[MS-KILE]: Kerberos Protocol Extensions

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.**
- **Copyrights.** modification, any schema, IDL's, or code samples that
- **No Trade Secrets.**
- **Patents.**
- **Trademarks.**

Reservation of Rights.

Tools.

Revision Summary

Date	Revision History	Revision Class	Comments
8;79<7:88(	96B(	((	(96B((
8<7987:88(	96B(	((	(96B((
8=79@7:88(	96(	((	(96((
8>78@7:88(	96 6B(	M (	Z (((((6(
8 7987:88(	96;(	U (	] (((6(
8@79 7:88(	96; 6B(	M (	Z (((((6(
8A7:97:88(	96<(	U (	Z ((((6(
987:>7:88(	:6B(	U (	K (((6(
897:=7:88@(	:6B6B(	M (	Z (((((6(
8;79<7:88@(	:6B(	U (	] (((6(
8>7:87:88@(	;6B(	U (	] (((((6(
8 7:=7:88@(	;6B(	U (	] (((6(
8@7:A7:88@(	<6B(	U (	] (((((6(
987:<7:88@(	<6B(	U (	] (((6(
9:78=7:88@(	=6B(	U (	] (((((6(
8979>7:88A(	=6B(	U (	] (((6(
8:7: 7:88A(	>6B(	U (	] (((((6(
8<7987:88A(	6B(	U (	] (((((6(
8=7::7:88A(	@6B(	U (	] (((((6(
8 78:7:88A(	A6B(	U (	] (((((6(
8@79<7:88A(	A6B(	U (	] (((6(

Contents

1 Introduction

S (X (M (0SQTM1(((((S (V (I (
[(0 =1((cZNK<9: 8e6((((((((
(((4(((4((((((
(((((((**Kerberos principals**6(

Note (((((((S (V (I ([(
0 =1((((((((S (=6(

1.1 Glossary

(((((((cU[5OTW[eB(

Active Directory(
AP exchange(
AS exchange(
Authentication Service (AS)(
authenticator(
authorization data(
directory(
directory service(
distinguished name (DN)(
domain(
fully qualified domain name (FQDN)(
Generic Security Services (GSS)(
Internet host name(
Kerberos principal(
key(
Key Distribution Center (KDC)(
KRB_AP_REQ/KRB_AP_REP(
KRB_AS_REQ/KRB_AS_REP(
KRB_PRIV exchange(
KRB_SAFE exchange(
object identifier (OID)(
objectGuid(
pre-authentication(
privilege attribute certificate (PAC)(
read-only domain controller (RODC)(
realm(
secret key(
Security Support Provider Interface (SSPI)(
service(
service principal(
service principal name (SPN)(
service ticket(
session(
session key(
SRV record(
TGS exchange(
ticket(
ticket-granting service (TGS)(
ticket-granting ticket (TGT)(

(((((((B(

—

context session key:

integrity level:

"RestrictedKrbHost" services:

security package:

ticket session key: **session key** **ticket**

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:

1.2 References

1.2.1 Normative References

dJ[5ZXKMe(U (K 4 Z (X (K (X (M 4R (: 88>6(

dJ[5[N]e(U (K 4 S (X (M B[((] ((K (L (X ([4R (: 88>6(

dJ[5[V Xe(U (K 4 V ((X (0V X1(I (M 4R (: 88>6(

dJ[5[XVOe(U (K 4 [((X (O ([([(I (X (Q (V (U (0[XVMOW1(X (M 4R (: 88>6(

cZ 599e(Z 4S64 (b 4T64 S (X (V (K ((SLK5 O (K 5Z (Z 4R (: 88@4 B7 6 6 7 5 7 5 5 5 5 5 599(

cZNK9A><e(T 4R64 (S ((=(O[[5I XQ(U 4ZNK(9A><4R (9AA>4 B7 6 6 7 7 9A><6 (

cZNK: 99Ae(J 4[64 S (((((ZNK ((Q (Z (T 4JKX(9<4ZNK(: 99A4U (9AA 4 B7 6 6 7 7 : 99A6 (

cZNK: <;e(T 4R64 O ([([(I (X (Q ((: 4] (9 4 ZNK(: <;4R (: 8884 B7 6 6 7 7 : <;6 (

cZNK: <<e(_ 4R64 O ([([(I XQ((: (BK5 4ZNK(: <<4R (: 8884 B7 6 6 7 7 : <<6 (

cZNK: : Ae(a 4N64] N5@4I((N ((Q W98><> 4ZNK(: : A4R (9AA@4 B7 6 6 7 7 : : A6 (

cZNK; A>9e(Z 4S64 M ((K ([((S (= 4ZNK(; A>94 N (: 88=4 B7 6 6 7 7 ; A>96 (

cZNK; A>: e(Z 4S64 I (M ([(0I M[1(M ((S (= 4ZNK(; A>: 4N (: 88=4 B7 6 6 7 7 ; A>: 6 (

cZNK<9: 8e(V 4K64a 4 64P 4[64 (Z 4S64 (S (V (I ([(0 =1 4ZNK(<9: 84R (: 88=4 B7 6 6 7 7 <9: 86 (

cZNK<9: 9e(b 4T64R 4S64 (P 4[64 (S ((=(O ([([(I (X (Q (0O[[5I XQ(U B((: 4ZNK(<9: 94R (: 88=4 B7 6 6 7 7 <9: 96 (

cZNK<==>e(b 4T64 (4J64 X (S (K ((Q (I ((S 4 ZNK(<==>4R (: 88>(B7 6 6 7 7 <==>6 (

cZNK< = e(R 4S64b 4T64 (J 4R64 (ZK<5PUIK(S (M (( ] ((U (_ 4ZNK(< = 4L (: 88>4 B7 6 6 7 7 < = 6 (

cZNK=: <Ae(b 4T64R 4S64 (T 4S64 M (K (K (0MKK1([((X (S (K ((Q (I ((S (0XSQVQ1 4ZNK(=; <A4[(: 88@4 B7 6 6 7 7 =; <A6 (

c >@8e(Q]5 4 I ([(V (W (0I [V691B[((J (V 4 Z (6>@84R (: 88: 4 B7 6 6 7 7 5ZMK5 6>@87 (

Note (((((((6(

c >A8e(Q] 5 4(Q ((5(I [V69(M (Z B([((J (M (
Z (0J MZ14(K (M (Z (0KMZ1((L (M (Z (0L MZ1 4(
Z (6>A84(R (: 88: 4(B7 6 6 7 7 5ZMK5 6>A87 (

