[MS-CSSP]: Credential Security Support Provider (CredSSP) Protocol

This topic lists the Errata found in the MS-CSSP 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 V17.0 – 2018/09/12.

Errata Published*	Description
2020/07/06	In 9 sections - Section 2, Message Syntax, through Section 2.2.1.2.3.1, TSRemoteGuardPackageCred - added behavior notes to indicate character encoding and each data type with ASN.1 data type in each field as unsigned integer encoded as ASN.1 INTEGER or ASN.1 OCTET STRING. Added the following Product Note in or after each introduction: <n> Where data is a text string, Windows uses a Unicode string defined by a UNICODE_STRING structure to encode to ASN.1 OCTET STRING format. For more information see [MSDOCS-UNICODE_STRING]. For a description of Octet String see [MS-DTYP] and [X690].
2020/07/06	In Section 2.2.1,TSRequest, added a product behavior note that TLS requires messages only be fragmented at TLS's maximum message length. Changed from: . . .The TSRequest message, section 2.2.1, is always sent over the TLS-encrypted channel between the client and server in a CredSSP Protocol exchange (see step 1 in section 3.1.5). Changed to: . . .The TSRequest message, section 2.2.1, is always sent over the TLS-encrypted channel between the client and server in a CredSSP Protocol exchange (see step 1 in section 3.1.5).<8> <8> Section 2.2.1: The CredSSP standard requires that a TLS encrypted message fragment contain an entire ASN.1 message. CredSSP expects that the entire first tag and length to fall in the initial block of decrypted data and for the client to encrypt TSRequest messages as single blocks subject only to fragmentation at TLS's maximum message length. The CredSSP server expects a TLS encryption of an entire TSRequest message without fragmentation. Otherwise, the server returns an error.
2020/07/06	In Section 3.1.5, Processing Events and Sequencing Rules, added to step 1 that TLS session resumption is not supported. Changed from: 1. The CredSSP client and CredSSP server first complete the TLS handshake, as specified in [RFC2246]. After the handshake is complete, all subsequent CredSSP Protocol messages are encrypted by the TLS channel. The CredSSP Protocol does not extend the TLS wire protocol. As part of the TLS handshake, the CredSSP server does not request the client's X.509 certificate (thus far, the client is anonymous). Changed to:

Errata Published*	Description
	1. The CredSSP client and CredSSP server first complete the TLS handshake, as specified in [RFC2246]. After the handshake is complete, all subsequent CredSSP Protocol messages are encrypted by the TLS channel. The CredSSP Protocol does not extend the TLS wire protocol. TLS session resumption is not supported. As part of the TLS handshake, the CredSSP server does not request the client's X.509 certificate (thus far, the client is anonymous).
2020/06/08	In Section 2.2.1.2.3.1, TSRemoteGuardPackageCred, clarified data structures and processing in product note 12. Changed from: In Windows, logon credentials (in the logonCred field of TSRemoteGuardCreds) are required in the KERB_TICKET_LOGON structure where the KRB_CRED message ([RFC4120], section 5.8.1) in the TicketGrantingTicket member is using the KERB_RPC_ENCRYPTION_KEY ([MS-RDPEAR] section 2.2.1.2.1) for the EncryptionKey. Supplemental credentials (in the supplementalCreds field of TSRemoteGuardCreds) are required in the following structure: Changed to: In Windows, the logon credentials that are in the logonCred field of TSRemoteGuardCreds structure are required to be in a KERB_TICKET_LOGON structure ([KERB-TICKET-LOGON]). The TicketGrantingTicket member within the KERB_TICKET_LOGON structure is an ASN.1-encoded KRB_CRED message ([RFC4120], section 5.8.1). The EncryptionKey in KrbCredInfo ([RFC4120], section 5.8.1) is required to be in a KERB_RPC_ENCRYPTION_KEY structure ([MS-RDPEAR] section 2.2.1.2.1). The ServiceTicket member within the KERB_TICKET_LOGON structure is a ticket to the computer account. Windows CredSSP clients will use Kerberos User to User tickets ([RFC4120], section 2.9.2) as the ServiceTicket, but the server does not enforce this. The session key of the ServiceTicket is used to encrypt the EncryptedData in the KRB_CRED message.

*Date format: YYYY/MM/DD