



公众网络统一身份认证服务及标准研究^{*}

孙韩林, 刘建华

(西安邮电大学计算机学院 西安 710121)

摘 要:统一身份认证的目标是实现一个身份多处访问,以简化用户访问多个服务的流程。统一身份认证研究尚处于起步阶段。从统一身份认证的功能需求出发,在公众网络上以服务方式实现统一身份认证,提出了一种公众网络统一身份认证服务的网络架构。统一身份认证服务网络由多个身份认证服务提供商组成,每个服务商负责本地用户或服务统一身份信息的管理和认证;不同服务商通过各自的桥接服务进行互操作,实现非本地身份的认证。本文提出了一种基于行政区划的层次式的公众网络统一身份网络部署模型,最后讨论了统一身份认证服务的标准体系。

关键词:统一身份认证;身份认证;公众网络;标准

doi: 10.3969/j.issn.1000-0801.2013.02.014

Study on Unified Identifier Authentication Service and Standards on Public Network

Sun Hanlin, Liu Jianhua

(School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract: The aim of unified identifier authentication (UIA) is to log in multiple services with only one identifier to simplify user's access. Currently, the study of UIA is on its early stage. Taking into account UIA's functionality requirements, implementation of UIA, as a service in public network, was suggested, and an architecture of UIA service network was proposed. The UIA service network consists of multiple UIA service providers. Each is responsible for management and authentication of unified identifiers of local users and services. A provider could interoperate with others to authenticate non-local identifiers through bridge services of themselves. A hierarchy deployment model of UIA service network based on political administration regions was proposed as well. Finally, the standards system of UIA service was discussed.

Key words: unified identifier authentication, identifier authentication, public network, standard

1 引言

身份认证是电子信息服务中的一项基础服务,用于确定用户身份,进而决定如何响应用户的请求。随着信息技术的发展,用户使用的信息服务越来越多,包括消费电子

服务、商业电子服务和政府电子服务等。在登录服务时,每次都要进行认证,用户需要记忆大量的认证信息(如账号、密码等),这给用户带来极大的不便。近年来提出了统一身份认证的相关概念,如统一身份管理(unified identity management)、联合身份(federation of identity)、以用户为中

^{*} 工业和信息化部软科学研究项目(No.2012-R-57)

心的认证(user centric authentication)、单点登录(single sign on)等,以实现一个身份多处访问。标准化组织,如 ITU-T、自由联盟(Liberty Alliance)、3GPP、OASIS(结构化信息标准促进组织)、IETF/ETSI(欧洲电信标准委员会)、ISO、W3C(国际网络联盟)等,也都纷纷研究统一身份认证问题。ITU-T 将统一身份认证定义为对某实体声称的标识为真提供证明,并实现单点登录,实体可以是人、动物、法人、组织、设备、软件应用、服务等或这些个体的组合。信息技术发达国家也纷纷提出了各自的身份认证战略:美国 2010 年 6 月发布了《国家网络空间可信身份战略》;韩国和日本自 2011 年以来,积极推行、制定网络身份管理战略,加强对公民网络信息的监督和保护;我国也成立了“全国信息安全标准化技术委员会鉴别与授权工作组”,推动身份识别和授权技术的发展。

鉴于统一身份认证在信息服务应用中的重要性,研究统一身份认证服务及其标准十分必要。本文研究在公众网络上以服务方式实现统一身份认证,提出了公众网络统一身份认证服务网络的架构和一种层次式的统一认证服务网络部署模型,并讨论了统一身份认证服务的标准体系。

2 统一身份认证服务功能需求

ITU-T、自由联盟、3GPP 等众多标准化组织都致力于统一身份认证的研究。由于利益、观点、关心的问题、优先顺序、技术、安全以及身份集成等诸多方面存在问题,实现统一身份认证很复杂,不同标准组织针对自己特定的需求各有侧重。统一身份认证的复杂性主要体现在:技术复杂性、互操作性、安全性、已有身份管理设施的集成性以及自适应性等方面,其中,互操作性是面临的主要问题。ITU-T 致力于研究全球可互操作的身份管理,重点解决目前各个“孤岛”身份管理方案的互通和互操作问题,如图 1 所示。

