

面向服务监管的信息标识生成与管理方案

李响¹, 王浩¹, 刘千歌¹, 王超², 毛剑¹, 刘建伟¹

(1. 北京航空航天大学 网络空间安全学院, 北京 100191;

2. 北京数字认证股份有限公司, 北京 100080)

摘要: 信息服务在对经济社会发展产生重大影响的同时, 也带来了一系列安全挑战。实现对信息服务的细粒度、持续、动态监管, 成为信息服务管理的重中之重。传统的静态身份认证和管理机制, 难以满足对信息服务实体与服务质量的持续性监管需求。提出一种面向服务监管的信息标识生成与管理方案, 从信息服务类别、服务等级、服务质量可信度等多个角度定义了一种信息标识格式, 使用层次分析法对信息服务进行评级, 并对信息标识进行动态管理, 可满足面向多维业务属性的信息标识的签发和细粒度动态管理的需求。

关键词: 信息服务; 可信标识; 信任评估; 动态管理

中图分类号: TP309

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021055

Information service identity generation and management scheme for service supervision

LI Xiang¹, WANG Hao¹, LIU Qiange¹, WANG Chao², MAO Jian¹, LIU Jianwei¹

1. School of Cyber Science and Technology, Beihang University, Beijing 100191, China

2. Beijing Certificate Authority Co., Ltd., Beijing 100080, China

Abstract: While information services have a significant impact on economic and social development, it also brings a series of security challenges. Realizing fine-grained, continuous, and dynamic supervision of information services has become the top priority of information service management. Traditional static identity authentication and management mechanisms, are difficult to meet the continuous monitoring requirements for information service entities and service quality. An information service identification generation and management scheme for service supervision was proposed. It defined an information service identification format from multiple perspectives such as

收稿日期: 2020-11-14; 修回日期: 2021-01-20

通信作者: 毛剑, maojian@buaa.edu.cn

基金项目: 国家重点研发项目 (2017YFB0802403); 北京市自然科学基金 (4202036); 国家自然科学基金 (U173315, 61571010, 61871023)

Foundation Items: The National Key R&D Program of China (2017YFB0802403), The Beijing Natural Science Foundation (4202036), The National Natural Science Foundation of China (U1733115, 61571010, 61871023)

论文引用格式: 李响, 王浩, 刘千歌, 等. 面向服务监管的信息标识生成与管理方案[J]. 网络与信息安全学报, 2021, 7(5): 169-177.

LI X, WANG H, LIU Q G, et al. Information service identity generation and management scheme for service supervision[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 169-177.

information service category, service grade, and service quality credibility. It used the analytic hierarchy process to evaluate information services and designed a dynamic management of information service identification. The scheme can meet the needs of issuance and fine-grained dynamic management of information service identification for multi-dimensional business attributes.

Keywords: information service, trusted identity, trust assessment, dynamic management

1 引言

随着互联网经济的飞速发展,信息服务已经渗透到社会生活的各个领域,对经济社会发展产生战略性和全局性的影响。然而,信息服务在为用户的工作生活带来极大便利的同时,也带来了诸多安全挑战。由于信息服务的运行环境更具开放性和动态性,传统的管理控制机制难以有效实施。其海量信息交互、共享和协作的功能特性使用户可能面临的信息安全、隐私泄露、钓鱼攻击等问题更加突出,且其异构、海量、动态的数据结构也引入了更高的信任风险,增加了信任成本。此外,当前信息服务种类繁多,用户规模也在不断扩大,有效的信息服务实体管理和鉴别机制却依然存在空缺。因此,构建安全可信的信息服务生态体系,实现对信息服务的良序治理,已然成为关系互联网经济与社会民生的重中之重。

多年来,各个国家与地区在针对信息服务实体的管理方面总是不遗余力。早在 1995 年,美国犹他州就颁布了一部全面确立电子商务运行规范的法律文件——《数字签名法》,并紧随其后颁布一系列相关条款^[1-2];与之类似的,欧盟所颁布的“电子商务指令”^[3]则专门规定了消费者知情权的行使和保护;随后在 2000 年,日本颁布了《数字签名及认证法》以确保电子签名被稳妥使用;而我国在 2000 年颁布的《互联网信息服务管理办法》^[4]则用以规范互联网信息服务活动,促进互联网信息服务健康、有序、发展;之后在 2017 年,我国发布的《网站可信标识技术指南》^[5]提出了用于识别网站真实信息的可信标识体系框架。

