Dia 1

Positionering presentatie:

- geen (pre-) sales, geen bit-niveau uitwerking
- wel overzicht 'traditionele' authenticatie versus 'nieuwe' authenticatie
- korte verklaring verschil authenticatie versus authorisatie
- nadruk op werkwijze, gebruikerservaring

Dia 2

Er is ruimte voor vragen, (kleine) diskussies, mogelijk een korte demo

Bedoeling is een overzicht te geven en de animo voor een sig-bijeenkomst te polsen, waar dan gericht en diepgaander authenticatie kan worden uitgewerkt.

Dia 3

Ton van der Zwet, (ton.vanderzwet@oooovms.dyndns.org) sinds versie 1.x met VMS bezig en lang lid van OpenVMS gebruikersverenigingen (DECUS, ...)

Deze presentatie is ontstaan omdat ik geïntresseerd geraakt ben in de nieuwe mogelijkheden die beschikbaar kwamen met de komst van ACME, Kerberos en LDAP op OpenVMS. Als gebruiker van LINUX, OpenSource en met name OpenOffice zijn mijn interesses al langer breder dan de VMS-only producten. In deze open wereld zijn VMS-only toepassingen nauwelijks bekend, maar de OpenSource functioneel “gelijkwaardige” producten des te meer. Het gebruiken van de kwaliteiten van OpenVMS in deze wereld is voor mij een uitdaging.

Het uitzoeken van de mogelijkheden van OpenVMS in een complexe client/server omgeving vereist een aantal (OpenVMS) servers. Deze hebben we heel snel en flexibel kunnen realiseren door een aantal laptop’s te voorzien van een ALPHA emulator (Personal Alpha). Deze methode is ook voor een hobbyist, eventueel met de hulp van een aantal mede-hobbyisten, zonder hoge kosten te realiseren.

Bij mijn werkgever is er al langer een wens om tot een single-signon werkwijze te komen. Deze is echter gebaseerd op een windows/AD/E-dir omgeving. Hoe past OpenVMS in dit plaatje...

Mijn dank gaat uit naar Fekko Stubbe en Martin Borgman voor hulp bij het realiseren van dit onderzoek. Zonder hun inhoudelijke bijdragen en feedback zou deze presentatie niet tot stand gekomen zijn.

Dia 4

De sysuaf vormt de basis voor de lokale authenticatie en autorisatie database. Voor het authenticatie gebruik wordt de index (username) - sleutel (password) combinatie vergeleken met de authenticatie aanvraag. Username komt functioneel overeen met de public-key; het password met de (shared) secret key. Dit is een long term key. (longterm kan zijn 1-malig tot oneindig zijn, afhankelijk van de beveiligings-strategie)

Zijstap: ALF (automatic login facility) met sysalf als database werkt op basis van poortnaam (device), een userproces wordt gestart zodra er een bijvoorbeeld een return wordt ingegeven op deze poort. Bijvoorkeur te gebruiken daar waar slechts één applicatie gebruikt wordt, bijvoorbeeld point of sales terminals.

Decnet proxy database heeft de vorm van “nodename”::”remote user” mapped naar “lokale user”. Velden in deze database mogen wildcards zijn! Wordt niet aanbevolen voor interaktief gebruik!

Batch: het submitten van een batchjob kan alleen vanuit een geauthenticeerd proces met de juiste authorisatie. De job-gegevens worden opgeslagen in de beveiligde queue-database. Een eenmaal gesubmitte job is in principe vwb authenticatie niet meer te wijzigen .

Voor een TCP/IP deamon wordt door een listener op een vastgesteld poortnummer geluisterd. Zodra daar een volgens het protocol geldige activiteit plaatsvind, wordt er lokaal een aktiviteit uitgevoerd (bijvoorbeeld telnet: start een nieuwe telnet sessie onder het account van de nieuwe gebruiker)

Authorisatie: wat zijn de resources die het proces mag benaderen/gebruiken/verwijderen. Bijvoorbeeld CPU-time, memory, devices, files --> “objecten”

Dia 5

Authenticatie betreft het zekerstellen van de identiteit van de aanvrager. De manier waarop dit veelal gebeurt is gebaseerd op het vertrouwen van één of meerdere kenmerken/attributen van de aanvrager. De traditionele attributen van de aanvrager zijn een unieke username en het bijbehorende password. Deze combinatie is ook vastgelegd in de authenticatie/authorisatie databases van de server. De username is te vergelijken met een public key en wordt gebruikt als index in de databases. Nadelen van deze methode zijn onder andere een beperkte lange termijn veiligheid omdat bij elke authenticatie dezelfde combinatie moet worden gebruikt. (kans op onderschepping, maatregelen: korte password lifetime, encrypted verbindingen)

Nieuwe technieken maken het gebruik van andere attributen mogelijk: bijvoorbeeld biometrische authenticatie

Een andere oplossingsrichting is de encryptie van de communicatie in combinatie met wederzijdse authenticatie voordat er geauthoriseerd kan worden. Deze methodiek wordt gebruikt door kerberos: Lokaal eenmalige authenticatie dmv de traditionele methode, daarna wordt er door het gebruik van een uniek eenmalig ticket met beperkte levensduur (TGT) per service een andere unieke eenmalige authenticatiekey aangemaakt. Ook voor de kerberos omgeving geldt dat er een trustrelatie tussen de authenticator (ook AS, of KDC genoemd) en de serviceleveranciers en clienten moet bestaan. In de volgende dias wordt aangegeven hoe kerberos dit realiseerd.

Dia 6

Het ACME mechanisme is de, door HP gedocumenteerde en beschikbaar gestelde interface voor de authenticatie van “gebruikers”.

Kerberos is een beveiligd, uitgaande van een onveilig (inter)netwerk, authenticatieprotocol. Het protocol is bedoeld voor client-server omgevingen, met ruime interpretatie van clients en servers (services).

LDAP, X.500 zijn gestandaardiseerde protocollen die het gebruik van directories (verzamelingen gegevens veelal gebruikt tbv authenticatie en authorisatie) beschrijven.

X.500 is gebaseerd op het OSI-model (7 laags-structuur), met de daarbij behorende zware, geformaliseerde protocol-beschrijvingen. Een X.500 implementatie vereiste behoorlijk veel ICT

resources.

LDAP is een een afgeslankte implementatie van directory gebruiksprotocollen. LDAP vereist (veel) minder ICT resources.

HP OpenVMS Enterprise Directory is een X.500 implementatie met DECNET- V en TCP/IP (LDAP) koppelingen.

