ICS 33.040.20
M 21

YD

中华人民共和国通信行业标准

YD/T 2917-2015

智能型通信网络支持开放标识（OpenID）和开放认证（OAuth）的技术要求

Technical requiremnets to support of OpenID and OAuth inNetwork Intelligent Capability Enhancement (NICE)

2015-07-14 发布　　2015-10-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准是智能型通信网络系列标准之一。该系列标准的名称和结构预计如下：

——《智能型通信网络 总体框架和要求》；

——《智能型通信网络 策略管控能力开放需求》；

——《智能型通信网络 策略管控能力开放架构与技术要求》；

——《智能型通信网络固定网络策略控制设备和策略执行设备技术要求》；

——《智能型通信网络 策略控制系统技术要求》；

——《智能型通信网络 支持云计算的技术要求》；

——《智能型通信网络支持云计算的广域网互联技术要求》；

——《智能型通信网络 支持开放标识（OpenID）和开放认证（OAuth）的技术要求》。

本标准参考了ITU-T建议Y.2723（2013）（在下一代网络（NGN）中支持OAuth）、Y.2724（2013）（在下一代网络中支持OAuth和OpenID的框架）和Y.2725（2014）（在下一代网络（NGN）中支持OpenID），并结合我国具体情况制定。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：上海贝尔股份有限公司、中国电信集团公司、中国信息通信研究院、中兴通讯股份有限公司。

本标准主要起草人：胡志远、周惠琴、粟　霄、李海花、郝振武、沈　蕾。

智能型通信网络
支持开放标识（OpenID）和开放认证（OAuth）的技术要求

1 范围

本标准规定了智能型通信网络对OpenID认证和OAuth授权的支持，以及智能型通信网络支持OpenID认证和OAuth授权的参考模型。

本标准适用于智能型通信网络中基于开放标识（OpenID）和开放认证（OAuth）的业务。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2592—2013 身份管理（IdM）术语

ITU-T X.800(1991) 适用于 CCITT 应用的开放系统互连安全结构(Security architecture for Open Systems Interconnection for CCITT applications)

ITU-T X.1254 (2012) 实体认证安全保证框架(Entity authentication assurance framework)

ITU-TY.2012(2012) NGN 功能要求和架构(Functional requirements and architecture of the NGN)

ITU-TY.2701 (2007) NGN 版本 1 的安全要求(Security requirements for NGN release 1)

ITU-TY.2702 (2008) NGN 版本 1 的身份认证和授权要求(Authentication and authorization requirements for NGN release 1)

ITU-T Y.2720 (2009) NGN 身份管理架构(NGN identity management framework)

ITU-TY.2721(2010) NGN 身份管理需求和应用案例(NGN identity management requirements and use cases)

ITU-TY.2722 (2011) NGN 身份管理机制(NGN identity management mechanisms)

ITU-T Y.2724 (2013) 在下一代网络中支持 OAuth 和 OpenID 的框架 (Framework for supporting OAuth and OpenID in next generation networks)

IETFRFC 6749 (2012) OAuth 2.0 授权框架(The OAuth 2.0 Authorization Framework)

IETF RFC 6750 (2012) OAuth 2.0 授权框架：承载令牌(The OAuth 2.0 Authorization Framework: Bearer Token Usage)

IETF RFC 6819 (2013) OAuth 2.0 风险模型和安全考虑(OAuth 2.0 Threat Model and Security Considerations)

3GPP TR33.924(Version 11.0.0) 身份管理和 3GPP 安全互通；身份管理和一般鉴权架构(GAA)互通(Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking)

OASISXRI SYNTAX V2.0 可扩展资源标识符（XRI）语法 2.0(Extensible Resource Identifier(XRI) Syntax V2.0)

OpenIDOpenID 认证 2.0 (OpenIDAuthentication V2.0)

Yadis 非集中的身份认证互通系统协议 (Yet Another Decentralized Identity Interoperability System (Yadis) protocol)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

