国家信息安全水平考试

NATIONAL INFORMATION SECURITY TEST PROGRAM

Kerberos协议

Kerberos简介

在古希腊神话故事中，kerberos是一只具有三颗头颅的地狱恶犬，他守护在地狱之外，能够识别所有经此路过的亡灵，防止活着的入侵者闯入地狱

Kerberos简介

在计算机中，Kerberos是一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。

kerberos协议角色组成

kerberos协议中也存在三个角色，分别是

1、客户端（client）：发送请求的一方

2、服务端（Server）：接收请求的一方

3、密钥分发中心（Key Distribution Center，KDC），而密钥分发中心一般又分为两部分，分别是:

AS（Authentication Server）：认证服务器，专门用来认证客户端的身份并发放客户用于访问 TGS 的 TGT（票据授予票据）

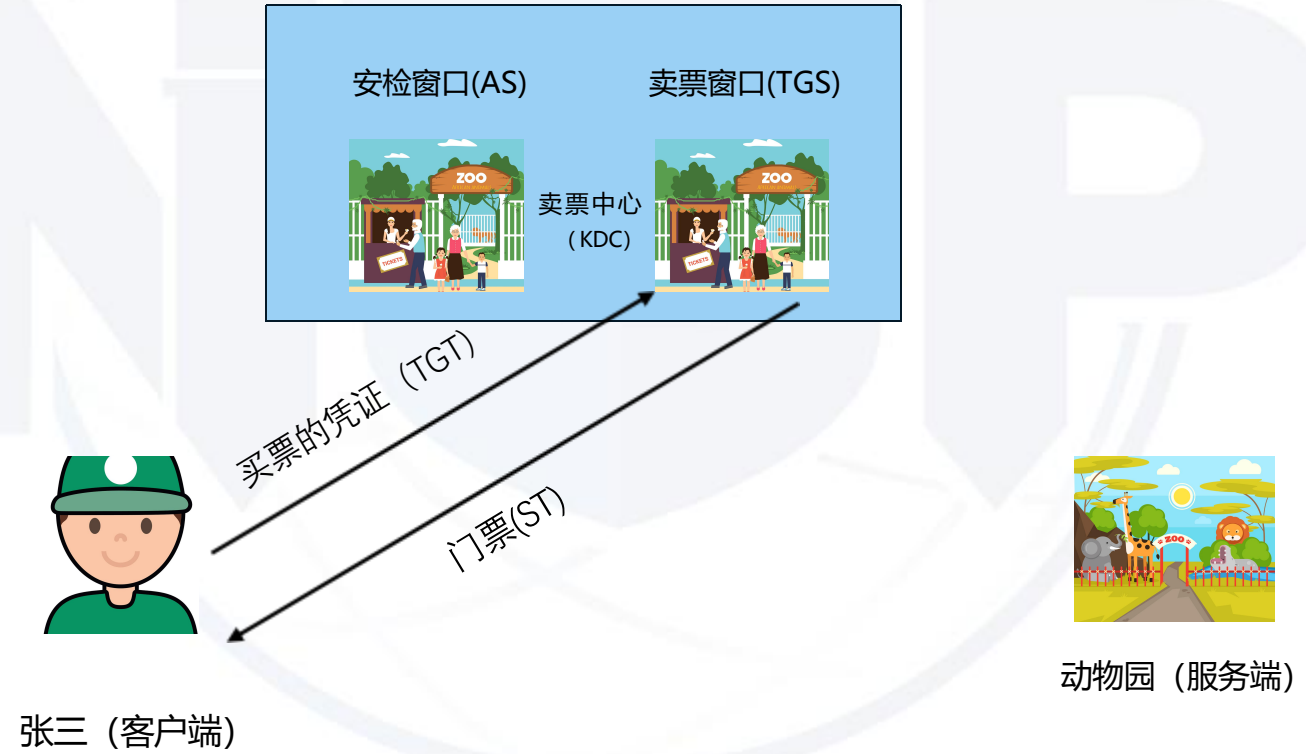
TGS（Ticket Granting Ticket）：票据授予服务器，用来发放整个认证过程以及客户端访问服务端时所需的服务授予票据（Ticket）