在图 1 所示的信息服务场景中,信息服务多种多样,且一个服务提供商可能提供多个信息服务,用户使用信息服务时无法获取该服务的服务内容、类别、等级、可信度等有效信息,因此需

对信息服务进行细粒度的管理。此外,信息服务质量是用户选择服务的主要标准,与服务质量和服务商的资质有关,但随着技术进步、使用对象的变化也会不断更新和丰富,因此需要对其进行持续性监管和动态更新。现有的实体认证和管理机制缺少对服务类别、服务可信度、服务质量、用户评价等多业务属性的细粒度身份认证和管理,如 X.509 证书将公钥与身份进行绑定用于实体身份认证,无法实现对实体细粒度属性信息的认证,难以满足多维业务场景下对信息服务实体与服务质量的持续性监管需求。

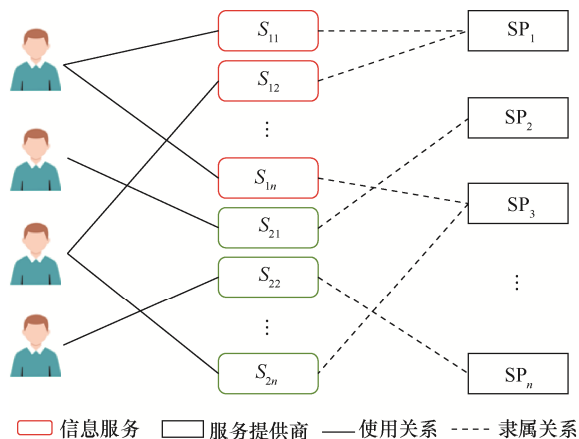


图 1 多维信息服务场景

Figure 1 A multi-dimensional information service scenario

2 相关研究

2.1 数字证书

数字证书是确保安全网络通信的关键组件之一,其中应用较为广泛的是国际电信联盟制定的 X.509 标准,该标准定义了公钥证书的基本结构,且在 X.500 确保用户名称唯一性的基础上,规定实体鉴别过程广泛适用的证书语法和数据接口,为用户提供通信实体鉴别机制。X.509 标准在编排公钥密码格式方面被广泛应用,已用于许多网络安全应用程序,如 IPSec、SSL 等,并且被多数认证中心作为签发

证书的遵循标准^[6]。

当前使用的证书标准版本是 X.509v3, 该版本除定义了一组按预定义顺序排列的强制字段外, 还定义了可选扩展字段。此外, X.509v3 证书为大多数字段提供多种编码方案, 具有很大的灵活性。

除 X.509 外, 还有简单公钥基础设施 (SPKI, simple public key infrastructure)、PGP (pretty good privacy) 等证书格式定义标准。由 IETF 发布的 SPKI 标准在颁发者、合法性等方面与 X.509 类似, 但两者在语法等方面不同, 如 SPKI 采用的名称约定来自简单分布式安全基础设施中的定义。PGP 是对电子邮件和文件进行加密和数字签名的一种方法, 其与 X.509 证书的信任模型完全不同, 两者协议也互不兼容^[7]。

2.2 信息服务身份认证研究现状

有效的实体认证是保障网络信息服务安全的关键环节, 其能够鉴别服务实体的真实身份并保证用户访问信息服务资源的合法性。在网络应用环境下, 主要采用的信息服务认证方式有基于公钥基础设施 (PKI, public key infrastructure) 和标识密码技术 (IBC, identity-based cryptography) 的认证方案^[8]。

基于 PKI 的认证方案是常见的 X.509 证书管理方法^[7], 由于 PKI 的成熟性、安全性其被普遍用于安全领域。PKI 通过公钥体制和数字签名服务管理密钥和证书, 使用第三方的可信任机构——认证中心 (CA), 绑定实体的公钥和身份, 用于实体的身份验证, 保证信息的机密性、真实性、完整性和不可否认性。但是基于 PKI 的认证方案在使用和密钥管理方面具有一定的复杂性, 且存在被攻击或恶意 CA 所导致的安全威胁, 证书误签一类的攻击事件频发^[9]。Google 于 2013 年提出证

书透明化 (CT, certificate transparency), 引入 CT 日志记录所有的证书签发行, 同时支持公开的监视和审计, 从而保证实体身份认证的安全性和可靠性^[10-11]。

