基于TPM的设备认证方案*

吕海峰[1] 丁 勇[1] 代洪艳[1] 李新国[2] / [1]桂林电子科技大学 [2]深圳数字电视国家工程实验室股份有限公司

【摘 要】可信平台模块是可信计算的核心，为建立可信终端提供了可信根。身份认证密钥是一个代表可信终端身份的签名密钥。当前，大多数认证协议在验证对方身份时，要求对方对指定数据进行签名，如SSL协议。由于AIK只能对TPM内部产生的信息做签名，无法满足认证协议的要求，本文提出一个基于TPM的设备认证方案，通过引入新的密钥—设备用户密钥，以及基于SKAE extension的设备用户证书，该方案满足了认证协议的要求，能够向挑战者提供可信终端的身份证明。

【关键词】可信平台模块 AIK SKAE EUK EU证书 可信终端

1 引言

要解决计算机终端安全，就要从硬件和底层软件抓起，从源头上保证系统的安全。由此就出现了可信计算技术，它是一种从终端解决安全问题的总体方案。“可信计算”的概念在世界范围内提出是在1999年由TCG（Trusted Computing Group）组织提出，主要思路是在PC机硬件平台上引入安全芯片架构，通过提供的安全特性来提高终端系统的安全性。而可信平台模块（Trusted Platform Module，TPM）是可信计算的核心。如果想充分利用可信计算平台的安全特性，需要数字证书参与，它是信任传递的基础。TCG设计的核心是TPM结合使用证书完成实体证明。

身份认证密钥（Attestation Identity Key，AIK）证书是可信计算中的关键证书之一。AIK证书由一个可信第三方CA（Certificate Authority）签发。对应的AIK密钥是一个签名密钥，当前的大多数认证协议在验证对方身份时，要求对方对指定数据进行签名，如SSL协议。但是AIK仅仅签名由TPM内部产生的信息，永不签名任何外部信息。因此，无法满足认证协议的要求。

AIK依靠EK得到了身份证明的功能，本文借鉴这个思路，在AIK及AIK证书基础上提出一个基于TPM的设备认证方案。通过引入新的密钥—设备用户密钥（Equipment User Key，EUK），以及基于SKAE（Subject Key Attestation Evidence）extension的设备用户证书（Equipment User，EU），用AIK

* 基金项目：国家“863”项目基金资助项目（2012AA011705），广西自然科学基金(2013GXNSFBB053005)，广西无线宽带通信与信号处理重点实验室开放基金支持。

对EUK签名，从而获得身份证明功能。最后测试了EUK密钥能够用于加密和签名外部数据。该方案满足了认证协议的要求，能够向挑战者提供可信终端的身份证明。

2 预备知识

2.1 TPM架构

TPM是一个含有密码运算部件和存储部件的小型片上系统，由输入和输出、密码协处理器、散列消息认证码HMAC（Hash Message Authentication Code）引擎、密钥发生器、随机数发生器等组件构成，TPM组件构成如图1。TPM通过提供密钥管理和配置管理等特性，提供平台的可靠性认证、用户身份认证和数字签名等功能。

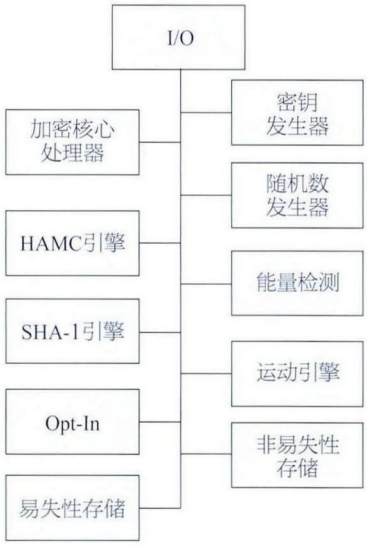


图1 TPM组成结构

2.2 TPM密钥与证书管理

签署密钥（Endorsement Key，EK）由厂商在制造TPM芯片时写入（外界不可读）。它是信任的基础，出于安全和隐私方面的考虑，EK并不直接用于进行数据的加密或签名，只用于生成AIK和获取TPM所有权。

AIK是一个签名密钥，TPM使用AIK来证明自己的身份，凡是经过AIK签名的内容都表明来自TPM的内部。

用户在获取TPM所有权时，TPM创建存储根密钥（Storage RootKey，SRK），并保存在TPM内部。SRK处于密钥管理结构的顶层，除EK外其余密钥都由SRK直接或间接加密存储。TPM密钥管理如图2所示。

