GM/Y5002- 2018

云计算身份鉴别服务密码标准体系

密码行业标准化技术委员会

CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2018 年 6 月

目 录

前　言

“云计算身份鉴别服务密码标准体系”标准研究项目是 2014 年 3 月密码行业标准化技术委员会下发的云计算领域密码标准相关的研究任务。该标准研究报告的目标范围与定位是研究云计算领域的身份鉴别服务中的密码应用相关标准和技术。

该标准的主要研究内容是：

1） 首先分析了云计算身份鉴别服务的研究背景和意义，调研了国内外云计算领域身份鉴别服务的需求，理清复杂云计算环境中身份鉴别服务的重要性及其应用情况。

2） 随后，给出了云计算身份鉴别相关标准进行现状和趋势分析。其次，研究主流云提供商的云计算身份鉴别服务应用情况，从而为云计算身份鉴别服务密码标准体系的构建提供参考。

3） 最后，根据国内外云计算中身份鉴别的标准及技术的研究和应用情况，提出云计算身份鉴别服务密码标准体系架构。

“云计算身份鉴别服务密码标准体系”标准研究项目组于 2014 年 3 月正式成立，标准项目组成员单位涵盖了国内主要的科研机构、商用密码检测检测机构、电子认证企业、商用密码产品生产企业等。

本研究报告的主要编制单位：中国科学院数据与通信保护研究教育中心，国家密码管理局商用密码检测中心，北京数字认证股份有限公司，兴唐通信科技有限公司，北京三未信安科技发展有限公司，卫士通信息产业股份有限公司。

本研究报告的主要编制人：高能，江伟玉，刘丽敏，高志权，李敏，彭佳，屠晨阳，张众，李向锋，吕春梅，刘尚焱，关旭，宋飞。

1. 云计算身份鉴别服务的研究背景及意义

云计算技术的发展促进了在线访问云服务的流行。人们通过网络可以随时随地访问其个人文档、照片、消费记录，甚至银行账户、医疗记录等敏感信息；企业也可借助于云计算丰富的资源、强大的计算能力和快速可扩展的特性，将计算服务和数据存储服务外包给云服务提供商。不同安全级别的数据和服务充斥于云环境中，云中资源的访问及其数据本身的安全问题自然成为了关注的焦点。为了保证云中数据的安全性，云端的服务应鉴别访问者的身份。

（一）云计算身份鉴别的安全性尤为重要和迫切。

根据 OWASP 最新发布的 Web 应用安全威胁排名，鉴别与会话管理威胁排在第 2 位，敏感数据泄露排在第 6 位，可见在云计算服务中安全部署和实施身份鉴别技术的重要性和迫切性。NIST 在 2013 发布的《NIST Cloud Computing Standards Roadmap》[32]文件中建议云计算身份鉴别采用 SAML（Security Assertion Markup Language）、OpenID（OpenID Authentication）、OAuth（Open Authorization Protocol）等协议验证用户的身份并实现联合身份鉴别，以便获取云应用或云服务，一旦用户完成身份鉴别，则用户应该登录到云应用或云服务中，而无需再次鉴别。因此，云计算身份鉴别自身也可以作为一种云计算服务，为其他云计算服务或者应用提供身份鉴别服务。

（二）身份鉴别技术发展迅速，除了传统的用户名/口令方式，基于智能设备、智能卡、生物识别技术的身份鉴别以及多因素鉴别逐渐发展成熟。

作为云安全的第一道门槛，云身份鉴别服务使用的身份鉴别技术是各种安全措施可以正常实施的前提，也成为了工业界和学术界的研究重点。身份鉴别是确定实体（用户、服务器、应用程序等）身份的过程，可根据实体了解的知识、拥有的物品以及身体固有的生物特性来划分不同类型的身份鉴别技术。目前，身份鉴别技术已得到了较长时间的发展与研究。例如，基于用户名/口令的身份鉴别技术已得到了普遍的使用；基于智能卡识别、基于生物特征识别的身份鉴别技术（线上快速身份鉴别联盟，即 FIDO 联盟）也不断出现在新的应用场景中；单点登录、委托鉴别、身份联合、多因素鉴别等鉴别机制也已得到了较为成熟的研究，并被许多服务提供商应用于其产品中。

（三）云计算环境中身份鉴别面临新的需求和挑战-凭据管理、强身份鉴别、联合身份鉴别（跨域、跨服务）等。

在云计算环境中，由于云计算环境具有其特有的特性以及云计算客户新的需求，对身份鉴别技术有了不同的需求，身份鉴别技术也面临不同的挑战。另外，尽管国内外各标准组织在身份鉴别方面出台了一系列的标准，但是难以满足云计算环境身份鉴别服务对身份鉴别技术的新需求。首先，云环境中的用户身份凭据的管理面临的安全威胁比传统的应用场景中更加严峻，安全性要求更高；其次，对于云中高度敏感的数据，需要更加安全的、用户可控的身份鉴别机制，可以使用一次性口令、基于生物特征（指纹、人脸、虹膜、生物行为等）的鉴别技术以及基于 USB 等智能卡识别的技术等强鉴别机制；最后，云环境下需要方便快捷的技术来解决联合身份鉴别（跨安全域或跨服务）。

（四）国内外研究机构纷纷出台相关云计算身份鉴别标准，但没有形成一个完整的服务标准体系。

针对云环境中身份鉴别服务新的发展趋势，国际相关标准组织均在研究云环境中的

身份鉴别服务的技术和机制。美国国家标准技术研究所（NIST）、第一联合技术委员会（ISO/IEO）、结构化信息标准促进组织（OASIS）均有相关的工作组在研究云环境中的身份管理和鉴别授权问题。国际互联网工作组（IETF）针对第三方资源访问问题，出台了一系列可用于云中身份鉴别的 OAuth 相关文档；开放的身份标识联盟（OpenID）提出的 OpenID 框架和系列规范已应用在各主要云服务提供商的服务中；国际电信联盟 ITU 也在其下一代网络中提出了支持 OpenID 和 OAuth 的技术规范；另外，新成立的在线快捷身份鉴别联盟（FIDO）近两年也制订了一系列基于生物识别技术的身份鉴别标准。

我国也在推动云计算环境中的身份鉴别技术标准化。例如，目前正在研制相关密码行业标准《开放的第三方资源授权协议框架》、《开放的身份标识鉴别框架》、《在线快捷身份鉴别密码技术应用规范》。但是，相比于国际标准组织对云计算中身份鉴别标准的研究情况，我国的相关研究还相对滞后，缺乏云计算身份鉴别服务的体系化研究成果。因此，我国亟需结合我国的实际国情，进行云计算身份鉴别服务的体系化研究，尤其是云计算身份鉴别服务的密码标准体系化研究。

（五）云计算身份鉴别服务是构建在 SaaS 层的云服务，为不同云计算服务模式的云服务提供身份鉴别服务。

在美国国家标准与技术研究院(National Institute of Standards and Technology，简称 NIST）的 SP 800-145《云计算的定义》(The NIST Definition of Cloud Computing）[33]文档中，根据云服务提供商提供的资源服务类型不同，云计算的服务模式主要可分为以下三类：

- 基础设施即服务（Infrastructure as a Service，IaaS）：在 IaaS 模式下，云服务提供商向用户提供对所有计算基础设施的使用，包括处理 CPU、内存、存储、网络和其它基本的计算资源。用户能够部署和运行任意软件，包括操作系统和应用程序。用户不管理或控制任何云计算基础设施，但能控制操作系统的选择、存储空间、部署的应用，也有可能获得有限制的网络组件（例如，路由器、防火墙、负载均衡器等）的控制能力。
- 平台即服务（Platform as a Service，PaaS）：PaaS 平台是指云环境中的应用基础设施服务，也可以说是中间件即服务。PaaS 平台在云架构中位于中间层，其上层是 SaaS，其下层是 IaaS。在 PaaS 模式下，云服务提供商向用户提供运行在云计算基础设施之上的软件开发和运行平台，如：标准语言与工具、数据访问、通用接口等。云客户可以利用该平台开发和部署自己的软件，通常不能管理或控制支撑平台运行所需的底层资源，如网络、服务器、操作系统、存储等，但可控制自己部署的应用程序，以及控制运行应用程序的托管环境配置。
- 软件即服务（Software as a Service，简称 SaaS）：在 SaaS 模式下，云服务提供商通过网络向用户提供运行在云基础设施之上的应用软件、开发软件等。云客户无需购买软件，而是向云服务提供商租用基于 Web 的软件，来管理其业务活动，可利用不同设备上的客户端（如 WEB 浏览器）或程序接口通过网络访问和使用云服务提供商提供的应用软件，如电子邮件系统、协同办公系统、客户关系管理系统等。云客户通常不能管理或控制支撑应用软件运行的底层资源，如网络、服务器、操作系统、存储等，但可对应用软件进行有限的配置管理。与传统软件相比，SaaS 服务依托于软件和互联网，不论从技术角度还是商务角度都拥有与传统软件不同的特性，表现在：互联网特性 、多租户特性以及服务特性。

IaaS、PaaS、SaaS 三种云服务模式提供的服务类型不同，面向的用户类型、访问接入方式（对服务、设备、数据资源的访问接入方式）、被访问对象的资源管理方式（用户数据资源、计算和存储设备、应用程序或服务等）也不尽相同，但是这三种云服务模式都面临对用户身份进行鉴别的需求和挑战。不管是这三种云服务模式，还是其他应用方，使用以云服务的方式提供的身份鉴别服务都是未来的发展方向。从本质上讲，云身份鉴别服务是部署在 SaaS 层的一种服务，本研究报告主要研究部署在 SaaS 层的云身份鉴别服务的需求和挑战、研究现状、关键技术以及体系架构。

本研究报告主要针对云计算环境中身份鉴别服务进行研究，尤其是其中使用的身份鉴别技术。本报告首先将分析云计算身份鉴别服务的技术需求和挑战，理清复杂云计算身份鉴别服务中身份鉴别技术的应用情况；随后，给出国内外相关标准组织对云计算中身份鉴别技术的标准研究情况，并对身份鉴别技术相关标准进行现状和趋势分析；其次，研究具体的云计算身份鉴别关键技术和身份鉴别技术在主要云服务提供商处的应用情况，从而为云计算身份鉴别密码标准体系的构建提供参考。最后，根据云计算中身份鉴别技术的需求分析、标准研究情况以及身份鉴别技术研究和应用情况，提出云计算身份鉴别服务密码标准体系构建的建议。

2. 云计算身份鉴别服务需求和挑战

当企业和组织机构等将他们的应用部署到云环境时，将遇到身份鉴别相关的新的需求和挑战，以云服务的方式提供身份鉴别是一种合适的解决方案。在 CSA 的《Domain 12: Guidance for Identity & Access Management》[24]中提出，将应用部署到云计算环境中时面临的身份鉴别挑战有凭据管理、强身份鉴别、委托身份鉴别（跨域或者跨服务身份鉴别）等等，以云服务的方式提供的身份鉴别服务同样面临以上安全挑战。

2.1. 凭据管理

凭据包括口令、数字证书、动态凭据等等。凭据管理包含凭据的发放和管理，在云环境中面临的挑战更加严峻。例如使用用户名口令来验证用户的身份鉴别应考虑以下挑战：

a) 保护口令的存储和口令的安全传输；
b) 冒充：当多个云服务使用相同的口令时，内部人员或者能够获得到口令存储访问权限的攻击者可以在其他站点冒充用户；
c) 保护口令防止受到字典暴力破解，以及防止针对口令重置自服务等的攻击；
d) 钓鱼攻击：云用户可能会被恶意钓鱼网站欺诈从而交付出其用户名和口令。钓鱼攻击还可以通过安装恶意软件或者键盘记录来捕获用户的用户名和口令。
e) 应定义并强制实施一个口令/凭据安全策略，包括
   - 凭据生命周期。口令有效期有多久？
   - 凭据长度：口令长度，证书密钥长度等等；
   - 存储凭据的安全性：是否经过单向散列？
   - 口令重置自服务；
   - 口令重置前的身份验证等等。

同样针对其他身份凭据，也存在以上安全需求和挑战。云计算身份鉴别服务应从以上几个方面考虑其凭据管理的技术要求和规范。

2.2. 强身份鉴别

高风险和高价值的应用程序会选择强身份鉴别技术，例如一次性口令或者数字证书。尤其是大企业，安全性较高的多因素身份鉴别的应用越来越普遍。根据成本、管理成本以及用户接受度，可以选择不同机制的强身份鉴别。为了解决用户的需求而支持多种强身份鉴别机制成本效益并不是很高，这个同样也是云服务提供商遇到的挑战。

用户会通过下几个方面选择云服务提供商：

a) 至少支持用户名口令的方式鉴别用户，并能够随着支持的服务风险的增加能够支持更多的强身份鉴别机制；
b) 企业管理范围应包含特权用户的管理；
c) 密码重置自服务功能应首先验证用户的身份；
d) 应能够定义并实施强口令策略；
e) 联合身份鉴别：委托身份鉴别的一种实现方法，见第 3.3 节；
f) 用户为中心的身份鉴别（例如 OpenID）-尤其是当应用能够被个人用户访问时应支持这种方式。用户为中心的身份鉴别，例如谷歌 ID 可以使得用户使用已经存在的凭据登录第三方应用，而不需要在该应用方存储凭据。

因此，云计算身份鉴别服务也应从以上几个方面考虑强身份鉴别的技术机制和规范，可以使用 Kerberos、令牌（如 SAML 令牌）、智能设备、智能卡或者 FIDO 协议等形成强身份鉴别机制。

2.3. 委托身份鉴别

云计算服务或者其他应用由于成本等原因无法实现对用户的身份鉴别，或者身份鉴别参与方需要对用户的身份进行身份属性交换等场景，会使用其他云计算身份鉴别服务提供商提供的身份鉴别服务。联合身份鉴别是委托身份鉴别的一种实现方法。

联合身份鉴别是在跨域身份鉴别需求下，企业采用的一种管理用户电子身份和属性的方法，能够用来实现企业间的联合身份鉴别和 web 服务之间的联合身份鉴别。联合身份技术与单点登录技术有很大的关联性，在实现了身份联合的基础上，结合单点登录技术，便可方便地跨域或跨应用访问。其中，Microsoft 利用活动目录技术提供了联合身份的单点登录服务，可实现不同安全域中的合作伙伴的相互访问；IBM 的 Tivoli 联合身份管理器向多种应用的用户提供 Web 和联合单点登录。针对私有云部署、公共云部署和混合云部署，它结合使用单点登录技术进行高度安全的信息共享。

在云环境中，联合身份鉴别在实现联盟组织之间的身份鉴别方面扮演重要角色，能够为多个不同的云计算安全域之间的服务提供单点登录、统一身份鉴别和交换身份属性等功能。

为了实现一个可操作的联合身份鉴别的云环境，应根据开放的标准来实现一个身份鉴别解决方案，主要包括《GB/T 29242-2012 信息安全技术 鉴别与授权 安全断言标记语言规范》（Security Assertion Markup Language，SAML），Web 服务联邦语言（Web Services Federation Language，WS-Federation）等。

3. 云计算身份鉴别标准研究现状

国内外大部分标准化组织和机构都致力于身份鉴别的研究，并在云计算下的身份鉴别领域，开展了一系列的探索和研究工作。

国际标准组织及其相关工作主要包括：

- 美国国家标准与技术研究院（National Institute of Standards and Technology，简称 NIST）。NIST 成立云计算工作组，目标是确立在云计算方面的领导力并提供相关指导。**NIST 发布的《云计算标准路线图》（NIST Cloud Computing Standards Roadmap）为云计算标准体系化奠定了一定的基础，在该文档中涵盖了云计算身份鉴别与授权建议采用的各个组织机构的标准规范（例如 OASIS 的 SAML 标准，OpenID 联盟的 OpenID 标准，IETF 的 OAuth 标准等），是云计算身份鉴别服务标准体系架构的重要参考文件。**
- 第一联合技术委员会（Information technology-Security techniques-A framework for identity management，简称 ISO/IEO）。ISO/IEO 在 JTC1 下成立 SC27 工作组，主要完成云计算领域的标准化工作，规范了云计算的基本概念和常用词汇，并从使用者角度和功能角度阐述云计算参考架构，不仅为云服务提供者和开发者搭建了一个基本的功能参考模型，也为云服务的评估和审计人员提供相关指南。**ISO/IEC 提出的《个人可识别信息（PII）处理者在公共云中保护 PII 的实践规程》为云计算身份鉴别服务中用户的个人可识别信息的定义和管理提供重要参考。ISO/IEC 提出的身份管理架构对云计算环境中的身份鉴别体系和身份管理架构有重要的参考意义。**
- 结构化信息标准促进组织（Organization for the Advancement of Structured Information Standards，简称 OASIS）。**OASIS 发布的 SAML、WS-Federation 系列标准已被广泛应用，主要应用于单点登录、身份联合和授权技术，在云计算身份鉴别服务中提供强身份鉴别和联合身份鉴别。**
- 国际互联网工程任务组（The Internet Engineering Task Force，简称 IETF）。**IETF 发布的 OAuth 系列实现了第三方应用使用授权服务器发放的访问令牌访问受保护资源。另外，IETF 提出的《跨域身份管理系统》（RFC 7642、RFC7643、RFC7644）为云计算身份鉴别服务的跨域身份鉴别和身份管理提供重要的参考。**
- 国际电信联盟-电信标准化部（International Telecommunication Union－Telecommunication Standardization Sector，简称 ITU-T）。**该组织发布了对 OpenID 和 OAuth 的支持标准，推进了 OAuth 和 OpenID 在云计算中的应用，且其成立的身份管理工作组发布的《多身份服务提供商环境中的联合鉴别通用框架》以及其他身份管理相关标准对云计算环境中的跨域身份鉴别和身份管理架构有重要的参考意义。**
- 开放的身份标识联盟（OpenID）。**该组织制定的 OpenID 系列标准是一种分布式的可解决用户使用同一种身份凭据访问多个网络应用或云服务的身份鉴别问题的解决方案，是以用户为中心的数字身份识别框架，该标准在云计算身份鉴别中应用较为广泛，是云计算身份鉴别标准体系重要组成部分。**
- 线上快速身份鉴别联盟（Fast IDentity Online，简称 FIDO）。该组织提出的 FIDO 规范针对安全设备和 Web 浏览器的规范，允许任何网站和云应用与支持

FIDO 的设备通信，实现便捷、安全的在线用户鉴别。**FIDO 系列标准提高了云计算身份鉴别服务的安全性，以应对云计算身份鉴别服务的强身份鉴别挑战。**

我国也紧跟国际标准发展方向，在身份鉴别方面进行研究，发布了《引入可信第三方的实体鉴别及接入架构规范》、《鉴别与授权 数字身份信息服务框架标准》等标准，形成《开放的身份标识鉴别框架》、《开放的第三方资源授权协议框架》、《基于可信执行环境的生物识别身份鉴别协议》等草案。

但是国内外的相关机构并没有形成一整套的云计算身份鉴别服务密码标准体系，在这方面的研究都比较欠缺。

本章后续小节将详细介绍国内外的相关标准研究情况。

3.1. 国际相关身份鉴别标准研究情况

3.1.1. NIST 的相关研究-标准路线图

NIST 的职责是推动测量科学、标准和技术的发展，改善经济安全与国民生活质量，并提高美国的创新能力和产业竞争力。NIST 云计算工作组的长期目标是确立在云计算方面的思维领导力并提供相关指导，以促进云计算在产业界和政府的应用。

NIST 在云计算领域的五大工作组：

— **参考架构与分类工作组**

云计算架构参考模型是对云计算概念与关系的抽提，为机构应用云计算概念提供了标准与指导。

— **云计算应用标准推进工作组**

工作组的主要任务是通过工作实例展示云系统是如何支持关键用例的，其中的云系统执行了一套获得鉴别的公共云系统规范，该工作的目标是推动高质量云计算标准的形成。

— **云安全工作组（Cloud Security）**

云计算安全工作组的成立是 NIST 促进云服务在整个美国政府部门安全采用的举措之一。该小组制定了以下标准：

a) 《云计算参考体系架构》(NIST Cloud Computing Reference Architecture)(标准)，该标准定义云计算体系架构、架构组成部件及面临的安全与隐私。

b) 《完全虚拟化技术安全指南》(Guide to Security for Full Virtualization Technologies)(标准)，该标准对虚拟机隔离、虚拟机监控以及虚拟机面临的安全威胁进行了描述。

c) 《公有云中的安全和隐私》(NIST: Guidelines on Security and Privacy in Public Cloud Computing)，该标准对公有云中身份管理和隐私保护进行标准化。

— **标准路线图工作组（Standards Roadmap）**

NIST 负责领导美国政府云计算技术路线图的制定。该路线图将确定美国政府对云计算互操作性、可移植性和安全的需求及这些需求的优先程度，以支持云计算在美国政府的安全有效应用。

