics Engineers, "Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Description", IEEE Std 802.3, 2002, http://standards.ieee.org/getieee802/download/802.3-2002.pdf

[MS-DTYP] Microsoft Corporation, "Windows Data Types", January 2007.

[MS-FSCC] Microsoft Corporation, "File System Control Codes", July 2006.

[MS-PPGRH] Microsoft Corporation, "Peer-to-Peer Graphing Protocol Specification", March 2010.

[MS-PPSEC] Microsoft Corporation, "Peer-to-Peer Grouping Security Protocol Specification", March 2010.

[MS-RPRN] Microsoft Corporation, "Print System Remote Protocol Specification", July 2006.

[PKCS1] RSA Laboratories, "PKCS #1: RSA Cryptography Standard", PKCS #1, Version 2.1, June 2002, http://www.rsa.com/rsalabs/node.asp?id=2125

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[RFC3447] Jonsson, J., and Kaliski, B., "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003, http://www.ietf.org/rfc/rfc3447.txt

[RFC3513] Hinden, R., and Deering, S., "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003, http://www.ietf.org/rfc/rfc3513.txt

[RFC3548] Josefsson, S., Ed., "The Base16, Base32, and Base64 Data Encodings", RFC 3548, July 2003, http://www.ietf.org/rfc/rfc3548.txt

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006, http://www.ietf.org/rfc/rfc4648.txt

[SP800-38A] National Institute of Standards and Technology. "Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques", December 2001, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

Copyright © 2011 Microsoft Corporation.

1.2.2 Informative References

[HomeGroupOvw] Microsoft Corporation, "HomeGroup Overview", October 2009, http://www.microsoft.com/downloads/details.aspx?familyid=7977F4FD-82B1-413D-8963-71A50E3030A4&displaylang=en

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

1.3 Overview

The HomeGroup Protocol is used to create a trust relationship that facilitates the advertising and publishing of content between machines via a **peer-to-peer** infrastructure.<1> This relationship is achieved with the use of **Web services on devices (WSD)** and a **PeerGroup** infrastructure. There is no client-server relationship in this protocol; in order to participate in **homegroup**, all machines implement the protocol in the same manner.

1.3.1 Role of Web Services on Devices (WSD)

WSD is used to publish messages that are discoverable to all machines on the subnet. These messages include the HomeGroup Invitation (section 2.2.1.1) and Shared Printer (section 2.2.1.2) messages.

1.3.2 Role of the PeerGroup

The PeerGroup is used as a secure line of communication between homegroup members.

1.3.3 High Level Homegroup Events

1.3.3.1 Creating a Homegroup

A machine that attempts to create a homegroup accomplishes this by first creating a PeerGroup, which is the secure peer-to-peer connection through which the homegroup is synchronized, as outlined in [MS-PPSEC]. This homegroup machine sets the homegroup password, which is used to secure the homegroup. Once the PeerGroup has been created, this first machine publishes an invitation to the homegroup via WSD, which allows new machines on the subnet to discover the homegroup.

1.3.3.2 Discovering and Joining the Homegroup

A machine detects that there is a homegroup on the subnet by receiving a HomeGroup Invitation message (section 2.2.1.1) over WSD. With the invitation and the correct homegroup password, the machine is able to join the PeerGroup, and by extension, the homegroup.

1.4 Relationship to Other Protocols

This protocol depends on [DPWS] to enable the discovery of a homegroup on the subnet, and [MS-PPSEC] to create a PeerGroup for communication between members of the homegroup. These two protocols are used independently of each other; that is, neither protocol sits above the other in the relationship hierarchy.

This protocol also requires that all machines implement the **Internet protocol version 6 (IPv6)** protocol.

Copyright © 2011 Microsoft Corporation.

1.5 Prerequisites/Preconditions

The prerequisites for this protocol include those for the WSD, as described in [DPWS], and PeerGroup, as described in [MS-PPSEC].

In addition, this protocol requires the following:

- The underlying PeerGroup is restricted to machines on the same subnet.
- All members of the homegroup are required to have an IPv6 address and to be able to support the cryptography technology defined in section 3.1.4.5.

1.6 Applicability Statement

The HomeGroup Protocol specifies a protocol for the creation of a trust relationship that facilitates the advertisement and publishing of content between machines on the same subnet.

1.7 Versioning and Capability Negotiation

This document describes version 1 of this protocol, therefore there are no issues with capability negotiation. This protocol does provide versioning capability within the HomeGroup Record message (section 2.2.2.2) in both the <SOURCEOS> and <VERSION> elements.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

Copyright © 2011 Microsoft Corporation.

2 Messages

2.1 Transport

Transport for this protocol is achieved through two channels: the PeerGroup and WSD, both of which are independent of the other. WSD is used to publish messages that are available to all machines on the subnet. The PeerGroup is used for sending secure communication between members of the homegroup.

2.2 Message Syntax

All messages are generated in XML format. The following sections use the terminology *sections*, *keys*, and *values* to specify concrete syntax for each message. This specification uses globally unique identifiers (**GUIDs**), as specified in [MS-DTYP] section 2.3.2.3.

2.2.1 WSD Messages

All messages described in this section MUST be transported using WSD and published to the local subnet. The HomeGroup Protocol uses WSD messages to advertise the presence of a homegroup, as well as shared resources on the home network.

2.2.1.1 HomeGroup Invitation

The HomeGroup Invitation message is used to advertise the presence of the homegroup to other machines on the home network and to provide the required details to allow them to join that homegroup. This message has the WSD type of: HomeGroup_Invitation.

