DOI:10.13413/j.cnki.jdxblxb.2010.01.030

异构信任域的跨域授权

孟 欣，胡 亮，初剑峰，林海群，刘博超
(吉林大学 计算机科学与技术学院，长春 130012)

摘要： 针对跨IBE(基于身份加密)和PKI(公开密钥基础构架)异构域可信互联，提出一种实现跨域授权的解决方案. 该方案将PKG和CA作为各自域 T_{PKG} 和 T_{CA} 内用户的代理，并把它们注册到对方域内成为特殊用户 $Client_{PKG}$ 和 $Client_{CA}$，借助映射后的 $Client_{PKG}$ 和 $Client_{CA}$ 构成跨异构域信任链，真实、客观地实现了PKI和IBE域内任意用户的跨域授权.

关键词： 基于身份加密(IBE)；公开密钥基础构架(PKI)；异构信任域；跨域授权
中图分类号： TP309.7 **文献标志码：** A **文章编号：** 1671-5489(2010)01-0089-05

The Cross-Domain Authorization of Heterogeneous Trustworthy Domains

MENG Xin, HU Liang, CHU Jian-feng, LIN Hai-qun, LIU Bo-chao
(*College of Computer Science and Technology, Jilin University, Changchun* 130012, *China*)

Abstract: There still exist two problems in the trustworthy interconnection of heterogeneous domains between IBE (Identity Based Encryption) and PKI (Public Key Infrastructure); one is cross-domain authorization, the other is mobile identity. In view of the above mention facts, the authors put forward a solution scheme of the cross-domain authorization among heterogeneous trustworthy domains. In this scheme, PKG (Private Key Generator) is regarded as the agency by its users to register in the PKI domain. Meanwhile CA (Certificate Authority) is regarded as the agency by its users to register in the IBE domain. Therefore, this kind of cross-domain authorization has intact trustworthy links. Finally, conclusion can be drawn that this scheme is fair for users in both PKI domain and IBE domain to cross-domain authorize by analyzing intact trustworthy links.

Key words: identity based encryption (IBE); public key infrastructure (PKI); heterogeneous trustworthy domains; cross-domain authorization

1 引 言

随着信息技术的发展，信息网络开始呈现开放化与私人化并重的特点，因而网络安全问题日益凸显. 除了要实现信息加密外，还必须解决网络间实体的信任问题. 信任是可信任程度的度量，它依赖于所能提供的可信事实. 网络信任体系将域内所有实体通过信任关系相连接，记录其历史表现并维护这种信任关系. 不同网域一般采用异构的信任体系提供安全保障，由于协同需求日益高涨，因此目前异构网域间可信互联和可信管理面临三方面问题亟待解决：(1) 如何保证实体在异构网域互访中真实

收稿日期：2008-12-09.

作者简介：孟 欣(1984—)，男，汉族，硕士研究生，从事网络与信息安全的研究，E-mail: mengxin19840201@hotmail.com.
通讯作者：胡 亮(1968—)，男，汉族，博士，教授，博士生导师，从事网格计算与网络安全的研究，E-mail: hul@mail.jlu.edu.cn.

基金项目：国家自然科学基金(批准号：60873235；60473099)、教育部新世纪优秀人才支持计划项目基金(批准号：NCET-06-0300)和吉林省重点科研项目基金(批准号：20080318).

可信;(2) 如何对合法实体进行适当授权;(3) 如何对实体进行责任认定.

本文针对公开密钥基础构架(PKI)和基于身份加密(IBE)网域,通过架构跨异构域可信互联模型实现跨异构域身份授权,解决了实体在异构网域互访中的可信问题.

RFC2822 协议将 PKI 定义为"由硬件、软件、人、策略和相应处理构成的体系",该体系用于创建、管理、存储、分发和撤销建立在非对称密码算法上的数字证书[1]. PKI 系统在证书管理恰当、使用者私钥保存妥善的情况下,具有较好的身份认证功能[2],但当互联设备数目激增、通信日趋频繁、认证领域越来越庞杂时,PKI 信任域之间的可信互联问题成为 PKI 建设以及电子商务应用建设的瓶颈. 美国审计总署认为 PKI 目前存在 4 个未解决的问题:国家标准、互联互通、资金和管理负担,而且在技术解决上要依赖第三方认证和数据库存储.