— **业务用例工作组（Business Use Cases）**

NIST 将领导相关的政府部门和产业界界定目标云计算业务用例，以确定具体的风险、问题和限制。

该机构发布的与云计算相关的标准主要有：

a) SP 800-146《云计算梗概和建议》（NIST Cloud Computing Synopsis and Recommendations）
b) SP 500-291《云计算标准路线图》（NIST Cloud Computing Standards Roadmap）
c) SP 800-145《云计算的定义》（The NIST Definition of Cloud Computing）
d) SP 500-292《云计算参考体系架构》（NIST Cloud Computing Reference Architecture）
e) SP 500-293《美国政府云计算技术路线图》(NIST US Government CLoud Computing Technology Roadmap Volume I Release 1.0)（草案）
f) NIST IR 7904 《云中的可信定位：概念实现证明》(Trusted Geolocation in the Cloud: Proof of Concept Implementation)（草案）

NIST 对于云计算下的身份鉴别技术已经开始研究。NIST 对云计算中的参考体系架构、公有云中的安全和隐私、云计算下的用户身份鉴别等方面的研究推动了云计算身份鉴别技术的发展。**NIST 发布的《云计算标准路线图》(NIST Cloud Computing Standards Roadmap）为云计算标准体系化奠定了一定的基础，在该文档中涵盖了云计算身份鉴别与授权建议采用的各个组织机构的标准规范，是云计算身份鉴别服务标准体系架构的重要参考文件。**

3.1.2. ISO/IEO 的相关研究-个人可识别信息、身份管理

ISO/IEO 目前已有的与云计算或云安全相关标准如下：

a) ISO/IEC CD 17788 分布式应用平台和服务-云计算-概述和词汇（Distributed application platforms and services -Cloud computing - Overview and Vocabulary)，该标准规范了云计算的基本概念和常用词汇
b) ISO/IEC CD 17789 云计算-参考架构（Cloud Computing-Reference Architecture）
c) ISO/IEC 27017 基于 ISO/IEC 27002 云计算服务器信息安全控制实施规程(Code of practice for information security controls for cloud computing services based on ISO/IEC 27002)（标准草案）
d) 云计算安全与隐私管理系统(标准草案)，为云计算服务过程中的安全控制提供指导，目前正在制定过程中。
e) ISO/IEC 17826:2012 云数据管理接口（Cloud Data Management Interface ，简称 CDMI）
f) ISO/IEC 27018: 2014《个人可识别信息（PII）处理者在公共云中保护 PII 的实践规程》(Code of practice for PII protection in public clouds acting as PII processors)
g) ISO/IEC 24760-1: 2015《身份管理框架第 1 部分：术语和概念》(A framework for identity management - Part 1: Terminology and concepts)
h) ISO/IEC 24760-2: 2015《身份管理框架第 2 部分：参考体系结构和要求》(A framework for identity management - Part 2: Reference architecture and requirements)

以上云计算国际标准，规范了云计算的基本概念和常用词汇，并从使用者角度和功能角度阐述云计算参考架构，不仅为云服务提供者和开发者搭建了一个基本的功能参考模型，也为云服务的评估和审计人员提供相关指南。在鉴别方面，主要包含了实体鉴别、

匿名鉴别、抗抵赖等方面，并逐渐发展成体系，这些标准是我国标准研制工作的重要指导。**个人可识别信息方面成为一个重要发展方向，ISO/IEC 提出的《个人可识别信息(PII)处理者在公共云中保护 PII 的实践规程》为云计算身份鉴别服务中用户的个人可识别信息的定义和管理提供重要参考，我国在此方面滞后发展。ISO/IEC 提出的身份架构对云计算环境中的身份鉴别体系和身份管理架构有重要的参考意义。然而，针对云环境下的身份鉴别服务，目前还没具体且明确的标准。**

3.1.3. OASIS 的相关研究-SAML、WS-Federation、身份管理

OASIS 组织在鉴别、授权、身份管理、云身份管理等方面均有研究。

— 鉴别方面：

a) SAML 标准是一种基于 XML 的单点登录开放标准，是实现站点之间相互操作的安全访问控制框架，适用于复杂环境下交换用户的身份识别信息，已被多个云服务提供商采用。用户仅需在一个安全域中登录，就可以使用由其他信任该域的站点提供的服务，此外，SAML 可以实现不同安全域之间的鉴别和数据交换，这些都为云环境下身份鉴别的发展提供了一定的技术方案支持。SAML2.0 已被国标 GB/T 29242-2012《信息安全技术　鉴别与授权　安全断言标记语言》采标。

b) 2009 年 5 月推出的 WS-Federation 标准主要用于身份联合场景，以解决联邦鉴别和授权信息交换问题。目前微软云服务（Microsoft Azure）、IBM 的联合身份管理（Tivoli Federated Identity Manager）使用了 WS-Federation 标准。

— 授权方面：

XACML（eXtensible Access Control Markup Language）标准现已被广泛应用，并提供基于 XACML 的配套技术规范。XACML2.0 已被国标 GB/T 30281-2013《信息安全技术　鉴别与授权　可扩展访问控制置标语言》采标。另外， OASIS 国际开放标准联盟成立了云授权技术委员会，旨在改进 SaaS、PaaS、IaaS 中的管理授权模型。

— 身份管理方面：

该组织的云身份（IDCloud）技术委员会于 2010 年成立，致力于解决云计算中身份管理带来的严重的安全挑战。主要的工作内容包括身份管理标准研究与制定、描述身份管理在云环境中的安全挑战、研究身份管理配置需求等。该组织的《身份在云中的使用》于 2011 年 2 月发布，对租户身份的部署，配置和管理用例进行定义。目前产出的成果包括《云中的身份用例版本 1.0》(Identity in the Cloud Use Cases Version 1.0)。

OASIS 提出的 SAML 标准和 XACML 标准主要应用于云计算身份鉴别和授权中的强身份鉴别、跨域身份鉴别以及授权，提高了云计算身份鉴别服务以及授权的安全性和可用性。OASIS 提出的 WS-Federation 系列标准在云计算身份管理和身份联合领域应用广泛，提高了身份管理和身份鉴别的安全性和便利性。SAML、WS-Federation 以及身份管理相关标准是云计算身份鉴别服务标准体系中强身份鉴别和联合身份鉴别的重要参考文件。

3.1.4. IETF 的相关研究-OAuth、跨域身份管理

IETF 的主要任务是负责互联网相关技术标准的研发和制定，是国际互联网业界具有一定权威的网络相关技术研究团体。IETF 大量的技术性工作均由其内部的各种工作组（Working Group，简称 WG）承担和完成。这些工作组依据各项不同类别的研究课题而组建。相关标准研究工作组有：

a) OAuth: OAuth 授权协议工作组（Web Authorization Protocol）。
   - OAuth 标准

b) SCIM: 跨域身份管理系统工作组（System for Cross-domain Identity Management），主要从事跨域身份管理相关工作。
   - RFC 7642：2015 《跨域身份管理系统：定义、概述、概念和要求》（System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements ）
   - RFC 7643:2015《跨域身份管理系统:核心机制》(System for Cross-domain Identity Management: Core Schema ）
   - RFC 7644：2015《跨域身份管理系统：协议》（System for Cross-domain Identity Management: Protocol ）

c) ACE: 受限环境下的鉴别与授权工作组（Authentication and Authorization for Constrained Environments）。

d) AAA: 鉴别、授权和审计工作组（Authentication, Authorization and Accounting），该工作组于 2006 年已经终止，其工作逐渐分布到其他工作组。

其中推出的第三方授权协议及框架 OAuth 系列技术规范已被广泛应用于云环境中的身份鉴别与授权领域。

OAuth 起源于 Twitter 身份鉴别服务器的委托鉴别问题。当时，某网络收藏夹应用需要委托 Twitter 的身份鉴别服务器来实现鉴别，允许通过 Twitter 鉴别的用户采用 Mac OS X 操作系统平台的应用程序 Dashboard 访问网络收藏夹服务，但尚没有开发标准解决委托鉴别问题。于是，2007 年 4 月成立了 OAuth 讨论组，并于 2007 年 10 月发布了 OAuth core 1.0 草案。2008 年 11 月，IETF 将 OAuth 纳入规范化工作中。但是，随着 OAuth 1.0 的广泛应用，OAuth1.0 的漏洞也不断暴露。2009 年 4 月 23 日，OAuth 宣告了一个 1.0 协议的安全漏洞。该漏洞影响了 OAuth 1.0 核心规范第 6 节的 OAuth 的鉴别流程（也称作 3 阶段 OAuth）。于是，OAuth 工作组发布了 OAuth Core 协议 1.0a 版本来解决这一问题。2010 年 4 月发布 RFC 5849（OAuth 1.0 协议）。随着对 OAuth1.0 进行不断修正，IETF 于 2012 年 12 月发公布了 OAuth 2.0（RFC6749）版本，即 OAuth 协议的最新版本，该版本考虑了不同 OAuth 工作流中的安全漏洞，给出了相应的安全考虑和应对措施。

与传统的授权机制不同，OAuth 协议通过引入授权层，将用户使用的客户端应用程序（即第三方应用程序）和资源拥有者的角色分开。在 OAuth 中，用户请求访问资源拥有者在服务器中的资源时，需要得到资源拥有者的授权。资源拥有者可以不向客户端应用程序揭露其身份凭证，通过发放一个访问令牌（一个字符串，包含具体的使用范围，使用时间，以及其他一些访问属性）给客户端应用程序的方式实现授权。在获得资源拥有者的授权后，客户端应用程序就可以使用这个访问令牌访问存储在资源服务器上的受保护资源。

OAuth 2.0 关注开发的简易性，及 Web 应用、桌面应用和移动终端的广泛适用性，因而得到广泛的应用。尽管 OAuth2.0 已经被腾讯 QQ、新浪微博、阿里巴巴淘宝、支付宝、搜狐网、网易、人人网、开心网、亚马逊、微软 Live、WordPress、eBay、PayPal、Facebook、Google、Yahoo、LinkedIn、VK.com、Mail.Ru、Odnoklassniki.ru、GitHubOAuth 等使用，但是由于实现时缺乏全面地安全考虑，实现技术门槛低，开发者往往忽视安全问题。某研究通过分析通过浏览器的数据分析了实现的逻辑漏洞，攻破了 Google、Facebook 等的实现机制。另有文章则专门分析了 OAuth 协议在实现中存在的安全威胁，

发现了访问令牌窃听、通过 XSS 窃取访问令牌、假冒、会话交换和强制登录型 CSRF 等 5 类攻击。2014 年 5 月，有文章指出 OAuth 和 OpenID 开源登录工具存在“隐蔽重定向漏洞”。目前，OAuth 针对发现的安全漏洞，已制定了专门的 OAuth 威胁模型和安全考虑文档，以指导开放者避免实现漏洞。

目前，OAuth 系列技术规范文档主要有：

- RFC 6749 OAuth 2.0 授权框架
- RFC 6750 OAuth 2.0 授权框架：不记名令牌使用
- RFC 6755 OAuth 的 IETF URN 子命名空间
- RFC 6819 OAuth 2.0 威胁模型和安全考虑
- RFC 7009 OAuth 2.0 令牌撤销
- RFC 7519 JSON 网页令牌（JWT）
- RFC 7521 OAuth 2.0 客户端鉴别与授权凭据的断言框架
- RFC 7522 OAuth 2.0 客户端鉴别与授权凭据的 SMAL 2.0 轮廓

IETF 多年来不间断鉴别与授权相关标准的研究工作，多领域发展，涉及 AAA、网络传输协议、无线局域网、多媒体等多方面的鉴别与授权。其中第三方授权框架及相关协议体系化（即 OAuth）发展迅速，近年来已被网络服务和应用广泛采用，在云计算中的应用也发展迅速，成为云计算身份鉴别服务的重要参考。跨域身份管理方面成为近几年的研究重点，跨域身份管理系统相关的三个标准也为云计算身份鉴别服务的联合身份鉴别提供重要参考。

3.1.5. ITU-T 的相关研究-联合身份管理

ITU-T 是一个研究和制定除无线电以外的所有电信领域设备和系统标准的国际性组织。ITU 对云环境下身份鉴别技术的研究逐步完善，正在研制《云计算中的身份管理需求》。ITU-T 的电信云安全研究小组 SG17 于 2009 年成立，该小组制定了《电信领域云计算安全指南》。2012 年 2 月，ITU-T SG13 WP6（云计算研究组），下设 Q26（云需求）、Q27(云架构)和 Q28(资源管理)三个工作组从事云计算标准的研制工作。SG13 和 ISO/IEC JTC1 /SC38 成立联合工作组，共同研制《云计算概述和词汇》和《云计算参考架构》标准。

ITU-T 于 2010 年 6 月成立了云计算焦点组 FG Cloud，致力于从通信角度为云计算提供支持，该组运行时间截止到 2011 年 12 月，后续云工作已经分散到别的研究组(SG)。云计算焦点组发布了包含《云安全》和《云计算标准制定组织综述》在内的 7 份技术报告。其中《云安全》报告旨在确定 ITU-T 与相关标准化制定组织需要合作开展的云安全研究课题。《云计算标准制定组织综述》报告包括：云生态系统、使用案例、需求和商业部署场景；功能需求和参考架构；安全、审计和隐私（包括网络和业务的连续性）；云服务和资源管理、平台及中间件；实现云的基础设施和网络；用于多个云资源分配的跨云程序、接口与服务水平协议；用户友好访问、虚拟终端和生态友好的云。

ITU 在联合身份、OpenID、OAuth、多因素鉴别等方面均有相关研究，这些身份鉴别技术均广泛应用于云计算中。制定的相关标准有：

- 《下一代网络的 OAuth 支持》（ITU-T Y.2723 Support for OAuth in next generation networks，2013 年 11 月发布）
- 《下一代网络中 OpenID 的支持》（ITU-T Y.2725 Support of OpenID in next generation networks，2014 年 7 月发布）
- 《使用移动设备的多因素鉴别机制》（ITU-T X.1158 Multi-factor

authentication mechanisms using a mobile device，2014 年 11 月发布）

— 《应用程序间共享网络鉴别结果的指南和框架》（ITU-T X.1256 Guidelines and framework for sharing network authentication results with service applications，2016 年 3 月发布）

— 《多身份服务提供商环境中的联合鉴别通用框架》（ITU-T X.1154 General framework of combined authentication on multiple identity service provider environments，2013 年 4 月发布）

— 《云计算中的身份管理需求》（ITU-T X.idmcc Requirement of IdM in cloud computing，在研标准）

— 《身份管理鉴别集成》（Authentication integration in identity management，在研标准）

— 《身份管理信息发现》（X.discovery Discovery of identity management information）

ITU 比较重视鉴别领域的标准研究工作，早期其工作重点是基于口令的鉴别、移动通信、家庭网络鉴别、数据通信网络中多媒体（网络会议等）鉴别、下一代通信网络鉴别等方面。**随后紧跟云计算的发展，在联合身份、OpenID、OAuth、多因素鉴别等方面均有相关研究，提出了《多身份服务提供商环境中的联合鉴别通用框架》，并且在云计算中的身份管理方面有多个在研标准，包括云计算身份管理需求、身份管理与鉴别的集成以及身份管理信息发现等。这些标准为云计算身份鉴别服务标准体系架构以及联合身份鉴别提供重要参考。**

3.1.6. OpenID 联盟的相关研究-开放身份标识

OpenID 技术最早由美国著名软件作者 Brad Fitzpatrick 创建。而后，Six Apart 和包括 veriSign 在内的其他几家公司对 OpenID 进行了技术支持。2007 年，OpenID 联盟（OIDF）成立，这个非盈利组织对 OpenID 技术进行管理和推广，Facebook、Intel 等公司都是 OIDF 的成员。在 2007 年，OpenID 推出 OpenID 2.0（已经废弃）。随后，Light-Weight Identity、Yadis、Sxip DIX protocol 和 XRI/i-names 等成员加入了 OpenID 联盟。目前，OpenID 联盟包括 Google、Microsoft、PayPal、Ping Identity, Symantec、Verizon、Yahoo!、Salesforce、VMWare、Cisco 等 34 个公司和 2 个非盈利组织。其中大部分成员都是 OpenID 的使用者，部分成员提供了 OpenID 服务。目前的 OpenID 是定义在《开放的第三方资源授权协议框架》（OAuth2.0）协议之上的一个简单身份鉴别框架。该框架使得依赖方（即为第三方应用程序）可以基于 OpenID 提供方（通常是一个授权服务器）执行的鉴别流程，来验证终端用户的身份，并获取关于终端用户的基本配置信息。对用户而言，OpenID 简化注册登录流程、减少了密码泄露风险，此外，用户拥有账号信息控制权。对网站而言，实现用户资源共享，避免建立会员系统或登录功能所需要的开发成本、机器、带宽、安全费用，用户数据不统一储存，用户可以任意选择、更换存储的服务器，提升了用户数据的安全性。在云环境下的身份鉴别中，有效降低用户负担和依赖方的身份管理成本。

OpenID 联盟制定的 OpenID 框架和系列规范已应用在各主要云服务提供商的服务中。OpenID 是一个以用户为中心的数字身份识别框架，是一个以 URL 为身份标识的分散式身份验证解决方案，由可信身份信息提供方提供身份鉴别服务。OpenID 系列标准成为云计算身份鉴别服务标准体系中用户身份标识以及鉴别协议的重要参考文件。

3.1.7. FIDO 联盟的相关研究-生物识别身份鉴别

针对传统的用户名/口令方式，在用户登录多个不同的网络应用或云服务时，用户需要记忆多个用户名/口令。如果口令简单，容易被破解；如果口令复杂，用户容易忘记。FIDO 联盟的 FIDO 系列标准致力于解决用户需要创建并记住多套用户名和口令的问题。

FIDO 联盟成员包括 Google、PayPal、MasterCard、微软、黑莓以及国内的厂商联想等。目前赞助者会员有 5 家中国公司，参与者会员有 15 家中国公司。FIDO 联盟于 2014 年 12 月发布 FIDO 1.0 在线加密与免口令鉴别标准，该标准使用生物信息和硬件密钥代替口令。FIDO 1.0 主要包括两类鉴别，即通用授权框架 Universal Authentication Framework（UAF）和通用第二因素鉴别 Universal Second Factor（U2F）。这一标准系列涉及到芯片厂商、手机制造商、App 开发商和互联网或者云服务提供商等整个产业链。目前已经有 Nok Nok Labs，Synaptics，PayPal，三星，Google，Yubico 和 Plug-Up 等公司厂商采用这一系列标准。例如三星 Galaxy S5 的指纹支付采用了 FIDO 的标准，支付宝钱包在华为 Mate7 上提供的指纹支付是在 FIDO 的标准之上进行改进后的产品。

FIDO 系列标准使用生物识别身份鉴别技术以及公钥密码技术提高了云计算身份鉴别服务的安全性，以应对云计算身份鉴别服务的强身份鉴别挑战。目前该领域的标准在我国发展滞后，作为云计算身份鉴别服务标准体系的一部分，FIDO 系列标准成为云计算身份鉴别服务强身份鉴别的重要参考文件。

3.1.8. 小结

国际上相关标准组织对云计算领域的身份鉴别技术很重视，从以上介绍中可以得出，各国际标准组织在身份鉴别方面的协议已有系列化研究：针对用户使用多个服务或应用的场景的鉴别技术已成为近两年的重点工作；第三方授权框架及相关协议已得到了系列化的研制并被多个云服务提供商采用，SAML 系列标准已被广泛应用；利用 OpenID、SAML 等标准技术来实现单点登录已成为一种常用的选择，身份的联合可依赖于 SAML、WS-Fedartion 等标准来实现完成；多因素鉴别也已在云环境中普遍使用；基于智能卡识别、OTP、生物特征的识别技术也将不断在云环境身份鉴别领域普及；身份管理以及隐私管理等也将成为近年来的重点研究方向，跨域身份管理也是重要发展趋势。

目前国际相关组织机构研究特点和趋势：

- 重视基础研究，针对 PKI、数字证书、电子签名等基础领域持续性的研究与发展。
- 鉴别与授权领域多样化发展，涉及领域广泛，紧跟网络应用的发展
  - 鉴别与授权相关框架、协议、接口、语言规范全方位研究
  - 紧跟新的网络技术和应用模式，不断更新和变化，出台新的标准，如多媒体、无线网络、移动网络、智能设备、跨域的联合身份等
- 身份与访问管理是近年来的工作重点
  - 重点研究身份管理方面的框架、互操作、元数据管理等通用技术
  - 不断追踪新应用场景和领域中的要求进行同步化研究，如跨域环境、云计算环境等
- 新领域、新应用中的鉴别与授权技术是发展趋势
  - 紧跟云计算、物联网、受限环境等新领域的需求，研究新领域中鉴别与授权技术。

- 基于生物特征的识别、光存储卡鉴别以及 NFC 的身份鉴别等成为研究重点研究趋势

3.2. 我国相关身份鉴别标准研究情况

近年来，我国标准化组织一直不间断在身份鉴别、身份管理相关技术方面的研究。

3.2.1. 国家标准

- **公钥基础设施**

云计算环境中应用较为广泛的一种鉴别方式是基于 PKI 的身份鉴别，目前我国还没有针对云计算环境下的基于 PKI 身份鉴别的标准，但是，我国在公钥基础设施相关标准方面发展完善，紧跟国际标准发展方向。例如，PKI 系统类的标准《PKI 组件最小互操作规范》、《PKI 系统安全等级保护技术要求》、《安全支撑平台技术框架》等均以国标的形式发布，电子签名方面的标准如《带消息恢复的数字签名方案》、《带附录的数字签名第 2 部分：基于身份的机制》等也已指导相关电子签名系统或应用的实施多年。