The HomeGroup invitation includes the PeerGroup invitation (which is required to join the PeerGroup) and other relevant information about the homegroup, as described in this section. The invitation is serialized into an XML string and then published on the local subnet using WSD.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="HOMEGROUP_RECORD">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="INVITATION" type="xs:string" minOccurs="1" />
        <xs:element name="NETWORKNAME" type="xs:string" minOccurs="0" />
        <xs:element name="GUIDNAME" type="xs:string" minOccurs="1" />
        <xs:element name="OWNER" type="xs:string" minOccurs="0" />
        <xs:element name="OWNERID" type="xs:string" minOccurs="0" />
        <xs:element name="OWNERMACHINENAME" type="xs:string" minOccurs="0" />
        <xs:element name="LASTCHANGED" type="xs:string" minOccurs="1" />
        <xs:element name="HOMEGROUPSIZE" type="xs:string" minOccurs="1" />
        <xs:element name="ADDRESS" type="xs:string" minOccurs="1" />
        <xs:element name="DIGITALHASH" type="xs:string" minOccurs="1" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="HOMEGROUP_RECORD" />
```


Copyright © 2011 Microsoft Corporation.

```
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

INVITATION: The actual invitation from the PeerGroup. The format for this message and the manner in which it is generated is described in [MS-PPSEC].

NETWORKNAME: If any member of the homegroup is connected wirelessly to the network, this value will be the **service set identifier (SSID)** of the **WAP**. If all machines are wired, then this value will be NULL. The value for this element will be the same across all of the homegroup members. If a new member of the homegroup is the first to use WAP, then this element will be updated to reflect the SSID of the WAP.

GUIDNAME: A unique GUID that represents this homegroup. The value will be the same for all homegroup members, and is generated when the PeerGroup is created [MS-PPSEC].

OWNER: The name of the User who last reset the pin on this homegroup, or if the Pin has never been reset, it is the User who created the homegroup. The value will be the same for all homegroup members.

OWNERID: The Peer Identity of the machine where the owner user resides [MS-PPSEC]. The value will be the same for all homegroup members.

OWNERMACHINENAME: The machine name of the machine that created the homegroup. The value will be the same for all homegroup members.

LASTCHANGED: The Int64 text representation of a FILETIME structure that represents the last time the pin was reset, or if never reset, the time that the homegroup was originally created, as described in [MS-FSCC]. The value will be the same for all homegroup members.

HOMEGROUPSIZE: The number of members in the PeerGroup, and by extension, the homegroup. This is expressed as an integer value.

ADDRESS: The **IPv6** addresses of the network adapter to which the PeerGroup is connected. This list of addresses is semicolon delimited and can be specified using any valid IPv6 address format, as described in [RFC3513]

DIGITALHASH: The values contained in the <NETWORKNAME> (if not empty), <GUIDNAME>, <OWNER>, <OWNERID>, <OWNERMACHINENAME>, <LASTCHANGED>, <HOMEGROUPSIZE>, and <ADDRESS> elements that are hashed together and then signed using the homegroup signing keys. The signing and hashing process is described in section 3.1.4.5.3.

2.2.1.2 Shared Printer

The Shared Printer message is used to advertise printers that are installed on the advertising machine. It is serialized into an XML string and then published on the local subnet using WSD. This message has the WSD type of: HomeGroup_Printer.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="HomeGroup"
targetNamespace="http://schemas.microsoft.com/windows/2007/HomeGroup/Printing"
xmlns:mstns="http://schemas.microsoft.com/windows/2007/HomeGroup/Printing"
xmlns="http://schemas.microsoft.com/windows/2007/HomeGroup/Printing"
```


Copyright © 2011 Microsoft Corporation.

```
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:msdata="urn:schemas-microsoft-com:xml-
msdata" attributeFormDefault="qualified" elementFormDefault="qualified">
  <xs:element name="HomeGroup" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element name="Printer">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Name" type="xs:string" minOccurs="1" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

NAME: The name of the printer being shared. It MUST be a valid printer name, as defined in [MS-RPRN] section 2.2.4.14.

This message is signed and encoded before being sent, as described in section 3.1.4.5.4.

2.2.2 PeerGroup Messages

All messages described in this section MUST be transported using PeerGroup. PeerGroup messages are used for secure communication between members of the homegroup. All messages sent via the PeerGroup are converted to binary before being sent.

2.2.2.1 HomeGroup Member Info

HomeGroup Member Info messages are used to broadcast a homegroup member's machine name and Peer ID.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="HOMEGROUP_RECORD">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="COMPUTERNAME" type="xs:string" minOccurs="1" />
        <xs:element name="PEERID" type="xs:string" minOccurs="1" />
        <xs:element name="RECORDID" type="xs:string" minOccurs="1" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="HOMEGROUP_RECORD" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

COMPUTERNAME: The machine name of the machine that is sending the message [MS-DTYP].

Copyright © 2011 Microsoft Corporation.

PEERID: The Peer Identity of the machine that is sending the message [MS-PPSEC].

RECORDID: A GUID-formatted string. This element SHOULD be an all null GUID formatted as: {00000000-0000-0000-0000-000000000000}. This element can be populated with another GUID-formatted string, but it MUST contain a value.

2.2.2.2 HomeGroup Record

The HomeGroup Record format is the base data structure that is used by the PeerGroup messages described in this section. Each subtype of message uses the HomeGroup Record to contain its relevant data. These records are structured by using the following format:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="HOMEGROUP_RECORD">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="VERSION" type="xs:string" minOccurs="1" />
        <xs:element name="RECORDSOURCE" type="xs:string" minOccurs="1" />
        <xs:element name="RECORDID" type="xs:string" minOccurs="1" />
        <xs:element name="EVENTTYPE" type="xs:string" minOccurs="1" />
        <xs:element name="FLAGS" type="xs:string" minOccurs="1" />
        <xs:element name="SOURCEOS" type="xs:string" minOccurs="1" />
        <xs:element name="PERSIST" type="xs:string" minOccurs="1" />
        <xs:element name="MACHINE" type="xs:string" minOccurs="1" />
        <xs:element name="PEERID" type="xs:string" minOccurs="1" />
        <xs:element name="HOMEGROUP_DATA" type="xs:string" minOccurs="1" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="HOMEGROUP_RECORD" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

VERSION: Denotes the version of the HomeGroup Protocol. The current version, as described in this, document is version one. The value of this element SHOULD be set to 1 for all messages.

