

▪ Copyrights.

[illegible][illegible]

Totals.

| Date | Revision History | Revision Class | Comments |
|----------------|------------------|----------------|-----------------|
| 987: : 7: 88>(| 889(| ((| UKXX(U (9Q (I (|
| 8979A7: 88 (| 98(| ((| UKXX(U (9(|
| 8; 78: 7: 88 (| 98(| ((| U ((|
| 8<78; 7: 88 (| 96 (| ((| U ((|

| Date | Revision History | Revision Class | Comments |
|----------------|------------------|----------------|---------------------|
| 8=7997: 88 (| 96(| ((| U ((|
| 8>7897: 88 (| 96 6(| M (| Z (((((6 |
| 8 78; 7: 88 (| 96<(| U (| U ((((6 |
| 8 7: 87: 88 (| 96<6(| M (| Z (((((6 |
| 8@7987: 88 (| 96<(| U (|] ((((6 |
| 8A7: @7: 88 (| 96<(| U (| U (6 (((((((|
| 987: ; 7: 88 (| 96<6(| M (| Z (((((6 |
| 997; 87: 88 (| 96<6 (| M (| Z (((((6 |
| 897: =7: 88@ | : 6(| U (|] (((((6 |
| 8; 79<7: 88@ | : 6(| U (|] ((((6 |
| 8=79>7: 88@ | ; 6(| U (|] (((((6 |
| 8>7: 87: 88@ | <6(| U (|] (((((6 |
| 8 7: =7: 88@ | <66(| M (| Z (((((6 |
| 8@7: A7: 88@ | <66 (| M (| Z (((((6 |
| 987: <7: 88@ | <6(| U (|] ((((6 |
| 9: 78=7: 88@ | <6 (| U (|] ((((6 |
| 8979>7: 88A(| <6 (| U (|] ((((6 |

Table of Contents

| | |
|--|-----------|
| 1 Introduction..... | 4 |
| 96(((O (| < |
| 96(((Z (| < |
| 96 ((V (Z (| < |
| 96 6(((Q (Z (| > |
| 96(((I (W (Q 1(| > |
| 96(((Z ((X ((W ([(| > |
| 96(((I ([(| > |
| 96(((((T (| > |
| 96(((5M (N (| > |
| 2 Structures | 7 |
| : ((K ((| @ |
| : 6(((K ([((| @ |
| : 6 ((SMZJg[Q gI VLgI ZQ] M[(| @ |
| : 6 6(((OZW] XgUMUJ MZ[PQ(| A |
| : 6(((XI K aXM(| A |
| : 6(((XI KgQ/NWgJ] NMZ(| 98 |
| : 6(((SMZJg I TQ I QWgQ/NW(| 99 |
| : 6(((XI K(K (| 9= |
| : 6((XI KgKZML MV Q TgQ/NW(| 9> |
| : 6 6(((XI KgKZML MV Q TgLI I (| 9 |
| : 6 6(((MKXSOg[] XXTMU MV I TgKZML (| 9 |
| : 6 6(((V TUG[] XXTMU MV I TgKZML MV Q T(| 9@ |
| : 6(((XI KgKTQMV gQ/NW(| 9@ |
| : 6(((XI Kg[QVI] ZMgLI I (| 9A |
| : 6 6(((([(| 8 |
| : 6 6(((SLK([(| 8 |
| : 6((K (L (Q (| 8 |
| : 6 8(((XVL V[gQ/NW(| 9 |
| : 6 9(((N (UQ TL (| : |
| 3 Structure Examples | 25 |
| ; ((T (I (Q (| : |
| ; 6(((K (Q (| A |
| ; 6((((| A |
| 4 Security Considerations..... | 30 |
| <(((XI K(L (| 8 |
| <6(((I ((N (| 8 |
| <6 ((Z (([Q(Q (((XI K(| 8 |
| <6 6(((Q(N (| 8 |
| <6 6((((N (| = |
| <6(((Q (([(X (| = |
| 5 Appendix A: Windows Behavior..... | 37 |
| 6 Change Tracking..... | 39 |
| 7 Index | 41 |

[illegible]

Interface Definition Language (IDL)
 Microsoft Interface Definition Language (MIDL)
 Network Data Representation (NDR)
 relative identifier (RID)
 remote procedure call (RPC)
 RPC transfer syntax
 security identifier (SID)
 Service for User (S4U)
 Service for User to Proxy (S4U2proxy)
 Service for User to Self (S4U2self)
 ticket-granting service (TGS)
 ticket-granting ticket (TGT)
 trusted domain object (TDO)
 Universal Naming Convention (UNC)
 UNC path

1.2.1 Normative References

- [illegible]