Dia 7

Het ACME mechanisme is de, door HP gedocumenteerde en beschikbaar gestelde interface voor de authenticatie van "gebruikers". Doordat dit mechanisme extendable is, kunnen er allerlei (toekomstige) authenticatiemethodieken op een OpenVMS systeem gebruikt gaan worden. Het vereist "alleen" een het schrijven van een nieuwe extensie/plug-in. Te denken valt aan bijvoorbeeld biometrische authenticatiemethoden (iris-scan, vingerafdruk, ...) of nieuwe technologieën (RFID,...)

Door HP zijn een aantal modules (extenties) geleverd (Traditioneel, MSLM, LDAP/MSAD, Kerberos)

Dia 8

Kerberos is ontwikkeld om authenticatie te doen over niet veilige verbindingen. Deze presentatie gaat uit van een Kerberos 5 implementatie. Microsoft gebruikt Kerberos 5 in AD

Kerberos is ontwikkeld als een authenticatie machine voor project Athena van het MIT in 1983. Het is vrijgegeven als Open Source in 1987 en in 1993 is het een IETF standard geworden.

Links naar de websites:

Website van het MIT, waar veel info te vinden valt:

http://web.mit.edu/kerberos/

Website van het kerberos consortium:

http://www.kerberos.org/

Onder de tab software zijn whitepapers te vinden.

http://www.kerberos.org/software/index.html

Dia 9

LDAP is een netwerkprotocol dat beschrijft hoe gegevens uit directoryservices benaderd moeten worden over bijvoorbeeld TCP/IP

For LDAP V2:

- RFC 1777 Lightweight Directory Access Protocol
- RFC 1558 A String Representation of LDAP Search Filters
- RFC 1778 The String Representation of Standard Attribute Syntaxes

For LDAP V3:

- RFC 2251 Lightweight Directory Access Protocol (v3)
- RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions

• RFC 2253 Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names

• RFC 2254 The String Representation of LDAP Search Filters

• RFC 2255 The LDAP URL Format

• RFC 2256 A Summary of the X.500 (96) User Schema for use with LDAP V3

MS AD is een Microsoft X.500 implementatie met Kerberos 5 voor authenticatie. AD registreerd LDAP en Kerberos poorten in Dynamic DNS (Bind 8 en hoger)

X.500 is een standaard die de protocollen definieert voor directoryservices om te gebruiken voor het uitwisselen van informatie. X.500 is ontwikkeld door de ITU-T (toen nog CITT genaamd) in samenwerking met *ISO*.

De opbouw van de X.500-standaard volgt het OSI-model

DUA – Directory User Agent

DSA – Directory System Agent

Directory Protocollen in X.500

DAP - Directory Access Protocol (DUA-DSA)

DSP - Directory System Protocol (DSA-DSA)

DISP - Directory Information Shadowing Protocol (DSA-DSA)

DOP - Directory Operational Binding Management Protocol (DSA-DSA)

(LDAP – Lightweight Directory Access Protocol)

HP Enterprise directory is een volledige X500 directory implementatie (ISO/OSI-model) waarbij in versie 5.4 de noodzaak om decnet te gebruiken vervallen is. Met deze versie is ook een TCP/IP-only benadering met LDAP mogelijk

Dia 10

Deze opmerking komt uit de ACME kerberos documentatie. Op dit moment is de status van de Kerberos agent “nog niet op productie-kwaliteit”

De voordelen van de ACME-integratie zijn echter dat bijvoorbeeld de password synchronisatie over het hele REALM bij het inloggen via ACME/KERBEROS gebeurt. Wij zijn nog met onderzoek bezig naar de mogelijkheden en inpasbaarheid van KERBEROS in een ACME omgeving.

Dia 11

Deze dia laat in grote stappen de werking van kerberos zien: Belangrijk is dat er altijd kontakt (tbv ticket, credentials) moet worden opgenomen met een KDC voordat er door een (application) server service verleend kan worden. Alle componenten (users, clients, hosts, services, kdc,...) moeten met hun LTK's opgenomen zijn in de “databases” (KDC alles, overigen alleen hun eigen keys).

Door encryptie, wederzijdse bekendheid (trust), single session (encryption) keys en tijdigheid als randvoorwaarde te gebruiken, is de betrouwbaarheid (positieve authenticatie) hoog. De strikte naleving van alle randvoorwaarden is echter cruciaal. Het niet invullen van een van de randvoorwaardes leidt tot afwijzing.

Voor meer detail zijn er dia's uit de whitepapers van het kerberos consortium toegevoegd. Tevens is er een stapsgewijze beschrijving van het authenticatie mechanisme (zonder tgt-schil) opgenomen.

Dia 12

Foto (of aanwijzen) van de lab-opstelling

Inrichting twee (drie) VMS 8.3 servers, 1 KDC, 1 (2) client

Ktelnet login client-(KDC)server en v.v., Ktelnet login client-client v.v.

Conclusies:
tcp/ip (NTP, DNS, local host, ...) inrichting kritisch!
Case-sensitive
Timing handelingen kritisch
Foutmeldingen cryptisch
Inzicht werking is cruciaal

Nog uit te voeren:
acme-koppeling
AD/ldap/E-dir/HPED integratie testen (vereist uitbreiding LAB...)

Dia 13

Te zien zijn twee laptops verbonden via een simpele netwerk-switch, ieder met een personal alpha implementatie. Beide draaien onder OpenVMS 8.3 met kerberos 3.1. Door gebruik te maken van een USB-stick kan snel een extra machine (kopie stick) worden opgetuigd. De linker machine is ingericht als KDC. De rechter machine is een client (applicatie server). Een aantal test-users zijn opgevoerd, en kunnen dmv ktelnet (telnet/authen 'node' 2323) of ssh single sign-on op deze 'infrastructuur' werken. Ook ReflectionX is in de single sign-on mode te gebruiken.

Dia 14

Ook als de “tijd” (show time) op alle systemen goed staat, moet de UTC tijd (=TIJD MET DIFF) gelijk zijn. Gebruik zonodig de procedure sys$startup:utc$time_setup.com

```
STAR> sh log *time*
  "SYS$LOCALTIME" = "SYS$SYSROOT:
[SYS$ZONEINFO.SYSTEM.EUROPE]AMSTERDAM."
  "SYS$TIMEZONE_DAYLIGHT_SAVING" = "1"
  "SYS$TIMEZONE_DIFFERENTIAL" = "7200"
  "SYS$TIMEZONE_NAME" = "CEST"
  "SYS$TIMEZONE_RULE" = "CET-1CEST-2,M3.5.0/02,M10.4.0/03"
STAR> sh time
  12-NOV-2008 10:12:54
STAR> sh log *time*
```

"SYS$LOCALTIME" = "SYS$SYSROOT:
[SYS$ZONEINFO.SYSTEM.EUROPE]AMSTERDAM."