RECORDSOURCE: Identifies the type of record being sent and is unique for each message type. For example, the HomeGroup Credentials message (section 2.2.2.2.1) will populate this element with a string in GUID format.

RECORDID: This element SHOULD be an all null GUID formatted as: {00000000-0000-0000-0000-000000000000}. This element can be populated with another GUID-formatted string, but it MUST contain a value.

EVENTTYPE: MUST be set to 0 for all messages.

FLAGS: MUST be set to 0 for all messages.

SOURCEOS: This value identifies the source operating system. In the current version of this protocol, this value SHOULD be set to 100728832 for all messages.

Copyright © 2011 Microsoft Corporation.

PERSIST: Determines if the record will persist on the PeerGroup after the machine that created the record has departed from the PeerGroup. The value SHOULD be set to either 1 (True) or 0 (False).

MACHINE: The machine name of the record creator.

PEERID: The PeerID of the machine that creates the record [MS-PPSEC].

HOMEGROUP_DATA: This element is used to transmit the data of the message subtypes and is populated by individual messages.

2.2.2.2.1 HomeGroup Credentials Message

HomeGroup Credentials messages are used to synchronize homegroup credentials that are common to all homegroup members. This message contains the common credential name, its password, and its creation time.<2>

The password is encrypted using the HomeGroup Encryption Key (section 3.1.4.5.1), and the creation time is used to decide conflicts when two different homegroups are created inside the same network.

HomeGroup Credentials messages are sent within the HomeGroup Record format (section 2.2.2.2), where the following elements are specified:

- The value of the <RECORDSOURCE> element is set to {929CB323-C5EA-48E7-A6D0-193DD432E769}.
- The value of the <PERSIST> element is set to 1.

The <HOMEGROUP_DATA> element is populated with the HomeGroup Credentials message content in the following manner:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="HOMEGROUP_DATA">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="USERNAME" type="xs:string" minOccurs="1" />
        <xs:element name="PASSWORD" type="xs:string" minOccurs="1" />
        <xs:element name="ACCOUNTCREATED" type="xs:string" minOccurs="1" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="HOMEGROUP_DATA" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

USERNAME: MUST be set to HomeGroupUser$.

PASSWORD: The binary version of the encrypted password, as described in section 3.1.4.5.5.

Copyright © 2011 Microsoft Corporation.

ACCOUNTCREATED: The Int64 representation of a FILETIME structure that represents the creation time of the account described in [MS-FSCC]. The value will be the same for all homegroup members.

2.2.2.2.2 HomeGroup MAC Address

HomeGroup MAC Address messages are used to broadcast the **MAC addresses** of all network adapters present in a homegroup member machine to all other members of the homegroup.

HomeGroup MAC Address messages are sent in the HomeGroup Record format (section 2.2.2.2), where the following elements are specified:

- The value of the <RECORDSOURCE> element is set to {A7BC622E-8238-4E38-9C88-34153B7D9AB1}.
- The value of the <PERSIST> element is set to 0.

The <HOMEGROUP_DATA> element is populated with the HomeGroup MAC Address message content in the following manner:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="HOMEGROUP_RECORD">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="MACADDRESSES" type="xs:string" minOccurs="1" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="HOMEGROUP_RECORD" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

MACADDRESSES: This element contains the MAC addresses of all of the network cards on the machine. It is a string of binaryized 6-byte MAC addresses, which consists of two terminating NULL characters. Each MAC address is a binary string that contains a terminating NULL character. The last MAC address is followed by a double NULL. The resulting string is Base64 encoded with beginning and ending certificate headers as described in [RFC3548].

2.2.2.2.3 HomeGroup Signing Key

HomeGroup Signing Key messages are used to distribute signing keys to the homegroup. The signing keys are used to verify the integrity of signed WSD messages that are sent by homegroup members over WSD.

HomeGroup Signing Key messages are sent within the HomeGroup Record format (section 2.2.2.2),where the following elements are specified:

Copyright © 2011 Microsoft Corporation.

- The value of the <RECORDSOURCE> element is set to {CA328F46-E759-4399-82AB-FA92651D1ED2}.
- The value of the <PERSIST> element is set to 1.

The <HOMEGROUP_DATA> element is populated with the HomeGroup Signing Key message content in the following manner:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="HOMEGROUP_DATA">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="SIGNINGKEYS" type="xs:string" minOccurs="1" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="HOMEGROUP_DATA" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

SIGNINGKEYS: The binary version of the encrypted signing key, which is encrypted as specified in section 3.1.4.5.5.

The binary <SIGNINGKEYS> element is sent in the following data format:

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
0x2D								0x00								0x2D								0x00							
0x2D								0x00								0x2D								0x00							
0x2D								0x00								0x42								0x00							
0x45								0x00								0x47								0x00							
0x49								0x00								0x4E								0x00							
0x20								0x00								0x43								0x00							
0x45								0x00								0x52								0x00							
0x54								0x00								0x49								0x00							

Copyright © 2011 Microsoft Corporation.