Note (((((((6(

1.2.2 Informative References

d L L TOe(U (K 4([(J B(K ((L 4([(: 88=4(
B7 6 6 7 7 78=78A7[J 7 6 (

d L NWTL QVOe(U (K 4(K [(N 4(B7 6 6 7 5
7 7 >< < >6 (

d_Q TWO] Me(J 4(J 6((/ 4(64(L ((I ([B(I (L ((N (
[4(N (9AA 4(B7 6 6 7 7 7 6 (

cSI] NUI Ve(S 4(K 64(X 4(Z64((U 6([4(V ([B(X (K (
((X (_ 4([(M 4(X (P 4(: 88: 4(Q] J VB(89; 8<>89A: 6(

dJ[5I XL[e(U (K 4(I (X (L ([([4(R (
: 88>6(

dJ[5[MKWe(U (K 4(([(W 4(L (: 88>6(

dJ[L V5KUX[ZOM e(U (K 4(K [M (N 4(
B7 6 6 7 5 7 7 >< < 0 [6@=16 (

dJ[L V5_ QJL e(U (K 4(_ (Q (U (L 4(
B7 6 6 7 5 7 7 >: =A>; 6 (

cZNK 9=98e(S 4(R64((V 4(K 64((S (V (I ([(0 =1 4(ZNK(
9=984([(9AA; 4(B7 6 6 7 7 9=986 (

cZNK: : : : e(U 4(R64([(I (([(T (0[I [T1 4(ZNK(: : : : 4(W (9AA 4(
B7 6 6 7 7 : : : : 6 (

cZNK: ; A>e(J 5T 4(64(N 4(Z64((U 4(T64( ] (Z (Q (0] ZQ(B(
O ([4(ZNK(: ; A>4(I (9AA@4(B7 6 6 7 7 : ; A>6 (

d[XVI e(U (K 4(D X V F 4(B7 6 6 7 5
7 7 ; < >A@6 (

d[[XQe(U (K 4([[XQ4(B7 6 6 7 5 7 7 ; @8<A; 6 (

c] VQ(XWL Me((] (K 4( ] (P (X 4(: 88>4(B7 6 6 7(

c]] SI 5O[[I XQe([4(U 64(J 4(R64((U 4(X64( ] ((] (S (I ((
O[[5I XQ4(W (: 8894(B7 6 6 7 7 7 5 5 : 5 5 : 5
8; 6 (

1.3 Protocol Overview

SQTM((((((((((((((**services**(
(((((((6(SQTM(((((S (=(
6(

1.3.1 Security Background

J (SQTM((((4((((0 (96 6 1((((((((((((((6Q ((4((((((((0 (((4(**key**4((1(((((((((((cZNK<9: 8e((96 6(

I (((((((((SQTM((S (=4(((((S (4(((((((S (6([(((0 (96 6 1 4((d L Q TWO] Me((cSI] NUI Ve4((((5 ((((S ((((6(cSI] NUI Ve(((((((((((4(((((((((((6(

N 4(((((cZNK<9: 8e((cZNK<9: 9e4(((((cZNK 9A><e4(cZNK: <; e4((cZNK 9=98e4((((((6(K ((((4((((**Generic Security Services (GSS)**(cZNK: <; e(((S (((O[[(cZNK<9: 9e((6(

1.3.2 Kerberos Network Authentication Service (V5) Synopsis

(S (=(6(S (=((((((((((cZNK<9: 8e((96 9((; 6(

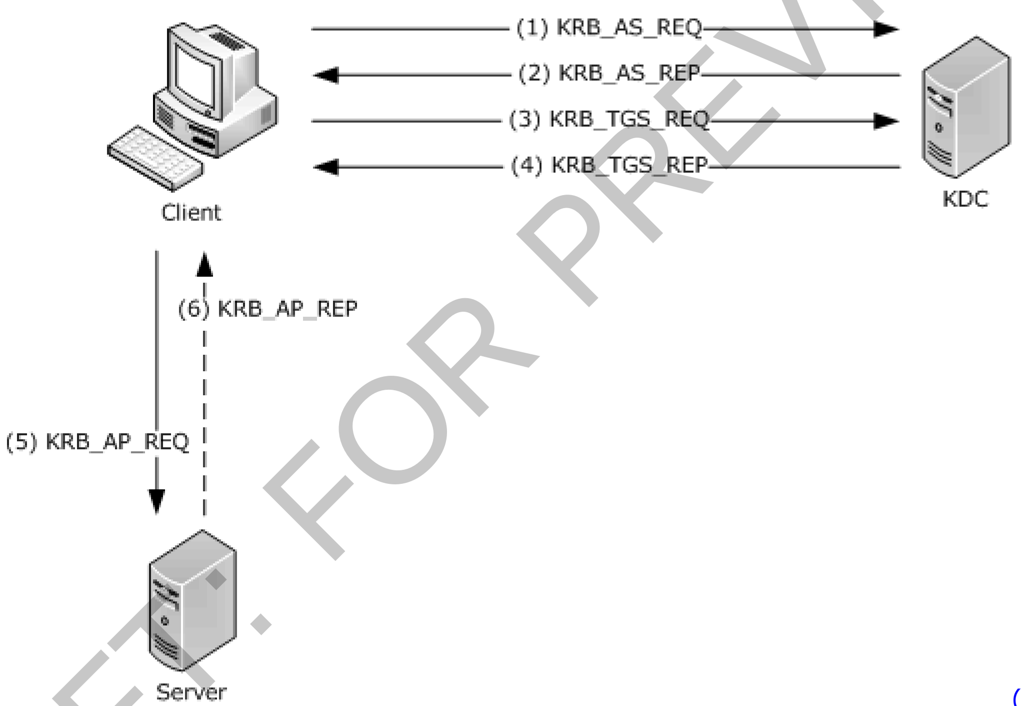


Figure 1: Kerberos V5 Exchanges

Note ((4(((**Key Distribution Center (KDC)**4(((((4(((S (=((((6] ((4((((((((((((((SQTM((((6(

(I ([(0I [1((0cZNK<9: 8e((; 6916(

- S ((((0SZJgI [gZMY1(0cZNK<9: 8e((=6<6916((((((((SLK(((**ticket-granting ticket (TGT)**(0cZNK<9: 8e((=6;16(((((((((5 (6(
- S ((((0SZJgI [gZMX1(0cZNK<9: 8e((=6<6 1B((SLK(((O (((**session key**((((((((((((SLK((**ticket-granting service (TGS)**(4(((((6(

(5O ([(0 O[1((0cZNK<9: 8e((; 6;1B(

- S (5 (((0SZJg O[gZMY1(0cZNK<9: 8e((=6<6916((((((((SLK((((0cZNK<9: 8e((=6;1(((6(((((O (0cZNK<9: 8e((=6;14((**authenticator**(0cZNK<9: 8e((=6=6914(((**Service Principal Name (SPN)**6(
- S (5 (((0SZJg O[gZMX1(0cZNK<9: 8e((=6<6 1B((SLK(((O (0cZNK<9: 8e((=6;1((((0cZNK<9: 8e((=6=6916(Q(((4((SLK((((0cZNK<9: 8e((=6;1(((((((((((6(

(K 7[(I (X (0I X1((0cZNK<9: 8e((; 6 1B(

- S ((((0SZJgI XgZMY1(0cZNK<9: 8e((=6=6916(((((((((((6(((((0cZNK<9: 8e((=6;1(((((0cZNK<9: 8e((=6=6916(((((4((((((**authorization data**(0cZNK<9: 8e((=6 6>1(((((((6(
- S ((((0SZJgI XgZMX1(0cZNK<9: 8e((=6=6 1B(W 4((((((((((((6(Q((((4((((((/(((((((((6(

(**AS exchange**((O[(((((S (6((I X(((((((5 ((((((**AP exchange**(6(I (((I X((((((((6(U (((((O ([([(I (X (Q (OO[[5 I XQ(((((((5 ((((([(I (([(T (O[I [T1(cZNK: : : : e4((((((((((6(

1.3.3 KILE Synopsis

J (((((0cZNK<9: 8e((=6 6>14(SQTM((((((((B(

- O ((
- Q (((
- Q ((

J (((SLK/((4(SQTM((((((((((((((((((((L (M ([(O L M[1(6(

P (((((**Privilege Attribute Certificate (PAC)**(cU[5XI Ke((((((cU[5[MKWe((; 6 6 6 6(

1.4 Relationship to Other Protocols

1.5 Prerequisites/Preconditions

1.6 Applicability Statement

1.7 Versioning and Capability Negotiation

1.7.1 Pre-Authentication

1.7.2 Encryption Types

1.8 Vendor-Extensible Fields

1.9 Standards Assignments

2 Messages

2.1 Transport

2.2 Message Syntax

2.2.1 KERB-PA-PAC-REQUEST

2.2.2 LSAP_TOKEN_INFO_INTEGRITY

LSAP_TOKEN_INFO_INTEGRITY

integrity level

Flags:

Value	Meaning
8 88888888(	N (6(
8 88888889(	] (I (K (0]IK1((6(

TokenIL: I(;:5 ((((((((((6(N (((((4((dU[LV5 QJLe6(((U][(((((6(

Value	Meaning
8 88888888(	] 6(
8 88889888(	T 6(
8 8888:888(	U 6(
8 8888;888(	P 6(
8 8888<888(	[6(
8 8888=888(	X (6(

