第 4 卷◆第 9 期◆版本 1.0◆2023 年
文章类型：论文|刊号（ISSN）：2737-4580(P) / 2737-4599(O)

# 基于物联网的 PKI 系统身份认证模型

徐娟娟
广东科技学院
DOI:10.12238/jpm.v4i9.6252

[摘　要] 在物联网下，基于传统 PKI 系统中身份注册认证模型，认证模型利用签名算法进行身份注册的方法，使得 PKI 系统的用户数据通信安全传输、达到可鉴别性保护和不可否认性保护。结果分析表明，该方法能够较好建立完善的系统认证模型，且在完成身份注册的情况下完成不可篡改性身份认证。
[关键词] 物联网；PKI 系统；身份认证模型；签名算法。

## System Identity Authentication Model Based on Internet of Things PKI System Identity Authentication Model

Xu Juanjuan
Guangdong University of Science and Technology, Guangdong 523668, China
[Abstract] Under the Internet of Things, based on the identity registration authentication model in the traditional PKI system, the authentication model uses the signature algorithm for identity registration, so that the user data communication of PKI system can be transmitted securely, and the authenticity protection and non-repudiation protection can be achieved. The results analysis show that this method can better establish a perfect system authentication model, and complete the tamper-proof identity authentication under the condition of completing identity registration.
[Key words] Internet of Things; PKI system; authentication model; Signature algorithm.

## 1 引言

物联网[1-3]（Internet of Things，IoT）是新一代信息技术的重要组成部分. 它是在互联网基础上进一步延伸和扩展的网络，将各种信息传感设备与网络结合起来而形成的一个巨大网络。能够实现数据的及时分析和处理，一方面领域应用场景广泛，如身份注册认证、安全检测等，另一方面物联网用户隐私、基础网络环境的安全事件频发.物联网安全问题已经成为隐私性保护的要求的关键。

PKI（Public key Infrastructure, PKI）系统是传统的密码认证基础设施[4-8]。PKI 系统模型由 CA（Certificate Authority ,CA）认证中心负责构建一条证书信任链接，通过信任链查找可信 CA 以验证证书，数字证书服务主要包含证书申请、更新、变更、解锁和撤销等相关操作，RA 负责审核用户的数字证书申请[9]，并将用户申请转交给证书颁发机构 CA，但是当用户需用执行大量的安全和下载认证证书时，需要大量的计算操作，且管理成本高，当用户涉及到多个 CA 的时候,不同 CA 之间的无法验证的问题又使得用户操作变得十分繁琐[10],存在多 CA 互信难过程复杂的问题。有必要在物联网环境下去实现批量跨域身份认证。实现批量 PKI 体系批量用户双向实体认证，完成安全通信，抵抗中间人、第三方等多类攻击[11]。

## 2 PKI 系统身份认证模型

物联网中的 PKI 系统身份认证模型由大量的 PKI 密码体系构建[12-15]，执行大量用户 user 获取合法资源申请的操作，同时服务器 server 认证申请用户，为合法用户提供资源，实现安全合法的资源共享通信模型，并解决了跨域用户身份认证问题。构建一个稳定、健壮、安全、简洁的身份认证模型，如图 1 所示。

CA 是 PKI 系统中的认证中心， user 和 server 都属于证书环境用户。PKI 系统身份认证模型由设置系统公共参数、密钥生成、生成临时身份签名和验证签名 4 个部分在模型中实现身份认证构建安全可靠的交互链接。

设置系统公共参数：输入安全参数 k，由 CA 计算生成系统公钥 P、主密钥 S，输出系统公共参数 param。“||”为链接符号。

密钥生成：PKI 环境中的用户向 CA 提交自己的身份 $ID_U$，临时身份进行哈希计算 $TID_U = H(ID_U||r_U P)$，其中 $r_U$ 为随机数，P 为设置参数，CA 为申请用户进行注册认证并为合法用户颁发证书，用户设置私钥，计算对应的公钥，公钥与 CA 颁发的证书进行绑定，用户公钥为 $P_U$、服务器 server 的公钥为 $P_S$，私钥分别为 $SK_U$、$SK_S$，密钥对为 $(P_U, SK_U)$、$(P_S, SK_S)$，证书分别为