ITU-T 全球兼容身份管理的功能需求如图 2 所示,具体包括以下方面。

- 身份信息的管理:包括身份信息的登记、创建、保存和注销。身份信息可细分为标识能力、证书能力、属性能力和模式能力 4 种基本类型。
- 身份信息的关联:将实体的标识信息与身份相关联。
- 身份信息的认证:能够准确地确认实体的身份。
- 身份信息的发现与桥接:在一个不断变化的、拥有大量游牧用户和身份提供商的分布式公共网络中,

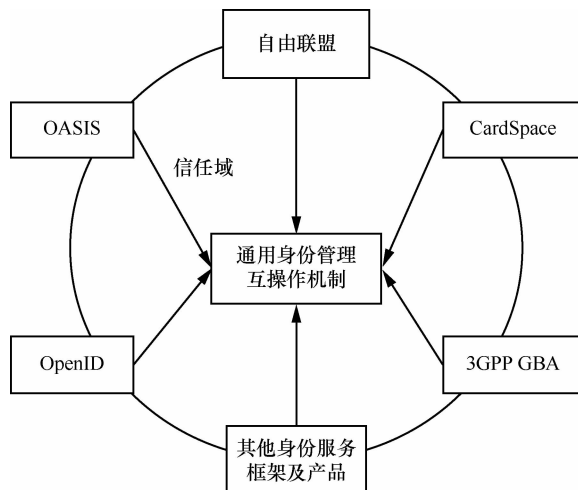


图 1 ITU-T 统一身份管理框架

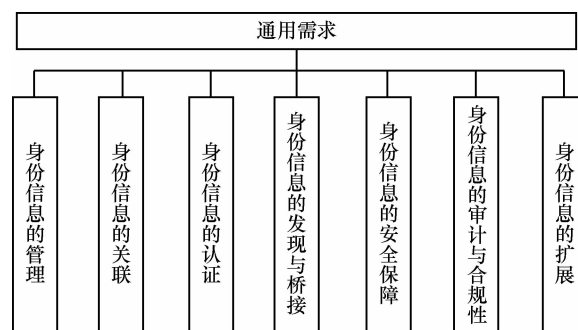


图 2 ITU-T 全球兼容身份管理通用需求

能够发现并使用新的身份服务,这要求提供身份管理资源的各方支持互操作性。

- 身份信息的安全保障:身份信息是敏感的数据,在基础设施中存储或在网络上传输时必须保证其安全性。
- 身份信息的审计与合规性:身份管理受各种法律、监管和业界经营要求的制约,有必要提供一定程度的审计与合规性。
- 身份信息的扩展:在设计和执行身份管理时应充分考虑到性能、可靠性、有效性和国际化(如支持各种字符集和语言)等需求。

3 公众网络统一身份认证服务

3.1 公众网络统一身份认证服务网络架构

本文将身份认证与 IT 服务相结合,提出一种在公众网络上实现统一身份认证服务的网络架构,如图 3 所示。统一身份认证服务由“公众网络统一身份认证网络”提供,后者由若干“统一认证服务提供商(unified authentication

