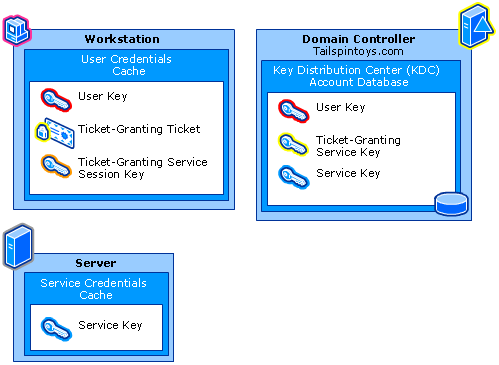
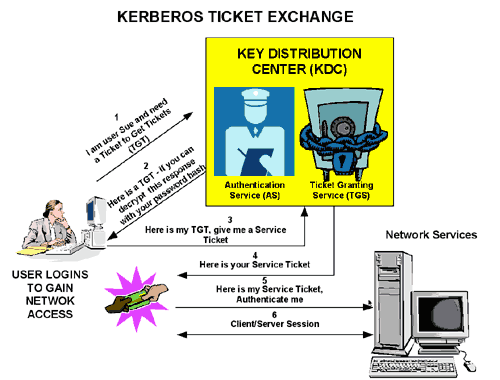
Kerberos简介

Authentication（认证）为了解决某个人确实是他生成的那个人的问题。Kerberos采用客户端/服务器结构与DES加密技术，并且能够相互认证，即客户端和服务器端均可以对对方进行身份认证，其物理结构如下图所示：



Kerberos中有三种角色: KDC 负责分发密钥的密钥分配中；Client 需要使用Kerberos服务的客户端；Server是需要提供具体服务的服务端。下图是Kerberor的连接原理图，如下所示：



过程如下所示：

1. 客户端登录，将用户名发送给KDC中的Authentication Service(AS)，并申请一个TGT，一般情况下KDC是在Domain Controller(DC)上。具体过程如下所示：



其中用户信息，包括用户名、用户地址、服务名、有效期及时间戳

1. DC中不保存用户明文密码，只保存密码的Hash值，AS将TGT用密码的Hash值进行加密，将加密后的TGT传送给客户端。客户端可以使用自己密码的Hash解密得到TGT如果解密错误，将得不到TGT，所以AS的作用是保证客户端的用户不是假冒的。
2. 当客户端申请网络中的服务时，客户端将TGT及要访问的Service Principal Name(SPN)发送给TGS(Ticket Granting Service)，申请用于访问服务的Service Ticket



1. TGS验证是否只有一个服务账号注册过该SPN，将SPN用账户信息进行加密，将后将Service Ticket返回给客户端
2. 客户端将要访问的服务的Service Ticket发送给服务端，如果服务端能够用自己的账户信息正确解密Service Ticket，那么建立连接。TGS的作用是为了保证服务器端不是假冒的，避免用户登录钓鱼网站



1. 服务器端发送session给客户端，表明建立连接



参考文献：

Kerberos原理的对话（雅典娜与Euripides）：

http://blog.sina.com.cn/s/blog\_5189da570100k6av.html

执行流程：

http://www.cnblogs.com/xwdreamer/archive/2012/08/21/2649601.html