在基于 IBC 的认证方案中, 每个实体都具备唯一的标识, 该标识就是实体的公钥, 能促成在无须协商密码或交换证书情况下的安全通信, 简化了系统管理的复杂性。表 1 对比了 PKI 与 IBC 认证系统进行身份认证时的密钥管理过程, 并列举了基于两种机制实现的身份认证方案。可供选择的信息系统认证机制很多, 然而如何选择稳定性好、可靠性高、为用户提供优质服务的认证机制至关重要。

3 信息服务标识的生成和管理方案设计

本节针对信息服务细粒度和动态监管的需求, 提出一种面向服务监管的信息标识的生成和管理方案, 如图 2 所示。本方案涉及的主体包括信息服务商 (SP, service provider)、签发机构 (IA, issuing authority) 和测评机构 (AA, assessment authority)。在本方案中, 信息服务商可以向签发机构提出标识请求, 待其身份验证通过后, 签发机构将相关信息转发给测评机构; 测评机构对该信息服务进行测评, 并将测评结果返回给签发机构; 签发机构对该信息服务签发信息服务标识, 并将标识发送给信息服务商。用户获取所使用信息服务的标识, 通过签发机构的标识动态管理模块进行标识检索和标识验证。此外, 签发机构的标识动态管理模块还支持标识更新和标识撤销功能。

3.1 标识格式

信息服务标识中, 签发机构通过签发信息服务标识对信息服务类别、服务可信度、服务等级、

表 1 PKI 认证与 IBC 认证系统对比
Table 1 The comparison of PKI and IBC authentication systems

对比项	密钥生成	密钥分发	密钥撤销	算法比较	适用场景	安全性	现有方案
PKI	分布式	证书目录	CRL OCSP	RSA	开放式的大范围应用	高 (基于离散对数、大数分解问题)	文献[12-14] 文献[15-16]
IBC	集中式	安全信道 分发私钥	短期密钥	ECC	封闭式的小范围应用	高 (基于双线性对问题)	文献[17-20] 文献[21-22]

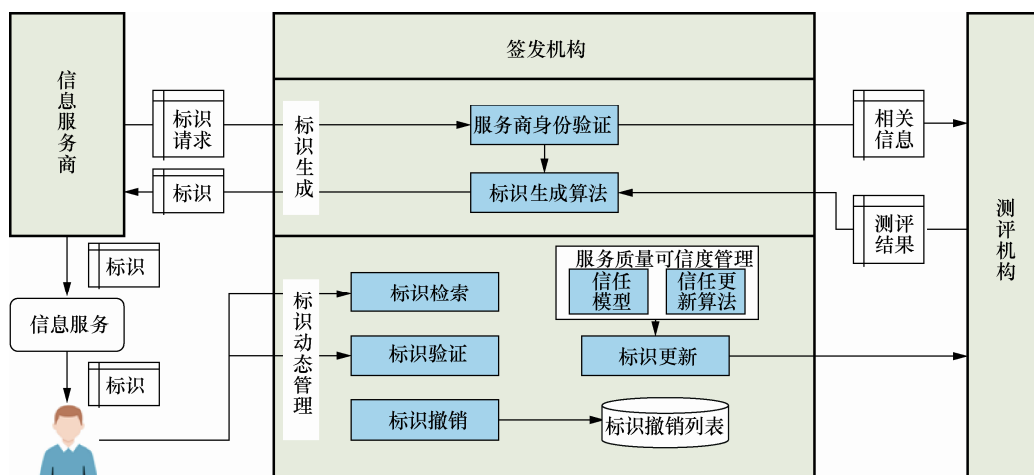


图 2 信息服务标识的生成和管理方案框架

Figure 2 The framework of the information service identity generation and management mechanism

服务商身份等进行明确标注，使监管更加全面，便于用户了解信息服务的基本信息，更好地选择和使用信息服务。信息服务标识满足唯一性、机密性、信息完整性和不可否认性。

面向多维业务属性的信息服务标识定义为多元组：Tag={版本号 (V, version), 序列号 (SN, serial number), 算法标识 (AI, algorithm identifier), 发布者 (IA, issuing authority), 有效期 (Val, validity), 信息服务类别 (CS, C-service), 服务质量可信度 (QoS, QoS-credibility), 信息服务等级 (GS, G-service), 测评机构 (AA, assessment authority), 测评标准 (AS, assessment standard), 信息服务编码 (ID-S, ID-service), 服务商身份 (ID-SP, ID-service provider), 扩展域 (Exten, extensions), 数字签名 (DS, digital signature)}。信息服务标识的格式如图 3 所示，表 2 列出了信息服务标识的字段描述。

