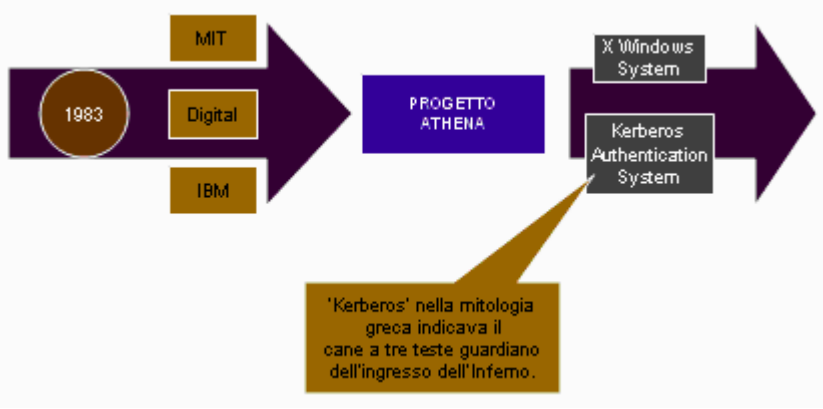
Origini

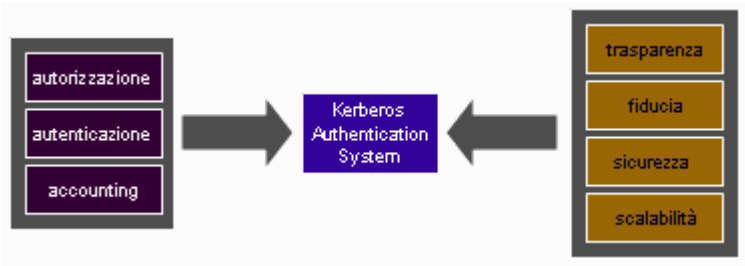
Il 27 Maggio del 1983 il MIT, supportato dalla IBM e dalla Digital, varò un progetto, chiamato Athena, della durata prevista di cinque anni, avente come scopo quello di integrare la potenza di calcolo e la capacità grafica degli elaboratori all'interno dell'esperienza educativa fornita.

Dal progetto, terminato dopo un'ennesima proroga, il 30 Giugno 1991, sono scaturite diverse importanti tecnologie fra le quali, il sistema X Windows ed il sistema di autenticazione Kerberos.



Scopi e obiettivi

Gli obiettivi che originariamente si intendevano raggiungere per il sistema Kerberos erano:



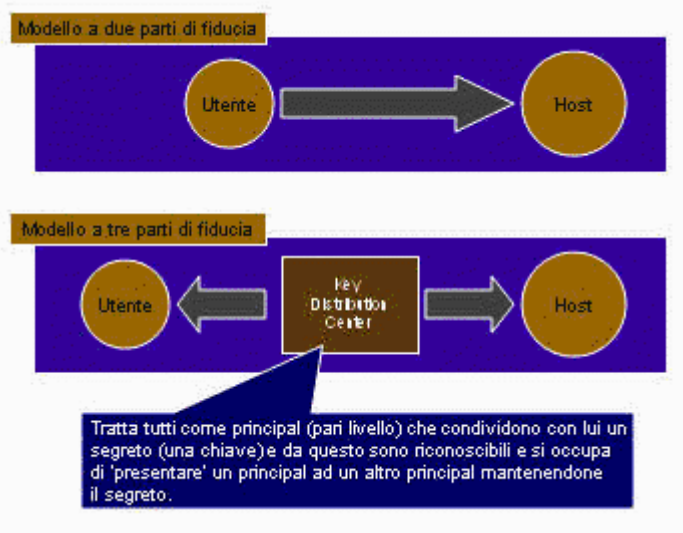
- **Autenticazione**: verificare l'identità di un client o di un servizio;
- **Autorizzazione**: autorizzare un client autenticato ad utilizzare un particolare servizio;
- **Accounting**: verificare la quantità di risorse utilizzate da un particolare client.

naturalmente fornendo all'utente un servizio con caratteristiche proprie di trasparenza, fiducia, sicurezza e scalabilità.

Sfortunatamente però degli obiettivi originali, l'unico portato veramente a termine è stato il primo e cioè quello relativo all'autenticazione.

Modelli di fiducia

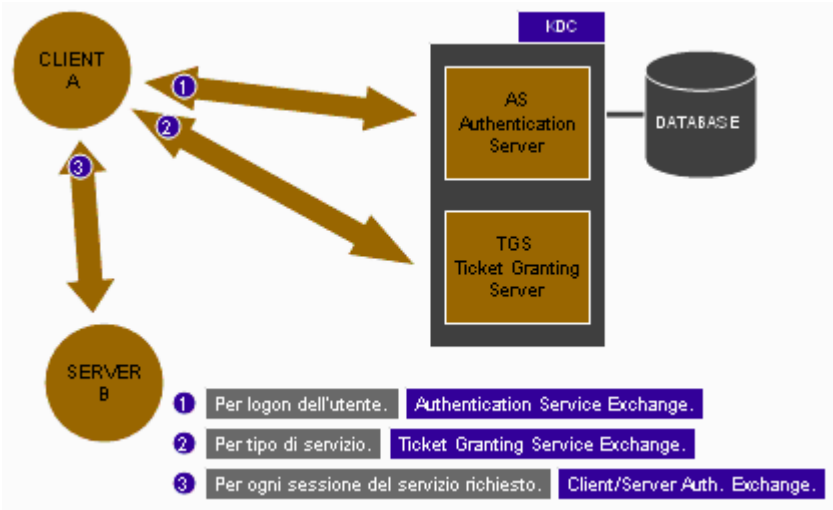
L'autenticazione nel sistema Kerberos si basa su un nuovo modello di fiducia. A differenza del modello a due parti, in cui è prevista la presenza di due elementi aventi fiducia reciproca, nel sistema Kerberos le due parti vengono a trovarsi in una relazione di fiducia verso una terza parte avente funzione di garante dell'identità dell'uno verso l'altro.



Funzionamento

Essenzialmente, il funzionamento è basato sul modello di distribuzione delle chiavi di Needham e Schroeder modificato con l'aggiunta di un marcatore orario.

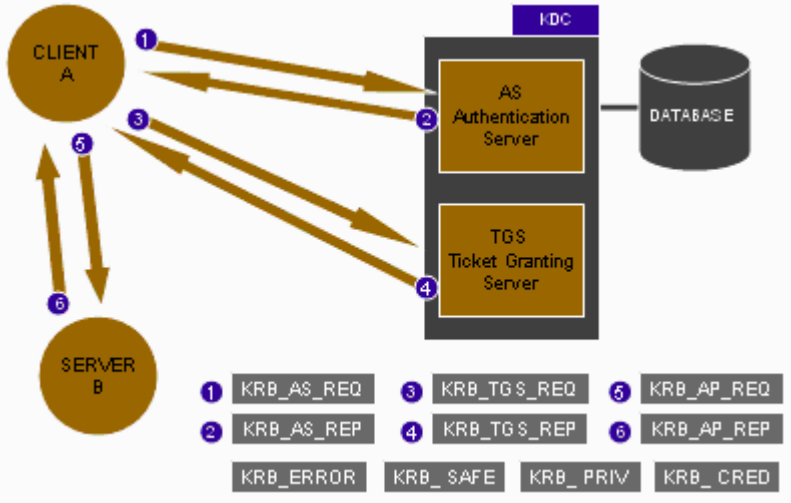
Supponiamo di avere una situazione di questo tipo:



Un client (A), vuole accedere ad un servizio presente su di un server (B) e per farlo richiederà le giuste credenziali al KDC.

La prima fase, l'Authentication Service Exchange, avviene all'atto del logon dell'utente. In seguito, richiedendo l'accesso ad un servizio, si passerà attraverso una seconda fase, il Ticket Granting Service Exchange ed infine per ogni sessione del servizio richiesto vi sarà un Client/server Authentication Exchange.

I tipi di messaggi scambiati durante le varie fasi sono i seguenti:



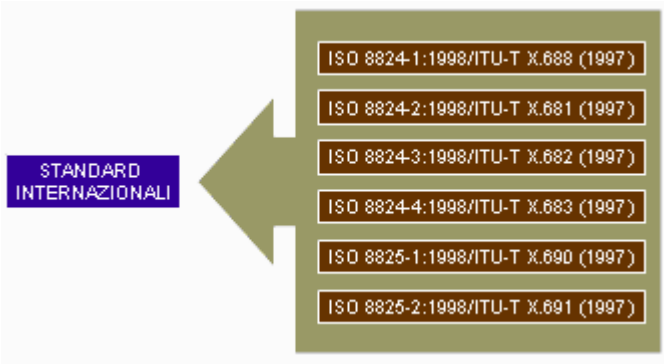
Tickets

Ma cos'è un ticket? Non è altro che un insieme di dati che permette ad un servizio di identificare un client. Ne esistono di diversi tipi, ognuno con uno scopo ben preciso:

- **Initial e Pre-authenticated**: il ticket è stato emesso utilizzando il protocollo AS e non servendosi di un ticket-granting ticket. Le opzioni PRE-AUTHENT e HW-AUTHENT possono essere utilizzate per fornire informazioni addizionali nella fase di autenticazione iniziale, sia che il ticket corrente sia stato emesso direttamente che sulla base di un ticket-granting ticket.
- **Invalid**: il ticket non è valido.
- **Renewable**: ogni ticket di questo tipo è caratterizzato da due 'tempi di scadenza'. Il tempo di scadenza associato al singolo ticket ed il massimo tempo di rinnovo possibile. I tickets rinnovabili vengono utilizzati per minimizzare i danni derivanti dal possibile furto di tickets.
- **Postdated**: ticket generato per essere utilizzato in seguito.
- **Proxiable e proxy**: vi potrebbe essere la necessità per un principal di permettere ad un servizio di effettuare delle operazioni al suo posto. Il servizio dovrà quindi essere in grado di impersonare il client, ma solo per un determinato scopo. Per fare questo, si utilizza un ticket proxy.
- **Forwardable**: è una versione particolare di ticket proxy nella quale al servizio è garantita l'impersonazione totale del client. Un esempio potrebbe essere: un utente si collega ad un sistema e vuole che l'autenticazione funzioni nel sistema come se il login fosse effettuato in locale.

ASN.1

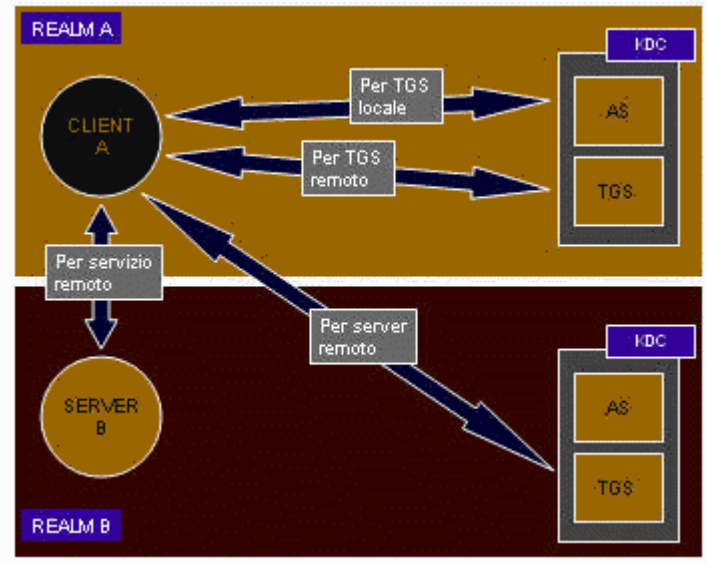
Tutti i ticket scambiati durante le varie fasi di dialogo vengono formattati utilizzando la notazione standard ASN.1.



Funzionamento tra realms diversi

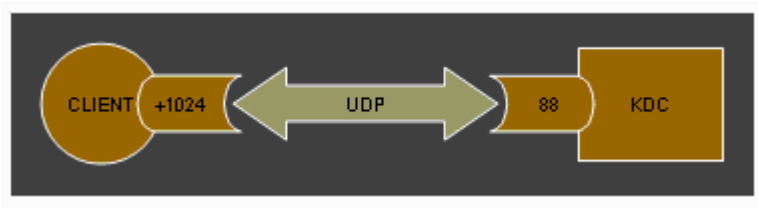
Cosa accadrebbe se un client dovesse accedere ad un servizio fornito da un server presente in un realm diverso dal proprio? Semplice, non farà altro che richiedere al suo TGS un ticket da presentare al TGS remoto per ottenere un nuovo ticket da utilizzare con il relativo server remoto.

Naturamente perchè il tutto funzioni occorrerà che, in precedenza, sia stata instaurata una relazione di fiducia fra i due realms.



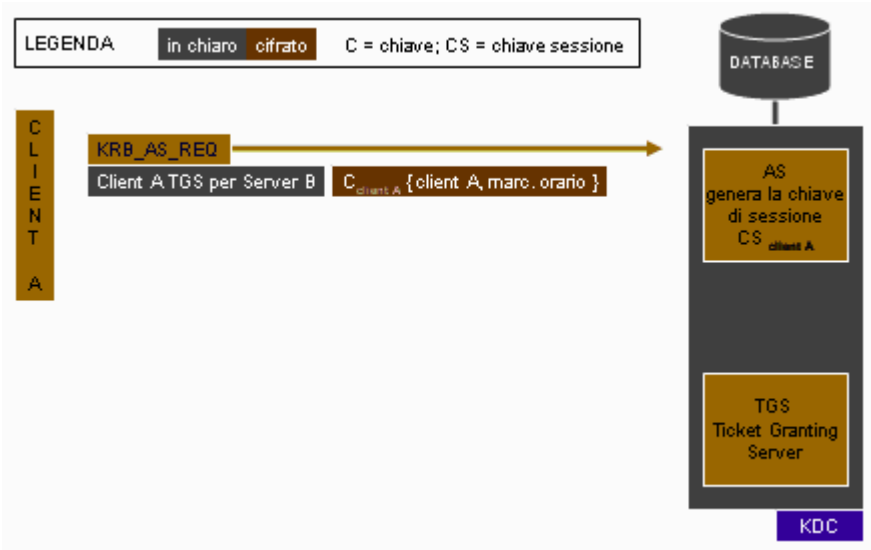
Trasporto

Il sistema Kerberos, su reti TCP/IP, utilizza come trasporto il protocollo non connesso UDP e come porta per il servizio, la porta 88.

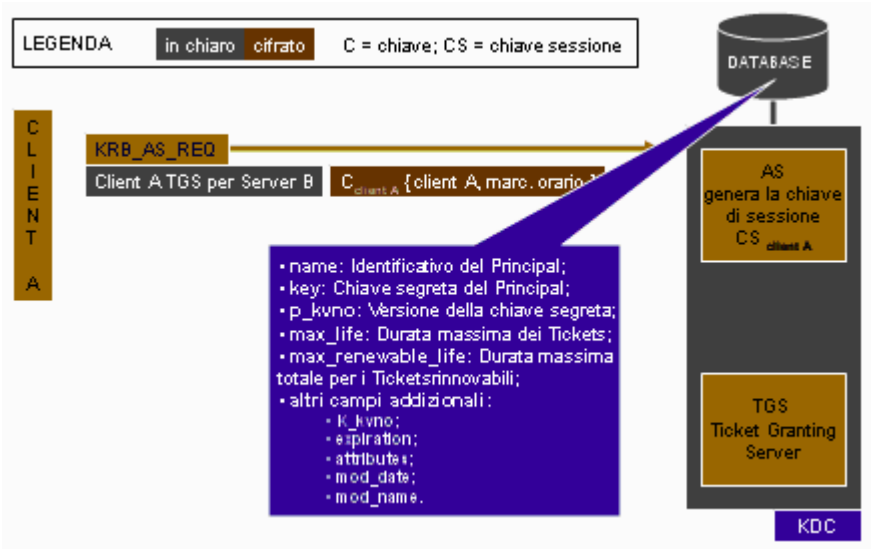


Authentication Service Exchange

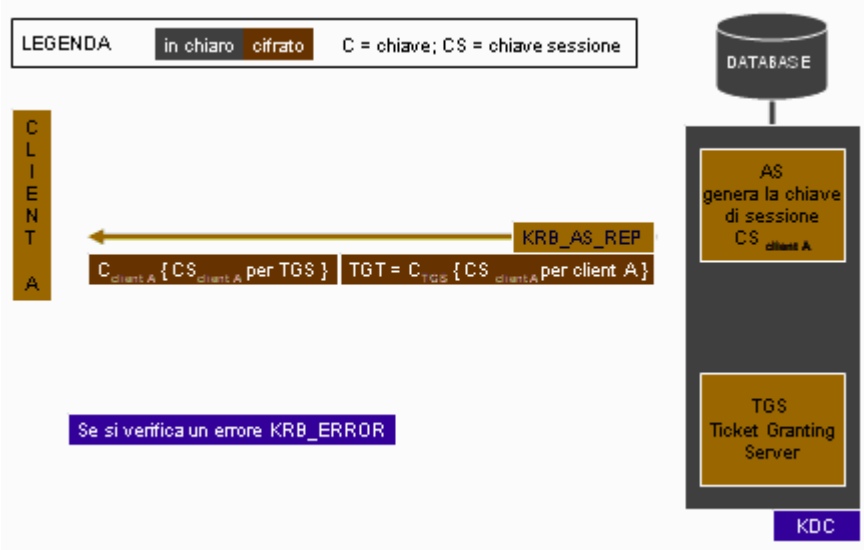
Questa fase rappresenta il primo passo verso l'accesso a qualsiasi servizio e di norma viene effettuata al primo logon dell'utente.



