[MS-IKEE]: Internet Key Exchange Protocol Extensions

This topic lists the Errata found in the MS-IKEE document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS

Atom

Errata below are for Protocol Document Version V24.0 – 2017/06/01.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2017/08/21</td><td>
<p>In Section 1.7, Versioning and Capability Negotiation, details for missing vendor IDs were added.</p>
<p>Changed from:</p>
<p>Capability Negotiation: IKE can advertise specific capabilities through vendor ID payloads, as specified in [RFC2408] section 3.16.&lt;6&gt;</p>
<p>&lt;6&gt; Section 1.7: The Microsoft implementation of IKE supports the following vendor IDs.</p>
<p>The Microsoft implementation vendor ID (the first rows of the second table that follows, where the common name starts with "Microsoft implementation") is constructed by appending a 32-bit (4-byte) version number in network order to the 128-bit (16-byte) MD5 hash of the "MS NT5 ISAKMPOAKLEY" string. The version number is the additional 4 bytes that denote the Windows version as detailed in the first table that follows.</p>
<p>…</p>
<table>
<tr><th>Common name</th><th>String representation</th><th>Wire representation (MD5 hash of string)</th><th>Version</th></tr>
<tr><td>Microsoft implementation Windows 2000</td><td>"MS NT5 ISAKMPOAKLEY" + version number 2</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 02</td><td>Windows 2000</td></tr>
<tr><td>Microsoft implementation Windows XP</td><td>"MS NT5 ISAKMPOAKLEY" + version number 3</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 03</td><td>Windows XP</td></tr>
<tr><td>Microsoft implementation Windows Server 2003</td><td>"MS NT5 ISAKMPOAKLEY" + version number 4</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 04</td><td>Windows Server 2003</td></tr>
<tr><td>Microsoft implementation Windows Vista</td><td>"MS NT5 ISAKMPOAKLEY" + version number 5</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 05</td><td>Windows Vista</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description			
	Microsoft implementation Windows Server 2008	"MS NT5 ISAKMPOAKLEY" + version number 6	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 06	Windows Server 2008
	Microsoft implementation Windows 7	"MS NT5 ISAKMPOAKLEY" + version number 7	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 07	Windows 7
	Microsoft implementation Windows Server 2008 R2	"MS NT5 ISAKMPOAKLEY" + version number 8	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 08	Windows Server 2008 R2
	Microsoft implementation Windows 8	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows 8
	Microsoft implementation Windows Server 2012	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows Server 2012
	Microsoft implementation Windows 8.1	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows 8.1
	Microsoft implementation Windows 10	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows 10
	Microsoft implementation Windows Server 2012 R2	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows Server 2012 R2
	Microsoft implementation Windows Server 2016	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows Server 2016
	Kerberos authentication supported (as specified in [GSS])	"GSSAPI"	62 1B 04 BB 09 88 2A C1 E1 59 35 FE FA 24 AE EE	All versions listed in the Product Behavior Appendix
	NLB/MSCS fast failover supported	"Vid-Initial-Contact"	26 24 4D 38 ED DB 61 B3 17 2A 36 E3 D0 CF B8 19	All versions listed in the Product Behavior Appendix
	NLB/MSCS fast failover supported	"NLBS_PRESENT"	72 87 2B 95 FC DA 2E B7 08 EF E3 22 11 9B 49 71	All versions listed in the Product Behavior Appendix