B7 : 6 6 7 5 7 7M<JL><A<58>I L 5< 5A@ ; 5<=<MA: 9KA>: < ((((

dK 8>€ (W (O (*LKM9@BZ (X (K *(K 8>(I (9AA (
 B7 6 6 7 7 7 7 8>6 (

dJ[5I LI 9€U (K (*1 (L (I (I (I 5T*(R (: 88 €

dJ[5I LI ; €U (K (*1 (L (I (I (V5b*(R (: 88 €

dJ[5I L [€U (K (*1 (L ((I **(R (: 88 €

dJ[5I XL [€U (K (*1 (X (L (I (I **(R (
 : 88 €

dJ[5L aX€U (K (*1 (L (**(R (: 88 €

dJ[5OTW [€U (K (*1 (X (U (O *(U (: 88 €

dJ[5SQTM€U (K (*S (X (M **(R (: 88 €

dJ[5VTUX€U (K (*V (I V(U (OV TU1(I (X (I *(
 R (: 88 €

dJ[5VZXK€U (K (*V (Z (X (I *(U (: 88 €

dJ[5XSKI €U (K (*X (S (K ((Q (I (OXSQ/Q 1((
 S (X (I **(R (: 88 €

dJ[5ZKU X€U (K (*Z (K (U (X (I *(I (
 : 88 €

dJ[5ZXKM€U (K (*Z (X (K (X (M **(R (: 88 €

dJ[5I U Z€U (K (*1 (I (U (Q I U1(Z (X (I (
 OK 5 5 1*(R (: 88 €

dJ[5I N] €U (K (*S (X (M B[((] ((K (
 L (X (I **(R (: 88 €

cZNK9A><€T (R6(* (S ((=O[[5I XQU *(ZNK(9A><(R (9AA>(
 B7 6 6 7 7 9A><6 (

cZNK: 99A€J (I 6(*S (((((ZNK((Q (Z (T *(JKX(9<(ZNK(
 : 99A(U (9AA (B7 6 6 7 7 : 99A6 (

cZNK; : <<€[(U 6((R6((J (R6(*U (((: 888(S (K (
 X ((X (X *(ZNK(; : <<(N (: 88: (
 B7 6 6 7 7 ; : <<6 (

cZNK; A>9€Z (S6(*M ((K (I ((S (=*(ZNK(; A>9(
 N (: 88=(B7 6 6 7 7 ; A>96 (

cZNK<9: 8€V (K 6(a (6(P (I 6((Z (S6(* (S (V (
 I (I (O =1*(ZNK(<9: 8(R (: 88=(B7 6 6 7 7 <9: 86 (

cZNK<==>€b (T6(((J 6(*X (S (K ((Q (I ((S *(
 ZNK(<==>(R (: 88>(B7 6 6 7 7 <==>6 (

[illegible]

```

(I L ( (I L 5Q5ZMTM I V (0<ZNK<9: 8e( (=6 6>1( ( ( (
    QQ( ( (I L 5_ Q: S5XI K(0<ZNK<9: 8e(
    ( 6=6>1QQ ( ( ( ( (PACTYPE( ( ( ( ( ( ( ( (
    (XI K( QQ ( ( (PACTYPE( ( ( ( ( (
PAC_INFO_BUFFER( QQ (PAC_INFO_BUFFER( ( ( ( ( ( ( (
    ( ( (XI K( ( ( ( QQ(
    ( ( ( ( (PAC_INFO_BUFFER( ( ( ( ( (9( ( (
    (: 6= ( ( ( ( (>( ( ( (: 6@Q

```

Note

2.1 Common Types

RPC_UNICODE_STRING(XI K(((((B BYTE USHORT ULONG ULONG64 FILETIME ((((dU SL aXeG (XI K(((((SID(

2.2 Constructed Security Types

2.2.1 KERB_SID AND ATTRIBUTES

[illegible]

```
typedef struct {
    PSID SID;
    ULONG Attributes;
} KERB_SID_AND_ATTRIBUTES,
*PKERB_SID_AND_ATTRIBUTES;
```

SID: I ((([Q (6

Attributes: I((((((((([Q6

Attributes(((((((((((

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|---------|--------|--------|--------|--------|------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|------------|--------|--------|--------|--------|--------|--------|--------|
| (8) | (9) | (: | (; | (^ | (_ | (\ | () | (@ | (A | (B | (C | (: | (; | (^ | (_ | (\ | () | (@ | (A | (B | (C | (: | (C | (: | (; | (^ | (_ | (\ | () | (@ | (A | (B | (C | (: | (C |
| 8(| 8(| M | 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(| L(| K(| J(| I | | | |

— (((((B

[illegible]
$$I \subset (\mathcal{U})^{\Gamma} \cap (\mathcal{V})^{\Gamma} = (\mathcal{U})^{\Gamma} \cap (\mathcal{V})^{\Gamma} = (\mathcal{U})^{\Gamma} \cap (\mathcal{V})^{\Gamma} = (\mathcal{U})^{\Gamma} \cap (\mathcal{V})^{\Gamma}$$

2.2.2 GROUP_MEMBERSHIP

```
(GROUP_MEMBERSHIP( ( ( ( ( ( ( Q( ( (
( (KERB\_VALIDATION\_INFO \(section 2.5\)(
( ( ( GROUP_MEMBERSHIP( ( ( ( R
```

```
typedef struct _GROUP_MEMBERSHIP {
    ULONG RelativeId;
    ULONG Attributes;
} GROUP_MEMBERSHIP,
*PGROUP_MEMBERSHIP;
```

RelativeId: I (; : 5 ((((((ZQ(((((

[illegible]

2.3 PACTYPE

(PACTYPE(((((((((XI K(((((((((PAC INFO BUFFER (section 2.4)(((PACTYPE(((((((((

(PACTYPE((((B

| | | | | | | | | | | | | | | | | | | | |
|-----|----|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (| (| (| (| (| (| (| (| (| (| (| (| (| (| (| (| (| (| (| (|
| (| | | | | | | | | | | | | | | | | | | |
| (| | | | | | | | | | | | | | | | | | | |
| J | (0 | 1(| | | | | | | | | | | | | | | | | |
| 666 | | | | | | | | | | | | | | | | | | | |

```

cBuffers (4 bytes): I( ; 5 ( ( ( ( 5 ( ( ( ( ( ( ( (
( ( ( Buffers( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( (

```

Version (4 bytes): I (;: 5 ((((5 (((((XI K(

Buffers (variable): I ((PAC_INFO_BUFFER(§

```
( ( ( ( (XI K( ( ( ( ( ( ( (PAC_INFO_BUFFER(
@ ( ( ( ( (XI K( (U)] ( ( (
```