"SYS$TIMEZONE_DAYLIGHT_SAVING" = "0"

"SYS$TIMEZONE_DIFFERENTIAL" = "3600"

"SYS$TIMEZONE_NAME" = "CET"

"SYS$TIMEZONE_RULE" = "CET-1CEST-2,M3.5.0/02,M10.4.0/03"

STAR> sh time

12-NOV-2008 10:15:27

Breng eerst de netwerkadministratie op orde, let op eenduidig gebruik FQDN, case, alias, DNS, local host tabellen, ip-adressen ipv FQDN. Test alle netwerkfunctionaliteiten beide kanten op. Let op firewall instellingen.

Eerst de KDC dan de hosts (services) op de KDC, dan de hosts local keytab, dan de users

Als er een wijziging nodig is, synchroniseer alle locaties waar die info (credentials, keytab's). Omdat de credentials in een lokale cache worden opgeslagen en zolang de lifetime (bijvoorbeeld 8 uur) niet verlopen is door een KINIT niet vernieuwd worden is KINIT alleen NIET voldoende: gebruik eerst een KDESTROY, dan een KINIT.

De wereld buiten OpenVMS is CASE-sensitive, Kerberos is geen uitzondering.... Zorg voor eenduidigheid bij het opvoeren van gegevens.

Namen binnen een REALM moeten uniek zijn, denk daarbij ook aan default-namen en functies... De username SYSTEM geeft in een Kerberos realm toegang tot alle servers op het lokale system-account.... Een apart password is daarbij niet meer nodig ;-)

Nadat een ontwerp gemaakt is, test de opzet op onverwachte effecten in een "LAB", Voer gefaseerd in: Tijdinstellingen en synchronisatie dmv NTP, Breng TCP/IP over het hele REALM in kaart en werk bij naar een ontwerp.

Dia 15

Dia 16

Deze dia komt uit "**The MIT Kerberos Administrator's How-to Guide, draft 1.0"** van de site van het kerberos consortium. http://www.kerberos.org/software/adminkerberos.pdf

Deze dia is nodig (legenda) om de volgende dias te kunnen lezen.

Dia 17

Deze dia komt uit "**The MIT Kerberos Administrator's How-to Guide, draft 1.0"** van de site van het kerberos consortium. http://www.kerberos.org/software/adminkerberos.pdf

Deze dia is functioneel gelijk aan dia 11, maar is tijdens de presentatie moeilijker te lezen....

Dia 18

Deze dia komt uit "**The MIT Kerberos Administrator's How-to Guide, draft 1.0"** van de site van het kerberos consortium. http://www.kerberos.org/software/adminkerberos.pdf

Deze dia geeft in meer detail de eerste stap (het verkrijgen van het TGT) weer. Belangrijk is dat de user zijn wachtwoord:

1 slechts 1-maal nodig heeft (per TGT lifetime)

2 zijn wachtwoord nooit unencrypted tussen de clients-host en de KDC verstuurd wordt.

Dia 19

Deze dia komt uit "**The MIT Kerberos Administrator's How-to Guide, draft 1.0"** van de site van het kerberos consortium. http://www.kerberos.org/software/adminkerberos.pdf

Deze dia geeft in meer detail de tweede stap (het verkrijgen van het TGS) weer. Belangrijk is dat de sessionkey:

1 opgeslagen wordt in de ticket cache

2 'onder water' gewijzigd wordt (ticket lifetime)

Dia 20

Simpele weergave van de eerste stap in de authenticatie tbv een service (geen tgt schil)

Dia 21

Antwoord van de AS bestaat uit twee pakketten:

1 user's credentials, encrypted met de user's LTK, met als inhoud de session random key en de service naam

2 service ticket, encrypted met de service's LTK, met als inhoud dezelfde session random key en de users name

Dia 22

De connectieaanvraag van de user naar de service bestaat (o.a.?) uit een tweetal pakketten:

-authenticator, deze bestaat (o.a.?) uit een timestamp encrypted met de session key

-service ticket, deze wordt ongewijzigd meegestuurd (zie vorige dia). Door de met de service's LTK encrypted session key en username kan de service niet alleen de authenticator decrypten, maar tegelijkertijd impliciet de authenticiteit valideren van de aanvraag, immers de AS heeft beide geauthenticeerd en heeft beider LTK's gebuikt voor de encryptie.

Windows event log entries often contain Kerberos failure codes (for an example, please see security event 676). These failure codes are the original error codes from the Kerberos RFC 1510 (see page 83 for the complete list).

For your convenience, we have extracted the error codes below and added some of our comments. Please note that in event log entries, a hexedicimal code is used (the number starts with 0x). Be sure to not mistakenly look up the decimal code below.

1 Error codes

Kerberos Error Label	Hex	Dec	Meaning or MIT code	Explanation
KDC_ERR_NONE	0x0	0	No error	
KDC_ERR_NAME_EXP	0x1	1	Client's entry in database has expired	
KDC_ERR_SERVICE_EXP	0x2	2	Server's entry in database has expired	
KDC_ERR_BAD_PVNO	0x3	3	Requested protocol version number not supported	
KDC_ERR_C_ OLD_MAST_KVNO	0x4	4	Client's key encrypted in oldmaster key	
KDC_ERR_S_ OLD_MAST_KVNO	0x5	5	Server's key encrypted in old master key	
KDC_ERR_C_ PRINCIPAL_UNKNOWN	0x6	6	Client not found in Kerberos database	• We have seen this code when Active Directory replication does not work correctly. In this case, it is possible that e.g. a computer account joins the domain using one DC. Then, this information is not replicated within AD. If the computer then tries to authenticate to another DC, it is not found there, resulting in this error code. • Also, make sure time synchronization between DCs is

				working well.
KDC_ERR_S_ PRINCIPAL_UNKNOWN	0x7	7	Server not found in Kerberos database	Could be the same cause as error 6 above.
KDC_ERR_ PRINCIPAL_NOT_UNIQUE	0x8	8	Multiple principal entries in database	
KDC_ERR_NULL_KEY	0x9	9	The client or server has a null key	
KDC_ERR_CANNOT_ POSTDATE	0xa	10	Ticket not eligible for postdating	
KDC_ERR_NEVER_VALID	0xb	11	Requested start time is later than end time	
KDC_ERR_POLICY	0xc	12	KDC policy rejects request	
KDC_ERR_BADOPTION	0xd	13	KDC cannot accommodate requested option	
KDC_ERR_ ETYPE_NOSUPP	0xe	14	KDC has no support for encryption type	
KDC_ERR_SUMTYPE_NOSUPP	0xf	15	KDC has no support for checksum type	
KDC_ERR_ PADATA_TYPE_NOSUPP	0x10	16	KDC has no support for padata type	
KDC_ERR_TRTYPE_NOSUPP	0x11	17	KDC has no support for transited type	
KDC_ERR_ CLIENT_REVOKED	0x12	18	Clients credentials have been revoked	This is due to a workstation restriction on the account, or a logon time restriction, or logon attempt outside logon hours, or accout disabled, expired, or locked out.
KDC_ERR_ SERVICE_REVOKED	0x13	19	Credentials for server have been revoked	
KDC_ERR_TGT_REVOKED	0x14	20	TGT has been revoked	