0x46	0x00	0x49	0x00
0x43	0x00	0x41	0x00
0x54	0x00	0x45	0x00
0x2D	0x00	0x2D	0x00
0x2D	0x00	0x2D	0x00
0x2D	0x00	0x0D	0x00
0x0A	0x00	EncodedKeyBlob	
...			
...			
...			
...			
...			
...			
...			
(EncodedKeyBlob cont'd for 807 rows)			
...		0x2D	0x00
0x2D	0x00	0x2D	0x00
0x2D	0x00	0x2D	0x00
0x45	0x00	0x4E	0x00
0x44	0x00	0x20	0x00
0x43	0x00	0x45	0x00
0x52	0x00	0x54	0x00
0x49	0x00	0x46	0x00

Copyright © 2011 Microsoft Corporation.

0x49	0x00	0x43	0x00
0x41	0x00	0x54	0x00
0x45	0x00	0x2D	0x00
0x2D	0x00	0x2D	0x00
0x2D	0x00	0x2D	0x00
0x0D	0x00	0x0A	0x00

EncodedKeyBlob (3260 bytes): This MUST be generated by the following procedure:

1. Randomly generate a 2048-bit **RSA** key pair and encode it as an **RSAKeyBlob** structure as specified in section 2.2.2.2.3.1. The RSA algorithm is specified in [RFC3447] and recommended methods for generating RSA keys are described in [FIPS186].
2. Generate a 256-bit **AES** key [FIPS197] by concatenating the homegroup **GUID** and the homegroup password and hashing the result with the **SHA-256** algorithm [FIPS180-3]. In this procedure, the homegroup GUID is represented in the Curly-Braced String Representation specified in [MS-DTYP] section 2.3.2.3 and encoded as a Unicode string in **little-endian** UTF-16 encoding with the terminating NULL character and the homegroup password is represented as a Unicode string in little-endian UTF-16 encoding with the terminating NULL character.
3. Encrypt the **RSAKeyBlob** generated in Step 1 with the AES key generated in Step 2, using the AES-256 block cipher [FIPS197] in Cipher Block Chaining mode [SP800-38A] with a zero Initialization Vector (IV).
4. Encode the result from Step 3 with the Base64 encoding scheme specified in [RFC4648] section 4, with a 64-bit line length and a terminating line feed. Note that line feeds are CR-LF combinations.
5. Represent the result from Step 4 as a Unicode string in little-endian UTF-16 encoding.

2.2.2.2.3.1 RSAKeyBlob Structure

This section provides the definition for the **RSAKeyBlob** structure that is used to encode the value of the **EncodedKeyBlob** field of the HomeGroup Signing Key messages defined in section 2.2.2.2.3.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0x07								0x02								0x00								0x00							
0x00								0x24								0x00								0x00							
0x52								0x53								0x41								0x32							

Copyright © 2011 Microsoft Corporation.

0x00	0x08	0x00	0x00
Public Exponent			
Modulus			
...			
...			
...			
...			
...			
...			
...			
(Modulus cont'd for 56 rows)			
Prime1			
...			
...			
...			
...			
...			
...			
...			
(Prime1 cont'd for 24 rows)			
Prime2			
...			
...			

Copyright © 2011 Microsoft Corporation.

...
...
...
...
...
(Prime2 cont'd for 24 rows)
Exponent1
...
...
...
...
...
...
...
(Exponent1 cont'd for 24 rows)
Exponent2
...
...
...
...
...
...
...

Copyright © 2011 Microsoft Corporation.

(Exponent2 cont'd for 24 rows)
Coefficient
...
...
...
...
...
...
...
(Coefficient cont'd for 24 rows)
Private Exponent
...
...
...
...
...
...
...
(Private Exponent cont'd for 56 rows)

Public Exponent (4 bytes): This MUST be a 32-bit unsigned number in little-endian format. It MUST be the public exponent of the key pair, which is referred to as **e** in [RFC3447] section 2.

Modulus (256 bytes): This MUST be the RSA modulus, which is referred to as **n** in [RFC3447] section 2. It MUST be equal to **Prime1** * **Prime2**. It MUST be encoded in little-endian format.

Prime1 (128 bytes): This MUST be the first prime factor of the RSA modulus, which is referred to as **p** in [RFC3447] section 2. It MUST be encoded in little-endian format.

Copyright © 2011 Microsoft Corporation.

Prime2 (128 bytes): This MUST be the second prime factor of the RSA modulus,which is referred to as **q** in [RFC3447] section 2. It MUST be encoded in little-endian format.

Exponent1 (128 bytes): This MUST be the Chinese Remainder Theorem exponent of **Prime1**, which is referred to as **dP** in [RFC3447] section 2. It MUST be encoded in little-endian format.

Exponent2 (128 bytes): This MUST be the Chinese Remainder Theorem exponent of **Prime2**, which is referred to as **dQ** in [RFC3447] section 2. It MUST be encoded in little-endian format.

Coefficient (128 bytes): This MUST be the Chinese Remainder Coefficient of **Prime1** and **Prime2**, which is referred to as **qInv** in [RFC3447] section 2. It MUST be encoded in little-endian format.

Private Exponent (256 bytes): This MUST be the RSA private exponent, which is referred to as **d** in [RFC3447] section 2. It MUST be encoded in little-endian format.

Copyright © 2011 Microsoft Corporation.

3 Protocol Details

3.1 Homegroup Member Details

3.1.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

To implement the HomeGroup Protocol, an individual homegroup member stores and updates the data about itself, as well as the data about other members of the homegroup, which is necessary for sending the messages specified in section 2. Whenever the data maintained by the machine changes, the messages in section 2 SHOULD be resent. Resending the messages ensures that new information is propagated to all members of the homegroup.

Note The homegroup password is required to join a homegroup, but is never transmitted by this protocol.<3>

3.1.2 Timers

None.