kerberos协议认证流程

第一步：客户端拿着身份证去AS认证，认证通过后返回一张去卖票窗口买票的票（TGT）

kerberos协议认证流程

第二步： 客户端拿着TGT去卖票窗口(TGS)买一张去动物园的票



kerberos协议认证流程

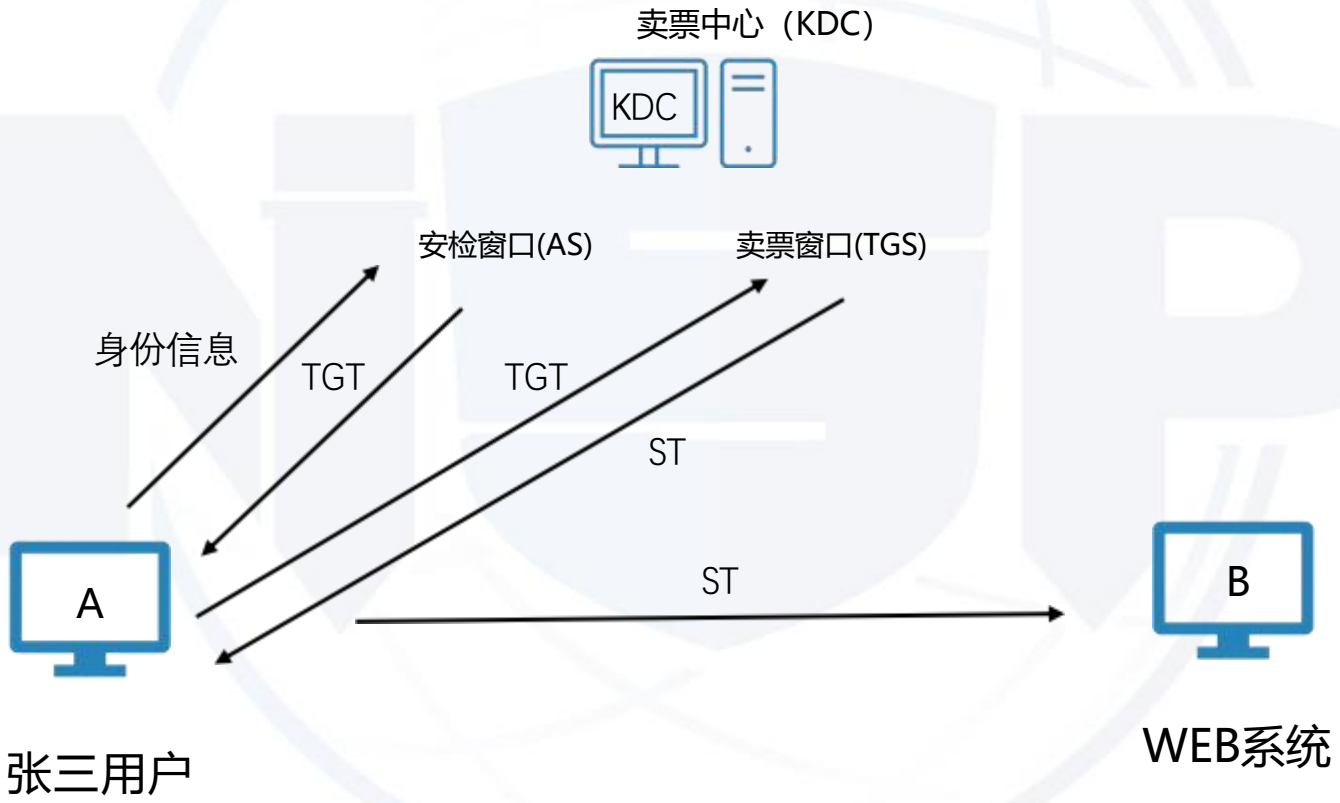
第三步： 客户端拿着ST去动物园

检票(ST)入园

张三（客户端）