N (([PACTYPE \(section 2.3\)](#)) ((((((PAC_INFO_BUFFER((((

(((((((((((X) K ((PAC_INFO_BUFFER(((((

(((((((((((PAC_INFO_BUFFER(((((((((((

P (((S (L (K (OSL K1(((((((((((

(((U)[(VW ((((((X) K(((((((((((

[illegible][illegible][illegible][illegible]

```
Offset (8 bytes): I(><5(      (      (      (      5      (      (      (      (      (      (
                     (      (      (      (      (      (      (      (      (PACTYPE(      (0      (
:616    (      (      (U][      (      (      (      (      (      (      (      (      (      (
                     (      (      (      (      (      (      (      (      (      (      (
```

2.5 KERB_VALIDATION_INFO

[illegible]

```
typedef struct {
    FILETIME LogonTime;
    FILETIME LogoffTime;
    FILETIME KickOffTime;
    FILETIME PasswordLastSet;
    FILETIME PasswordCanChange;
    FILETIME PasswordMustChange;
    RPC_UNICODE_STRING EffectiveName;
    RPC_UNICODE_STRING FullName;
    RPC_UNICODE_STRING LogonScript;
    RPC_UNICODE_STRING ProfilePath;
    RPC_UNICODE_STRING HomeDirectory;
    RPC_UNICODE_STRING HomeDirectoryDrive;
    USHORT LogonCount;
    USHORT BadPasswordCount;
    ULONG UserId;
    ULONG PrimaryGroupId;
    ULONG GroupCount;
    [size_is(GroupCount)] PGROUP_MEMBERSHIP GroupIds;
    ULONG UserFlags;
    UCHAR UserSessionKey[16];
    RPC_UNICODE_STRING LogonServer;
    RPC_UNICODE_STRING LogonDomainName;
    PSID LogonDomainId;
    ULONG Reserved1[2];
    ULONG UserAccountControl;
    ULONG Reserved3[7];
    ULONG SidCount;
    [size_is(SidCount)] PKERB_SID_AND_ATTRIBUTES ExtraSids;
    PSID ResourceGroupDomainSid;
}
```

```
LogonTime: I(FILETIME(
    (0dJ[5 LI 9e) (: 6 = 1( ([ PW] TL( (8( (
    &

LogoffTime: I(FILETIME(
    &Q( ([ PW] TL( (dwHighDateTime(
    ( (8 NNNNNN( (dwLowDateTime( ( (8 NNNNNN&I(
    ( XI K([ PW] TL D:F( ( ( ( ( ( ( ( ( ( ( ( ( (
    ( ( ( ( &

KickOffTime: I(FILETIME( (LogoffTime( (/
    T ( (0dJ[5 LI 9e) (: 6 ; ; 1( &Q( ( ( ( ( ( ( (
    ( ([ PW] TL( (dwHighDateTime( ( (8 NNNNNN( ( (
    dwLowDateTime( ( (8 NNNNNN& (S ( ( ( ( ( ( (
    ( (KickOffTime& ( ([ PW] TL(VW ( ( ( ( ( ( (
    KickOffTime( ( ( &I( ( ( XI K([ PW] TL D<F( ( ( ( ( ( (
    ( ( ( ( ( ( ( ( &

PasswordLastSet: I(FILETIME( (/ T [ ( (
    0dJ[5 LI ; e) (: 8 < 1( ( ( ( ( ([ PW] TL( (8( ( ( ( &Q(
    ( ( ( ( ( ( ( (U)] ( (dwHighDateTime( ( ( (
    8 888888888( (dwLowDateTime( ( (8 888888888&

PasswordCanChange: I(FILETIME( (/
    ( ( ( ( ( ( ( ( ([ PW] TL( (8( ( ( ( &Q(
    ( ( ( ( ( ( ( ( ( ( ( ( (U)] ( (
    ( ( ( ( &

PasswordMustChange: I(FILETIME( (/
    ( ( ( ( ( ( ( ( ([ PW] TL( (8( ( ( ( &Q( ( ( (8 NNNNNN(
    ( ( ( (U)] ( (dwHighDateTime( ( ( (8 NNNNNN&
    (dwLowDateTime( ( (8 NNNNNN&(

EffectiveName: I(RPC_UNICODE_STRING( (/
    I V ( (0dJ[5 LI ; e) (: 6 : 91( ( ( ( ( (
    [ PW] TL( (8( ( ( ( &

FullName: I(RPC_UNICODE_STRING( (/ ( ( (
    ( ( ([ PW] TL( (8( ( ( &Q(FullName( ( ( ( ( (
    U)] ( (RPC_UNICODE_STRING( ( (T ( ( ( ( &

LogonScript: I(RPC_UNICODE_STRING( (/ X (
    (0dJ[5 LI ; e) (: 6 : 91( ( ( ( ( ([ PW] TL( (8( (
    &Q( LogonScript( ( ( ( ( (U)] ( (
    RPC_UNICODE_STRING( ( (T ( ( ( ( &

ProfilePath: I(RPC_UNICODE_STRING( (/ X (
    (0dJ[5 LI ; e) (: 8 >> 1( ( ( ( ( ([ PW] TL( (8( (
    &Q( ProfilePath( ( ( ( ( (U)] ( (
    RPC_UNICODE_STRING( ( (T ( ( ( ( &
```


2.6 PAC Credentials



15 / 42

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (| (| (| (| (| (| (| (| (| (| 9 | (| (| (| (| (| (| (| : | (| (| (| (| (| (| (| @ | A | 8 | (| 9 | : | (| ; | (| (| (| (| (| (| (| (| (| (|
| K Q(| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 666 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| V T (| | | | | | | | | | | | | | | | | | | | V (0 1(| | | | | | | | | | | | | | | | | | | | | | | |
| 666 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Name (variable): I (((9>5 [] ((((5 ((((((((/ (((6D98F(

```
(PAC_SIGNATURE_DATA( ( ( (XI K( ( (SLK(
0 (:61( ( (Offset( ( (PACTYPE(
PAC_INFO_BUFFER( (0 (:61( (Buffers( (ulType( (
PAC_INFO_BUFFER( ( ( (8 8888888)( (
ulType( ( (PAC_INFO_BUFFER( ( (SLK( ( (
8 8888888 &XI K( ( ( (XI K( ( (UJ_5SQM(
( ( ( ( ( ( ( ( ( (SLK&V(
( ( (XI K( &(
( ( (PAC_SIGNATURE_DATA( ( (B(
```