3.1.3 Initialization

This protocol is initialized when a machine creates or joins a homegroup. When this protocol is first initialized, the machine SHOULD check for the HomeGroup Invitation WSD message (section 2.2.1.1). If a HomeGroup Invitation is detected, then the machine MAY join the homegroup, as described in section 3.1.4.2.

If no invitation is detected, then the machine MAY create a homegroup, as described in section 3.1.4.1.

3.1.4 Higher-Layer Triggered Events

3.1.4.1 Creating the Homegroup

To participate in a homegroup, a machine MUST create the homegroup when a Homegroup Invitation message (section 2.2.1.1) does not exist. This requires a homegroup password. All other machines will then be able to join the homegroup when the first machine's HomeGroup Invitation is detected.

A new homegroup is created by creating a new PeerGroup with a secure Peer ID [MS-PPSEC]. The Peer ID is a unique identifier that other members in the PeerGroup can use to identify a particular member [MS-PPSEC]. The machine then generates the signing keys, as described in section 3.1.4.5.2. The machine MUST then take the following actions:

- Send a HomeGroup Signing Key message (section 2.2.2.2.3), a HomeGroup Member Info message (section 2.2.2.1), a HomeGroup Credentials message (section 2.2.2.2.1), and a HomeGroup MAC Address message (section 2.2.2.2.2) to the PeerGroup. If the data contained in a message changes, the machine MUST create new messages and send them to the PeerGroup.

Copyright © 2011 Microsoft Corporation.

- Publish a HomeGroup Invitation WSD message (section 2.2.1.1). If the data contained in the HomeGroup Invitation WSD message changes, the machine MUST create a new HomeGroup Invitation WSD message and publish it on the WSD channel.
- When a printer is attached to the machine that is to be shared, the machine SHOULD also publish a HomeGroup Printer WSD message (section 2.2.1.2) on the WSD channel. If the printer is unshared, the machine SHOULD remove the printer from the HomeGroup Printer WSD message.

There is no required order for sending or publishing these messages.

3.1.4.2 Joining the Homegroup

Joining an existing homegroup requires the presence of a HomeGroup Invitation message. Multiple HomeGroup Invitation messages can be present on the network.<4> When a HomeGroup Invitation message has been detected, the machine MUST use the PeerGroup invitation located in the <INVITATION> element of the HomeGroup Invitation message (section 2.2.1.1), as well as the homegroup password, to join the PeerGroup.

The machine joins the PeerGroup in the manner described in [MS-PPSEC] section 3.1.4.3. Once the machine has joined the PeerGroup, it is considered a member of the homegroup.<5>

After joining the PeerGroup, the machine MUST then take the following actions:

- Send a HomeGroup Signing Key message (section 2.2.2.2.3), a HomeGroup Member Info message (section 2.2.2.1), a HomeGroup Credentials message (section 2.2.2.2.1), and a HomeGroup MAC Address message (section 2.2.2.2.2) to the PeerGroup. If the data contained in a message changes, the machine MUST create new messages and send them to the PeerGroup.
- Publish a HomeGroup Invitation WSD message (section 2.2.1.1). If the data contained in the HomeGroup Invitation WSD message changes, the machine MUST create a new HomeGroup Invitation WSD message and publish it on the WSD channel.
- When a printer is attached to the machine that is to be shared, the machine SHOULD also publish a HomeGroup Printer WSD message (section 2.2.1.2) on the WSD channel. If the printer is unshared, the machine SHOULD remove the printer from the HomeGroup Printer WSD message.

3.1.4.3 Departing the Homegroup

To depart from the homegroup, the machine MUST remove all messages that it sent to the PeerGroup from the group [MS-PPGRH], except those that are flagged to persist after the machine's departure, as described in sections 2.2.2.2.1 and 2.2.2.2.3 and [MS-PPGRH].

The machine MUST stop publishing the HomeGroup Invitation WSD message and, if applicable, the HomeGroup Printer WSD message.

The machine MAY then close and delete the PeerGroup [MS-PPGRH].<6>

3.1.4.4 Changing the Homegroup Password

Changing the homegroup password is accomplished by departing the homegroup and creating a new homegroup with the new password.

To change the homegroup password, the machine departs the homegroup, as described in section 3.1.4.3. The machine then creates a new homegroup, as described in section 3.1.4.1. When doing so, both the GUIDNAME name and the signing keys MUST be reused from the departed homegroup. This is done so that when the new homegroup broadcasts its invitation, it will contain the old

Copyright © 2011 Microsoft Corporation.

homegroup name and the digital signature will be signed with the signing keys of the previous homegroup.

The other homegroup machines then detect the new HomeGroup Invitation WSD message and can join the homegroup by supplying the new password, as described in section 3.1.4.2.

3.1.4.5 Message Signing and Encryption

3.1.4.5.1 Encryption Key

An encryption key is generated when a homegroup is created. A 256-bit AES key is formed by taking the SHA-256 hash of the PeerGroup name (GUID) and the homegroup password as the **salt**. AES is specified in [FIPS197] and SHA-256 is specified in [FIPS180-3] section 6.2.

This encryption key is used to encrypt the HomeGroup Credentials message (section 2.2.2.2.1) account credentials, as well as the public/private signing keys, before sending over the network.

3.1.4.5.2 Public/Private Signing Keys

The creator of the homegroup generates a 2048-bit RSA key pair, as specified in [RFC3447] and [PKCS1].

These keys are encrypted, as described in section 3.1.4.5.5, and sent to the other members of the homegroup over the PeerGroup channel via a HomeGroup Signing Key message (section 2.2.2.2.3).

The keys are used to sign or verify the integrity of signed WSD messages sent over the homegroup.