动物园（服务端）

kerberos协议认证流程

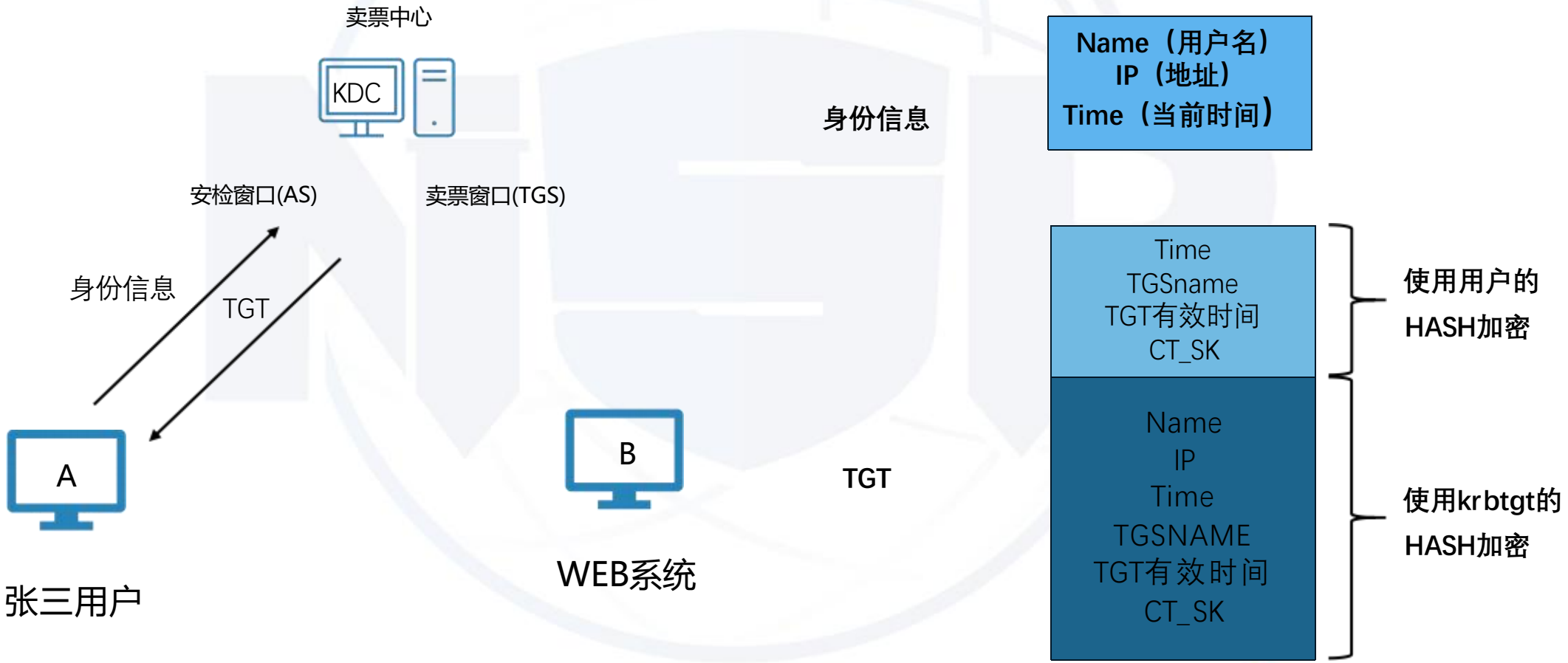


客户端和AS通信原理

第一步：客户端拿着身份证去安检窗口（AS）认证，认证通过后返回一张去卖票窗口买票的票（TGT）

客户端和AS通信原理

第一步：客户端拿着身份证去AS认证，认证通过后返回一张TGT



客户端和AS通信原理