- **鉴别与授权**

在鉴别与授权方面，全国信息安全标准化技术委员会已开展了相关工作，包括《引入可信第三方的实体鉴别及接入架构规范》、《轻量级鉴别与访问控制机制》等，对《数字身份信息服务框架标准》和《网络电子身份格式规范》进行了立项，通过对国内外数字身份管理技术进行研究总结，为数字身份服务框架建立规范。形成了《安全断言标记语言规范》和《可扩展访问控制置标语言》等标准。

- **身份管理**

相比于国际标准组织在身份管理方面的研究情况，我国在此方面发展相对缓慢，目前形成《网络电子身份标识验证服务协议规范》、《移动接入的身份鉴别和身份管理》、《云计算身份管理标准研究》、《云计算身份管理标准化研究》等草案。

- **云计算安全**

在 2014 年我国发布的《GB/T 31168-2014 信息安全技术 云计算服务安全能力要求》中，对标识符管理、鉴别凭证管理、鉴别凭证反馈等方面提出了安全能力要求。

➢ 标识符管理

■ 一般要求

云服务商应通过以下步骤管理云计算平台中的标识符：

a) 明确由授权人员分配个人、组、角色或设备标识符；
b) 设定或选择个人、组、角色或设备的标识符；
c) 将标识符分配给有关个人、组、角色或设备；
d) 在[赋值：云服务商定义的时间段]内防止对用户或设备的标识符的重用；
e) 在[赋值：云服务商定义的时间段]后禁用不活动的用户标识符。

■ 增强要求

云服务商应：

a) 对[赋值：云服务商定义的人员类型]进行进一步标识，如合同商或境外公民，便于了解通信方的身份（如将电子邮件的接收方标识为合同商，以便与本组织人员相区分）；
b) 在标识跨组织、跨平台的用户时，应确保与相关机构相协调，以满足多个组织或平台的标识符管理策略。

➢ 鉴别凭证管理

■ 一般要求

云服务商应：

a) 通过以下步骤管理鉴别凭证：
   1) 验证鉴别凭证接收对象（个人、组、角色或设备）的身份；
   2) 确定鉴别凭证的初始内容；
   3) 确保鉴别凭证能够有效防止伪造和篡改；
   4) 针对鉴别凭证的初始分发、丢失处置以及收回，建立和实施管理规程；
   5) 强制要求用户修改鉴别凭证的默认内容；
   6) 明确鉴别凭证的最小和最大生存时间限制以及再用条件；
   7) 对[赋值：云服务商定义的鉴别凭证]，强制要求在[赋值：云服务商定义的时间段]之后更新鉴别凭证；
   8) 保护鉴别凭证内容，以防泄露和篡改；
   9) 采取由设备实现的特定安全保护措施来保护鉴别凭证；
   10) 当组或角色账号的成员资格发生变化时，变更该账号的鉴别凭证。
b) 对于基于口令的鉴别：
   1) 建立相关机制，能够强制执行最小口令复杂度，该复杂度满足[赋值：云服务商定义的口令复杂度规则]；
   2) 建立相关机制，能够在用户更新口令时，强制变更[赋值：云服务商定义的数目]个字符，确保新旧口令不同；
   3) 对存储和传输的口令进行加密；
   4) 强制执行最小和最大生存时间限制，以满足[赋值：云服务商定义的最小生存时间和最大生存时间]。
c) 对于基于硬件令牌的鉴别，定义令牌安全质量要求，并部署相关机制予以满足，如基于 PKI 的令牌。

■ 增强要求

云服务商应：

a) 对于基于 PKI 的鉴别：
   1) 通过构建到信任根的认证路径并对其进行验证，包括检查证书状态信息，以确保认证过程的安全；
   2) 对相应私钥进行保护。
b) 确保未加密的静态鉴别凭证未被嵌入到应用、访问脚本中；
c) 接受[赋值：云服务商定义的鉴别凭证]时，必须通过本人或可信第三方实施。

➢ 鉴别凭证反馈

■ 一般要求

云服务商应确保信息系统在鉴别过程中能够隐藏鉴别信息的反馈，以防止鉴别信息被非授权人员利用。

■ 增强要求

无。

3.2.2. 密码行业标准

我国对国际上云计算中身份鉴别方面的主要技术和协议（如 OpenID、OAuth、FIDO）进行了采标，并根据我国实际情况进行了补充完善，形成《开放的身份标识鉴别框架》、

《开放的第三方资源授权协议框架》、《基于可信执行环境的生物识别身份鉴别协议》等草案。

- **《开放的身份标识鉴别框架》**

该标准规定了建立在《开放的第三方资源授权协议框架》之上的终端用户身份鉴别协议框架，定义了框架参与实体的要求、鉴别协议流程以及关于终端用户信息的声明等。适用于终端用户访问网络应用时的身份鉴别需求，尤其适用于用户访问多种不同安全域的应用场景中，用户身份鉴别的开放、测试、评估和采购。

- **《开放的第三方资源授权协议框架》**

该标准规定了第三方资源授权协议的流程、不同类型的授权许可、协议各端点的功能要求以及系统实体之间传递消息的格式和参数要求等。适用于在互联网跨安全域应用场景中，身份鉴别与授权服务的开发、测试、评估和采购。

- **《在线快捷身份鉴别密码技术应用规范》**

该标准规定了基于生物特征识别的在线快捷身份鉴别协议。

3.2.3. 小结

目前全国信息安全标准化技术委员会共发布鉴别类标准 16 余项，涵盖了 LDAP、SAML、实体鉴别及匿名实体鉴别、第三方的鉴别与接入、身份管理以及云计算服务的安全要求等方面。密码行业标准制定 3 项，涵盖 OpenID、OAuth 等相关标准。但相对于国际标准，国内对云计算环境中身份鉴别方面的研究还不够充分。我国在此方面发展滞后，尚未形成体系，跟随国际相关标准较为缓慢。

3.3. 云计算中主要的身份鉴别相关标准

3.3.1. SAML

SAML（Security Assertion Markup Language，安全断言标记语言）是由 OASIS 组织安全服务技术委员会（Security Services Technical Committee）为解决认证和授权信息交换问题于 2001 年首次推出的，随后自由联盟和 Shibboleth 联手发展，于 2005 年推出 SAML2.0 开发标准，SAML 的推广消除了多协议复杂性，促进联合身份鉴别更广范围的应用。近年来，SAML 主要应用于单点登录与授权技术。目前，SAML 规范是业界最为认可的单点登录规范，很多大厂商如 RSA、IBM、Oracle、BEA、Microsoft 等纷纷推出了相应的产品来支持 SAML 规范。

SAML 是一个基于 XML 的标准，用于在不同的安全域（security domain）之间交换认证和授权数据。SAML 标准定义了身份提供者（Identity Provider，即 IDP）和服务提供者（Service Provider）两个参与实体，二者构成了不同的安全域。SAML 标准中主要包括认证声明、属性声明、授权声明。在 SAML 协议通信中，只要通信实体之间存在信任关系，符合 SAML 接口和消息交互定义，以及应用场景，实体之间就可相互通信。

SAML 的基本部分包括 Protocol、Bingding、Profile、Metadata、AuthenticationContext。其中 Protocol 是交互消息的格式，例如 AuthnRequest/Response（认证请求/响应）消息对；Bingding 是指协议所采用的传输方式，例如使用 HTTP Redirect 或 HTTP POST 或 SOAP 的方式传输协议中所定义的消息；Profile 是系统角色间交互消息的各种场景，例如单点登录是一种 Profile、单点登出也是一种 Profile、身份联合也是一种 Profile；各个参与方所提供的服务描述信息为

metadata，系统的认证方法通常是千差万别的；AuthenticationContext 是 SAML 中定义的认证扩展点，可以是最普通的 User Password 认证，也可以是 Kerberos 认证，也可以是电信常用的 Radius，或者是动态密码卡。SAML 依靠 SSL 和 X.509 等完善的安全标准，保护 SAML 源站点与目标站点之间通信安全，以及双方站点的身份鉴别。

SAML 相关协议可用于实现单点登录，其应用场景如图 1 所示。

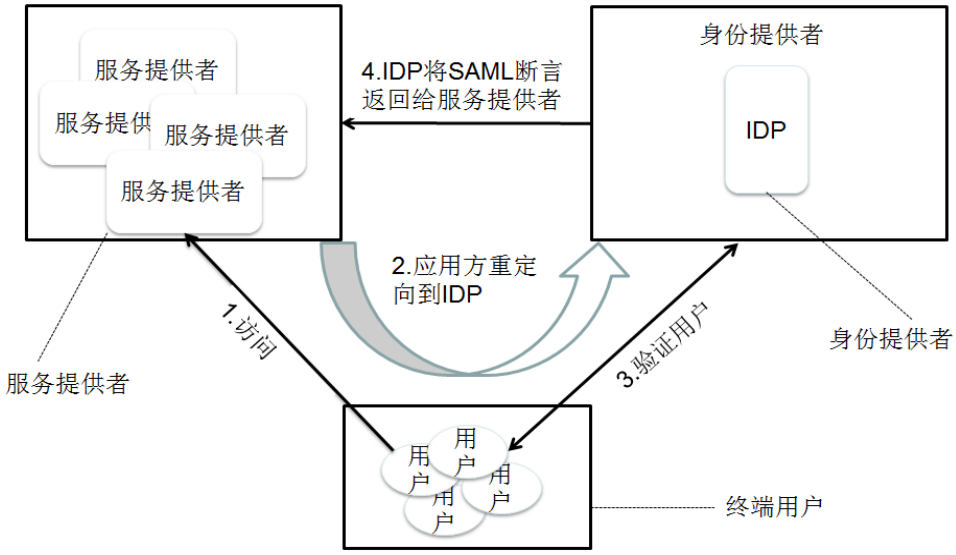

图 1 SAML 应用场景

当用户访问服务提供方时，服务提供方将用户重定向到 IDP，IDP 对用户进行验证后，向服务提供方返回 SAML 断言，服务提供方随后对 SAML 断言进行验证。

在国际上已经通过 SAML2.0 互操作性测试的主要产品有如下一些：

a) Shibboleth 协议

Shibboleth 协议是基于 SAML 标准的联合身份管理解决方案，是全球使用最多的统一身份管理协议之一，目前广泛应用在校园网中，美国、英国、德国、法国等都建立了自己的 Shibboleth 联盟。例如美国的 InCommon 组织为美国高校和研究组织提供安全和私密性保护，它的身份管理联盟已包含 135 个成员组织，800 余万用户。

b) Entrust IdentityGuard Federation Module 9.2

Entrust IdentityGuard 作为一个权威的 SAML 2.0 身份提供者，为不同组织之间的协作提供了基于 SAML2.0 开放标准的互操作性，并且支持众多的身份验证方法，企业、组织、机构有权为他们的用户访问选择正确的身份验证方法，支持包括用户名&密码，数字证书，IP，设备 ID，问题和答案，OTP 软令牌（通过语音、短信、电子邮件）、以及一系列的 OTP 硬件令牌。该系统能够快速部署，集中策略管理和易于集成到企业。

c) IBM Tivoli Federated Identity Manager（TFIM）

IBM Tivoli Federated Identity Manager（TFIM）提供了一个全功能的 web 访问管理解决方案来管理身份和资源的跨公司访问。通过提供一个简单的、松散耦合的模型来管理可信身份，并为用户访问信息资源和服务提供统一认证和分散授权。为企业部署面向服务的体系架构(SOA)和 Web Services， TFIM 提供了一个集中的身份中介服务，用于跨域的联邦 Web Services 身份管理。TFIM 支持以下标准:SAML 1.0/1.1/2.0 协议，OpenID Authentication 1.1/2.0， Information CardProfile， WS-Federation Passive

Requestor Profile， Liberty ID-FF 1.1/1.2， WS-Trust 1.2/1.3。

d) SAP Net Weaver Identity Management

SAP Net Weaver Identity Management 7.2 通过采用 SAML2.0 断言支持了基于 Web 的单点登录，提供了在线身份服务(概念上称之为 Identity Provider)和安全令牌服务(STS)。集中管理用户身份信息的认证中心和虚拟目录服务组件被扩展以支持和其他的身份提供者(IDP)进行集成。新的 IDP 和 STS 服务添加了访问管理功能到 SAPNetWeaver 的身份管理，为企业级的单点登录集成提供了解决方案。

除此之外，还包括以下产品：

— IBM Tivoli Access Manager
— Weblogic
— Oblix NetPoint
— SunONE Identity Server
— Baltimore, SelectAccess
— Entegrity Solutions AssureAccess
— Internet2 OpenSAML
— Yale CAS 3
— Netegrity SiteMinder
— Sigaba Secure Messaging Solutions
— RSA Security ClearTrust
— VeriSign Trust Integration Toolkit
— Entrust GetAccess 7

SAML 标准是一种基于 XML 的单点登录开放标准，是实现站点之间相互操作的安全访问控制框架，适用于复杂环境下交换用户的身份识别信息，已被多个云服务提供商采用。

3.3.2. WS-Federation

WS-Federation（Web Services Federation Language，Web 服务联邦语言）是由 OASIS 组织网络服务联邦技术委员会(Web Services Federation Technical Committee）为解决联邦认证和授权信息交换问题于 2009 年 5 月推出的。WS-Federation 是一个身份联邦标准，由 BEA Systems、BMC Software、CA Inc.、 IBM、Microsoft、 Novell、HP Enterprise 和 VeriSign 等公司联合制定。作为网络服务安全框架（Web Services Security framework）的一部分，WS-Federation 定义了不同安全域之间代理身份、身份属性以及认证等信息的机制，即不同的安全域联合在一起成为联邦的机制，例如可以将一个安全域内的授权访问资源管理提供给使用另一个安全域内身份管理的安全实体。尽管最终的访问控制决策由拥有资源的安全域严格实施，但是 WS-Federation 提供的控制决策可以基于不同安全域的身份、身份属性以及认证授权断言。

通用的联邦框架必须在不增加基础设施投资的情况下将已有的基础设施集成到框架中。WS-Federation 定义的联邦框架建立在 WS-Security、WS-Trust 等 WS 系列标准之上，提供了丰富的可扩展机制。WS-Security、WS-Trust 等标准允许不同的安全令牌、基础设施和信任拓扑结构，WS-Federation 则定义额外的联邦机制来扩展以上标准。WS-Federation 定义的机制不仅仅 Web 浏览器请求者（Web browser requestors）可以使用，Web 服务请求者（Web service requestors）也可以使用，这里的 Web 服务请求者必须支持 WS-Security、WS-Trust，并且有能力和 Web 服务提供方（Web service

providers）交互。Web 浏览器机制描述了将 WS 系列标准的消息编码到 HTTP 消息中并在参与方之间传输的机制。

WS-Federation 的目的是使得安全主体的身份和属性能够按照建立好的规则在信任边界共享。WS-Federation 规则除了规定格式和选项外，还包括信任、隐私/共享需求。而在 Web 服务的情形中，WS-Federation 的目的是允许身份和安全令牌发放方将身份和属性在不需要用户介入的情况下传递给服务方或者其他依赖方。下图表示出几种简单的 WS-Federation 应用场景。

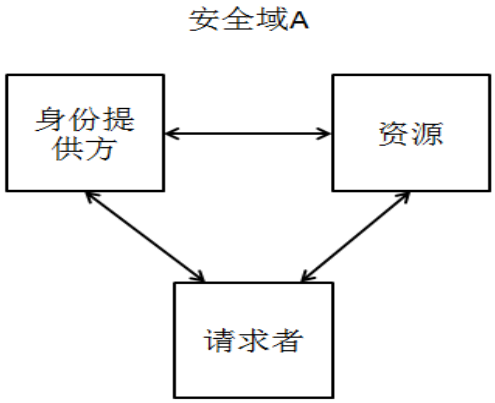

图 2 联邦应用场景 A

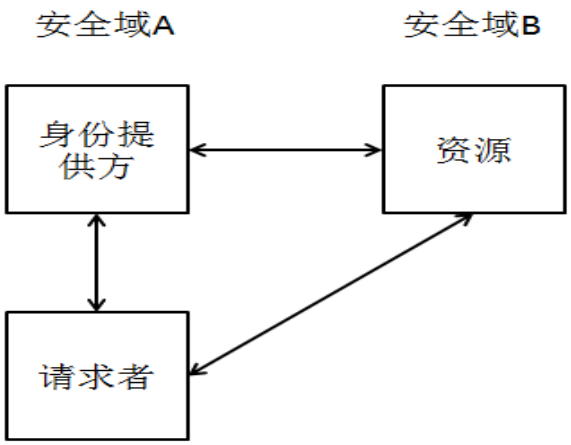

图 3 联邦应用场景 B

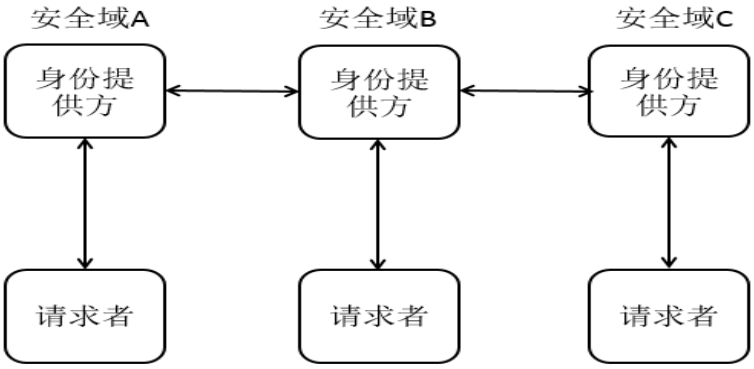

图 4 联邦应用场景 C

WS-Federation 系列标准主要用于身份联合场景，以解决联邦鉴别和授权信息交换问题。系列标准中的 WS-Federation 提供不同安全域的联合身份机制，使某一个域可以使用另一个安全域管理的身份来控制对资源的访问权限；另一个标准 WS-Security 定义了签名和加密方案，以及安全令牌如何附加上用户的身份信息，同时还定义了安全令牌的不同类型（例如 X.509 证书、Kerberos 票据、用户名/口令凭据、SAML 断言以及其他令牌等）；而 WS-Trust 标准则定义了安全令牌服务、安全令牌请求消息的格式以及该请求的响应消息的格式、密钥交换机制等内容。目前微软云服务（Microsoft Azure）、IBM 的联合身份管理（Tivoli Federated Identity Manager）使用了 WS-Federation 系列标准。

3.3.3. OpenID

OpenID 是一种分布式、去中心化可解决用户使用多个网络应用或云服务时的身份鉴别问题的解决方案，是以用户为中心的数字身份识别框架，其核心思想是通过 URI 来标识一个合法用户，即，用户可以在一个 OpenID 服务提供商处注册一个账号，然后利用该账号登录支持该 OpenID 的所有第三方应用。使用 OpenID 时，用户的个人信息会被安全地存储在一个 OpenID 服务器中（用户可以自己建立一个 OpenID 服务网站，也可以选择一个可信任的 OpenID 服务网站来完成注册）。OpenID 是一种开放的服务，不需要一个中心的身份服务提供商，任何应用服务提供商都可以实现自己的 OpenID 服务，用户可以自由的选择在其信任的服务提供商处注册账号，并利用该 OpenID 服务登录访问所有支持该 OpenID 服务的第三方应用。

OpenID 协议使得网络中的应用（被称为第三方应用程序，也称为依赖方）可以基于某一身份鉴别服务提供方（通常是一个授权服务器，也称身份服务提供方）执行鉴别流程，以验证终端用户的身份，并获取关于终端用户身份标识的基本配置信息。OpenID 协议在 OAuth 2.0 的授权流程基础上扩展了身份鉴别功能，使用断言声明的方式在通信双方传输关于终端用户的信息。OpenID 具有以下特点：

— 提供统一的身份鉴别框架，建立云内用户的“身份证”；
— 减轻用户记忆负担，提高用户认证效率；
— 实现用户在第三方应用的匿名认证，降低隐私泄露风险。

OpenID 协议建立在 OAuth 2.0 授权框架基础之上，将用户身份信息作为一种资源：

— 每个第三方应用使用 OpenID 提供方发放的 ID 令牌来确认用户的身份，使用与 ID 令牌同时发放的访问令牌获取用户详细的身份信息；
— 用户只需要记忆其在 OpenID 提供方上的口令凭据，不需要在第三方应用程序执

行注册流程就可以使用第三方应用程序提供的服务。

OpenID 适用于互联网站点及应用，特别是云计算环境下，第三方应用的身份鉴别场景。OpenID 旨在建立一个去中心化的网上身份鉴别系统。用户要预先在一个作为身份提供者（如 Google, Microsoft、腾讯、新浪等）的网站上注册，其他第三方网络应用（网站）都可以使用开放统一的身份标识来进行登录。主要应用场景如图 5 所示。