Il sistema client invia un messaggio composto da due componenti, una in chiaro e l'altra cifrata. Nella prima è contenuta una richiesta per ottenere il TGS che permetta l'accesso al Server B, nella seconda i dati necessari al AS, e quindi al KDC, per verificare l'identità del client: nome del sistema client e marcatore orario, il tutto cifrato con la chiave segreta del client.



A questo punto, l'AS utilizzando la chiave segreta del client, contenuta insieme ad altri dati nell'archivio del KDC, decifrerà la componente cifrata, ed in questo modo sarà sicuro che la richiesta sia stata effettuata realmente dal client. Il marcatore orario è fondamentale perchè farà si che la richiesta non possa essere ripresentata nuovamente.

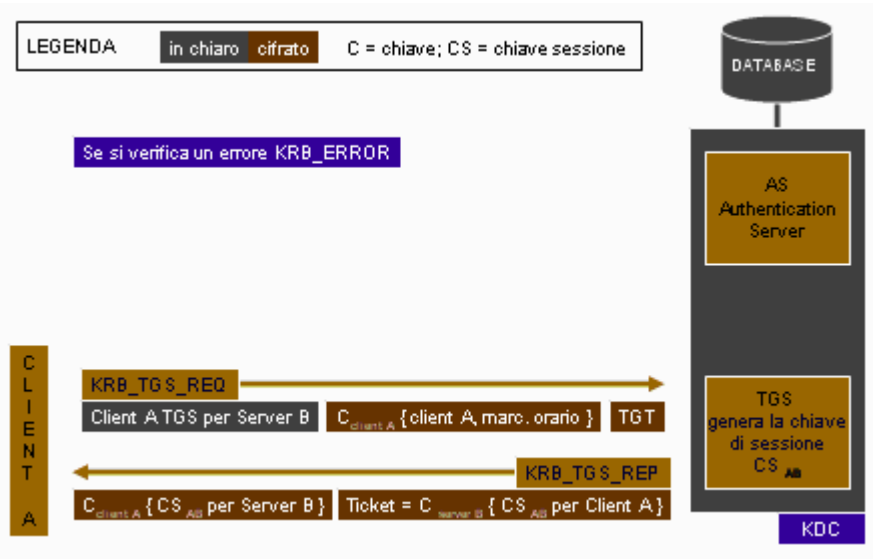


Una volta verificata l'identità del client, l'AS invierà un messaggio di risposta composto, anche in questo caso, da due componenti. La prima, cifrata con la chiave segreta del client, conterrà la chiave di sessione (CS) necessaria al client per comunicare con il TGS mentre la seconda, a parità del contenuto, sarà cifrata con la chiave segreta del TGS e quindi accessibile solo a quest'ultimo.

Se nella procedura si verifica un qualsiasi errore, il messaggio di risposta sarà del tipo KRB_ERROR.

Ticket Granting Service Exchange

In questa fase, il client, invierà al TGS un messaggio composto da tre parti distinte. Una in chiaro contenente la richiesta di un TGS per il server B, una cifrata con la chiave segreta del client, contenente il nome del client ed un marcatore orario, e l'ultima costituita dal TGT ottenuto dall'AS nella fase AS_Exchange.



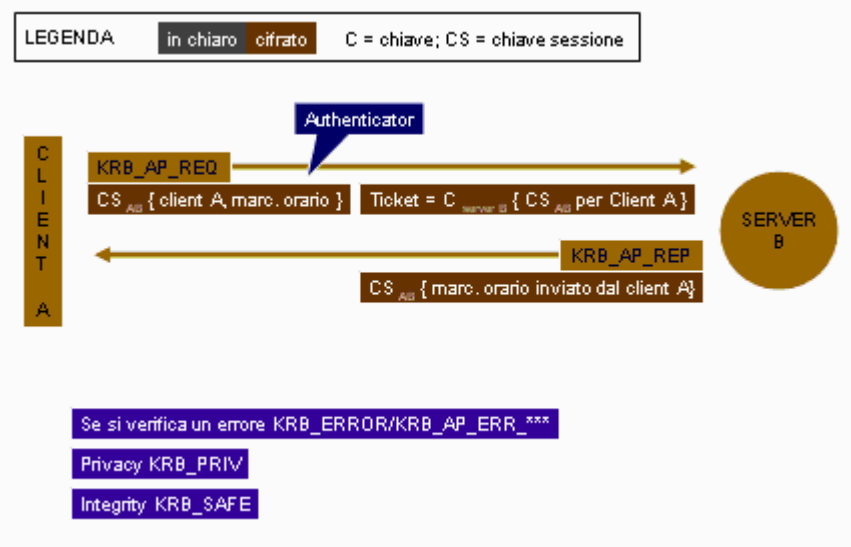
Il TGS risponderà con un messaggio composto da due parti, una cifrata con la chiave segreta del client e quindi accessibile solo a quest'ultimo, contenente la chiave di sessione (CS) da utilizzare con il Server B ed un ticket cifrato con la chiave segreta del Server B ma contenente la stessa chiave di sessione (CS) passata al Client A.

Anche in questo caso, se nella procedura si verifica un errore, il messaggio inviato sarà del tipo KRB_ERROR.

Client/Server Authentication Exchange

Nell'ultima fase, il client si presenta al server, sfruttando i dati ottenuti dal TGS, con un messaggio composto da due parti completamente cifrate.

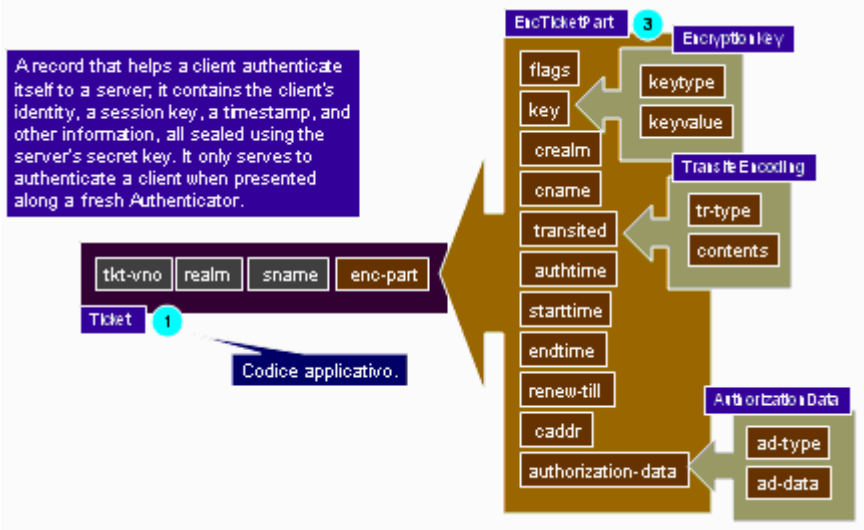
La prima parte, cifrata con la chiave di sessione ottenuta dal TGS, è chiamata anche Authenticator, e contiene, fra l'altro, il nome del client ed un marcatore orario. La seconda è costituita dal ticket, ottenuto sempre dal TGS, contenente la stessa chiave di sessione vista in precedenza, ma cifrato con la chiave segreta del server.



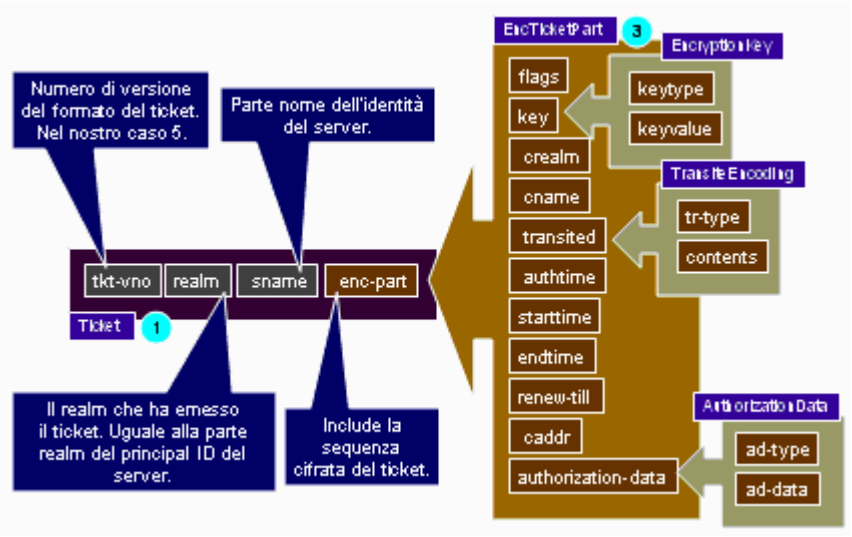
Il server risponderà con un messaggio, cifrato utilizzando la chiave di sessione estratta dal messaggio ricevuto dal client, contenente il marcatore orario ricevuto nel precedente messaggio dal client.

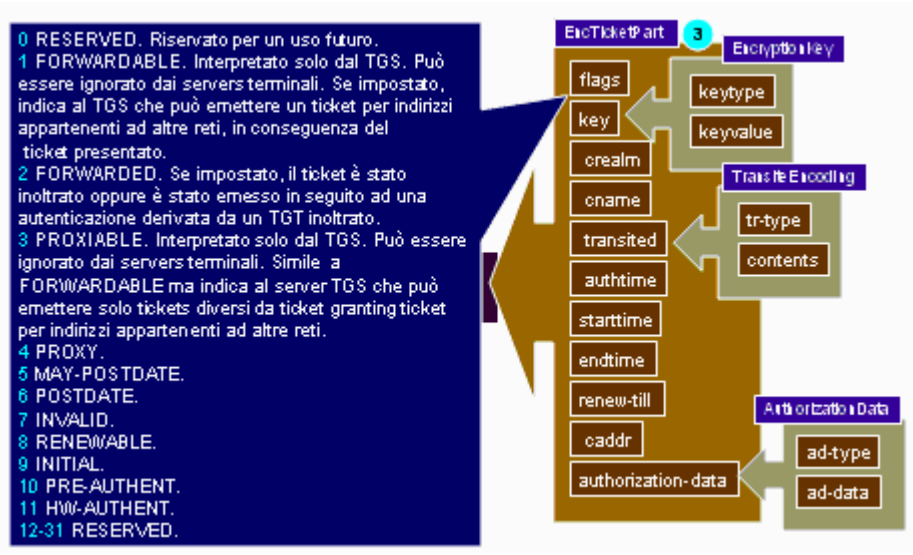
Ticket

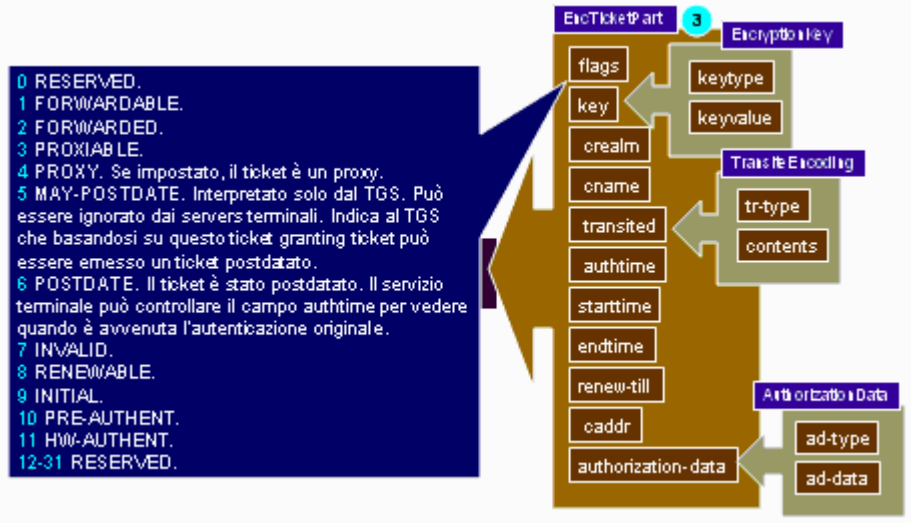
Che cos'è un ticket? Vediamolo partendo dalla definizione data all'interno dell'RFC relativa al Kerberos:

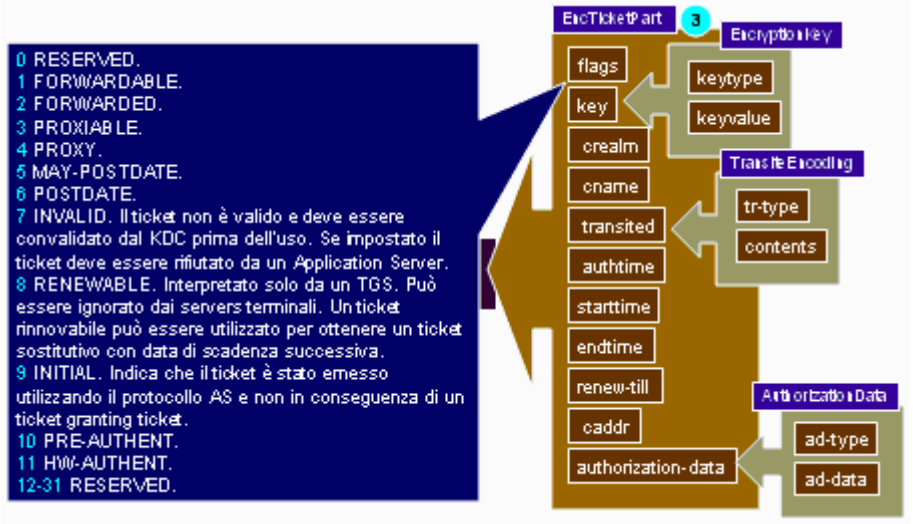


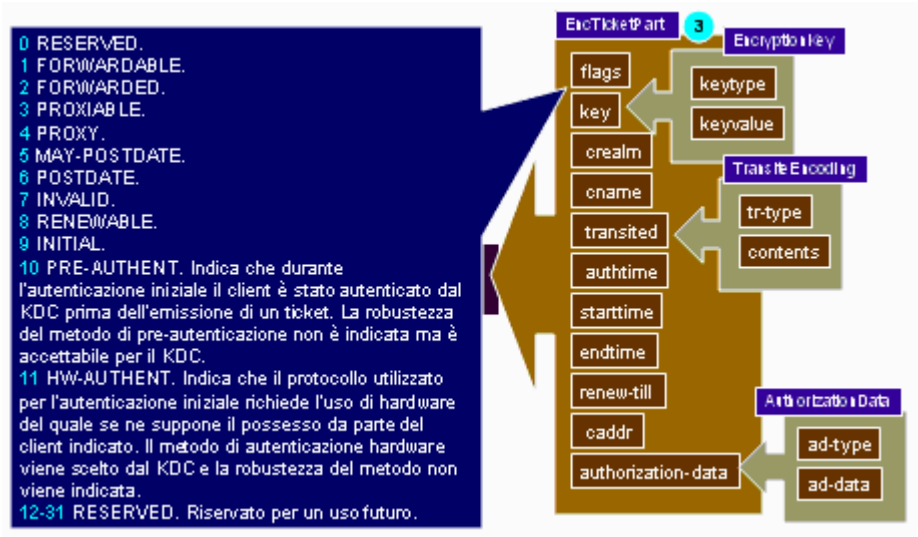
E proseguendo con l'analisi dei singoli elementi:

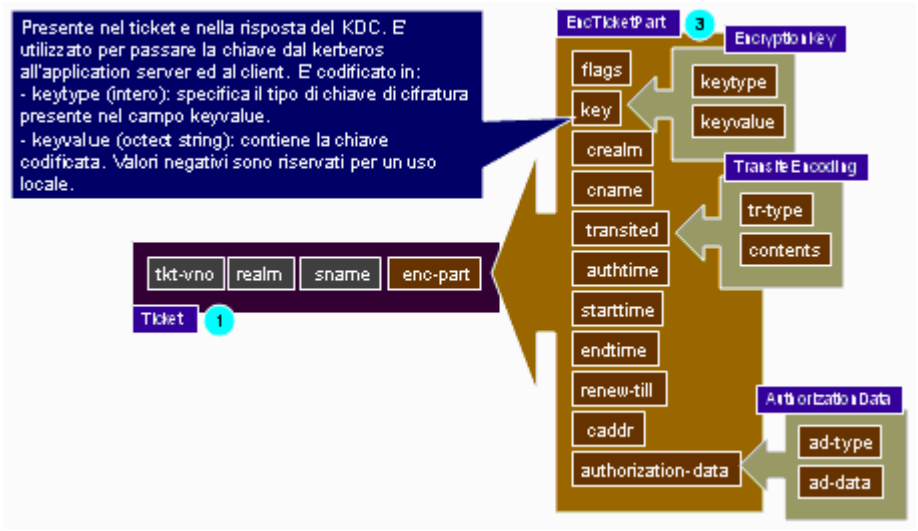


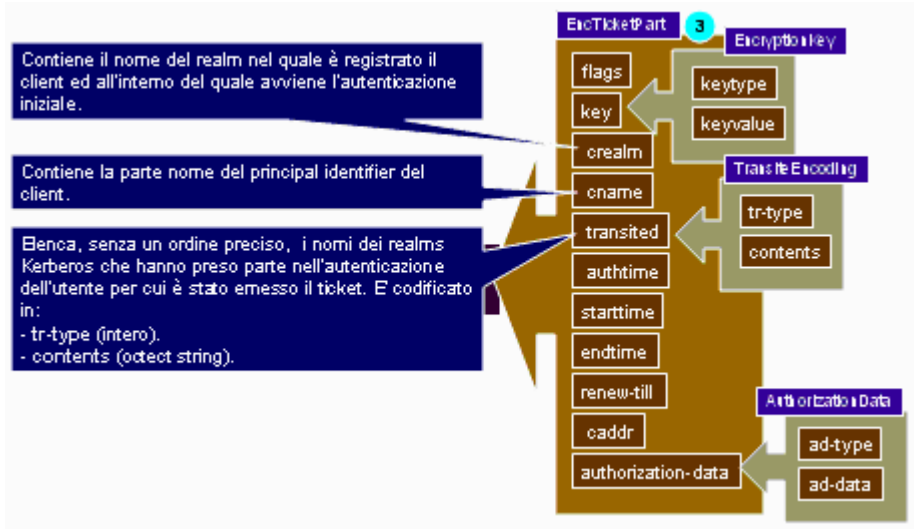

0 RESERVED. Riservato per un uso futuro.
1 FORWARDABLE. Interpretato solo dal TGS. Può essere ignorato dai servers terminali. Se impostato, indica al TGS che può emettere un ticket per indirizzi appartenenti ad altre reti, in conseguenza del ticket presentato.
2 FORWARDED. Se impostato, il ticket è stato inoltrato oppure è stato emesso in seguito ad una autenticazione derivata da un TGT inoltrato.
3 PROXIABLE. Interpretato solo dal TGS. Può essere ignorato dai servers terminali. Simile a FORWARDABLE ma indica al server TGS che può emettere solo tickets diversi da ticket granting ticket per indirizzi appartenenti ad altre reti.
4 PROXY.
5 MAY-POSTDATE.
6 POSTDATE.
7 INVALID.
8 RENEWABLE.
9 INITIAL.
10 PRE-AUTHENT.
11 HW-AUTHENT.
12-31 RESERVED.
EncTicketPart
3
EncryptionKey
flags
key
keytype
keyvalue
crealm
cname
TransitedEncoding
transited
tr-type
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data

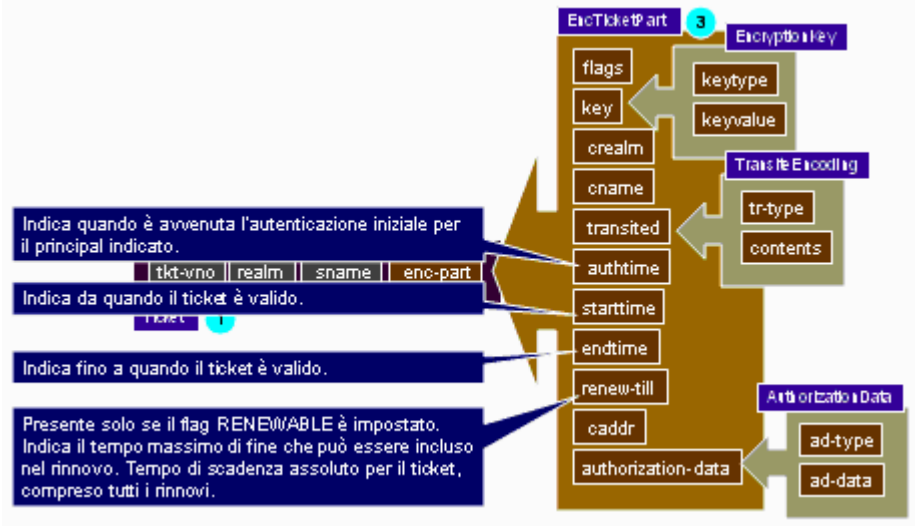

0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE.
4 PROXY. Se impostato, il ticket è un proxy.
5 MAY-POSTDATE. Interpretato solo dal TGS. Può essere ignorato dai servers terminali. Indica al TGS che basandosi su questo ticket granting ticket può essere emesso un ticket postdatato.
6 POSTDATE. Il ticket è stato postdatato. Il servizio terminale può controllare il campo authtime per vedere quando è avvenuta l'autenticazione originale.
7 INVALID.
8 RENEWABLE.
9 INITIAL.
10 PRE-AUTHENT.
11 HW-AUTHENT.
12-31 RESERVED.
EncTicketPart
3
EncryptionKey
flags
key
keytype
keyvalue
crealm
cname
TransitedEncoding
transited
tr-type
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data

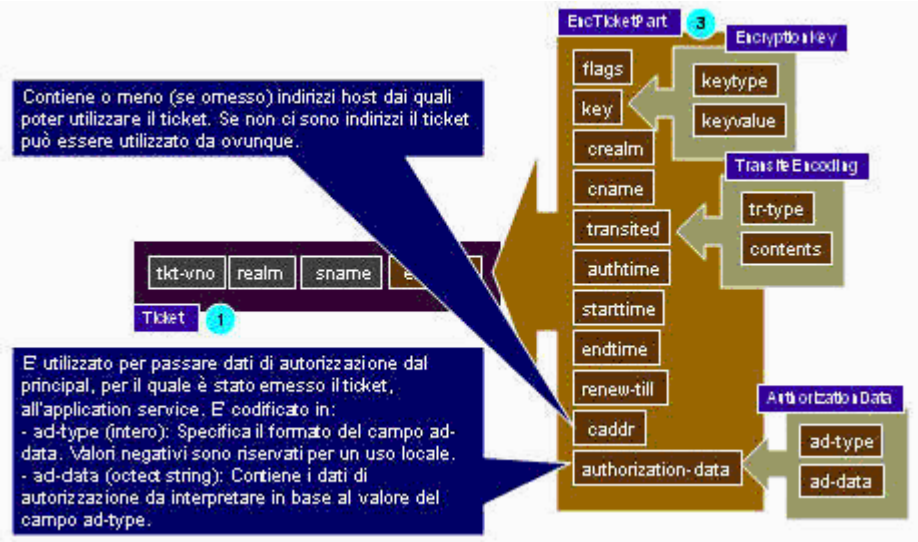

0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE.
4 PROXY.
5 MAY-POSTDATE.
6 POSTDATE.
7 INVALID. Il ticket non è valido e deve essere convalidato dal KDC prima dell'uso. Se impostato il ticket deve essere rifiutato da un Application Server.
8 RENEWABLE. Interpretato solo da un TGS. Può essere ignorato dai servers terminali. Un ticket rinnovabile può essere utilizzato per ottenere un ticket sostitutivo con data di scadenza successiva.
9 INITIAL. Indica che il ticket è stato emesso utilizzando il protocollo AS e non in conseguenza di un ticket granting ticket.
10 PRE-AUTHENT.
11 HW-AUTHENT.
12-31 RESERVED.
EncTicketPart
3
EncryptionKey
flags
key
keytype
keyvalue
crealm
cname
TransitedEncoding
transited
tr-type
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data


0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE.
4 PROXY.
5 MAY-POSTDATE.
6 POSTDATE.
7 INVALID.
8 RENEWABLE.
9 INITIAL.
10 PRE-AUTHENT. Indica che durante l'autenticazione iniziale il client è stato autenticato dal KDC prima dell'emissione di un ticket. La robustezza del metodo di pre-autenticazione non è indicata ma è accettabile per il KDC.
11 HW-AUTHENT. Indica che il protocollo utilizzato per l'autenticazione iniziale richiede l'uso di hardware del quale se ne suppone il possesso da parte del client indicato. Il metodo di autenticazione hardware viene scelto dal KDC e la robustezza del metodo non viene indicata.
12-31 RESERVED. Riservato per un uso futuro.
EncTicketPart
3
EncryptionKey
flags
key
keytype
keyvalue
crealm
cname
TransitEncoding
transited
tr-type
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data


Presente nel ticket e nella risposta del KDC. E' utilizzato per passare la chiave dal kerberos all'application server ed al client. E' codificato in:
- keytype (intero): specifica il tipo di chiave di cifratura presente nel campo keyvalue.
- keyvalue (octect string): contiene la chiave codificata. Valori negativi sono riservati per un uso locale.
tkt-vno
realm
sname
enc-part
Ticket
1
EncTicketPart
3
EncryptionKey
flags
key
keytype
keyvalue
crealm
cname
TransitEncoding
transited
tr-type
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data

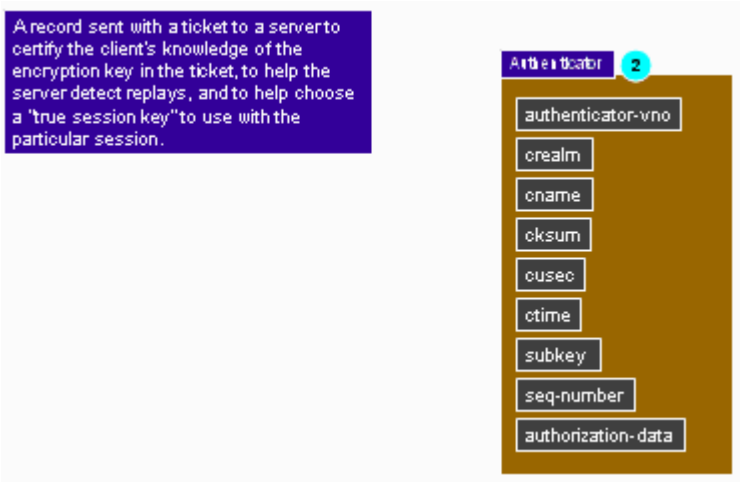

Contiene il nome del realm nel quale è registrato il client ed all'interno del quale avviene l'autenticazione iniziale.
Contiene la parte nome del principal identifier del client.
Elenca, senza un ordine preciso, i nomi dei realms Kerberos che hanno preso parte nell'autenticazione dell'utente per cui è stato emesso il ticket. E' codificato in:
- tr-type (intero).
- contents (octect string).
EncTicketPart
3
EncryptionKey
flags
key
keytype
keyvalue
crealm
cname
TransitEncoding
transited
tr-type
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data


EncTicketPart
3
EncryptionKey
flags
keytype
key
keyvalue
crealm
cname
TransitEncoding
tr-type
transited
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data
Indica quando è avvenuta l'autenticazione iniziale per il principal indicato.
tkt-vno
realm
sname
enc-part
Indica da quando il ticket è valido.
Indica fino a quando il ticket è valido.
Presente solo se il flag RENEWABLE è impostato. Indica il tempo massimo di fine che può essere incluso nel rinnovo. Tempo di scadenza assoluto per il ticket, compreso tutti i rinnovi.

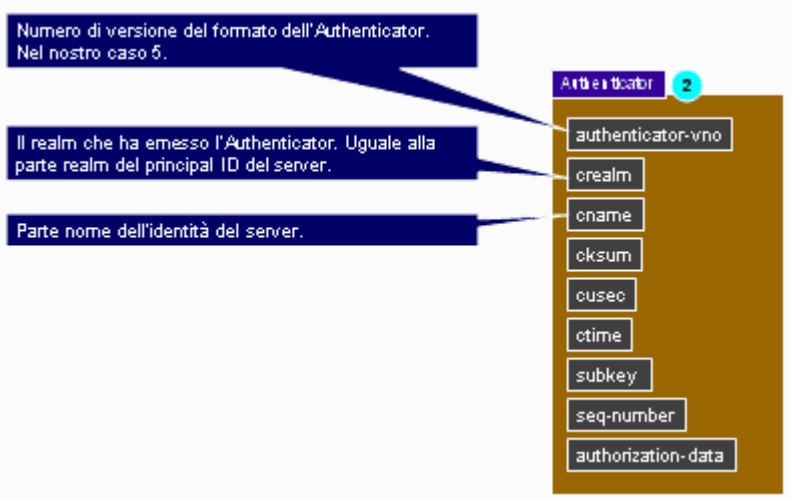

EncTicketPart
3
EncryptionKey
flags
keytype
key
keyvalue
crealm
cname
TransitEncoding
tr-type
transited
contents
authtime
starttime
endtime
renew-till
caddr
AuthorizationData
authorization-data
ad-type
ad-data
Contiene o meno (se omesso) indirizzi host dai quali poter utilizzare il ticket. Se non ci sono indirizzi il ticket può essere utilizzato da ovunque.
tkt-vno
realm
sname
Ticket
1
E' utilizzato per passare dati di autorizzazione dal principal, per il quale è stato emesso il ticket, all'application service. E' codificato in:
- ad-type (intero): Specifica il formato del campo ad-data. Valori negativi sono riservati per un uso locale.
- ad-data (octect string): Contiene i dati di autorizzazione da interpretare in base al valore del campo ad-type.

Authenticator

L'authenticator è un elemento molto importante. Partiamo dalla definizione data all'interno dell'RFC relativa al Kerberos:



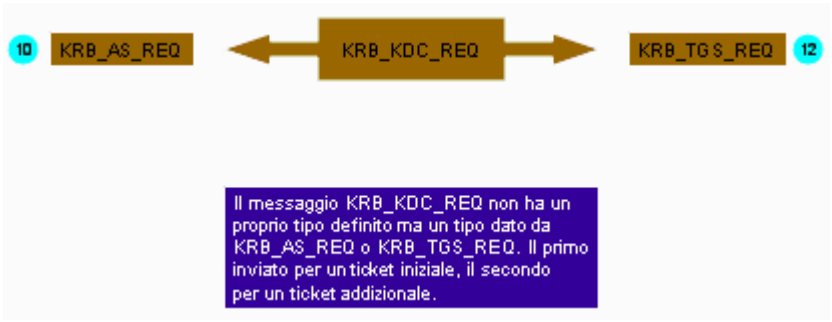
E proseguiamo analizzando i singoli elementi:

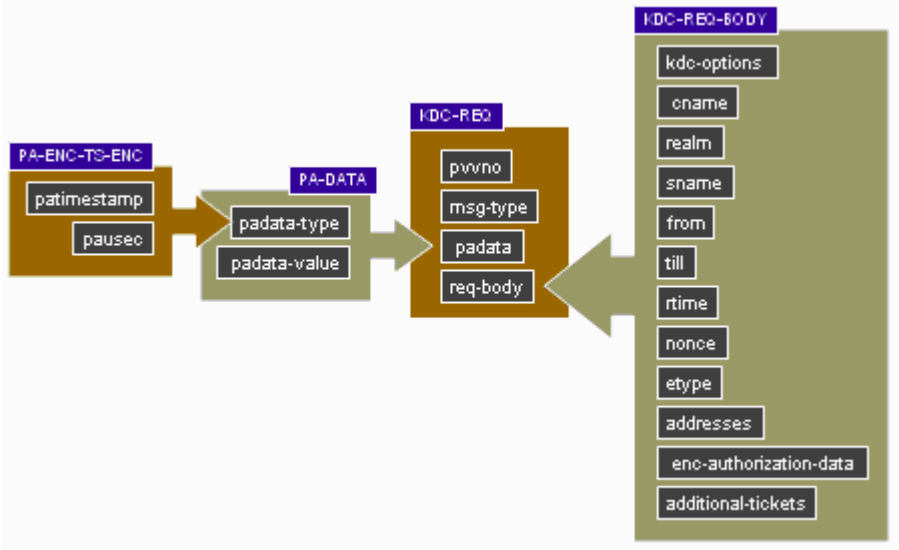


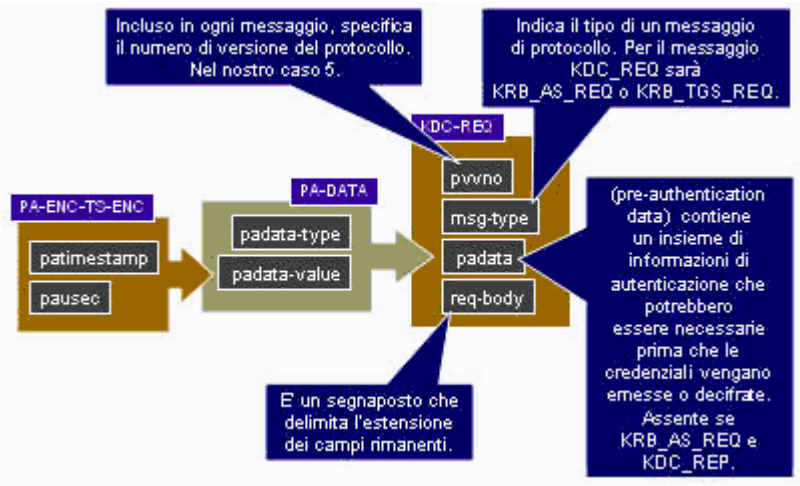

Authenticator
2
authenticator-vno
crealm
cname
cksum
cusec
ctime
subkey
seq-number
authorization-data
Opzionale. Assume diversi significati:
- Numero di sequenza iniziale da utilizzare nei messaggi KRB_PRIV o KRB_SAFE per rilevare ritrasmissioni (o per altri compiti specifici).
- Nell'Authenticator specifica il numero di sequenza iniziale per i messaggi dal client al server.
- Nel messaggio AP-REP specifica il numero di sequenza iniziale dal server al client.
- Nei messaggi KRB_PRIV e KRB_SAFE viene incrementato di 1 dopo l'invio di ogni messaggio.
Opzionale. Utilizzato per aggiungere maggiori restrizioni a quelle presenti nel medesimo campo del ticket.

