3.1.5.4 Encryption Supported

The KDC MUST<14> return in the encrypted part of the AS-REP message PA-DATA with padata-type set to PA-SUPPORTED-ENCTYPES (165), to indicate what encryption types are supported by the KDC. If the server or service has an **msDS-SupportedEncryptionTypes** attribute ([MS-ADA2] section 2.324) populated with supported encryption types, then the KDC MUST<15> return in the encrypted part ([Referrals-11] Appendix A) of AS-REP and TGS-REP message PA-DATA with padata-type set to PA-SUPPORTED-ENCTYPES (165), to indicate what encryption types are supported by the server or service. Else the KDC SHOULD <WB: Supported in Windows Server 2008 and Windows Server 2008 R2.> check the server or service account's userAccountControl attribute ([MS-ADA3] Section 2.341), if the DK bit ([MS-ADTS] Section 2.2.15) is set to:

- TRUE, the KDC SHOULD return 0x3 in the encrypted part ([Referrals-11] Appendix A) of AS-REP and TGS-REP message PA-DATA with padata-type set to PA-SUPPORTED-ENCTYPES (165).
- FALSE, the KDC SHOULD return 0x7 in the encrypted part ([Referrals-11] Appendix A) of AS-REP and TGS-REP message PA-DATA with padata-type set to PA-SUPPORTED-ENCTYPES (165).

When the client requests a delegation TGT for the application server, the client SHOULD<16>:

- Set the **etype** field of the TGS-REQ to the contents of the ***keytype*** field in the previous TGS-REP to specify the common encryption type.
- Provide a PA-SUPPORTED-ENCTYPES value for padata, based on the encryption types mutually supported by the KDC and the application server for the session key with the delegated TGT. The client uses the KDC encryption types provided in the AS-REP from the KDC and the application server encryption types provided in the previous TGS-REP for the application server.

The KDC SHOULD use the **etype** field for TGT encryption. If the **etype** value that is provided cannot be used by the KDC and a PA-SUPPORTED-ENCTYPES is provided, then the KDC SHOULD use this list to select the strongest encryption type to use with the delegated TGT. See section 3.1.5.2 for the relative strengths of KILE-supported encryption types.

The data in the **msDS-SupportedEncryptionTypes** attribute ([MS-ADA2] section 2.324) and padata-value field contains a 32-bit unsigned integer in **little-endian** format that contains a combination of the following flags and which specifies what encryption types are supported by the server or service. An encryption type is supported if its value is equal to 1.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	E	D	C	B	A

Where the bits are defined as:

Value	Description
A	DES-CBC-CRC
B	DES-CBC-MD5
C	RC4-HMAC
D	AES128-CTS-HMAC-SHA1-96
E	AES256-CTS-HMAC-SHA1-96

All other bits MUST be set to zero and MUST be ignored when they are received.