[MS-GKDI]: Group Key Distribution Protocol

This topic lists Errata found in [MS-GKDI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications. RSS

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

Errata below are for Protocol Document Version V8.0 - 2021/06/25.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2023/08/16</td><td>
<p>Section 2.2.4 Group Key Envelope</p>
<p>Description: In the Group Key Envelope structure, updated the 'IsPublicKey' field by renaming it to 'dwFlags' and specifying bit settings that enable this structure to transport a public key or to be used for encrypting new data.</p>
<p>Changed from:</p>
<table>
<tr><th colspan="4">Version</th></tr>
<tr><td>0x4B</td><td>0x44</td><td>0x53</td><td>0x4B</td></tr>
<tr><td colspan="4">IsPublicKey</td></tr>
</table>
<p>Changed to:</p>
<table>
<tr><th colspan="4">Version</th></tr>
<tr><td>0x53</td><td colspan="3"></td></tr>
<tr><td colspan="4">dwFlags</td></tr>
</table>
<p>Changed from:</p>
<p>"IsPublicKey (4 bytes): A 32-bit unsigned integer. This field MUST be set to 1 when this structure is being used to transport a public key, and otherwise set to 0. This field is encoded using little-endian format."</p>
<p>Changed to:</p>
<p>"dwFlags (4 bytes): A 32-bit unsigned integer. Bit 31 (LSB) MUST be set to 1 when this structure is being used to transport a public key, and otherwise set to 0. Bit 30, when set to 1, indicates that this key can be used for encrypting new data. This field is encoded using little-endian format."</p>
</td></tr>
<tr><td>2023/08/16</td><td>
<p>Section 2.2.4 Group Key Envelope: Changed isPublicKey to dwFlags and updated requirements for usage of bit 31 to indicate public key transportation and bit 30 to indicate the use of encryption.</p>
<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>20</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>30</th><th>1</th></tr>
<tr><td colspan="32">Version</td></tr>
<tr><td colspan="8">0x4B</td><td colspan="8">0x44</td><td colspan="8">0x53</td><td colspan="8">0x4B</td></tr>
<tr><td colspan="32">isPublicKey</td></tr>
<tr><td colspan="32">... etc...</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>. . .
isPublicKey (4 bytes): A 32-bit unsigned integer. This field MUST be set to 1 when this structure is being used to transport a public key, and otherwise set to 0. This field is encoded using little-endian format.
. . .
cbL1Key (4 bytes): A 32-bit unsigned integer. This field MUST be the length, in bytes, of the L1 key field. This field is encoded using little-endian format. This field MUST be set to zero if the isPublicKey field is set to 1, or if the L1 index field is set to zero and the value in the L2 index field is not equal to 31.
. . .
L2 key (variable, optional): The L2 seed key ADM element or the group public key ADM element with group key identifier (L0 index, L1 index, L2 index) in binary form. If the value in the cbL2Key field is zero, this field is absent. If this field is present and the isPublicKey field is set to 1, then the length, in bytes, of this field MUST be equal to the value of the Public Key Length field. If this field is present and the isPublicKey field is set to 0, the length of this field MUST be equal to 64 bytes.
Changed to:
<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>20</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>30</th><th>1</th></tr>
<tr><td colspan="32">Version</td></tr>
<tr><td colspan="8">0x4B</td><td colspan="8">0x44</td><td colspan="8">0x53</td><td colspan="8">0x4B</td></tr>
<tr><td colspan="32">dwFlags</td></tr>
<tr><td colspan="32">... etc...</td></tr>
</table>
. . .
dwFlags (4 bytes): A 32-bit unsigned integer. Bit 31 (LSB) MUST be set to 1 when this structure is being used to transport a public key, otherwise set to 0. Bit 30 MUST be set to 1 when the key being transported by this structure might be used for encryption and decryption, otherwise it should only be used for decryption. This field is encoded using little-endian format.
. . .
cbL1Key (4 bytes): A 32-bit unsigned integer. This field MUST be the length, in bytes, of the L1 key field. This field is encoded using little-endian format. This field MUST be set to zero if bit 31 of the dwFlags field is set to 1, or if the L1 index field is set to zero and the value in the L2 index field is not equal to 31.
. . .
L2 key (variable, optional): The L2 seed key ADM element or the group public key ADM element with group key identifier (L0 index, L1 index, L2 index) in binary form. If the value in the cbL2Key field is zero, this field is absent. If this field is present and bit 31 of the dwFlags field is set to 1, then the length, in bytes, of this field MUST be equal to the value of the Public Key Length field. If this field is present and bit 31 of the dwFlags field is set to 0, the length of this field MUST be equal to 64 bytes.

Section 3.2.4.1 Client Side Processing: Changed isPublicKey to bit 31 of the dwFlags field.
Changed from:
If the client successfully retrieves a key from the server, it will have received a group key in the format specified in section 2.2.4. The client MUST parse this format as follows:
1. If the isPublicKey field of the returned Group Key Envelope is set to 1, the value in the L2 key field is a public key with group key identifier (L0 field, L1 field, L2 field).
2. If the isPublicKey field of the returned Group Key Envelope is set to 0 and the L2 Key field is present, the value in the L2 key field is an L2 seed key with group key identifier (L0 field, L1 field, L2 field).</td></tr>
</table>

Errata Published*	Description
	3. If the isPublicKey field of the returned Group Key Envelope is set to 0 and the L1 Key field is present, then: Changed to: If the client successfully retrieves a key from the server, it will have received a group key in the format specified in section 2.2.4. The client MUST parse this format as follows: 1. If bit 31 of the dwFlags field of the returned Group Key Envelope is set to 1, the value in the L2 key field is a public key with group key identifier (L0 field, L1 field, L2 field). 2. If bit 31 of the dwFlags field of the returned Group Key Envelope is set to 0 and the L2 Key field is present, the value in the L2 key field is an L2 seed key with group key identifier (L0 field, L1 field, L2 field). 3. If bit 31 of the dwFlags field of the returned Group Key Envelope is set to 0 and the L1 Key field is present, then:

*Date format: YYYY/MM/DD