IBE 的初衷为简化电子邮件系统中的证书管理[3]. IBE 加密方案的安全性建立在 CDH(Computational Diffie-Hellman)[4]困难问题的一个变形上——WDH(Weil Diffie-Hellman)[5]困难问题. 其核心是使用了超奇异椭圆曲线上的一个双线性映像 Weil pairing[6]. IBE 系统将用户公开的字符串信息(如邮件地址、电话号码、IP 地址等)作为公钥,使用户能够在不交换私钥和公钥的情况下验证其他用户的签名以进行安全通信,并且不需要保存密钥目录及第三方服务.

基于信任服务的 IBE 系统由四部分组成:定时更换的密钥管理机制、统一身份的标识管理机制、集中审计的权限管理机制和域间互联模块的管理机制[7],其结构如图 1 所示. 其中:密钥管理模块主要为系统用户生成对应 ID(用户标识)的私钥,以及完成系统初始化和主密钥定时更换的工作,它是整个系统的核心;标识管理模块对 ID 进行管理,包括用户注册、身份验证、维护及注销等问题;权限管理模块根据域内用户的不同信任程度实现对用户可信任域的划分;域间互联模块解决域间用户可信身份移动和跨域授权问题. 密钥管理模块只信任三角区域内的 3 个模块,它们之间的交互采用紧耦合方式通讯. 同时,密钥管理模块只对权限管理、标识管理和域内互联模块以及它们所信任的用户和服务发放对应于用户身份的私钥.

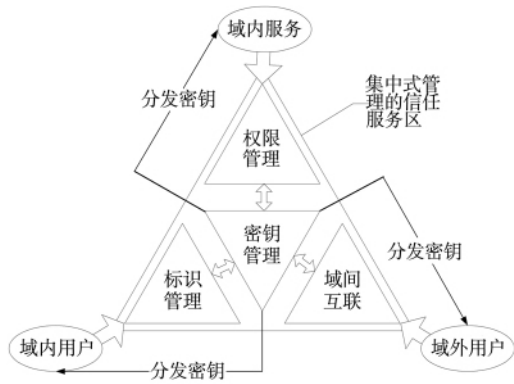

图1 基于信任服务的 IBE 体系结构

Fig. 1 IBE system based on trusted servers

IBE 和 PKI 系统的本质区别在于密钥产生方式:分布式和集中式[8]. PKI 属于分布式密钥产生方式,用户自己产生并保存私钥,公钥由第三方权威机构认证并公布,密钥分发不需要安全信道,交易的安全性由用户自己承担. IBE 属于集中式密钥产生方式,密钥分发通过安全信道(物理信道或秘密信道)实现,交易的安全性由密钥产生中心保证.

PKI 适用于密钥持有者经济利益与密钥安全性相关的电子商务领域(虽然其设计初衷并非为了解决企业之间的安全通信),IBE 更适用于具有严格权限等级、服务及数据报可以定时销毁的电子政务和电子军务领域. 虽然 PKI 和 IBE 在模型上是异构的,但由于二者的互联需求日益增长,所以发展 PKI 和 IBE 的跨异构域可信互联必将成为趋势.

2 异构域间的跨域授权

目前,PKI 已经成为解决网上交易认证成熟的解决方案,基于其部署情况可知,只有依托于 PKI 同构域间的可信互联体系,才能以最小代价实现跨 IBE 与 PKI 异构域的可信互联. 而实现跨异构域可信互联将涉及异构域间的身份移动和跨域授权两部分内容.

2.1 基本概念

定义 2.1 IBE 域:T_{PKG};PKI 域:T_{CA},且 $T_{PKG} \cap T_{CA} = \varnothing$. 若 T_{PKG} 与 T_{CA} 有至少一个公共实体,则设其中一个公共实体为 $\mathrm{Client}_{PKG \cap CA} = T_{PKG} \cap T_{CA}$.

如果交互双方企图通过 $\mathrm{Client}_{\mathrm{PKG}\cap\mathrm{CA}}$传递公钥以建立信任链，则基于信任的单向性以及 $\mathrm{Client}_{\mathrm{PKG}\cap\mathrm{CA}}$在 T_{PKG}和 T_{CA}域内权限等级的差异性等原因，将产生单向信任链不能传递双向信任关系以及在交互过程中权限等级混杂等问题.

定义 2.2　PKG 标识符: N_{PKG}; CA 标识符: N_{CA}; A 标识符: N_{A}; B 标识符: N_{B}.