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>Fragmentation avoidance supported</td><td>"FRAGMENTATION"</td><td>40 48 B7 D5 6E BC E8 85 25 E7 DE 7F 00 D6 C2 D3</td><td>All versions listed in the Product Behavior Appendix</td></tr>
<tr><td>NAT-T supported</td><td>"draft-ietf-ipsec-nat-t-ike-02\n"</td><td>90 CB 80 91 3E BB 69 6E 08 63 81 B5 EC 42 7B 1F</td><td>All versions listed in the Product Behavior Appendix</td></tr>
<tr><td>NAT-T supported</td><td>"RFC 3947"</td><td>4A 13 1C 81 07 03 58 45 5C 57 28 F2 0E 95 45 2F</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows Server 2003</td></tr>
<tr><td>AuthIP supported</td><td>"MS-MamieExists"</td><td>21 4C A4 FA FF A7 F3 2D 67 48 E5 30 33 95 AE 83</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows Server 2003</td></tr>
<tr><td>CGA supported</td><td>"IKE CGA version 1"</td><td>E3 A5 96 6A 76 37 9F E7 07 22 82 31 E5 CE 86 52</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows Server 2003</td></tr>
<tr><td>Negotiation discovery supported</td><td>"MS-Negotiation Discovery Capable"</td><td>FB 1D E3 CD F3 41 B7 EA 16 B7 E5 BE 08 55 F1 20</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows Server 2003</td></tr>
<tr><td>Microsoft Xbox One 2013</td><td>"Microsoft Xbox One 2013"</td><td>8A A3 94 CF 8A 55 77 DC 31 10 C1 13 B0 27 A4 F2</td><td>Windows 10 and Windows Server 2016</td></tr>
<tr><td>Xbox IKEv2 Negotiation</td><td>"Xbox IKEv2 Negotiation"</td><td>66 08 22 B3 A7 3A 24 41 49 57 8D 62 E0 EB 46 A0</td><td>Windows 10 and Windows Server 2016</td></tr>
<tr><td>Security Realm ID</td><td>"MSFT IPsec Security Realm Id"</td><td>68 6A 8C BD FE 63 4B 40 51 46 FB 2B AF 33 E9 E8</td><td>Windows 10 and Windows Server 2016</td></tr>
</table>
Changed to:
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<p>Capability Negotiation: IKE can advertise specific capabilities through vendor ID payloads, as specified in [RFC2408] section 3.16.&lt;6&gt;</p>
<p>&lt;6&gt; Section 1.7: The Microsoft implementation of IKE supports the following vendor IDs.</p>
<p>The Microsoft implementation vendor ID (the first rows of the second table that follows, where the common name starts with "Microsoft implementation") is constructed by appending a 32-bit (4-byte) version number in network order to the 128-bit (16-byte) MD5 hash of the "MS NT5 ISAKMPOAKLEY" string. The version number is the additional 4 bytes that denote the Windows version as detailed in the first table that follows.</p>
<p>…</p>
<p>In other cases, a keying module vendor ID is constructed by appending a 32-bit (4-byte) module value in network byte order to the 128-bit (16-byte) MD5 hash of the “KEY_MODS” string to create its wire representation. Examples of this are shown in the table immediately below in rows where the Common name contains the text “Microsoft supported keying modules”. A similar organization applies to constructing a vendor ID for the “AUTHIP_INIT_KE_DH_GROUP” strings shown in rows of the table that follows which have the Common name “AuthIP Initiator DH type sent in KE”. Other vendor IDs are as stated in the same table.</p>
<p>Additional tables that follow the table immediately below specify key module values and Diffie Hellman (DH) group values that are available for constructing vendor IDs for keying modules and AuthIP Initiator DH groups, respectively.</p>
<table>
<tr><th>Common name</th><th>String representation</th><th>Wire representation (MD5 hash of string)</th><th>Version</th></tr>
<tr><td>Microsoft implementation Windows 2000</td><td>"MS NT5 ISAKMPOAKLEY" + version number 2</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 02</td><td>Windows 2000</td></tr>
<tr><td>Microsoft implementation Windows XP</td><td>"MS NT5 ISAKMPOAKLEY" + version number 3</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 03</td><td>Windows XP</td></tr>