SRK和EK存放在TPM内部，其他密钥由SRK父密钥加密存储。密钥的使用和生成都离不开证书。TCG定义了五类证书，每类都被用于为特定操作提供必要的信息。证书的种类包括：

（1）EK证书：一般由厂商签发，包含TPM制造者名、TPM型号、TPM版本号和EK公钥。由于是鉴别TPM身份的唯一证据，所以也是秘密和敏感的，除了生成AIK，其他时候都不应该使用它。

（2）一致性证书：它指出了评估者认可TPM的设计和实现符合评估准则。它由独立的可信机构发布，包含评估者名、平台制造者名、平台型号、平台版本号等。

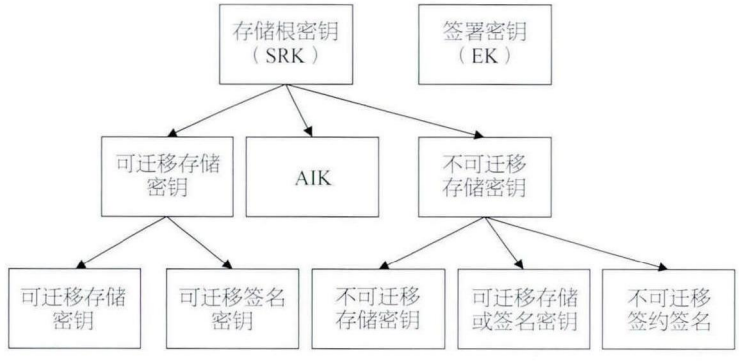


图2 TPM密钥管理

（3）平台证书：它由平台制造者发行，确认平台制造者和描述平台属性。

（4）验证证书：由第三方发的对系统中的某个硬件或软件证书。如微软给某显卡的驱动证书。

（5）AIK证书：被用来鉴定对PCR值进行签名的AIK私钥。AIK证书由一个可信的、能验证各种证书和保护客户端的隐私的服务发表，比如privacy CA 。通过发表AIK证书，签名者证明提供TPM信息的TPM的真实性。

2.3 SKAE extension证书

SKAE extension 规范定义了一个标准机制来表示一个X509 v.3格式的合法证书。该机制由相应的公钥证书表示，允许验证，以确保私钥的使用。而且它在TCG兼容的TPM环境中进行，确保在执行私钥操作环境中严格安全性的验证。SKAE extension可以被用来作为X509 v.3证书，证书请求以及各种认证和授权协议的扩展。

创建一个不可迁移签名密钥的SKAE extension证书过程由两部分组成：

（1）TPM用户创建不可迁移签名密钥以及该密钥的证书请求，发送给设备用户CA。具体过程为：

①TPM创建AIK密钥及AIK证书请求，并发送请求给Privacy CA。

②Privacy CA接收并验证AIK证书请求，验证通过则签发AIK证书并加密发送给TPM。

③TPM创建不可迁移签名密钥，并用AIK密钥签名该密钥。

④TPM创建SKAE extension数据结构，并生成证书请求。

⑤TPM发送证书请求给设备用户CA。

（2）设备用户CA接收到证书请求后，验证请求，通过则签发证书，并发送证书给TPM。

3 基于 TPM 的设备认证方案

在AIK及AIK证书基础上，提出一个基于TPM的设备认证方案。通过引入新的密钥—设备用户密钥EUK，以及基于SKAE extension的设备用户证书EU，用AIK对EUK签名，从而获得身份证明功能。与创建AIK不同的是，privacy CA没有验证AIK的合法性，因此返回的是EK加密的数字信封，借此来验证AIK的合法性。而EUCA验证了AIK对EUK的签名，因此不再需要数字信封了，直接返回的是明文的EU证书。EUK是一个签名密钥，是为TPM内部创建的不可迁移但其他功能不受限制的密钥。它既能代表可信终端的身份，也能满足认证协议的要求，向挑战者提供可信终端的身份证明。图3为TPM创建EUK密钥和EU证书请求过程；图4为EUCA签发EU证书过程。

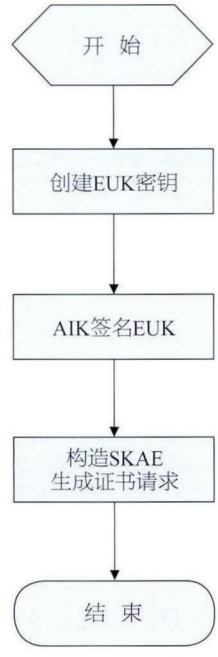


图3 创建EUK及EU证书请求

3.1 创建EUK密钥和EU证书请求

（1）由图3知，TPM创建EUK密钥，载入SRK父密钥，首先调用Tspi_Key_CreateKey()函数，生成EUK，并且SRK加密EUK。接着调用Tspi_Key_LoadKey()把已封装的EUK载入TPM并SRK解密EUK。