3.1.4.5.3 WSD Hash

HomeGroup Invitation messages (section 3.1.5.1) are hashed. This hash is signed with the HomeGroup signing key and the signed version is included in the message in the <DIGITALHASH> element.

The hash is an SHA-256 hash of the following values in the order specified:

- <NETWORKNAME> (if it contains a value)
- <GUIDNAME>
- <OWNER> (if it contains a value)
- <OWNERID> (if it contains a value)
- <OWNERMACHINENAME> (if it contains a value)
- <LASTCHANGED>
- <HOMEGROUPSIZE>
- <ADDRESS>

This hash is computed, as specified in [FIPS180-3]. The optional fields are ignored when they do not contain a value. The hash is then signed with the public signing key described in section 3.1.4.5.2, using the RSASSA-PKCS1-v1_5 signature algorithm specified in [PKCS1] section 8.2.

Copyright © 2011 Microsoft Corporation.

3.1.4.5.4 Printer Messages

HomeGroup Printer messages are signed with the public signing key, described in section 3.1.4.5.2, using the RSASSA-PKCS1-v1_5 signature algorithm specified in [PKCS1] section 8.2.

3.1.4.5.5 Encrypting HomeGroup Credentials, Signing Key and MAC Address

The <PASSWORD> element in the HomeGroup Credentials message and the <SIGNINGKEYS> element in the HomeGroup Signing Key message are encrypted using the Encryption Key (section 3.1.4.5.1) with the AES-256 algorithm [FIPS197] in Cipher Block Chaining mode [SP800-38A] with a zero Initialization Vector (IV).

3.1.5 Processing Events and Sequencing Rules

3.1.5.1 HomeGroup Invitation Messages

When a HomeGroup Invitation message is received by a machine that is not a member of the homegroup, the machine will not be able to verify the HomeGroup Invitation message. Instead, the machine can join the homegroup using the HomeGroup Invitation message as described in section 3.1.4.2.

When a HomeGroup Invitation message is received by a machine that is currently a member of the homegroup, the message hash SHOULD be verified using the RSASSA-PKCS1-v1_5 signature algorithm specified in [PKCS1] section 8.2. Once the HomeGroup Invitation message is verified, if the value of the <GUIDNAME> element for the message matches the <GUIDNAME> value for the current homegroup, and if the value of the <LASTCHANGED> element element for the message is newer than the <LASTCHANGED> value for the current homegroup, then a password reset condition is detected and the machine MUST change the password as defined in section 3.1.4.4.

3.1.5.2 Printer Messages

When a Printer message is received, it MUST be decoded from Base64, as described in [RFC3548], and SHOULD then be verified using the RSASSA-PKCS1-v1_5 signature algorithm, specified in [PKCS1] section 8.2.

Once verified, the machine SHOULD add the printer as described in [MS-RPRN].

3.1.5.3 HomeGroup Credentials and Signing Key Messages

Whenever a HomeGroup Credentials message or a HomeGroup Signing Key message is received, its encrypted fields MUST be decrypted using the Encryption Key (section 3.1.4.5.1) with the AES-256 algorithm [FIPS197] in Cipher Block Chaining mode [SP800-38A] with a zero Initialization Vector (IV).

3.1.6 Timer Events

None.

3.1.7 Other Local Events

For the purposes of participating in this protocol, any messages that are received over WSD or PeerGroup that do not conform to the message formats described in section 2 SHOULD be ignored.

Copyright © 2011 Microsoft Corporation.

4 Protocol Examples

4.1 HomeGroup Invitation Example

An example of a WSD HomeGroup message that uses the layout of the HomeGroup Invitation message (section 2.2.1.1).

```
<HOMEGROUP_RECORD>
<INVITATION>
&lt;PEERINVITATIONVERSION="1.1"&gt;&lt;CLOUDNAME&gt;LinkLocal_ff00::%10/8&lt;/C
LOUDNAME&gt;&lt;SCOPE&gt;LINKLOCAL&lt;/SCOPE&gt;&lt;CLOUDFLAGS&gt;1&lt;/CLOUDFL
AGS&gt;&lt;GROUPPEERNAME&gt;2bcba40abd09492eb706b74f8f8932a6efb10979.HomeGroupP
eerGroupClassifier&lt;/GROUPPEERNAME&gt;&lt;GROUPFRIENDLYNAME&gt;HomeGroup Peer
Group&lt;/GROUPFRIENDLYNAME&gt;&lt;/PEERINVITATION&gt;
</INVITATION>
<NETWORKNAME>
2PC-airlinkN
</NETWORKNAME>
<GUIDNAME>
{A4C99DD2-EF9E-4447-89DC-19BF65323D19}
</GUIDNAME>
<OWNER>
DT1
</OWNER>
<OWNERID>
f8f4182fd7302b07a7d1aeae3cb2b69adaa9d595.HomeGroupClassifier_1
</OWNERID>
<OWNERMACHINENAME>
KYLEDELL32C-PC
</OWNERMACHINENAME>
<LASTCHANGED>
128907808427918671
</LASTCHANGED>
<HOMEGROUPSIZE>
5
</HOMEGROUPSIZE>
<ADDRESS>
[fe80::b424:f131:8bcc:b134%12]:3587
</ADDRESS>
<DIGITALHASH>
-----BEGIN CERTIFICATE-----
ToilYyp9knjZKpNitWjU0pNrFa0qZoQicHSmbalp4ClE4wWOu6JqXyigxUG7se0T
MDojQPDG076ozmT8K4I0dbXdVpcHLPbbhJanM7QXqof/rGSM+Y+UrmR+CDiwCHzH
6qaRN81WWkkFrq8tIhl/as5NM2md4eY7kHhgUNGf+XEm2JKO20dAYjmnh1Lwt+ka
qxauNuqKc2JsujWooe85pbfomHZN5AHX2wuap1zwt2/g9xEXy2X69LruGuj5vihy
fGtv4w1o7QeZETmcPoaTBCyBsCyAC7zdWiZ/Q3qtFrA0wh5NlV1Od1UJDOy7pGZu
CaHtY6vD22wKYYXdU7OjoQ==
-----END CERTIFICATE-----
</DIGITALHASH>
</HOMEGROUP_RECORD>
```

Some points to consider regarding specific elements of this message:

- **NETWORKNAME**: A value of "2PC-airlinkN" indicates that at least one of the machines in the HomeGroup is connected wirelessly; otherwise, the value would be NULL.