表 2 信息服务标识的字段描述
Table 2 The description of fields of the information service identity

字段	描述
版本号	信息服务标识使用的标准版本
序列号	IA 给每个信息服务标识生成唯一整数值
算法标识	IA 签名信息服务标识使用的算法
发布者	IA 的标识信息
有效期	包含两个日期时间值 (生效时间和失效时间)
信息服务类别	信息服务的类别
服务质量可信度	信息服务可信度的量化值
信息服务等级	AA 对信息服务质量的评级
测评机构	AA 的标识信息
测评标准	AA 使用的测评标准
信息服务编码	信息服务的唯一标识号
服务商身份	SP 的标识信息
扩展域	信息服务标识的其他属性
数字签名	签发机构对信息服务可信标识的签名

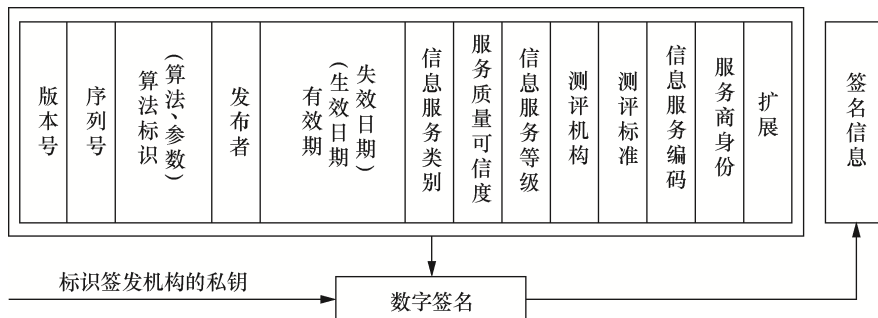


图 3 信息服务标识的格式

Figure 3 The format of the information service identity

3.2 信息服务等级的测评

传统的身份认证机制，如数字证书，可以鉴别服务实体的真实身份并保证用户访问信息服务资源的合法性，但服务实体身份的真实性并不能保证信息服务的高质量，用户从证书中无法获取服务质量等信息。本文方案提出的信息服务标识中引入信息服务等级字段用于标识信息服务的质量，并使用层次分析法确定信息服务等级。层次分析法^[23]是一种解决多指标综合性问题的经典方法，将多指标的复杂问题分解为相互关联的组成因素，根据元素间的隶属关系获得层次结构，最终得到各元素的权重值。

测评机构定义统一的信息服务质量指标为 $p_1, p_2, \dots, p_n$ ，如服务完整性、服务机密性、隔离性、可靠性、用户体验、服务纠纷等指标。信息服务等级的测评步骤如下。

(1) 测评机构对该信息服务的 n 个质量指标进行两两对比，确定两个属性的重要性程度即相对权重值 a_{ij} ，构造判断矩阵： $A = (a_{ij})_{n \times n}$ 。其中， a_{ij} 使用 1~9 标度法进行对比赋值，如表 3 所示，且 $a_{ij} = \frac{1}{a_{ji}}$ 。

表 3 相对权重值的赋值和含义
Table 3 The value and definition of the relative weight

赋值	含义 (p_i 比 p_j)
1	重要性相同
3	稍微重要
5	明显重要
7	强烈重要
9	极端重要
$2n(n=1,2,3,4)$	重要性介于 $2n-1$ 与 $2n+1$ 之间

(2) 对判断矩阵进行一致性检验。一致性比率为 $CR = \frac{CI}{RI}$ ，其中， $CI = \frac{\lambda_{\max} - n}{n - 1}$ 为一致性指数， $\lambda_{\max}$ 为成对比较矩阵的最大特征根，随机一致性指数为 $RI = f(n)$ ，如表 4 所示。当一致性比率 $CR < 0.1$ 时，认为成对比较矩阵的不一致性程度可以接受；否则，需要重新构造判断矩阵。