MachineID: I(;:5 ((((((((((((6(

2.2.3 KERB-AD-RESTRICTION-ENTRY

(SMZJ5IL5ZM[ZQK QJWV5MV Za((((((6D;F(Q (((((I[V6((((((6(

Restriction-TypeB(U][((((8 888888886(

RestrictionB(I (**LSAP_TOKEN_INFO_INTEGRITY**(((((((((6(

2.3 Directory Service Schema Elements Used by Kerberos Protocol Extensions

SQJM(((**directory service**(((((((((6((

N (((((((DK F((DK FDI F(4(((I (L (L ([(0I L(L[1(0dU[5ILI:e4(dU[5ILI;e((dU[5IL[Ke16(

Class	Attribute
(	L[5I L (
L (	L[5[M (

Class	Attribute
(	L[5I L (L[5[M (X V (I K (X V (

—

3 Protocol Details

(((((SQTM4((((((((4((B(

- K (L (0 (; 691(((((6(
- K (L (0 (; 6 1(((((((((I [4(O[4((I X(6(
- SLK(L (0 (; 6 1((((((SLK(((I [((O[(6(
- I ([(L (0 (; 6<1(((((((((I X(6(

3.1 Common Details

3.1.1 Abstract Data Model

S (=((((((((6(

SQTM(((((((B D<F(

- Z (K (
- K (U (
- (K (
- U (QL(

3.1.1.1 Replay Cache

S (=((((U][((((((((((((0 cZNK<9: 8e((; 6 6 16(

SQTM(U][(((((((((((6(

3.1.1.2 Cryptographic Material

S (=((((((((((((SLK(((((...

] (SQTM4(((0 (4(KQN[7[UJ(1(UIa(... (**SSPI**(I XQ6(

((((**EncAPRepPart**(((SZJgI XgZMX(... cZNK9A><e6(...

4((((((((((SZJgI XgZMX(C(((I M[(((0 (
cZNK<9: 9e14((((((((((SZJgI XgZMX([P W] TL((6(0 (
SZJgI XgZMY((((((=6=69((cZNK<9: 8e16(

3.1.1.3 Ticket Cache

S (=((((UI a((O (0cZNK<9: 8e((; 6 6916(

SQTM((((((((((O 6D=F(

3.1.1.4 Machine ID

SQTM((((QL((((((((6(

3.1.2 Timers

V 6(

3.1.3 Initialization

(((((((((((((((
(dNQX[9<8e((<6 696(

3.1.4 Higher-Layer Triggered Events

V 6(

3.1.5 Message Processing Events and Sequencing Rules

((((((((((((((((((
S (6(

3.1.5.1 Pre-authentication Data

X 5 (0cZNK<9: 8e((; 6969 4(=6<69 4((=6 6 1(((((((
S (=(6(X 5 ((((((((5 (
(((XI 5 ((((I [5ZMY(6(

SQTM((((5 ((((0cZNK<9: 8e((6=6 1B(

- XI 5 O[5ZMY(c9e(
- XI 5MVK5 QUM[I U X(c e(
- XI 5M a XM5QVNW(c99e(
- XI 5XS5I [5ZMXg WTL(c9=e(
- XI 5XI K5ZMY] M[(c9: @e(

SQTM((((5 ((((0cZ 599e(I (I 1B(

- XI 5[Z5ZMNMZZI T5QVNW(c: 8e(

] (5 ((U] [((((SLK 6((

—

_ ((((5 ((4((U][(((XI5MVK5
QUM[IUX(5 (((((((I[(6(([PW]TL(
4(((XI5XIK5ZMY]M[(5 (4(((((
0XIK1(((((6(SQTM(B(

- X (S (K ((Q (I ((S (0XSQVQ1(cZNK<==>e6(
- X (S (K ((Q (I (0XSQVQ1((S (X ([(
  cU[5XSKIe6(
- MKK(((XSQVQ(cZNK=;<Ae6(D>F(

Q((SLK(((((5 ((((I[(4(((
U][(((((6((((((5 (((
6(

SQTM((((5 (4(XI5[]XXWZ MLgMVK aXM[4(((((
;6966<6(

3.1.5.2 Encryption Types

SQTM(U][(((I (M ([(QIM[1((((UIaD F((
((((4(((((((B(

- IM[:=>5K [5PUIK5[PI95A>(c9 e(0cZNK;A>:e((1D@F(
- IM[9:@5K [5PUIK5[PI95A>(c9@e(0cZNK;A>:e((1DAF(
- ZK<5PUIK(c ;e(cZNK< = e(
- ZK<5PUIK5M X(c <e(cZNK< = e(
- LM[5KJK5UL=(c;e(cZNK;A>9e(D98F(
- LM[5KJK5KZK(c9e(cZNK;A>9e(D99F(

S (=(((((((cZNK;A>9e((@4(cZNK< = e(
(=4((cZNK;A>:e((6D9:F(

3.1.5.3 Encryption Checksum Types

SQTM(((((6(M ((((4(((((
4((((ZNK6(

- KZK;:(c9e(cZNK;A>9e(
- 5 <(c e(cZNK;A>9e(
- 5 <5 (c;e(cZNK;A>9e(
- 5 (c<e(cZNK;A>9e(
- 5 5(c=e(cZNK;A>9e(
- 5 <5 5(c>e(cZNK;A>9e(
- 5 =(c e(cZNK;A>9e(

_

- 5 =5 (c@e(cZNK; A>9e(
- 9(0 1(c98e(cZNK; A>9e(
- 5 95A>5 9: @(c9=e(cZNK; A>: e(
- 5 95A>5 : =>(c9>e(cZNK; A>: e(
- 5 =5 (c59; @e(cZNK< = e(

3.1.5.4 Encryption Supported

(SLK(U][D9; F((((((((I[5ZMX((XI5LI I((5 (
((XI5[]XXWZ ML5MVK aXM[(09>=14(((((((((
SLK6Q(((((((**msDS-SupportedEncryptionTypes**((0cU[5ILI:e(
(:6j:<1(((((4(((SLK(U][D9<F((((
((0cZ 599e(I (I1((I[5ZMX(0 (((1((O[5ZMX(
(XI5LI I((5 (((XI5[]XXWZ ML5MVK aXM[(09>=14((((
(((((((6(

_ (((((O (((4((([PW]TL D9=F B(

- [(((((O[5ZMY(((((((((O[5ZMX(
((((6(
- X ((XI5[]XXWZ ML5MVK aXM[(4((((((((
((SLK((((((((((O 6((((
(SLK((((((I[5ZMX(((SLK(((((
(((((O[5ZMX((((6(

(SLK([PW]TL(((((O (6Q(((((((((
SLK(((XI5[]XXWZ ML5MVK aXM[((4(((SLK([PW]TL((((((
((((((((O 6[((;696=6(((
((SQTM5 ((6(

((((L[5[M ((0cU[5ILI:e((:6j:<1((5
((((;:5 ((((5 ((((((((
((((((((((((((6(

(8(	(9(	(:(	(;(	(<(	(=(	(>(	((	(@(	(A(	9(8(	(9(	(:(	(;(	(<(	(=(	(>(	((	(@(	(A(	:(8(	(9(	(:(	(;(	(<(	(=(	(>(	((	(@(	(A(	;(8(	(9(
8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	8(	M(	L(	K(	J(	I(

_ (((((B(

Value	Description
I(	LM[5KJK5KZK(
J(	LM[5KJK5UL=(
K(	ZK<5PUIK(
L(	IM[9:@5K [5PUIK5[PI95A>(