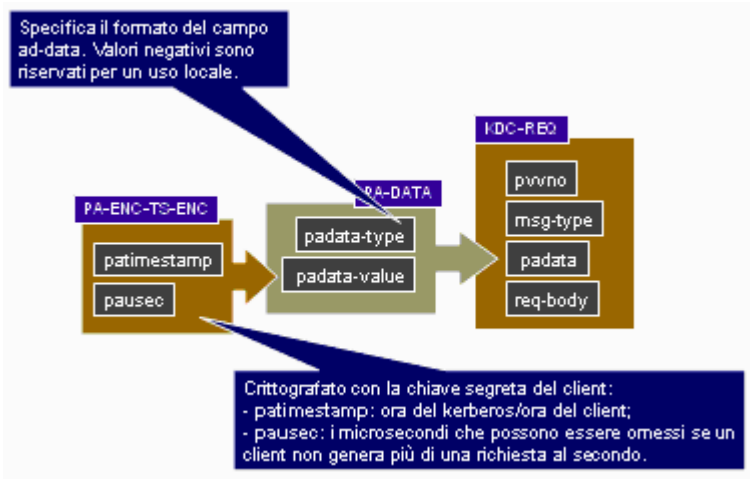
KRB_KDC_REQ

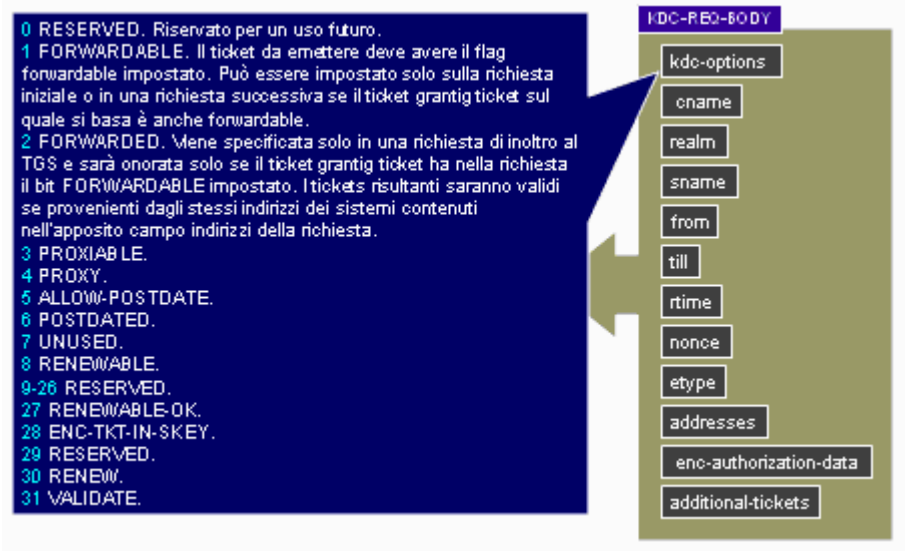
Analizziamo nei singoli elementi un messaggio di tipo KRB_KDC_REQ/KRB_TGS_REQ:

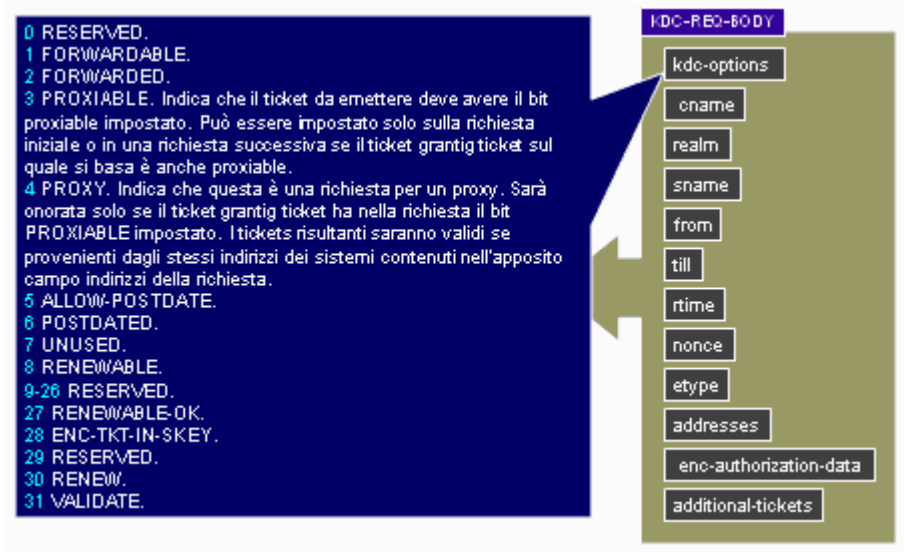


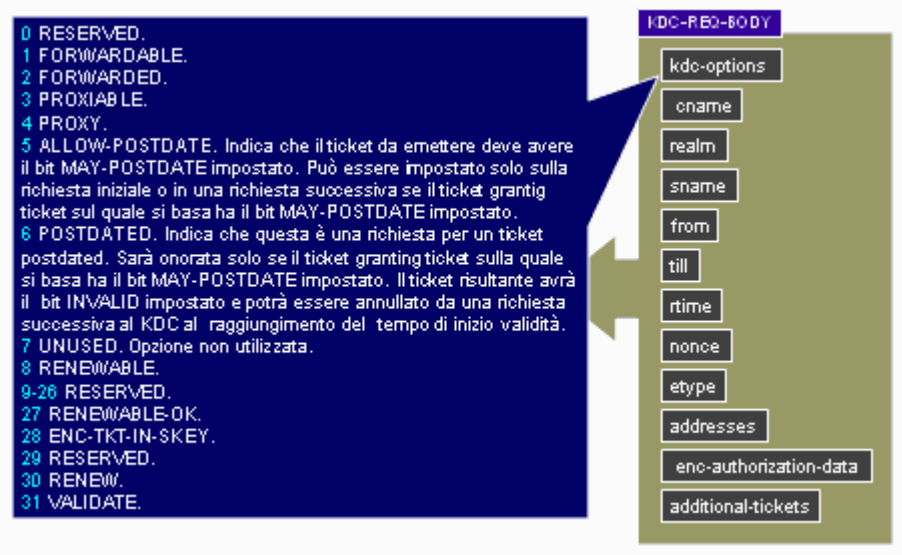


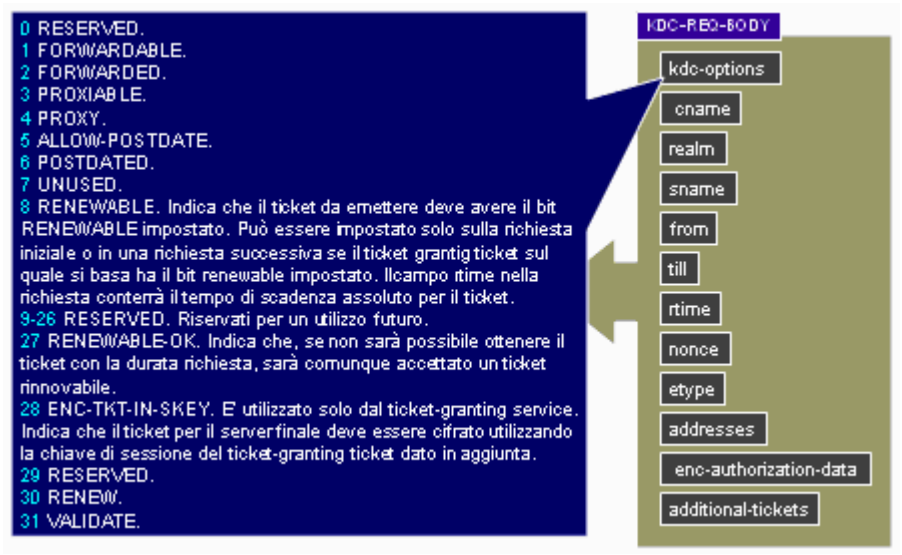


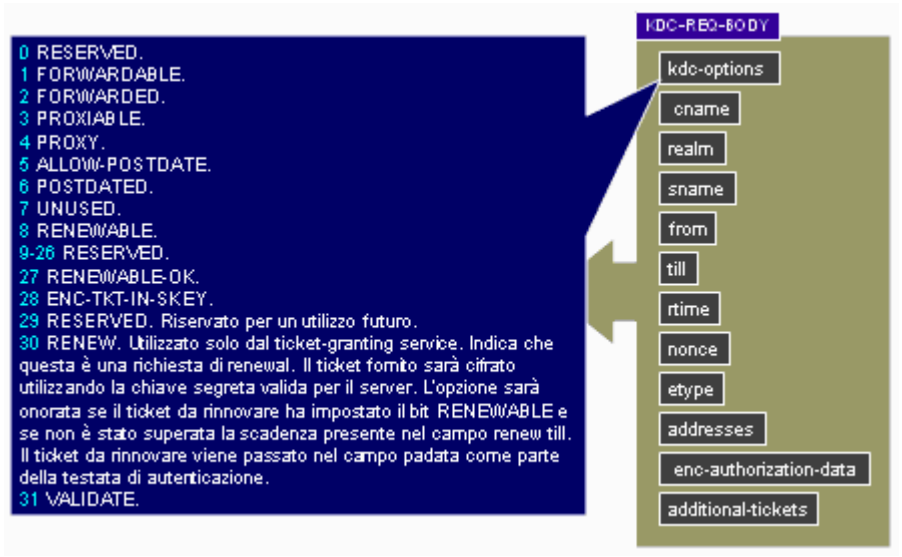

Specifica il formato del campo ad-data. Valori negativi sono riservati per un uso locale.
KDC-REQ
pvno
msg-type
padata
req-body
PA-DATA
padata-type
padata-value
PA-ENC-TS-ENC
patimestamp
pausec
Crittografato con la chiave segreta del client:
- patimestamp: ora del kerberos/ora del client;
- pausec: i microsecondi che possono essere omessi se un client non genera più di una richiesta al secondo.

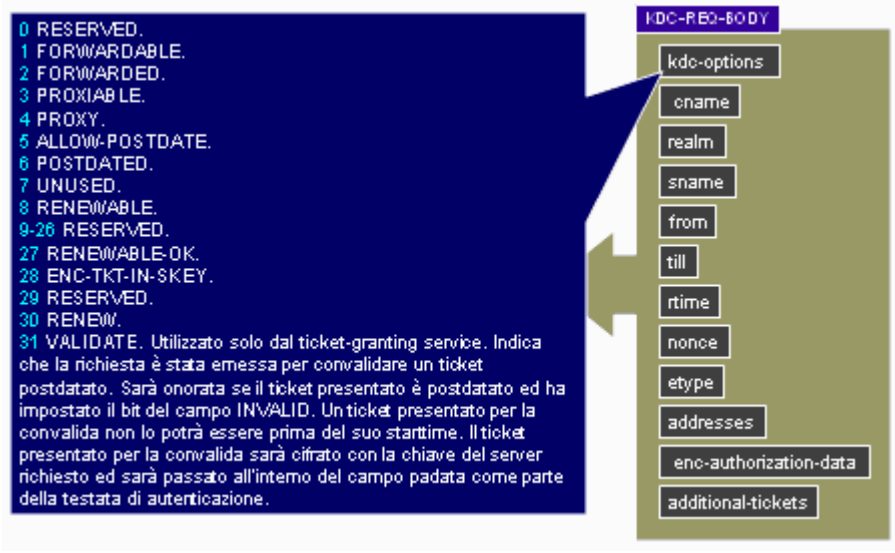

0 RESERVED. Riservato per un uso futuro.
1 FORWARDABLE. Il ticket da emettere deve avere il flag forwardable impostato. Può essere impostato solo sulla richiesta iniziale o in una richiesta successiva se il ticket grantig ticket sul quale si basa è anche forwardable.
2 FORWARDED. Viene specificata solo in una richiesta di inoltro al TGS e sarà onorata solo se il ticket grantig ticket ha nella richiesta il bit FORWARDABLE impostato. I tickets risultanti saranno validi se provenienti dagli stessi indirizzi dei sistemi contenuti nell'apposito campo indirizzi della richiesta.
3 PROXIABLE.
4 PROXY.
5 ALLOW-POSTDATE.
6 POSTDATED.
7 UNUSED.
8 RENEWABLE.
9-26 RESERVED.
27 RENEWABLE-OK.
28 ENC-TKT-IN-SKEY.
29 RESERVED.
30 RENEW.
31 VALIDATE.
KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets

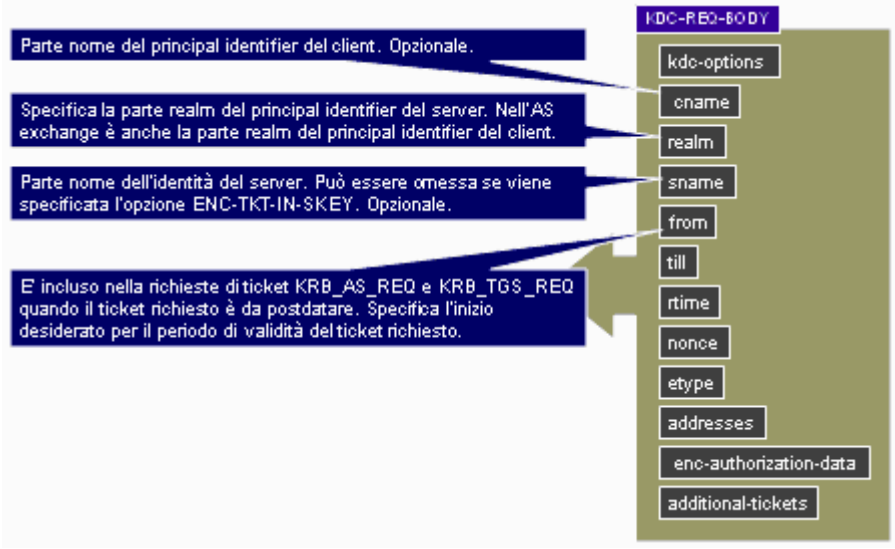

0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE. Indica che il ticket da emettere deve avere il bit proxiable impostato. Può essere impostato solo sulla richiesta iniziale o in una richiesta successiva se il ticket grantig ticket sul quale si basa è anche proxiable.
4 PROXY. Indica che questa è una richiesta per un proxy. Sarà onorata solo se il ticket grantig ticket ha nella richiesta il bit PROXIABLE impostato. I tickets risultanti saranno validi se provenienti dagli stessi indirizzi dei sistemi contenuti nell'apposito campo indirizzi della richiesta.
5 ALLOW-POSTDATE.
6 POSTDATED.
7 UNUSED.
8 RENEWABLE.
9-26 RESERVED.
27 RENEWABLE-OK.
28 ENC-TKT-IN-SKEY.
29 RESERVED.
30 RENEW.
31 VALIDATE.
KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets

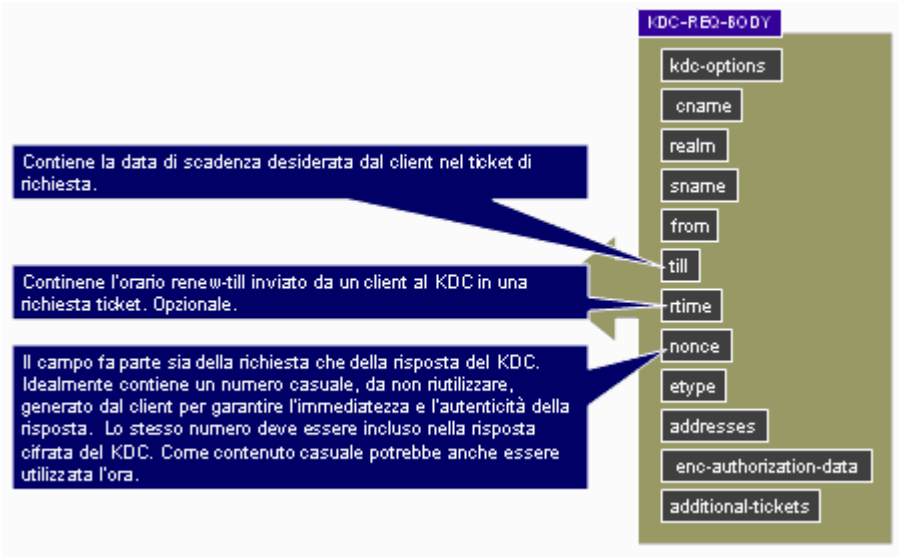

0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE.
4 PROXY.
5 ALLOW-POSTDATE. Indica che il ticket da emettere deve avere il bit MAY-POSTDATE impostato. Può essere impostato solo sulla richiesta iniziale o in una richiesta successiva se il ticket grantig ticket sul quale si basa ha il bit MAY-POSTDATE impostato.
6 POSTDATED. Indica che questa è una richiesta per un ticket postdated. Sarà onorata solo se il ticket granting ticket sulla quale si basa ha il bit MAY-POSTDATE impostato. Il ticket risultante avrà il bit INVALID impostato e potrà essere annullato da una richiesta successiva al KDC al raggiungimento del tempo di inizio validità.
7 UNUSED. Opzione non utilizzata.
8 RENEWABLE.
9-26 RESERVED.
27 RENEWABLE-OK.
28 ENC-TKT-IN-SKEY.
29 RESERVED.
30 RENEW.
31 VALIDATE.
KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets

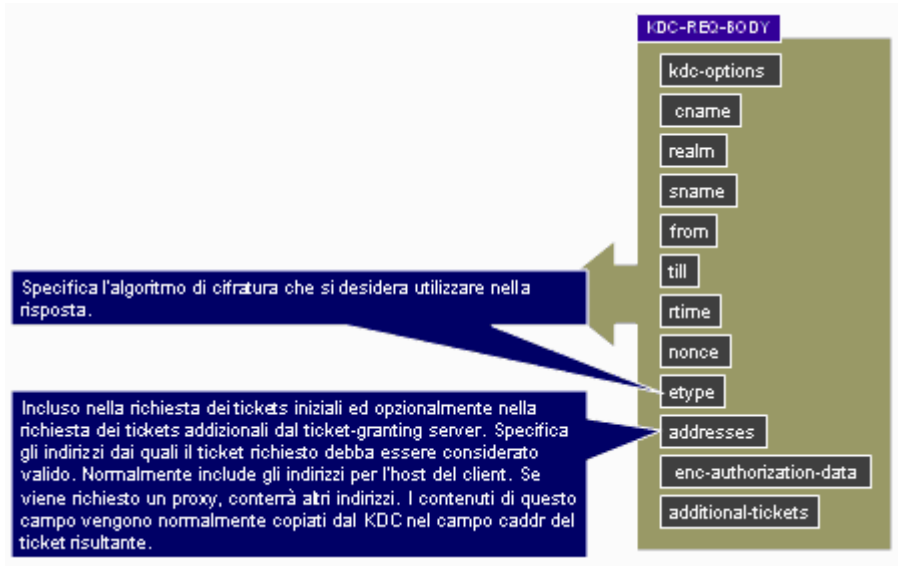

0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE.
4 PROXY.
5 ALLOW-POSTDATE.
6 POSTDATED.
7 UNUSED.
8 RENEWABLE. Indica che il ticket da emettere deve avere il bit RENEWABLE impostato. Può essere impostato solo sulla richiesta iniziale o in una richiesta successiva se il ticket grantig ticket sul quale si basa ha il bit renewable impostato. Il campo rtime nella richiesta conterrà il tempo di scadenza assoluto per il ticket.
9-26 RESERVED. Riservati per un utilizzo futuro.
27 RENEWABLE-OK. Indica che, se non sarà possibile ottenere il ticket con la durata richiesta, sarà comunque accettato un ticket rinnovabile.
28 ENC-TKT-IN-SKEY. E' utilizzato solo dal ticket-granting service. Indica che il ticket per il server finale deve essere cifrato utilizzando la chiave di sessione del ticket-granting ticket dato in aggiunta.
29 RESERVED.
30 RENEW.
31 VALIDATE.
KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets

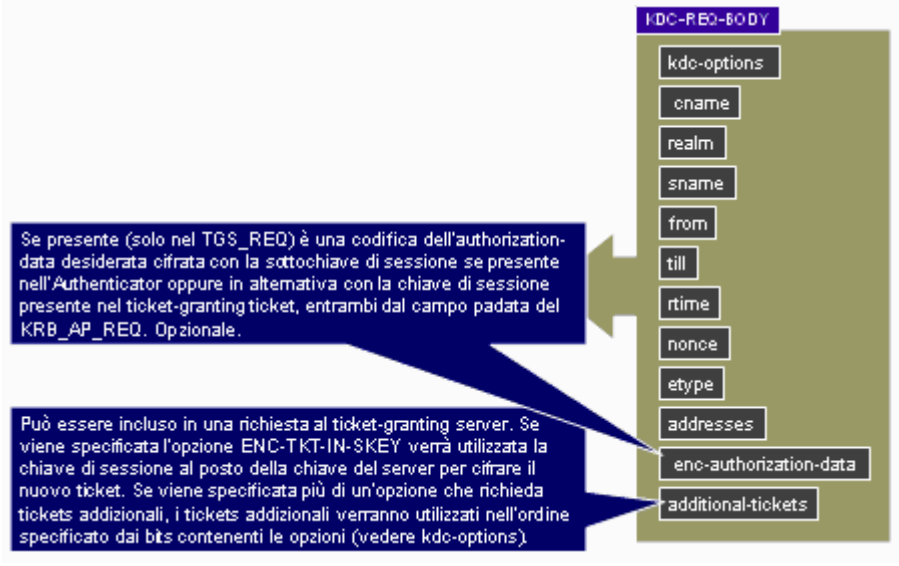

0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE.
4 PROXY.
5 ALLOW-POSTDATE.
6 POSTDATED.
7 UNUSED.
8 RENEWABLE.
9-26 RESERVED.
27 RENEWABLE-OK.
28 ENC-TKT-IN-SKEY.
29 RESERVED. Riservato per un utilizzo futuro.
30 RENEW. Utilizzato solo dal ticket-granting service. Indica che questa è una richiesta di renewal. Il ticket fornito sarà cifrato utilizzando la chiave segreta valida per il server. L'opzione sarà onorata se il ticket da rinnovare ha impostato il bit RENEWABLE e se non è stato superata la scadenza presente nel campo renew till. Il ticket da rinnovare viene passato nel campo padata come parte della testata di autenticazione.
31 VALIDATE.
KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets


0 RESERVED.
1 FORWARDABLE.
2 FORWARDED.
3 PROXIABLE.
4 PROXY.
5 ALLOW-POSTDATE.
6 POSTDATED.
7 UNUSED.
8 RENEWABLE.
9-26 RESERVED.
27 RENEWABLE-OK.
28 ENC-TKT-IN-SKEY.
29 RESERVED.
30 RENEW.
31 VALIDATE. Utilizzato solo dal ticket-granting service. Indica che la richiesta è stata emessa per convalidare un ticket postdatato. Sarà onorata se il ticket presentato è postdatato ed ha impostato il bit del campo INVALID. Un ticket presentato per la convalida non lo potrà essere prima del suo starttime. Il ticket presentato per la convalida sarà cifrato con la chiave del server richiesto ed sarà passato all'interno del campo padata come parte della testata di autenticazione.
KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets


Parte nome del principal identifier del client. Opzionale.
Specifica la parte realm del principal identifier del server. Nell'AS exchange è anche la parte realm del principal identifier del client.
Parte nome dell'identità del server. Può essere omessa se viene specificata l'opzione ENC-TKT-IN-SKEY. Opzionale.
E' incluso nella richieste di ticket KRB_AS_REQ e KRB_TGS_REQ quando il ticket richiesto è da postdatare. Specifica l'inizio desiderato per il periodo di validità del ticket richiesto.
KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets

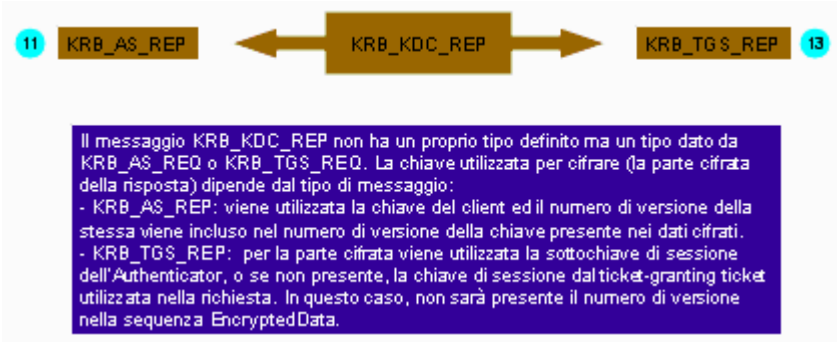

KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets
Contiene la data di scadenza desiderata dal client nel ticket di richiesta.
Continene l'orario renew-till inviato da un client al KDC in una richiesta ticket. Opzionale.
Il campo fa parte sia della richiesta che della risposta del KDC. Idealmente contiene un numero casuale, da non riutilizzare, generato dal client per garantire l'immediatezza e l'autenticità della risposta. Lo stesso numero deve essere incluso nella risposta cifrata del KDC. Come contenuto casuale potrebbe anche essere utilizzata l'ora.

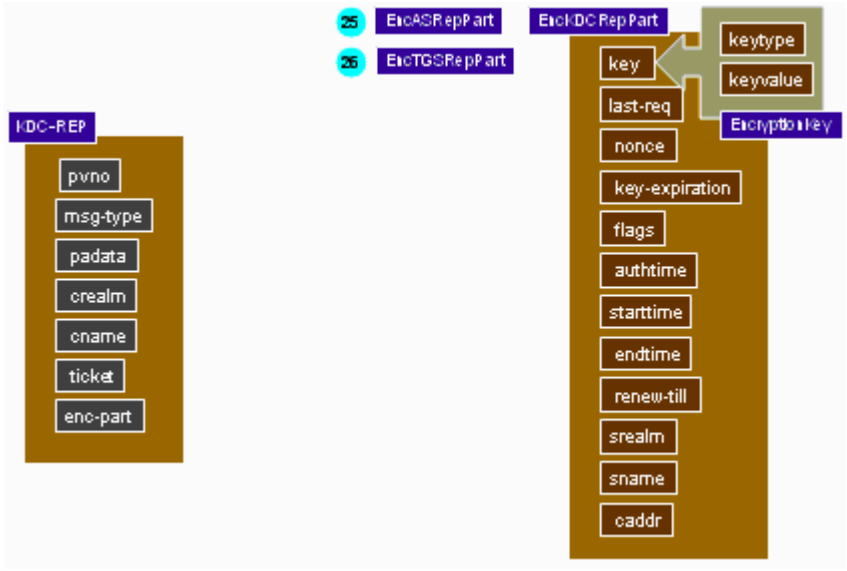

KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets
Specifica l'algoritmo di cifratura che si desidera utilizzare nella risposta.
Incluso nella richiesta dei tickets iniziali ed opzionalmente nella richiesta dei tickets addizionali dal ticket-granting server. Specifica gli indirizzi dai quali il ticket richiesto debba essere considerato valido. Normalmente include gli indirizzi per l'host del client. Se viene richiesto un proxy, conterrà altri indirizzi. I contenuti di questo campo vengono normalmente copiati dal KDC nel campo caddr del ticket risultante.

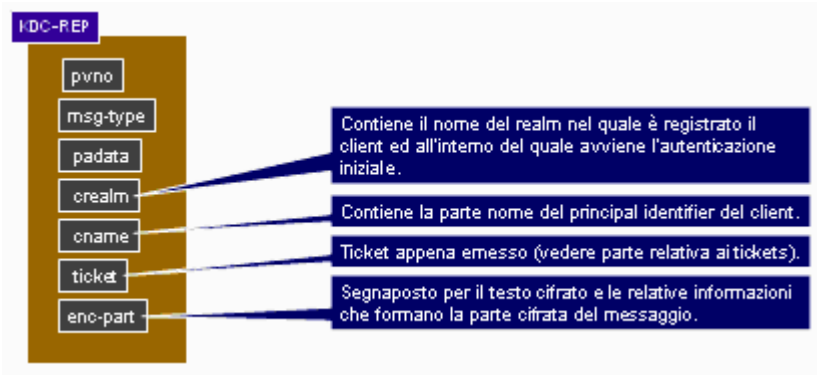

KDC-REQ-BODY
kdc-options
cname
realm
sname
from
till
rtime
nonce
etype
addresses
enc-authorization-data
additional-tickets
Se presente (solo nel TGS_REQ) è una codifica dell'authorization-data desiderata cifrata con la sottochiave di sessione se presente nell'Authenticator oppure in alternativa con la chiave di sessione presente nel ticket-granting ticket, entrambi dal campo padata del KRB_AP_REQ. Opzionale.
Può essere incluso in una richiesta al ticket-granting server. Se viene specificata l'opzione ENC-TKT-IN-SKEY verrà utilizzata la chiave di sessione al posto della chiave del server per cifrare il nuovo ticket. Se viene specificata più di un'opzione che richieda tickets addizionali, i tickets addizionali verranno utilizzati nell'ordine specificato dai bits contenenti le opzioni (vedere kdc-options).

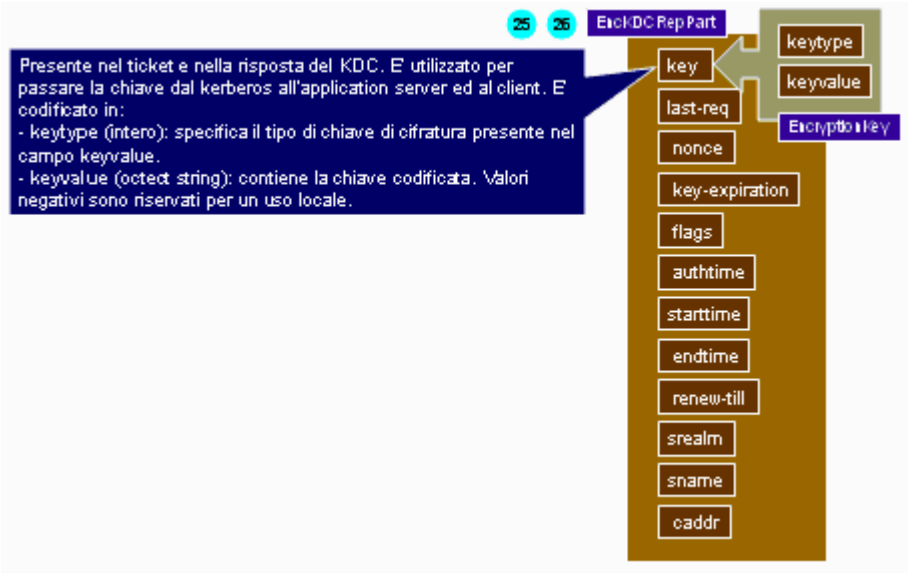
KRB_KDC_REP

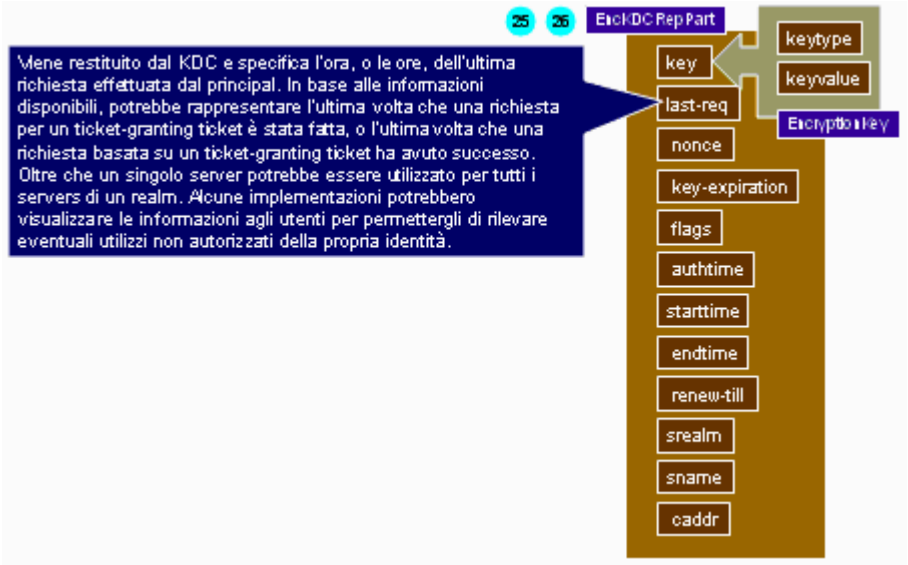
Analizziamo nei singoli elementi un messaggio di tipo KRB_AS_REP/KRB_TGS_REP:

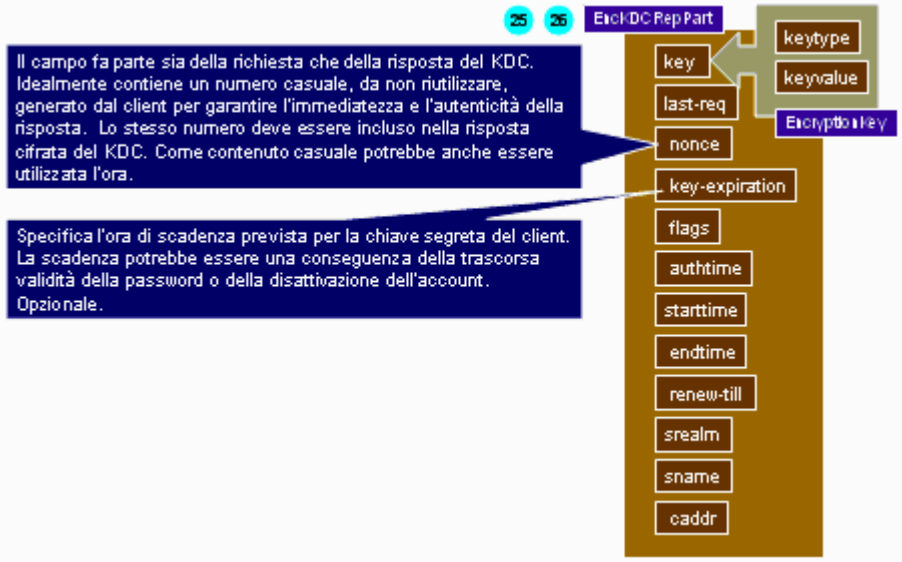


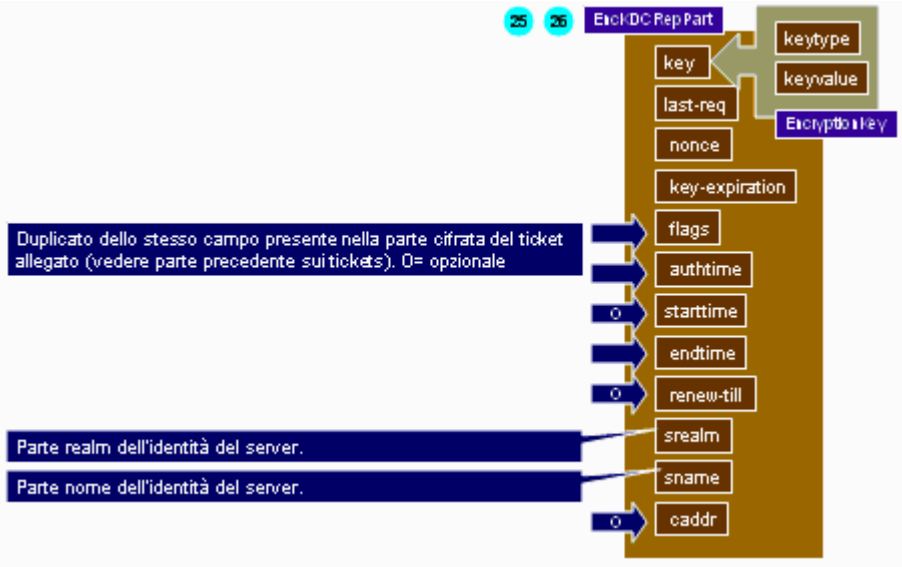



KDC-REP
pvno
msg-type
padata
crealm
cname
ticket
enc-part
Contiene il nome del realm nel quale è registrato il client ed all'interno del quale avviene l'autenticazione iniziale.
Contiene la parte nome del principal identifier del client.
Ticket appena emesso (vedere parte relativa ai tickets).
Segnaposto per il testo cifrato e le relative informazioni che formano la parte cifrata del messaggio.


25
26
EncKDCRepPart
key
last-req
nonce
key-expiration
flags
authtime
starttime
endtime
renew-till
srealm
sname
caddr
keytype
keyvalue
EncryptionKey
Presente nel ticket e nella risposta del KDC. E' utilizzato per passare la chiave dal kerberos all'application server ed al client. E' codificato in:
- keytype (intero): specifica il tipo di chiave di cifratura presente nel campo keyvalue.
- keyvalue (octect string): contiene la chiave codificata. Valori negativi sono riservati per un uso locale.

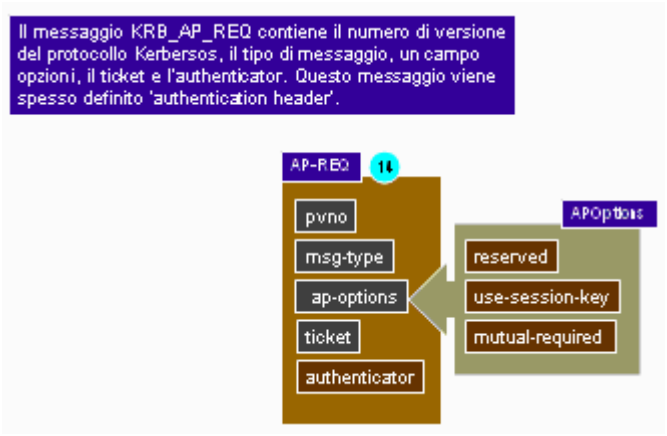

25
26
EncKDCRepPart
key
last-req
nonce
key-expiration
flags
authtime
starttime
endtime
renew-till
srealm
sname
caddr
keytype
keyvalue
EncryptionKey
Viene restituito dal KDC e specifica l'ora, o le ore, dell'ultima richiesta effettuata dal principal. In base alle informazioni disponibili, potrebbe rappresentare l'ultima volta che una richiesta per un ticket-granting ticket è stata fatta, o l'ultima volta che una richiesta basata su un ticket-granting ticket ha avuto successo. Oltre che un singolo server potrebbe essere utilizzato per tutti i servers di un realm. Alcune implementazioni potrebbero visualizzare le informazioni agli utenti per permettergli di rilevare eventuali utilizzi non autorizzati della propria identità.

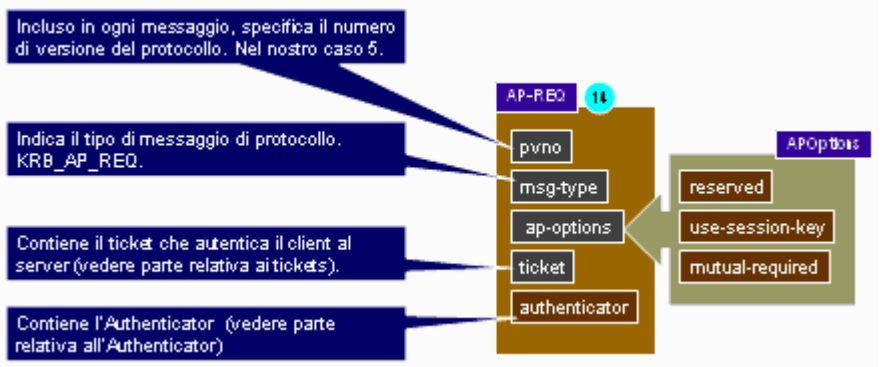

25
26
EncKDCRepPart
keytype
key
keyvalue
last-req
EncryptionKey
nonce
key-expiration
flags
authtime
starttime
endtime
renew-till
srealm
sname
caddr
Il campo fa parte sia della richiesta che della risposta del KDC. Idealmente contiene un numero casuale, da non riutilizzare, generato dal client per garantire l'immediatezza e l'autenticità della risposta. Lo stesso numero deve essere incluso nella risposta cifrata del KDC. Come contenuto casuale potrebbe anche essere utilizzata l'ora.
Specifica l'ora di scadenza prevista per la chiave segreta del client. La scadenza potrebbe essere una conseguenza della trascorsa validità della password o della disattivazione dell'account. Opzionale.

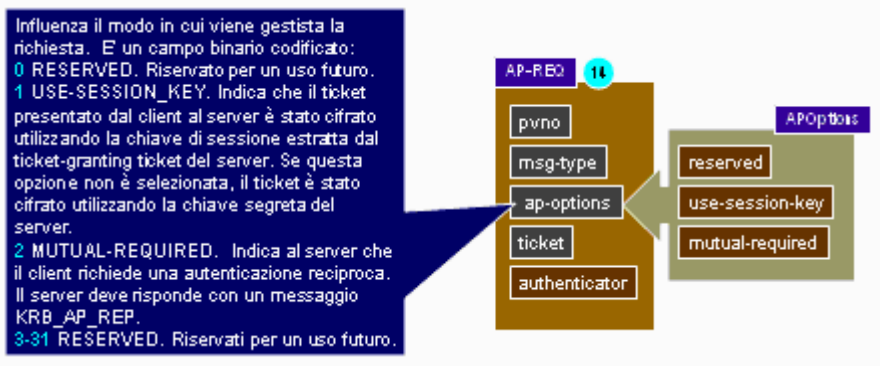

25
26
EncKDCRepPart
keytype
key
keyvalue
last-req
EncryptionKey
nonce
key-expiration
flags
authtime
O
starttime
endtime
O
renew-till
srealm
sname
O
caddr
Duplicato dello stesso campo presente nella parte cifrata del ticket allegato (vedere parte precedente sui tickets). O= opzionale
Parte realm dell'identità del server.
Parte nome dell'identità del server.

KRB_AP_REQ

Analizziamo nei singoli elementi un messaggio di tipo KRB_AP_REQ:

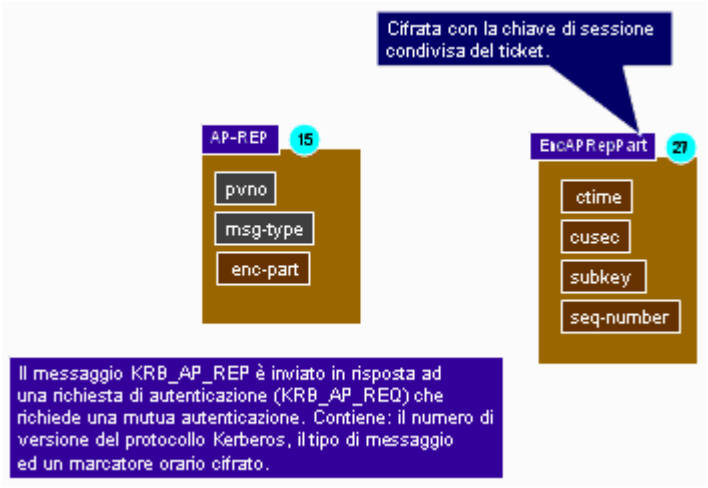


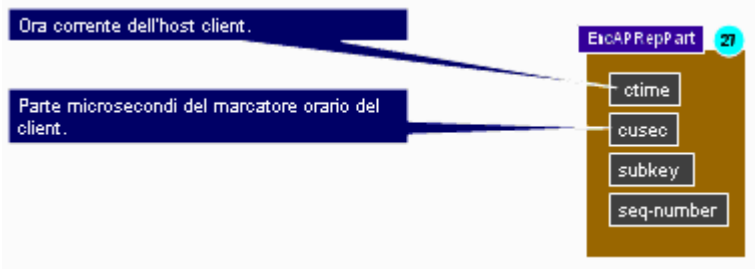


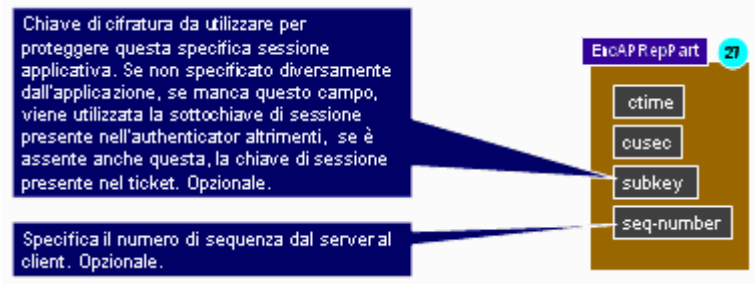


KRB_AP_REP

Analizziamo nei singoli elementi un messaggio di tipo KRB_AP_REP:

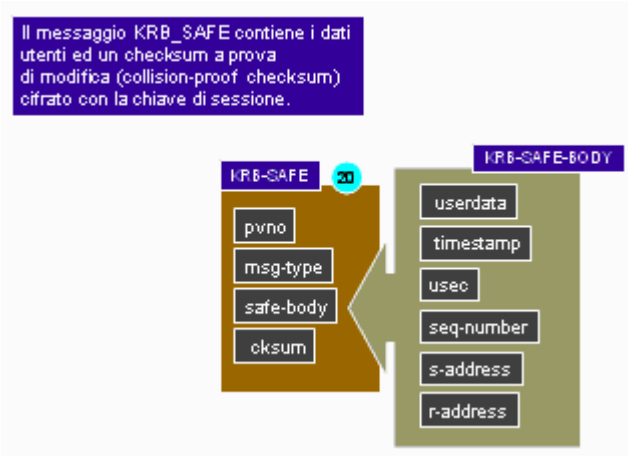


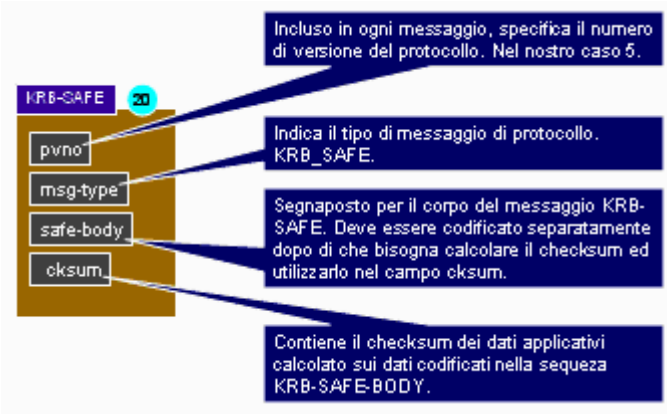


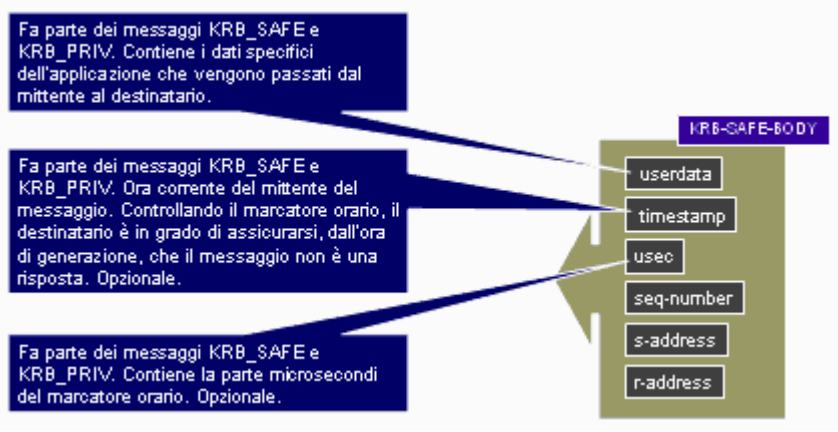


KRB_SAFE

Analizziamo nei singoli elementi un messaggio di tipo KRB_SAFE:



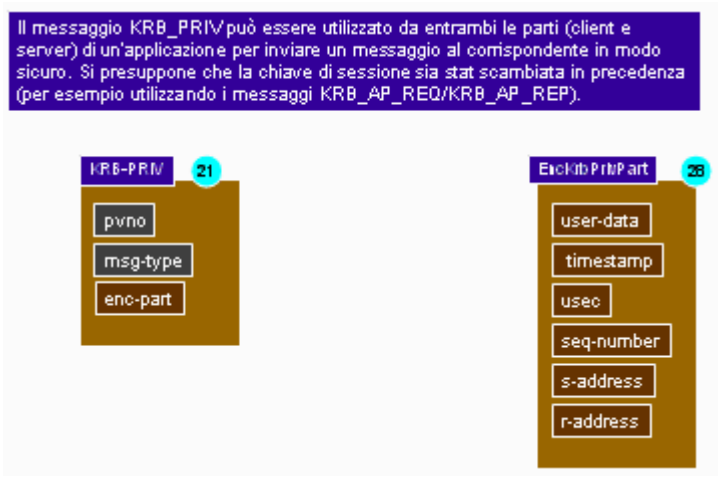


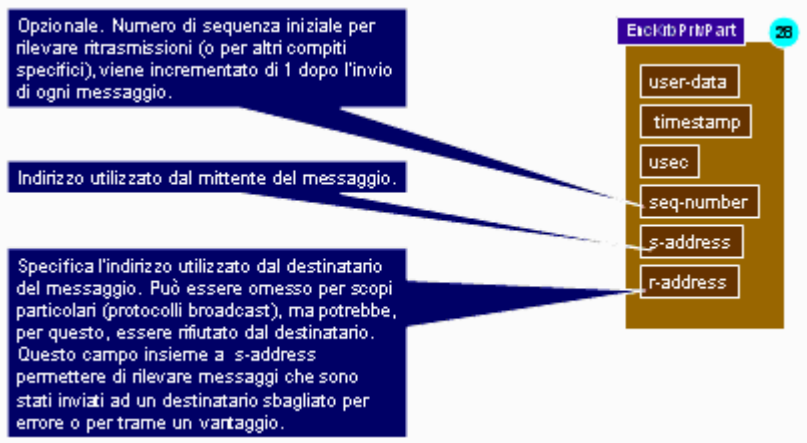



Opzionale. Numero di sequenza iniziale per rilevare ritrasmissioni (o per altri compiti specifici), viene incrementato di 1 dopo l'invio di ogni messaggio.
Indirizzo utilizzato dal mittente del messaggio.
Specifica l'indirizzo utilizzato dal destinatario del messaggio. Può essere omesso per scopi particolari (protocolli broadcast), ma potrebbe, per questo, essere rifiutato dal destinatario. Questo campo insieme a s-address permettere di rilevare messaggi che sono stati inviati ad un destinatario sbagliato per errore o per trarne un vantaggio.
KRB-SAFE-BODY
userdata
timestamp
usec
seq-number
s-address
r-address

KRB_PRIV

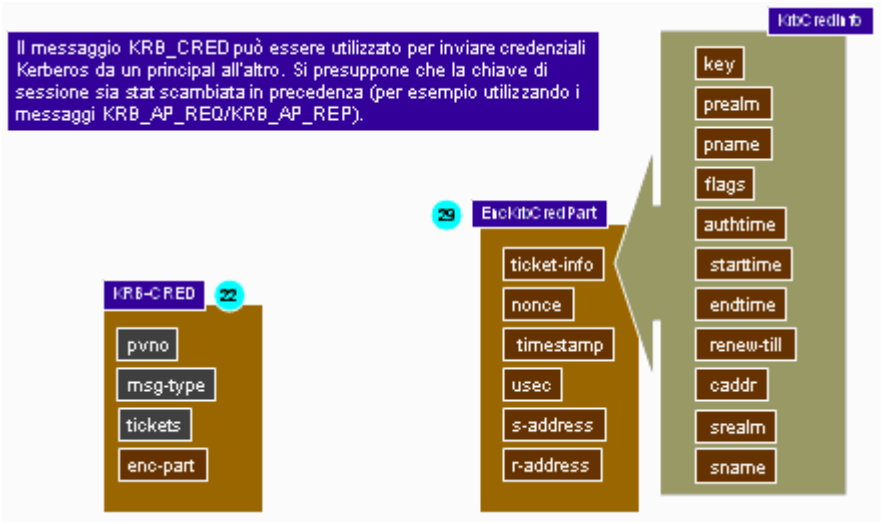
Analizziamo nei singoli elementi un messaggio di tipo KRB_PRIV:

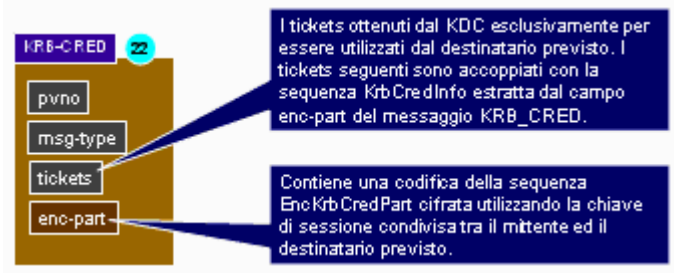


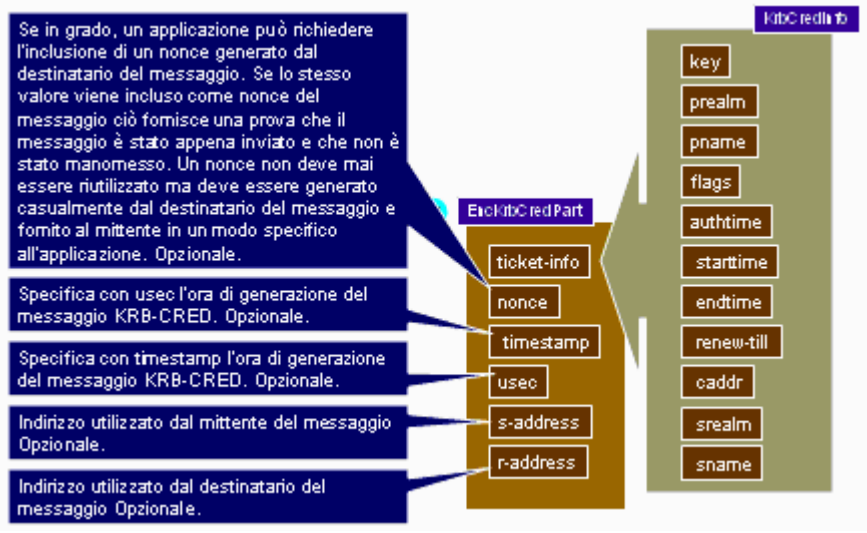

Opzionale. Numero di sequenza iniziale per rilevare ritrasmissioni (o per altri compiti specifici), viene incrementato di 1 dopo l'invio di ogni messaggio.
Indirizzo utilizzato dal mittente del messaggio.
Specifica l'indirizzo utilizzato dal destinatario del messaggio. Può essere omesso per scopi particolari (protocolli broadcast), ma potrebbe, per questo, essere rifiutato dal destinatario. Questo campo insieme a s-address permettere di rilevare messaggi che sono stati inviati ad un destinatario sbagliato per errore o per trarne un vantaggio.
user-data
timestamp
usec
seq-number
s-address
r-address

KRB_CRED

Analizziamo nei singoli elementi un messaggio di tipo KRB_CRED:



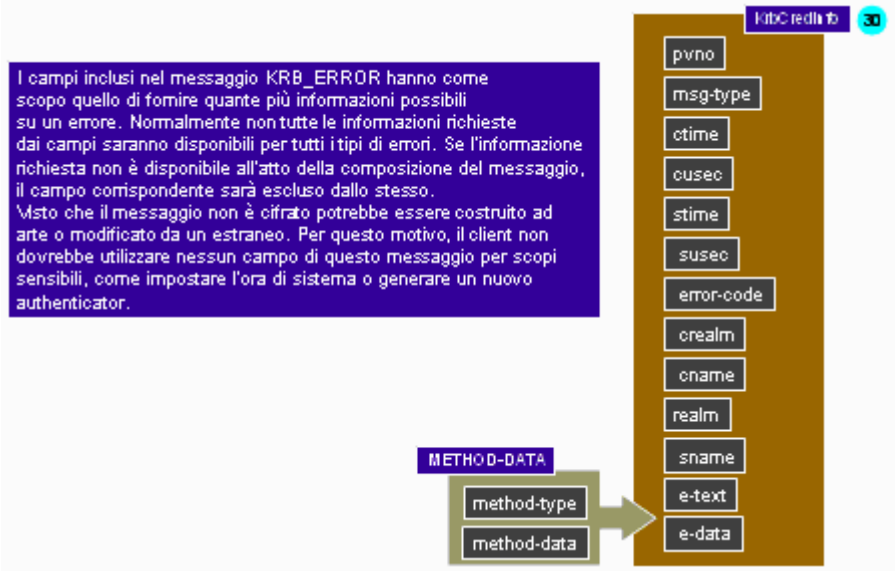


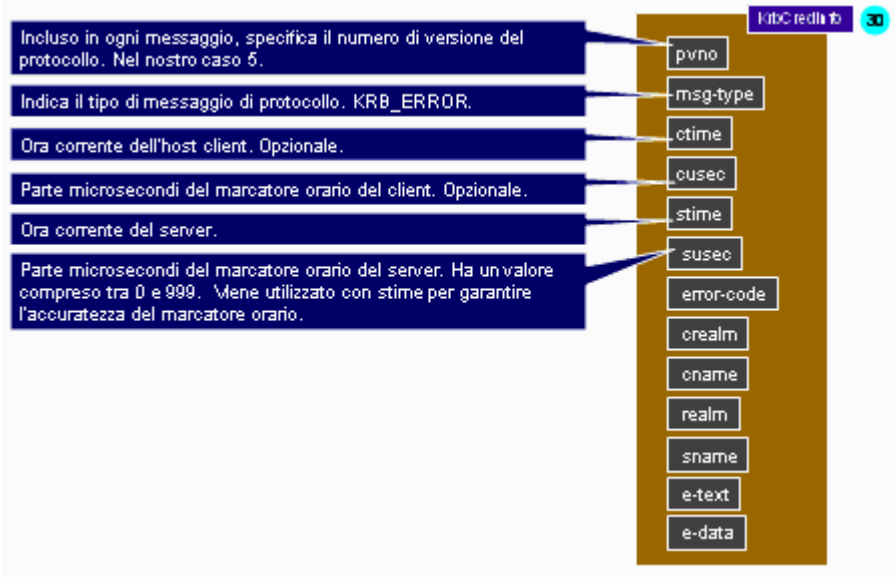

Se in grado, un applicazione può richiedere l'inclusione di un nonce generato dal destinatario del messaggio. Se lo stesso valore viene incluso come nonce del messaggio ciò fornisce una prova che il messaggio è stato appena inviato e che non è stato manomesso. Un nonce non deve mai essere riutilizzato ma deve essere generato casualmente dal destinatario del messaggio e fornito al mittente in un modo specifico all'applicazione. Opzionale.
Specifica con usec l'ora di generazione del messaggio KRB-CRED. Opzionale.
Specifica con timestamp l'ora di generazione del messaggio KRB-CRED. Opzionale.
Indirizzo utilizzato dal mittente del messaggio Opzionale.
Indirizzo utilizzato dal destinatario del messaggio Opzionale.
EncKrbCredPart
ticket-info
nonce
timestamp
usec
s-address
r-address
KrbCredInfo
key
prealm
pname
flags
authtime
starttime
endtime
renew-till
caddr
srealm
sname

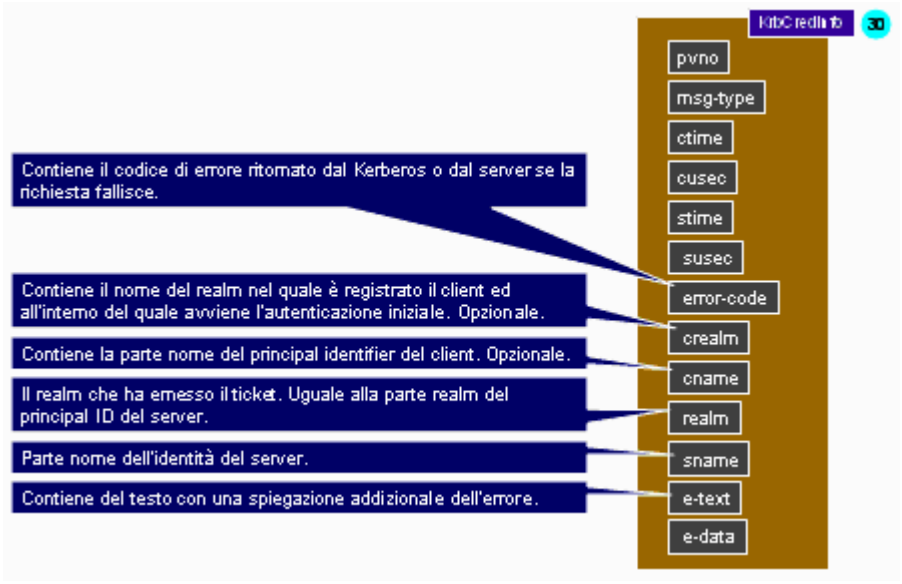

Il campo esiste nel ticket corrispondete passato dal messaggio KRB-CRE. E' utilizzato per passare la chiave di sessione dal mittente al destinatario previsto.
I campi seguenti sono opzionali. Se presenti possono essere associati con le credenziali nel file del ticket remoto. Se assenti si assume che il destinatario delle credenziali ne conosca già il valore:
- prealm e pname: Il nome ed il realm dell'identità del principal delegato.
- flags, authtime, starttime, endtime, renew-till, srealm, sname e caddr: Questi campi contengono i valori dei campi corrispondenti a quelli presenti nel ticket estratto dal campo ticket. La descrizione dei singoli campi è simile a quella dei campi del messaggio KDC-REP (vedere messaggio KDC-REP).
KrbCredInfo
key
prealm
pname
flags
authtime
starttime
endtime
renew-till
caddr
srealm
sname

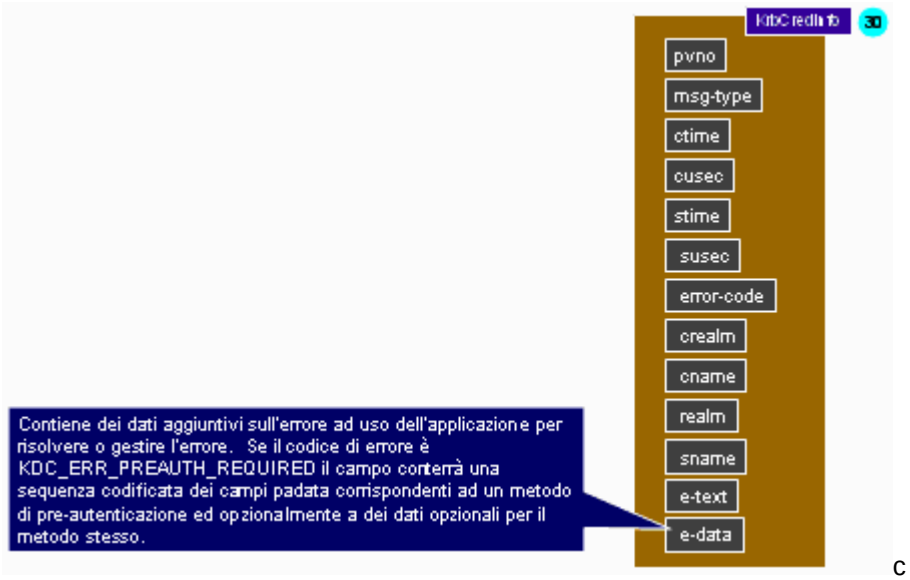
KRB_ERROR

Analizziamo nei singoli elementi un messaggio di tipo KRB_ERROR:



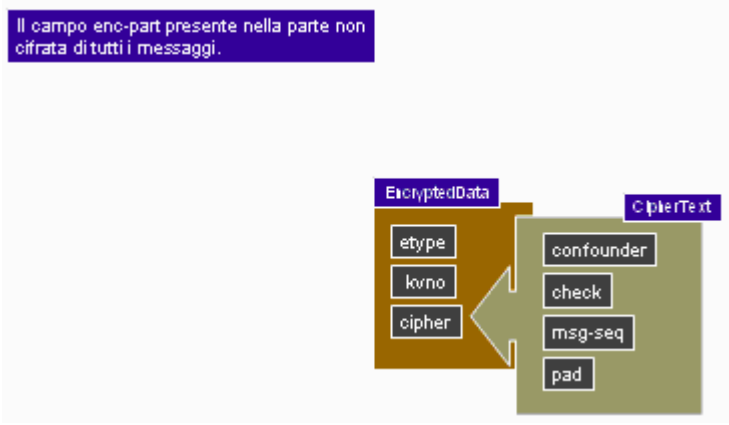


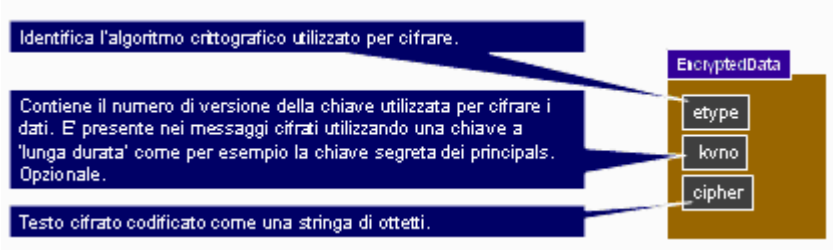

KrbCredInfo
30
pvno
msg-type
ctime
cusec
stime
susec
error-code
crealm
cname
realm
sname
e-text
e-data
Contiene il codice di errore ritornato dal Kerberos o dal server se la richiesta fallisce.
Contiene il nome del realm nel quale è registrato il client ed all'interno del quale avviene l'autenticazione iniziale. Opzionale.
Contiene la parte nome del principal identifier del client. Opzionale.
Il realm che ha emesso il ticket. Uguale alla parte realm del principal ID del server.
Parte nome dell'identità del server.
Contiene del testo con una spiegazione addizionale dell'errore.