定义 2.3　设 $\mathrm{Client}_{\mathrm{A}}$ 为域 T_{PKG}内普通用户，则 $\mathrm{Client}_{\mathrm{A}}\in T_{\mathrm{PKG}}$，同理 $\mathrm{Client}_{\mathrm{B}}\in T_{\mathrm{CA}}$; 设 $\mathrm{Client}_{\mathrm{CA}}$为 CA 在 T_{PKG}域内注册形成的虚拟映射用户，则 $\mathrm{Client}_{\mathrm{CA}}\in T_{\mathrm{PKG}}$ 且 $\mathrm{Client}_{\mathrm{CA}}\neq\mathrm{CA}$，同理 $\mathrm{Client}_{\mathrm{PKG}}\in T_{\mathrm{CA}}$ 且 $\mathrm{Client}_{\mathrm{PKG}}\neq\mathrm{PKG}$.

定义 2.4　基于 RSA 算法所产生的 CA 密钥: $\mathrm{pub}_{\mathrm{CA}}$和 $\mathrm{pri}_{\mathrm{CA}}$; CA 颁发给 $\mathrm{Client}_{\mathrm{PKG}}$的数字证书: $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{PKG}}=E(\mathrm{pri}_{\mathrm{CA}},[N_{\mathrm{PKG}}\|\mathrm{pub}_{\mathrm{PKG}}\|\mathrm{Others}])$; PKG 密钥: $\mathrm{pub}_{\mathrm{PKG}}$和 $\mathrm{pri}_{\mathrm{PKG}}$; CA 颁发给 $\mathrm{Client}_{\mathrm{B}}$ 的数字证书: $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}=E(\mathrm{pri}_{\mathrm{CA}},[N_{\mathrm{B}}\|\mathrm{pub}_{\mathrm{B}}\|\mathrm{Others}])$.

定义 2.5　基于 ECC 算法产生的 CA 公钥: $\mathrm{ID}_{\mathrm{CA}}=N_{\mathrm{CA}}@N_{\mathrm{PKG}}.\mathrm{COM}\|\mathrm{Time}\|\mathrm{Others}$; CA 私钥: d_{CA}; A 公钥: $\mathrm{ID}_{\mathrm{A}}=N_{\mathrm{A}}@N_{\mathrm{PKG}}.\mathrm{COM}\|\mathrm{Time}\|\mathrm{Others}$; A 私钥: d_{A}.

定义 2.6　始于 CA 的信任链成功路由到 A: CA 〈PKG〉PKG 〈A〉; 始于 PKG 的信任链成功路由到 B: PKG 〈CA〉CA 〈B〉. A 信任 B: A⇒B; A 和 B 相互信任: A⇔B.

2.2　方案描述

由目前解决 PKI 体系下同构域间可信互联的方案可知，若实体 $X\Rightarrow\mathrm{CA}$，则 $X\Rightarrow\forall\,\mathrm{Client}_{\mathrm{B}}\in T_{\mathrm{CA}}$(为表述方便，假设所有证书均有效); 而在承认 PKG 对由其授权的所有 Client 组成的域 T_{PKG}负责的前提下可知，如果 $X\Rightarrow\mathrm{PKG}$，则 $X\Rightarrow\forall\,\mathrm{Client}_{\mathrm{A}}\in T_{\mathrm{PKG}}$(只要 $\mathrm{Client}_{\mathrm{A}}$ 的身份 ID_{A} 有效). 所以，若将 PKG 作为一个特殊实体注册到 T_{CA}域中成为其客户即完成了跨域映射($\mathrm{Client}_{\mathrm{PKG}}\in T_{\mathrm{CA}}$)，于是，($\forall\,\mathrm{Client}_{\mathrm{B}}\in T_{\mathrm{CA}}$)⇒$\mathrm{Client}_{\mathrm{PKG}}$，即($\forall\,\mathrm{Client}_{\mathrm{B}}\in T_{\mathrm{CA}}$)⇒($\forall\,\mathrm{Client}_{\mathrm{A}}\in T_{\mathrm{PKG}}$). 同理可知将 CA 映射到 T_{PKG} 中的情况，即($\forall\,\mathrm{Client}_{\mathrm{A}}\in T_{\mathrm{PKG}}$)⇒($\forall\,\mathrm{Client}_{\mathrm{B}}\in T_{\mathrm{CA}}$). 所以，将 PKG 映射到 T_{CA}域中成为 $\mathrm{Client}_{\mathrm{PKG}}$，同时将 CA 映射到 T_{PKG}中成为 $\mathrm{Client}_{\mathrm{CA}}$，即可借助互相在对方域内的 $\mathrm{Client}_{\mathrm{PKG}}$和 $\mathrm{Client}_{\mathrm{CA}}$形成信任传递的桥梁，以实现跨异构 PKI 和 IBE 域内任意用户的可信互联($\forall\,\mathrm{Client}_{\mathrm{A}}\in T_{\mathrm{PKG}}$)⇔($\forall\,\mathrm{Client}_{\mathrm{B}}\in T_{\mathrm{CA}}$).