Copyright © 2011 Microsoft Corporation.

- **HOMEGROUPSIZE**: Indicates the number of homegroup members which in this case is five.
- **INVITATION:** Supplies the invitation to the actual PeerGroup, which has been generated according to the Peer-to-Peer Grouping Security Protocol Specification [MS-PPSEC].
- **DIGITALHASH**: Provides an example of the hashed certificate.

4.2 HomeGroup Member Info Message

An example HomeGroup Member Info message (section 2.2.2.1).

```
<?xml version="1.0" encoding="UTF-16"?>
<HOMEGROUP_RECORD>
     <COMPUTERNAME>MICHMCK2</COMPUTERNAME>
     <PEERID>
     f0eb97049320127acd2a8f4990a389c3725a7a08.HomeGroupClassifier</PEERID>
     <RECORDID>{00000000-0000-0000-0000-000000000000}</RECORDID>
</HOMEGROUP_RECORD>
```

4.3 HomeGroup Credentials Message

An example HomeGroup Credentials message (2.2.2.2.1).

```
<?xml version="1.0" encoding="UTF-16"?>
<HOMEGROUP_RECORD>
<VERSION>1</VERSION>
<RECORDSOURCE>{929CB323-C5EA-48E7-A6D0-193DD432E769}</RECORDSOURCE>
<RECORDID>{00000000-0000-0000-0000-000000000000}</RECORDID>
<EVENTTYPE>0</EVENTTYPE>
<FLAGS>0</FLAGS>
<SOURCEOS>100728832</SOURCEOS>
<PERSIST>1</PERSIST>
<MACHINE>MICHMCK2</MACHINE>
<PEERID>f0eb97049320127acd2a8f4990a389c3725a7a08.HomeGroupClassifier</PEERID>
<HOMEGROUP_DATA>
<USERNAME>HomeGroupUser$</USERNAME>
<PASSWORD>
     -----BEGIN CERTIFICATE-----
/XomoIDoi8lbL/26jqr7EbjJ2qV/2/kAACULvW3B9zW4UcScaVzWdJmjgsRNgzk0..U9k1+vkitCius
ybNVAaZWFCdhxCIvx9xnEyfsi+dqSENIqyYTxKKd6IEGaGuPziy..fh0YYu6Z8DFNn+UIDnzNzpdjM7
F1hbES7WM3Cz+2URsfhdMI+cb8NvdXc231a3QC..p3e6pvRBy5AOPcKmX5mEPyeNtoYxtV8ckm23WT3
6mcY=
     -----END CERTIFICATE-----</PASSWORD>
     <ACCOUNTCREATED>128986520996250000</ACCOUNTCREATED>
</HOMEGROUP_DATA>
</HOMEGROUP_RECORD>
```

4.4 HomeGroup MAC Address Message

An example HomeGroup MAC Address message (section 2.2.2.2.2).

```
<?xml version="1.0" encoding="UTF-16"?>
```


Copyright © 2011 Microsoft Corporation.

```
<HOMEGROUP_RECORD>
<VERSION>1</VERSION>
<RECORDSOURCE>{A7BC622E-8238-4E38-9C88-34153B7D9AB1}</RECORDSOURCE>
<RECORDID>{00000000-0000-0000-0000-000000000000}</RECORDID>
<EVENTTYPE>0</EVENTTYPE>
<FLAGS>0</FLAGS>
<SOURCEOS>100728832</SOURCEOS>
<PERSIST>0</PERSIST>
<MACHINE>MICHMCK2</MACHINE>
<PEERID>f0eb97049320127acd2a8f4990a389c3725a7a08.HomeGroupClassifier</PEERID>
<HOMEGROUP_DATA>
     <?xml version="1.0" encoding="UTF-16"?>
     <HOMEGROUP_RECORD>
     <MACADDRESSES>
        -----BEGIN CERTIFICATE----
        MAAwAC0AMAAyAC0AQgAzAC0AOQA2AC0ANgA5AC0ARAA3AAAAMAAwA
        C0AMABFAC0A..QQA2AC0AOABFAC0ARgBGAC0AQQA3AAAAAAA
        -----END CERTIFICATE-----
     </MACADDRESSES>
     </HOMEGROUP_RECORD>
</HOMEGROUP_DATA>
</HOMEGROUP_RECORD>
```

