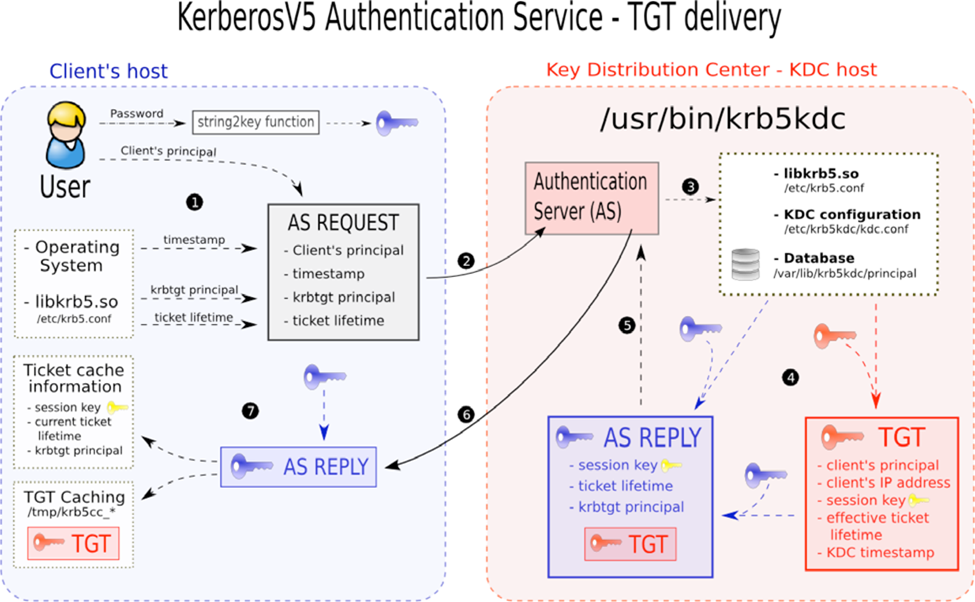
**一．客户端向KDC获取TGT**



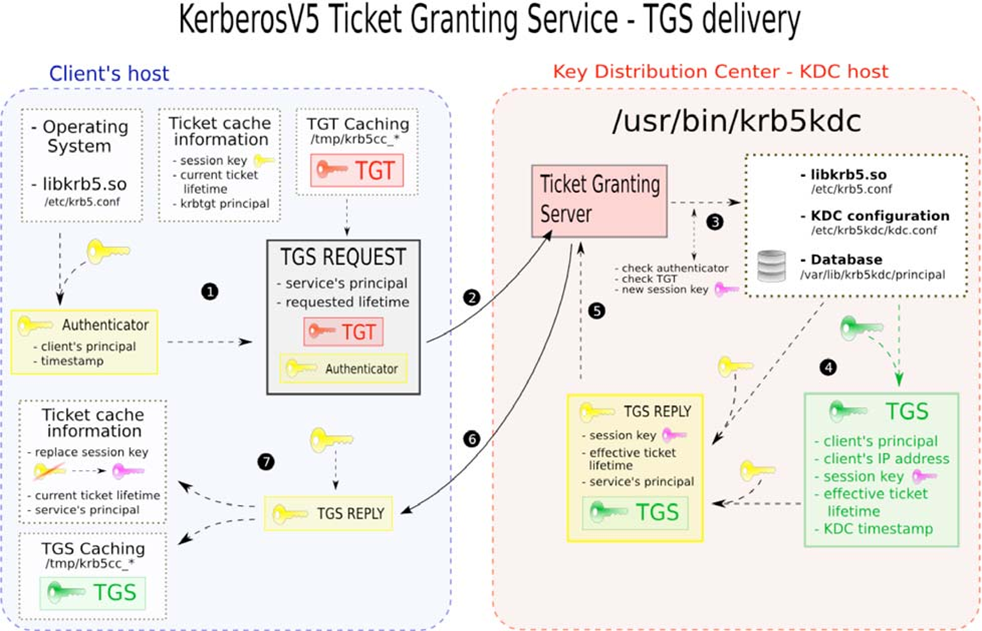
**注：紫色钥匙\*为客户端密码**

**红色钥匙\*为服务器server密码**

**黄色钥匙\*为生成的session key**

1. 获取client principal ,KDC principle(krbtgt principal)， 系统时间戳(timestamp)，ticket存活时间(ticket lifetime)，
2. 发送AS REQUEST(client principal, krbtgt principal,timestamp,ticket lifetime)发送到KDC
3. KDC生成session key\*，查询客户端密码\*
4. 从服务器获取相关信息，生成TGT（client principal，client ip address，session key\*，ticket lifetime,KDC timestamp），使用服务器server密码\*加密
5. 生成应答信息AS reply（session key\*,ticket lifetime,krbtgt principal，TGT），使用客户端密码\*加密
6. 发送结果
7. 客户端使用自己的密码解密应答信息，获取到session key\*,ticket lifetime,krbtgt principal,然后缓存TGT

二．**客户端向KDC获取TGC**



**注：黄色钥匙\*为原来的session key**

**绿色钥匙\*为service的密码**

**粉色钥匙\*为新生成的service session key**

1. 使用上一步的session key\*，加密得到Authenticator(client principal,timestamp)
2. 发送TGS REQUEST（**service principal**,lifetime,TGT,Authenticator）
3. TGS服务器校验Authenticator，TGT，生成新的session key\*
4. 从服务器获取相关信息，并生成TGS(client principle,client ip address, session key,ticket lifetime,KDC timestamp)，使用服务service密码**\***加密
5. 生成应答信息TGS reply(session key\*,ticketlifetime,service principal,TGS)，使用原来的session key\*加密
6. 发送结果
7. 客户端解析TGS reply ,使用新的service session key\*替换原来的session key\*，缓存TGS

参考资料：

1.Kerberos安装教程及使用详解 http://www.jb51.net/article/94875.htm

2.Kerberos认证流程详解 http://blog.csdn.net/jewes/article/details/20792021

3.Kerberos 认证原理笔记 http://blog.csdn.net/scythe666/article/details/53429722

4.安全知识&kerberos初识http://blog.csdn.net/u011239443/article/details/52079874

5.Kerberos 基本安装与配置http://blog.csdn.net/post\_yuan/article/details/54406148

6. kerberos 安装和配置http://blog.csdn.net/tonyhuang\_google\_com/article/details/40861179