Table 15.1 Summary of Kerberos Version 4 Message Exchanges

(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C $\mathrm{E}(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$$Ticket_{tgs} = \mathrm{E}(\mathrm{K}_{tgs}, [\mathrm{K}_{c,tgs} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_{tgs} \| \mathrm{TS}_2 \| \mathrm{Lifetime}_2])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $\mathrm{E}(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$$Ticket_{tgs} = \mathrm{E}(\mathrm{K}_{tgs}, [\mathrm{K}_{c,tgs} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_{tgs} \| \mathrm{TS}_2 \| \mathrm{Lifetime}_2])$$

$$Ticket_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{K}_{c,v} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_v \| \mathrm{TS}_4 \| \mathrm{Lifetime}_4])$$

$$Authenticator_c = \mathrm{E}(\mathrm{K}_{\mathrm{c},tgs}, [\mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{TS}_3])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Ticket_v \| Authenticator_c$

(6) V → C $\mathrm{E}(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$$Ticket_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{K}_{c,v} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_v \| \mathrm{TS}_4 \| \mathrm{Lifetime}_4])$$

$$Authenticator_c = \mathrm{E}(\mathrm{K}_{\mathrm{c},v}, [\mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{TS}_5])$$

(c) Client/Server Authentication Exchange to obtain service

Table 15.2 Rationale for the Elements of the Kerberos Version 4 Protocol
(page 1 of 3)

Message (1)	Client requests ticket-granting ticket.
ID_C	Tells AS identity of user from this client.
ID_{tgs}	Tells AS that user requests access to TGS.
TS_1	Allows AS to verify that client's clock is synchronized with that of AS.
Message (2)	AS returns ticket-granting ticket.
K_c	Encryption is based on user's password, enabling AS and client to verify password, and protecting contents of message (2).
$K_{c,tgs}$	Copy of session key accessible to client created by AS to permit secure exchange between client and TGS without requiring them to share a permanent key.
ID_{tgs}	Confirms that this ticket is for the TGS.
TS_2	Informs client of time this ticket was issued.
$Lifetime_2$	Informs client of the lifetime of this ticket.
$Ticket_{tgs}$	Ticket to be used by client to access TGS.

(a) Authentication Service Exchange

Table 15.2 Rationale for the Elements of the Kerberos Version 4 Protocol
(page 2 of 3)

Message (3)	Client requests service-granting ticket.
ID_V	Tells TGS that user requests access to server V.
$Ticket_{tgs}$	Assures TGS that this user has been authenticated by AS.
$Authenticator_c$	Generated by client to validate ticket .
Message (4)	TGS returns service-granting ticket.
$K_{c,tgs}$	Key shared only by C and TGS protects contents of message (4).
$K_{c,v}$	Copy of session key accessible to client created by TGS to permit secure exchange between client and server without requiring them to share a permanent key.
ID_V	Confirms that this ticket is for server V.
TS_4	Informs client of time this ticket was issued.
$Ticket_V$	Ticket to be used by client to access server V.
$Ticket_{tgs}$	Reusable so that user does not have to reenter password.
K_{tgs}	Ticket is encrypted with key known only to AS and TGS, to prevent Tampering.
$K_{c,tgs}$	Copy of session key accessible to TGS used to decrypt authenticator, thereby authenticating ticket.
ID_C	Indicates the rightful owner of this ticket.
AD_C	Prevents use of ticket from workstation other than one that initially requested the ticket.
ID_{tgs}	Assures server that it has decrypted ticket properly.
TS_2	Informs TGS of time this ticket was issued.
$Lifetime_2$	Prevents replay after ticket has expired.
$Authenticator_c$	Assures TGS that the ticket presenter is the same as the client for whom the ticket was issued has very short lifetime to prevent replay.
$K_{c,tgs}$	Authenticator is encrypted with key known only to client and TGS, to prevent tampering.
ID_C	Must match ID in ticket to authenticate ticket.
AD_C	Must match address in ticket to authenticate ticket.
TS_3	Informs TGS of time this authenticator was generated.

(b) Ticket-Granting Service Exchange

Table 15.2 Rationale for the Elements of the Kerberos Version 4 Protocol

(page 3 of 3)

Message (5)	Client requests service.
$Ticket_V$	Assures server that this user has been authenticated by AS.
$Authenticator_c$	Generated by client to validate ticket.
Message (6)	Optional authentication of server to client.
$K_{c,v}$	Assures C that this message is from V.
$TS_5 + 1$	Assures C that this is not a replay of an old reply.
$Ticket_v$	Reusable so that client does not need to request a new ticket from TGS for each access to the same server.
K_v	Ticket is encrypted with key known only to TGS and server, to prevent Tampering.
$K_{c,v}$	Copy of session key accessible to client; used to decrypt authenticator, thereby authenticating ticket.
ID_C	Indicates the rightful owner of this ticket.
AD_C	Prevents use of ticket from workstation other than one that initially requested the ticket.
ID_V	Assures server that it has decrypted ticket properly.
TS_4	Informs server of time this ticket was issued.
$Lifetime_4$	Prevents replay after ticket has expired.
$Authenticator_c$	Assures server that the ticket presenter is the same as the client for whom the ticket was issued; has very short lifetime to prevent replay.
$K_{c,v}$	Authenticator is encrypted with key known only to client and server, to prevent tampering.
ID_C	Must match ID in ticket to authenticate ticket.
AD_c	Must match address in ticket to authenticate ticket.
TS_5	Informs server of time this authenticator was generated.