表 4 随机一致性指数 RI 的数值
Table 4 Random consistency index (RI) list

阶数	RI
1	0
2	0
3	0.58
4	0.90
5	1.12
6	1.24
7	1.32
8	1.41
9	1.45

(3) 判断矩阵通过一致性检验后，计算得到判断矩阵的标准化特征向量

$$\alpha = (b_1, b_2, L, b_n)^T. \quad (1)$$

其中， b_i 为信息服务质量指标 p_i 的权重，且

$$\sum_{i=1}^n b_i = 1.$$

(4) 测评机构评估信息服务的每个服务质量指标的得分 s_i ，计算信息服务质量的综合评分

$$S = \sum_{i=1}^n s_i b_i \quad (2)$$

根据综合评分对应的等级所属范围，如表 5 所示，确定信息服务的等级。

表 5 信息服务等级分级标准
Table 5 The grading standard of information services

等级	范围
A	(90,100]
B	(80,90]
C	(70,80]
D	(60,70]
E	[0,60]

3.3 信息服务标识的生成

信息服务标识的生成涉及的参与方包括信息服务商、测评机构和签发机构。生成信息服务标识的流程（如图 4 所示）具体如下。

第 1 步：申请。信息服务商向 IA 提交信息服务标识请求，包括服务商公钥、信息服务名称等相关信息及相关证明材料。标识请求结构参考 PKCS#10 证书申请结构^[24]。

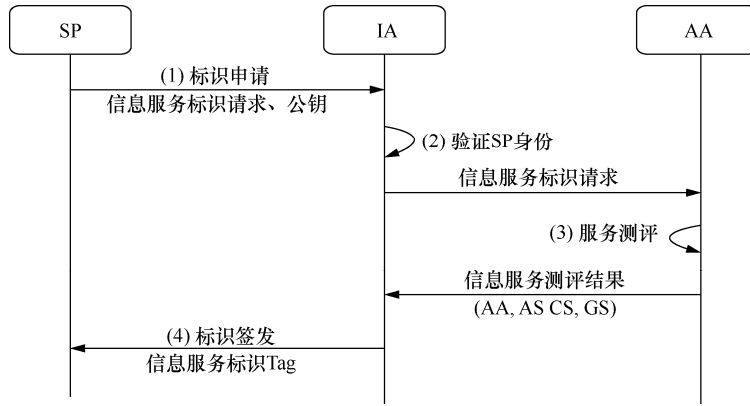


图 4 生成信息服务标识的流程

Figure 4 The flow of the information service identity deployment generation

第 2 步：验证。IA 验证服务商公钥，检查服务商拥有与标识请求中发送的公钥相对应的私钥，即检查私钥的拥有证明。验证通过后，IA 将信息服务的相关信息以及证明材料转发给 AA。

第 3 步：服务测评。AA 验证服务商材料，检查服务商的营业记录、历史文件和信用证明的真假；根据一定的测评标准对信息服务的类别和等级进行测评，并将测评结果发送给 IA。

第 4 步：标识签发。IA 对信息服务标识所需的所有字段进行必要的验证，使用 SHA-256 算法对 Tag 的所有字段计算摘要，如式(3)所示。

$$H_{\text{Tag}} \leftarrow \text{Hash}(V \parallel \text{SN} \parallel \text{AI} \parallel \text{IA} \parallel \text{Val} \parallel \text{CS} \parallel \text{QoS} \parallel \text{GS} \parallel \text{AA} \parallel \text{AS} \parallel \text{ID_S} \parallel \text{ID_SP} \parallel \text{Exten}) \quad (3)$$

使用私钥对摘要进行签名： $\text{DS} \leftarrow \text{Sig}_{\text{KR}_{\text{IA}}}(H_{\text{Tag}})$ ，将标识发给信息服务商，并在本地数据库中保留

一份标识记录。

3.4 信息服务标识的动态管理机制

为实现对信息服务的持续性监管，信息服务标识的动态管理机制支持标识检索、标识验证、标识更新、标识撤销功能。

(1) 标识检索和标识验证。用户使用信息服务时，可以检索相应的信息服务标识，验证标识的签名和有效性，即验证标识是否属于相应的信息服务商，验证标识是否有效，是否被撤销。

(2) 标识更新。信息服务的时效性、属性和可信度变化都会触发标识更新，签发机构对该信息服务重新签发标识，标识更新流程如图 5 所示。在信息服务标识中，信息服务质量、可信度以及服务等级是动态变化的。在图 2 所示的框架中，服务质量可信度管理子模块实际为一个专家库，其中包括信任模型和信任更新算法，信息服务质