_

Value	Description
M(	I M[:=>5K [5PUIK5[PI95A>(

3.1.5.5 Ticket Flag Details

(S (=((((((((((((((
0cZNK<9:8e((:1((((((6(

SQTM(((((B(

- (QVQQT((XZM5I] PMV ((0cZNK<9:8e((:691B(J (4(SLK ((5 ((((6(K ([PW]TL(5 6(SLK(U][((5 6(4((((((((((S (5 4(((((XZM5I] PMV ((6(
- (P_5I] PMV ((0cZNK<9:8e((:691B((((((((5 ((((5 6((((((((S (=(6(SLK(U][(VW(((((((6(SLK([PW]TL(VW((((((((SLK6(
- (ZMVM_IJTM((0cZNK<9:8e((:6;1B(Z (([PW]TL((((SQTM6(
- (XW[LI ML7UIa5XW[LI M((0cZNK<9:8e((:6<1B(X (([PW]TL(VW(((((SQTM6(
- (XZW a7XZW QJJTM((0cZNK<9:8e((:6=1B(X (([PW]TL(VW(((((SQTM6(
- (NWZ_IZLIJTM7NWZ_IZLML((0cZNK<9:8e((:6>1B(N (([PW]TL(((((SQTM6(
- (ZIV[QML5XWTQKa5KPMKSML((0cZNK<9:8e((:61B(SQTM(U][(VW((((((((((SLK6(I ((U][(((ZIV[QML5XWTQKa5 KPMKSML(6(
- (WS5I[5LMTMOI M((0cZNK<9:8e((:6@1B((SLK(U][(((WS5I[5LMTMOI M((((((((((0 (;6696916(N ((4((dILLTOe6(

3.1.5.6 Other Elements and Options

(S (=(((((((0cZNK<9:8e((=6 6>16(

SQTM(((((B(

- ILSI] P5LI I5IX5WX QWV[(0 (;6 6=6 16(
- SMZJgI] PgLI Ig WSMVgZM[ZQK QWV[(0 (;6 6=6((;6<6=6 16(

SQTM([PW]TL(VW((((B(

- (IL5SLK5Q[]ML((0cZNK<9:8e((=6 6>6 16(
- (IL5IVL5WZ((0cZNK<9:8e((=6 6>6 16(
- (IL5UIVLI WZa5NWZ5SLK((0cZNK<9:8e((=6 6>6<16(

SQTM([PW]TL(VW((((((0cZNK<9:8e((96=6916(((
[PW]TL(VW(((C(4([PW]TL((((((((
((6(

SQTM(U][(((SZJgMZZgZM[XWV[Mg WWgJQD(((0cZNK<9:8e((6 6916(

3.1.5.7 Addressing

SQTM(U][((QX>((0cZNK<9:8e((6916D9>F(

SQTM(U][(VW((((0cZNK<9:8e((6916(Q((((
(4((U][((6(

3.1.5.8 Internationalization and Case Sensitivity

(S (=((((((((4(((((
((0cZNK<9:8e((>16(

V (4(((((**domains**4(U][(VW(((((SQTM6(SQTM(U][(
(] N5Q(((((cZNK:: Ae6(V (U][(VW((((
(U][(VW((6 ((4((O _ [S ((0cU[5
]KWLMZMNe((;696=6 6<1(((((VWZUgQDVWZMKI[M4(
VWZUgQDVWZMSIVI aXM4(VWZUgQDVWZMVWV[XIKM4((VWZUgQDVWZM_QL P([PW]TL(((
((K [S ((0cU[5]KWLMZMNe((;696=6 61([PW]TL((((
((6V ((((((C((0 (((((
(((1((((((((0cZNK<9:8e4(cZNK< = e4(
(cZNK;A>:e16(

3.1.5.9 Key Version Numbers

(S (=((((((0cZNK<9:8e((=6 6A16(S ((
(((((S (=(((((((((
6(

SQTM((((((**read-only domain controllers (RODCs)**6(M (ZWLK((
((((((6D9F(((((((((
((((((ZWLK 6(

((((((;:(6(((9>(([PW]TL(((ZWLK(((
(9>(([PW]TL(((((((6(

3.1.5.10 Key Usage Numbers

(S (=((((((0cZNK<9:8e((6=6916((

dU[5SQTMe(((((S (] (V B(

- SMZJgVWVgSMZJg[IT(c9>e(
- SMZJgVWVgSMZJgKS[]Ug[IT(c9 e(

3.1.5.11 Referrals

(S (=(((5**realm**(((((((0cZNK<9:8e(
(96 16(

SQTM(U][((5 ((0cZNK<9:8e((96((;6691((((
cZ 599e6(

3.1.5.12 PAC Generation

(XIK(dU[5XIKe(U][(((((SLK(((((E6(

- L ((I ([(0I[1((((((5 6(
- L ((O[((((O ((((((((((((XIK(((
((((((5 ((O (0cZNK<9:8e((9616(
- L ((O[(((((((6(

(SLK(U][(((/((((((((((XIK(((O 6(

(XIK(U][(((((((((**service ticket**(((
((((((((/(6(

J (4 (SLK(U][(((XIK6P 4(((UIa(((((XIK((
((((((SMZJ5XI5XIK5ZMY]M[(XI5LI I((0:66916(

3.1.6 Timer Events

SQTM((((6(

3.1.7 Other Local Events

SQTM((((6(

3.1.8 Implementing Public Keys

((((((SQTM((((dU[5XSKIe6(

3.2 Client Details

3.2.1 Abstract Data Model

I (((((((IX(4S (=(((((
((6((((U][(((((((((
((((((6((5 (((((
((5 (6(((((((((
((6((((((5 (6(

Note ((((4((((((U][(
((((((((6P ((((((
(((((6(

ChannelBinding: Q ((/((((0cZNK: <;e((9696>(
(cZNK: <<e16(D9@F([(((((IL5I] P5LI I5IX5WX QWV[(((
(((IX5ZMY((0 (;66=616(

Confidentiality: Q ((((((((((((
((((6([((((((O[[gKgKWVNgNTIO(((((
/((0cZNK9A><e((9696((cZNK<9:9e((<6961(

Datagram Style: Q ((((cZNK9A><e4 (((((
(6Q (((((((((

0cZNK<9:8e((;66(((;66<16N ((4((cZNK: <;e((
966696C (S (I (X ((U]]ITSZMY]QZML(0cZNK<9:8e((
;66<(((=6=6916C ((O[[gKgU]]ITgNTIO(0cZNK9A><e((9696916M ((
(4(((((((((((((
(((((((6(

Replay Detect: Q ((((((((((((
((((6[((((((O[[gKgZMXTIagNTIO(
((((/(((0cZNK9A><e((9696969((cZNK<9:9e(
(<6969916(

Sequence Detect: Q ((((((((((
(((((6[((((((O[[gKg[MY]MVKMgNTIO((
(((/(((0cZNK9A><e((9696969((cZNK<9:9e((
<6969916(

Use Session Key: (((((((5 5 ((
(0cZNK<9:8e((;6 16[((((((][M5[M[QWV5SMa((
((((**ap-options**((((IX5ZMY(0cZNK<9:8e((=6=6916(

3.2.2 Timers

_ (((((I[5ZMY((O[5ZMY(((SLK4((((((((
6(((((4(((((4(((((;66>6(

3.2.3 Initialization

J ((((((I[((O[(4((U][(((SLK((((I[((O[(
(((6(K ([PW]TL((**SRV record**((0cZNK<9:8e((66616((
6(_ ([Z (((((((SLK4((((((SLK(((
(6(

Q(((((4((((U][(((((6(

3.2.4 Higher-Layer Triggered Events

3.2.4.1 Initial Logon

Q ((((((((((SLK6((((((
I[((0 ((9661(((SLK4((((((((
(((O(((6((O((((((((((
(((SLK((((6((

(([PW]TL((((((((((((SLK(
(((((((((((((/(XIK(
(((6((((((((XIK((((6(

N ((((XSQVQ(0cZNK<==>e((dU[5XSKIe14((SLK((((((
(((((((0dU[5XIKe16(

[(S (((((((0]XV1(((((((SLK(
(0 (4(H 6 6 16(SQTM([PW]TL(((((
IL(L[(]XV(0dU[5IL[e((=6969696916(

3.2.4.2 Authentication to Services

_ ((((((O ((4 (((((((
((6N ((S 5 (4 (S ((((**TGS exchange**(
(((((((4 (4 7 6 6 6(