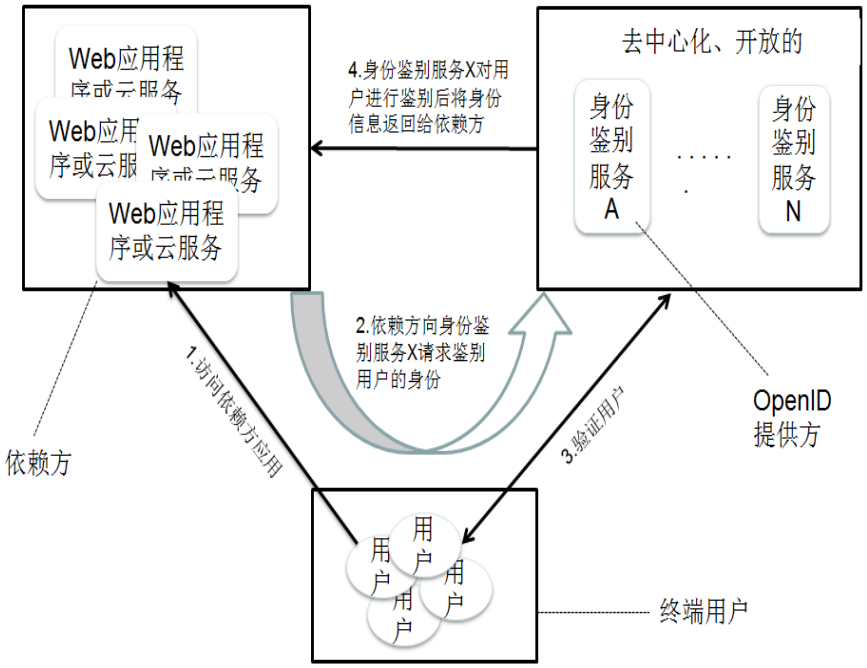

图 5 OpenID 应用场景

当终端用户访问依赖方提供的服务时，如果依赖方要求对终端用户进行鉴别且支持本标准定义的协议，依赖方可将终端用户重定向到一个该依赖方信任的身份鉴别提供方，执行以下协议流程（图 6 所示）。

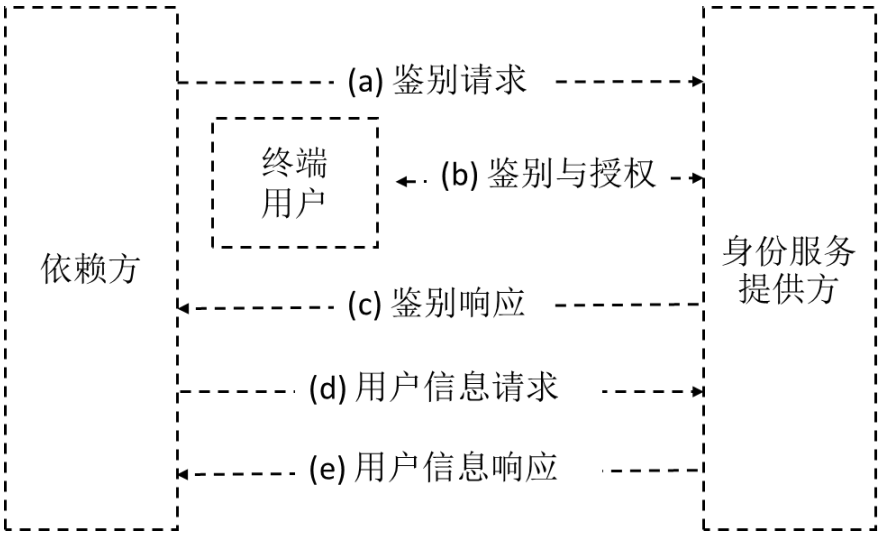

图 6 OpenID 基本协议流程

a） 依赖方向身份服务提供方发送一个关于终端用户的鉴别请求。

b) 身份服务提供方鉴别终端用户，并向终端用户获取关于依赖方访问其数据的授权。

c) 身份服务提供方返回一个 ID 令牌，通常还会返回一个访问令牌，从而响应第 a）步的请求。

d) 依赖方发送带有访问令牌的请求到身份服务提供方的用户信息端点。

e) 用户信息端点返回关于终端用户的声明信息。

OpenID 除了使用 OAuth 的访问令牌，还定义了 ID 令牌的概念。ID 令牌包含了用户的授权信息，使得第三方应用能够对用户进行身份鉴别。第三方应用还可以使用与 ID 令牌同时发放的访问令牌向 OpenID 提供方获取用户的详细身份信息。基于 OAuth2.0 授权流程，OpenID 定义了三种身份鉴别协议流程：授权码鉴别流程、隐式鉴别流程和混合鉴别流程。

在授权码鉴别流程中授权服务器给依赖方返回一个授权码，依赖方直接用授权码从 OpenID 提供方的令牌端点换取 ID 令牌和访问令牌。授权码鉴别流程如图 7 所示。

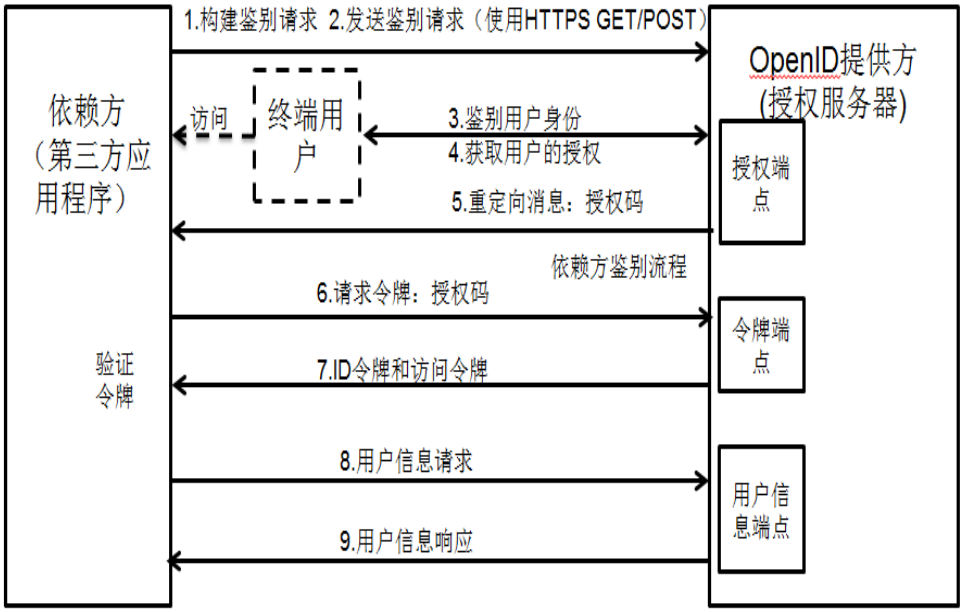

图 7 授权码鉴别流程

隐式鉴别流程主要用于在浏览器中使用脚本语言实现的依赖方或本机应用程序类型的依赖方。隐式鉴别流程如图 8 所示。

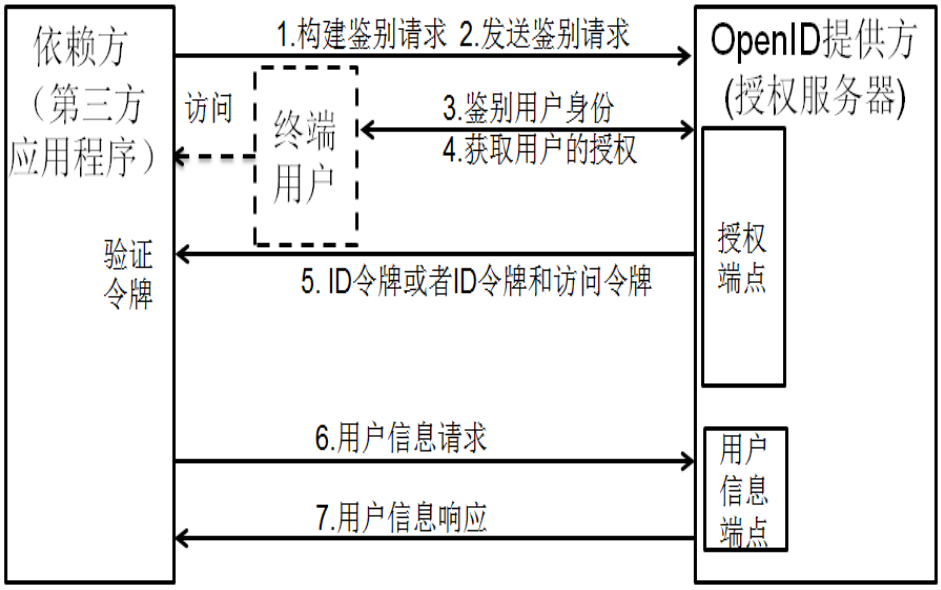

图 8 隐式鉴别流程

混合授权流程是授权码鉴别流程与隐式鉴别流程的结合，该流程允许依赖方请求 ID 令牌、访问令牌和授权码的任意组合。混合鉴别流程如图 9 所示。

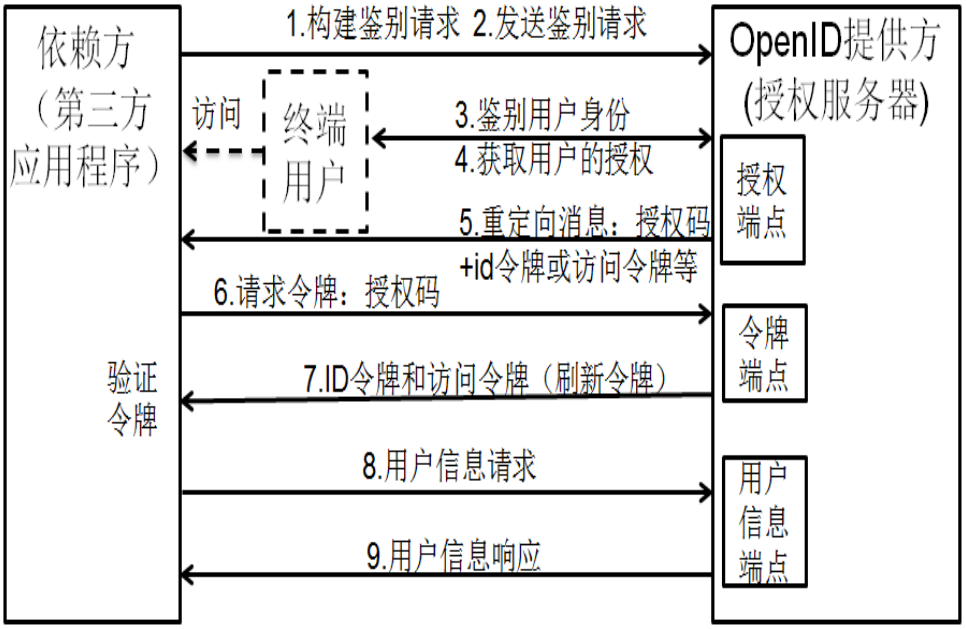

图 9 混合鉴别流程

以下介绍几个有代表性的云服务提供商对 OpenID 的支持情况：

— Google

Google 最开始为 Google 开发平台的应用程序提供了 OpenID 2.0 版本的协议支持，其 Google Apps 为 Google Apps for Business、Google Apps for Education 和 Google Apps for ISPs 的用户提供基于 OpenID2.0 协议的单点登录服务。但是随着 OpenID 中的

一些安全问题的暴露和研究，OpenID 联盟不断推进 OpenID 标准的研究，Google 也从 OpenID 2.0 迁移到了新的 OpenID 连接协议。

— Microsoft

Microsoft 的 Azure Active Directory (Azure AD) 中支持 OpenID Connect 1.0 ，实现了在 OAuth 2.0 协议基础上的单一登录功能。OAuth 2.0 是一种授权协议，但 OpenID Connect 扩展了 OAuth 2.0 的身份验证协议用途。OpenID Connect 协议的主要功能是返回 id_token，后者用于对用户进行身份验证。

— Facebook

Facebook 作为 RP 支持 OpenID—2009 年 5 月 19 日，facebook 宣布正式启用 OpenID 登录系统，允许用户使用 Gmail 或其它支持 OpenID 的网站账号登录 Facebook。可以用 Gmail 账号登录 Facebook，也就是说，当用户在 Gmail 里浏览邮件时，点击了一个 Facebook 的链接，用户不需要再输入密码，就能进入用户自己的 Facebook 页面里。

OpenID 框架和系列规范已应用在各主要云服务提供商的服务中，提供一种以用户为中心的身份鉴别框架。另外，OpenID 2.0 是基于 OAuth 协议的，通常与 OAuth 标准同时使用，完成对用户的身份鉴别和资源授权。

3.3.4. OAuth

OAuth（Open Authorization Protocol Framework），即开放的资源授权协议框架，由 IETF 发布。OAuth Core 1.0 版本发布于 2007 年 12 月 4 日，2009 年 6 月 24 日发布了 OAuth Core 1.0 Revision A 版本用于修复 OAuth Core 1.0 版本的一个安全漏洞。2010 年 4 月，OAuth 成为 RFC 文档，即 RFC 5849：The OAuth 1.0 Protocol。2012 年 10 月，OAuth 2.0 发布，即 RFC 6749：The OAuth 2.0 Authorization Framework，该版本与 OAuth 1.0 完全不兼容，以下所介绍的协议内容都是 OAuth 2.0 协议。

OAuth 2.0 协议通过引入一个授权层，将第三方应用程序与资源拥有者的角色进行分离，在资源拥有者的授权下，授权实体（即授权服务器）向第三方应用程序发放不同于资源拥有者身份凭据的访问令牌，第三方应用程序使用访问令牌代替资源拥有者口令凭据去访问受保护资源。访问令牌是授权服务器发送给第三方应用程序用于访问受保护资源的凭据，令牌中给出了访问资源的特定范围和访问时长，这个特定的范围和访问时长是由资源拥有者授权同意的，并由资源服务器和授权服务器实施。OAuth 的授权模型如图 10 所示：

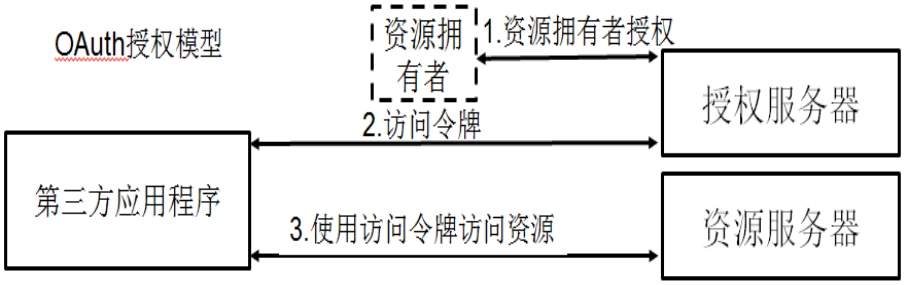

图 10 OAuth 授权模型

通过引入授权层（即授权服务器），每个第三方应用使用授权服务器发放的访问令牌访问受保护资源，访问令牌包含了访问资源的范围、访问资源的有效期等；资源拥有者只需撤销发放给第三方应用程序的访问令牌，就可以撤销其对受保护资源的访问权限，

不影响其他第三方应用程序对资源的访问。

OAuth 2.0 应用场景如图 11 所示：

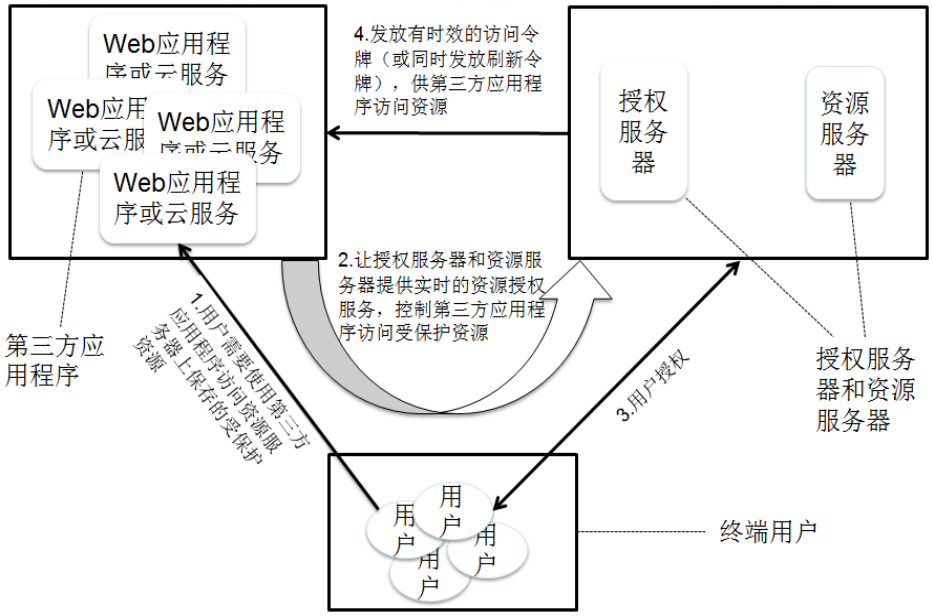

图 11 OAuth 应用场景

第三方应用程序是当前互联网上广泛部署的 Web 应用程序、云服务或者其他手机 APP 等应用程序。当用户需要使用第三方应用程序访问资源服务器上的受保护资源时，第三方应用程序将重定向到授权服务器，授权服务器在获取到用户授权后，发放给第三方应用程序有时效性的访问令牌，第三方应用程序使用访问令牌访问受保护资源。

OAuth 2.0 根据第三方应用程序的类型以及不同的使用场景，定义了四种授权许可，第三方应用程序可以使用这四种授权许可向授权服务器换取访问令牌，然后使用访问令牌访问受保护资源。四种授权许可分别是授权码许可、隐式许可、资源拥有者口令凭据许可和第三方应用程序身份凭据许可。

授权码形式的授权许可可用于获取访问令牌和刷新令牌，适合有保密能力型的第三方应用程序。由于该流程是一个基于重定向的流程，所以要求第三方应用程序能够与资源拥有者的用户代理（通常是一个 Web 浏览器）进行交互，并能够接收到来自授权服务器的请求（通过重定向）。授权码许可流程如图 12 所示。

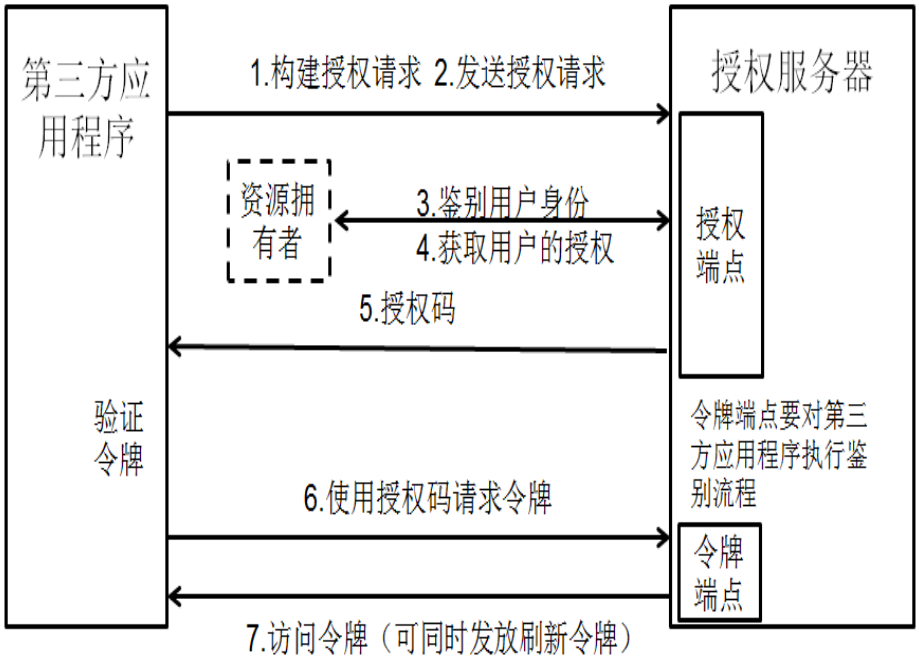

图 12 授权码许可流程

隐式许可类型可以用于获取访问令牌，但该类型不支持刷新令牌的发放，适用于操作某一特定重定向 URI 的无保密能力型第三方应用程序。这些第三方应用程序通常是浏览器中脚本语言（如 Javacript）实现的。隐式许可类型没有包含第三方应用程序的身份鉴别流程，需要依赖于资源拥有者的参与和重定向 URI 的提前注册来验证第三方应用程序。在该流程中，第三方应用程序直接获得访问令牌作为授权请求的结果。被编码到重定向 URI 中的访问令牌可能会暴露给资源拥有者以及在相同设备上驻留的其他程序。

