[MS-NKPU]: Network Key Protector Unlock Protocol

This topic lists the Errata found in [MS-NKPU] 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 V7.0 – 2017/09/15.

Errata Published*	Description
2017/10/02	In Section 2.2.1.2, DHCPv6 Vendor Specific Information Option Structure, updated the Option-Len and Option-Data field definitions. Changed from: … Encrypted Buffer Suboption: Opt-Code (2 bytes): This field MUST be set to 2 (0x0002). Option-Len (2 bytes): In the client request, this field MUST be set to 256 (0x0100), which is the length of the KP ADM element data. In the server response, this field MUST be set to 32 (0x20), which is the length of the CK ADM element data encrypted with the SK ADM element content. Option-Data: In a client request, this field contains the KP ADM element data. In a server response, this field contains the CK ADM element data that is encrypted with the SK ADM element content by using the AES-CCM [FIPS197] [RFC3610] mode of encryption without authentication data and 16 bytes of MAC that precedes 32 bytes of encrypted result. The nonce used is 12 bytes, all zeros, and is not transmitted. Changed to: … Encrypted Buffer Suboption: Opt-Code (2 bytes): This field MUST be set to 2 (0x0002). Option-Len (2 bytes): In the client request, this field MUST be set to 256 (0x0100), which is the length of the KP ADM element data as specified in section 3.1.1. In the server response, this field MUST be set to the length of the KPR ADM element as specified in section 3.2.1. Option-Data: In a client request, this field contains the KP ADM element data. In a server response, this field contains the KPR ADM element. In Section 2.2.1.4, DHCPv4 Vendor Specific Information Option Structure, updated the Suboption Length and Suboption Data field definitions. Changed from: … Encrypted Buffer Suboption: Suboption Code (1 byte): This field MUST be set to 2 (0x02). Suboption Length (1 byte): In the client request, this field MUST be set to 128 (0x80), which is half the length of the KP ADM element data. In the server response, this field MUST be set to 32 (0x20), which is the length of the CK ADM element data encrypted with the SK ADM element content. Suboption Data: In a client request, this field contains the first 128 bytes of the KP ADM element data. In a server response, this field contains the CK ADM element data that is encrypted with the SK ADM element data by using the AES-CCM

Errata Published*	Description
	[FIPS197] [RFC3610] mode of encryption without authentication data and 16 bytes of MAC that precedes 32 bytes of encrypted result. The nonce used is 12 bytes, all zeros, and is not transmitted. Changed to: … Encrypted Buffer Suboption: Suboption Code (1 byte): This field MUST be set to 2 (0x02). Suboption Length (1 byte): In the client request, this field MUST be set to 128 (0x80), which is half the length of the KP ADM element data as specified in section 3.1.1. In the server response, this field MUST be set to the length of the KPR ADM element as specified in section 3.2.1. Suboption Data: In a client request, this field contains the first 128 bytes of the KP ADM element data. In a server response, this field contains the KPR ADM element. In Section 3.1.1, Abstract Data Model, updated the definition of the Client Key (CK) ADM element. Changed from: … NKPU clients also maintain the following state: Client Key (CK): This is the key that the client expects the server to return in this protocol. It is RSA-encrypted [RFC3447] with the PK ADM element content in the KP ADM element data that is sent to the server in the NKPU client request, and is AES-CCM [FIPS197] [RFC3610] encrypted with the 256-bit SK ADM element content in the server response received by the client. … Changed to: … NKPU clients also maintain the following state: Client Key (CK): The key data that the client sends to the server in the KP ADM element and expects the server to return in the KPR ADM element (section 3.2.1). It is RSA-encrypted [RFC3447] with the PK ADM element content in the KP ADM element data that is sent to the server in the NKPU client request, and is AES-CCM [FIPS197] [RFC3610] encrypted with the 256-bit SK ADM element content in the KPR server response received by the client. … In Section 3.2.1, Abstract Data Model, added the definition for the Key Protector Response (KPR) ADM element. Changed from: … NKPU servers also maintain the following state: Public Key (PK): As defined in section 3.1.1. … Changed to: … NKPU servers also maintain the following state:

Errata Published*	Description
	Key Protector Response (KPR): The key data that the server returns to the client, encrypted with the SK ADM element (section 3.1.1) content by using the AES-CCM [FIPS197], [RFC3610], mode of encryption. The server uses AES-CCM to encrypt the concatenation of an implementation-specific<2> header and the CK ADM element (section 3.1.1) and to produce the MAC. When calling AES-CCM, there is no authentication data and the nonce used is 12 bytes, all zeros, and is not transmitted. The KPR is the encrypted output prepended with the 16-byte MAC. Public Key (PK): As defined in section 3.1.1. … In the following sections, replaced the CK ADM element with the KPR ADM element in the server response. 3.2.5.1 Sending a DHCPv4 BOOTREPLY for NKPU 3.2.5.2 Sending a DHCPv6 Reply for NKPU 3.2.5.3 Receiving a DHCPDISCOVER Message for NKPU 3.2.5.4 Receiving a DHCPv6 Information-Request Message for NKPU In the following sections, updated the examples for server response with the KPR ADM element. 4.1 Client Requesting Unlock over DHCPv4 4.2 Client Requesting Unlock Over DHCPv6 For details on these changes, see the Diff document: [MS-NKPU].PDF.

*Date format: YYYY/MM/DD