(S (((((I X(((UI a(((((O[[–I XQ((
4 (((S 5 (((6(

SQTM(((((((((S (**KRB_SAFE**((**KRB_PRIV**(6(

((((((I X((((4 ((((((
4 ((6 (S ((((((((cZNK<9: 8e((
((6 (I X(((((((; 6<6(

3.2.5 Message Processing Events and Sequencing Rules

3.2.5.1 Request Flags Details

S (=((S (5 (((((((((((
(SLK(((I [((O[(6(

K ([PW] TL(((((0cZNK<9: 8e((=6<6916(

3.2.5.2 AS Exchange

(S (=((((I [((0cZNK<9: 8e((; 6916(SQTM(((
(((I [(((((cZ 599e4(cZNK=; <Ae4(cZNK<==>e4((dU[5
XSKI e6(

((((((XI K((XI 5 (((((I [5ZMY(6((
XI K(((((dU[5XI Ke6(

3.2.5.3 AP Exchange

((UI a(((((((I X(((((((
0cZNK<9: 8e((=6 6>1(((SMZJgI] PgLI Ig WSMVgZM[ZQX QWV[(09<914(((
SMZJ5I L5ZM[ZQX QWV5MV Za((0 (: 6 6 16D9AF(

((UI a((I L5I] P5LI I 5I X5WX QWV[((((I L5QN5ZMTM I V ((0cZNK<9: 8e(
(=6 6>691((I (L ((I L5I] P5LI I 5I X5WX QWV[((5 ((9<;(
(5 ((SMZJgI XgWX QWV[gKJ (08 <8881((((((((
((((((((((0cZNK: <; e(
(9696>((cZNK: <<e1((I X(((S ((((((
"outer channel" such as TLS. Channel binding is provided using the ((
(((; 6 696(

3.2.6 Timer Events

(S (=(((((((SLK(((((SLK(
((((((((6((((((((
cZNK<9: 8eC (((((((6L (((SLK/(
(((((6K ((((5 (((5 ((
((((((((I [5ZMY((O[5ZMY(6D: 8F((

3.2.7 Other Local Events

SQTM((((6

3.3 KDC Details

3.3.1 Abstract Data Model

SQTM((((((((((((S (=6(SQTM(
4((((IL((((4[PW]TL(B(

- **MaxRenewAge**((((S (X (Q (0dU[5T[ILe((;6969691 6(
- **MaxClockSkew**((((S (X (Q (0dU[5T[ILe((;6969691 6(

Q(((((((((((((S (=4(SQTM(((
((6(

- U (B(8(6(
- U (((B(98(6(SQTM(4((((IL(((
(4[PW]TL(((**MaxServiceTicketAge**((((S (X (
Q (0dU[5T[ILe((;6969691 6(
- U (O (B(98(6(SQTM(((((IL((((
([PW]TL(((**MaxTicketAge**((((S (X (Q (0dU[5T[ILe(
(;6969691 6((

SQTM(((((((((((B(

- Inbound trusts: <all upper case name of the remote realm> | “krbtgt” | <all upper case name of
((F(
- W (B(D ((((((F((((D (((((
((F(

SQTM(((SLK((B(

- I W B((((6(W (XWTQXagSMZJMZW[g ITQLI MgKTQMV ((
(([PW]TL((((6(SQTM(4((((IL(((
(4[PW]TL(((**AuthenticationOptions**((((S (X (
Q (0dU[5T[ILe((;6969691 6(

3.3.1.1 Account Database Extensions

(S (=((((SLK(U][(((((((
(6(

(((((SQTM4((((U][((((((
(((((B(

- O (B((((U][((((((((XIK(
6(N ((4(((;6 6=6 6(((;6 6=6<6 6(
- Z ((B((((U][((((((((
(((((6(N ((4(((;6 6=6 69 6(

▪ [((((((B((((U] [(6(N ((4(((; 6 6=6<6<6(SQTM(((((I L((((([P W] TL(((**msDS-AllowedToDelegateTo**((0dU [5 I L I : e((: 6(9@ 16(

SQTM(((((I L((((([P W] TL(((**userAccountControl**((0dU [5 I L [e((: 6 6(9=1((((B(

▪ L S(5(] (L M[(B(_ (((((((4(((5 5 =(7 (5 5 ((cZNK; A>9e([P W] TL(((((S ((((6(

▪ L Z(5(X 5I ((B(_ (((((((4((SLK(U] [(((O (((5 ((0cZNK<9: 8e((6=6 1(6(

▪ VI (5(I (((ired: When this flag is set on the Application Server's service 4((SLK(U] [(VW (((XI K((((6(

▪ VL (5(L ((B(_ (((((((4((SLK(U] [(VW (((XZW Q] J TM((NWZ_I ZLI J TM(((0cZNK<9: 8e((: 6=((: 6>16(

▪ I (5(((((B(_ ((((((((((((([<] [(dU [5[N] e((4((SLK(U] [(((NWZ_I ZLI J TM(((0cZNK<9: 8e((: 6>16(_ (((((4((SLK(U] [(VW (((NWZ_I ZLI J TM(((0cZNK<9: 8e((: 6>1((([<] [((6(

▪ L (5(((B(_ (((((((4((SLK(U] [(((WS 5I [5 L MTMOI M(((0cZNK<9: 8e((: 6@16(

3.3.2 Timers

(((SLK(6(

3.3.3 Initialization

S (=((((SLK ((((U] [((((4(((((((((O[((7 5 ([XV(0cZNK<9: 8e((>6 16(

Q ((SQTM(SLK ((((I L((((((U] [(((((((I L 6(

Q((SLK(((((4((U] [(((((SLK((6(

Q((SLK((((4((((U] [((((((6(

3.3.4 Higher-Layer Triggered Events

(((SLK(5 ((6(

3.3.5 Message Processing Events and Sequencing Rules

3.3.5.1 Request Flag Details

S (=((S (5 (((((((((((((SLK(((I [((O[(6(

3.3.5.2 User Account Objects Without UPN

3.3.5.3 AS Exchange

3.3.5.3.1 Referrals

3.3.5.3.2 Initial Population of the PAC

3.3.5.4 TGS Exchange

3.3.5.4.1 Check Account Policy for Every Session Ticket Request

Error condition

3.3.5.4.4 Constrained Delegation

3.3.5.4.5 Cross-Domain Trust and Referrals

3.3.5.5 Naming

-

-

-

-

-

- (0cZNK: ; A>e((;6 6 1(((((((((6(([PW] TL(((((((0NY L V16(
- (0cZNK: ; A>e((;6 6 1((((((((((6(
- ((((((**distinguished name (DN)**4**objectGuid**4 **Internet host name**4 (**fully qualified domain name (FQDN)**(((6(

3.3.6 Timer Events

SQTM((((6(

3.3.7 Other Local Events

SQTM((((6(

3.4 Application Server Details

S (=((((((((4 (O[[5I XQ(cZNK<9: 9e6(SQTM((O[[5I XQ(0 (O[[g M (0 (;6<6=6<1((O[[g] M (0 (;6<6=6=116(

(I X((((((((((((((5 (((((((SQTM6(

3.4.1 Abstract Data Model

3.4.1.1 Application Parameters

((((((((((((((I ([(((((((((;6 6996(

3.4.1.2 Security Context Parameters

(((((((((((((((I ([(((((((((;6 6996(

I 4(((((B(

I Z KJ B5I(J (((((((6D: >F(

3.4.2 Timers

(I X(((((((6(

3.4.3 Initialization

I ((((((((;6<69(((((((((5 (((6(

(((U][((((((6(

3.4.4 Higher-Layer Triggered Events

3.4.5 Message Processing Events and Sequencing Rules

3.4.5.1 Three-Leg DCE-Style Mutual Authentication

- (((((((U][(VW ((((((
(C ((((ZNK(9A><– (cZNK9A><e6
- ((U][((((IX((((((((
0cZNK<9:8e((;66<1((((((((6QQ(O[[(4 ((
(((((((6Q((((((((
(((6
- ((U][((((IX(((((((((
((0cZNK<9:8e((;66=16