第三方应用程序应能够与资源拥有者的用户代理（通常是一个 Web 浏览器）交互，并能够接收到来自授权服务器的请求（通过重定向）。隐式许可流程如图 13 所示。

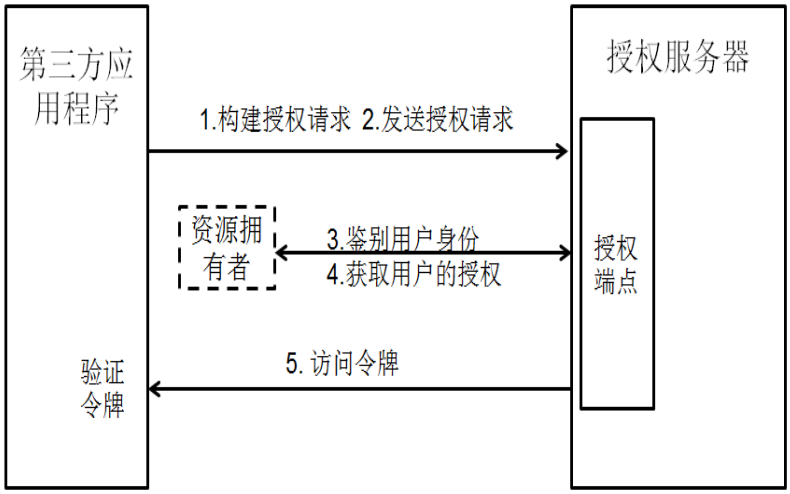

图 13 OAuth 隐式许可流程

资源拥有者口令凭据许可类型适用于资源拥有者与第三方应用程序之间存在互信

的情况，例如，第三方应用程序是操作系统的一部分或者某个特权应用。授权服务器应当谨慎采用此种类型的授权许可，只有无法采用其他流程时，才允许使用该流程。资源拥有者口令凭据许可流程如图 14 所示。

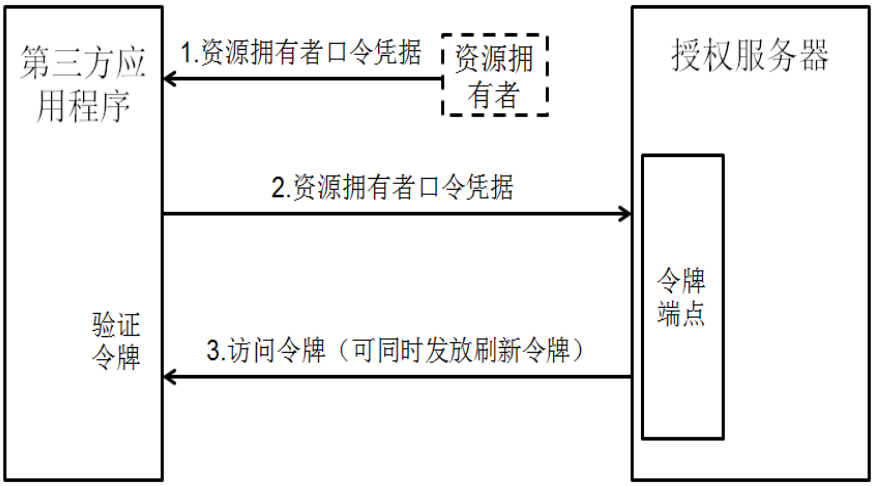

图 14 OAuth 资源拥有者口令凭据许可流程

当授权的范围仅限于第三方应用程序直接控制的资源，或者此前第三方应用程序与授权服务器经过协商同意的其他资源拥有者的资源时，第三方应用程序可以只用自身的第三方应用程序凭据来请求一个访问令牌。第三方应用程序凭据许可流程如图 15 所示。

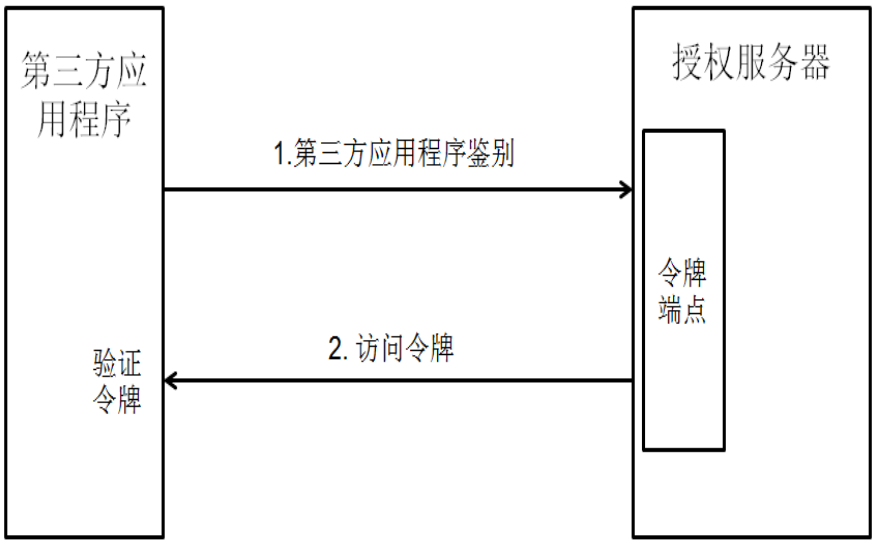

图 15 第三方应用程序凭据许可流程

OAuth 方便第三方应用安全的访问资源拥有者在资源服务器上的资源，在云计算中应用广泛。目前，很多互联网服务公司如 Twitter、Google、Microsoft、新浪、腾讯等都提供了 OAuth 服务。Twitter、Google、新浪、腾讯都提供了 OAuth 接口供其他第三方应用程序使用。

3.3.5. FIDO

FIDO 规范主要依赖于安全设备和 Web 浏览器作为客户端来实现 FIDO 客户端的安全

环境，允许任何网站和云应用与支持 FIDO 的设备通信，实现便捷、安全的在线用户鉴别。2014 年 2 月，FIDO-UAF-V1.0 和 FIDO-U2F-V1.0 草案发布，2014 年 12 月，FIDO-UAF-V1.0 和 FIDO-U2F-V1.0 正式发布。

FIDO1.0 标准使用公钥密码机制来提供安全保障，在 FIDO1.0 标准的草案中使用的是 ECDSA 算法。当用户登录服务器注册信息时，用户使用自己拥有的设备产生一对公私钥对，私钥保留在设备的可信执行环境中，攻击者无法读取，而公钥传给服务器，服务器将此公钥与用户对应的账户相关联。当用户登录到服务器并验证信息时，服务器发送挑战信息给用户，用户使用其拥有的设备中的私钥对服务器的挑战信息进行签名，然后返回给服务器。随后服务器使用对应的公钥对签名进行验证，从而完成用户身份鉴别。用户所拥有的设备中的私钥，必须经过用户解锁（如虹膜扫描，刷取指纹等），才能被用来做挑战数据的签名操作。FIDO 协议从设计之初就考虑了保护用户隐私。该协议不会向在线服务提供可供它们之间协作或者跨设备跟踪用户的任何信息。如果采集了用户的生物特征，则该特征不会离开用户设备。

典型的 FIDO 应用场景如图 16 所示。

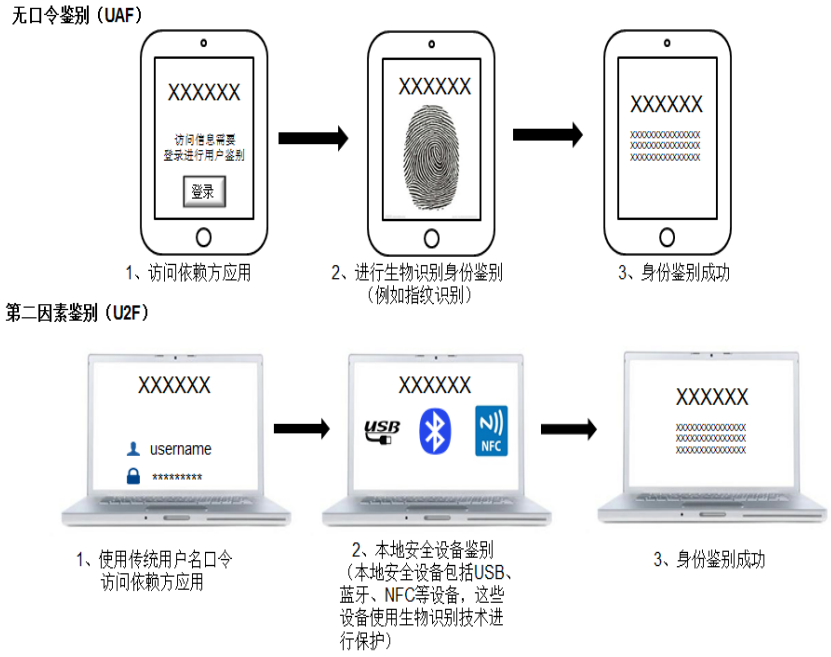

图 16 FIDO 应用场景

— **无口令鉴别（UAF）**

无口令鉴别通过 UAF（Universal Authentication Framework）协议支持。这种应用场景下，用户需要向在线服务注册自己的设备，并选择一种本地验证机制，比如指纹识别、虹膜识别、语音识别，或者输入 PIN 码。

注册后，再次向在线服务进行鉴别只需重复之前的本地验证操作即可，而无需通过设备再次输入密码。UAF 同样支持组合使用多种验证机制，比如指纹+PIN。

— **第二因素鉴别（U2F）**

第二因素鉴别（Universal Second Factor，简称 U2F）即在传统用户名/口令的鉴别方式之上增加一种新的因素来增强鉴别的协议。这种应用场景下，在线服务可以增强原有的口令鉴别机制，即再使用第二因素验证用户。用户还像以前一样使用用户名和密

码登录，但服务可以提示用户出示第二因素设备。有了第二因素设备，服务可以简化口令的复杂度（如只有 4 位的 PIN），但并不牺牲安全性。

注册和认证过程中，用户需要出示第二因素设备，比如在某个 USB 设备上按一下按钮，或者通过 NFC 刷一下。只要在线服务利用的 Web 浏览器支持 U2F 协议，用户就可以在使用该在线服务时使用 FIDO U2F 设备。

FIDO 注册流程如图 17 所示。

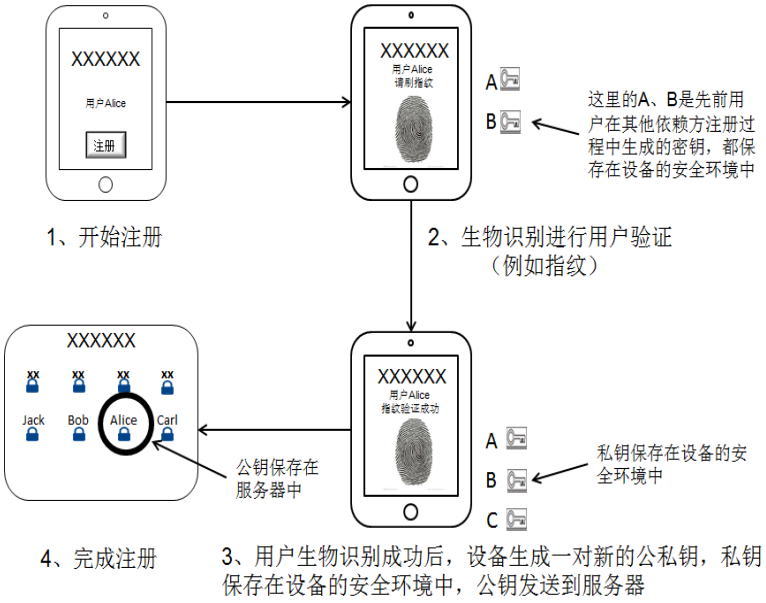

图 17 FIDO 注册流程

在用户使用 FIDO 1.0 标准定义的鉴别协议进行鉴别之前，用户需要将自己的设备以及鉴别方式在 FIDO 鉴别服务器（以下简称 FIDO 服务器）中注册，该注册过程实际上就是将用户的设备和鉴别方式与一对公私钥相关联，私钥存储在用户设备上，公钥存储在 FIDO 服务器上并与用户的账户相关联。

FIDO 鉴别流程如图 18 所示。

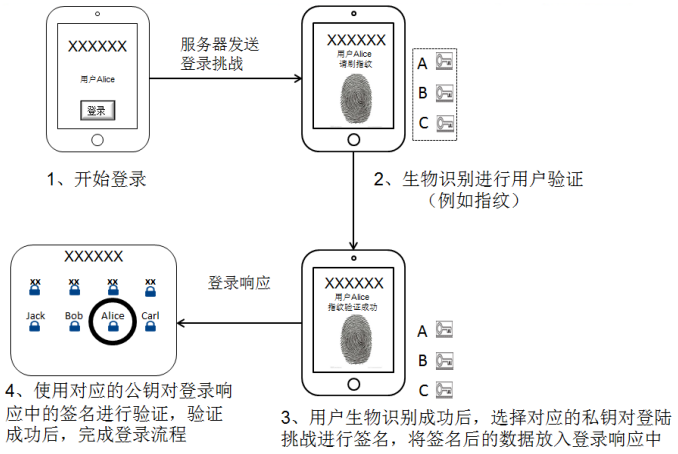

图 18 FIDO 鉴别流程

当用户进行鉴别时，即用户向 FIDO 服务器发起鉴别请求，FIDO 服务器首先组织一个在线鉴别请求（即 FIDO 服务器的挑战），其中可以包含事务明细（UAF 鉴别中有两种鉴别请求，其中一种是普通的身份鉴别，该鉴别请求只包含服务请求方的一些基本信息；另一种是与事务相关的身份鉴别，除了包含服务请求方的一些基本信息，还包含事务明细），然后将该请求发送到本地设备进行本地设备鉴别，本地设备鉴别可以通过指纹、语音等生物鉴别信息鉴别完成。本地身份鉴别完成后，本地设备将 FIDO 服务器的挑战使用存储的对应私钥进行签名然后返回给 FIDO 服务器，随后 FIDO 服务器使用服务器上存储的公钥对签名后的挑战进行验证，完成用户鉴别，鉴别成功。

FIDO 目前得到了很多设备生产厂商以及服务提供商的支持，Nok Nok Labs、Google、BlackBerry、ARM、英特尔、PayPal、Lenovo 和 MasterCard 等厂商都是 FIDO 联盟成员，并且积极推进 FIDO 的发展。Google 目前在其 Chrome 中添加了对 FIDO U2F 协议的支持。**FIDO 系列标准使用生物识别身份鉴别技术以及公钥密码技术加强了传统的用户名口令鉴别用户机制的安全性，用户不需要记忆口令使用生物识别信息即可登陆相关应用，提高了云计算身份鉴别服务的安全性，以应对云计算身份鉴别服务的强身份鉴别挑战。**

3.3.6. Kerberos

Kerberos 是麻省理工学院研发的一种计算机网络认证协议，依赖于可信的第三方来生成票据以实现安全的认证。该协议面向客户端/服务器模型，能够在非安全的网络环境中提供双向认证。Kerberos 基于对称密码学技术，在协议过程中，对传输的消息采用对称加密算法加密，能够提供数据的机密性和完整性。目前，Windows2000 及其后续操作系统、Mac OSX、Redhat Enterprise Linux 4 及其后续操作系统均用到了 Keberos 认证协议。Kerberos 版本 1-3 都只在麻省理工内部发行，Kerberos 版本 4 于 1980 年末发布，主要针对 Project Athena。Kerberos 版本 5 在 1993 年作为 RFC 1510 颁布，后来在 2005 年由 RFC 4120 取代，目的在于克服版本 4 的局限性和安全问题。

Kerberos 具体的协议流程如下图所示

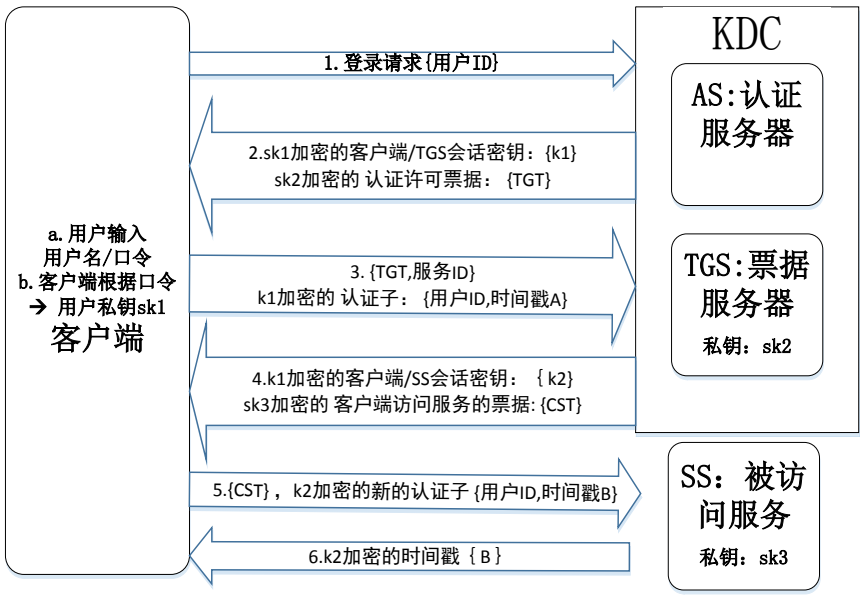

图 19 Kerberos 协议

协议流程如下：

1. 用户在客户端输入用户名和口令后，客户端根据口令计算出用户私钥（如将口令作为单向函数的输入,得到用户私钥 sk1),随后向可信的 KDC 发送登陆请求，请求中包含用户标识 ID。
2. KDC 的认证服务器根据用户 ID，从数据库中查找对应的口令，并根据口令计算出用户私钥 sk1，生成一个客户端与票据服务器 TGS 共享的密钥 k1，构建一个认证许可票据 TGT={用户 ID，用户网址，有效期，k1}。随后使用 sk1 加密 k1，并使用 TGS 的私钥 sk2 加密 TGT，将加密后的 Ek1(sk1)和 Esk2 (TGT)返回给客户端。
3. 客户端使用用户私钥 sk1 解密得到 k1。随后，根据接收到的加密 TGT 和请求访问的服务的 ID,构建消息{TGT,服务 ID},生成一个认证子{用户 ID,时间戳 A}，并使用 k1 加密认证子，将消息{TGT,服务 ID}和加密后的认证子发送给票据服务器 TGS。
4. TGS 收到客户端消息后，使用私钥 sk2 解密票据 TGT，得到 k1，产生一个客户端与被访问服务之间共享的会话密钥 k2，同时产生一个客户端访问服务的票据 CST={用户 ID，用户网址，有效期}。最后，使用 k1 加密 k2，使用被访问服务的私钥 sk3 加密 CST，并将加密后的 k2 和 CST 返回给客户端。
5. 客户端向目标服务发送访问请求时，发送一个新的被加密的认证子 {用户 ID，时间戳 B} 和上一步收到的 CST。其中认证子使用 k2 加密。
6. 目标服务解密 CST，得到共享的会话密钥 k2，利用 k2 解密认证子得到时间戳，并再次使用 k2 加密时间戳，将加密后的时间戳返回给客户端。

最后，客户端可验证收到的时间戳的正确性。如果时间戳正确，客户端信任该 SS 返回的消息。

Windows2000 和后续的操作系统都将 Kerberos 作为其默认认证方法。RFC 3244 记录整理了微软对 Kerberos 协议软件包的一些补充。另外还有 RFC4757，即“Windows2000 Kerberos 修改密码并设定密码协议”。苹果的 Mac OS X 以及 Red Hat Enterprise Linux4 和后续的操作系统同样使用了 Kerberos 客户端和服务器版本。**Kerberos 协议一般用于统一认证，解决安全域之间共享用户身份的问题，一般应用于单点登录以及 Hadoop 等分布式环境中。**

3.3.7. 小结

在云计算服务场景中，可以分成三种不同的应用场景：

1、开放的身份标识鉴别场景，即用户使用某一种身份标识可以随时登陆不同的应用，典型的实现方案是采用基于 OAuth 的 OpenID 协议，用户标识是一个 URI，该方案在公有云和私有云中都可以实现，应用场景如下图所示，身份提供方和依赖方一般部署在不同的云中，并且当用户登录某个依赖方时可以选择使用其在某一个身份提供方注册的身份信息。