(c) Client/Server Authentication Exchange

Table 15.3 Summary of Kerberos Version 5 Message Exchanges

(1) C → AS $\mathit{Options} \parallel \mathit{ID}_c \parallel \mathit{Realm}_c \parallel \mathit{ID}_{tgs} \parallel \mathit{Times} \parallel \mathit{Nonce}_1$

(2) AS → C $\mathit{Realm}_c \parallel \mathit{ID}_C \parallel \mathit{Ticket}_{tgs} \parallel \mathrm{E}(K_c, [K_{c,tgs} \parallel \mathit{Times} \parallel \mathit{Nonce}_1 \parallel \mathit{Realm}_{tgs} \parallel \mathit{ID}_{tgs}])$

$$\mathit{Ticket}_{tgs} = \mathrm{E}(K_{tgs}, [\mathit{Flags} \parallel K_{c,tgs} \parallel \mathit{Realm}_c \parallel \mathit{ID}_C \parallel \mathit{AD}_C \parallel \mathit{Times}])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $\mathit{Options} \parallel \mathit{ID}_v \parallel \mathit{Times} \parallel \parallel \mathit{Nonce}_2 \parallel \mathit{Ticket}_{tgs} \parallel \mathit{Authenticator}_c$

(4) TGS → C $\mathit{Realm}_c \parallel \mathit{ID}_C \parallel \mathit{Ticket}_v \parallel \mathrm{E}(K_{c,tgs}, [K_{c,v} \parallel \mathit{Times} \parallel \mathit{Nonce}_2 \parallel \mathit{Realm}_v \parallel \mathit{ID}_v])$

$$\mathit{Ticket}_{tgs} = \mathrm{E}(K_{tgs}, [\mathit{Flags} \parallel K_{c,tgs} \parallel \mathit{Realm}_c \parallel \mathit{ID}_C \parallel \mathit{AD}_C \parallel \mathit{Times}])$$

$$\mathit{Ticket}_v = \mathrm{E}(K_v, [\mathit{Flags} \parallel K_{c,v} \parallel \mathit{Realm}_c \parallel \mathit{ID}_C \parallel \mathrm{AD}_C \parallel \mathit{Times}])$$

$$\mathit{Authenticator}_c = \mathrm{E}(K_{c,tgs}, [\mathit{ID}_C \parallel \mathit{Realm}_c \parallel \mathit{TS}_1])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $\mathit{Options} \parallel \mathit{Ticket}_v \parallel \mathit{Authenticator}_c$

(6) V → C $\mathrm{E}_{K_{c,v}}[\ \mathit{TS}_2 \parallel \mathit{Subkey} \parallel \mathit{Seq\#}\ ]$

$$\mathrm{Ticket}_v = \mathrm{E}(K_v, [\mathrm{Flags} \parallel K_{c,v} \parallel \mathit{Realm}_c \parallel \mathit{ID}_C \parallel \mathit{AD}_C \parallel \mathit{Times}])$$

$$\mathit{Authenticator}_c = \mathrm{E}(K_{c,v}, [\mathit{ID}_C \parallel \mathit{Realm}_c \parallel \mathit{TS}_2 \parallel \mathit{Subkey} \parallel \mathit{Seq\#}])$$

(c) Client/Server Authentication Exchange to obtain service

Table 15.4 Kerberos Version 5 Flags

INITIAL	This ticket was issued using the AS protocol and not issued based on a ticket-granting ticket.
PRE-AUTHENT	During initial authentication, the client was authenticated by the KDC before a ticket was issued.
HW-AUTHENT	The protocol employed for initial authentication required the use of hardware expected to be possessed solely by the named client.
RENEWABLE	Tells TGS that this ticket can be used to obtain a replacement ticket that expires at a later date.
MAY-POSTDATE	Tells TGS that a postdated ticket may be issued based on this ticket-granting ticket.
POSTDATED	Indicates that this ticket has been postdated; the end server can check the authtime field to see when the original authentication occurred.
INVALID	This ticket is invalid and must be validated by the KDC before use.
PROXIABLE	Tells TGS that a new service-granting ticket with a different network address may be issued based on the presented ticket.
PROXY	Indicates that this ticket is a proxy.
FORWARDABLE	Tells TGS that a new ticket-granting ticket with a different network address may be issued based on this ticket-granting ticket.
FORWARDED	Indicates that this ticket has either been forwarded or was issued based on authentication involving a forwarded ticket-granting ticket.