3.4.5.2 Datagram-Style Authentication

L 5 ((((LKM(ZXK5 (6Q(4 ((
(((((((((6Q 4 ((
(((((((((5 (((
((((6 (4 ((((((4
((((((6I ((4 ((((
(((((((6I (
((6(

_ (((4 ((((((6I (
(((((((U][((((((
((((((((((((0 (((((
S (=(((14 ((((((0 ((1(((
(((((6N (LKM(ZXK((((((
6 4 (((((((U][((((((((
(((6 (((5 (((((S (=(
6

3.4.5.3 Processing Authorization Data

S (=(((((((((cZNK<9:8e((=66>6(

SQTM(U][((((((0cZNK<9:8e((=66>1(((((IL5
_QV:S5XIK((0cZNK<9:8e((6=6<16Q((((((((XIK(
(cU[5XIKe4 ((U][((((6 ((((4
([((((((((XIK(((((6 (((
((cZNK< = e(((((((((((0cU[5XIKe(
(:6@691([((6Q((XIK((4 ([PW]TL((((((
6(

((U][(((SMZJgI] PgLI Ig WSMVgZM[ZQK QWV[(c9<9e(I (L (
(((SMZJ5IL5ZM[ZQK QWV5MV Za((0 (:66_16D:AF(

3.4.5.4 GSS_WrapEx() Call

((((((O[[g_ (0cZNK: <;e((:66_1((((6(

Q B(

- g (KWV M (PIVLTM(
- g (QV MOMZ(55(8(((Y ((X (0YWX1(
- g (WZLMZML(TQ (B(

DRAFT - FOR PREVIEW ONLY

- g g (JWWTMI V(
- (JWWTMI V(
- (WK M ([ZQVO(

W B(

- g (QV MOMZ(
- g (QV MOMZ(
- g (WZL MZML(TQ (0 ((((g 1(B(
  - g (JWWTMI V(
  - (JWWTMI V(
  - (WK M ([ZQVO(
- (WK M ([ZQVO(

(((((O[[g_ 4((((((6Q (((
((g g EE Z]M((((g 6Q (((((
EE Z]M(((((4((((; 6<6=6<6966(

3.4.5.4.1 Kerberos Binding of GSS_WrapEx()

S (O[[g_ M 01((((((((((6((
((((S (((((((S (6(

Q(((((((IM[9:@5K [5PUIK5[PI95A>((IM[:=>5K [5PUIK5[PI95A>(
0 (((cZNK;A>9e14(((((cZNK<9:9e4((((((cZNK;A>9e(
0 (cZNK<9:9e(((1(((6(

((3 5 (((((((((O[[g_ M 01(
(((((((4(g 6(

(ZZK((((((<6 6=((cZNK<9:9e((9:(((((((9>((
((6((ZZK((((((((((((6(
((5 (P9(((9:((9>((0 (((ZZK(1(((((
<6 6=((cZNK<9:9e6(((((((((((<6 6>6((
cZNK<9:9e((((P9((((((((((6(

Q(((((((LM[5KJK5UL=((LM[5KJK5KZK((cZNK;A>9eB(

- ((((cZNK9A><e6(
- ((((((((96 6((cZNK9A><e((4((
LMZ0S (WQL((((M (L ((X 16(

—

- ((((6(

(5 5 ((((96 6 69((cZNK 9A><e((((((g (
(((EE Z]M6(W (((((((Z]M((((
g 6((Q K ((((((96 9((cZNK 9A><ee((
(((((((6(

N (cU[5ZXKMe4((((((((I[V69((((((((
(((((cZNK 9A><e((6(

Q(((((((ZK<5PUIK((ZK<5PUIK5M X((cZNK; A>9eB(

- (((((cZNK< = e6(
- ((((((((6;((cZNK< = e6(
- ((0 ((g g (((NI T[M1((((6(

(5 5 ((((6;((cZNK< = e(((((((((
(EE Z]M6((Q K ((I[V69((((((((
((6((

3.4.5.5 GSS_UnwrapEx() Call

((((((O[[g] (0cZNK: <; e((: 6; 6<1(((((6((

Q B(

- g (KWV M (PI VL TM(
- g (WZL MZML(TQ[(B(
  - g (JWWTMI V(
  - (JWWTMI V(
  - (WK M([ZQVO(
- (WK M([ZQVO(

W B(

- g (QV MOMZ4(55(8(((YWX(
- g (QV MOMZ(
- g (QV MOMZ(
- g (WZL MZML(TQ[(0 ((((g 1(B((
  - g (JWWTMI V(
  - (WK M([ZQVO(

(((((O[[g] 4(((((((6(Q ((
(((g EE Z]M((((g 6((((((
(((((EE Z]M4((((((((; 6<6=6<69 6((

3.4.5.6 GSS_GetMICEx() Call

Q B(

- g (KWV M (PI VL TM(
- g (QV MOMZ4[55(8(((YWX(
- (WZL MZML(TQ (B(
  - (J WWTMI V(
  - (WK M ([ZQVO(

W B(

- g (QV MOMZ(
- g (QV MOMZ(
- (WZL MZML(TQ (B(
  - (J WWTMI V(
  - (WK M ([ZQVO(
- g g (WK M ([ZQVO(

(((((O[[gO UQK4((((((6Q ((
((EE Z]M(((((((WK M ([ZQVO((((
((((ZNK 4((((((B(

- LM[5KJK5UL=((LM[5KJK5KZK(cZNK9A><e(cZNK;A>9e(
- ZK<5PUIK((ZK<5PUIK5M X((cZNK;A>9e(cZNK< = e(
- IM[9:@5K [5PUIK5[PI95A>((IM[:=>5K [5PUIK5[PI95A>(cZNK;A>9e(cZNK<9:9e(

3.4.5.7 GSS_VerifyMICEx() Call

Q B(

- g (KWV M (PI VL TM(
- (WZL MZML(TQ (B(
  - (J WWTMI V(
  - (WK M ([ZQVO(
- g g (WK M ([ZQVO(

W B(

- g (QV MOMZ(
- g (QV MOMZ(
- g (QV MOMZ(

(((((O[[g UQX4 ((((6Q ((
((EE Z]M((((((((((
((6

3.4.6 Timer Events

SQTM((((6

3.4.7 Other Local Events

(((((((((((((6

4 Protocol Examples

((((((((((((SQTM6(

4.1 Interactive Logon Using Passwords

(

Figure 2: Interactive logon that uses passwords

[(9E(I(((((((((((((4(((I[5
ZMY(((5 ((0 O 1((5 (((6((I[5ZMY4((
(((((4((((S (L (K (0SLK16(

[(:E(Q(((((I[5ZMY(((O 4((SLK((((((
((((((((I[5ZMY(((((((/(0cZNK<9:8e(
(;6916((SLK(((I[5ZMX(((O ((((4(((((
(6(

(SLK(((XIK(0 (;6 6=6 16(L (((XIK((((((((
(((((6(((((((((SLK((
((((((6((SLK(((XIK(((((
((((((((g (((O 6(

[(;E(((((O[5ZMY((((O ((((((:((((
(((((((((S ((((((((
((6(((((((7 6 4((
(((((((4((((((((((
6(

[(<E((SLK((((O[5ZMY(((O[5ZMX(((((((
(6(((((:(((((4((
(((0 (;6 6=<16(((((((((S (
((((6(

(((((XIK(0cU[5XIKe((((((((
((1(((((S (((((((((
4(((((((((E(

- **LogonTime**
- **LogoffTime**
- **KickOffTime**
- **PasswordLastSet**
- **PasswordCanChange**
- **EffectiveName**
- **FullName**
- **LogonScript**
- **ProfilePath**
- **HomeDirectory**
- **HomeDirectoryDrive**
- **LogonCount**
- **BadPasswordCount**
- **LogonServer**
- **LogonDomainName**
- **UserAccountControl**