信任是单向且不可度量的，而可信互联要求交互双方平等互信，又由于 PKG 与 CA 的异构性和不对称性，因此只有对 $\mathrm{Client}_{\mathrm{A}}\Rightarrow\mathrm{Client}_{\mathrm{B}}$ 和 $\mathrm{Client}_{\mathrm{B}}\Rightarrow\mathrm{Client}_{\mathrm{A}}$ 分别讨论才能最终实现 $\mathrm{Client}_{\mathrm{A}}\Leftrightarrow\mathrm{Client}_{\mathrm{B}}$.

(1) 讨论 PKG 能否接受 T_{CA}域内 $\mathrm{Client}_{\mathrm{B}}$ 的跨域授权请求，即讨论 $\mathrm{Client}_{\mathrm{A}}\Rightarrow\mathrm{Client}_{\mathrm{B}}$ 是否为真.

在确定路径 PKG 〈CA〉CA 〈B〉完整存在的前提下，如果 $\mathrm{Client}_{\mathrm{A}}$ 能够验证 $\mathrm{Client}_{\mathrm{B}}$ 的身份(该路径为真)即实现了 $\mathrm{Client}_{\mathrm{B}}$ 在域 T_{PKG}下的跨域授权请求. PKG 接受 $\mathrm{Client}_{\mathrm{A}}$ 关于跨域寻求认证 $\mathrm{Client}_{\mathrm{B}}$ 身份(或服务)的请求后，$\mathrm{Client}_{\mathrm{CA}}$计算 $E(\mathrm{ID}_{\mathrm{CA}},[N_{\mathrm{CA}}\|\mathrm{pub}_{\mathrm{CA}}\|\mathrm{Others}])$ 并发送给 $\mathrm{Client}_{\mathrm{A}}$. $\mathrm{Client}_{\mathrm{A}}$ 收到信息后，利用私钥 d_{A} 计算 $D(d_{\mathrm{A}},[E(\mathrm{ID}_{\mathrm{CA}},[N_{\mathrm{CA}}\|\mathrm{pub}_{\mathrm{CA}}\|\mathrm{Others}])])=N_{\mathrm{CA}}\|\mathrm{pub}_{\mathrm{CA}}\|\mathrm{Others}$，继而绑定了 $\mathrm{pub}_{\mathrm{CA}}$，$N_{\mathrm{CA}}$和一些其他限制条件. $\mathrm{Client}_{\mathrm{A}}$ 使用得到的 $\mathrm{pub}_{\mathrm{CA}}$ 计算 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}$ 获取 $\mathrm{Client}_{\mathrm{B}}$ 的身份和 $\mathrm{pub}_{\mathrm{B}}$，$D(\mathrm{pub}_{\mathrm{CA}},[\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}])=D(\mathrm{pub}_{\mathrm{CA}},[E(\mathrm{pri}_{\mathrm{CA}},[N_{\mathrm{B}}\|\mathrm{pub}_{\mathrm{B}}\|\mathrm{Others}])])=N_{\mathrm{B}}\|\mathrm{pub}_{\mathrm{B}}\|\mathrm{Others}$. 在 $\mathrm{Client}_{\mathrm{A}}$ 获知 $\mathrm{Client}_{\mathrm{B}}$ 的公钥并检测真伪后，开始验证证书 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}$是否有效，例如: 提取 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}$和 ID_{A} 中的限制条件 Others(Others 为有效时限和访问控制策略信息等限制条件，通过设置域内访问控制策略，可以实现跨越不同安全认证体系保障下的网域间授权操作，并可获取针对跨入本地管理域的外来应用控制权)做 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}\cap\mathrm{ID}_{\mathrm{A}}$ 操作，如果各限制项交集均不为空，且时间和当前时间不矛盾、策略和声明策略不矛盾，则判定证书有效，可以进行跨域授权，否则放弃.