KDC_ERR_CLIENT_NOTYET	0x15	21	Client not yet valid - try again later	
KDC_ERR_ SERVICE_NOTYET	0x16	22	Server not yet valid - try again later	
KDC_ERR_KEY_ EXPIRED	0x17	23	Password has expired - change password to reset	
KDC_ERR_ PREAUTH_FAILED	0x18	24	Pre-authentication information was invalid	Be sure to check time synchronization within your tree.
KDC_ERR_ PREAUTH_REQUIRED	0x19	25	Additional pre-authentication required	
KRB_AP_ERR_ BAD_INTEGRITY	0x1f	31	Integrity check on decrypted field failed	
KRB_AP_ERR_TKT_ EXPIRED	0x20	32	Ticket expired	
KRB_AP_ERR_TKT_NYV	0x21	33	Ticket not yet valid	
KRB_AP_ERR_REPEAT	0x22	34	Request is a replay	
KRB_AP_ERR_NOT_US	0x23	35	The ticket isn't for us	
KRB_AP_ERR_BADMATCH	0x24	36	Ticket and authenticator don't match	
KRB_AP_ERR_SKEW	0x25	37	Clock skew too great	
KRB_AP_ERR_BADADDR	0x26	38	Incorrect net address	
KRB_AP_ERR_ BADVERSION	0x27	39	Protocol version mismatch	
KRB_AP_ERR_MSG_TYPE	0x28	40	Invalid msg type	
KRB_AP_ERR_MODIFIED	0x29	41	Message stream modified	
KRB_AP_ERR_ BADORDER	0x2a	42	Message out of order	
KRB_AP_ERR_ BADKEYVER	0x2c	44	Specified version of key	

			is not available	
KRB_AP_ERR_NOKEY	0x2d	45	Service key not available	
KRB_AP_ERR_MUT_FAIL	0x2e	46	Mutual authentication failed	
KRB_AP_ERR_ BADDIRECTION	0x2f	47	Incorrect message direction	
KRB_AP_ERR_METHOD	0x60	48	Alternative authentication method required*	
KRB_AP_ERR_BADSEQ	0x31	49	Incorrect sequence number in message	
KRB_AP_ERR_ INAPP_CKSUM	0x32	50	Inappropriate type of checksum in message	
KRB_ERR_GENERIC	0x3C	60	Generic error (description in e-text	
KRB_ERR_FIELD _TOOLONG	0x3D	61	Field is too long for this implementation	

Uit:

2 Kerberos V5 System Administrator's Guide

http://web.mit.edu/kerberos/www/krb5-1.5/krb5-1.5.4/doc/krb5-admin/index.html#Top

3 A.1.1 Kerberos V5 Library Error Codes

This is the Kerberos v5 library error code table. Protocol error codes are ERROR_TABLE_BASE_krb5 + the protocol error code number; other error codes start at ERROR_TABLE_BASE_krb5 + 128.

1. KRB5KDC_ERR_NONE: No error
2. KRB5KDC_ERR_NAME_EXP: Client's entry in database has expired
3. KRB5KDC_ERR_SERVICE_EXP: Server's entry in database has expired
4. KRB5KDC_ERR_BAD_PVNO: Requested protocol version not supported
5. KRB5KDC_ERR_C_OLD_MAST_KVNO: Client's key is encrypted in an old master key

6. KRB5KDC_ERR_S_OLD_MAST_KVNO: Server's key is encrypted in an old master key
7. KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN: Client not found in Kerberos database
8. KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN: Server not found in Kerberos database
9. KRB5KDC_ERR_PRINCIPAL_NOT_UNIQUE: Principal has multiple entries in Kerberos database
10. KRB5KDC_ERR_NULL_KEY: Client or server has a null key
11. KRB5KDC_ERR_CANNOT_POSTDATE: Ticket is ineligible for postdating
12. KRB5KDC_ERR_NEVER_VALID: Requested effective lifetime is negative or too short
13. KRB5KDC_ERR_POLICY: KDC policy rejects request
14. KRB5KDC_ERR_BADOPTION: KDC can't fulfill requested option
15. KRB5KDC_ERR_ETYPE_NOSUPP: KDC has no support for encryption type
16. KRB5KDC_ERR_SUMTYPE_NOSUPP: KDC has no support for checksum type
17. KRB5KDC_ERR_PADATA_TYPE_NOSUPP: KDC has no support for padata type
18. KRB5KDC_ERR_TRTYPE_NOSUPP: KDC has no support for transited type
19. KRB5KDC_ERR_CLIENT_REVOKED: Clients credentials have been revoked
20. KRB5KDC_ERR_SERVICE_REVOKED: Credentials for server have been revoked
21. KRB5KDC_ERR_TGT_REVOKED: TGT has been revoked
22. KRB5KDC_ERR_CLIENT_NOTYET: Client not yet valid - try again later
23. KRB5KDC_ERR_SERVICE_NOTYET: Server not yet valid - try again later
24. KRB5KDC_ERR_KEY_EXP: Password has expired
25. KRB5KDC_ERR_PREAUTH_FAILED: Preauthentication failed
26. KRB5KDC_ERR_PREAUTH_REQUIRED: Additional pre-authentication required
27. KRB5KDC_ERR_SERVER_NOMATCH: Requested server and ticket don't match
28. KRB5PLACEHOLD_27: KRB5 error code 27
29. KRB5PLACEHOLD_28: KRB5 error code 28
30. KRB5PLACEHOLD_29: KRB5 error code 29
31. KRB5PLACEHOLD_30: KRB5 error code 30
32. KRB5KRB_AP_ERR_BAD_INTEGRITY: Decrypt integrity check failed
33. KRB5KRB_AP_ERR_TKT_EXPIRED: Ticket expired
34. KRB5KRB_AP_ERR_TKT_NYV: Ticket not yet valid
35. KRB5KRB_AP_ERR_REPEAT: Request is a replay
36. KRB5KRB_AP_ERR_NOT_US: The ticket isn't for us
37. KRB5KRB_AP_ERR_BADMATCH: Ticket/authenticator don't match
38. KRB5KRB_AP_ERR_SKEW: Clock skew too great
39. KRB5KRB_AP_ERR_BADADDR: Incorrect net address
40. KRB5KRB_AP_ERR_BADVERSION: Protocol version mismatch
41. KRB5KRB_AP_ERR_MSG_TYPE: Invalid message type
42. KRB5KRB_AP_ERR_MODIFIED: Message stream modified
43. KRB5KRB_AP_ERR_BADORDER: Message out of order
44. KRB5KRB_AP_ERR_ILL_CR_TKT: Illegal cross-realm ticket
45. KRB5KRB_AP_ERR_BADKEYVER: Key version is not available
46. KRB5KRB_AP_ERR_NOKEY: Service key not available
47. KRB5KRB_AP_ERR_MUT_FAIL: Mutual authentication failed
48. KRB5KRB_AP_ERR_BADDIRECTION: Incorrect message direction
49. KRB5KRB_AP_ERR_METHOD: Alternative authentication method required
50. KRB5KRB_AP_ERR_BADSEQ: Incorrect sequence number in message
51. KRB5KRB_AP_ERR_INAPP_CKSUM: Inappropriate type of checksum in message
52. KRB5KRB_AP_PATH_NOT_ACCEPTED: Policy rejects transited path
53. KRB5KRB_ERR_RESPONSE_TOO_BIG: Response too big for UDP, retry with TCP
54. KRB5PLACEHOLD_53: KRB5 error code 53
55. KRB5PLACEHOLD_54: KRB5 error code 54
56. KRB5PLACEHOLD_55: KRB5 error code 55