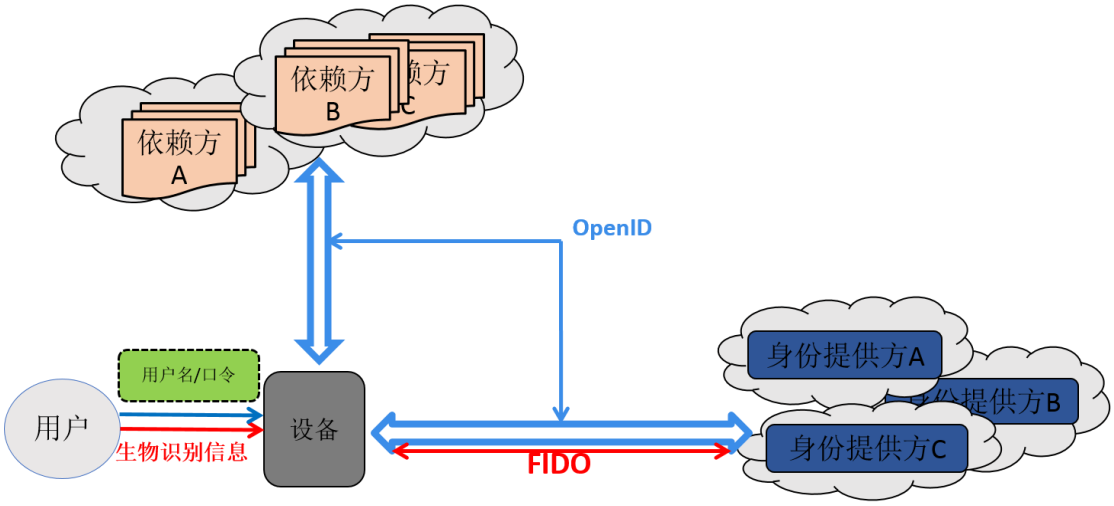

图 20 开放身份标识鉴别场景

2、单点登录场景，用户在企业或者组织内部有多个应用时，登陆其中一个应用后可以直接登陆其他应用，不需要再次对用户进行身份鉴别（例如重新输入用户名/口令）。典型的解决方案可以采用 SAML 协议，如下图所示（身份提供方和依赖方可以在一个私有云中，也可以部署在不同的云中）。

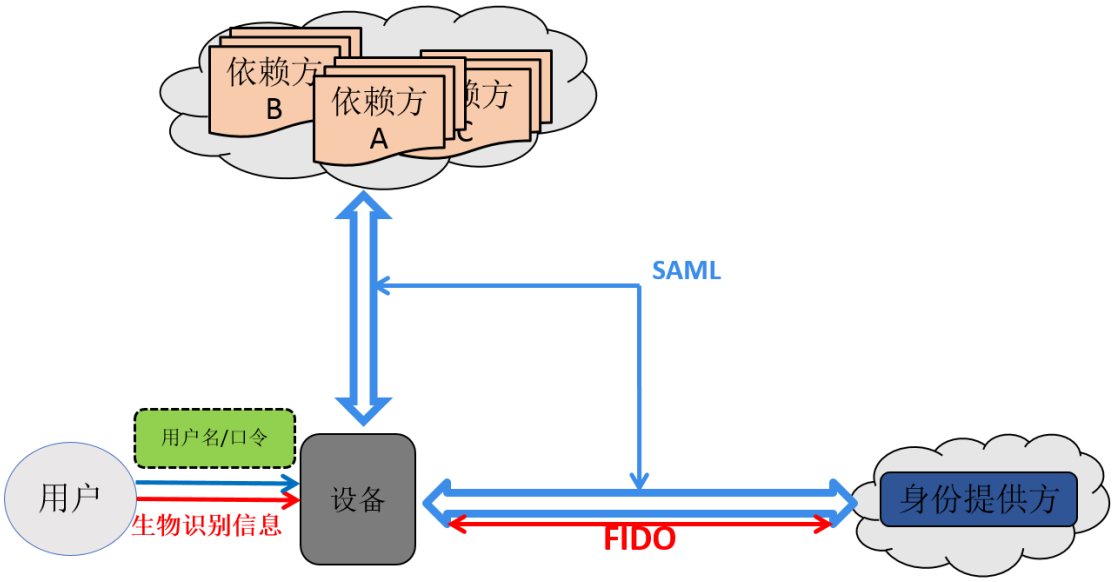

图 21 单点登录场景

3、跨域的联合身份场景，不同安全域之间可以代理身份、身份属性以及认证等信息，即不同的安全域联合在一起成为联邦的机制，例如可以将一个安全域内的身份管理服务提供给另一个安全域内的访问资源管理授权服务。典型的解决方案是 WS-Federation 系列标准，如下图所示，在这种应用场景中，某一安全域中在不部署身份提供方应用的情况下，依然可以使用其他安全域中的身份提供方应用提供的联合身份管理和鉴别功能。

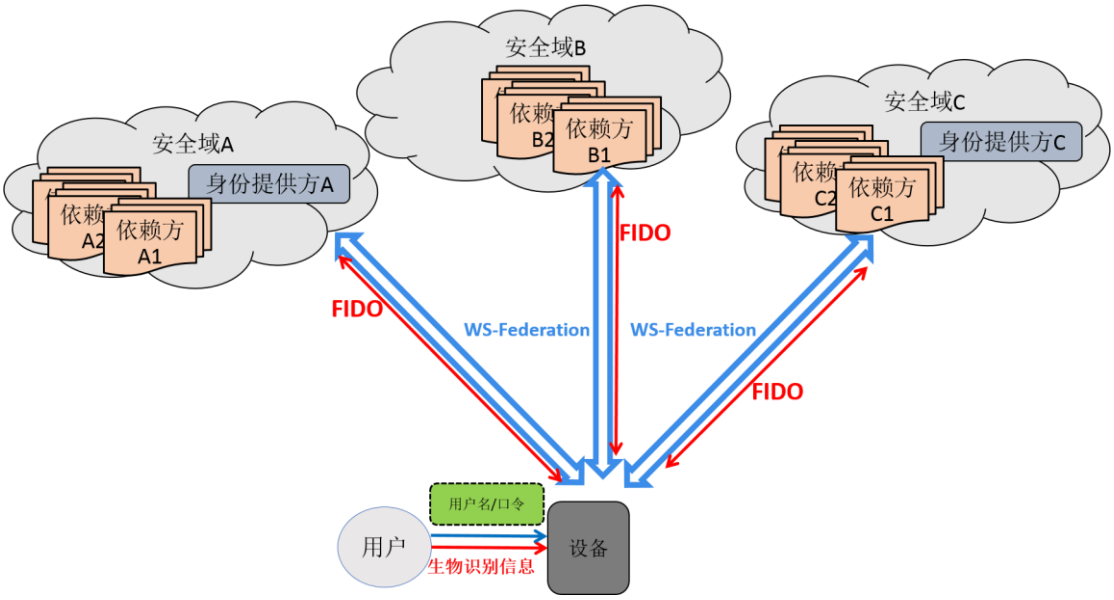

图 22 跨域联合身份应用场景

在以上三种应用场景中，当用户身份验证时，可以采用 FIDO 协议的生物识别鉴别技术机制加强传统的用户名口令机制的安全性，以提高用户体验和身份鉴别的安全性。

4. 业界典型的云计算身份鉴别服务及密码技术应用案例

本章描述各典型云服务提供商在其各产品中应用的身份鉴别技术以及这些身份鉴别技术需要结合使用的密码技术。

4.1. Google 云身份鉴别技术

谷歌云平台为用户提供了各种各样的服务，如谷歌云存储、谷歌 BigQuery 等，通常用户通过 API 调用（或者直接通过用户界面或命令行工具）访问云服务。为了确保用户的安全与隐私，所有的谷歌云平台 API 需要经过正确的鉴别和授权。

谷歌云存储的身份鉴别通常包括以下几种方式：

a) OAuth 2.0

谷歌云存储服务使用 OAuth 2.0 进行 API 的鉴别与授权，包括两种类型：以服务为中心的鉴别流和以用户为中心的鉴别流。以用户为中心的鉴别流允许应用程序从终端用户获得凭证，如果应用程序需要访问用户数据则使用该种鉴别流。以服务为中心的鉴别流允许应用程序直接持有服务账户的凭证来完成鉴别，如果应用程序运行其自身的数据而不是用户的数据时使用该种方式。以服务为中心的鉴别更易使用并满足谷歌云平台的大多数场景，但与用户数据相关的，如 Gmail、YouTube、项目管理需要使用以用户为中心的鉴别。一旦应用获得凭证，便可与鉴别提供者联系获得 OAuth 访问令牌来访问特定服务，如 API 调用。

OAuth 使用范围值 Scopes 来决定授权，有 ready-only、read-write、full-control、

Cloud platform read-only、cloud-platform 等。Scopes 是 OAuth 的一个属性，该属性用户限制 OAuth 凭证访问资源的权限。一个用户账户或服务账户可能拥有资源的很多权限，如云存储数据的读和写操作。由于安全和隐私的原因，云用户的应用可能不需要所有的权限。该属性可以使用户将凭证限制在所有权限的一个子集中。

谷歌云存储服务推荐使用 OAuth 完成身份鉴别。

b） 使用 Gsutil 工具进行身份鉴别

Gsutil 是一个谷歌云存储提供给用户的一个基于 Python 的命令行工具，提供类似 Linux 的命令，用于和存储区交互。该方式提供了一种和 OAuth 相似的技术，但所有操作均是手动完成。

c） 使用客户端库进行身份鉴别

客户端库是谷歌提供的功能库，可以很简单的将多种身份提供方集成到应用中，减少用户的代码量，并且使得客户的代码更加健壮，主要应用在通过 API 访问云存储服务的应用场景。客户端库支持多种主流的编程环境，包括 Java、JavaScript、Python、Object C 等。用户可以像在 Windows 环境下使用网络服务账户一样去使用谷歌应用默认凭据。

d） 基于 Cookie 的鉴别方式

用户可以通过基于浏览器的鉴别方式从云存储服务下载文件，用户需要有谷歌账户但是不需要有云存储账户。该种方式下，需要使用基于谷歌账户的访问控制列表（ACL）映射到访问对象，然后提供给用户一个重定向到该对象的 URL。当一个用户点击浏览器中的 URL 时，如果他之前没有登录，那么会自动重定向到谷歌账户的登录界面，经过鉴别之后，浏览器获得带有封装身份令牌的 cookie。然后重定向到云存储库的对象，云存储验证该用户允许读该对象，然后将所需对象下载到计算机。

e） 账户凭证

1） 服务账户凭证

服务账户是一种代表软件而非自然人的特殊账户，是代表用户的应用程序访问云存储最常用的鉴别方式。当使用服务账户鉴别应用时，不需要用户先经过鉴别获得一个访问令牌。相反，用户从谷歌云平台控制台获得一个私钥，然后发送一个签名的请求获得访问令牌，然后使用该访问令牌访问云存储服务。

2） 服务账户凭证的生成

用户可以在云平台控制台通过创建一个 OAuth 客户端 ID 为服务账户创建一个私钥。私钥有 JSON 和 PKCS12 两种格式。JSON 格式的密钥在谷歌云平台之外使用应用默认凭证的时候需要，且不能转换成其他格式。PKCS12 支持许多不同的编程语言和库。如果需要，可以通过 OpenSSL 转换成其他格式，但是不能转换成 JSON 格式。一个服务账户的 OAuth 客户端 ID 唯一标识被鉴别的账户。创建服务账户的客户端 ID 后，会获得客户端 ID、邮件地址、证书指纹。注意服务账户有两个标识，一个客户端 ID、一个邮件地址，邮件地址必须使用 RSA 签名。

3） 用户账户凭证

当应用程序（如 Web 服务器应用、桌面应用、客户端的 JavaScript）需要访问用户端数据时使用用户账户凭证。

可见，Google 云服务中支持多种身份鉴别方式，然而所有的身份鉴别方式的安全都依赖于身份凭证的安全以及身份鉴别流程中协议交互的安全。为了保护身份凭证的安全，Google 需采用密码技术来保护凭证的机密性和完整性以防止内外部网络攻击窃取或破坏身份凭证。而在 OAuth 技术中，也常采用了非对称密码算法、对称密码算法、杂凑算

法来确保协议的安全，以防止敏感的信息的被窃取和防止攻击者假冒等。

4.2. Amazon 云身份鉴别技术

亚马逊云服务（Amazon Web Service，AWS）通过实施和采用身份和访问管理服务（Identity and Access Management，IAM）安全地控制用户（用户可以是一个自然人、系统或应用程序）对 AWS 服务和资源的访问。如图 所示，AWS 账号可以通过 IAM 创建和管理 AWS 用户与用户组，并使用各种权限来允许或拒绝用户和用户组对 AWS 资源的访问，每个用户都拥有一个安全凭证，用户以及安全凭证均通过 AWS 账号控制。下面将对 AWS 云服务中 IAM 用户的创建与管理、用户安全身份凭证及管理进行描述。

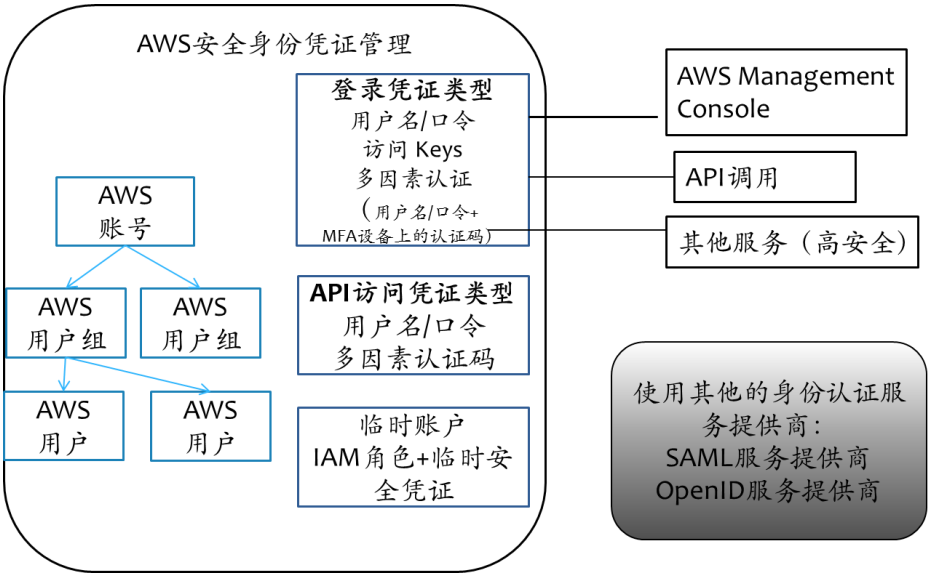

图 23 AWS 安全身份凭证管理

— IAM 用户的创建和管理

IAM 用户可以通过 AWS 的管理控制台、命令行界面（Command Line Interface，CLI）或 API 创建。如果 IAM 用户需要访问 AWS 管理控制台，那么需要为用户创建用户名/口令作为登录凭证。如果用户需要通过 CLI 或 API 访问 AWS 服务，那么需要为用户创建 API 访问密钥（包括访问密钥 ID 和一个秘密的访问密钥）作为访问凭证。创建的 IAM 用户通过使用一个特定的 URL 在 AWS 账户中进行注册或关联。

— 用户安全凭证及管理

为了访问 AWS 账户资源，IAM 用户必须提供相关凭证；使用 AWS 管理控制台，用户必须提供正确的口令；使用 CLI 或 API 调用，用户必须提供正确的访问密钥。如果用户仅通过 API 或 CLI 访问资源则不需要口令，拥有访问密钥即可。此外，为了提高安全性，用户凭证可以采用多因素鉴别的方式。

— 用户名/口令

AWS 账号（根账号或者超级账号）口令管理：可以通过注册 AWS 账号时的邮件地址和口令，以及 AWS 管理控制台来更改账号口令。可以对口令设置安全策略，如口令长度、口令字符组成限制、口令更改周期、口令过期无效等。

IAM 用户口令管理：可以通过 AWS 管理控制台、CLI 或 API 三种方式对 IAM 用户的

口令进行创建、更改、删除等操作。

— 访问密钥

当用户创建完访问密钥后，IAM 返回给用户一个访问密钥 ID 和秘密的访问密钥。默认情况下，创建完的访问密钥状态为激活状态，意味着用户可以使用该密钥发起 API 调用请求，该访问密钥可以被执行禁用、启用、撤销、更改、删除操作。AWS 账号即超级账号可以授予 IAM 用户权限来列出、轮换并管理其访问密钥。

IAM 用户访问密钥管理主要包括通过 AWS 管理控制台完成对访问密钥的创建、更改和查看操作，或者通过 AWS CLI 和 API 完成对访问密钥的创建、更改、查看以及轮换操作。

— 多因素鉴别

AWS IAM 的多因素鉴别，通过要求用户输入附加的鉴别码来提高安全保障，该鉴别码是在用户访问 AWS 网站或服务时由鉴别设备发送给用户的。如访问 AWS 网站，需要用户提供用户名、口令以及 MFA 鉴别码，访问基于 MFA 保护的 API，需要用户提供访问密钥、设备序列号(硬件设备)或亚马逊资源名称(针对虚拟设备，Amazon Resource Name ，ARN）以及 MFA 鉴别码。

使用多因素鉴别方式，必须分配给 IAM 用户或根账户一个多因素鉴别设备。多因素鉴别设备对于每一个用户都是唯一的，一个用户不能输入来自其他多因素鉴别设备的鉴别码进行鉴别。该设备可以是硬件设备也可以是虚拟设备，如安装在智能手机上的一个 MFA 应用。MFA 设备可以通过 AWS 管理控制台、IAM 命令行工具或 IAM API 启用。

— IAM 标识符

IAM 使用三种不同的标识符标识 IAM 用户、IAM 用户组、策略以及服务器证书，包括可读的名称和路径、IAM ARN、唯一 ID。当创建一个用户、一种角色、一个用户组或一个策略或上传一个服务器证书时，会为其分配一个友好的、可读的名称和唯一 ID。如果使用 IAM API 或 AWS CLI 创建 IAM 实体，也可以为该实体分配一个路径，不同的实体路径不应相同。IAM ARNs 主要针对访问的资源而言，AWS 的身份与访问管理服务对此有严格的格式要求。

— IAM 支持的身份提供方

通过使用身份提供方，用户可以创建一个 IAM 身份提供方实体来建立 AWS 账号与外部身份提供方之间的信任关系。IAM 支持兼容 SAML 或者 OpenID 的身份提供方。

身份鉴别技术的安全依赖于密码技术的采用。在 Amazon 云中有专门的密钥管理机制来管理其云服务中所用到的密钥。在 Amazon 云服务的身份鉴别技术中，无论是身份账户的存储、使用，还是 SAML、OpenID 等协议的使用，都需要采用密码技术来保障安全，如采用对称加密技术来加密敏感的身份信息和传输中的身份凭证等敏感信息，采用数字签名技术来防止协议消息被篡改等。

4.3.Microsoft 云身份鉴别技术

微软云服务（Microsoft Azure）利用活动目录技术（Azure Active Directory，Azure AD）提供了联合身份的单点登录服务，可实现不同安全域中的合作伙伴的相互访问，使应用能够重定向到活动目录来进行用户鉴别。Azure AD 为云用户提供身份管理服务，包括多因素鉴别、设备注册、自服务口令管理、自服务组管理、特权账户管理、基于角色的访问控制、应用程序使用监控、审计和安全监控与报警，支持 SAML、OpenID、

OAuth、WS-Federation 协议，同时支持不同开发平台的开源库。

Azure AD 相当于身份提供方，验证组织机构目录中的用户和应用程序的身份，最终为成功鉴别的用户和应用程序发行令牌。应用程序要想经过 Azure AD 的鉴别必须提前注册，并在目录中进行唯一标识，Azure AD 支持的应用程序包括单租户应用程序和多租户应用程序。一旦用户经过 Azure AD 鉴别，应用程序必须验证来自用户的安全令牌以确保该用户身份的合法性。开发人员可以利用 Azure AD 提供的鉴别库处理来自 Azure AD 的任何令牌的验证，包括 JWT（JSON Web Token）或 SAML 断言。鉴别过程中的请求和响应信息流取决于所采用的鉴别协议。

— Azure AD 及其管理

Azure AD 为微软云服务提供核心目录和身份管理功能，如 Azure、Office 365、Microsoft Intune 等云服务。微软云用户注册其中任意一个云服务账户后，便可获得 Azure AD，用户也可以根据自己的需求增加额外的目录。用户可以在 Azure 管理门户下添加多个 Azure AD，每个活动目录之间资源、管理和数据同步均是独立的，互不影响。

微软云服务订阅者的管理者可以使用 Azure 管理门户、微软 Intune 账户门户、Office 365 管理中心管理目录中的数据，或者运行支持 Windows PowerShell 的微软 Azure AD 模块来管理存储在 Azure AD 中的数据，通过以上任何一种方式均可以创建用户和用户组账号，并管理用户相关的云服务。

Azure AD 访问管理运作的核心思想是安全组，利用安全组控制对资源的访问管理是一个常用的范例，资源拥有者（目录的管理者）可以指定一个组提供对其拥有的资源的特定访问权限。该组的成员会拥有访问权限，资源拥有者可以委托其他角色来管理组的成员列表，如部门经理或管理员。

