数字证书签名验签原理及在手机端的应用

白双元
（北京科蓝软件系统股份有限公司，太原 030000）

摘要：个人电脑端网上银行处理风险金融交易有一套成熟的UKey数字签名技术，安全性高，如何将个人电脑端网上银行的数字签名技术移植于手机银行，中国金融认证中心（CFCA）推出了基于数字签名技术的云证通解决方案，CFCA云证通采用自主研发的分离式密钥签名算法及金融级安全基础设施，其云服务运营环境安全可靠，确保用户交易安全。

关键词：手机银行；数字签名；中国金融认证中心；云证通
doi：10.3969/J.ISSN.1672-7274.2018.03.125
中图分类号：TN929.53，F83　　**文献标示码：**A　　**文章编码：**1672-7274（2018）03-0164-02

1 引言

近年来，由于电信诈骗的频发，造成了恶劣的社会影响，对广大民众的财产安全造成威胁。2016年9月30日，中国人民银行下发了《关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261号）（简称261号文），从账户管理、银行管理以及转账管理等多个方面来强化管控，加大对电信网络诈骗的大计力度。而电信诈骗之所以猖獗很大程度上因为短信验证码验证交易安全有很多漏斗。需要注意的是在261号文件的第二部分“加强转账管理”之中，明确了银行非柜面转账的具体要求，“除向本人同行账户转账外，银行为个人办理非柜面转账业务，单日累计金额超过5万元的，应当采用数字证书或者电子签名等安全可靠的支付指令验证方式。”数字签名技术（又称公钥数字签名、电子签章）其所发挥的作用与纸上普通的物理签名类似，但是其是利用公钥加密技术领域之中的技术实现的。在一套完整的数字签名之中定义了两种互补的运算，其中一中运算用来签名，另外一种运算用来验证。数字签名技术是国际上公认的一种安全验证方式，这种验证方式在网上银行已经应用多年，而中国金融认证中心（CFCA）“云证通”实现了数字签名技术在手机银行上的应用。

2 数字签名原理

2.1 非对称加密

非对称加密算法需要两个密钥来进行加密和解密，这两个秘钥是公开密钥（public key，简称公钥）和私有密钥（private key，简称私钥）。公钥和私钥是成对出现的，也就说，如果用私钥加密，就用公钥解密，如果用公钥加密，就用私钥解密。如图1所示，B生成一对秘钥给A，A的明文经过B的公钥加密形成密文发送给B，B收到A的密文，用B的私钥加密得到A发给B的明文，如果传输过程中B的公钥和密文被黑客得到也无妨，没有B的私钥，他们无法解析密文。

图1 非对称加密算法

2.2 报文摘要

报文摘要（MD）是一种用于检查报文是否正确的方法。报文摘要指的是用单向哈希函数算法将任意长度的输入报文处理，算出固定输出。这个输出便是报文摘要，由于使用了单向哈希函数算法，这个过程是不可逆的，也就是不能通过摘要反推出报文。消息摘要是用来保证数据完整性的。传输的数据一旦被修改那么计算出的摘要就不同，只要对比两次摘要就可确定数据是否被修改过。

2.3 数字签名验签

数字签名验签技术是对非对称加密技术以及报文摘要技术的综合运用，利用发送者的私钥将报文摘要信息进行加密，并与原文一起发送给接收者。接收者只可以采用发送者所提供的公钥来对所加密的摘要信息进行解密，并利用HASH函数来讲解密得到的摘要信息和所发送过来的原文摘要信息进行对比。如果对比的结果相同，那么就代表了所得到的信息是完整的，在传输的过程之中没有被修改过，否则就代表了信息是被修改过的，因此数字签名可以对信息的完整性进行验证。数字签名是加密的过程，数字签名验签是解密的过程。它可以保证传输信息的完整性，认证发送者的身份等。