[illegible]

| Value | Meaning |
|--|---|
| SMZJgKPMKS[] UgPUI KgUL=(8 NNNNNN >(\ | I (((cZNK<9: 8€ ((cZNK<= € (<€[(((9>(\ ((9=€ |
| PUI Kg[PI 9gA>gI M[9: @ 8 8888888N(\ | I (((cZNK; A>: € (€[(((9: (€ L (((9=€ |
| PUI Kg[PI 9gA>gI M[: =>(8 88888898(\ | I (((cZNK; A>: € (€[(((9: (€ L (((9>€ |

2.8.1 Server Signature

```
( ( ( ( ( (cZNK< = &( ( ( (XI K( ( ( (Signature(
( ( (PAC_SIGNATURE_DATA( ( ( ( ( ( ( ( ( (
( ( (Signature( ( ( ( / (PAC_SIGNATURE_DATA( ( (
```

(SLK((((((CZNK< = € (([([(((XIK(§ (

(((((Signature(((SLK/(PAC_SIGNATURE_DATA(§

[illegible]

Release: Wednesday, January 14, 2009

[illegible]

```

[ ] XVgLV[ gQ/NW( ( ( ( / ( ) XV( ( LV[ ( Q( ( ( ( ( (
] XV( ( LV[ ( ( ( ( ( ( ( ( ( ( ) XVgLV[ gQ/NW( ( ( (
( ( ( ( ( Buffers( ( ( ( ( XI K aXM( (0 (: 6 1 ( ( (
( ( ( Offset( ( ( ( ( XI KgQ/NWgJ ] NMZ( (0 (: 6 1 ( ( (
Buffers( ( ( ulType( ( ( ( ( XI KgQ/NWgJ ] NMZ( ( ( (8 8888888K(
D9: F

```

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (| (| : | : | < | = | > | (| @ | A | g | (| : | : | : | < | = | (| (| @ | A | : | g | (| : | : | < | = | (| (| @ | A | : | g | (|
|] T (| | | | | | | | | | | | | | | | |] W (| | | | | | | | | | | | | | | | | |
| L L V T (| | | | | | | | | | | | | | | | | L L V W (| | | | | | | | | | | | | | | | | |
| N (| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

21 / 42


```

*PPAC_CREDENTIAL_DATA;

typedef struct _PAC_CLIENT_INFO {
    FILETIME ClientId;
    USHORT NameLength;
    WCHAR Name[1];
} PAC_CLIENT_INFO, *PPAC_CLIENT_INFO;

typedef struct _NTLM_SUPPLEMENTAL_CREDENTIAL {
    ULONG Version;
    ULONG Flags;
    UCHAR LmPassword[16];
    UCHAR NtPassword[16];
} NTLM_SUPPLEMENTAL_CREDENTIAL, *PNTLM_SUPPLEMENTAL_CREDENTIAL;

typedef struct _SID *PISID;

typedef struct _CYPHER_BLOCK {
    CHAR data[8];
} CYPHER_BLOCK;

typedef struct _USER_SESSION_KEY {
    CYPHER_BLOCK data[2];
} USER_SESSION_KEY;

typedef struct _KERB_SID_AND_ATTRIBUTES {
    PISID Sid;
    ULONG Attributes;
} KERB_SID_AND_ATTRIBUTES, *PKERB_SID_AND_ATTRIBUTES;

typedef struct _GROUP_MEMBERSHIP {
    ULONG RelativeId;
    ULONG Attributes;
} GROUP_MEMBERSHIP, *PGROUP_MEMBERSHIP;

typedef struct _KERB_VALIDATION_INFO {
    FILETIME LogonTime;
    FILETIME LogoffTime;
    FILETIME KickOffTime;
    FILETIME PasswordLastSet;
    FILETIME PasswordCanChange;
    FILETIME PasswordMustChange;
    RPC_UNICODE_STRING EffectiveName;
    RPC_UNICODE_STRING FullName;
    RPC_UNICODE_STRING LogonScript;
    RPC_UNICODE_STRING ProfilePath;
    RPC_UNICODE_STRING HomeDirectory;
    RPC_UNICODE_STRING HomeDirectoryDrive;
    USHORT LogonCount;
    USHORT BadPasswordCount;
    ULONG UserId;
    ULONG PrimaryGroupId;
    ULONG GroupCount;
    [size_is(GroupCount)]
    PGROUP_MEMBERSHIP GroupIds;
    ULONG UserFlags;
    USER_SESSION_KEY UserSessionKey;
    RPC_UNICODE_STRING LogonServer;
    RPC_UNICODE_STRING LogonDomainName;

```

```

    PISID LogonDomainId;
    ULONG Reserved1[2];
    ULONG UserAccountControl;
    ULONG Reserved3[7];
    ULONG SidCount;
    [size_is(SidCount)]
    PKERB_SID_AND_ATTRIBUTES ExtraSids;
    PISID ResourceGroupDomainSid;
    ULONG ResourceGroupCount;
    [size_is(ResourceGroupCount)]
    PGROUP_MEMBERSHIP ResourceGroupIds;
} KERB_VALIDATION_INFO, *PKERB_VALIDATION_INFO ;

typedef struct _S4U_DELEGATION_INFO {
    RPC_UNICODE_STRING S4U2proxyTarget;
    ULONG TransitedListSize;
    [size_is( TransitedListSize )]
    PRPC_UNICODE_STRING S4UTransitedServices;
} S4U_DELEGATION_INFO, * PS4U_DELEGATION_INFO;

typedef struct _UPN_DNS_INFO {
    USHORT UpnLength;
    USHORT UpnOffset;
    USHORT DnsDomainNameLength;
    USHORT DnsDomainNameOffset;
    ULONG Flags;
} UPN_DNS_INFO, *PUPN_DNS_INFO;