$Gert_U$ 、 $Gert_S$ 。

生成临时身份签名：CA 生成签名信息，输入消息为 M，执行签名 $\delta_U = SK_U H(TID_U \| T_U)$，其中 $T_U$ 为时间戳，输出签名 σ．CA 发送签名信息给系统用户。

验证签名：系统用户根据收到的签名和获取的证书，验证 σ 的正确性来判断证书的合法性和时间戳 $T_U$ 的有效性。

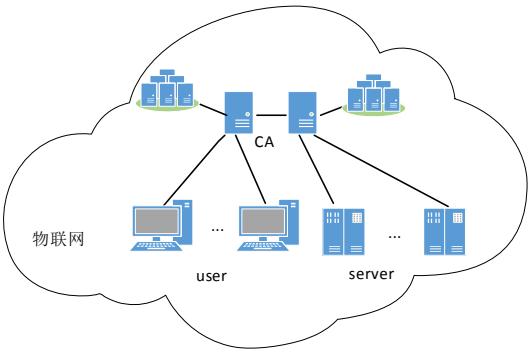


图 1　PKI 系统身份认证模型

Figure1 PKI System Identity Authentication Model

## 3 PKI 系统身份认证过程

（1）跨域认证协议

①CA 证书的合法性，验证证书是否在规定有效期内；②发行方 CA 是否可靠，验证跨域签名算法是否通过，比如验证公钥和证书发行者签名是否正确，；③进行签名和验证签名得到的身份信息是否前后一致，包括临时身份、时间戳、和秘密值等；④认证时间是否在有效时间戳里面。只有以上验证均通过才跨域身份验证通过。

（2）系统身份跨域认证

User 用户向 server 服务器发出申请进行通信，选取一个秘密值 $\partial$，并对临时身份 $TID_U$ 进行签名获取值 $A = \partial TID_U$，发送申请消息至跨域系统 server 服务器 $(A, TID_U, apply)_{P_S}$，接收方服务器收到申请消息，利用自身的私钥对消息进行解密并查看是否是 $apply$，再查看自身数据库的信息身份保存列表中是否存在临时身份 $TID_U$ ，存在则说明是之前注册申请通过用户，直接提供资源访问，如果不存在责需要身份认证，server 服务器发送消息至本地域认证中心 CA，CA 计算签名消息 $AP = PTID_U$ 的值是否成立，成立，则返回 server 的值为 true，认证通过，服务器保存申请数据到列表中，若为 false 为认证不通过，以上均为认证通过，服务器才提供资源。

服务器响应消息至跨域用户，先选取随机数 $\ell$，计算签名消息 $B = \ell TID_S$，向用户提供响应消息 $(B, TID_S, respond)_{P_U}$，用户利用自身私钥解密消息，并检查 $TID_S$ 是否注册过，注册过则直接接收响应，无注册则向本地域认证中心发送认证信息，CA 验证 $BP = PTID_S$ 前后是否一致，一致向用户返回 true，反之为 false，以上消息认证通过则用户接收资源服务。

## 4 身份认证安全性能分析

模型安全性：本模型适用与大量的 PKI 体系用户，模型系统用户通过利用证书和签名进行本地用户注册和认证，认证证书和用户身份进行绑定保证认证的可靠性，采用签名完成证书的认证，保证本地身份的认证安全，使得一些常见的身份攻击变得不再可行，模型框架实现健壮性、安全性注册。

认证安全性：系统模型的建立构造一个完成的认证过程，利用签名算法完成跨域身份认证，保证用户身份信息的合法性、真实性、安全性，抵抗重放攻击、替换攻击和中间人攻击。实现安全双向的实体认证。

