[MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting

<table>
<tr><td>This topic lists the Errata found in [MS-RDPBCGR] 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.</td><td>RSS

Atom</td></tr>
</table>

Errata below are for Protocol Document Version V8.0 – 2019/03/13.

Errata Published*	Description
2020/08/17	In Section 2.2.1.4.4 Server Network Data (TS_UD_SC_NET), we updated the channelIdArray description to remove inaccurate information. Changed from: channelIdArray (variable): A variable-length array of MCS channel IDs (each channel ID is a 16-bit, unsigned integer) which have been allocated (the number is given by the channelCount field). Each MCS channel ID corresponds in position to the channels requested in the Client Network Data structure. A channel value of 0 indicates that the channel was not allocated. Changed to: channelIdArray (variable): A variable-length array of MCS channel IDs (each channel ID is a 16-bit, unsigned integer) which have been allocated (the number is given by the channelCount field). Each MCS channel ID corresponds in position to the channels requested in the Client Network Data structure.
2020/08/17	In Section 2.2.1.3.4.1 Channel Definition Structure (CHANNEL_DEF), modified the meaning of the CHANNEL_OPTION_INITIALIZED flag to indicate that the flag is unused and MUST be ignored by the server. Changed from: CHANNEL_OPTION_INITIALIZED 0x80000000 Absence of this flag indicates that this channel is a placeholder and that the server MUST NOT set it up. Changed to: CHANNEL_OPTION_INITIALIZED 0x80000000 This flag is unused and its value MUST be ignored by the server.
2020/07/20	In Section 2.2.10.1.1.4.1.1, Logon Errors Info (TS_LOGON_ERRORS_INFO), added the LOGON_MSG_SESSION_BUSY_OPTIONS notification type. Changed from:

Errata Published*	Description
	ErrorNotificationType (4 bytes): A 32-bit, unsigned integer that specifies an NTSTATUS value (see [ERRTRANS] for information about translating NTSTATUS error codes to usable text strings), or one of the following values. **Value** / **Meaning** LOGON_MSG_DISCONNECT_REFUSED 0xFFFFFFF9 / The "Disconnection Refused" dialog is being displayed by Winlogon. The session identifier is specified by the ErrorNotificationData field. Changed to: ErrorNotificationType (4 bytes): A 32-bit, unsigned integer that specifies an NTSTATUS value (see [ERRTRANS] for information about translating NTSTATUS error codes to usable text strings), or one of the following values. **Value** / **Meaning** LOGON_MSG_SESSION_BUSY_OPTIONS 0xFFFFFFF8 / The "Session is Busy" dialog is being displayed by Winlogon. The session identifier is specified by the ErrorNotificationData field. LOGON_MSG_DISCONNECT_REFUSED 0xFFFFFFF9 / The "Disconnection Refused" dialog is being displayed by Winlogon. The session identifier is specified by the ErrorNotificationData field.

2020/07/06	In Section 2.2.17.4, RDSTLS Authentication Response PDU, revised ResultCode description to match definition – 16-bit to 32-bit unsigned integer.
	
	Changed from:
	
	ResultCode (4 bytes): A 16-bit unsigned integer that specifies the user authentication result.
	
	Changed to:
	
	ResultCode (4 bytes): A 32-bit unsigned integer that specifies the user authentication result.
	
	In Section 4.1.3, Client MCS Connect Initial PDU with GCC Conference Create Request, revised comment for TS_UD_CS_CORE::connectionType.
	
	Changed from:
	
	`00 -> TS_UD_CS_CORE::connectionType = 0 (not used as RNS UD CS VALID CONNECTION TYPE not set)`
	`00 -> TS_UD_CS_CORE::pad1octet`
	
	Changed to:
	
	`00 -> TS UD CS CORE::connectionType = 0 (ignored as RNS_UD_CS_VALID_CONNECTION_TYPE not set)`

Errata Published*	Description
	``
00 -> TS_UD_CS_CORE::pad1octet
```

In Section 4.1.14, Client Synchronize PDU, revised annotated dump to match revision made in section 2.2.17.4.

Changed from:

```
00 01 ->TS_SYNCHRONIZE_PDU::messageType = SYNCMSGTYPE_SYNC (1)
ea 03 ->TS_SYNCHRONIZE_PDU::targetUser = 0x03ea
```

Changed to:

