隐式证书下的椭圆曲线数字签名算法的批认证方法

申请（专利）号：CN202010944227.7

专利名称：OTP生成方法、验证方法、终端、服务器、芯片和介质

专利申请时间：2020.09.10

专利授予时间：2020.12.08

## 摘要

本发明提出一种OTP生成方法、验证方法、终端、服务器、芯片和介质,其中,密码OTP生成方法包括：客户端向安全服务器发起验证请求；所述客户端从所述安全服务器接收第一散列值；其中,所述第一散列值由所述安全服务器使用第一密钥对第一时间戳计算得到,所述第一密钥为所述安全服务器与验证服务端共享的密钥,所述第一时间戳用于指示所述客户端发起所述验证请求的时间；所述客户端使用第二密钥对所述第一散列值进行计算,得到第二散列值；其中,所述第二密钥为所述客户端和所述验证服务端共享的密钥；所述客户端根据所述第二散列值生成待验证OTP。本发明的方法和终端、服务器、芯片和介质使得客户端和验证端都在用户侧的使用环境中,OTP的生成和验证过程都是安全的。

## 可能应用的场景

1. 如图5所示,在--个实施例中,本申请的方法应用于门锁的0TP(--次性密码，0neTimePassword)开锁。手机APP为客户端,门锁为验证服务端,门锁的应用服务端为安全服务器。

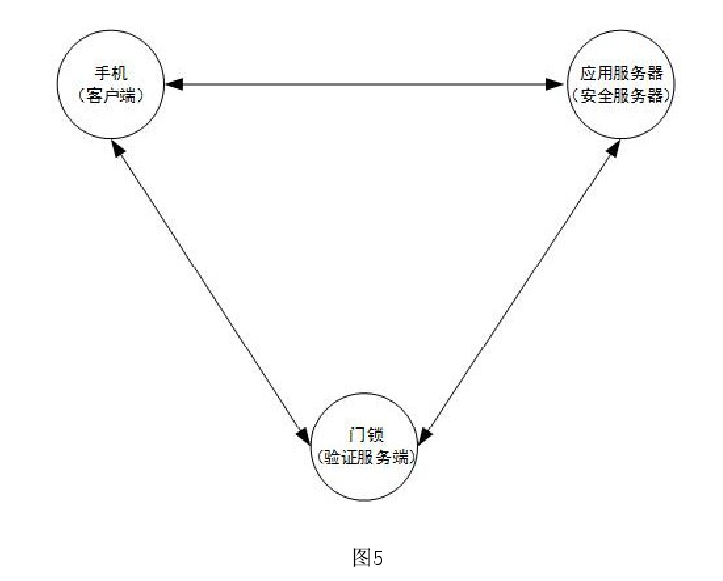
在门锁生产时在门锁的应用服务端(安全服务器)和每个门锁(验证服务端)之间共享一个随机的密钥作为第一密钥K1。在门锁安装时使用用户设置的管理员密码做密钥种子生成第二密钥K2。

安全服务器和验证服务端之间的密钥(第一密钥K1)采用复杂的、安全等级比较高的密钥;验证服务端和客户端之间共享的密钥(第二密钥K2)则采用相对简单的、安全等级相对较低的密钥,例如以用户在客户端中设置的密码作为密钥种子生成的密钥。这样就可以兼顾安全性和使用便利性。第一密钥K1和第二密钥K2互相不受影响。

当用户在手机APP上输入管理员密码生成0OTP(开锁密码)时，手机APP向安全服务器发起请求。安全服务器找到对应门锁,并根据当前时间取整30秒(以30秒为一个时间点)，得到第-一时间戳。安全服务器通过后台的加密机使用第一密钥K1计算出第一密值mac1并返回给手机APP。手机APP使用第二密钥K2计算出第二密值mac2。可选地,手机APP使用第二密值ma.c2的最前面三个字节和最后面三个字节拼成字符串,并做base64编码,得到一个6位的字符串,将其作为待验证0TP。

门锁接收用户输入的待验证0TP后,跟据门锁的当前时间,取整30秒,得到第二时间戳。门锁计算在第二时间窗对应的时间窗口内的每个时间点所对应的比较0TP,计算方法同前述第一密值、第二密值的计算方法。门锁比对用户输入的待验证OTP和多个比较0TP。如果有任何一个比较0TP和用户输入的待验证0TP比对成功，则认为用户输入合法,可以开锁。否则失败,不能开锁。

可选地,门锁接收的待验证0TP也可以由客户端直接发送给验证服务端。比如,远程的屋主可以将在手机端生成的待验证OTP通过无线通讯的方式发送给门锁，然后门锁直接验证完成,为保洁人员开门(无需告知保洁人员生成的待验证0TP,也无需保洁人员输入)。在这种情况下,计算出来的待验证0TP,即便长度很长或者不能打印,也不影响本申请实施例中方法的正常执行。



2. 本申请实施例提出一种用户终端,包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现本申请任--实施例中所述的0TP的生成方法。该用户终端具体可以是手机、平板电脑、个人数字助理(personaldigi talassistant ,PDA)、可穿戴设备等。

可选地,该用户终端包括发送器,发送器通过有线或无线方式向安全服务器发起验证请求,处理器执行其他步骤。