（2）TPM调用Tspi_Key_CertifyKey()完成

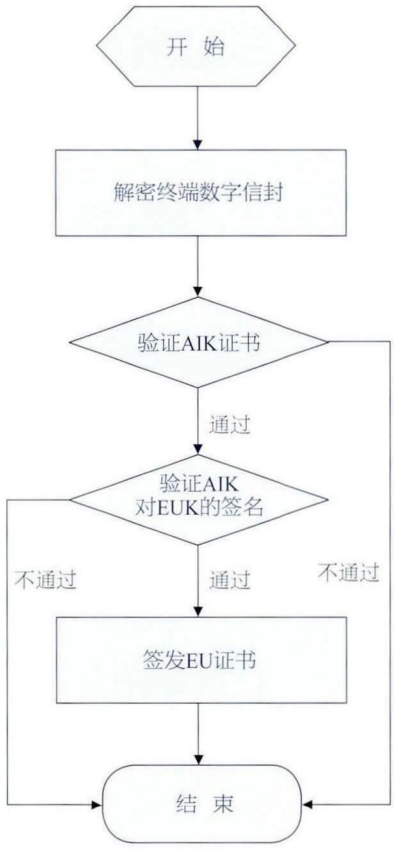


图4 签发EU证书

AIK密钥签名EUK，得到一个TPM_CERTIFY_INFO结构信息以及这个结构的签名{CertifyInfo, CertifyInfosignature }。其中CertifyInfo结构信息还包含了EUK公钥摘要值pubkeyDigest。

（3）构造SKAE extension数据结构，定义的SKAE结构信息包括：

{TPM_VERSION; CertifyInfoLen; CertifyInfo; CertifyInfosignatureLen; CertifyInfosignature; aikCredLen; aikCredLen; }

（4）生成EU证书请求并加密发送给EUCA。

①先获取EUK公钥以及建立X509证书请求。建立的EU证书请求块requestBlob由X509证书请求、euk公钥、skae这三部分构成。

②建立EU证书请求数字信封。TPM利用随机数发生器生成随机数即对称密钥K1，用K1加密EU证书请求块requestBlob；接着TPM用EUCA的公钥加密K1形成数字信封发送给EUCA。

3.2 EUCA签发EU证书

（1）由图4知，EUCA接收到TPM发送的EU证书请求后，解密终端数字信封，获取X509证书请求，EUK公钥以及skae数据结构。

（2）EUCA解析出X509证书请求的EUK公钥，与从requestBlob解析出的EUK公钥比较是否一致。接着计算eukPubkey的摘要，并与skae结构中的skae.pubkeyDigest相比较是否一致。

（3）验证AIK证书。载入Privacy CA根证书，验证AIK证书是否合法。

（4）验证AIK对EUK签名。从skae结构中解析得到AIK证书，并从AIK证书获取AIK公钥，用AIK公钥验证TPM_CERTIFY_INFO结构的签名CertifyInfosignature。

（5）若以上步骤全部验证通过，EUCA则肯定EU证书请求是由TPM可信终端发送，签发EU证书。

4 实验结果分析

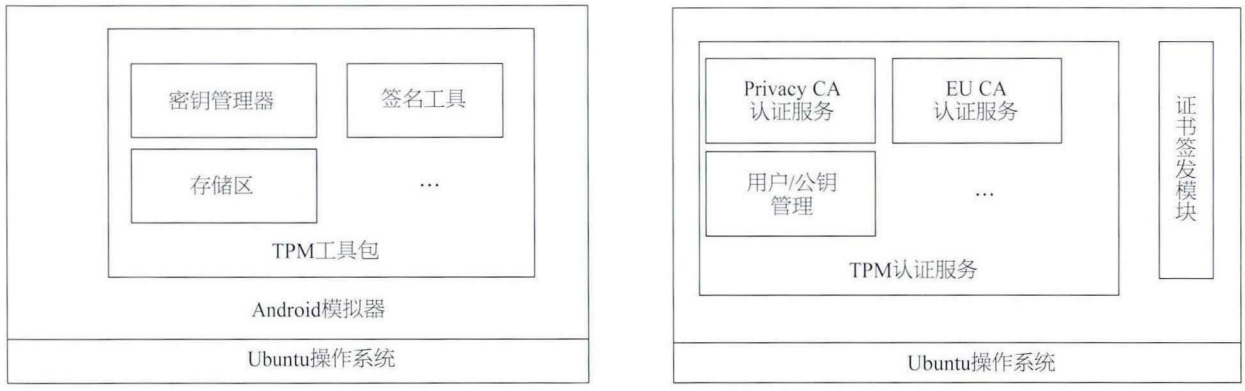
AIK必须配备CA签发的证书，没有证书的AIK不具备身份认证功能。同理，EUK也必须配备CA签发的证书。为了方便搭建实验平台，文中利用Ubutun操作系统以及安装了TPM的Android模拟器为终端，颁发AIK证书及EU证书的CA为前端，模拟实现创建EUK密钥和EU证书，并测试EUK密钥能够加密和签名外部数据。为了终端证书申请的正常工作，需要模拟两个CA的实现，Privacy CA和EUCA。建设Privacy CA，为TPM的AIK密钥颁发证书。建设EUCA，为EUK密钥颁发EU证书。