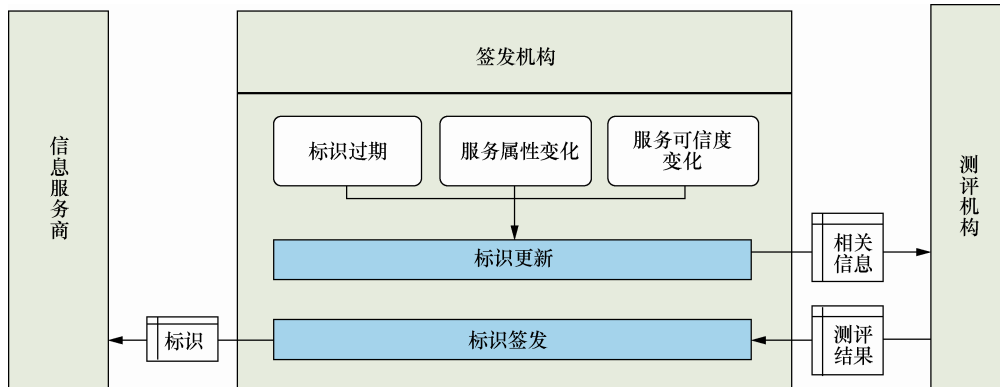


图 5 信息服务标识更新流程

Figure 5 The flow of the information service identity update

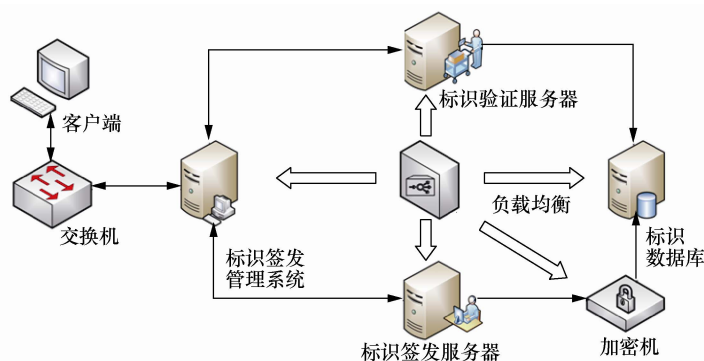


图6 系统部署的拓扑结构
Figure 6 The structure of system topology

量可信度变化较大时触发标识更新机制, 测评机构对信息服务进行重新评级, 签发机构对信息服务重新签发标识。

(3) 标识撤销。当标识失效时(如超过有效期, 服务商自行撤销, 置信度降至阈值以下), 需要对标识进行撤销处理。撤销的信息服务标识会存放在标识撤销列表中。

4 系统实现

在信息服务标识签发管理系统的仿真环境中, 服务器使用 JDK 1.8、MySQL 5.7 和 Apache tomcat 8, 系统部署的拓扑结构如图 6 所示。

信息服务商通过客户端向标识签发管理系统请求标识签发服务, 标识签发服务器签发标识后将标识通过客户端发送给信息服务商, 同时对标识进行加密处理并保存在标识数据库中。信息服务标识的示例如图 7 所示。

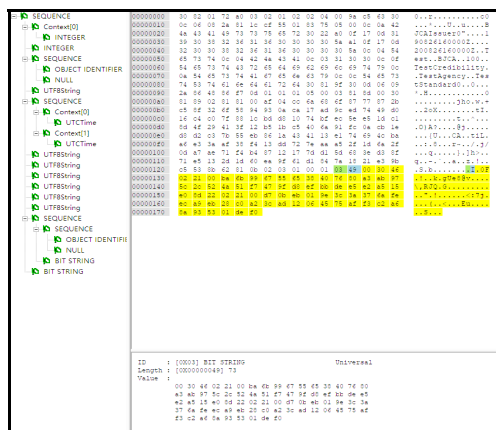


图7 信息服务标识的示例
Figure 7 A example of the information service identity

用户可以通过客户端向标识签发管理系统请求标识验证服务, 标识验证服务器通过查询标识数据库中的相应记录来验证标识是否有效。图 8 为信息服务标识正常日志和异常日志的示例, 本标识签发管理系统可以实现对信息服务标识全生命周期的管理, 包括标识签发、标识验证、标识更新和标识撤销。