```
01 00 ->TS_SYNCHRONIZE_PDU::messageType = SYNCMSGTYPE_SYNC (1)
ea 03 ->TS_SYNCHRONIZE_PDU::targetUser = 0x03ea
``` |
| 2020/07/06 | In Section 4.1.12, Server Demand Active PDU, revised annotated dump – pad1octet to drawingFlags & pad2octetsB to orderSupportExFlags.

Changed from:

```
00 -> TS_BITMAP_CAPABILITYSET::highColorFlags = 0
00 -> TS_BITMAP_CAPABILITYSET::pad1octet
01 00 -> TS BITMAP CAPABILITYSET::multipleRectangleSupport = TRUE
00 00 -> TS_BITMAP_CAPABILITYSET::pad2octetsB

Order Capability Set (88 bytes)
```

Changed to:

```
00 -> TS_BITMAP_CAPABILITYSET::highColorFlags = 0
00 -> TS BITMAP CAPABILITYSET::drawingFlags
01 00 -> TS_BITMAP_CAPABILITYSET::multipleRectangleSupport = TRUE
00 00 -> TS BITMAP CAPABILITYSET::pad2octetsB

Order Capability Set (88 bytes)
```

In that same section, changed from:

```
a1 06 -> TS_ORDER_CAPABILITYSET::textFlags = 0x06a1

00 00 -> TS_ORDER_CAPABILITYSET::pad2octetsB
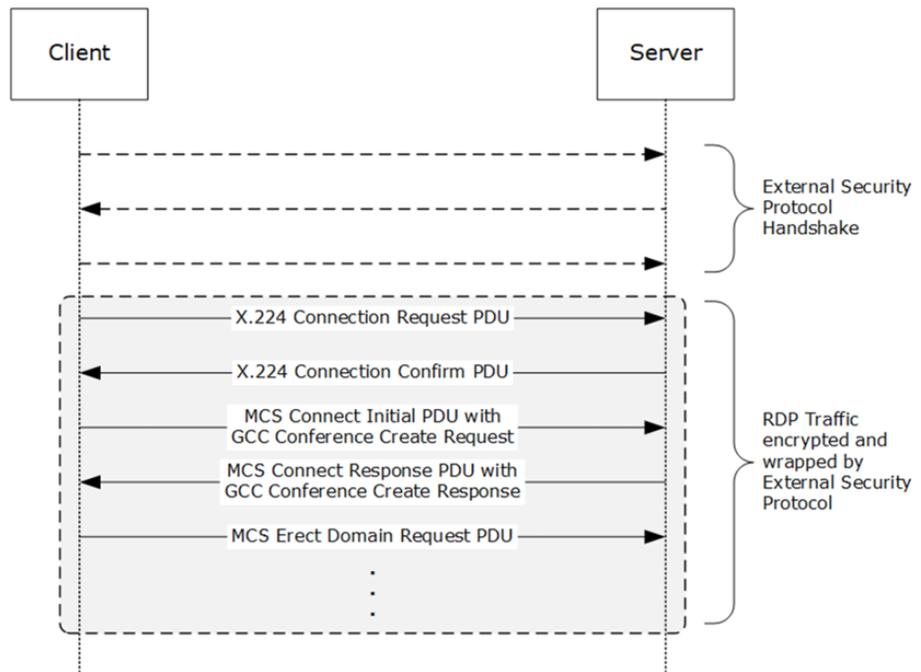40 42 0f 00 -> TS ORDER CAPABILITYSET::pad4octetsB
``` |

Errata Published*	Description
	<pre> 40 42 0f 00 -> TS_ORDER_CAPABILITYSET::desktopSaveSize = 0xf4240 = 1000000</pre>Changed to:<pre> a1 06 -> TS_ORDER_CAPABILITYSET::textFlags = 0x06a1

    00 00 -> TS_ORDER_CAPABILITYSET::orderSupportExFlags
    40 42 0f 00 -> TS_ORDER_CAPABILITYSET::pad4octetsB

    40 42 0f 00 -> TS_ORDER_CAPABILITYSET::desktopSaveSize = 0xf4240 = 1000000</pre>In Section 4.1.13, Client Confirm Active PDU, revised annotated dump – pad2octets to pad2Octets & pad1octet to drawingFlags & pad2octetsB to orderSupportExFlags.

Changed from:<pre>   4d 53 54 53 43 00 -> TS_CONFIRM_ACTIVE_PDU::sourceDescriptor = "MSTSC"

    12 00 -> TS_CONFIRM_ACTIVE_PDU::numberCapabilities = 18
    00 00 -> TS_CONFIRM_ACTIVE_PDU::pad2octets

    General Capability Set (24 bytes)</pre>Changed to:<pre>   4d 53 54 53 43 00 -> TS_CONFIRM_ACTIVE_PDU::sourceDescriptor = "MSTSC"

    12 00 -> TS_CONFIRM_ACTIVE_PDU::numberCapabilities = 18
    00 00 -> TS_CONFIRM_ACTIVE_PDU::pad2Octets

    General Capability Set (24 bytes)</pre>In that same section, changed from:<pre>   00 -> TS_BITMAP_CAPABILITYSET::highColorFlags = 0
    00 -> TS_BITMAP_CAPABILITYSET::pad1octet
    01 00 -> TS_BITMAP_CAPABILITYSET::multipleRectangleSupport = TRUE
    00 00 -> TS_BITMAP_CAPABILITYSET::pad2octetsB

    Order Capability Set (88 bytes)</pre>Changed to:<pre>   00 -> TS_BITMAP_CAPABILITYSET::highColorFlags = 0
    00 -> TS_BITMAP_CAPABILITYSET::drawingFlags
    01 00 -> TS_BITMAP_CAPABILITYSET::multipleRectangleSupport = TRUE
    00 00 -> TS_BITMAP_CAPABILITYSET::pad2octetsB</pre> |

Errata Published*	Description
	``
                    Order Capability Set (88 bytes)

Changed from:

     TS_TEXTFLAGS_ALLOWDELTAXSIM |
     TS TEXTFLAGS CHECKFONTASPECT

   00 00 -> TS ORDER CAPABILITYSET::pad2octetsB
   00 00 00 00 -> TS_ORDER_CAPABILITYSET::pad4octetsB
   00 84 03 00 -> TS_ORDER_CAPABILITYSET::desktopSaveSize = 0x38400 = 230400

Changed to:

     TS_TEXTFLAGS_CHECKFONTASPECT

   00 00 -> TS_ORDER_CAPABILITYSET::orderSupportExFlags
   00 00 00 00 -> TS ORDER CAPABILITYSET::pad4octetsB
   00 84 03 00 -> TS_ORDER_CAPABILITYSET::desktopSaveSize = 0x38400 = 230400
``` In Section 4.1.18, Client Font List PDU, revised annotated dump – numberEntries to numberFonts & totalNumEntries to totalNumFonts & added a couple of lines.<br><br>Changed from:<br><br>```
   00 00 -> TS_SHAREDATAHEADER::compressedLength = 0

   00 00 -> TS_FONT_LIST_PDU::numberEntries = 0
   00 00 -> TS_FONT_LIST_PDU::totalNumEntries = 0
   03 00 -> TS_FONT_LIST_PDU::listFlags = 0x0003 = 0x0002 | 0x0001 =
   FONTLIST LAST | FONTLIST FIRST
   32 00 -> TS_FONT_LIST_PDU::entrySize = 0x0032 = 50 bytes
```<br><br>Changed to:<br><br>```
   00 00 -> TS_SHAREDATAHEADER::compressedLength = 0

   00 00 -> TS_FONT_LIST_PDU::numberFonts = 0
   00 00 -> TS_FONT_LIST_PDU::totalNumFonts = 0

   03 00 -> TS_FONT_LIST_PDU::listFlags = 0x0003
   0x0003
   = 0x0002 | 0x0001
   FONTLIST_LAST | FONTLIST_FIRST

   32 00 -> TS_FONT_LIST_PDU::entrySize = 0x0032 = 50 bytes
```<br><br>In Section 4.4, Annotated Server-to-Client Virtual Channel PUD, revised HEADER to HEADER1. |
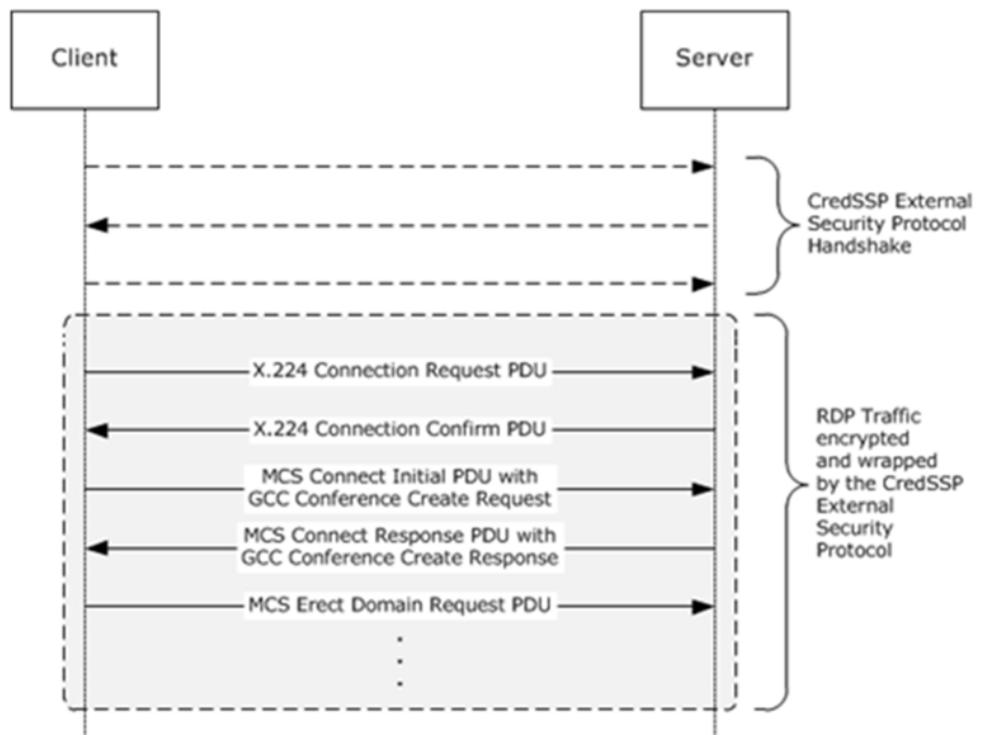
Errata Published*	Description

	Changed from:
	
	``` 01 00 -> TS_SECURITY_HEADER::flagsHi - ignored as flags field does not contain SEC_FLAGSHI_VALID (0x8000) 47 bd eb cb 29 51 ae 0a -> TS_SECURITY_HEADER::dataSignature f6 07 33 ce fc a5 f7 09 de 67 4e a3 2a 2c 38 29 -> Encrypted static virtual channel data```
	
	Changed to:
	
	``` 01 00 -> TS SECURITY HEADER::flagsHi - ignored as flags field does not contain SEC_FLAGSHI_VALID (0x8000) 47 bd eb cb 29 51 ae 0a -> TS_SECURITY_HEADER1::dataSignature f6 07 33 ce fc a5 f7 09 de 67 4e a3 2a 2c 38 29 -> Encrypted static virtual channel data```
	
	In Section 4.5, Annotated Standard Security Server Redirection PDU, revised HEADER to HEADER1.
	
	Changed from:
	
	`` = SEC_SECURE_CHECKSUM
		SEC_REDIRECTION_PKT 00 00 -> TS SECURITY HEADER::flagsHi - ignored as flags field does not contain RDP_SEC_FLAGSHI_VALID (0x8000) 58 dd 3f e5 f3 de 80 26 -> TS_SECURITY_HEADER::dataSignature c0 d6 3f 26 0e 2c b5 93 dd 26 d5 4b 84 a1 1d 2a```
		
		Changed to:
		
		`` = SEC_SECURE_CHECKSUM
			SEC_REDIRECTION_PKT 00 00 -> TS_SECURITY_HEADER::flagsHi - ignored as flags field does not contain RDP_SEC_FLAGSHI_VALID (0x8000) 58 dd 3f e5 f3 de 80 26 -> TS_SECURITY_HEADER1::dataSignature c0 d6 3f 26 0e 2c b5 93 dd 26 d5 4b 84 a1 1d 2a```

2020/07/06	In Section 2.2.4.1, Server Auto-Reconnect Status PDU, revised Client Auto-Reconnection Packet to Client Auto-Reconnect Packet. Changed from: The Auto-Reconnect Status PDU is sent by the server to the client to indicate that automatic reconnection using the Client Auto-Reconnection Packet (section 2.2.4.3), sent as part of the extended information of the Client Info PDU (section 2.2.1.11.1), has failed. Changed to:

Errata Published*	Description
	The Auto-Reconnect Status PDU is sent by the server to the client to indicate that automatic reconnection using the Client Auto-Reconnect Packet (section 2.2.4.3), sent as part of the extended information of the Client Info PDU (section 2.2.1.11.1), has failed.
	In Section 2.2.5.1.1, Set Error Info PDU Data, revised description for ERRINFO_CONTROLPDUSEQUENCE.
	Changed from:
	<table><tr><td>ERRINFO_CONTROLPDUSEQUENCE 0x000010CD</td><td>An out-of-sequence Slow-Path Non-Data PDU (section 2.2.8.1.1.1.1) has been received.</td></tr></table>
	Changed to:
	<table><tr><td>ERRINFO_CONTROLPDUSEQUENCE 0x000010CD</td><td>An out-of-sequence Server Demand Active PDU (section 2.2.1.13.1), Client Confirm Active PDU (section 2.2.1.13.2), Server Deactivate All PDU (section 2.2.3.1) or Enhanced Security Server Redirection PDU (section 2.2.13.3.1) has been received.</td></tr></table>
	In Section 2.2.8.1.1.3.1.1, Slow-Path Input Event, revised definition for slowPathInputData.
	Changed from: slowPathInputData (variable): TS_KEYBOARD_EVENT, TS_UNICODE_KEYBOARD_EVENT, TS_POINTER_EVENT, TS_POINTERX_EVENT, or TS_SYNC_EVENT. The actual contents of the input event specified by the messageType field (sections 2.2.8.1.1.3.1.1.1 through 2.2.8.1.1.3.1.1.6).
	Changed to: slowPathInputData (variable): TS_KEYBOARD_EVENT, TS_UNICODE_KEYBOARD_EVENT, TS_POINTER_EVENT, TS_POINTERX_EVENT, TS_SYNC_EVENT, or TS_UNUSED_EVENT. The actual contents of the input event specified by the messageType field (sections 2.2.8.1.1.3.1.1.1 through 2.2.8.1.1.3.1.1.6).
2020/07/06	In Section 5.4.2.2, Direct Approach, revised the figure.
	Changed from:

Errata Published*	Description
	  Changed to:

Errata Published*	Description
	In that same section, changed from: When using the Direct Approach, no negotiation of the security protocol takes place. The client and server are hard-coded to use the Credential Security Support Provider (CredSSP) Protocol (section 5.4.5) when a connection is initiated. Once the security protocol handshake has completed successfully, the RDP Connection Sequence begins, starting with (a) the X.224 messages which form the Connection Initiation phase (section 1.3.1.1); or (b) the Early User Authorization Result PDU (section 2.2.10.2) followed by the X.224 messages. From this point all RDP traffic is encrypted using the CredSSP External Security Protocol. The RDP Negotiation Request (section 2.2.1.1.1) will still be appended to the X.224 Connection Request PDU (section 2.2.1.1) and the requested protocol list will contain the identifier of the CredSSP protocol (section 2.2.1.1.1). If this is not the case, the server will append an RDP Negotiation Failure (section 2.2.1.2.2) to the X.224 Connection Confirm PDU (section 2.2.1.2) with a failure code of INCONSISTENT_FLAGS (0x04). Similarly, the server will indicate that the hard-coded security protocol is the selected protocol in the RDP Negotiation Response (section 2.2.1.2.1) which is appended to the X.224 Connection Confirm PDU. Changed to: When using the Direct Approach, no negotiation of the security protocol takes place. The client and server are hard-coded to use the Credential Security Support Provider (CredSSP) Protocol (section 5.4.5) when a connection is initiated. The Early User Authorization Result PDU (section 2.2.10.2) is not supported in the Direct Approach. Once the security protocol handshake has completed successfully, the RDP Connection Sequence begins, starting with the X.224 messages which form the Connection Initiation phase (section 1.3.1.1). From this point all RDP traffic is encrypted using the CredSSP External Security Protocol. The RDP Negotiation Request (section 2.2.1.1.1) MUST be appended to the X.224 Connection Request PDU (section 2.2.1.1) and the requested protocol list MUST contain the PROTOCOL_HYBRID (0x00000002) flag identifying the CredSSP protocol (section 2.2.1.1.1). If this is not the case, the server will append an RDP Negotiation Failure (section 2.2.1.2.2) to the X.224 Connection Confirm PDU (section 2.2.1.2) with a failure code of INCONSISTENT_FLAGS (0x04). Similarly, the server MUST indicate that CredSSP is the selected protocol in the RDP Negotiation Response (section 2.2.1.2.1) which is appended to the X.224 Connection Confirm PDU.

*Date format: YYYY/MM/DD