```


3 Structure Examples

| (| (| (| (| (| (| (| (| (| X | K | (| (| (AD-IF-RELEVANT) |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 00000000 | 30 | 82 | 05 | 52 | 30 | 82 | 05 | 4e | a0 | 04 | 02 | 02 | 00..R0..N..... |
| 00000010 | 05 | 44 | 04 | 82 | 05 | 40 | 04 | 00 | 00 | 00 | 00 | 00 | .D...@..... |
| 00000020 | 00 | 00 | b0 | 04 | 00 | 00 | 48 | 00 | 00 | 00 | 00 | 00 |H..... |
| 00000030 | 00 | 00 | 12 | 00 | 00 | 00 | f8 | 04 | 00 | 00 | 00 | 00 | |
| 00000040 | 00 | 00 | 14 | 00 | 00 | 00 | 10 | 05 | 00 | 00 | 00 | 00 | |
| 00000050 | 00 | 00 | 14 | 00 | 00 | 00 | 28 | 05 | 00 | 00 | 00 | 00 |(..... |
| 00000060 | 08 | 00 | cc | cc | cc | cc | a0 | 04 | 00 | 00 | 00 | 00 | |
| 00000070 | 02 | 00 | d1 | 86 | 66 | 0f | 65 | 6a | c6 | 01 | ff | ff |f.ej..... |
| 00000080 | ff | 7f | ff | ff | ff | ff | ff | ff | 7f | 17 | d4 | 39 |9.xJ |
| 00000090 | c6 | 01 | 17 | 94 | a3 | 28 | 42 | 4b | c6 | 01 | 17 | 54 |(BK...T\$.z. |
| 000000a0 | c6 | 01 | 08 | 00 | 08 | 00 | 04 | 00 | 02 | 00 | 24 | 00 |\$.\$.... |
| 000000b0 | 02 | 00 | 12 | 00 | 12 | 00 | 0c | 00 | 02 | 00 | 00 | 00 | |
| 000000c0 | 02 | 00 | 00 | 00 | 00 | 00 | 14 | 00 | 02 | 00 | 00 | 00 | |
| 000000d0 | 02 | 00 | 54 | 10 | 00 | 00 | 97 | 79 | 2c | 00 | 01 | 02 | ..T....y,..... |
| 000000e0 | 00 | 00 | 1c | 00 | 02 | 00 | 20 | 00 | 00 | 00 | 00 | 00 | |
| 000000f0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 16 | 00 | 18 | |
| 00000100 | 02 | 00 | 0a | 00 | 0c | 00 | 24 | 00 | 02 | 00 | 28 | 00 |\$...(..... |
| 00000110 | 00 | 00 | 00 | 00 | 00 | 00 | 10 | 00 | 00 | 00 | 00 | 00 | |
| 00000120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000130 | 00 | 00 | 00 | 00 | 00 | 00 | 0d | 00 | 00 | 00 | 2c | 00 |, |
| 00000140 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 04 | 00 | 00 | |
| 00000150 | 00 | 00 | 04 | 00 | 00 | 00 | 6c | 00 | 7a | 00 | 68 | 00 |l.z.h.u... |
| 00000160 | 00 | 00 | 00 | 00 | 00 | 00 | 12 | 00 | 00 | 00 | 4c | 00 |L.i.q. |
| 00000170 | 69 | 00 | 61 | 00 | 6e | 00 | 67 | 00 | 28 | 00 | 4c | 00 | i.a.n.g.(.L.a.r. |
| 00000180 | 72 | 00 | 79 | 00 | 29 | 00 | 20 | 00 | 5a | 00 | 68 | 00 | r.y.). .Z.h.u... |
| 00000190 | 00 | 00 | 00 | 00 | 00 | 00 | 09 | 00 | 00 | 00 | 6e | 00 |n.t.d. |
| 000001a0 | 73 | 00 | 32 | 00 | 2e | 00 | 62 | 00 | 61 | 00 | 74 | 00 | s.2...b.a.t..... |
| 000001b0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001c0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001d0 | 00 | 00 | 1a | 00 | 00 | 00 | 61 | c4 | 33 | 00 | 07 | 00 |a.3..... |
| 000001e0 | 2d | 00 | 07 | 00 | 00 | 00 | 5e | b4 | 32 | 00 | 07 | 00 | -.....^2..... |
| 000001f0 | 00 | 00 | 07 | 00 | 00 | 00 | 97 | b9 | 2c | 00 | 07 | 00 |+. |
| 00000200 | 32 | 00 | 07 | 00 | 00 | 00 | ce | 30 | 33 | 00 | 07 | 00 | 2.....03..... |
| 00000210 | 2e | 00 | 07 | 00 | 00 | 00 | 2a | f1 | 32 | 00 | 07 | 00 |*.2..... |
| 00000220 | 2c | 00 | 07 | 00 | 00 | 00 | 62 | c4 | 33 | 00 | 07 | 00 | ,.....b.3..... |
| 00000230 | 33 | 00 | 07 | 00 | 00 | 00 | 76 | c4 | 33 | 00 | 07 | 00 | 3.....v.3..... |
| 00000240 | 2d | 00 | 07 | 00 | 00 | 00 | 32 | d2 | 2c | 00 | 07 | 00 | -.....2, |

```

00000340 00 20 50 00 02 00 07 00 00 20 54 00 02 00 07 00 . P..... T.....
00000350 00 20 58 00 02 00 07 00 00 20 5c 00 02 00 07 00 . X..... \.....
00000360 00 20 60 00 02 00 07 00 00 20 05 00 00 00 01 05 . `.....
00000370 00 00 00 00 00 05 15 00 00 00 b9 30 1b 2e b7 41 .....0...A
00000380 4c 6c 8c 3b 35 15 01 02 00 00 05 00 00 00 01 05 Ll.;5.....
00000390 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
000003a0 5d 25 64 63 3b 0b 74 54 2f 00 05 00 00 00 01 05 ]%dc;.tT/.....
000003b0 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
000003c0 5d 25 64 63 3b 0b e8 38 32 00 05 00 00 00 01 05 ]%dc;..82.....
000003d0 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
000003e0 5d 25 64 63 3b 0b cd 38 32 00 05 00 00 00 01 05 ]%dc;..82.....
000003f0 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
00000400 5d 25 64 63 3b 0b 5d b4 32 00 05 00 00 00 01 05 ]%dc;.]2.....
00000410 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
00000420 5d 25 64 63 3b 0b 41 16 35 00 05 00 00 00 01 05 ]%dc;.A.5.....
00000430 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
00000440 5d 25 64 63 3b 0b e8 ea 31 00 05 00 00 00 01 05 ]%dc;...1.....
00000450 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
00000460 5d 25 64 63 3b 0b c1 19 32 00 05 00 00 00 01 05 ]%dc;...2.....
00000470 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
00000480 5d 25 64 63 3b 0b 29 f1 32 00 05 00 00 00 01 05 ]%dc;.)2.....
00000490 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
000004a0 5d 25 64 63 3b 0b 0f 5f 2e 00 05 00 00 00 01 05 ]%dc;.._.....
000004b0 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
000004c0 5d 25 64 63 3b 0b 2f 5b 2e 00 05 00 00 00 01 05 ]%dc;./[.....
000004d0 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
000004e0 5d 25 64 63 3b 0b ef 8f 31 00 05 00 00 00 01 05 ]%dc;...1.....
000004f0 00 00 00 00 00 05 15 00 00 00 59 51 b8 17 66 72 .....YQ..fr
00000500 5d 25 64 63 3b 0b 07 5f 2e 00 00 00 00 00 00 49 ]%dc;..._.....I
00000510 d9 0e 65 6a c6 01 08 00 6c 00 7a 00 68 00 75 00 ..ej....l.z.h.u.
00000520 00 00 00 00 00 00 76 ff ff ff 41 ed ce 9a 34 81 .....v...A...4.
00000530 5d 3a ef 7b c9 88 74 80 5d 25 00 00 00 00 76 ff ]:..{.t.]%....v.
00000540 ff ff f7 a5 34 da b2 c0 29 86 ef e0 fb e5 11 0a ....4....).....
00000550 4f 32 00 00 00 00 02....