<tr><td>Microsoft implementation Windows Server 2003</td><td>"MS NT5 ISAKMPOAKLEY" + version number 4</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 04</td><td>Windows Server 2003</td></tr>
<tr><td>Microsoft implementation Windows Vista</td><td>"MS NT5 ISAKMPOAKLEY" + version number 5</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 05</td><td>Windows Vista</td></tr>
<tr><td>Microsoft implementation Windows Server 2008</td><td>"MS NT5 ISAKMPOAKLEY" + version number 6</td><td>1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 06</td><td>Windows Server 2008</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description			
	Microsoft implementation Windows 7	"MS NT5 ISAKMPOAKLEY" + version number 7	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 07	Windows 7
	Microsoft implementation Windows Server 2008 R2	"MS NT5 ISAKMPOAKLEY" + version number 8	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 08	Windows Server 2008 R2
	Microsoft implementation Windows 8	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows 8
	Microsoft implementation Windows Server 2012	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows Server 2012
	Microsoft implementation Windows 8.1	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows 8.1
	Microsoft implementation Windows 10	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows 10
	Microsoft implementation Windows Server 2012 R2	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows Server 2012 R2
	Microsoft implementation Windows Server 2016	"MS NT5 ISAKMPOAKLEY" + version number 9	1E 2B 51 69 05 99 1C 7D 7C 96 FC BF B5 87 E4 61 00 00 00 09	Windows Server 2016
	Microsoft supported keying modules	“KEY_MODS” + Key Module (IKE)	01 52 8b bb c0 06 96 12 18 49 ab 9a 1c 5b 2a 51 00 00 00 00	Windows 7 and later, and Windows Server 2008 R2 operating system and later
	Microsoft supported keying modules	“KEY_MODS” + Key Module (AuthIP)	01 52 8b bb c0 06 96 12 18 49 ab 9a 1c 5b 2a 51 00 00 00 01	Windows 7 and later, and Windows Server

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>2008 R2 and later</td></tr>
<tr><td>Microsoft supported keying modules</td><td>“KEY_MODS” + Key Module (IKEv2)</td><td>01 52 8b bb c0 06 96 12 18 49 ab 9a 1c 5b 2a 51 00 00 00 02</td><td>Windows 7 and later, and Windows Server 2008 R2 and later</td></tr>
<tr><td>Kerberos authentication supported (as specified in [GSS])</td><td>"GSSAPI"</td><td>62 1B 04 BB 09 88 2A C1 E1 59 35 FE FA 24 AE EE</td><td>All versions listed in the Product Behavior Appendix</td></tr>
<tr><td>NLB/MSCS fast failover supported</td><td>"Vid-Initial-Contact"</td><td>26 24 4D 38 ED DB 61 B3 17 2A 36 E3 D0 CF B8 19</td><td>All versions listed in the Product Behavior Appendix</td></tr>
<tr><td>NLB/MSCS fast failover supported</td><td>"NLBS_PRESENT"</td><td>72 87 2B 95 FC DA 2E B7 08 EF E3 22 11 9B 49 71</td><td>All versions listed in the Product Behavior Appendix</td></tr>
<tr><td>Fragmentation avoidance supported</td><td>"FRAGMENTATION"</td><td>40 48 B7 D5 6E BC E8 85 25 E7 DE 7F 00 D6 C2 D3</td><td>All versions listed in the Product Behavior Appendix</td></tr>
<tr><td>NAT-T supported</td><td>"draft-ietf-ipsec-nat-t-ike-02\n"</td><td>90 CB 80 91 3E BB 69 6E 08 63 81 B5 EC 42 7B 1F</td><td>All versions listed in the Product Behavior Appendix</td></tr>
<tr><td>NAT-T supported</td><td>"RFC 3947"</td><td>4A 13 1C 81 07 03 58 45 5C 57 28 F2 0E 95 45 2F</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>Server 2003</td></tr>
<tr><td>AuthIP supported</td><td>"MS-MamieExists"</td><td>21 4C A4 FA
FF A7 F3 2D
67 48 E5 30
33 95 AE 83</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows Server 2003</td></tr>