（实体）认证 (Entity) Authentication

一种用来对实体和其所呈现身份之间的绑定关系进行充分确认的过程。

注1：术语“认证”在身份管理(IdM)环境中的用途是用来表示实体认证。

3.1.2

授权 Authorization

权利准许以及基于这些权利的访问准许。

[ITU-T Y.2720(2009), X.800(1991)]。

3.1.3

资源拥有者 Resource Owner

能为受保护的资源授予访问许可的实体。当资源所有者是一个人时，该资源所有者即为最终用户。

3.1.4

资源服务器 Resource Server

托管受保护的资源的服务器，能够使用访问令牌接受和响应受保护的资源的访问请求。

3.1.5

客户端 Client

一个应用，在获得资源拥有者授权情况下代表资源拥有者访问其受保护的资源。术语“客户端”，不意味着任何特定的实现特性（例如，应用是否在服务器、桌面或其他设备上执行）。

3.1.6

授权服务器 Authorization Server

在成功认证资源拥有者并获得授权后，服务器向客户端发放访问令牌。

3.1.7

授权许可 Authorization Grant

代表资源拥有者授权（访问其受保护资源）的一种信任凭证，客户端可以凭借授权许可获取一个访问令牌。

3.1.8

访问令牌 Access Token

用于访问受保护资源的信任凭证。访问令牌是一个字符串，代表发放给客户端的授权。该字符串通常对客户端不透明。令牌代表具体的访问范围和访问持续时间，这些范围值和令牌生命周期由资源拥有者授予，由资源服务器和授权服务器执行。

3.1.9

机密类型客户端 Confidential Clients

该类型的客户端能安全管理其认证凭证的机密性（例如，实现在安全服务器上的客户端，而且该服务器受限地访问客户端的凭证），或能使用其他方式对客户端进行安全认证。

3.1.10

公开类型客户端　Public Clients

该类型的客户端不能确保其认证凭证的机密性，（在资源拥有者的设备上执行，如本地应用或基于用户代理的应用），且不能使用其他方式执行客户端的安全认证。

3.1.11

实体　Entity

独立存在并在环境中能被识别的事物。

注：实体可以是一个自然人、动物、法人、组织、主动或被动物、设备、软件应用、服务等，或一组这样的实体。在电信领域中，实体的范例包括访问点、用户、网元、网络、软件应用、服务、设备和接口等。

3.1.12

身份服务提供商（身份服务提供方）　Identity Service Provider (IdSP)

一个验证、维护、管理且能为其他实体生成和分配身份信息的实体。

3.1.13

身份提供者　Identity Provider (IdP)

见身份服务提供商（身份服务提供方）。

3.1.14

标识符　Identifier

在环境中用来识别一个实体的一个或多个属性。

3.1.15

更新令牌　Refresh Token

由授权服务器下发到客户端，并在当前的访问令牌无效或过期时，用来获取新的访问令牌，或获得额外的具有相同或更窄的范围的访问令牌（相对资源拥有者的授权，访问令牌可能寿命较短，权限较少）。下发更新令牌是根据授权服务器的判断灵活可选的。如果授权服务器下发更新令牌，会包括何时发出访问令牌。

3.2　缩略语

下列缩略语适用于本文件。

AKA	Authentication and Key Agreement	认证和密钥协商
ANI	Application-to-Network Interface	应用到网络接口
API	Application Programme Interface	应用编程接口
GBA	Generic Bootstrapping Architecture	通用自举架构
HAMC	Keyed-hash Message Authentication Code	基于密钥的哈希消息认证码
IdM	Identity Management	身份管理
IdP	Identity Provider	身份提供者
IdSP	Identity Service Provider	身份服务提供商
NGN	Next Generation Networks	下一代网络
NNI	Network NetworkInterface	网络网络接口
OAuth	Open Authentication	开放认证