— Azure AD 安全令牌断言

Azure AD 发布的安全令牌包含关于对象被鉴别的声明或断言信息，应用程序可以利用该断言信息验证令牌、识别对象的目录租户、显示用户信息、确定对象权限等。

— 支持 Azure AD 的应用场景及其鉴别方法

a) 通过 Web 浏览器访问 Web 应用程序：Web 应用程序将用户浏览器重定向到 Azure AD 来验证用户身份，Azure AD 返回用户一个安全令牌，安全令牌包含关于用户的断言信息，该场景支持 SAML、OpenID、WS-Federation 协议。

b) 单页面应用程序：当用户登录时，JavaScript 前端使用支持 JavaScript 的活动目录鉴别库和隐式授权许可从 Azure AD 处获得 ID 令牌，令牌被缓存，客户端将其附在发起 Web API 调用时的请求中。

c) 访问 Web API 的本地应用程序：该种场景支持 OAuth，本地应用程序通过该协议获得用户访问令牌，该访问令牌在发起 Web API 请求时发送给接收方，验证成功后授权用户并返回相应的请求资源。

d) 访问 Web API 的 Web 应用程序：该场景下，Web 应用程序可以两种身份类型来鉴别和访问 Web API，应用程序身份或委托的用户身份，第一种身份支持 OAuth，第二种身份支持 OpenID 和 OAuth。

e) 访问 Web API 的进程或服务器应用程序：支持 OAuth 协议。

— Azure AD 采用多因素鉴别机制

2016 年 1 月微软 Azure 多因素鉴别功能正式添加到 Azure AD 中。Azure 多因素鉴别可以帮助保护对数据和应用程序的访问，同时可以满足用户对简单登录过程的需求。它通过各种简单的验证选项（例如电话、短信、移动应用通知或验证码）来提供强大的

身份鉴别。如果启用多因素鉴别功能，用户需要先确认自己的身份，然后才能运转虚拟机、管理存储或使用其他 Azure 服务。如，Office 365 采用 Azure 多因素鉴别功能对用户身份的合法性进行验证。

通过 Azure AD 来完成身份验证的 Microsoft 服务还有 Azure 密钥保管库，对 Azure 密钥保管库发出的所有请求必须经过身份验证。Azure 密钥保管库支持可使用 OAuth 技术获取的 Azure Active Directory 访问令牌。

微软云服务对各个协议的支持较为完善，包括了 SAML、OpenID、OAuth、WS-Federation 协议，最近，微软在最新的操作系统中将支持生物识别身份鉴别的 FIDO 协议。

4.4. IBM 云身份鉴别技术

2015 年 1 月 IBM 研究人员公布了一种新的基于云的技术帮助用户保障个人数据安全，该技术称为身份混合器（IBM Identity Mixer），是一个身份鉴别隐私保护和认证属性安全传输的密码协议套件。

身份混合器允许用户完成身份鉴别，而无需采集任何个人数据。因此，并不存在个人数据需要被保护、管理。对于发起方来说，通过使用身份混合器发行服务，提供方能够通过发行隐私保护凭证来鉴别用户的属性。对于验证方来说，通过使用身份混合器验证服务，提供方能够定义隐私保护访问控制策略，并随后使用定义的策略鉴别用户而无需采集用户个人数据信息。

身份混合器可以被用在数字钱包中，包含可信第三方的鉴别凭证，如政府颁发的电子身份证。凭证的颁发者并不知道该凭证何时以及如何被使用。身份混合器可以使用户精确选择哪些数据与谁共享，当前 IBM BlueMix（IBM 云应用程序开发平台）已经与身份混合器结合。

IBM 的 Tivoli 联合身份管理器向多种应用的用户提供单点登录。

4.5. 典型云身份鉴别服务及密码应用对比

表 1 典型云身份鉴别服务及密码应用对比

	采用的技术	支持的协议	特色
Google	OAuth 2.0 鉴别、Gsutil 鉴别、客户端库鉴别、基于 Cookie 的鉴别、账户凭证等技术	OAuth、OpenID、FIDO	支持多种身份鉴别方式，所有的身份鉴别方式的安全都依赖于身份凭证的安全以及身份鉴别流程中协议交互的安全
Amazon	使用身份和访问管理服务（Identity and Access Management，IAM）	SAML、OpenID	Amazon 使用自己的 IAM 服务提供身份鉴别服务，云中有专门的密钥管理机制来管理其云服务中所用到的密钥
Microsoft	活动目录技术	OAuth、SAML、OpenID、LDAP 、WS-Federation	通过 Azure AD 来完成身份鉴别，另外使用 Azure 密钥保管库管理密钥

IBM	身份混合器技术	SAML 、 OpenID 、 WS-Federation 、LDAP	身份混合器提供发行服务和验证服务完成云身份鉴别服务，IBM BlueMix 服务已经与身份混合器结合在一起。IBM 的 Tivoli 联合身份管理器向多种应用的用户提供单点登录。

5. 云计算身份鉴别服务密码标准体系架构

5.1.概述

云计算身份鉴别服务作为其他云服务和应用的基础服务，面临着不同的安全鉴别需求，为了保障云环境下身份鉴别服务的身份凭证管理安全、访问通信以及鉴别协议的安全，应采取相应的密码技术应对可能存在的网络攻击和安全漏洞带来的安全威胁。

为了业界可以方便的使用云计算身份鉴别服务的相关产品和服务，并使得业界对云身份鉴别服务产生共识，促进跨域云计算身份鉴别的应用，另外为了简化标准以及减少不必要的资源浪费和产生不同解释的标准，从整个云计算环境中身份鉴别技术的角度，本研究报告给出了支撑云计算身份鉴别的密码标准体系框架。

此外，通过提供一个有共同依据的、具有互操作性的、技术整合的标准体系规范，可以确保各个解决方案能够符合相关规范并具有互操作性。

5.2.云环境中的身份鉴别密码技术要求

5.2.1. 云身份鉴别需求和技术框架

云服务可以认为包括以下几个层级的服务：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS），在各个服务层级中，不同的服务功能具有不同的安全要求，而有关云端访问者的鉴别安全则是首要条件。云服务中可以采用单点登录、跨域鉴别、多因素鉴别等机制来实现对服务请求者进行身份验证，为了确保鉴别过程中身份凭证、身份鉴别协议以及访问通信的安全，需采用加/解密、数字签名等密码技术提供支撑。

通过前面章节对云计算中涉及的安全风险和身份鉴别需求分析，进行综合和提炼，构建了如下图所示的云计算身份鉴别服务框架。该框架包括如下几部分：

1） 云计算身份鉴别服务安全及需求

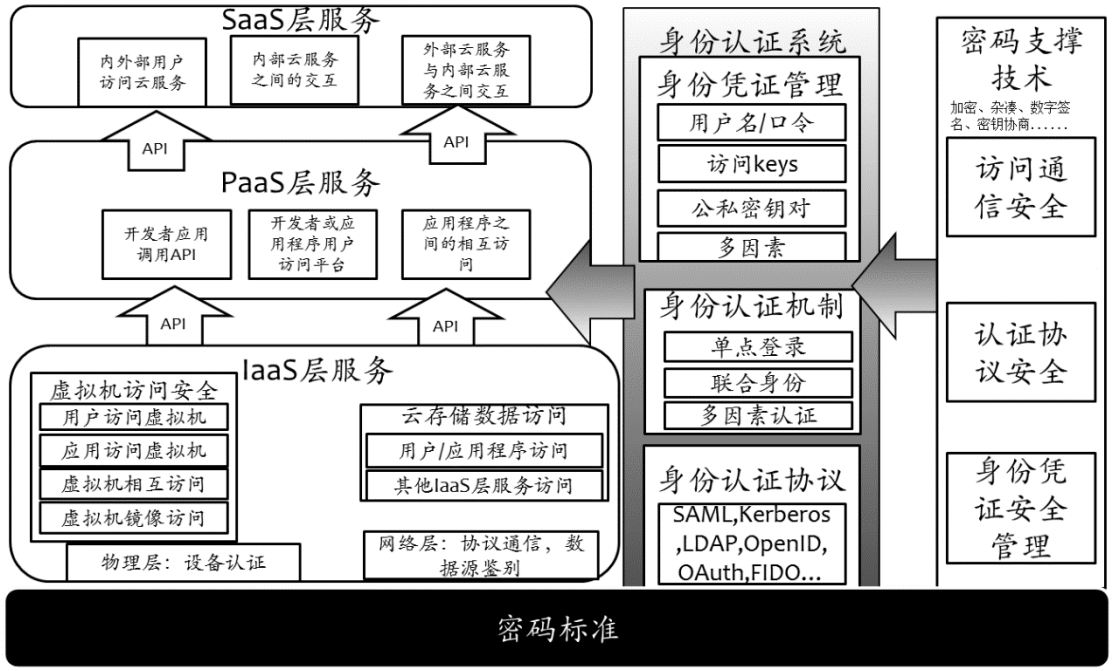

图 24 云计算身份鉴别服务技术体系框架

5.2.2. IaaS 层云身份鉴别密码技术要求

在 IaaS 服务模式下，云用户通过向云服务提供商租用虚拟机的方式来部署计算资源。在使用虚拟机之前，云用户首先需要检查云服务提供商提供虚拟机镜像的安全性。其次，在使用云服务的过程中，IaaS 层的云用户需要以一种安全的方式与运行的虚拟机实例进行交互。因此，IaaS 层中需采用云用户与设备的双向鉴别技术以及访问控制机制使云租户的资源在物理或逻辑上各自独立并在访问上可控，如采用单点登录、多因素鉴别等机制。

（1） 物理设备接入鉴别

为了保证 IaaS 层中各种接入物理设备的合法性，需要对接入的设备进行安全接入鉴别。物理设备接入鉴别包括两个方面，一是对拥有设备的人进行身份验证，二是对设备本身进行验证。对拥有设备的人进行身份验证可以通过多因素鉴别的方式实现（如，用户名+口令+多因素鉴别码）或者基于 FIDO 鉴别协议的鉴别方式，对设备本身进行验证可以采用对设备进行数字签名的方式。

（2） 虚拟化安全鉴别

在虚拟机镜像鉴别方面，为了确保虚拟机镜像来源于可信的权威实体且保证该虚拟机镜像没有被篡改，需要对虚拟机镜像的真实性进行验证。云服务提供商可以对其提供的虚拟机镜像模板进行数字签名，云用户根据该签名结果验证该虚拟机镜像模板的真实性。

在通信双方身份合法性鉴别方面，为了确保应用程序、用户、虚拟机之间的通信安全，防止非授权用户的非法访问，需要对通信双方进行身份鉴别。

在 API 接口鉴别方面，为了确保虚拟机实例由合法的用户和应用程序接口（API）调用，需要鉴别 API 的合法性。云用户可以通过对虚拟机管理接口的 API 调用进行签名，

并通过受信任的实体签署公钥证书，云服务提供商通过该公钥证书验证云用户身份的合法性。

当在 VM 实例上执行管理操作时或在云服务使用过程中，应当确保应用程序实例间的通信的安全。IaaS 层云用户的服务级管理员需要 root /管理员权限来远程访问由云用户部署或租用的 VM 实例，为了确保远程访问的安全需采用数字签名技术将公钥与 VM 实例中的用户账户进行关联,服务级管理员通过把公钥添加到VM实例的授权密钥文件，来识别一个云用户是否相应的私钥拥有者。在应用程序实例之间进行通信时，可以采用 TLS 进行相互鉴别。

在桌面虚拟化模式下，云用户的相关的所有程序和数据均存储在云端，因此应当采取云用户和云端设备与资源的双向鉴别和访问控制机制来确保数据的访问安全。

为了满足虚拟机的匿名身份、隐藏虚拟机的身份信息和具体的地理位置，虚拟化安全鉴别可以采用匿名鉴别机制。

（3） 存储数据访问控制

在多租户隔离鉴别方面，为了确保只有合法的用户或应用程序或虚拟机才能使用资源，需要采取基于身份鉴别的虚拟机隔离技术。可以通过采用为不同的用户或应用程序分配不同的访问密钥的方式来确保资源的合法授权访问。

（4） 网络身份鉴别

为了避免来自网络的非法访问，需要对用户、目标资源进行双向的身份鉴别，并结合访问控制技术防止对资源的非法访问，如单点登录、数据源鉴别等技术手段。

综上，IaaS 层的安全鉴别包括物理设备接入鉴别、虚拟化安全鉴别以及多租户隔离安全鉴别，上述鉴别需求可以采用基于 OAuth、OpenID 等鉴别协议，并采用匿名鉴别、多因素鉴别等机制来实现对 IaaS 层的鉴别需求。为了保障鉴别过程中鉴别凭证的安全（如令牌、口令、访问密钥等）、通信协议的安全需要采取加密、数字签名等密码措施实施保护。

5.2.3. PaaS 层云身份鉴别密码技术要求

PaaS 层主要为开发或部署应用程序的云用户提供可信计算平台和一组必要的应用程序及开发工具。在云用户使用 PaaS 层服务的过程中，需要确保云用户与应用程序或开发工具之间通信的安全性。为了确保 PaaS 层服务中开发者应用调用 API、开发者用户访问平台、应用程序之间相互访问等的安全性，安全鉴别应包括如下几个方面：

a） 云用户接入鉴别

在云用户访问云服务提供商提供的应用程序或开发工具前，需对用户身份的合法性进行验证，为了提高安全性，可以进行云用户与云服务之间的双向鉴别。

b） API 接口调用鉴别

为防止对敏感 API 的非授权访问，调用此类 API 时需要进行身份鉴别，鉴别方式可以采用基于 OAuth2.0 等鉴别协议的多因素鉴别机制，也可以采用对 API 进行数字签名以及分配访问密钥的方式进行验证。

c） 平台迁移鉴别

为了保证平台迁移过程的安全，需要采取基于身份鉴别与访问控制技术对云管理员和云用户的身份和权限进行管理。

综上，PaaS 层的安全鉴别包括云用户接入鉴别、API 接口调用鉴别以及平台迁移鉴别，上述鉴别需求可以采用基于 OAuth、OpenID、SAML 等鉴别协议的单点登录、多因素

鉴别、身份联合鉴别机制来实现对 PaaS 层的鉴别需求。为了保障鉴别过程中鉴别凭证的安全（如令牌、口令、访问密钥等）、通信协议的安全需要采取加密、数字签名等密码措施实施保护。

5.2.4. SaaS 层云身份鉴别密码技术要求

SaaS 层主要向云用户提供访问云环境中应用程序的服务。在云用户使用 SaaS 层服务的过程中，需要确保云用户与应用程序实例交互的安全性。SaaS 层服务所需的安全鉴别包括终端鉴别、SaaS 层服务接入鉴别、云用户与 SaaS 层服务的交互鉴别以及访问控制等。

终端鉴别包括用户终端鉴别以及云服务客户端程序鉴别。用户在登录终端系统时，需对用户身份的合法性进行验证，比如提供正确的用户名/口令或其他身份凭证。云服务客户端程序需采用数字签名技术，确保为云用户提供的程序来自合法的云服务提供商。

服务接入鉴别为云用户访问或登录云服务时进行身份验证的过程，如访问第三方应用程序或某个门户网站，云用户需提供正确的用户名/口令、访问密钥或其他身份凭证才能访问。

由于共用 SaaS 层服务的租户或云提供商可能会秘密查看云用户的数据，因此云用户产生的数据除需要采用加密技术存储外，云存储服务还需对其存储数据的访问者的身份进行合法性验证。

SaaS 层服务存在用户、用户组、管理员、超级用户等多种角色和权限范围，因此需要采用一种角色清楚、权限分明的访问控制方式对用户的访问权限进行控制。

同时考虑到云计算环境下云用户的便利性，使用单点登录技术和跨域鉴别技术。目前常用的一些云计算中身份鉴别方法有开放式身份鉴别协议 OAuth（用于不披露凭证的情况下进行第三方授权访问），OpenID 技术（用于联合身份鉴别、单点登录）。

综上，SaaS 层的安全鉴别包括终端鉴别、云用户接入鉴别、用户与服务的交互访问鉴别，上述鉴别需求可以采用基于 OAuth、OpenID、SAML 等鉴别协议的单点登录、多因素鉴别、身份联合鉴别机制来实现对 SaaS 层的鉴别需求。其中，终端鉴别可以采用基于 FIDO 的鉴别方式，为了保障鉴别过程中鉴别凭证的安全（如令牌、口令、访问密钥等）、通信协议的安全需要采取加密、数字签名等密码措施实施保护。

5.3.标准分类维度

为了满足云计算身份鉴别服务需求，应对其挑战，本研究报告提出了以下云计算身份鉴别服务密码标准体系架构分类方案。

本研究报告从技术维度和标准体系维度分别将云计算身份鉴别服务密码标准体系架构分为 4 个功能领域和 4 种标准文档类型，形成一个立体的标准体系架构。技术维度主要分为 4 个功能领域，分别是身份鉴别机制类、鉴别设备类、密码算法套件类、云计算身份鉴别服务提供商类,其中身份鉴别机制类又分为5个子领域,分别为身份标识类、鉴别机制类、鉴别框架与协议类、系统实现与安全测试类、身份管理类。标准体系维度分为 4 种标准类型，分别为基础类、应用类、检测类以及管理类。

5.3.1. 功能领域

云计算身份鉴别服务密码标准体系技术架构如下图所示。

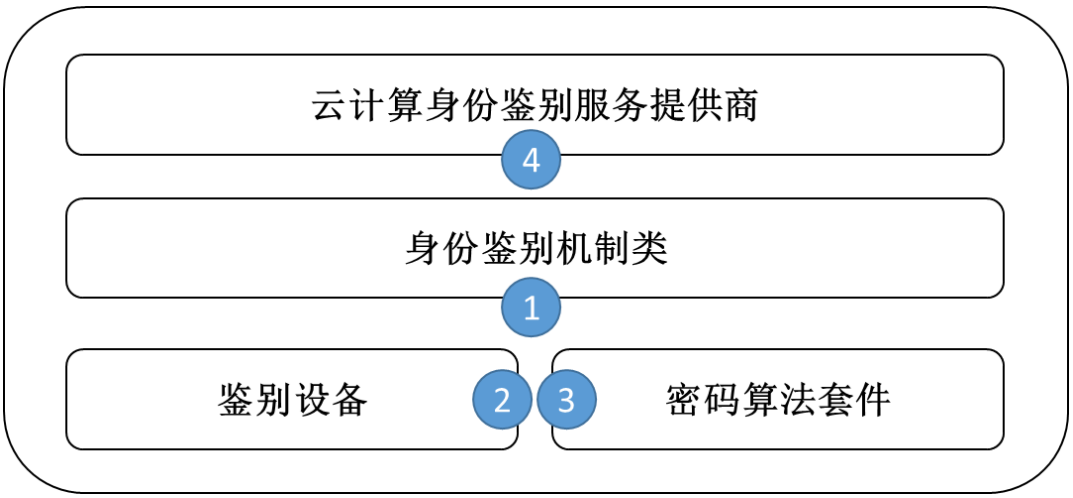

图 25 云计算身份鉴别服务密码标准体系技术架构

该体系技术架构包括如下几个功能领域：

2) 身份鉴别机制类

身份鉴别机制类是云计算身份鉴别服务密码标准体系的核心，主要内容有 5 个部分，分别是身份标识类、鉴别机制类、鉴别框架与协议类、系统实现与安全要求类、身份管理类等。

3) 鉴别设备类

鉴别设备涉及安全身份鉴别设备以及其他相关设备等。云计算身份鉴别过程中所使用的各种密码设备，如数字签名验证服务器、时间戳服务器、服务器密码机等，应遵循相应的产品和技术规范。

4) 密码算法套件类

密码算法套件包括与云计算身份鉴别服务密钥生成算法、对称加密算法、公钥算法、杂凑算法等。

5) 云计算身份鉴别服务提供商类

云计算身份鉴别服务提供商是指提供云计算身份鉴别服务的提供商等。该功能领域主要规范云计算身份鉴别服务提供商的策略、安全要求及实施和管理要求等。

5.3.2. 标准类型

在第 6.2.1 节所述的体系架构中的每一个功能域中需要标准化的文档主要围绕以下四种类型：

1) 基础类标准

基础类技术规范主要是云计算身份鉴别服务密码标准体系总体框架和各密码要素，对涉及到密码基础设施在云计算身份鉴别服务中的应用提出具体的技术要求和规范并提供指南。

2) 应用类标准

应用类技术规范是对云计算身份鉴别服务所涉及到的各种具体的身份鉴别服务业务，基于云计算身份鉴别服务密码标准体系总体框架和各密码要素，做出密码应用的技术要求和规范。

3) 检测类标准

检测类规范主要用来确保云计算身份鉴别服务对密码技术应用的有效性和合规性。

4) 管理类标准

管理类规范面向云计算身份鉴别服务系统的密码使用管理、运营机构管理、资质申请和维护提出一系列管理上的规定。从非技术因素的角度来保障云计算身份鉴别服务的的合规性。

表 2 体系结构中的标准文档类型

基础类技术规范
应用类技术规范
检测类技术规范
管理类技术规范

5.4. 标准体系架构

在本研究报告提出的体系架构中，建议的技术规范使用以下缩写表示：

TS：技术规范

在以下的内容中，对标准编号仅仅是为了叙述条理性，并非对标准发布编号的要求，例如 TS 000 代表的是总体技术规范中基础类技术规范的第 0 号技术规范。如果该技术规范已制定，则在下述每一个标准的最后一列进行标注。如果该标准具有参照性技术规范，则在标准的最后一列以“参照 XXX 标准”的形式体现。