效率分析：通过模拟实验结果，分析协议的计算开销，并与文献［16、17］比较。进行效率对比结果见表 1，单位为运算次数，表中记录分步次数合计值。

表 1　计算对比表

Table1 Calculation Comparison Table

| 方案 | 公钥加解密次数 | 签名和验证次数 |
|---|---|---|
| 本方案 | 2 | 2 |
| 文献[16] | 6 | 6 |
| 文献[17] | 12 | 8 |

## 5 总结

物联网的广泛发展，大大提高了我们的生活质量和生产效率的同时，也增加了我们生活中各项安全风险，将物联网与 PKI 系统有效结合实现身份认证，不仅能够实现双向实体认证，完成跨域认证，降低跨域身份认证成本。认证身份模型为信息安全通信提供了可靠信道，提高物联网内网身份认证安全，通信安全，提高认证效率。

## [参考文献]

[1]秦体红汪宗斌张宇刘洋.物联网 PKI 技术研究[J].信息安全研究，2022，8(12):1156-1162.

[2]金杰.物联网通信和区块链技术的结合点及应用研究[J]. 数字通信世界，2018，No.161(05)：86.DOI:NKI:SUN:SZTJ.0.2018-05-149.

[3]BaekJ, Kim M, LeeJ. Study on security architecture and public key infrastructure for ITS [J]. Communications of the Korean Institute of Information Scientists& Engineers,2017, 35 (1):32-36.

[4]DieterUckelmann,MarkHarrison,FlorianMichahelles, 等．物联网架构:物联网技术与社会影响[M].科学出版社,2013.

[5]霍灿炘.浅谈区块链技术在物联网中的应用[J].数字化用户，2018. OI:10.3969/j.issn. 009 0843. 018. 6.095.

[6]解剑波.基于 PKI 的网络安全认证信息访问控制方法研究[J].电子世界，2020(19):2.

[7]王诚,郑红,黄建华,等.基于双区块链的 PKI 模型[J].应用科学学报，2022，40(3):11.

[8]黄逸翔,王亚威,陈文轩,等.基于联盟链的 PKI 跨域认证模型[J]. 计算机工程与设计，2021，42(11):9.DOI:10.16208/j.issn1000-7024.2021.11.006.

[9]卢加元.身份认证系统的评价模型[J].电脑知识与技术：

学术版, 2006(7):3.DOI:10.969/j.issn. 009-3044. 006.07.029.

[10]孟博,王潇潇,郑绪睿,等.一种安全的 PKI 与 IBC 之间的双向异构数字签名方案[J].中南民族大学学报：自然科学版, 2021, 40(2):9.

[11]姚瑶,王兴伟.基于跨域认证与密钥协商的协议模型[J].计算机工程, 2012, 38(9):3.DOI:10. 969/j. ssn.1000-3428. 2012.09.004.

[12]李春梅,柴涌,汪小勇.一种基于 PKI 模型在信号系统中进行身份认证的方法[J].铁路通信信号工程技术, 2019, 16(11):5.DOI:CNKI:SUN:TLTX.0.2019-11-017.

[13]时晨.云环境下异构跨域身份认证及控制方案研究[D].桂林电子科技大学,2020.

[14]顾文刚,程朝辉,荆金华,等.基于 PKI 的 Kerberos 跨域认证协议的实现与分析[J].计算机科学, 2001, 28(10):3.DOI:10.3969/j.issn.1002-137X.2001.10.020.

[15]刘小琼,潘进,李国朋.基于无证书的两方跨域认证密钥协商协议[J].计算机应用研究, 2012, 29(2):4.DOI:10.3969/j.issn.1001-3695.2012.02.065.

[16]毕宇.基于区块链智能合约的 PKI-CA 体系设计[J].金融科技时代, 2018, 26(7):3.DOI:10.3969/j. ssn.2095-0799.2018.07.012.

[17]Maurizio Talamo, Franco Arcieri, Andrea Dimitri, etal. Ablockchain based PKI validation system based on rare events management [J].FutureInternet,2020,12 (2):40-48.