4.1 系统架构

实验平台采用Android模拟器和TPM可信计算技术相结合，图5展示系统的整体架构。

系统架构说明如下：

（1）实验平台终端采用装载有TPM的Android模拟器，TPM中的密钥管理器模块提供



（a）终端　　（b）前端

图5　系统整体架构

用户密钥的基本操作。签名工具模块帮助进行签名。存储区又分为易失性存储和非易失性存储，后者只要存放EK证书，TPM芯片出厂后不可更改EK证书。

（2）实验平台前端的用户/公钥管理主要负责EU账户注册和更新。Privacy CA认证服务主要验证AIK证书请求，EUCA认证服务主要验证EU证书请求。如果验证通过，签发证书模块负责签发相应的密钥证书。

4.2 实验结果

文中利用搭建的实验平台，模拟实现生成能够代表可信终端身份的EUK密钥和EU证书，如图6。另外用实验平台终端测试EUK密钥实现对外部数据的加密和签名，如图7。

由图6可知，用户首次使用TPM时，需要对TPM进行初始化。初始化过程包括植入EK证书，获取TPM所有权，固化EK证书到TPM芯片的NV存储区，防止修改。接着TPM创建AIK密钥及生成AIK证书请求，并发送证书请求数字信封给服务端的Privacy CA。Privacy CA接收到请求后，验证请求以及验证EK证书。验证通过则用自己的私钥签发AIK证书，并加密发送给TPM。TPM激活并保存AIK和AIK证书。然后TPM又创建EUK密钥，并载

