Kerberos Example with simulated keys for demonstration purposes

note excel / coding limitations in this simple model, i.e. string decrypt limits
Kerberos sends two messages in most interactions, represented here as one flow of data.

Client Alice wants to use service provider Bob, and they initially have no trust in each other

Date	T	IP Alice
21/11/2014	22/11/2014	**1.2.3.4**

Alice = Client

1

Kas	**6/T+PijS**
username	alice@xyz
password	fdqwedf

2 Hi I am alice@xyz, may I have a TGT?

3 **KDC**

KDC@kerberos.ker

Kkdc	**j2BxMfo7**
Kas	**6/T+PijS**
Sa	**QoMLIEJS**
{TGT}	alice@xyz, 1.2.3.4, KDC@kerberos.ker, QoMLIEJS, 41966
{TGT}Kkdc	♂Ì¯sØäý´¦_Í>2¯#†$↕ RD¿Œ€ekÊæúàskÁ@6– CG·LÁED┤ÖdÀ1◀–‼
	Sa TGT*Kkdc
apply Kas	go±æY!/S =lSÙ♀¼y5¬┐ Ö2¡‹:(ø ÄRhfeYØV¾ðsòÓÅ*. ÓS»ÐvEz └³ v1±Äã

All encoded with Kas

Sa	{TGT}Kkdc
go±æY!/S	=lSÙ♀¼y5¬┐ Ö2¡‹:(ø ÄRhfeYØV¾ðsòÓÅ*. ÓS»ÐvEz └³ v1±Äã

4

Alice decodes message from 3 using Kas to get Sa

Sa	**QoMLIEJS**
{TGT}Kkdc	♂Ì¯sØäý´¦_Í>2¯#†$↕ RD¿Œ€ekÊæúàskÁ@6– CG·LÁED┤ÖdÀ1◀–‼
T =	41967
Alice Authenticator	alice@xyz, 1.2.3.4, 41967
to KDC	{{TGT}Kkdc, {Authenticator}Sa, Bob}
Service Desired	Bob

{TGT}Kkdc	Authenticator*Sa	Service
♂Ì¯sØäý´¦_Í>2¯#†$↕ RD¿Œ€ekÊæúàs	0l¾Ë◘\¸yÑ¯–uR2\ｙ	Bob

* TGT and authenticator are separately encrypted.

5

Decode TGT to get Sa, verify authenticator, generate service ticket

{TGT}	alice@xyz, 1.2.3.4, KDC@kerberos.ker, QoMLIEJS, 41966		
Sa from TGT	**QoMLIEJS**		
Authenticator	alice@xyz, 1.2.3.4, 41967		
Service	Bob		
Authenticator Validated		**Yes**	**NB**
Kbs	**TTPJM2Br**		
Kab	**KC5pIqkb**		
{Service Ticket}	alice@xyz, 1.2.3.4, KC5pIqkb, 41968		
{Service Ticket}Kbs	5l™÷^ÐyÔ~£┼}.az♀┬¾,é2Fcìp¹ÕNzƒ &ž†)ƒ8		

All encrypted with Sa

Bob Role	Kab	Service Ticket
‼oµ	→CâØ$m«b	dlN_q”┼y T┴T .‼0eòo,→²hï˜pA36« o<↑♬8

6

Alice prepares a request to go to Bob

{Service Ticket}Kbs	5l™÷^ÐyÔ~£┼}.az♀┬¾,é2Fcìp¹ÕNzƒ &ž†)ƒ8
Kab	**KC5pIqkb**
T =	41969
Alice Authenticator	alice@xyz, 1.2.3.4, 41969
to Service	{{Service Ticket}Kbs, {Authenticator}Kab}

Alice Role	Service Ticket	{Authenticatc 6->
alice@xyz	5l™÷^ÐyÔ~£┼}.az♀┬¾,é2Fcìp¹ÕNzƒ ¿*l6C◘┘ öy•¾r¡(2ì├à┼☼ S&˜ñ‼9	

Bob =Service Provider

7

Bob, decodes the Service Ticket

{Service Ticket}	alice@xyz, 1.2.3.4, KC5pIqkb, 41968		
Kbs	**TTPJM2Br**		
Kab	**KC5pIqkb**		
Authenticator	alice@xyz, 1.2.3.4, 41969		
Authenticator Validated		**Yes**	**NB**
T + 1	41970		

{T+1}Kab

1f┤]	Bob

8

Alice decodes Bob's reply using Kab

T+1	41970

Success

Alice and Bob have authenicated each other via KDC and are both in possession of Kab