提供身份信息的数据包是AS-REQ(AS-requests)
发送TGT的数据包是AS-REP（AS-response）

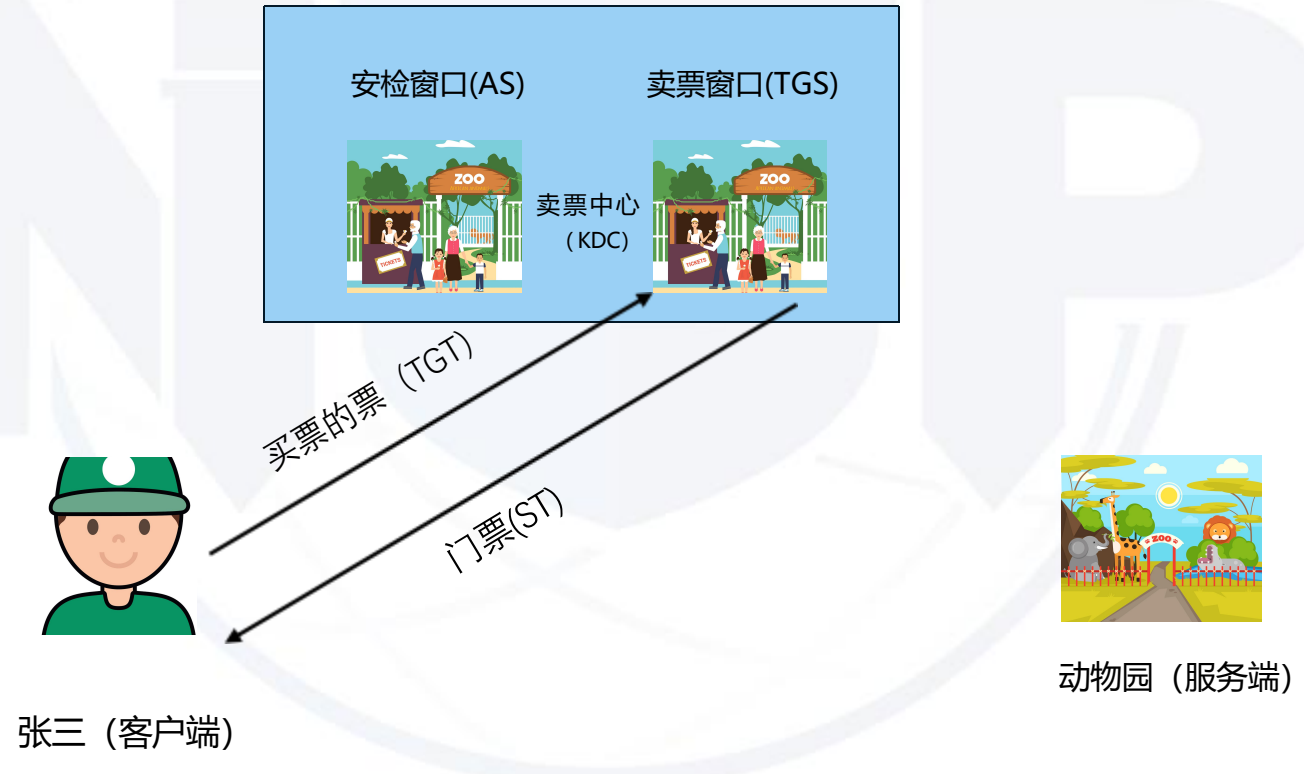
当用户收到TGT时候对TGT进行解密

AS发过来的TGT

用户解密后重新封装的TGT

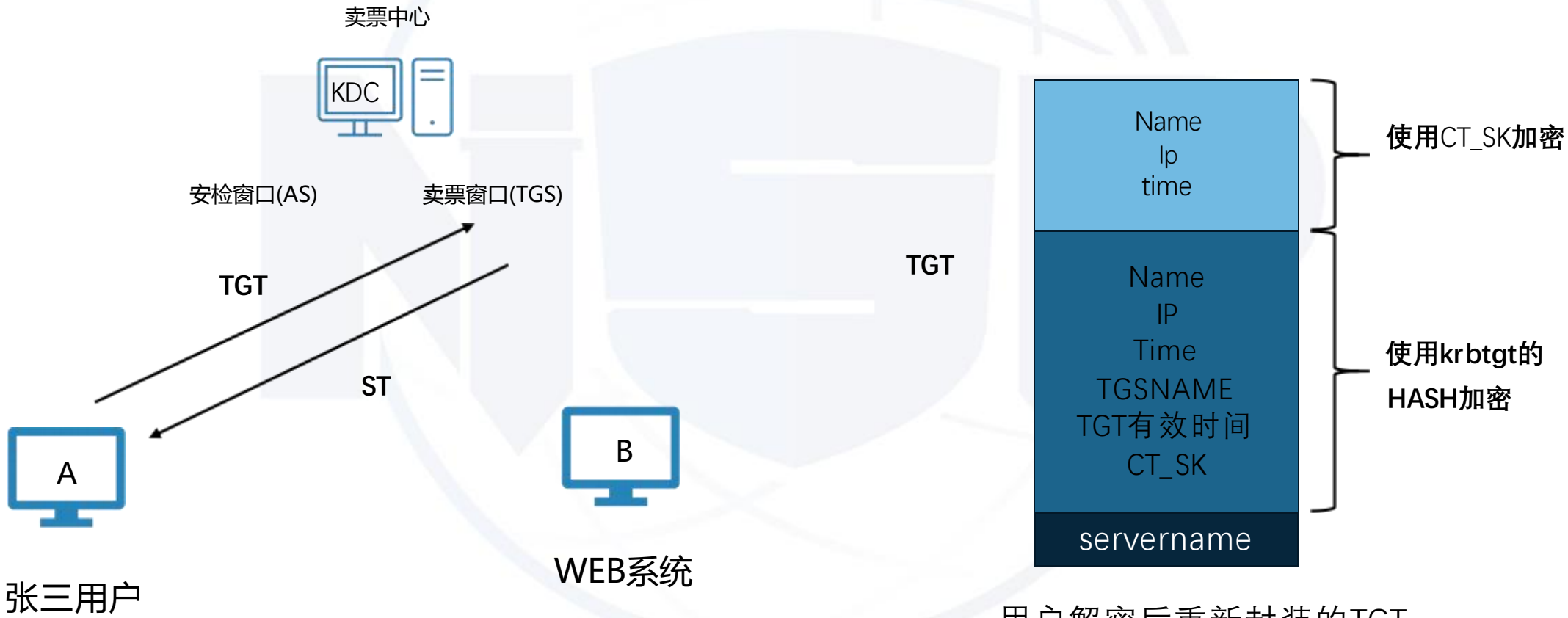
客户端和TGS通信原理