4.2 Network Logon

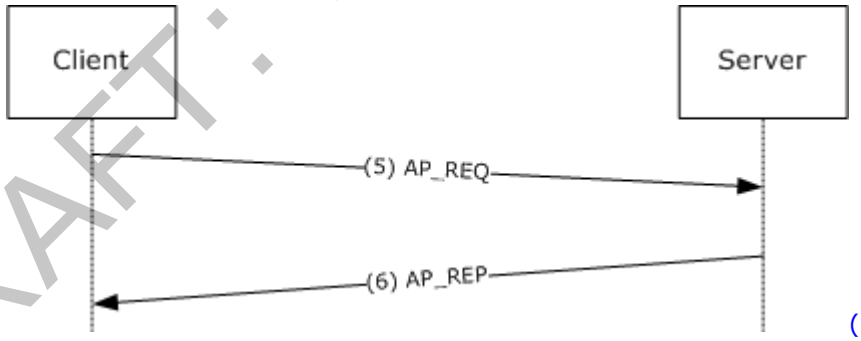
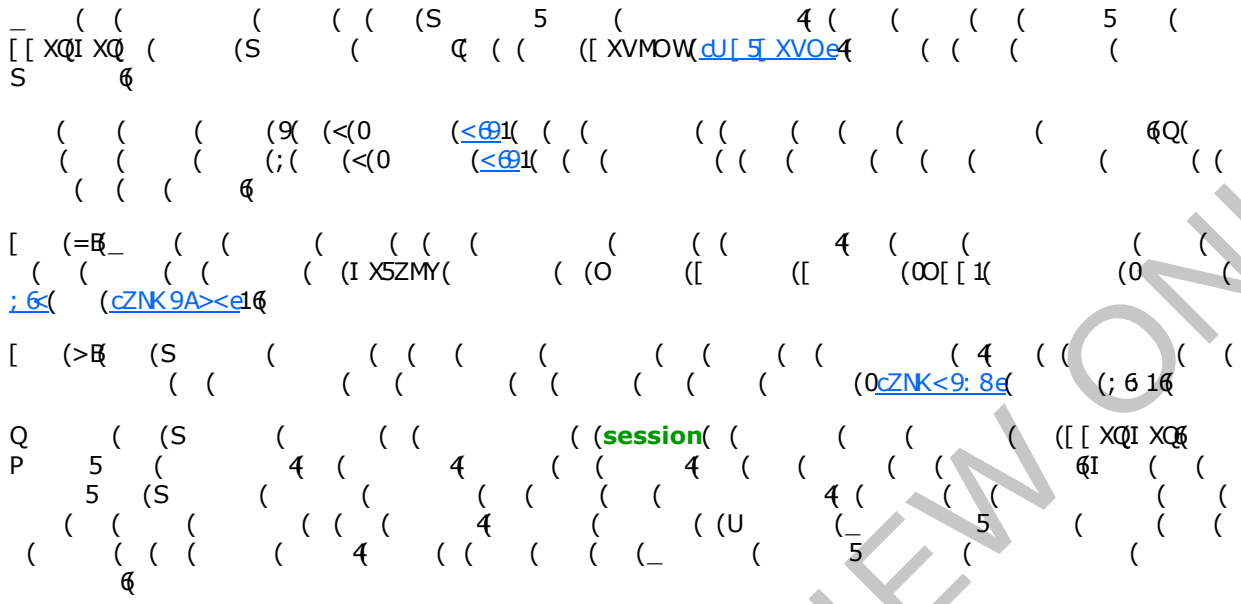


Figure 3: Network Logon



4.3 GSS_WrapEx with AES128-CTS-HMAC-SHA1-96

-
-
-
-

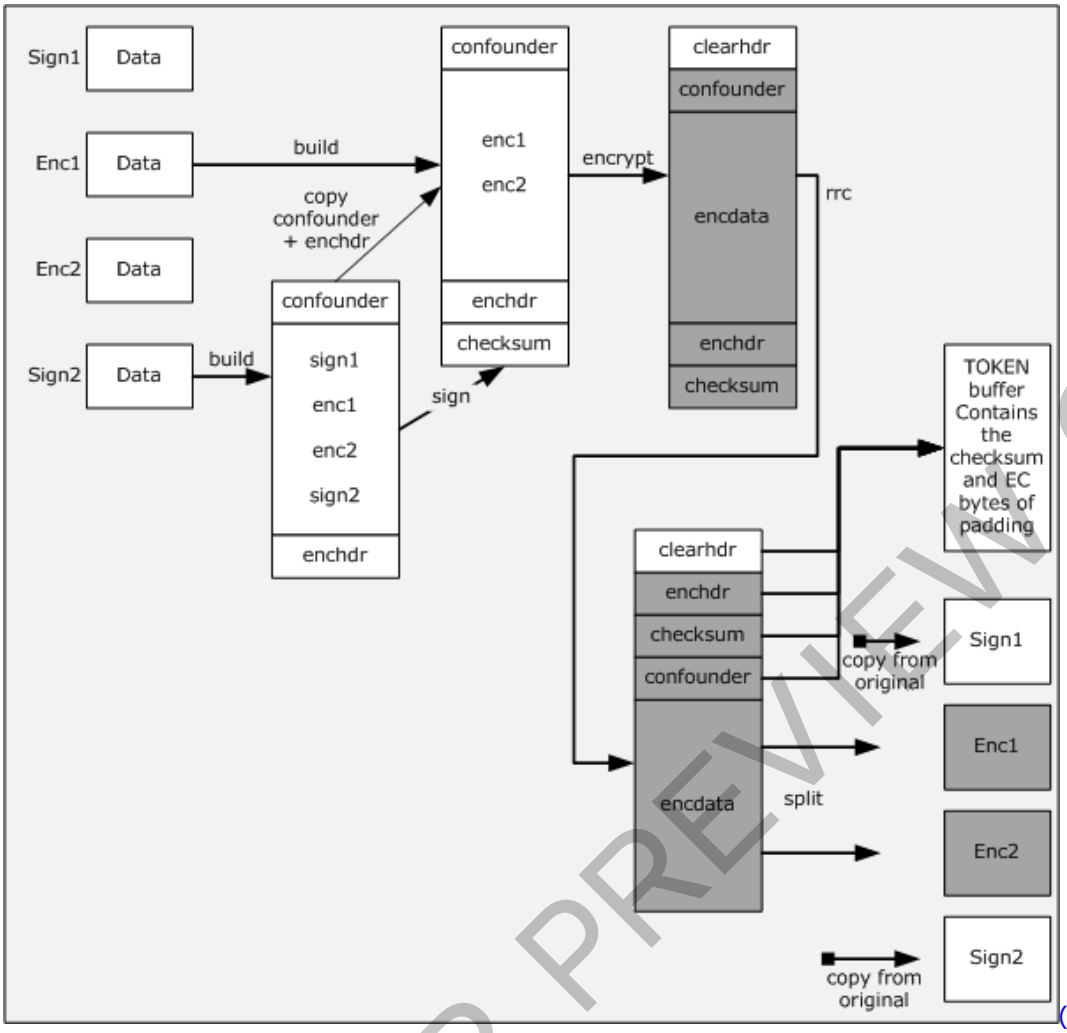


Figure 4: Example of RRC with output message with 4 buffers

(**enchdr**((((0cZNK<9: 9e((<6 6<1(((6((**clearhdr**(((
((0cZNK<9: 9e((<6 6>6 16(**GSS_WrapEx()**((((**output_message**(
((B(