2.4 数字证书

数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字证书都有它的有效期。数字证书相当于数字身份证上的一个签名，人们可以用它在网络上识别身份。数字证书都是由证书授权（Certificate Authority）中心发行的。如果通讯的话，通信双方必须信任对方证书，网银的数字证书便储存在Usbkey中。

拥有数字证书的数字签名验签过程如图2所示。

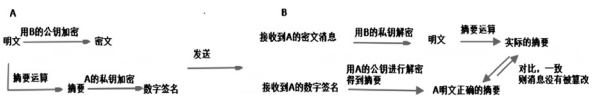

图2 拥有数字证书的数字签名验签过程

首先A与B都信任对方证书，A与B开始通信，A将明文进行摘要运算后得到摘要，再将摘要用A的私钥加密，得到数字签名，将密文和数字签名一块发给B。B收到A的消息后，先将密文用自己的私钥解密，得到明文。将数字签名用A的公钥进行解密后，得到正确的摘要。对明文进行摘要运算，得到实际收到的摘要，将两份摘要进行对比，如果一致，说明消息没有被篡改。这也就是证书签名验签的过程。

3 CFCA基于手机端的签名验签的应用

只要用户在手机上安装“云证通”APP或集成SDK到应用APP，“云证通”APP可以通过云证通平台下发数字证书。数字证书储存在客户的手机中，互联网应用接入云证通平台，无需部署硬件设备。用户使访问互联网服务，将手机作为安全认证载体，进行业务的认证与签名。详细如图3所示。

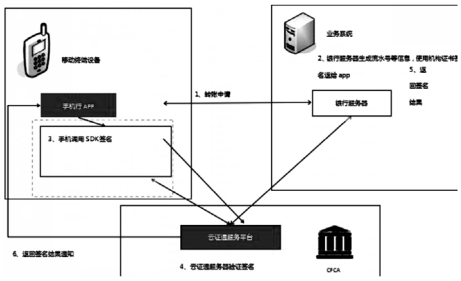

图3 CFCA基于手机端的签名验签的应用 （下转第280页）

在准备阶段对于选择的技术进行反复的实验，一般发现选择的技术并不适用于这个项目工程，马上停止采用这个技术，然后对整个项目进行全面的分析，根据项目的实际情况采用效果最佳的技术。针对投标报价错误的情况，可以采用风险减轻方法来解决，通过合理的手段深入了解竞争对手的基本资料，然后根据项目的实际情况进行最合理的报价。针对招标文件错误的情况，可以采用风险接受的方法解决，提前做好索赔的准备，如果出现签订合同条款不明确的情况，同样可以采用风险接受的方法解决，解决方法也是提前做好索赔的准备。

3.3 机电设备安装施工阶段的风险管理

机电设备安装施工阶段可能出现安装人员专业技能不达标的情况，这时候可以通过减低风险的方式处理这个问题。对安装人员进行专业化的培训，提高安装人员的专业技能水平。针对材料供应不上的情况，可以通过风险转移的方式解决材料供应不上的情况。在签订的合同中明确的规定双方应该承担的责任，将可能发生的损失转移到其它地方。针对采用新材料的情况，可以通过规避风险的方法解决，坚决不使用不熟悉、或者不是常用合作商所提供的材料。

3.4 机电设备安装收尾阶段的风险管理

机电设备安装收尾阶段最有可能出现的风险就是工程达不到验收标准，在这个时候需要及时的制定应急计划，对机电设备安装工程项目存在的问题进行及时的处理。

4 结束语

机电设备安装工程项目在安装过程中的影响因素非常多，因此导致机电设备安装工程项目存在一定的风险性。安装单位应该重视机电设备安装工程项目，明确安装过程中的影响因素，在安装的时候尽可能的消除影响因素，将机电设备安装工程项目出现风险的可能性降到最低，并且对机电设备安装工程项目进行实时的严密监测，及时的识别风险，一旦发生风险能够采取最佳的解决方案，从而将风险造成的损失降到最低，为工作人员的生命安全提供最高的保障。

参考文献

[1] 王群 . 机电安装工程项目施工安全风险管理研究 [J]. 中国建材科技，2017，06（06）：67-68.
[2] 赵小军 . 建筑安装工程项目风险管理分析 [J]. 四川水泥，2017，05（09）：186.