```

```

( (XIK( ( (AuthorizationData( (0cZNK<9: 8e( (=6 6>1( (AD-
IF-RELEVANT( ( (AD-WIN2K-PAC( ( ( ( ( ( ( ( ( (
( (I [ V6( ( ( ( (W MZ1( B

```

```

00000000 30 82 05 52 30 82 05 4e a0 04 02 02 00 80 a1 82 0..R0..N.....
00000010 05 44 04 82 05 40 .D...@

```

```

N ( ( ( ( (XIK aXM( (: 6 1( V ( ( (XIK aXM( ( (
(VL Z5 ( ( ( ( (cBuffers( ( ( 5 ( ( B(

```

```

00000010 04 00 00 00 ....

```

```

Q( ( ( (cBuffers( ( ( (PAC INFO BUFFER (section 2.4)( (
( ( (Buffers( ( ( ( (Version( ( ( ( ( (
8 88888888B

```

```

00000010 00 00 00 00 ....

```

```

( ( ( ( ( ( ( (PAC_INFO_BUFFER( B(

```

```

00000010                                01 00                ..
00000020  00 00 b0 04 00 00 48 00 00 00 00 00 00 00 00 00  .....H.....

( (PAC_INFO_BUFFER( ( (ulType( ( (8 9M( (8 : 9( ( (
5 ( ( (8 88888889( ( ( (0 (KERB_VALIDATION_INFO
(section 2.5)1 ( ( ( (8 ::( (8 :=( ( (cbBufferSize( ( (
5 ( ( (8 88888<J8 (N (Offset( (><5 ( ( ( (8 :>( (
8 : L ( ( ( (8 88888888/888888<@ (K ( ( ( ( ( (
PACTYPE( ( ( ( ( ( ( ( ( (8 8888889>(3(8 888888<@ ( (
8 888888=M (

N ( ( (PAC_INFO_BUFFER( ( ( ( (PAC_INFO_BUFFER( ( (

00000020                                0a 00                ..
00000030  00 00 12 00 00 00 f8 04 00 00 00 00 00 00 06 00  .....
00000040  00 00 14 00 00 00 10 05 00 00 00 00 00 00 07 00  .....
00000050  00 00 14 00 00 00 28 05 00 00 00 00 00 00 00 00  .....(.....

( ( (PAC_INFO_BUFFER( ( (ulType(8 8888888I (8 8888888>( (
8 8888888 ( ( ( (0 (PAC_CLIENT_INFO (section 2.7)1 ( ( ( (
(0 (PAC_SIGNATURE_DATA (section 2.8)1 ( ( ( ( ( ( (
( ( (08 8888889>(3(8 88888<N@1 (08 8888889>(3(8 88888=981 ( (
08 8888889>38 88888=: @1 (