第二步： 客户端拿着TGT去卖票窗口(TGS)买一张去动物园的票



客户端和TGS通信原理

第二步： 客户端拿着TGT去卖票窗口(TGS)买一张去动物园的票



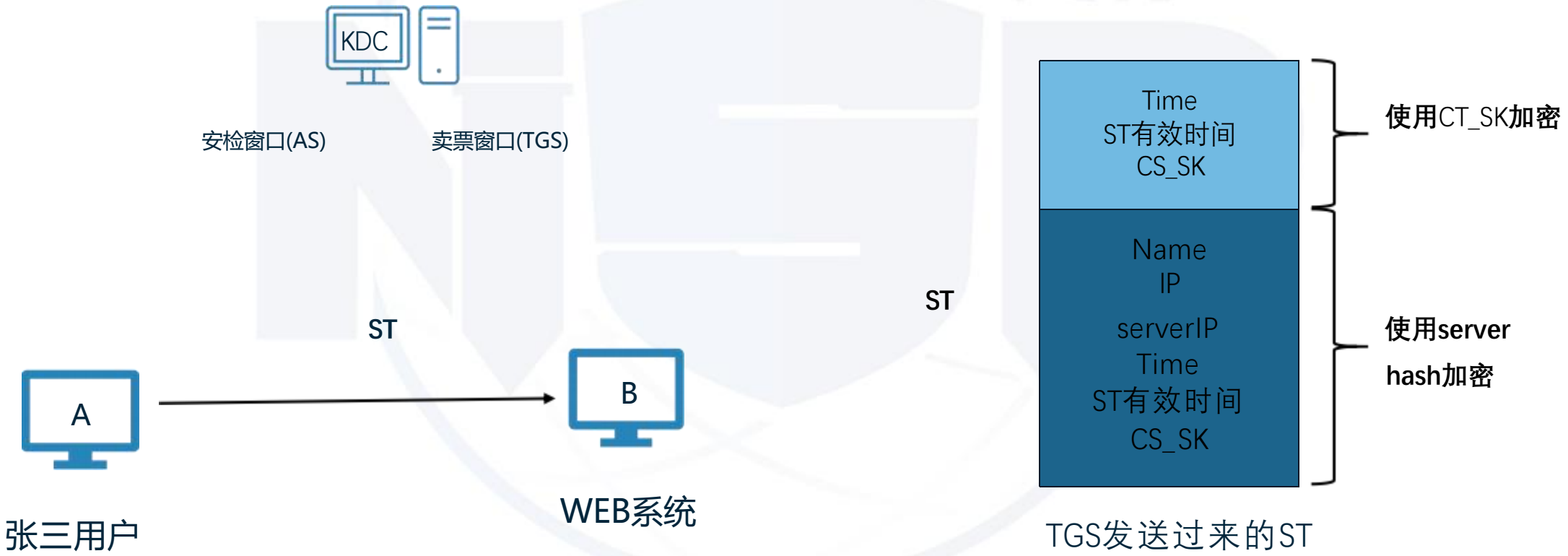
客户端和TGS通信原理

用户解密后重新封装的TGT

TGS封装ST发送给客户端

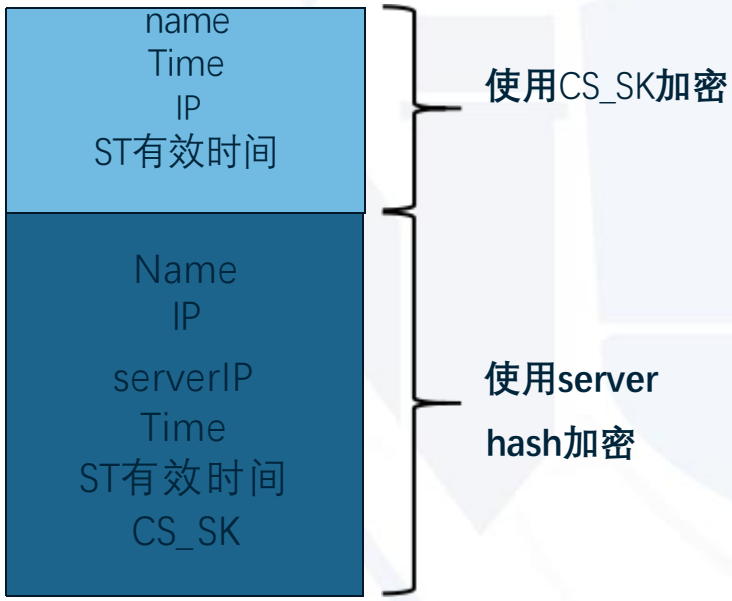
客户端和服务端通信原理

第三步： 客户端拿着ST去动物园



客户端和服务端通信原理

客户端和服务端通信原理



ST

客户端重新封装的ST

1、使用本机的机器用户HASH值解密ST得到 CS_SK
2、拿着CS_SK解密第一部分得到相关信息
3、进行对比后成功访问

国家信息安全水平考试

NATIONAL INFORMATION SECURITY TEST PROGRAM

Thanks