- (9((((9(((K g (E E(N T[M4((E E(Z] M(
- (:((((9(((K g (E E(Z] M4((E E(N T[M(
- (;((((:(((K g (E E(Z] M4((E E(N T[M(
- (<((((:(((K g (E E(N T[M4((E E(Z] M((
((((((3((3((3((0 (4(((
cZNK; A>9e16(
((((((B(
- (

▪ (

▪ (

▪ (((0MK3ZZK1((

▪ (

MK(((((((((((((C(((<6 6<((
cZNK<9: 9e6(

4.4 AES 128 Key Creation

((((((I M[(9: @((B(

] (((B(

[B(

```
0000000: 44 00 4f 00 4d 00 41 00 49 00 4e 00 2e 00 43 00   D•O•M•A•I•N•.•C•
0000010: 4f 00 4d 00 68 00 6f 00 73 00 74 00 63 00 6c 00   O•M•h•o•s•t•c•l•
                                 0 2e 00 64 00 6f 00 6d 00   i•e•n•t•.•d•o•m•
0000030: 61 00 69 00 6e 00 2e 00 63 00 6f 00 6d 00         a•i•n•.•c•o•m•
```

Q K B(

(I M[(9: @((((((((((([(0] N9>1((((
] N@((0c] VQK WL Me4((; 6A16(

] N@[B(

((((((] (0] N9>1((((] N@[(0c] VQKWL Me4 (; 6A16(

] N@[B(

V 4((] N@[((((((0cZNK; A>: e4((<16(_ (((I M[((
9: @[4((((4((: 0XJSL N: 0] N@[4] N@[4(Q K 4(
9: @1(B(

(S (((((((I M[(9: @[((((L SQI M[(9: @[4 1(
0cZNK; A>: e4((<16(

((((9: @5 (B(

4.5 RC4 GSS_WrapEx

(**GSS_WrapEx()**(((((; 6<6=6<69 6((ZK<5PUI K(((((
cZNK< = e(((6((((((((((((((
S ((((((6(

[(S B(

```
                                                                üóπÉ»⌂┬┬òTíP╪·SY

X      (    (     (                          (    (              Ɐ(

  0000000: 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff      ·"3DUfwêÖ¬╕╠ε

   (        ( (      ( (       ( (cZNK< = e(      ( 6(    (   (       (      Ɐ(
S  Ɐ(

  0000000: 81 a2 cb 90 af 7f c2 d1 95 54 a1 50 d8 18 53 59   üóπÉ»⌂┬┬òTíP╪·SY


[  g    (0 (   5     (    ( (       ( (cZNK< = e(      ( 6Ɐ1Ɐ(

  0000000: 60 cb ac d3                                       `╦¼╙╚

L   Ɐ(

  0000000: 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff      ·"3DUfwêÖ¬╕╠ε

K        Ɐ(

                     3 0c f1 2a                            RV≤√c·±*

   (     (       (    (   (        ( (      (    (SEAL()(       ( (      (; 6<6<6(
Output_message(   (      (                  4(                ( (   (       Ɐ(

L   Ɐ(

  0000000: 8e d6 3f 0a c8 38 15 33 5b 72 e2 93 ba e1 f6 60   Ä╓?·╚8·3[rΓô╟ß÷`

[       Ɐ(

  0000000: 60 3b 06 09 2a 86 48 86 f7 12 01 02 02 02 01 11   `;··*åHå≈·······
                                                             ΓⱭï╝cHτ@δ¬a
                                                               ÷^<!╣¬
```

—

5 Security

W (((UQ(S ((((ZK<4 (4 (((((
((LM[6 (((((((9:@5 (4 (((
(((UQ(S 6

W ((S ((((((cZNK<9:8e((986

5.1 Security Considerations for Implementers

SQTM(((((((S (=(0cZNK<9:8e4(cZNK;A>9e4(cZNK;A>:e((
cZNK< =e14(O[[5I XQ(0cZNK: <;e4(cZNK9A><e((cZNK<9:9e14 (XSQVQ(cZNK<==>e6(

5.1.1 RODC Key Version Numbers

J (5 (((0ZWLK1((((((4(ZWLK(
(((((0 (;696=6A1(((((((((
(/(LK 6 (((((ZWLK((6(

5.1.2 SPNs with Serviceclass Equal to "RestrictedKrbHost"

[((Z S P (((((((S (
(((((((((((((6 (
(((5 5 ((4 ((5 5 ((
6[((((((((((((
(/(((((((((((((
6

5.1.3 Account Revocation Checking

S (=(((((((O[(4 ((O(
((((((((((O (((((((
6(SQTM(((((0 (;6_6=6<6911((((((((
(6(SQTM(SLK((((((((((((O ((
((:8(6 (((((((((((((
((((((IL(6

5.2 Index of Security Parameters

((((((((6

6 Appendix A: Product Behavior

((((((((((B(

- U (_ (: 888(((
- _ (X(((
- _ ([(: 88;(((
- _ ((((
- _ ([(: 88@(((
- _ ((((
- _ ([(: 88@Z: (((

M 4((4((((6Q(((((((((4(
((((((6((((((((((((
(((((6(

] ((4((((((((((((((
(([PW] TL(([PW] TL(VW ((_ (((((([PW] TL((
[PW] TL(VW (6] ((4(((UI a(((_ (((
((6(

D9F([(: 6ΘB((((((((((((((
((((_ 6(

Windows version	

7 Change Tracking

((((((cU[5SQTMe((((R (: 88A((
I (: 88A(6K ((((4 4 (6

Major((((((6M ((((B(((((((((

- I((((((((((6
- I ((4 4 ((((((6
- I(((6
- (((((((6
- K ((((6

Minor(((((((6M ((((
((((((4 4 ((6(((((((((

Editorial((((4 4 ((6(((((((((

No changes(((((((((6(((((((((

U (((((((((((B(

- V ((6
- K (6
- K (6
- V ((((6
- X (((6
- X (((6
- V (((6
- X ((6
- X ((6
- V (((((6
- K ((((6
- K ((((6
- V ((((((6
- X (((((6
- X (((((6
- V ((((6
- K ((((6

- K ((((
- W (((

M (((((((M (6(

[((((((((((((B(

Protocol syntax(((((0 ((4(4(4((1(((((

Protocol revision(((((((((((((((((

K ((((((6(Q((((4(((H 6 (

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
969(O (	;>;>=(I (((g ((cZNK: <;e(	V(	K ((
96 69(V (Z (	:>88=(I (dU[5ILI9e4{dU[5ILI:e4{dU[5 ILI;e4{dU[5IL[Ke4((dU[5IL [e(	V(	K ((
96 6 (O (Z (	:>88=(Z (dU[5IL [e4((((((	V(	K ((
96< (Z ((W (X (	:>88=(I (dU[5ILI9e4{dU[5ILI:e4{dU[5 ILI;e4{dU[5IL[Ke4((dU[5IL [e((((5ZNK((	V(	K ((
96= (X 7X (	:>88=(Z ((((	V(	X ((((
;6969(I (L (U (	;> A>(I (U Q-((((((	V(	K ((
;6966<(M ([(	:;;;;(K ((((O[5ZMY (((((((O[5ZMX (	V(	K ((
;6966<(M ([(	:;;;;(K (((((((((O (	V(	X ((((
;6966<(M ([(	:;;;;( ] (((((((((O (	V(	K ((

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
;0D6=6<(M ([(	:;;;;(K (I[5ZMY((O[5ZMY6(	V(	K (6(
;6<6=(U (X (M (([(Z (	;>;>=(I (((g ((cZNK: <;e6(	V(	K (6(
<6<(IM[(9:@S (K (	; 8:9( ] (((((6(	V(	K (6(

8 Index