(2) 讨论 CA 能否接受 T_{PKG}域内 $\mathrm{Client}_{\mathrm{A}}$ 的跨域授权请求，即讨论 $\mathrm{Client}_{\mathrm{B}}\Rightarrow\mathrm{Client}_{\mathrm{A}}$ 是否为真.

在确定路径 CA 〈PKG〉PKG 〈A〉完整存在的前提下，如果 $\mathrm{Client}_{\mathrm{B}}$ 能够验证 $\mathrm{Client}_{\mathrm{A}}$ 的身份(该路径为真)即实现了 $\mathrm{Client}_{\mathrm{A}}$ 在域 T_{CA} 下的跨域授权请求. 已知 $\mathrm{Client}_{\mathrm{B}}$ 拥有 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}=E(\mathrm{pri}_{\mathrm{CA}},[N_{\mathrm{B}}\|\mathrm{pub}_{\mathrm{B}}\|\mathrm{Others}])$，且已知 $\mathrm{pub}_{\mathrm{CA}}$和 $\mathrm{pub}_{\mathrm{PKG}}$，$\mathrm{Client}_{\mathrm{A}}$ 拥有 $\mathrm{ID}_{\mathrm{A}}=N_{\mathrm{A}}@N_{\mathrm{PKG}}.\mathrm{COM}\|\mathrm{Time}\|\mathrm{Others}$ 和 d_{A}，$\mathrm{Client}_{\mathrm{PKG}}$拥有 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{PKG}}$，$\mathrm{pub}_{\mathrm{PKG}}$和 $\mathrm{pri}_{\mathrm{PKG}}$，并已知 $\mathrm{pub}_{\mathrm{CA}}$和 $\mathrm{pub}_{\mathrm{B}}$，$\mathrm{Client}_{\mathrm{B}}$ 和 $\mathrm{Client}_{\mathrm{PKG}}$都能通过证书撤销列表得知对方证书是否为真和有效. 在 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{PKG}}$和 $\mathrm{Certi}_{\mathrm{CA}\Rightarrow\mathrm{B}}$均为真且有效的前提下，PKG 计算 $E(\mathrm{pub}_{\mathrm{B}},[E(\mathrm{pri}_{\mathrm{PKG}},[N_{\mathrm{A}}\|\mathrm{ID}_{\mathrm{A}}\|\mathrm{Others}])])$ 并发送给 $\mathrm{Client}_{\mathrm{B}}$. 由于 $\mathrm{Client}_{\mathrm{B}}$ 没有处于 T_{PKG}中，故不能凭空确

定 T_{PKG} 关于其域内用户的命名规则，因此，要想获知 $Client_A$ 的身份标识 ID_A，需要 $Client_B$ 先使用 pri_B 对消息解密，再用 pub_{PKG} 确认消息的可靠性及来源，

$$D(pub_{PKG}, [D(pri_B, [E(pub_B [E(pri_{PKG}, [N_A \| ID_A \| Others])])])]) = N_A \| ID_A \| Others.$$

(3) 交互双方跨域授权，即 $Client_A \Leftrightarrow Client_B$ 的全局实现.

$Client_B$ 在 T_{CA} 内注册，所以有 $Client_B \Leftrightarrow CA$，且已知 $Certi_{CA \Rightarrow PKG}$ 为真，则 $CA \Rightarrow Client_{PKG}$，根据信任传递关系传递法则可知有 $Client_B \Rightarrow Client_{PKG}$(但仅考虑局部不一定有 $Client_B \Leftrightarrow Client_{PKG}$，因为 $Client_{PKG} \Leftrightarrow Client_B$ 不一定成立. $Client_{PKG}$ 接受证书 $Certi_{CA \Rightarrow PKG}$ 只能说明 $Client_{PKG}$ 被 CA 认证，但并不代表其信任该 CA，除非该 CA 是 rootCA 并且已经自签名或者 $Client_{PKG}$ 一直向上找到已经自签名的其他 rootCA). 又因为 $Client_{PKG} \Rightarrow Client_A$，所以可以最终得出 $Client_B \Rightarrow Client_A$. 为了在双向认证、平等互信的前提下实现跨域授权，将 CA 注册成为 T_{PKG} 域内的用户 $Client_{CA}$ 就可以实现 $Client_A \Rightarrow Client_B$，所以在全局上实现了 $Client_A \Rightarrow Client_B$. 这样双向注册既保证了 IBE 源于设计上的优点未被妥协，又保证了向 PKI 兼容. 最终，交互双方 $Client_B$ 和 $Client_A$ 与对方在各自域内的代理 $Client_{CA}$ 和 $Client_{PKG}$ 映射建立信任关系，实现了各自的跨域授权请求.