4.5 HomeGroup Signing Key Message

An example (in Base64 representation) of the HomeGroup Signing Key message (section 2.2.2.2.3).

```
<SIGNINGKEYS>
-----BEGIN CERTIFICATE-----
..ZB+KXUU/I3Dr09SsqlFLgutnti0xR0/q7k1Y1Y/yTRBKBwwnCiKyulH8Eh+fmXb/
..YXZ2AsCx3dT9yrOlrzMx4VHSQuO0fpFqqrIhjaAZu3pw6Hcuga1Pz6CxSy0JlbhS
..At5749kc0igPNgwDBGkaz7W563GbNNoGMUUCxyK1rm+xw2S2ZxwurU/eqeJextpM
..qrjRwO+ynAQI1bol9jZUKIzO+XXk7KJkS4NJFxCXeZCA7tByedOqMKoBj6NNGo72
..BYLawtt7rRcOGtdcr3b5ApcI2S5Zgovd63R/8obhEfepmb5r1WX7aLkpF9UiDHMn
..z1Xtp3p+BaWp0NphVpJM+iIPdMfd87EhUIKDoexh29CHxAOyTdQxaLBIHD5UBGrs
..zKB3DDKbm/J0uKqCdswCE3mq3pyStZZbQ80Zcspcr77S27ELSWDbfIuwT/vWHwmp
..DKx+VOE/F6QxHty63O2e8LQoY7AQNqLtekrx/zmZvyzqIQ1qGZEI72NBmmyMbL5P
..kA+B5tW0pi20mmEXARKcAXSqbes9ITyYcQp2gu0npaXTvMbymZvgdl2TijlRGbDF
..qMnXzummVm+CxZH77wUdftWn8jaGNvytzOKxshnmj1y/jJd5eE6THImOBSXSAdth
..xPXrgBLvuWjxqEN1Fl8ZAvxQBjYv41Fy2xtDVCM5XcW6vg5R1PINnnpwV2Yvgkan
..0td8sjVjxAqukcWIVHsaA91w6+nxWFy7DR9Cm1I2M+kOjKBj2ayc1mprPvVB6dn+
..8GFuDZ8kYDH4xWZLqtkZPJ+WR5d0keSqkB7dwL4UVU0bBEnmwcwYD6p+VFD9jeWV
..GvkkxBbglU7m3hJ40KFpfz72C2Ahc9ervQkE626sNcFQh0eotOgKAexhOxTnfnrS
..b3hBDDEEoF8FA/oUGf4/jRM8tMHJsgIty3ZUG4d0LfK77IuXnuvB2eEOL/Iuodkn
..nnLNfyJ5r8gWuRJVP2QhVXe17/4AdwBdr3z3zhkAVRqEqMpaRz5CQAmNIWyGURFg
..xCe1XCyCPXOHLiA9GRfSWtDrH0M3LocrH+lbUJ1+dhKqugVE6Nfr2m6kwTCb33iR
..PlUQEQy68tj00GKAUBuAGDH+UIie9G4YzRzRrhHMWNdDCXJGaZFNXRHLTLBdDvTY
..huOgy7GcEE20V6UjkO1osUDek5kuMdE46w57vGDQuRA1JGC3rZvmvVlda0YFltZG
..iDYGe/WU3PspTKkZCsUOXigd/4EPEwjvsmgThIGeUHxn7rieElSwOhwke7RR80nY
..5ShZ2bjiZ0rvkSW/T9k6XnajBslRlSZWgobpxChH72G50smv28ITjBSKhXT621/v
..IBhp8QHhJpgBSbB0k5O+FTY7HM8osKOhY00SVmMkVAke49sPORhX7yt27MycRXUp
..gMhie3EWUV3q6RUk9vaARkGRfa3Wj7LeDM8NIxzXuvs2Fy+rx4DRYg5cbVry6kfp
..ZSw/9NTVOC1llr/tZbmKC8xDjSlvSEhidTw9I91JniT7PiDRon370sxAgwjxLzqp
..OQ7e7vLKpvfkhYTb9/+v1BVlsN+O55asSni20zSrguI=..
-----END CERTIFICATE-----
..</SIGNINGKEYS>
```


Copyright © 2011 Microsoft Corporation.

5 Security

5.1 Security Considerations for Implementers

The HomeGroup Protocol relies partially on the Peer-to-Peer Grouping Security Protocol [MS-PPSEC] to secure the PeerGroup traffic. Encryption and hashing within the sent messages is achieved through open cryptographic standards.

5.2 Index of Security Parameters

Security parameter	Section
<DIGITALHASH>	Section 2.2.1.1
<PASSWORD>	Section 2.2.2.2.1
<SIGNINGKEYS>	Section 2.2.2.2.3
Message Signing and Encryption	Section 3.1.4.5

Copyright © 2011 Microsoft Corporation.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Windows® 7 operating system
- Windows® Home Server 2011 server software

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 1.3: In Windows 7 and Windows Home Server 2011, the protocol excludes the relationship to machines that exist on the same subnet.

<2> Section 2.2.2.2.1: In Windows 7 and Windows Home Server 2011, every homegroup member has a common user account with the same password, which is used to authenticate between members of the homegroup.

<3> Section 3.1.1: In Windows 7 and Windows Home Server 2011, this password can be auto-generated by the machine that is creating the homegroup, or supplied by a user.

<4> Section 3.1.4.2: In Windows 7 and Windows Home Server 2011, if more than one HomeGroup Invitation message is found, then the protocol will attempt to join the PeerGroup specified in each HomeGroup Invitation until successful. The order in which the HomeGroup Invitation messages are processed is undefined.

<5> Section 3.1.4.2: In Windows 7 and Windows Home Server 2011, after the PeerGroup invitation has been issued, the machine then collects and stores the information from the HomeGroup Credentials message and the HomeGroup MAC address message, as well as from the signing keys found in the HomeGroup Signing Key message.

<6> Section 3.1.4.3: In Windows 7 and Windows Home Server 2011, the machine closes and deletes the Peergroup after departing the homegroup when it is the last member of the homegroup. In the case where the password change has occurred and the machine is not the last member of the homegroup, the homegroup is not closed and deleted.

Copyright © 2011 Microsoft Corporation.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

Copyright © 2011 Microsoft Corporation.

8 Index

Copyright © 2011 Microsoft Corporation.

T

V

W

Copyright © 2011 Microsoft Corporation.