图中George是子域sh.sayms.local的用户，而ServerA位于另一个子域cn.sayms.local内，当George要访问共享文件夹\\ServerA\tools时，George的计算机需要先取得一个用来与ServerA通信的**service ticket**（服务票证）。George的计算机取得service ticket并与ServerA通信成功后，ServerA会发放一个access token给George，以便让George利用这个access token来访问位于ServerA内的资源。以下详细说明其流程（请参照图8-1-2中的数字）：

（1）George利用所属域sh.sayms.local内的用户账户登录。

当George在工作站A登录时，会由其所属域的域控制器DC1来负责验证George的用户名称与密码，同时发放一个Ticket-Granting-Ticket （TGT，索票凭证）给George，以便让George利用TGT来索取一个用来与ServerA通讯的service ticket。用户George登录成功后，开始访问共享文件夹\\ServerA\tools的流程。

附注

可以将TGT视为**通行证**，用户必须拥有TGT后，才可以索取service ticket。

（2）工作站A会向所属域内扮演Key Distribution Center（KDC）角色的域控制器DC1，索取一个用来与服务器ServerA通信的service ticket。

（3）域控制器DC1检查其数据库后，发现ServerA并不在它的域内（sh.sayms.local），因此转向全局编录服务器来查询ServerA是位于哪一个域内。

全局编录服务器根据其AD DS数据库的记录，得知服务器ServerA是位于子域cn.sayms.local内，便将此信息通告域控制器DC1。

（4）域控制器DC1得知ServerA是位于域cn.sayms.local后，它会根据信任路径，通知工作站A去找信任域sayms.local的域控制器DC2。

（5）工作站A向域sayms.local的域控制器DC2查询域cn.sayms.local的域控制器。域控制器DC2通知工作站A去找域控制器DC3。

（6）工作站A向域控制器DC3索取一个能够与ServerA通讯的service ticket。域控制器DC3发放service ticket给工作站A。

（7）工作站A取得service ticket后，它会将service ticket发送给ServerA。ServerA读取service ticket内的用户身份数据后，会根据这些数据来建立access token，然后将access token发送给用户George。

从上面的流程可知，当用户要访问另外一个域内的资源时，系统会根据信任路径，依序跟每一个域内的域控制器交互后，才能够取得access token，并依据access token内的SID数据来决定用户拥有何种权限。