57. KRB5PLACEHOLD_56: KRB5 error code 56
58. KRB5PLACEHOLD_57: KRB5 error code 57
59. KRB5PLACEHOLD_58: KRB5 error code 58
60. KRB5PLACEHOLD_59: KRB5 error code 59
61. KRB5KRB_ERR_GENERIC: Generic error (see e-text)
62. KRB5KRB_ERR_FIELD_TOOLONG: Field is too long for this implementation
63. KRB5PLACEHOLD_62: KRB5 error code 62
64. KRB5PLACEHOLD_63: KRB5 error code 63
65. KRB5PLACEHOLD_64: KRB5 error code 64
66. KRB5PLACEHOLD_65: KRB5 error code 65
67. KRB5PLACEHOLD_66: KRB5 error code 66
68. KRB5PLACEHOLD_67: KRB5 error code 67
69. KRB5PLACEHOLD_68: KRB5 error code 68
70. KRB5PLACEHOLD_69: KRB5 error code 69
71. KRB5PLACEHOLD_70: KRB5 error code 70
72. KRB5PLACEHOLD_71: KRB5 error code 71
73. KRB5PLACEHOLD_72: KRB5 error code 72
74. KRB5PLACEHOLD_73: KRB5 error code 73
75. KRB5PLACEHOLD_74: KRB5 error code 74
76. KRB5PLACEHOLD_75: KRB5 error code 75
77. KRB5PLACEHOLD_76: KRB5 error code 76
78. KRB5PLACEHOLD_77: KRB5 error code 77
79. KRB5PLACEHOLD_78: KRB5 error code 78
80. KRB5PLACEHOLD_79: KRB5 error code 79
81. KRB5PLACEHOLD_80: KRB5 error code 80
82. KRB5PLACEHOLD_81: KRB5 error code 81
83. KRB5PLACEHOLD_82: KRB5 error code 82
84. KRB5PLACEHOLD_83: KRB5 error code 83
85. KRB5PLACEHOLD_84: KRB5 error code 84
86. KRB5PLACEHOLD_85: KRB5 error code 85
87. KRB5PLACEHOLD_86: KRB5 error code 86
88. KRB5PLACEHOLD_87: KRB5 error code 87
89. KRB5PLACEHOLD_88: KRB5 error code 88
90. KRB5PLACEHOLD_89: KRB5 error code 89
91. KRB5PLACEHOLD_90: KRB5 error code 90
92. KRB5PLACEHOLD_91: KRB5 error code 91
93. KRB5PLACEHOLD_92: KRB5 error code 92
94. KRB5PLACEHOLD_93: KRB5 error code 93
95. KRB5PLACEHOLD_94: KRB5 error code 94
96. KRB5PLACEHOLD_95: KRB5 error code 95
97. KRB5PLACEHOLD_96: KRB5 error code 96
98. KRB5PLACEHOLD_97: KRB5 error code 97
99. KRB5PLACEHOLD_98: KRB5 error code 98
100. KRB5PLACEHOLD_99: KRB5 error code 99
101. KRB5PLACEHOLD_100: KRB5 error code 100
102. KRB5PLACEHOLD_101: KRB5 error code 101
103. KRB5PLACEHOLD_102: KRB5 error code 102
104. KRB5PLACEHOLD_103: KRB5 error code 103
105. KRB5PLACEHOLD_104: KRB5 error code 104
106. KRB5PLACEHOLD_105: KRB5 error code 105
107. KRB5PLACEHOLD_106: KRB5 error code 106
108. KRB5PLACEHOLD_107: KRB5 error code 107