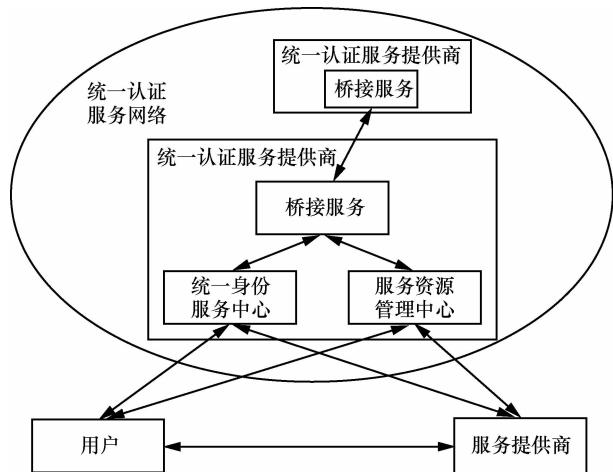


图3 公众网络统一认证服务架构

service provider, UASP)”构成。与IP地址管理类似,统一身份标识由管理机构统一进行监管,各身份服务提供商可向管理机构申请身份标识符区段,并以一致的方式在全网管理统一身份标识(包括用户身份标识和服务身份标识),即身份标识格式一致且唯一。统一认证服务由统一身份服务中心、服务资源管理中心和桥接服务组成。其中,统一身份服务中心实现了ITU-T全球兼容身份管理通用需求的几乎所有服务,如身份信息管理、身份信息关联、身份信息认证、身份服务发现和身份审计与合规性等;服务资源管理中心提供支持统一认证服务的列表,供用户查询,并保存用户对服务的评价(可用于服务推荐或选择);而桥接服务则提供不同身份服务提供商之间的互操作接口。各身份服务商可采用不同的技术实现上述服务,但用户(或服务)访问接口、桥接服务接口以及身份信息交换协议等需要遵循一致的标准,以支持互操作性。

3.2 公众网络统一身份认证服务使用

服务提供商要支持用户以统一身份进行访问,必须首先在某个统一身份认证服务提供商处进行注册。实际上,服务(包括统一身份认证服务自身)也需要一种身份,例如,可用于用户对服务的认证。注册后服务提供商从统一身份服务中心获得唯一的身份标识,该标识可用于服务管理过程中的唯一识别。服务提供商注册时,同时将服务属性(如QoS等)提交给服务资源管理中心,供用户查询。

用户向统一身份服务提供商注册,从统一身份服务中心获得全网唯一的统一身份标识。此后,用户可向服务资源管理中心查询通过统一身份可访问的服务。首次访问某服务时,用户直接向该服务提交自己的统一身份标识,服务则向统一身份服务中心发送请求验证该用户身份,若通

过验证则允许用户接入服务。服务提供商可能需要获得访问用户的一些属性信息(如用于服务分析),而提供哪些信息则由用户决定。用户从统一身份服务中心获得身份信息后,以安全的方式发送给服务提供商,但不允许服务提供商从身份提供商处直接获得。服务提供商也可能需要使用自己的认证系统(即需要整合已有的认证基础设施),此时用户首先向服务提供商注册该服务的用户标识;而后服务提供商将用户服务标识和用户统一身份标识发送给统一认证服务中心,后者将用户的两种身份进行关联绑定。当该用户再次使用该服务时,服务提供商获得用户的统一身份标识后,向统一认证服务中心发送请求验证用户身份,认证服务中心返回用户服务身份,由服务提供商自己进行验证。用户使用完服务后,可将本次服务的评价发送给服务资源管理中心,服务提供商可以利用这些评价改进服务,而身份提供商也可以利用这些评价进行服务查询推荐。

用户或应用的统一身份在全网通用。用户可以用统一身份访问不在本地(注册)身份服务提供商处注册的服务;相应地,服务提供商也可验证在其他统一身份服务提供商处注册的用户,这需要使用身份发现与桥接服务。本地用户可向服务资源管理中心查询在其他统一身份服务提供商处注册的服务(通过桥接服务);本地服务提供商也可向统一身份服务中心发送请求验证在其他身份服务提供商处注册的用户(通过桥接服务)。

3.3 安全考虑

网络空间中出现的安全风险也会出现在统一身份认证服务网络中,如系统安全、窃听、身份窃取、身份欺诈(钓鱼)等。用户、服务提供商和统一身份服务提供商需要通过安全基础设施(如PKI)、数字签名、加密、安全协议等技术,保证身份信息存储和传输的安全性。