5.4.1. 整体架构

按照功能领域维度，标准体系整体架构下图所示。

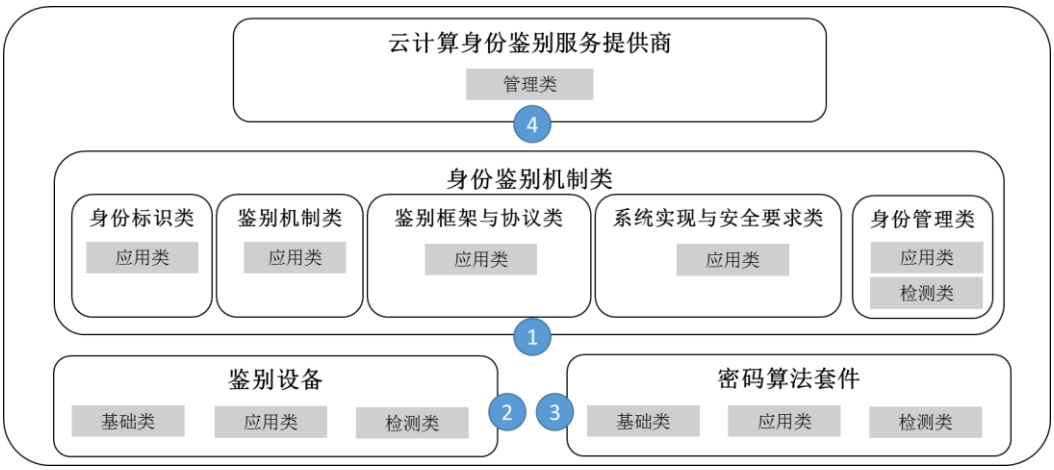

图 26 云计算身份鉴别服务密码标准体系整体架构

按照标准类型维度，标准体系架构如图 27 所示，其中绿色表示该标准已经制定并发布，红色表示该标准正在制定中，白色表示该标准尚未制定。未来的标准研制中，建议关注尚未制定的标准，针对联合身份鉴别、身份管理、密码分级检测等领域或技术点制定新的标准。

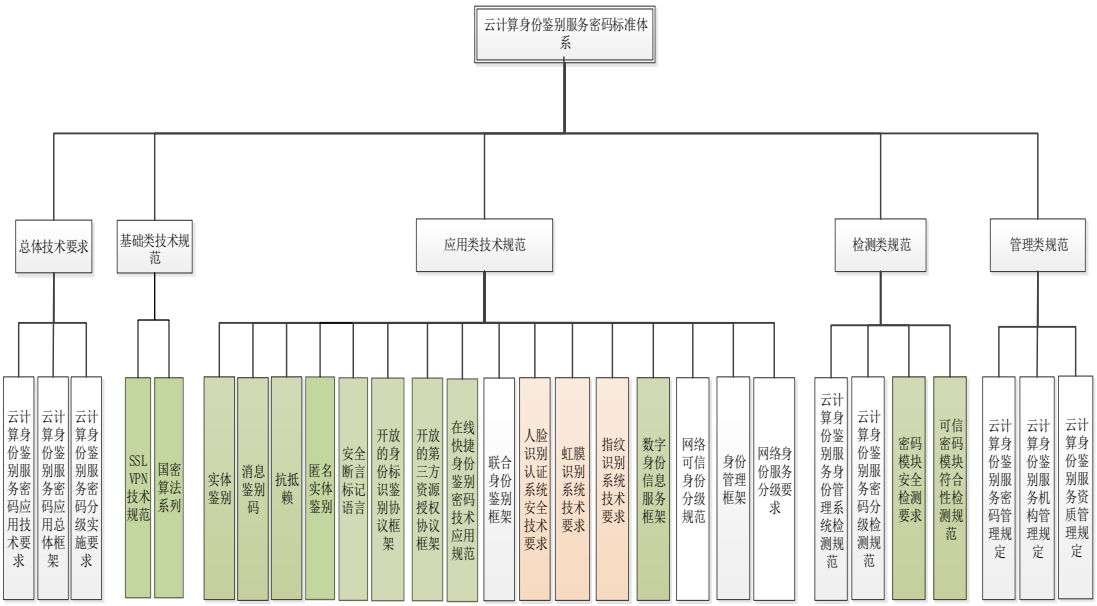

图 27 云计算身份鉴别服务密码标准体系架构

5.4.2. 总体技术要求

总体技术要求主要是对云计算身份鉴别服务在整体上提出技术要求。包括云计算身份鉴别服务密码应用技术要求、云计算身份鉴别服务密码应用总体框架、云计算身份鉴别服务密码分级实施要求。如表 3 所示，下面将对每个技术规范进行具体描述。

表 3 总体技术要求

					制定情况
	总体技术要求				
TS	0	0	0	云计算身份鉴别服务密码应用技术要求	
TS	0	0	1	云计算身份鉴别服务密码应用总体框架	
TS	0	0	2	云计算身份鉴别服务密码分级实施要求	

TS 000 《云计算身份鉴别服务密码技术应用要求》

《云计算身份鉴别服务密码应用技术要求》提出云计算身份鉴别服务的密码分级要求、密码要素以及各密码要素针对不同密码分级的具体应用要求。

TS 001 《云计算身份鉴别服务密码应用总体框架》

《云计算身份鉴别服务密码应用总体框架》提出云计算身份鉴别服务的密码应用总体技术框架并对该框架的组成结构、各组成要素进行具体的描述和说明。

TS 002 《云计算身份鉴别服务密码分级实施要求》

该文档对云计算身份鉴别服务密码分级的具体实施方法提出要求并提供指南。

5.4.3. 身份鉴别机制类规范

主要内容有五个部分，分别是身份标识类、鉴别机制类、身份鉴别框架与协议类、系统实现与安全要求类、身份管理类等。

5.4.3.1. 身份标识类

身份标识类如表 4 所示，下面将对每个标准进行具体描述。

表 4 身份标识类

					制定情况
	身份标识类				
		子领域			
			应用类		
TS	1-1	1	0	云计算身份鉴别服务个人可识别信息技术规范	参照 ISO/IEC 27018: 2014《Code of practice for PII protection in public clouds acting as PII processors》、NIST SP 800-122(2010)：《PII 机密性保护》

5.4.3.2. 应用类

TS 1-110 《云计算身份鉴别服务个人可识别信息技术规范》

要包括公有云中个人可识别信息的基本概念、个人可识别信息的确定等内容。国际上主要参照标准为 ISO/IEC 27018: 2014《Code of practice for PII protection in public clouds acting as PII processors》。

5.4.3.3. 鉴别机制类

鉴别机制类如表 5 所示，下面将对每个技术规范进行具体描述。

表 5 鉴别机制类

					制定情况
	鉴别机制类				
		子领域			
			应用类		
TS	1-2	1	0	实体鉴别	已发布国家标准：GB/T 15843 实体鉴别（共五部分），第六部分在研。以及《GB/T 28455-2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范》
TS	1-2	1	1	消息鉴别码	已发布国家标准：GB/T 15852 消息鉴别码（共两部分）
TS	1-2	1	2	抗抵赖	已发布国家标准：GB/T17903 抗抵赖（共两

					部分）
TS	1-2	1	3	匿名实体鉴别	国家标准在研： 匿名实体鉴别（共四部分）

5.4.3.3.1. 应用类

TS 1-210 《实体鉴别》

已发布国家标准：GB/T 15843 实体鉴别（共五部分），第六部分在研。以及《GB/T 28455-2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范》。

TS 1-211 《消息鉴别码》

已发布国家标准：GB/T 15852 消息鉴别码（共两部分）

TS 1-212 《抗抵赖》

已发布国家标准：GB/T17903 抗抵赖（共两部分）

TS 1-213 《匿名实体鉴别》

国家标准在研：匿名实体鉴别（共四部分）

5.4.3.4. 鉴别框架与协议类

鉴别框架与协议类如表 6 所示，下面将对每个技术规范进行具体描述。

表 6 鉴别框架与协议类

					制定情况
	鉴别框架与协议类				
		子领域			
			应用类		
TS	1-3	1	0	安全断言标记语言（SAML）	已发布国家标准： 《GB/T 29242-2012 信息安全技术 鉴别与授权 安全断言标记语言规范》
TS	1-3	1	1	开放的身份标识鉴别协议框架	密码行业标准在研： 《开放的身份标识鉴别协议框架》
TS	1-3	1	2	开放的第三方资源授权协议框架	密码行业标准在研： 《开放的第三方资源授权协议框架》
TS	1-3	1	3	在线快捷身份鉴别密码技术应用规范	密码行业标准在研： 《在线快捷身份鉴别密码技术应用规范》
TS	1-3	1	4	联合身份鉴别框架	参照 ITU-T X.1154 《多身份服务提供商环境中的联合鉴别通用框架》

5.4.3.4.1. 应用类

TS 1-310《安全断言标记语言》

根据云计算环境的身份鉴别技术需求，给出解决单点登录和跨域身份鉴别问题的SAML 身份鉴别协议及语言定义。目前有国家标准《GB/T 29242-2012 信息安全技术 鉴别与授权 安全断言标记语言规范》。

TS 1-311《开放的身份标识鉴别协议框架》

根据云计算环境的身份鉴别技术需求，规定开放的身份标识鉴别协议，使得网络中的应用（被称为第三方应用程序）可以基于某一身份鉴别服务提供方（通常是一个授权服务器）执行鉴别流程，以验证用户的身份，并获取关于用户身份标识的基本配置信息。目前有密码行业标准征求意见稿《开放的身份标识鉴别协议框架》。

TS 1-312《开放的第三方资源授权协议框架》

根据云计算环境的身份鉴别技术需求，将第三方应用程序与资源拥有者的角色进行分离，在资源拥有者的授权下，授权实体向第三方应用程序发放不同于身份凭据的令牌方式，实现开放的第三方资源授权。目前有密码行业标准征求意见稿《开放的第三方资源授权协议框架》。

TS 1-313《在线快捷身份鉴别密码技术应用规范》

根据云计算环境的身份鉴别技术需求，给出基于生物特征识别的在线快捷身份鉴别协议。目前有密码行业标准草案《在线快捷身份鉴别密码技术应用规范》。

TS 1-314《联合身份鉴别框架》

根据云计算环境的身份鉴别技术需求，给出联合身份鉴别框架，将多身份服务提供商环境中的身份服务联合起来。参照 ITU-T X.1154 《多身份服务提供商环境中的联合鉴别通用框架》。

5.4.3.5. 系统实现与安全要求类

系统实现与安全要求类如表 7 所示，下面将对每个技术规范进行具体描述。

表 7 系统实现与安全要求类

					制定情况
	系统实现与安全要求类				
		子领域			
			应用类		
TS	1-4	1	0	人脸识别认证系统安全技术要求	国家标准在研
TS	1-4	1	1	虹膜识别系统技术要求	国家标准在研
TS	1-4	1	2	指纹识别系统技术要求	国家标准在研

5.4.3.5.1. 应用类

TS 1-410 《人脸识别认证系统安全技术要求》

国家标准在研。

TS 1-411 《虹膜识别系统技术要求》

国家标准在研。

TS 1-412 《指纹识别系统技术要求》

国家标准在研。

5.4.3.6.　身份管理类

身份管理类技术规范如表 8 所示，下面将对每个技术规范进行具体描述。

表 8 身份管理类

					制定情况
	身份管理类				
		子领域			
			应用类		
TS	1-5	1	0	数字身份信息服务框架规范	国家标准已发布：《GB/T 31504-2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范》
TS	1-5	1	1	网络可信身份分级规范	待制定
TS	1-5	1	2	身份管理框架	参照 ISO/IEC 24760《身份管理框架》共三个部分，以及 IETF 的跨域身份管理框架 RFC 7642、RFC 7643、RFC 7644
TS	1-5	1	3	网络身份服务分级要求	待制定
			检测类		
TS	1-5	2	0	云计算身份鉴别服务身份管理系统检测规范	

5.4.3.6.1. 应用类

TS 1-510 《数字身份信息服务框架规范》

目前已有国家标准《GB/T 31504-2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范》

TS 1-511 《网络可信身份分级规范》

待制定标准，提出基于网络可信身份分级的基本概念和基于可信身份的分级依据，以及基于上述依据进行网络身份分级方法和策略，并定义网络身份分级的表示方式。

TS 1-512 《身份管理框架》

参照 ISO/IEC 24760《身份管理框架》共三个部分，以及 IETF 的跨域身份管理框架 RFC 7642、RFC 7643、RFC 7644。

TS 1-513 《网络身份服务分级要求》

待制定标准，定义网络身份服务的可信度概念，从安全服务要求、安全管理要求、安全技术要求、互联互通要求、隐私保护要求等方面，提出网络身份服务可信度的定性、定量度量指标体系，并依据指标体系元素建立可信度分级评价方法。

5.4.3.6.2. 检测类

TS 1-520 《云计算身份鉴别服务身份管理系统检测规范》

根据云计算身份鉴别服务身份管理系统的功能组件和性能要求，从功能、性能、安全性和互操作性等方面给出具体的身份鉴别系统的功能、性能、安全性和互操作性的检

测要求、检测方法等。

5.4.4. 鉴别设备类规范

鉴别设备类技术规范如表 9 所示，下面将对每个技术规范进行具体描述。

表 9 鉴别设备类

					制定情况
	鉴别设备类				
		子领域			
			基础类		
TR	2	0	0	SSL VPN 技术规范	GM/T 0024-2014
			应用类		
TS	2	1	0	可信密码模块接口规范	GM/T 0012-2012
TS	2	1	1	密码设备应用接口规范	GM/T 0018-2012
			检测类		
TS	2	2	0	可信密码模块接口符合性检测规范	GM/T 0013-2012
TS	2	2	1	密码模块安全检测要求	GM/T 0039-2015

5.4.4.1. 基础类

TR 200 《SSL VPN 技术规范》

该标准主要对 SSL VPN 的技术协议、产品的功能、性能和管理以及检测进行了规定。现在是密码行业标准 GM/T 0024-2014。

5.4.4.2. 应用类

TS 210 《可信密码模块接口规范》

该标准主要定义可信密码模块的接口，目前已有密码行业标准 GM/T 0012-2012。

TS 211 《密码设备应用接口规范》

主要定义密码设备应用接口相关技术规范，目前已有密码行业标准 GM/T 0018-2012。

5.4.4.3. 检测类

TS 220 《可信密码模块接口符合性检测规范》

该标准对可信密码模块接口的符合性检测作出规范，目前已有密码行业标准 GM/T 0013-2012。

TS 221《密码模块安全检测要求》

针对密码模块的安全性等方面给出具体的测评要求，目前已有密码行业标准 GM/T 0039-2015。

5.4.5. 密码算法套件类规范

密码算法套件类技术规范如表 10 所示，下面将对每个技术规范进行具体描述。

表 10 密码算法套件类

					制定情况
	密码算法套件类				
		子领域			
			基础类		
TS	3	0	0	国密算法系列	基于 GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》、GM/T 0009-2012《SM2 密码算法使用规范》、GM/T 0010-2012《SM2 密码算法加密签名消息语法规范》、GM/T 0004-2012《SM3 密码杂凑算法》、GM/T 0002-2012《SM4 分组密码算法》、GM/T 0044-2016《SM9 标识密码算法》
			检测类		
TS	3	2	0	云计算身份鉴别服务密码分级检测规范	
			管理类		
TS	3	3	0	云计算身份鉴别服务密码管理规定	

5.4.5.1. 基础类

TR 300 国密算法系列

主要包含 SMx 系列算法，GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》、GM/T 0009-2012《SM2 密码算法使用规范》、GM/T 0010-2012《SM2 密码算法加密签名消息语法规范》、GM/T 0004-2012《SM3 密码杂凑算法》、GM/T 0002-2012《SM4 分组密码算法》、GM/T 0044-2016《SM9 标识密码算法》等。

5.4.5.2. 检测类

TS 320《云计算身份鉴别服务密码分级检测规范》

该标准主要包括云计算身份鉴别服务在密码应用时的分级检测规范，确保密码分级正确，维护相关服务提供商和用户的利益。。

5.4.5.3. 管理类

TS 330《云计算身份鉴别服务密码管理规定》

该标准主要定义云计算中安全的身份鉴别服务密码管理要求，包括一系列的杂凑算法、公钥算法等等，还包括推荐的算法组合从而实现安全的云计算身份鉴别服务。

5.4.6. 云计算身份鉴别服务提供商类规范

云计算身份鉴别服务提供商类技术规范如表 11 所示，下面将对每个技术规范进行

具体描述。

表 11 云计算身份鉴别服务提供商类

					制定情况
	云计算身份鉴别服务提供商类				
		子领域			
			管理类		
TS	4	3	0	云计算身份鉴别服务机构管理规定	
TS	4	3	1	云计算身份鉴别服务资质管理规定	

5.4.6.1. 管理类

TS 430《云计算身份鉴别服务机构管理规定》

该标准包含对实施云计算身份鉴别服务密码标准体系的服务提供商的管理规定和要求。

TS 431《云计算身份鉴别服务资质管理规定》

该标准包含云计算身份鉴别服务提供商资质的申请以及维护的相关规定和要求。

参考文献

[1]The OAuth 2.0 Authorization Protocol, draft-ietf-oauth-v2-25. September, 2011.

[2] E. Hammer-Lahav, Ed. The OAuth 1.0 Protocol RFC 5984, April 2010

[3] OAuth 1.0 API Reference, Google, April, 2011

[4] OAuth Core 1.0, December, 2007

[5] OAuth Core 1.0 Revision A, June, 2009

[6] Rui Wang, Shuo Chen, XiaoFeng Wang: Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services. IEEE Symposium on Security and Privacy, 2012, 365-379.

[7] Rui Wang, Shuo Chen, XiaoFeng Wang, Shaz Qadeer, How to Shop for Free Online — Security Analysis of Cashier-as-a-Service Based Web Stores. IEEE Symposium on Security and Privacy,2011

[8] Shilpashree Srinivasamurthy, David Q. liu.Survey on cloud computing security. 2nd IEEE International Conference on Cloud Computing Technology and Science, 2010.

[9] San-Tsai Sun and Konstantin Beznosov.The Devil is the (Implementation) Details:An Empirical Analysis of OAuth SSO Systems[C], roceedings of the 2012 ACM conference on Computer and Communications Security,ACM,2012:378-390.

[10] Covert Redirect. Tetraph. May 01 2014.

[11]OpenID Authentication 2.0 – Final. http://openid.net/specs/openid-authentication-2_0.html

[12] Jan De Clercq. Single sign-on architectures. In George I. Davida, Yair Frankel, and Owen Rees, editors, Infrastructure Security, International Conference, InfraSec 2002 Bristol, UK, October 1-3, 2002, Proceedings,volume 2437 of Lecture Notes in Computer Science, pages 40-58. Springer Verlag, 2002.

[13] M Gaedke, J Meinecke. A modeling approach to federated identity and access management. Proceeding WWW'05 Special interest tracks and posters of the 14th international conference on World Wide Web Pages 1156 – 1157,2005

[14] K. D. LEWIS , J. E. LEWIS.Web Single Sign-On Authentication using SAML.International Journal of Computer Science Issues (IJCSI), Volume 1, pp41-48, August 2009

[15] Andreas Pashalidis,Chris J.Mitchell. A Taxonomy of Single Sign-On Systems. Information Security and Privacy Lecture Notes in Computer Science, 2003.

[16]Liberty Alliance. Liberty Protocols and Schemas Specication v.1.1, January 2003.

[17] Marlena Erdos ,Scott Cantor. Shibboleth-Architecture DRAFT v05,May 2002

[18]SAML V2.0, OASIS Standard. March, 2005.

[19]Passport Authentication,http://technet.microsoft.com/en-us/library/cc758561(v=WS.10).aspx , Microsoft, January 21, 2005.

[20]Using kerberos version5, IETF.MAY,2011

[21]Active Directory Federation Services (AD FS 2.0), http://technet.microsoft.com/en-us/library/dd727958(v=ws.10).aspx, Microsoft, June 9, 2011.

[22] Rui Wang, Shuo Chen, XiaoFeng Wang, Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services. IEEE Symposium on Security and Privacy, 2012, 365-379

[23] Rui Wang, Shuo Chen, XiaoFeng Wang, Shaz Qadeer, How to Shop for Free Online — Security Analysis of Cashier-as-a-Service Based Web Stores. IEEE Symposium on Security and Privacy,2011

[24] CSA guide-dom12-v2.10.Cloud Security Alliance,Domain 12: Guidance for Identity & Access Management V2.1, April 2010.

[25] Web Services Federation Language (WSFederation) Version 1.2,OASIS Standard,22 May 2009

[26] FIDO UAF Protocol Specification v1.0, FIDO Alliance Proposed Standard 08 December 2014

[27] Universal 2nd Factor (U2F) Overview, FIDO Alliance Proposed Standard 14 May 2015

[28] The Kerberos Network Authentication Service (V5), RFC 4120, IETF July 2005

[29] Lightweight Directory Access Protocol (LDAP): The Protocol, RFC 4511, IETF June 2006

[30] Remote Authentication Dial In User Service (RADIUS), RFC 2865, IETF June 2000.

[31] Rationalised structure for Electronic Signature Standardisation, TR 119 000, ETSI Sep 2013.

[32] NIST US Government CLoud Computing Technology Roadmap Volume I Release 1.0, NIST July 2013.

[33] The NIST Definition of Cloud Computing, SP 800-145, NIST Oct 2011