109. KRB5PLACEHOLD_108: KRB5 error code 108
110. KRB5PLACEHOLD_109: KRB5 error code 109
111. KRB5PLACEHOLD_110: KRB5 error code 110
112. KRB5PLACEHOLD_111: KRB5 error code 111
113. KRB5PLACEHOLD_112: KRB5 error code 112
114. KRB5PLACEHOLD_113: KRB5 error code 113
115. KRB5PLACEHOLD_114: KRB5 error code 114
116. KRB5PLACEHOLD_115: KRB5 error code 115
117. KRB5PLACEHOLD_116: KRB5 error code 116
118. KRB5PLACEHOLD_117: KRB5 error code 117
119. KRB5PLACEHOLD_118: KRB5 error code 118
120. KRB5PLACEHOLD_119: KRB5 error code 119
121. KRB5PLACEHOLD_120: KRB5 error code 120
122. KRB5PLACEHOLD_121: KRB5 error code 121
123. KRB5PLACEHOLD_122: KRB5 error code 122
124. KRB5PLACEHOLD_123: KRB5 error code 123
125. KRB5PLACEHOLD_124: KRB5 error code 124
126. KRB5PLACEHOLD_125: KRB5 error code 125
127. KRB5PLACEHOLD_126: KRB5 error code 126
128. KRB5PLACEHOLD_127: KRB5 error code 127
129. KRB5_ERR_RCSID: (RCS Id string for the krb5 error table)
130. KRB5_LIBOS_BADLOCKFLAG: Invalid flag for file lock mode
131. KRB5_LIBOS_CANTREADPWD: Cannot read password
132. KRB5_LIBOS_BADPWDMATCH: Password mismatch
133. KRB5_LIBOS_PWDINTR: Password read interrupted
134. KRB5_PARSE_ILLCHAR: Illegal character in component name
135. KRB5_PARSE_MALFORMED: Malformed representation of principal
136. KRB5_CONFIG_CANTOPEN: Can't open/find Kerberos configuration file
137. KRB5_CONFIG_BADFORMAT: Improper format of Kerberos configuration file
138. KRB5_CONFIG_NOTENUFSPACE: Insufficient space to return complete information
139. KRB5_BADMSGTYPE: Invalid message type specified for encoding
140. KRB5_CC_BADNAME: Credential cache name malformed
141. KRB5_CC_UNKNOWN_TYPE: Unknown credential cache type
142. KRB5_CC_NOTFOUND: Matching credential not found
143. KRB5_CC_END: End of credential cache reached
144. KRB5_NO_TKT_SUPPLIED: Request did not supply a ticket
145. KRB5KRB_AP_WRONG_PRINC: Wrong principal in request
146. KRB5KRB_AP_ERR_TKT_INVALID: Ticket has invalid flag set
147. KRB5_PRINC_NOMATCH: Requested principal and ticket don't match
148. KRB5_KDCREP_MODIFIED: KDC reply did not match expectations
149. KRB5_KDCREP_SKEW: Clock skew too great in KDC reply
150. KRB5_IN_TKT_REALM_MISMATCH: Client/server realm mismatch in initial ticket request
151. KRB5_PROG_ETYPE_NOSUPP: Program lacks support for encryption type
152. KRB5_PROG_KEYTYPE_NOSUPP: Program lacks support for key type
153. KRB5_WRONG_ETYPE: Requested encryption type not used in message
154. KRB5_PROG_SUMTYPE_NOSUPP: Program lacks support for checksum type
155. KRB5_REALM_UNKNOWN: Cannot find KDC for requested realm
156. KRB5_SERVICE_UNKNOWN: Kerberos service unknown
157. KRB5_KDC_UNREACH: Cannot contact any KDC for requested realm
158. KRB5_NO_LOCALNAME: No local name found for principal name

159. KRB5_MUTUAL_FAILED: Mutual authentication failed
160. KRB5_RC_TYPE_EXISTS: Replay cache type is already registered
161. KRB5_RC_MALLOC: No more memory to allocate (in replay cache code)
162. KRB5_RC_TYPE_NOTFOUND: Replay cache type is unknown
163. KRB5_RC_UNKNOWN: Generic unknown RC error
164. KRB5_RC_REPLAY: Message is a replay
165. KRB5_RC_IO: Replay I/O operation failed XXX
166. KRB5_RC_NOIO: Replay cache type does not support non-volatile storage
167. KRB5_RC_PARSE: Replay cache name parse/format error
168. KRB5_RC_IO_EOF: End-of-file on replay cache I/O
169. KRB5_RC_IO_MALLOC: No more memory to allocate (in replay cache I/O code)
170. KRB5_RC_IO_PERM: Permission denied in replay cache code
171. KRB5_RC_IO_IO: I/O error in replay cache i/o code
172. KRB5_RC_IO_UNKNOWN: Generic unknown RC/IO error
173. KRB5_RC_IO_SPACE: Insufficient system space to store replay information
174. KRB5_TRANS_CANTOPEN: Can't open/find realm translation file
175. KRB5_TRANS_BADFORMAT: Improper format of realm translation file
176. KRB5_LNAME_CANTOPEN: Can't open/find lname translation database
177. KRB5_LNAME_NOTRANS: No translation available for requested principal
178. KRB5_LNAME_BADFORMAT: Improper format of translation database entry
179. KRB5_CRYPTO_INTERNAL: Cryptosystem internal error
180. KRB5_KT_BADNAME: Key table name malformed
181. KRB5_KT_UNKNOWN_TYPE: Unknown Key table type
182. KRB5_KT_NOTFOUND: Key table entry not found
183. KRB5_KT_END: End of key table reached
184. KRB5_KT_NOWRITE: Cannot write to specified key table
185. KRB5_KT_IOERR: Error writing to key table
186. KRB5_NO_TKT_IN_RLM: Cannot find ticket for requested realm
187. KRB5DES_BAD_KEYPAR: DES key has bad parity
188. KRB5DES_WEAK_KEY: DES key is a weak key
189. KRB5_BAD_ENCTYPE: Bad encryption type
190. KRB5_BAD_KEYSIZE: Key size is incompatible with encryption type
191. KRB5_BAD_MSIZE: Message size is incompatible with encryption type
192. KRB5_CC_TYPE_EXISTS: Credentials cache type is already registered.
193. KRB5_KT_TYPE_EXISTS: Key table type is already registered.
194. KRB5_CC_IO: Credentials cache I/O operation failed XXX
195. KRB5_FCC_PERM: Credentials cache file permissions incorrect
196. KRB5_FCC_NOFILE: No credentials cache found
197. KRB5_FCC_INTERNAL: Internal credentials cache error
198. KRB5_CC_WRITE: Error writing to credentials cache
199. KRB5_CC_NOMEM: No more memory to allocate (in credentials cache code)
200. KRB5_CC_FORMAT: Bad format in credentials cache
201. KRB5_INVALID_FLAGS: Invalid KDC option combination (library internal error) [for dual tgt library calls]
202. KRB5_NO_2ND_TKT: Request missing second ticket [for dual tgt library calls]
203. KRB5_NOCREDS_SUPPLIED: No credentials supplied to library routine
204. KRB5_SENDAUTH_BADAUTHVERS: Bad sendauth version was sent
205. KRB5_SENDAUTH_BADAPPLVERS: Bad application version was sent (via sendauth)
206. KRB5_SENDAUTH_BADRESPONSE: Bad response (during sendauth exchange)
207. KRB5_SENDAUTH_REJECTED: Server rejected authentication (during sendauth exchange)