OP	OpenID Provider	OpenID 提供者
OpenID	Open Identification	开放标识
SAML	Security Assertion Markup Language	安全断言标记语言
SHA	Secure Hash Algorithm	安全哈希算法
SNI	Service Network Interface	业务网络接口
TLS	Transport Layer Security	传输层安全协议
UNI	User Network Interface	用户网络接口
URI	Uniform Resource Identifier	统一资源标识符
URL	Uniform Resource Locator	统一资源定位符
XML	eXtension Markup Language	可扩展的标记语言
XRDS	Extensible Resource Descriptor Sequence	扩展资源描述符的顺序
XRI	Extensible Resource Identifier	可扩展资源标识符
Yadis	Yet Another Decentralized Identity Interoperability System	非集中的身份认证互通系统协议

4 智能型通信网络支持 OpenID 认证和 OAuth 授权的参考模型

智能型通信网络支持 OpenID 认证和 OAuth 授权的参考模型，如图 1 所示。智能型通信网络包含多个功能单元（具体描述见 ITU-T Y.2720（2009）。这些功能单元使用实体身份标识来实现用户身份的关联，为其他提供商提供开放式身份认证服务。功能实体 OpenId 和 OAuth 与智能型通信网实体之间的接口，目前并没有相关的国际国内标准，该接口的实现由运营商定义。