```

3.1 Logon Authorization Information

```

( ( ( (PAC_INFO_BUFFER (section 2.4)( ( ( ( ( (
( ( ( (8 888888=M ( ( ( ( ( ( ( (
KERB_VALIDATION_INFO( ( ( ( ( ( ( (VL Z5 ( (

00000050                                01 10                ..
00000060  08 00 cc cc cc cc a0 04 00 00 00 00 00 00 00 00 00  .....
00000070  02 00                ..

( ( (8( ( (8 888888=M ( (8 888888 9( ( ( (ZXK( (dJ[ 5
ZXMe ( ( ( ( ( ( ( ( ( ( ( ( ( (VL Z(
( ( (ZXK( ( ( ( ( ( ( ( ( ( (dJ[ 5ZXMe( ( ( (
( ( ( ( ( ( ( (

N ( ( (8( ( ( ( ( ( ( (KERB_VALIDATION_INFO( ( (

00000070  d1 86 66 0f 65 6a c6 01                ..f.ej..

( ( ( ( (LogonTime( ( (FILETIME( ( ( ( ( ( (
( ( ( ( (

00000070                                ff ff ff ff ff ff                .....
00000080  ff 7f ff ff ff ff ff ff ff 7f 17 d4 39 fe 78 4a  .....9.xJ
00000090  c6 01 17 94 a3 28 42 4b c6 01 17 54 24 97 7a 81  .....(BK...T$.z.
000000a0  c6 01                ..

```

[MS-PAC] — v20090114
Privilege Attribute Certificate Data Structure
Copyright © 2009 Microsoft Corporation.
Release: Wednesday, January 14, 2009

K (((((((((ZQ((8 88;;K<>9((8 8888888 (((((((((U(L ((M (([**KERB_SID_AND_ATTRIBUTES \(section 2.2.1\)**](#)) ((& (ZQ(((((((([Q((**LogonDomainId**((((((((B

(8 888: 88: @((B

```
( ([ Q( ( ( L ( ( ( ([ Q( (* 595=5; A A==<9 5
>; >@@99: >59@@<<9<<<6( ([ Q( ( ( ( ( ( (* 595=5; A A==<9 5: >@@99: >5
9@@<<9<<<5; ; A: >8A*( ( ZQ( ( (GROUP_MEMBERSHIP( ( ( ([ Q(
( (
( ( (KERB_VALIDATION_INFO( ( ( ( ( ( ( ( (
```

(PAC CLIENT INFO (section 2.7)) (((((((VL Z5 6

Q((((((((**ClientId**((((8 89K>>I >=/8ML A<A886 (((((((((((O ((((((((N ((((((((((((8 888@ ((((@5 (<5 (([((((((((((((* *6

PAC SIGNATURE DATA (section 2.8)

Q(((SignatureType((8 NNNNN > (59; @ ((((((9>((8 88888=: I((8 88888=; A\$

((((\$

[illegible]

| Trust boundary type | Description |
|------------------------|---|
| Local domain | Domain within the organization's perimeter, managed by the organization's IT department. |
| Non-trusted domain | Domain that is not managed by the organization's IT department, such as a partner or vendor domain. |
| Y - Non-trusted domain | Domain that is not managed by the organization's IT department, such as a partner or vendor domain. (trusted domain object (TDO)) |
| K - Non-trusted domain | Domain that is not managed by the organization's IT department, such as a partner or vendor domain. (5) |
| M - | Domain that is not managed by the organization's IT department, such as a partner or vendor domain. (U) (A) |
| Y - M - | Domain that is not managed by the organization's IT department, such as a partner or vendor domain. (A) |

$$[\mathbb{Q}(\sqrt[6]{2}, \sqrt{-3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}, \sqrt{-3}) : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}]$$

| Action | Rules |
|--------|--|
| I N (| ((((([Q ((U) [(VW (((((((((|
| N [(| <p>(N [(((((([Q (((((((((X) K(((</p> <p>Y (</p> <p>— N (</p> <p>[Q ((((U) [(((((Y ((((((((((</p> <p>M ((Y M ((((((((((</p> |
| M L K(| <p>(M L K(((((((((5 ((((([Q ((((</p> <p>((</p> <p>K N (M ((Y M ((((((((((</p> |
| L [(| <p>(L [(((((([Q ((((((((((</p> <p>(((X) K((((((((((((((([Q (U) [(</p> <p>((((X) K(((((((((((((((</p> <p>(([Q ((X) K(((((((((((((((U) [((((</p> <p>T ((((((((((X) K(([Q (((((</p> <p>((U) [((((((((((</p> <p>I ((([Q (((((((((([595=5: 95DL F 5DK Z F (</p> <p>[(((((5 (((((L (</p> <p>(((((((((((</p> <p>▪ [Q (((((([Q (((X) K(((([Q ((((</p> <p>(((((((((((K Z (((((</p> <p>(ZQ ((((((([Q (U) [((((((((</p> <p>X) K (</p> <p>▪ N (([Q (((X) K((([Q (((((((((T L Q ((</p> |

| SID pattern | Description of the pattern | Action |
|---------------------------|----------------------------|---------|
| [595=5A((| M (L (K (| M.L.K((|
| [595=598((| [(| I N (|
| [595=599((| I (] (| I N (|
| [595=59: ((| Z (| I N (|
| [595=59; ((| ([(] (| I N (|
| [595=59<((| Z (Q (] (| I N (|
| [595=59=((| * (W *(| V N (|
| [595=59@((| T ([(| I N (|
| [595=59A((| T ([(| I N (|
| [595=5 8((| V ([(| I N (|
| [595=5 9((| V (I (L (| I N (|
| [595=5 95 ((| X (([Q (| I N (|
| [595=5 95 5 ((| X (([Q (| I N (|
| [595=5 95 5a5b5Z52((| Q (([Q (0 ((ZQ 1(| I N (|
| [595=5 95 5a5b((| Q ((((| I N (|
| [595=5 95DL F 5Z(ZD=88(| _ 5 ([Q ((| N [(|
| [595=5 95DL F 5=88((| I (| L [(|
| [595=5 95DL F 5=89((| O (| L [(|
| [595=5 95DL F 5=8: (| S (| L [(|
| [595=5 95DL F 5=9: ((| L (I (| L [|