3 可行性

虽然 IBE 基于异于 RSA 算法的 ECC 算法，但利用 RSA 算法为 $Client_{PKG}$ 计算产生 pub_{PKG} 和 pri_{PKG} 是可行的[9]. 由 PKI 属于分布式密钥产生方式，而分布式的私钥由用户自己产生并保存的特点，将“计算产生一对 RSA 密钥”作为 PKG 寻求跨域授权的一个组件是可行的.

交叉证书(CA 证书)的定义：由一个颁发机构 CA 创建并用于验证另一个 CA 公钥的证书[10]. 广义上可以将该定义理解为由两个授权机构互相颁发的证书，因此 $Certi_{CA \Rightarrow PKG} = E(pri_{CA}, [N_{PKG} \| pub_{PKG} \| Others])$ 也可以归入交叉证书的范畴. 根据 X.509V3 相关规范，只需在“证书扩展项”[11]中做出相应修改以便标识(本文仅就证书中的扩展为“Must”还是“Should”提出建议)即可扩展交叉证书的应用范围. 在“密钥和策略信息”扩展项中 “密钥使用”规定对 pub_{PKG} 的适用领域(Mus)，“证书策略”规定针对 PKG 的特殊策略集、限定信息和环境信息(Mus)，“策略映射”规定只允许 T_{CA} 映射到 T_{PKG} 域，以及声明允许的服务或授权映射(Must). 在“证书主体和发行商属性”扩展项中规定传递证书主体为 PKG 以及其他附加信息和说明(Should). 在“证书路径约束”扩展项中 “基本限制”标识该主体为 PKG(Mus)，“策略限制”对证书路径中继承的策略映射进行限制，体现为 $Client_B$ 在验证 $Client_{PKG}$ 交叉证书时可以得知该 PKG 对何种请求予以回应和能够提供何种服务等信息(Must)[12]. 总之，将 CA 体系内的交叉证书扩展为跨异构域的交叉证书可以通过设定一些参数实现，并可以通过设定 Must 和 Should 控制证书的严谨程度.

PKG(或 CA)以权限等同于(或略高于)普通用户 $Client_B$(或 $Client_A$)的身份在 CA(或 PKG)下进行注册，即完成了将 PKG(或 CA)映射为 T_{CA}(或 T_{PKG})中用户的工作. 同属于 T_{PKG} 域内的用户一定具有某些共有属性，则很可能 $\exists Client_{A'}(\neq Client_A) \in T_{PKG}$，也期望进行此交互，因此方案中没有直接将 $Client_A$(或 $Client_B$)映射至 T_{CA}(或 T_{PKG})，而是采用将 PKG(或 CA)作为 $Client_A$(或 $Client_B$)的代理映射到 T_{CA}(或 T_{PKG})与其进行交互的方案. 另外，根据“尽可能减少信任路径上中间人的数目，中间人越少，信任的局部性越高，信任水平越高”的原则，使用 PKG(或 CA)作为双方域内所有用户的代理进行交互是一种折衷且有效的方案.

身份信息在域内和域间存在属性差异，导致用户在不同域中的身份信息和权限信息具有不确定性，只有保证用户的身份权限信息被完整地映射到目的域中，才能客观地实现用户跨异构域授权时身份信息的规范和限定[13]. 使用 PKG(或 CA)作为双方域内所有用户的代理进行交互的方案，可以更加真实、客观地实现用户的身份权限信息在目的域中进行完整的策略映射，以最终实现基于身份的访问控制策略在多域安全应用中的互操作以及多域应用环境下的角色映射.

利用本文中跨 PKI 和 IBE 异构域实现跨域授权的思想，可将其推广为任意其他两种或两种以上异构域间的跨域授权；如果采用桥 CA 代理 PKG 联入 PKI 体系的模型，则可使该模型建立的信任链接长

久有效并且普遍可用；如果期望在互联过程中发生争议时，模型能提供证据并进行裁定，则可在 PKG 和 CA 外加入中立第三方仲裁机构，以对异构域间的可信互联及其后续交换信息操作进行跟踪并取证.