KrbCredInfo
30
pvno
msg-type
ctime
cusec
stime
susec
error-code
crealm
cname
realm
sname
e-text
e-data
Contiene dei dati aggiuntivi sull'errore ad uso dell'applicazione per risolvere o gestire l'errore. Se il codice di errore è KDC_ERR_PREAUTH_REQUIRED il campo conterrà una sequenza codificata dei campi padata corrispondenti ad un metodo di pre-autenticazione ed opzionalmente a dei dati opzionali per il metodo stesso.
c

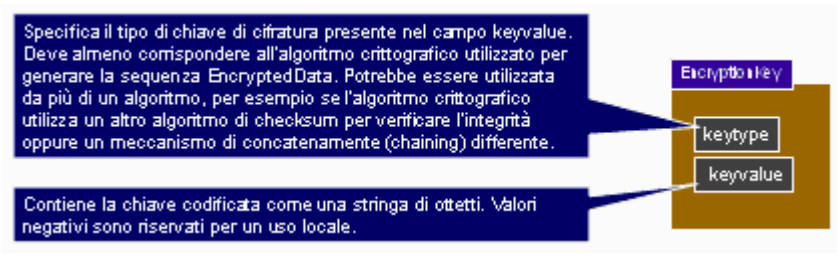
Componente cifrata

Come abbiamo visto, la parte cifrata riveste un ruolo fondamentale all'interno dei singoli passaggi legati al processo di scambio delle credenziali alla base del Kerberos:



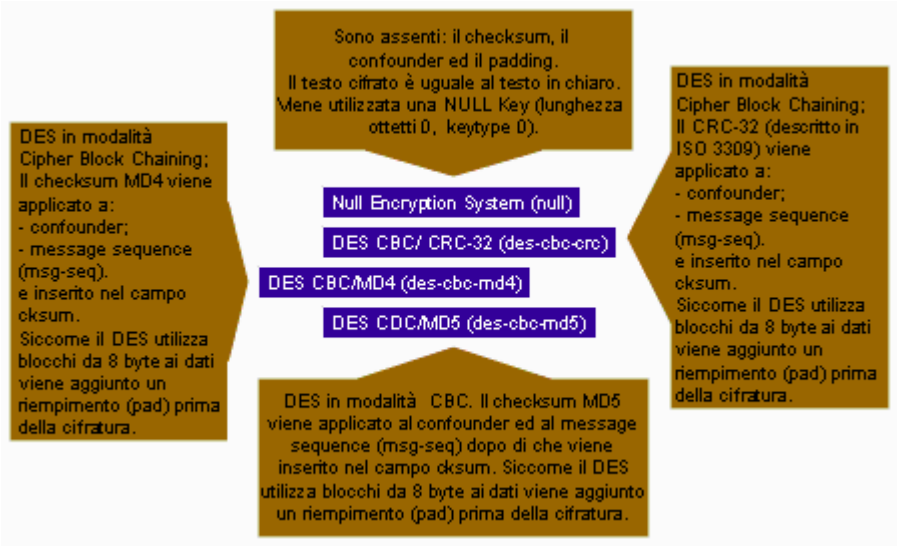


Chiavi di cifratura



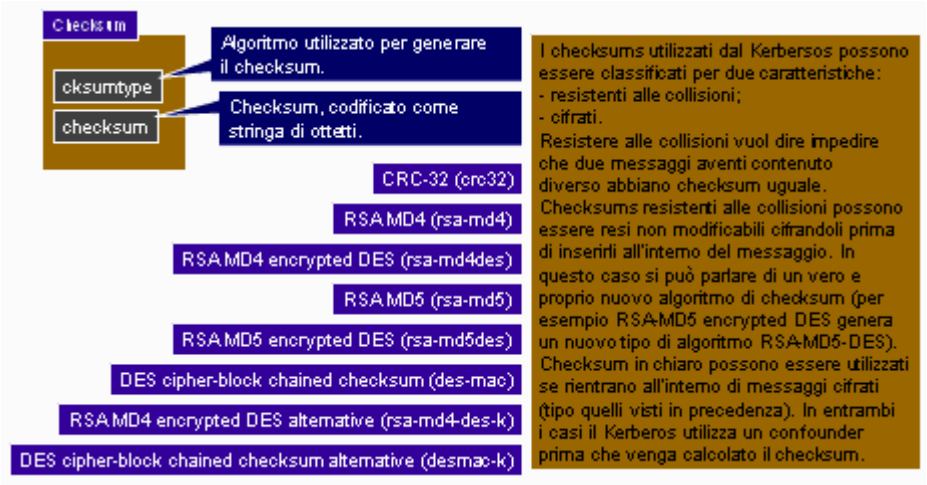
Sistemi di cifratura

Vengono utilizzati diversi algoritmi crittografici e all'interno degli stessi, diverse modalità di concatenazione/funzionamento:



Checksums

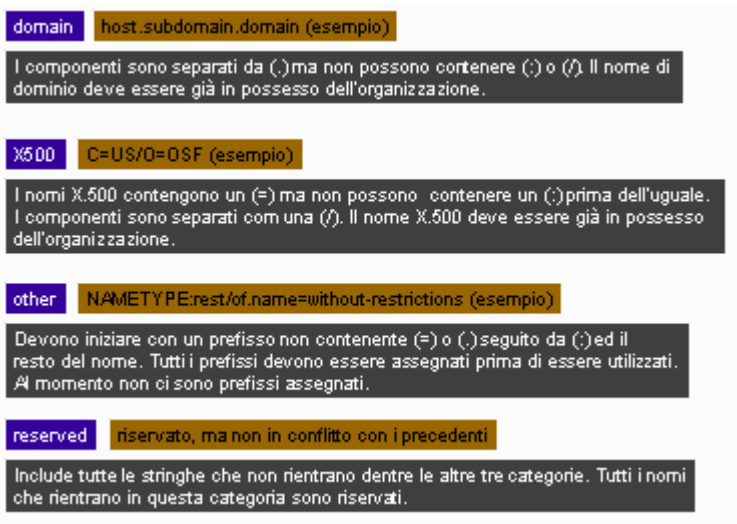
Lo stesso dicasi per gli algoritmi di controllo:

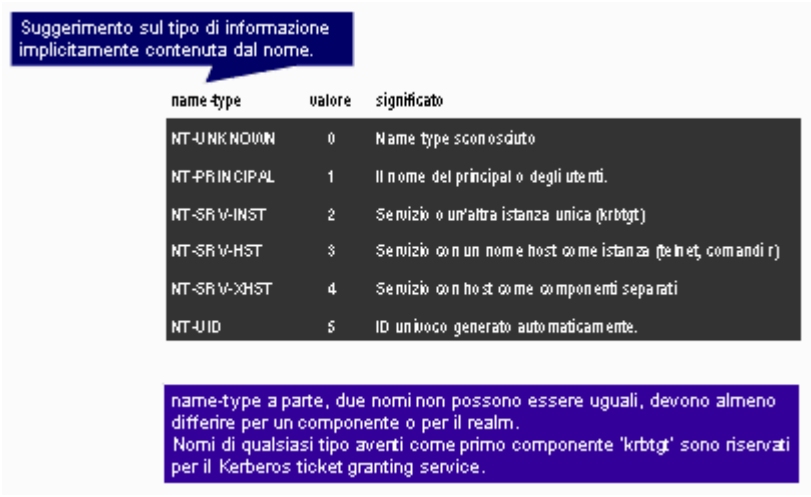


Nomi

Nomi realms

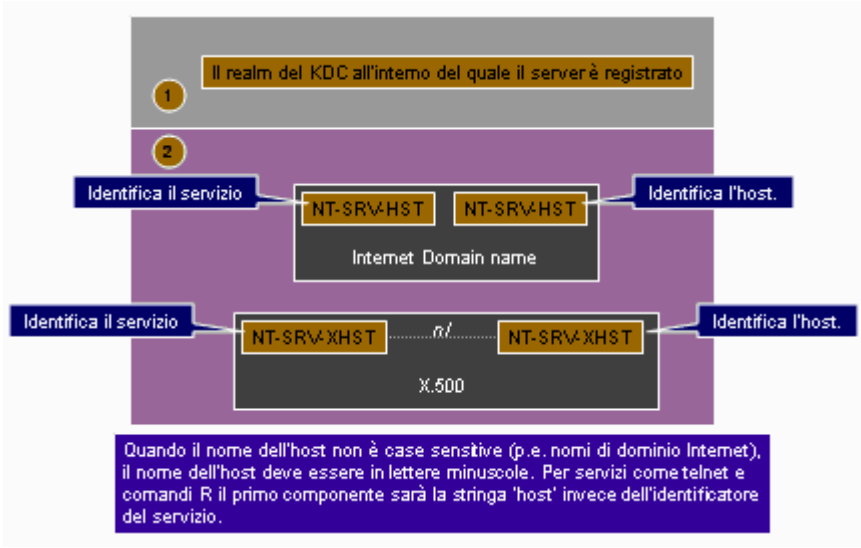
I nomi dei realms variano naturalmente in base al sistema utilizzato:





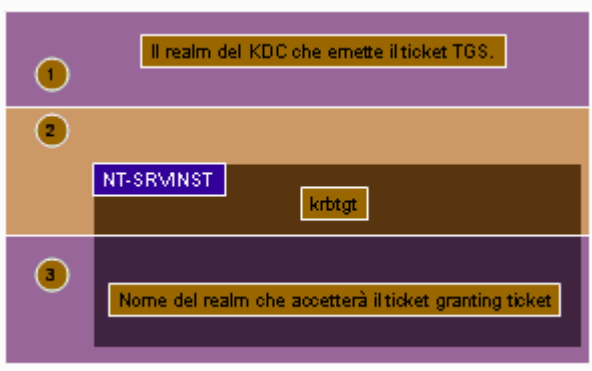
Nomi principal server

Vediamo su cosa si basa il nome del principal:

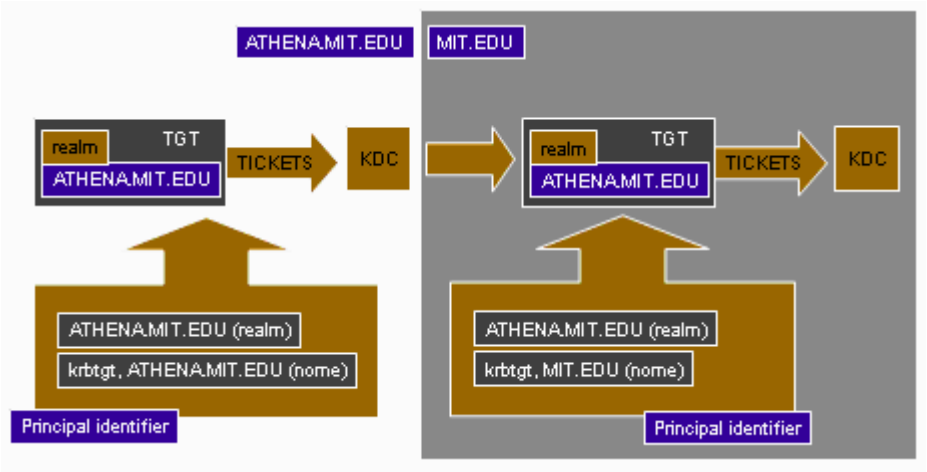


Nome del TGS

La struttura del nome è così costituita:



Vediamo un esempio fra realms differenti:



Gestione

All'interno dei sistemi MS Windows, le funzioni di AS e TGS sono svolte da un unico servizio, il Kerberos Key Distribution Center, che non offre particolari strumenti di configurazione.

Le uniche possibilità offerte all'amministratore ed all'utente per gestire alcuni aspetti del servizio sono date dall'uso di diversi snap-in, dipendenti dal ruolo del sistema:

- Local Security Settings;
- Domain Controller Security Policy;
- Domain Security Policy.

e da alcuni programmi di utilità forniti con il Resource Kit di MS Windows 2000.

Snap-in

Per quanto riguarda l'uso degli snap-in, basterà selezionare la voce 'Account Policies' e quindi 'Kerberos Policy' per visualizzare la lista degli attributi gestibili:

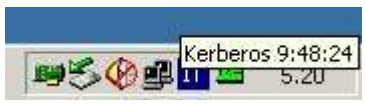
Doppio clic sulla voce da modificare per ottenere la relativa finestra di configurazione.

Resource Kit

Il Resource Kit di MS Windows 2000 ci offre due programmi di utilità dedicati:

- **Kerbtray**: è uno strumento dotato di interfaccia grafica dedicato ai sistemi Microsoft che utilizzano la versione V5 del Kerberos. Permette la visualizzazione e la cancellazione della cache dei ticket ottenuti dal momento del logon.
  Dopo l'installazione basterà avviare l'eseguibile Kerbtray.exe per ottenere la relativa icona all'interno del system tray:

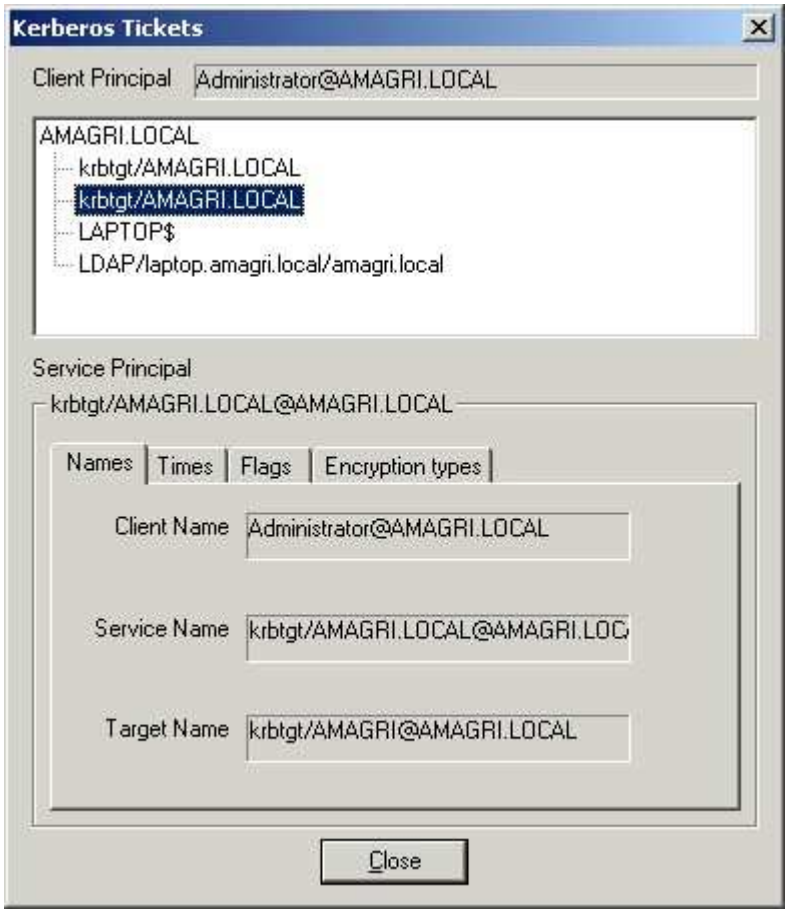
Posizionandosi al di sopra dell'icona con il mouse si otterrà la visualizzazione del tempo rimasto all'ultimo TGT prima della scadenza:



L'icona cambia aspetto nell'ultima ora di validità.

Cliccando sull'icona con il tasto destro del mouse verrà visualizzato il relativo menu con le opzioni a nostra disposizione:

La selezione della prima voce di menu, 'List Tickets', visualizza una finestra contenente informazioni circa i ticket presenti nel sistema:



L'operazione è equivalente ad un doppio clic sull'icona nel system tray. In particolare, la finestra visualizzata è suddivisa in diverse aree:

- **Parte superiore della finestra (Client principal)**: visualizza il nome del principal Kerberos associato con l'account Windows.
- **Lista a scorrimento**: contiene una lista dei domini e dei ticket per i servizi utilizzati dal logon. Selezionando un elemento ne verranno visualizzate le caratteristiche nelle altre due sezioni della finestra.
- **Sezione di mezzo (Service Principal)**: visualizza il service principal per il ticket selezionato nella lista a scorrimento.
- **Parte inferiore**: contiene un insieme di proprietà (nomi, orari, opzioni e tipi di cifratura) che descrivono gli attributi del ticket, non scaduto, selezionato nella lista a scorrimento.

Selezionando invece l'opzione 'Purge Tickets' si otterrà la cancellazione di tutti i ticket presenti all'interno della cache.

Fare particolare attenzione nel selezionare questa voce perchè una volta effettuata l'operazione vi potrebbero essere dei problemi di autenticazione verso alcuni servizi di rete. In questo caso, occorrerà effettuare nuovamente il logon.

- **Klist**: programma a linea di comando in grado di visualizzare ed eliminare i ticket associati alla sessione corrente.