Feature	Reference	Req. in 4120	Test Software
des-cbc-crc	RFC3961 §6.2.3	MAY	kvno
des-cbc-md4	RFC3961 §6.2.2	MAY	kvno
des-cbc-md5	RFC3961 §6.2.1	SHOULD	kvno
des3-cbc-hmac-sha1-kd	RFC3961 §6.3	SHOULD	gssMonger
aes128-cts-hmac-sha1-96 Implemented	RFC3962 §6	SHOULD	gssMonger
aes256-cts-hmac-sha1-96 Encrypt/Decrypt	RFC3961 §5.3 RFC3962 §6	MUST	gssMonger
aes256-cts-hmac-sha1-96 cipher state chaining	RFC3961 §3	MAY	rsh
aes256-cts-hmac-sha1-96 S2K	RFC3962 §4	MUST	kinit
aes256-cts-hmac-sha1-96 S2K parameters	RFC3962 §4	MUST	
aes256-cts-hmac-sha1-96 PRF	RFC3961 §5.3 RFC3962 §6	MAY	t_prf
crc-32	RFC3961 §6.1.3	MAY	kvno, test vectors
rsa-md4	RFC3961 §6.1.2	MAY	kvno
rsa-md5	RFC3961 §6.1.1	MAY	kvno
rsa-md4-des	RFC3961 §6.2.5	MAY	kvno
rsa-md5-des	RFC3961 §6.2.4	SHOULD	kvno
hmac-sha1-des3-kd	RFC3961 §6.3	SHOULD	gssMonger
hmac-sha1-96-aes128 Implemented	RFC3962 §6	SHOULD	gssMonger
hmac-sha1-96-aes256 Get/Verify MIC	RFC3961 §5.4 RFC3962 §6	MUST	gssMonger

Feature	Reference	Req. in 4120	Test Software
INITIAL, PRE-AUTHENT	RFC4120 §2.1		kinit
HW-AUTHENT	RFC4120 §2.1		PKINIT, SAM
Renewable Tickets	RFC4120 §2.3, §2.9.1		kinit
Postdated Tickets	RFC4120 §2.2, §2.4		kinit
Proxiable Tickets	RFC4120 §2.5	MUST	
Forwardable Tickets	RFC4120 §2.6	MUST	gssMonger
Transited Policy Checking - KDC	RFC4120 §2.7	SHOULD	kvno
Transited Policy Checking - SERVER	RFC4120 §2.7	SHOULD	gssMonger
OK-as-Delegate	RFC4120 §2.8	MAY	gssMonger
AS Exchange – CLIENT	RFC4120 §3.1	MUST	gssMonger
AS Exchange – KDC	RFC4120 §3.1	MUST	KDC
AP Exchange – CLIENT	RFC4120 §3.2	MUST	gssMonger
AP Exchange – SERVER	RFC4120 §3.2	MUST	gssMonger
TGS Exchange – CLIENT	RFC4120 §3.3	MAY	gssMonger
TGS Exchange – KDC	RFC4120 §3.3	MUST	KDC
KRB-SAFE (timestamp) – SENDER	RFC4120 §3.4	MAY	kprop
KRB-SAFE (timestamp) – RECIPIENT	RFC4120 §3.4	MAY	kpropd
KRB-SAFE (seqno) – SENDER	RFC4120 §3.4	MAY	kprop
KRB-SAFE (seqno) – RECIPIENT	RFC4120 §3.4	MAY	kpropd
KRB-PRIV (timestamp) – SENDER	RFC4120 §3.5	MAY	gssMonger (passwd)?
KRB-PRIV (timestamp) – RECIPIENT	RFC4120 §3.5	MAY	kpasswdd?
KRB-PRIV (seqno) – SENDER	RFC4120 §3.5	MAY	gssMonger (passwd)?
KRB-PRIV (seqno) – RECIPIENT	RFC4120 §3.5	MAY	kpasswdd?
KRB-CRED – SENDER	RFC4120 §3.6	MAY	gssMonger
KRB-CRED – RECIPIENT	RFC4120 §3.6	MAY	gssMonger
U2U – CLIENT	RFC4120 §3.7	MUST	ktalk
U2U – SERVER	RFC4120 §3.7	MUST	ktalk
U2U – KDC	RFC4120 §3.7	MUST	KDC
Cross-Realm (single-hop)	RFC4120 §1.2, §3.3.1		kvno
Cross-Realm (multi-hop)	RFC4120 §1.2, §3.3.1		kvno
Cross-Realm (transited-encoding)	RFC4120 §1.2, §3.3.1		kvno
Directional Addresses	RFC4120 §7.1	SHOULD	
IPv6 Addresses	RFC4120 §7.1		kinit/kvno
UDP Transport - CLIENT	RFC4120 §7.2.1	SHOULD	kinit
UDP Transport - KDC	RFC4120 §7.2.1	MUST	KDC
TCP Transport - CLIENT	RFC4120 §7.2.2	MUST	kinit
TCP Transport - KDC	RFC4120 §7.2.2	MUST	KDC
PA-ENC-TIMESTAMP	RFC4120 §5.2.7.2	MUST	kinit
AD-IF-RELEVANT - KDC	RFC4120 §5.2.6.1		

Feature	Reference	Req. in 4120	Test Software
AD-IF-RELEVANT - SERVER	RFC4120 §5.2.6.1		
AD-KDC-ISSUED	RFC4120 §5.2.6.2		
AD-AND-OR	RFC4120 §5.2.6.3		
AD-MANDATORY-FOR-KDC	RFC4120 §5.2.6.4		
KDC Cross-Realm Referral - KDC	RFC4120 §3.3.1	MAY	kvno
KDC Cross-Realm Referral - CLIENT	RFC4120 §3.3.1	MUST	kvno
Fail on unknown AD	RFC4120 §1.5.1	MUST	
enc-authorization-data	RFC4120 §3.3.1		
subsession keys - SERVER	RFC4120		gssMonger
subsession keys - TGS	RFC4120		kgetcred
accept hmac-sha1-96-aes256 when enctype is aes256-cts-hmac-sha1-96 (AP_REQ)	RFC3961 §5.3	MUST	
accept hmac-sha1-96-aes256 when enctype is aes256-cts-hmac-sha1-96 (KRB_SAFE)	RFC3961 §5.3	MUST	
last-req	RFC4120 §5.4.2		
KRB_ERR_RESPONSE_TOO_BIG	RFC4120 §7.2.1		

Feature	Reference	Req. in 4121	Test Software
use session key (no subkey)	RFC4121 §2		gssMonger-hacked
use initiator-asserted subkey	RFC4121 §2		gssMonger
use acceptor-asserted subkey	RFC4121 §2		gssMonger
Context Establishment	RFC4121 §4.1	MUST	gssMonger
Generation of KRB-ERROR context tokens	RFC4121 §4.1		gssMonger
Credential Delegation	RFC4121 §4.1.1		gssMonger
Mutual Authentication	RFC1964 §1.1.2		gssMonger
Replay Detection	RFC4121 §4.2.1		gssMonger
Sequencing	RFC4121 §4.2.1		gssMonger
Confidentiality	RFC4121 §4.2.4		gssMonger
Channel Bindings	RFC4121 §4.1.1.2	MUST	ftp
Wrap/Unwrap (64K message)	RFC4121 §4.2.4		gssMonger
GetMIC/VerifyMIC (64K message)	RFC4121 §4.2.4		gssMonger
EC	RFC4121 §4.2.3	MUST	gssMonger
RRC	RFC4121 §4.2.5	MUST	gssMonger