4 层次式统一身份认证服务部署模型

4.1 层次式部署模型

身份服务提供商之间可以采用多种方式组成统一身份服务网络,最关键的问题是身份和身份服务的发现与定位。结合目前身份信息管理的实际情况,本文提出一种基于行政区划的层次式公众网络统一身份认证服务网络部署模型,如图4所示。下级身份提供商以自己的统一身份标识向上级身份提供商注册,并提供自己所管理的身份标识符区段等信息,组成统一身份认证服务网络。用户或服务提供商在本地身份提供商(县、区、市或省级)进行注册。

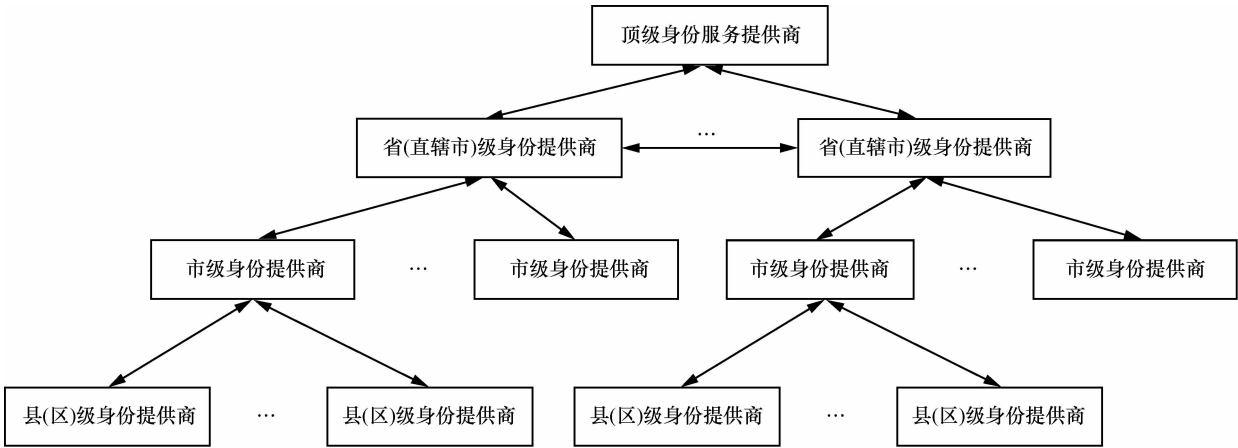


图4 层次式统一身份服务网络部署模型

上级身份提供商除了给本地用户和服务提供身份认证服务外,还通过桥接服务与下级身份提供商协作,完成身份查询、认证等。顶级身份服务提供商包含所有省(直辖市)级身份服务提供商信息,辅助省(直辖市)级身份服务商之间的定位与发现,不直接提供身份认证服务。

4.2 层次式统一身份认证服务访问流程

在层次化的统一身份服务网络中,一次完整的统一身份服务访问流程如图5所示,包括服务查询和用户认证两个阶段。

首先,用户向本地身份提供商查询支持统一身份认证的所需服务,若本地身份提供商中没有该类型服务的注册信息,则通过发现与桥接服务向上一级身份提供商查询;

类似地,若上一级身份提供商也没有相关服务注册信息,则向更高级身份提供商查询,直到找到相关服务信息。查询到的服务信息最终返回给用户。而后用户以自己的统一身份直接向该服务发起请求,服务则向自己的本地身份提供商发送请求验证用户身份。验证过程中,若本地身份提供商中不存在该用户,则向高级身份提供商发送验证请求,而高级身份提供商也可向更高级身份提供商提交验证请求。省(直辖市)级身份提供商之间的发现与定位需借助于顶级身份提供商。认证通过后,用户就可以统一身份访问服务(服务查询阶段和用户认证阶段所访问的身份提供商可能不同,图5中为了简化采用了同一组身份提供商)。