| SID pattern | Description of the pattern | Action |
|--|----------------------------|--------------------------|
| [595=5: 95DL F 5 =9>((| L (K (| L [(|
| [595=5: 95DL F 5 =9 ((| K (X (| L [(|
| [595=5: 95DL F 5 =9@((| [(I (| N [(|
| [595=5: 95DL F 5 =9A((| M (I (| N [(|
| [595=5: 95DL F 5 = 8((| O (X (K (| L [(|
| [595=5: 95DL F 5Z(=88(DE(Z(D(9888((| Z ((5 ((V (| L [(|
| [595=5: 95DL F 5=9@((| (((| |
| [595=5: 95DL F 5=9A((| (((| |
| [595=5: 95DL F 5Z(Z(F E(9888((| Q 5 (((| V (((((((((|
| | (((| U ((((((((5 |
| | (((| (|
| [595=5: 95 5a5b5Z((5a5b(((| I (M (((| Q(((((((((|
| ((D F | L (W (O L W(| ((O L W(((((((|
| | | (([Q (((((((|
| [595=5: 95 5a5b5Z((5a5b(((| I (M ((N (| Q(((((((((|
| ((((| (Q (| ((N Q (((((((|
| ((((| ON Q 1(| (([Q (((((((|
| ((((| Q (((| (((((((((N Q ((|
| (((| (| (([Q (((((((|
| | | (((((((((N Q ((|
| | | ((((((((([Q (|
| | | ((((((((|
| [595=5: ; ((| J 5 (L (| I N (|
| [595=5: ; 5=<<((| I (| I N (|
| [595=5: ; 5=<=(|] (| I N (|
| [595=5: ; 5=<>((| O (| I N (|
| [595=5: ; 5=< ((| X (] (| I N (|
| [595=5: ; 5=<@((| I (W (| I N (|
| [595=5: ; 5=<A((| [(W (| I N (|
| [595=5: ; 5==8((| X (W (| I N (|

| Security parameter | Section |
|--------------------|---------|
|--------------------|---------|

[illegible]

[MS-PAC] — v20090114
Privilege Attribute Certificate Data Structure
Copyright © 2009 Microsoft Corporation.
Release: Wednesday, January 14, 2009

(R (: 88A(K((dJ[5XI Kq(L (: 88@

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

- I((((((((q
- I ((((((((q
- I(((q
- (((((((q
- K ((((q

Minor((((((((M((((((((B(((((((

Editorial((((((((B(((((((

No changes((((((((B(((((((

U ((((((((((q

- V ((q
- K (q
- K (q
- V _ (((q
- _ (((q
- _ (((q
- V (((q
- X ((q
- X ((q
- V (((((((q
- K (((((q
- K (((((q
- V ((((((((q
- X (((((((q
- X (((((((q
- V ((((((q
- K (((((q

7 Index

A(

I _____(
I _____(_____(

C(

K _____(
K _____(_____(
K _____(
K _____(_____(
K _____(_____(
_____(
K _____(

D(

L _____(_____(5 _____(

E(

M _____(
_____ (_____(
_____ (_____(_____(
_____ (_____(
_____ (_____(

F(

N (5 _____ 5 _____(
N _____(
_____ (5 _____(
_____ (_____(
[Q (5 _____(

G(

O _____(
OZW] XgUMUJMJZ[PQX _____(

I(

Q _____(_____(_____(
Q _____(_____(
Q _____(

K(

SMZJg[Q.gI VL.gI ZQ] M _____(
SMZJg I TQ.I QWgQ/NW _____(

L(

T _____(
T _____(_____(_____(

N(

V _____(_____(
V TUg[] XXTMU MV I TgKZML.MV Q T _____(

P(

XI K(_____(
XI K((5 _____(
XI KgKTQM gQ/NW _____(
XI KgKZML.MV Q TgLI I _____(
XI KgKZML.MV Q TgQ/NW _____(
XI KgQ/NWgJ] NNMZ _____(
XI Kg[QVI] ZMgLI I _____(
XI K aXM _____(
X _____((5 _____(
XOZW] XgUMUJMJZ[PQX _____(
XSMZJg[Q.gI VL.gI ZQ] M _____(
XV TUg[] XXTMU MV I TgKZML.MV Q T _____(
XXI KgKZML.MV Q TgLI I _____(
X <] gL MTMOI QWgQ/NW _____(
X MKXSOG[] XXTMU MV I TgKZML _____(

R(

Z _____(
_____ (_____(
_____ (_____(
_____ (_____(
Z _____(

S(

[<] gL MTMOI QWgQ/NW _____(
[MKXSOG[] XXTMU MV I TgKZML _____(
[_____(_____(
_____ (_____(_____(
_____ (_____(
_____ (_____(
_____ (_____(
[Q _____(_____(
[Q _____(_____(
_____ (XI K _____(
[Q _____(
_____ (_____(
[_____(_____(5 _____(
_____ (_____(
[_____(_____(
[_____(_____(_____(_____(
_____ (_____(_____(
_____ (_____(
XI K _____(_____(5 _____(
_____ (_____(5 _____(

T(

_____ (X K(_____(
_____(_____(
_____(5 _____(

U(

] XVg L V[g Q/NW(_____(

V(

_____ 5 _____ (_____(
_____(

W(

_____ (_____(