APP 自动登录的实现方案

App 首次登录的流程：

客户端： App 用 RSA 公钥加密（用户名，密码，时间，mac，随机数），发送到服务器。

服务器： 服务器用 RSA 私钥解密并判断以完成登录验证，生成 APP 的 Token 保存本地并下发给客户端 APP。具体如下：

判断时间，如果时间不在有效期（如 1 天到 7 天）之内，则登录失败；

验证用户名和密码，如果验证不通过，则登录失败；

在服务器缓存中存储：key=用户名+mac，value=随机 salt+时间；

AES 加密(随机 salt，用户名，mac，时间)生成 Token 返回给客户端 APP。

客户端：保存服务器返回的 Token。

App 后续自登录流程：

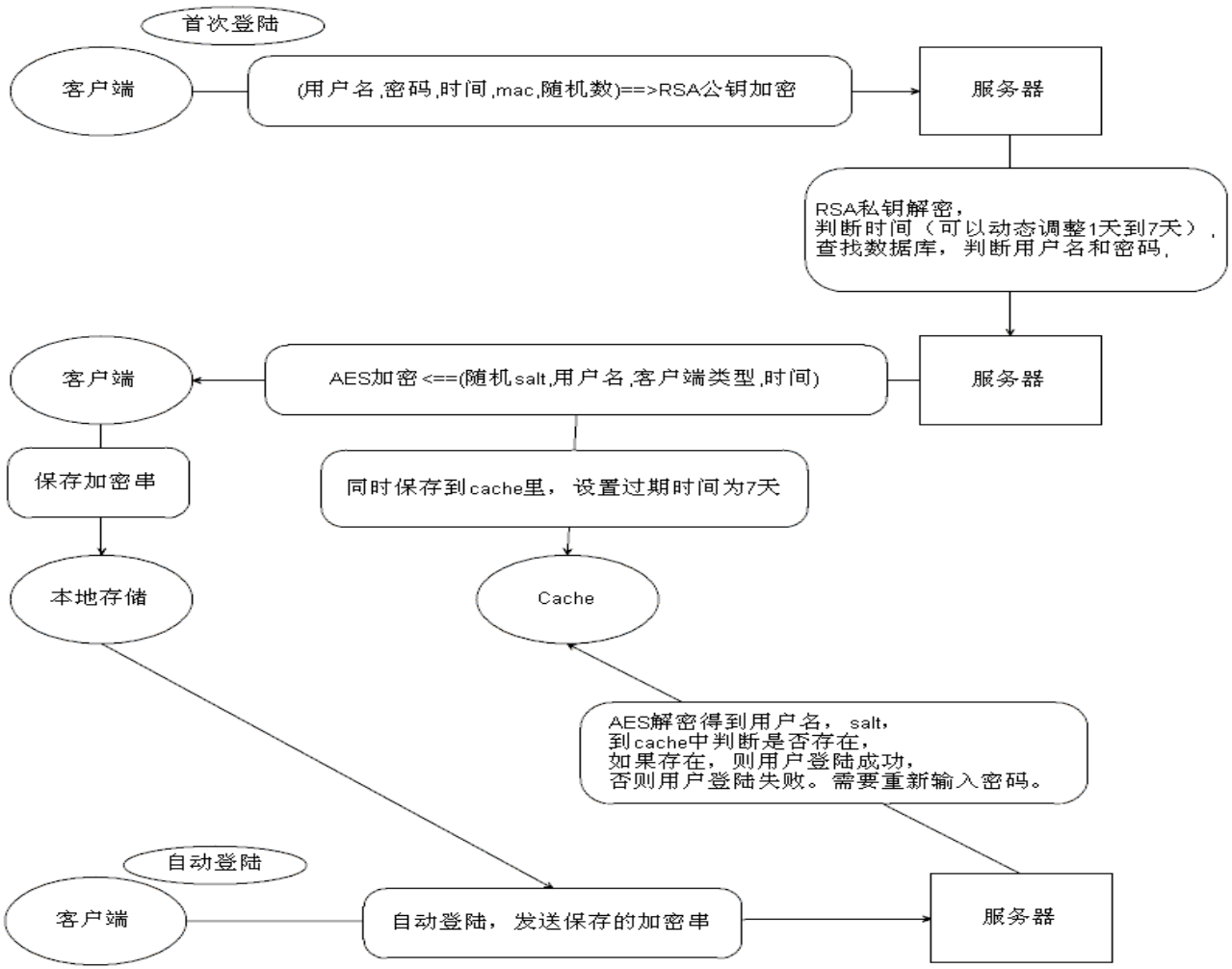
客户端：App 用 RSA 公钥加密（Token，用户名，mac，随机数），发送给服务器。

服务器：服务器用 RSA 私钥解密得到全部的字段，再用 AES 解密 Token 进行信息验证。

判断 Token 中的用户名和 mac 与 Token 外的用户名和 mac 是否一致。如果不一致，则登录失败。

判断时间，如果时间不在有效期（更长时间）之内，则登录失败；

以（用户名+mac）为 key 到缓存里查询，其 value 中 salt 和 Token 中 salt 一致则登录成功，否则登录失败。


首次登陆
客户端
(用户名,密码,时间,mac,随机数)==>RSA公钥加密
服务器
RSA私钥解密，
判断时间（可以动态调整1天到7天），
查找数据库，判断用户名和密码，
客户端
AES加密<==(随机salt,用户名,客户端类型,时间)
服务器
保存加密串
同时保存到cache里，设置过期时间为7天
本地存储
Cache
AES解密得到用户名，salt，
到cache中判断是否存在，
如果存在，则用户登陆成功，
否则用户登陆失败。需要重新输入密码。
自动登陆
客户端
自动登陆，发送保存的加密串
服务器