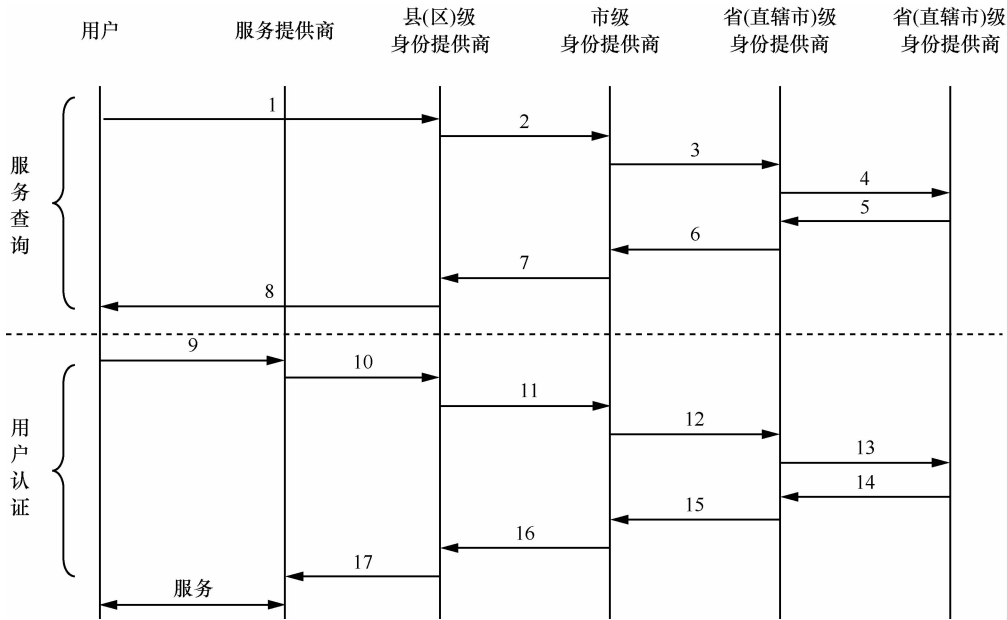


图5 层次式统一身份认证网络的服务访问流程

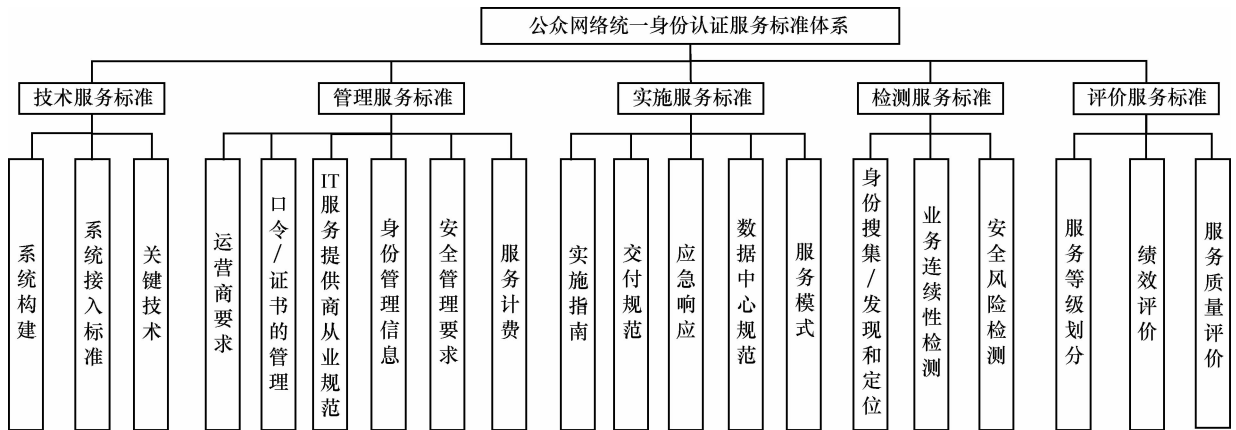


图 6 公众网络统一身份认证服务标准体系

孙韩林,男,博士,西安邮电大学计算机学院讲师,主要研究方向为互联网测量、复杂网络、云计算等。

刘建华,男,学士,西安邮电大学正高级工程师、计算机学院副院长,主要研究方向为信息安全等。