<tr><td>CGA supported</td><td>"IKE CGA version 1"</td><td>E3 A5 96 6A
76 37 9F E7 07
22 82 31 E5
CE 86 52</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows Server 2003</td></tr>
<tr><td>Negotiation discovery supported</td><td>"MS-Negotiation Discovery Capable"</td><td>FB 1D E3 CD
F3 41 B7 EA
16 B7 E5 BE
08 55 F1 20</td><td>All versions listed in the Product Behavior Appendix except Windows 2000, Windows XP, and Windows Server 2003</td></tr>
<tr><td>AuthIP Initiator DH type sent in KE</td><td>“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_GROUP_NONE)</td><td>7B B9 38 67
D7 6C 8D 80
DF 0F 40 FA
E8 FC 3B 19
00 00 00 00</td><td>Windows 8 and later, and Windows Server 2012 and later</td></tr>
<tr><td>AuthIP Initiator DH type sent in KE</td><td>“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_GROUP_1)</td><td>7B B9 38 67
D7 6C 8D 80
DF 0F 40 FA</td><td>Windows 8 and later, and Windows Server</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description			
			E8 FC 3B 19 00 00 00 01	2012 and later
	AuthIP Initiator DH type sent in KE	“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_GROUP_2)	7B B9 38 67 D7 6C 8D 80 DF 0F 40 FA E8 FC 3B 19 00 00 00 02	Windows 8 and later, and Windows Server 2012 and later
	AuthIP Initiator DH type sent in KE	“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_GROUP_14 / IKEEXT_DH_GROUP_2048)	7B B9 38 67 D7 6C 8D 80 DF 0F 40 FA E8 FC 3B 19 00 00 00 03	Windows 8 and later, and Windows Server 2012 and later
	AuthIP Initiator DH type sent in KE	“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_ECP_256)	7B B9 38 67 D7 6C 8D 80 DF 0F 40 FA E8 FC 3B 19 00 00 00 04	Windows 8 and later, and Windows Server 2012 and later
	AuthIP Initiator DH type sent in KE	“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_ECP_384)	7B B9 38 67 D7 6C 8D 80 DF 0F 40 FA E8 FC 3B 19 00 00 00 05	Windows 8 and later, and Windows Server 2012 and later
	AuthIP Initiator DH type sent in KE	“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_GROUP_24)	7B B9 38 67 D7 6C 8D 80 DF 0F 40 FA E8 FC 3B 19 00 00 00 06	Windows 8 and later, and Windows Server 2012 and later
	AuthIP Initiator DH type sent in KE	“AUTHIP_INIT_KE_DH_GROUP” + Diffie Hellman group (IKEEXT_DH_GROUP_MAX)	7B B9 38 67 D7 6C 8D 80 DF 0F 40 FA E8 FC 3B 19 00 00 00 07	Windows 8 and later, and Windows Server 2012 and later
	Microsoft Xbox One 2013	"Microsoft Xbox One 2013"	8A A3 94 CF 8A 55 77 DC 31 10 C1 13 B0 27 A4 F2	Windows 10 and Windows Server 2016
	Xbox IKEv2 Negotiation	"Xbox IKEv2 Negotiation"	66 08 22 B3 A7 3A 24 41 49 57 8D 62 E0 EB 46 A0	Windows 10 and Windows Server 2016

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>Security Realm ID</td><td>"MSFT IPsec Security Realm Id"</td><td>68 6A 8C BD FE 63 4B 40 51 46 FB 2B AF 33 E9 E8</td><td>Windows 10 and Windows Server 2016</td></tr>
</table>
<table>
<tr><th>Keying Module</th><th>4-Byte Value</th></tr>
<tr><td>IKEEXT_KEY_MODULE_IKE</td><td>00 00 00 00</td></tr>
<tr><td>IKEEXT_KEY_MODULE_AUTHIP</td><td>00 00 00 01</td></tr>
<tr><td>IKEEXT_KEY_MODULE_IKEV2</td><td>00 00 00 02</td></tr>
</table>
<table>
<tr><th>DH Group</th><th>4-Byte Value</th></tr>
<tr><td>IKEEXT_DH_GROUP_NONE</td><td>00 00 00 00</td></tr>
<tr><td>IKEEXT_DH_GROUP_1</td><td>00 00 00 01</td></tr>
<tr><td>IKEEXT_DH_GROUP_2</td><td>00 00 00 02</td></tr>
<tr><td>IKEEXT_DH_GROUP_14 /
IKEEXT_DH_GROUP_2048</td><td>00 00 00 03</td></tr>
<tr><td>IKEEXT_DH_ECP_256</td><td>00 00 00 04</td></tr>
<tr><td>IKEEXT_DH_ECP_384</td><td>00 00 00 05</td></tr>
<tr><td>IKEEXT_DH_GROUP_24</td><td>00 00 00 06</td></tr>
<tr><td>IKEEXT_DH_GROUP_MAX</td><td>00 00 00 07</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD