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

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.

RSS
Atom

Errata below are for Protocol Document Version V43.0 – 2016/10/13.

Errata Published*	Description
2017/01/23	In this document: 1) Clarified that Redirection PDU has to contain a variable-length routing token in Section 1.3.8, Server Redirection. 2) Added the PROTOCOL_RDSTLS flag to the requestedProtocols field table in Section 2.2.1.1.1, RDP Negotiation Request (RDP_NEG_REQ), and added the PROTOCOL_RDSTLS value to the selectedProtocol field table in Section 2.2.1.2.1, RDP Negotiation Response (RDP_NEG_RSP). 3) Added RedirectionGuidLength, RedirectionGuid, TargetCertificateLength, and TargetCertificate fields; and added LB_PASSWORD_IS_PK_ENCRYPTED, LB_REDIRECTION_GUID, and LB_TARGET_CERTIFICATE to the RedirFlags field table in Section 2.2.13.1, Server Redirection Packet (RDP_SERVER_REDIRECTION_PACKET). 4) Added the RDSTLS external security protocol to Section 5.4, Enhanced RDP Security. 5) Added the following new sections: 1.3.8.1 RDSTLS 2.2.17 RDSTLS PDUs 2.2.17.1 RDSTLS Capabilities PDU 2.2.17.2 RDSTLS Authentication Request PDU with Password Credentials 2.2.17.3 RDSTLS Authentication Request PDU with Auto-Reconnect Cookie 2.2.17.4 RDSTLS Authentication Response PDU 5.4.5.3 RDSTLS Security 5.4.5.3.1 RDSTLS Connection Sequence For details on these changes, see the [MS-RDPBCGR] DIFF doc in PDF format here.
2017/01/09	In this document: • Added the normative reference [ITUX691] to Section 1.2.1, Normative References. • Clarified how MCS Send Data Request and MCS Send Data Indication structures avoid implementing ASN.1 PER extended size determinant encoding in Section 2.2, Message Syntax. • Clarified the overall PDU length in the length1 and length2 field descriptions in the following sections: 2.2.8.1.2, Client Fast-Path Input Event PDU (TS_FP_INPUT_PDU) and 2.2.9.1.2, Server Fast-Path Update PDU (TS_FP_UPDATE_PDU). • Replaced instances of "secFlags" field with "flags" field in the following sections: 2.2.8.1.2 Client Fast-Path Input Event PDU (TS_FP_INPUT_PDU) 2.2.9.1.2 Server Fast-Path Update PDU (TS_FP_UPDATE_PDU) 3.2.5.8.1.2 Sending Fast-Path Input Event PDU 3.2.5.9.3 Processing Fast-Path Update PDU 3.3.5.8.1.2 Processing Fast-Path Input Event PDU 3.3.5.9.3 Sending Fast-Path Update PDU

Errata Published*	Description
	4.7 Annotated Fast-Path Input Event PDU In Section 1.2.1, Normative References, changed from: [International] Dr. International, "Developing International Software (2nd Edition)", Microsoft Press, 2003, ISBN: 0735615837. [MS-CSSP] Microsoft Corporation, "Credential Security Support Provider (CredSSP) Protocol". ... Changed to: [International] Dr. International, "Developing International Software (2nd Edition)", Microsoft Press, 2003, ISBN: 0735615837. [ITUX691] ITU-T, "ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER)", Recommendation X.691, July 2002, http://www.itu.int/ITU-T/studygroups/com17/languages/X.691-0207.pdf [MS-CSSP] Microsoft Corporation, "Credential Security Support Provider (CredSSP) Protocol". ... In Section 2.2, Message Syntax, changed from: ... Version 2 MCS Encoding Rules (defined in [T125] section 9) are used when encoding MCS structures defined in [T125]. Changed to: ... Version 2 MCS Encoding Rules (defined in [T125] section 9) are used when encoding MCS structures defined in [T125]. The MCS Send Data Request ([T125] section 11.32) and MCS Send Data Indication ([T125] section 11.33) structures MUST be restricted to 16,383 or fewer bytes in length to avoid implementing ASN.1 Packed Encoding Rules (PER) extended size determinant encoding ([ITUX691] section 10.9.3, excluding 10.9.3.8). In Section 2.2.8.1.2, Client Fast-Path Input Event PDU (TS_FP_INPUT_PDU), changed from: .... fpInputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Three pieces of information are collapsed into this byte: • Security flags • Number of events in the fast-path input PDU • Action code The format of the fpInputHeader byte is described by the following bitmask diagram. 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action numEvents secFlags ...