5 结束语

基于当前针对信息服务的细粒度动态监管需求, 本文提出了一种面向服务监管的信息标识生成和管理方案。方案从信息服务类别、服务等级、服务质量可信度等多角度定义了一种信息服务标识格式, 实现了对信息服务细粒度属性信息的认证。除基本功能(标识检索、验证和撤销)外, 方案还支持标识更新的功能, 当信息服务时效性、服务属性和可信度变化时进行标识更新, 实现信息服务的动态持续性监管需求。

参考文献:

- [1] 魏伶俐, 张淑霞, 晏杰, 等. 国际电子签名立法状况介绍[C]//信息社会档案理论与实践. 2006: 8.
WEI L L, ZHANG S X, YAN J, et al. Introduction to legislation of international electronic signature[C]//Theory and Practice of Archival Science in Information Society. 2006: 8.
- [2] 国际电子商务立法[J]. 国际化工信息, 2005(7): 47.
International electronic commerce legislation[J]. Global Chemical Information, 2005(7): 47.
- [3] PEARCE G, PLATTEN N. Promoting the information society : The EU directive on electronic commerce[J]. European Law Journal, 2000, 6: 363-378.
- [4] 互联网信息服务管理办法[J]. 信息安全与通信保密, 2001, 1: 36-37.

序号	信息服务标识序列号/操作人员	操作类型	日志类型	操作时间	结果	操作
1	9ac563	签发	正常日志	2020-11-10	签发成功	审计
2	cb773d	验证	正常日志	2020-07-01	验证/审计成功	审计
3	cb773d	验证	正常日志	2020-07-01	验证/审计成功	审计
4	cb773d	验证	正常日志	2020-07-01	验证/审计成功	审计
5	cb773d	验证	正常日志	2020-07-01	验证/审计成功	审计
6	cb773d	签发	正常日志	2020-07-01	签发成功	审计
7	7aa298	签发	正常日志	2020-07-01	签发成功	审计
8	542365	签发	正常日志	2020-03-04	签发成功	审计
1 2 3 ... 8 到第 1 页 确定 共 60 条 8 条/页						
序号	信息服务标识序列号/操作人员	操作类型	日志类型	操作时间	结果	操作
1	c24d49	签发	异常日志	2020-07-01	标识签发制作失败	审计
2	c24d49	签发	异常日志	2020-07-01	标识签发制作失败	审计
3	c24d49	验证	异常日志	2020-03-04	标识已被注销	审计
4	a41ead	验证	异常日志	2020-02-20	标识已被注销	审计
5	a41ead	更新	异常日志	2020-02-20	标识已被注销	审计
6	a41ead	更新	异常日志	2020-02-20	标识已被注销	审计
7	a41ead	更新	异常日志	2020-02-20	请求参数错误	审计
8	a41ead	更新	异常日志	2020-02-20	请求参数错误	审计
1 2 3 ... 6 到第 1 页 确定 共 48 条 8 条/页						