综上所述，本文通过对比 IBE 和 PKI 系统，阐述了 IBE 系统的优点，表明 IBE 系统向已经部署的 PKI 系统兼容是实现跨域授权乃至实现跨异构域可信互联的必然趋势. 在不妥协各自优点的前提下（保持 IBE 和 PKI 的内部优点，采用 PKI 体系同构域域间可信互联方案），提出一种将 PKG（或 CA）作为 Client_A（或 Client_B）的代理映射到 T_{CA}（或 T_{PKG}）与其进行交互以实现跨域授权的方案，解决了跨异构域授权将面临的如何跨域形成信任链以及如何校验信任链有效性等问题，并对该方案的完备性、公平性和可行性进行了说明，提出了建立模型时所面临的问题并针对这些问题给出了建议和解决方案.

参　考　文　献

[1] LIU Yuan-hang, JU Jiu-bin. Overview of Cross Certification [C]//The National Network and Information Security Seminars. Beijing: [s. n.], 2004: 402-409. (刘远航，鞠九滨. 交叉认证问题研究综述 [C]. 全国网络与信息安全技术研讨会. 北京: [出版者不详], 2004: 402-409.)

[2] HU De-bin, WANG Jin-ling, YU Meng-tao, et al. ID Alias IBE Scheme with a Trusted Third Party [J]. Journal of Jilin University: Engineering and Technology Edition, 2008, 38(2): 419-422. (胡德斌，王金玲，于孟涛，等. 基于身份别名的加入辅助认证方的 IBE 方案 [J]. 吉林大学学报: 工学版, 2008, 38(2): 419-422.)

[3] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing [C]//Kilian J CRYPTO 2001. Berlin: Springer-Verlag, 2001: 213-229.

[4] Joux A, Nguyen K. Separating Decision Diffie-Hellman from Computational Diffie-Hellman in Cryptographic Groups [J]. Journal of Cryptology, 2003, 16(4): 239-247.

[5] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing [C]//Kilian J CRYPTO 2001. Berlin: Springer-Verlag, 2001.

[6] Menezes A J, Okamoto T, Vanstone S A. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field [J]. IEEE Trans on Information Theory, 1993, 39(5): 1639-1646.

[7] HU Liang, CHU Jian-feng, LIN Yu, et al. IBE System Based on Trust Service [J]. Journal of Jilin University: Engineering and Technology Edition, 2009, 39(3): 737-742. (胡　亮，初剑峰，林　宇，等. 基于信任服务的 IBE 系统 [J]. 吉林大学学报: 工学版, 2009, 39(3): 737-742.)

[8] GUAN Hai-ming. The Comparison between CPK and PKI [J]. Computer Security, 2003(8): 17-18. (管海明. CPK 与PKI 的性能分析 [J]. 计算机安全, 2003(8): 17-18.)

[9] YUAN Wei, HU Liang, LIN Yu, et al. Structure Analysis and Optimization Implementation of Advanced Encryption Standard Algorithm [J]. Journal of Jilin University: Science Edition, 2008, 46(5): 885-890. (袁　巍，胡　亮，林　宇，等. AES 算法的结构分析与优化实现 [J]. 吉林大学学报: 理学版, 2008, 46(5): 885-890.)

[10] 胡　磊，王　鹏，译. 应用密码学手册 [M]. 北京: 电子工业出版社, 2005: 509.

[11] 孟庆树，傅建明，译. 密码编码学与网络安全 [M]. 北京: 电子工业出版社, 2005: 311.

[12] YUAN Wei, ZHANG Yun-ying, HU Liang, et al. Structure Cryptanalysis of Rijndael Algorithm [J]. Journal of Jilin University: Information Science Edition, 2008, 26(5): 487-493. (袁　巍，张云英，胡　亮，等. Rijndael 算法的结构归纳与攻击分析 [J]. 吉林大学学报: 信息科学版, 2008, 26(5): 487-493.)

[13] LIN Yu, YU Meng-tao, WANG Jin-ling, et al. Scheme of Electronic Seal Based on IBE and Digital Watermark [J]. Journal of Jilin University: Information Science Edition, 2007, 25(4): 406-411. (林　宇，于孟涛，王金玲，等. 基于IBE 和数字水印的电子印章解决方案 [J]. 吉林大学学报: 信息科学版, 2007, 25(4): 406-411.)