Errata Published*	Description
	secFlags (2 bits): A 2-bit, unsigned integer that contains the flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). ... Changed to: .... fpInputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Three pieces of information are collapsed into this byte: • Security flags • Number of events in the fast-path input PDU • Action code The format of the fpInputHeader byte is described by the following bitmask diagram. 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action numEvents flags ... flags (2 bits): A 2-bit, unsigned integer that contains the flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes. length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes. In Section 2.2.9.1.2, Server Fast-Path Update PDU (TS_FP_UPDATE_PDU), changed from: ... fpOutputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Two pieces of information are collapsed into this byte:

Errata Published*	Description
	• Security flags • Action code The format of the fpOutputHeader byte is described by the following bitmask diagram. 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action reserved secFlags ... secFlags (2 bits): A 2-bit, unsigned integer that contains flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). ... Changed to: ... fpOutputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Two pieces of information are collapsed into this byte: • Security flags • Action code The format of the fpOutputHeader byte is described by the following bitmask diagram. 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action reserved flags ... flags (2 bits): A 2-bit, unsigned integer that contains flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes. length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is

Errata Published*	Description
	set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes. ... In Section 3.2.5.8.1.2, Sending Fast-Path Input Event PDU, changed from: ... If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level (section 5.3.1) and Encryption Method selected by the server as part of the negotiation described in section 5.3.2), using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded secFlags field of the fpInputHeader field MUST contain the FASTPATH_INPUT_ENCRYPTED (2) flag. ... Changed to: ... If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level (section 5.3.1) and Encryption Method selected by the server as part of the negotiation described in section 5.3.2), using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded flags field of the fpInputHeader field MUST contain the FASTPATH_INPUT_ENCRYPTED (2) flag. ... In Section 3.2.5.9.3, Processing Fast-Path Update PDU, changed from: ... If the embedded secFlags field of the fpOutputHeader field contains the FASTPATH_OUTPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data cannot be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_OUTPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol provider. ... Changed to: ... If the embedded flags field of the fpOutputHeader field contains the FASTPATH_OUTPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data cannot be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_OUTPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol provider. ... In Section 3.3.5.8.1.2, Processing Fast-Path Input Event PDU, changed from: ... If the embedded secFlags field of the fpInputHeader field contains the FASTPATH_INPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data cannot

Errata Published*	Description

	be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_INPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol Provider.
	...
	
	Changed to:
	...
	If the embedded flags field of the fpInputHeader field contains the FASTPATH_INPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data
	cannot be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_INPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol Provider.
	...
	
	In Section 3.3.5.9.3, Sending Fast-Path Update PDU, changed from:
	...
	If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level and Encryption Method selected by the server as part of the negotiation described in section 5.3.2) using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded secFlags field of the fpOutputHeader field MUST contain the FASTPATH_OUTPUT_ENCRYPTED (2)
	flag.
	...
	
	Changed to:
	...
	If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level and Encryption Method selected by the server as part of the negotiation described in section 5.3.2) using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded flags field of the fpOutputHeader field MUST contain the FASTPATH_OUTPUT_ENCRYPTED (2) flag.
	...
	
	In Section 4.7, Annotated Fast-Path Input Event PDU, changed from:
	
	The following is an annotated dump of a Fast-Path Input Event PDU (section 2.2.8.1.2) that was sent from a Microsoft RDP 5.1 client to a Microsoft RDP 5.1 server.
	
	`00000000 c4 11 30 35 6b 5b b5 34 c8 47 26 18 5e 76 0e de ..05k[.4.G&.^v..`
	`00000010 28 (`
	
	`c4 -> TS_FP_INPUT_PDU::fpInputHeader = 0xc4`
	`Binary of 0xc4 = 11 0001 00`
	`action = FASTPATH_INPUT_ACTION_FASTPATH (0)`
	`numEvents = 1`
	`secFlags = 0x3`
	`0x3`
	`= 0x1 | 0x2`

Errata Published*	Description
	= FASTPATH_INPUT_SECURE_CHECKSUM | FASTPATH_INPUT_ENCRYPTED ... Changed to: The following is an annotated dump of a Fast-Path Input Event PDU (section 2.2.8.1.2) that was sent from a Microsoft RDP 5.1 client to a Microsoft RDP 5.1 server. 00000000 c4 11 30 35 6b 5b b5 34 c8 47 26 18 5e 76 0e de ..05k[.4.G&.^v.. 00000010 28 (c4 -> TS_FP_INPUT_PDU::fpInputHeader = 0xc4 Binary of 0xc4 = 11 0001 00 action = FASTPATH_INPUT_ACTION_FASTPATH (0) numEvents = 1 flags = 0x3 0x3 = 0x1 | 0x2 = FASTPATH_INPUT_SECURE_CHECKSUM | FASTPATH_INPUT_ENCRYPTED ...
2016/10/13	In this document: • Added RDP version 10.2 to multiple sections and product behavior notes. • Clarified that only RDP 8.0 and 8.1 servers support the RDP-UDP FEC lossy transport. • Added the INFO_RESERVED1 flag to the flags field table. • Updated the meaning for flag NEGRSP_FLAG_RESERVED in the flags field table. • Updated the meaning for flags PERF_RESERVED1 and PERF_RESERVED2 in the performance flags field table. For details on these changes, see the [MS-RDPBCGR] DIFF doc in PDF format here.

*Date format: YYYY/MM/DD