图8 信息服务标识日志示例
Figure 8 A example of logs of information service identities

- Measures for the administration of Internet Information Services[J]. China Information Security, 2001, 1: 36-37.
- [5] GB/T 35287-2017. 信息安全技术网站可信标识技术规范[Z]. GB/T 35287-2017. Information security technology-Guidelines of trusted identity technology for website[Z].
- [6] 魏宗秀. 基于 X.509 身份认证协议的研究[J]. 信息安全与通信保密, 2008, 11: 54-57.
WEI Z X. A research based on X.509 authentication and its usage[J]. Information Security and Communications Privacy, 2008, 11: 54-57
- [7] 秦余勇. X. 509 V3 证书格式及语义[J]. 通信技术, 2001, 6: 20-23.
YU Q Y. The form and semantic description of X.509 V3 certificate[J]. Communications Technology, 2001, 6: 20-23.
- [8] 杨萍. Kerberos 的安全性分析及其认证模式的研究与改进[D]. 天津: 天津理工大学, 2015.
YANG P. Security analysis of Kerberos and research and improvement on the authentication scheme[D]. Tianjin: Tianjin University of Technology, 2015.
- [9] KUMAR D, WANG Z, HYDER M, et al. Tracking certificate misissuance in the wild[C]//IEEE Symposium on Security and Privacy. 2018: 785-798.
- [10] 张婕, 王伟, 马迪, 等. 数字证书透明性 CT 机制安全威胁研究[J]. 计算机系统应用, 2018, 27(10): 232-239.
ZHANG J, WANG W, MA D, et al. Overview on security issues of certificate transparency[J]. Computer Systems & Applications, 2018, 27(10): 232-239.
- [11] LI B, LIN J, LI F, et al. Certificate transparency in the wild: Exploring the reliability of monitors[C]//ACM SIGSAC Conference on Computer and Communications Security. 2019: 2505-2520.
- [12] 吴涛. 基于 PKI 技术的 CA 系统研究及其数字证书管理的实现[D]. 武汉: 武汉理工大学, 2004.
- WU T. The research on CA system based on PKI technology and the implementation of management of digital certificat[D]. Wuhan: Wuhan University of Technology, 2004
- [13] 钱思杰, 陈立全, 王诗卉. 基于改进 PBFT 算法的 PKI 跨域认证方案[J]. 网络与信息安全学报, 2020, 6(4): 37-44.
QIAN S J, CHEN L Q, WANG S H. PKI cross-domain authentication scheme based on advanced PBFT algorithm[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 37-44.
- [14] LU Z, LIU W, WANG Q, et al. A privacy-preserving trust model based on blockchain for VANETs[J]. IEEE Access, 2018, 6: 45655-45664.
- [15] FU P, LI Z, XIONG G, et al. SSL/TLS security exploration through X.509 certificate's life cycle measurement[C]//IEEE Symposium on Computers and Communications. 2018: 652-655.
- [16] LINN J. Trust models and management in public-key infrastructures[J]. RSA laboratories, 2000, 12.
- [17] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281.
PENG H X. An identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8): 1271-1281.
- [18] 杨宇, 谭平嶂, 李锴, 等. 基于标识的跨域认证系统研究[J]. 信息安全与通信保密, 2009, 8: 193-195.
YANG Y, TAN P Z, LI L, et al. Identity-based authentication system in multi trust domain[J]. Information Security and Communications Privacy, 2009, 8: 193-195
- [19] WU L, WANG J, CHOO K K R, et al. An efficient provably- secure identity-based authentication scheme using bilinear pairings for Ad hoc network[J]. Information Security Technical Report, 2017, 37: 112-121.
- [20] 林俊燕, 张兆雷, 袁智伟. 物联网中基于 IBC 的认证加密机制研究[J]. 信息安全与通信保密, 2020, 8: 95-101.
LIN J, ZHANG Z, YUAN Z. Research on authentication encryption mechanism based on IBC in internet of things[J]. Information

Security and Communications Privacy, 2020, 8: 95-101.

- [21] 许盛伟, 郭春锐, 李新玉. 基于多方共管的IBC改进密钥管理方案[J]. 计算机应用与软件, 2020, 37(8): 314-317.

XU S W, GUO C R, LI X Y. IBC improved key management scheme based on multi-party co-management[J]. Computer Application and Software, 2020, 37(8): 314-317.

- [22] 黄仁季, 吴晓平, 李洪成. 基于身份标识加密的身份认证方案[J]. 网络与信息安全学报, 2016, 2(6): 32-37.

HUANG R J, WU X P, LI H C. Identity authentication scheme based on identity-based encryption[J]. Chinese Journal of Network and Information Security, 2016, 2(6): 32-37.

- [23] SAATY R. The analytic hierarchy process-what it is and how it is used[J]. Mathematical Modelling, 1987, 9(3): 161-176.

- [24] RFC 2986. PKCS#10: Certificate request syntax specification version 1.7[S]. 2000.

[作者简介]



李响（1996-），女，河南辉县人，北京航空航天大学硕士生，主要研究方向为信任模型。



王浩（1995-），男，黑龙江哈尔滨人，北京航空航天大学硕士生，主要研究方向为物联网安全。



刘千歌（1997-），女，新疆克拉玛依人，北京航空航天大学硕士生，主要研究方向为物联网安全。



王超（1980-），男，贵州贵阳人，主要研究方向为非对称密码算法。



毛剑（1978-），女，江苏溧水人，博士，北京航空航天大学副教授、博士生导师，主要研究方向为Web安全和物联网安全。



刘建伟（1964-），男，山东莱州人，博士，北京航空航天大学教授、博士生导师，主要研究方向为密码学与网络安全。