（上接第 164 页）比如客户做一笔转账交易，手机通过手机银行 APP 将转账申请发送至手机银行后台服务，手机银行后台将这笔转账交易详细的交易信息（这笔交易生成流水号等）发送给手机银行，手机银行将信息签名后发送到云证书服务平台进行验签，再将验签结果返回给手机银行后台和手机银行 APP，如果验签成功，说明交易的发起人和交易信息没有被篡改过。确保了交易的安全。

（上接第 199 页）由四个板块构成，分别是推荐版块、空间板块、活动板块和会员板块。推荐版块将最新、最实时的共享空间数据和活动推送给用户。空间板块则全部是由用户发布的可共享空间构成，活动板块则由公司举办的各种活动构成，用户可以随意报名自己想要参加的活动。最后则是会员版块，是一个盈利板块，用户可以购买机遇空间专属的会员来获得会员特权，每一种会员卡的标价都是物超所值，可以放心购买。

其次是社区界面，这款共享空间平台不仅仅是一个外租空间平台，还实现了社交功能。因此我们添加了“机遇星球”功能，这功能和微博推送类似。通过平台认证的用户就可以发送自己的动态到机遇星球中，供其他用户观看，同时还可以在机遇星球中开展自己的活动。与此同时，还添加了群组功能，用户可以自己将志同道合的群体拉入到自己的群组之中，方便开展活动。

之后是用户界面，用户界面有一个特别的功能就是“我的咖啡券”，平台为了推广，采用赠送咖啡券的形式发展用户，每个新用户都可以获得一杯咖啡券。同时用户之间也可以互相赠送咖啡券，凭借咖啡券可以去指定地点兑换一杯咖啡。此外，用户界面还有充值、编辑个人信息等常用功能，这里不再阐述。

4 项目未来的走向

该平台为共享空间平台，而平台未来的走向将不局限于几处共享空间。平台未来将会考虑和更多传统咖啡厅等行业进行合作。实现随处共享、处处共享、时时共享。未来计划将平台扩展到身边的每个地方，只要成为平台的用户，就可以租用在身边绝大多数公共场所进行活动，在进行活动的同时，也可以参与平台的活动，推广平台，获取奖励。此外，甚至可以使用平台货币进行消费，试想在未来的某一天，可以使用平台进行用餐支付、旅店支付，是本平台的终极目标。

参考文献

[1] 杰里米 · 里夫金 . 走向物联网和共享经济 [J]. 企业研究，2015.2.
[2] 篠原聪子，王也，许懋彦 . 共享住宅——摆脱孤立的居住方式 [J]. 城市建筑，2016 第 4 期 .
[3] 麦冬，陈涛，梁宗湾 . 轻量级响应式框架 Vue.js 应用分析 . 信息与电脑（理论版），2017 年 4 月 .

（上接第 268 页）首先，将资源的更新制度固化至系统平台，做到流程闭环管理。

其次，以手机客户端软件为突破口，轻量化资源系统，提高现场人员的使用便利性。

最后可通过下达任务进行存量资源核查，督促普查人员和后台管控人员严格按照规范操作，在确保核查进度和资源数据质量，让传输存量资源做到实时更新，更为准确。

4 结束语

前期的工作，主要任务在于体系的建设，在将来拟从如下方面深化开展工作：

（1）开展网络指标自动测算算法研究：基于平台中的资源大数据按照指标考核要求制定灵活的算法，实时得出指标现状。

（2）资源动态呈现：对现场资源信息可以转化为更为易用的动态图形，便于更好的展示资源整体或某一部分的情况。

参考文献

[1] 李建荣 .ODN 网络哑资源智能管理研究 [J]. 电信工程技术与标准化，2015(4).