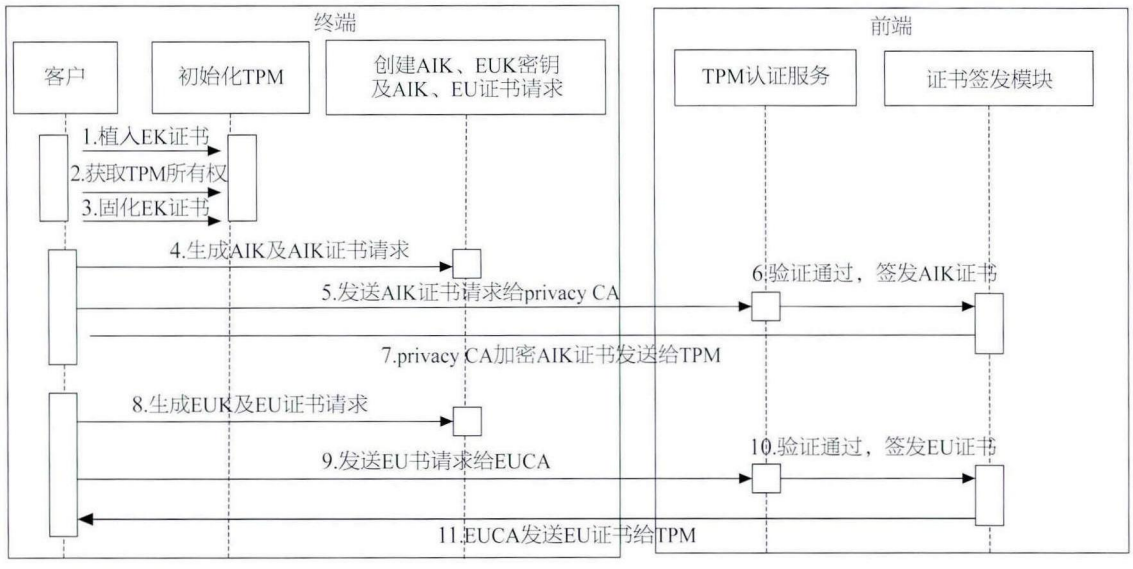


图6　EUK密钥和EU证书生成过程

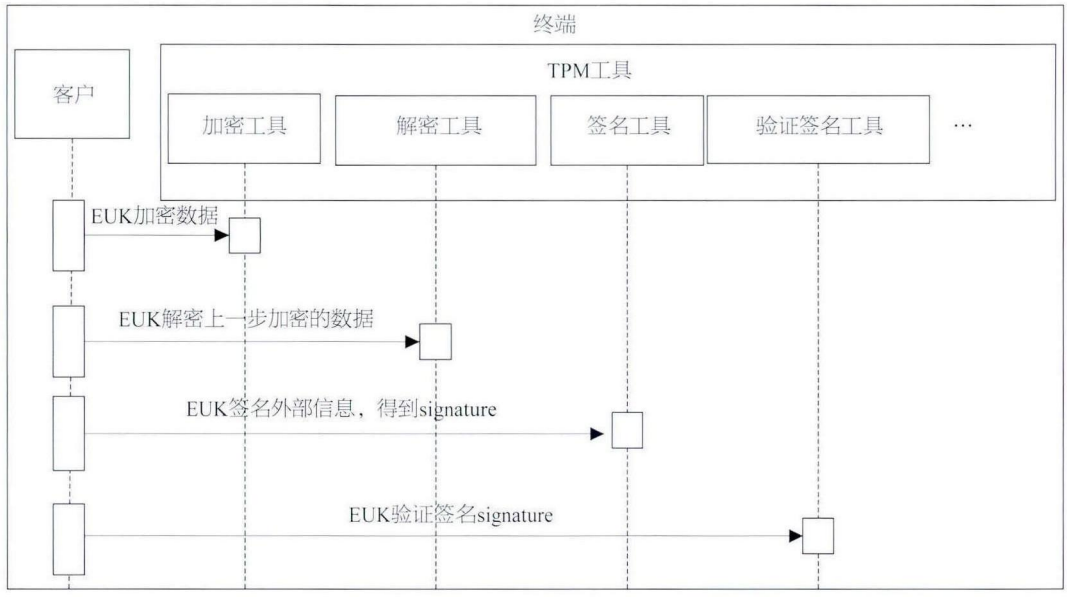


图7　测试EUK加密和签名数据过程实现

入AIK对EUK签名，构造SKAE数据结构，生成EU证书请求数字信封并发送给服务端的EUCA。最后EUCA验证EU证书请求，验证通过则签发EU证书并发送给TPM。图7给出了EUK密钥对外部数据进行加密解密，签名以及验证签名等实现过程。得出结论，生成的EU证书也能够代表合法可信终端身份，对应的密钥EUK，为TPM内部创建的不可迁移但其他功能不受限制的密钥。EUK可签名或加解密外部数据，向外部提供可信终端证明。

通过实验得出结论，EUK密钥是一个签名密钥，它既能代表可信终端的身份，也能满足认证协议的要求，向挑战者提供可信终端的身份证明。证明了本文提出的基于TPM设备认证方案的有效性与可行性，能够防止冒名顶替，运行效率也得到很大提高。

5 结语

本文在AIK及AIK证书基础上，提出一个基于TPM的设备认证方案，通过引入新的密钥—设备用户密钥EUK，以及基于SKAE extension的设备用户证书EU。文中搭建以Ubutun操作系统以及安装了TPM的Android模拟器为终端，颁发AIK证书及EU证书的CA为前端的实验平台，模拟实现创建EUK密钥和EU证书，并成功测试EUK密钥能够加密和签名外部数据。实验结果表明该方案的有效性与可行性，满足了认证协议的要求，能够向挑战者提供可信终端的身份证明。END

参考文献：

[1] 徐贤,龙宇,毛贤平. 基于TPM的强身份认证协议研究[J].计算机工程,2012,38(04):24~27.

[2] 沈为君,赵一鸣,翟耀,等.可信计算中AIK密钥生成改进方案[J].计算机工程,2009,35(10):147~149.

[3] 漆佑军,姚栋,魏占祯,等.可信计算平台AIK证书的生成研究与实现[J].北京电子科技学院学报,2010,18(04):21~24.

[4] 韩春林,叶里莎.基于可信计算平台的认证机制的设计[J].通信技术,2010,43(07):92~97.

[5] 潘雷.TPM中身份证明密钥AIK的研究[J].南京晓庄学院学报,2007,(06):72~74.