208. KRB5_PREAUTH_BAD_TYPE: Unsupported preauthentication type
209. KRB5_PREAUTH_NO_KEY: Required preauthentication key not supplied
210. KRB5_PREAUTH_FAILED: Generic preauthentication failure
211. KRB5_RCACHE_BADVNO: Unsupported replay cache format version number
212. KRB5_CCACHE_BADVNO: Unsupported credentials cache format version number
213. KRB5_KEYTAB_BADVNO: Unsupported key table format version number
214. KRB5_PROG_ATYPE_NOSUPP: Program lacks support for address type
215. KRB5_RC_REQUIRED: Message replay detection requires rcache parameter
216. KRB5_ERR_BAD_HOSTNAME: Hostname cannot be canonicalized
217. KRB5_ERR_HOST_REALM_UNKNOWN: Cannot determine realm for host
218. KRB5_SNAME_UNSUPP_NAMETYPE: Conversion to service principal undefined for name type
219. KRB5KRB_AP_ERR_V4_REPLY: Initial Ticket response appears to be Version 4 error
220. KRB5_REALM_CANT_RESOLVE: Cannot resolve KDC for requested realm
221. KRB5_TKT_NOT_FORWARDABLE: Requesting ticket can't get forwardable tickets
222. KRB5_FWD_BAD_PRINCIPAL: Bad principal name while trying to forward credentials
223. KRB5_GET_IN_TKT_LOOP: Looping detected inside krb5_get_in_tkt
224. KRB5_CONFIG_NODEFREALM: Configuration file does not specify default realm
225. KRB5_SAM_UNSUPPORTED: Bad SAM flags in obtain_sam_padata
226. KRB5_KT_NAME_TOOLONG: Keytab name too long
227. KRB5_KT_KVNONOTFOUND: Key version number for principal in key table is incorrect
228. KRB5_APPL_EXPIRED: This application has expired
229. KRB5_LIB_EXPIRED: This Krb5 library has expired
230. KRB5_CHPW_PWDNULL: New password cannot be zero length
231. KRB5_CHPW_FAIL: Password change failed
232. KRB5_KT_FORMAT: Bad format in keytab
233. KRB5_NOPERM_ETYPE: Encryption type not permitted
234. KRB5_CONFIG_ETYPE_NOSUPP: No supported encryption types (config file error?)
235. KRB5_OBSOLETE_FN: Program called an obsolete, deleted function
236. KRB5_EAI_FAIL: unknown getaddrinfo failure
237. KRB5_EAI_NODATA: no data available for host/domain name
238. KRB5_EAI_NONAME: host/domain name not found
239. KRB5_EAI_SERVICE: service name unknown
240. KRB5_ERR_NUMERIC_REALM: Cannot determine realm for numeric host address

4 A.1.2 Kerberos V5 Database Library Error Codes

This is the Kerberos v5 database library error code table.

1. KRB5_KDB_RCSID: (RCS Id string for the kdb error table)
2. KRB5_KDB_INUSE: Entry already exists in database
3. KRB5_KDB_UK_SERROR: Database store error

4. KRB5_KDB_UK_RERROR: Database read error
5. KRB5_KDB_UNAUTH: Insufficient access to perform requested operation
6. KRB5_KDB_NOENTRY: No such entry in the database
7. KRB5_KDB_ILL_WILDCARD: Illegal use of wildcard
8. KRB5_KDB_DB_INUSE: Database is locked or in use–try again later
9. KRB5_KDB_DB_CHANGED: Database was modified during read
10. KRB5_KDB_TRUNCATED_RECORD: Database record is incomplete or corrupted
11. KRB5_KDB_RECURSIVELOCK: Attempt to lock database twice
12. KRB5_KDB_NOTLOCKED: Attempt to unlock database when not locked
13. KRB5_KDB_BADLOCKMODE: Invalid kdb lock mode
14. KRB5_KDB_DBNOTINITED: Database has not been initialized
15. KRB5_KDB_DBINITED: Database has already been initialized
16. KRB5_KDB_ILLDIRECTION: Bad direction for converting keys
17. KRB5_KDB_NOMASTERKEY: Cannot find master key record in database
18. KRB5_KDB_BADMASTERKEY: Master key does not match database
19. KRB5_KDB_INVALIDKEYSIZE: Key size in database is invalid
20. KRB5_KDB_CANTREAD_STORED: Cannot find/read stored master key
21. KRB5_KDB_BADSTORED_MKEY: Stored master key is corrupted
22. KRB5_KDB_CANTLOCK_DB: Insufficient access to lock database
23. KRB5_KDB_DB_CORRUPT: Database format error
24. KRB5_KDB_BAD_VERSION: Unsupported version in database entry
25. KRB5_KDB_BAD_SALTTYPE: Unsupported salt type
26. KRB5_KDB_BAD_ENCTYPE: Unsupported encryption type
27. KRB5_KDB_BAD_CREATEFLAGS: Bad database creation flags
28. KRB5_KDB_NO_PERMITTED_KEY: No matching key in entry having a permitted enc type
29. KRB5_KDB_NO_MATCHING_KEY: No matching key in entry

5 A.1.3 Kerberos V5 Magic Numbers Error Codes

This is the Kerberos v5 magic numbers error code table.

1. KV5M_NONE: Kerberos V5 magic number table
2. KV5M_PRINCIPAL: Bad magic number for krb5_principal structure
3. KV5M_DATA: Bad magic number for krb5_data structure
4. KV5M_KEYBLOCK: Bad magic number for krb5_keyblock structure
5. KV5M_CHECKSUM: Bad magic number for krb5_checksum structure
6. KV5M_ENCRYPT_BLOCK: Bad magic number for krb5_encrypt_block structure
7. KV5M_ENC_DATA: Bad magic number for krb5_enc_data structure
8. KV5M_CRYPTOSYSTEM_ENTRY: Bad magic number for krb5_cryptosystem_entry structure
9. KV5M_CS_TABLE_ENTRY: Bad magic number for krb5_cs_table_entry structure
10. KV5M_CHECKSUM_ENTRY: Bad magic number for krb5_checksum_entry structure
11. KV5M_AUTHDATA: Bad magic number for krb5_authdata structure
12. KV5M_TRANSITED: Bad magic number for krb5_transited structure
13. KV5M_ENC_TKT_PART: Bad magic number for krb5_enc_tkt_part structure
14. KV5M_TICKET: Bad magic number for krb5_ticket structure
15. KV5M_AUTHENTICATOR: Bad magic number for krb5_authenticator structure
16. KV5M_TKT_AUTHENT: Bad magic number for krb5_tkt_authent structure
17. KV5M_CREDS: Bad magic number for krb5_creds structure

18. KV5M_LAST_REQ_ENTRY: Bad magic number for krb5_last_req_entry structure
19. KV5M_PA_DATA: Bad magic number for krb5_pa_data structure
20. KV5M_KDC_REQ: Bad magic number for krb5_kdc_req structure
21. KV5M_ENC_KDC_REP_PART: Bad magic number for krb5_enc_kdc_rep_part structure
22. KV5M_KDC_REP: Bad magic number for krb5_kdc_rep structure
23. KV5M_ERROR: Bad magic number for krb5_error structure
24. KV5M_AP_REQ: Bad magic number for krb5_ap_req structure
25. KV5M_AP_REP: Bad magic number for krb5_ap_rep structure
26. KV5M_AP_REP_ENC_PART: Bad magic number for krb5_ap_rep_enc_part structure
27. KV5M_RESPONSE: Bad magic number for krb5_response structure
28. KV5M_SAFE: Bad magic number for krb5_safe structure
29. KV5M_PRIV: Bad magic number for krb5_priv structure
30. KV5M_PRIV_ENC_PART: Bad magic number for krb5_priv_enc_part structure
31. KV5M_CRED: Bad magic number for krb5_cred structure
32. KV5M_CRED_INFO: Bad magic number for krb5_cred_info structure
33. KV5M_CRED_ENC_PART: Bad magic number for krb5_cred_enc_part structure
34. KV5M_PWD_DATA: Bad magic number for krb5_pwd_data structure
35. KV5M_ADDRESS: Bad magic number for krb5_address structure
36. KV5M_KEYTAB_ENTRY: Bad magic number for krb5_keytab_entry structure
37. KV5M_CONTEXT: Bad magic number for krb5_context structure
38. KV5M_OS_CONTEXT: Bad magic number for krb5_os_context structure
39. KV5M_ALT_METHOD: Bad magic number for krb5_alt_method structure
40. KV5M_ETYPE_INFO_ENTRY: Bad magic number for krb5_etype_info_entry structure
41. KV5M_DB_CONTEXT: Bad magic number for krb5_db_context structure
42. KV5M_AUTH_CONTEXT: Bad magic number for krb5_auth_context structure
43. KV5M_KEYTAB: Bad magic number for krb5_keytab structure
44. KV5M_RCACHE: Bad magic number for krb5_rcache structure
45. KV5M_CCACHE: Bad magic number for krb5_ccache structure
46. KV5M_PREAUTH_OPS: Bad magic number for krb5_preauth_ops
47. KV5M_SAM_CHALLENGE: Bad magic number for krb5_sam_challenge
48. KV5M_SAM_KEY: Bad magic number for krb5_sam_key
49. KV5M_ENC_SAM_RESPONSE_ENC: Bad magic number for krb5_enc_sam_response_enc
50. KV5M_SAM_RESPONSE: Bad magic number for krb5_sam_response
51. KV5M_PREDICTED_SAM_RESPONSE: Bad magic number for krb5_predicted_sam_response
52. KV5M_PASSWD_PHRASE_ELEMENT: Bad magic number for passwd_phrase_element
53. KV5M_GSS_OID: Bad magic number for GSSAPI OID
54. KV5M_GSS_QUEUE: Bad magic number for GSSAPI QUEUE

6 A.1.4 ASN.1 Error Codes

1. ASN1_BAD_TIMEFORMAT: ASN.1 failed call to system time library
2. ASN1_MISSING_FIELD: ASN.1 structure is missing a required field
3. ASN1_MISPLACED_FIELD: ASN.1 unexpected field number
4. ASN1_TYPE_MISMATCH: ASN.1 type numbers are inconsistent
5. ASN1_OVERFLOW: ASN.1 value too large

6. ASN1_OVERRUN: ASN.1 encoding ended unexpectedly
7. ASN1_BAD_ID: ASN.1 identifier doesn't match expected value
8. ASN1_BAD_LENGTH: ASN.1 length doesn't match expected value
9. ASN1_BAD_FORMAT: ASN.1 badly-formatted encoding
10. ASN1_PARSE_ERROR: ASN.1 parse error
11. ASN1_BAD_GMTIME: ASN.1 bad return from gmtime
12. ASN1_MISMATCH_INDEF: ASN.1 non-constructed indefinite encoding
13. ASN1_MISSING_EOC: ASN.1 missing expected EOC

7 A.1.5 GSSAPI Error Codes

Generic GSSAPI Errors:

1. G_BAD_SERVICE_NAME: No in SERVICE-NAME name string
2. G_BAD_STRING_UID: STRING-UID-NAME contains nondigits
3. G_NOUSER: UID does not resolve to username
4. G_VALIDATE_FAILED: Validation error
5. G_BUFFER_ALLOC: Couldn't allocate gss_buffer_t data
6. G_BAD_MSG_CTX: Message context invalid
7. G_WRONG_SIZE: Buffer is the wrong size
8. G_BAD_USAGE: Credential usage type is unknown
9. G_UNKNOWN_QOP: Unknown quality of protection specified
10. G_BAD_HOSTNAME: Hostname in SERVICE-NAME string could not be canonicalized
11. G_WRONG_MECH: Mechanism is incorrect
12. G_BAD_TOK_HEADER: Token header is malformed or corrupt
13. G_BAD_DIRECTION: Packet was replayed in wrong direction
14. G_TOK_TRUNC: Token is missing data
15. G_REFLECT: Token was reflected
16. G_WRONG_TOKID: Received token ID does not match expected token ID

Kerberos 5 GSSAPI Errors:

1. KG_CCACHE_NOMATCH: Principal in credential cache does not match desired name
2. KG_KEYTAB_NOMATCH: No principal in keytab matches desired name
3. KG_TGT_MISSING: Credential cache has no TGT
4. KG_NO_SUBKEY: Authenticator has no subkey
5. KG_CONTEXT_ESTABLISHED: Context is already fully established
6. KG_BAD_SIGN_TYPE: Unknown signature type in token
7. KG_BAD_LENGTH: Invalid field length in token
8. KG_CTX_INCOMPLETE: Attempt to use incomplete security context
9. KG_CONTEXT: Bad magic number for krb5_gss_ctx_id_t
10. KG_CRED: Bad magic number for krb5_gss_cred_id_t
11. KG_ENC_DESC: Bad magic number for krb5_gss_enc_desc
12. KG_BAD_SEQ: Sequence number in token is corrupt
13. KG_EMPTY_CCACHE: Credential cache is empty
14. KG_NO_CTYPES: Acceptor and Initiator share no checksum types