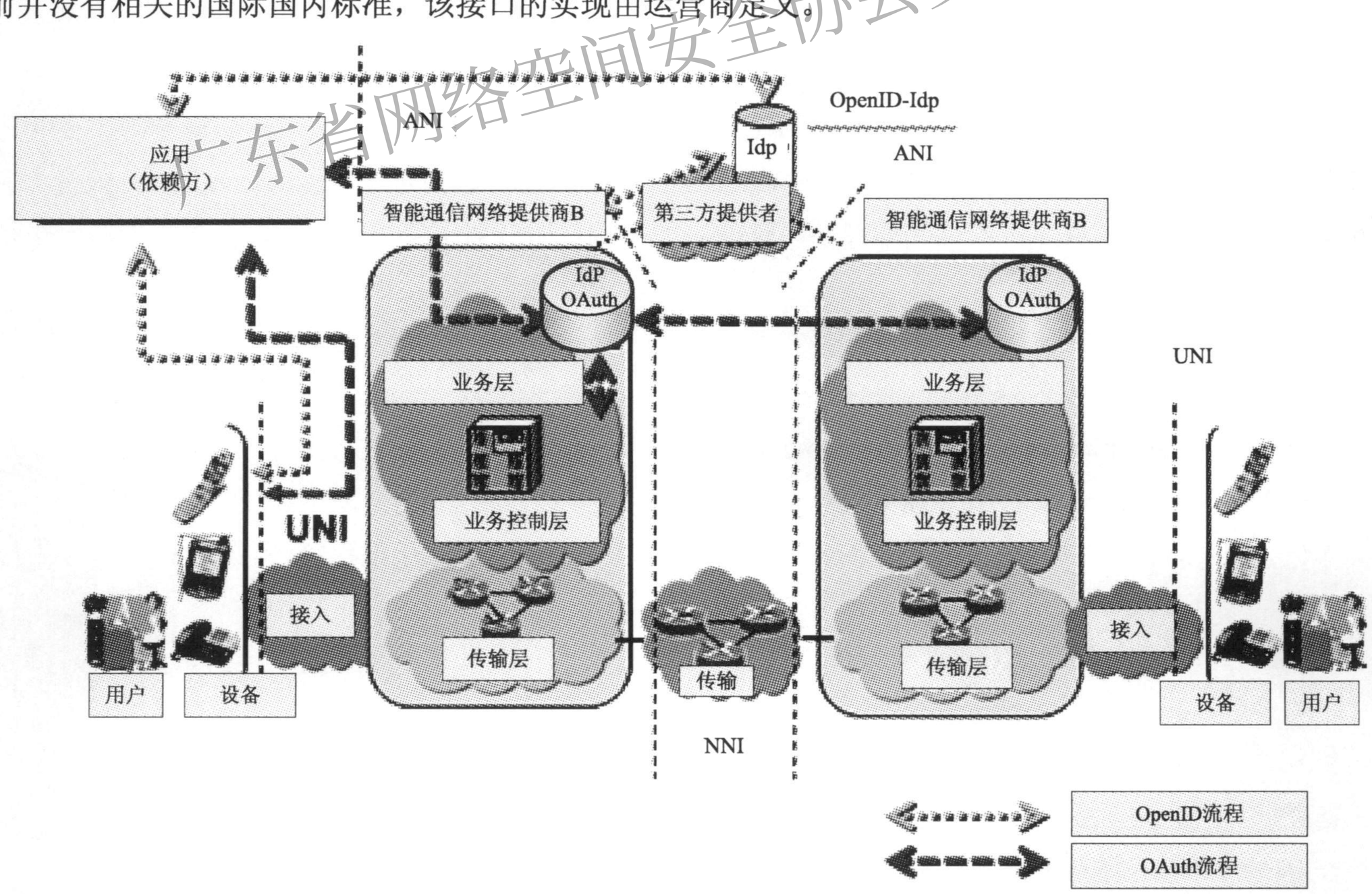

图1 智能型通信网络支持 OpenID 认证和 OAuth 授权的参考模型

智能型通信网络提供商可以使用 OpenID 和 OAuth 提供 IdSP 服务，并可与内容和应用提供商和/或其

他服务提供商进行合作。

OpenID是一种通过 URI 来认证用户身份的技术。

OAuth是一种能让第三方应用无需知道用户秘密信息（如用户名/密码）而申请访问用户资源的技术。

智能型通信网络能支持话音、数据和多媒体等多种业务，具有开放的业务API接口以及对业务灵活的配置和客户化能力。

通过在智能型通信网络中使用OpenID和OAuth，更便于用户安全地访问业务；同时也能让网络提供商安全地以业务API接口方式开放其网络能力，以支持多服务提供商环境下的应用能快速地开发、部署及安全地投入运营。

5 智能型通信网络对 OpenID 的支持

5.1 OpenID 的协议消息格式

OpenID的协议应使用OpenID认证2.0。

支持智能型通信网络的实体在发送一个协议消息时，应符合OpenID认证2.0中定义的键值形式的编码和HTTP编码两种协议消息格式的相关要求。

5.2 通信类型

支持智能型通信网络的实体在发送一个协议消息时，应符合OpenID认证2.0中定义的直接通信和间接通信相关要求。

5.3 生成签名

OpenID认证支持两种签名算法：

- HMAC-SHA1 - 160 比特密钥长度；
- HMAC-SHA256 - 256 比特密钥长度。

本标准建议使用 HMAC-SHA256。

5.4 智能型通信网络中的 OpenID 认证过程

5.4.1 认证请求

5.4.1.1 发起 OpenID 认证请求的相关规定

本标准要求应用方（依赖方）在智能型通信网络中使用Yadis协议来发布其有效的“返回到”（return_to）URL消息。

有关认证请求的规定见OpenID认证2.0的第9章。

应用（依赖方）与最终用户交互时，应：

- 发起OpenID认证；
- 规范化用户提供的标识符；
- 为发起请求发现必要信息。

本标准要求应用（依赖方）实体在智能型通信网络中呈现的表单内列入openid_identifier字段，该字段定义见OpenID认证2.0的7.1节。

5.4.1.2 规范用户提供的标识符

本标准定义了三种类型的标识符：“http”或“https”、 URI（在本文件中通常被称为一个“URL”，其相关定义见OpenID认证2.0的第7章），或XRI，其相关定义见OASIS XRI SYNTAX V2.0。

5.4.1.3 为发起请求发现必要信息

本标准中的发现功能是应用（依赖方）使用标识符来为发起请求查找（“发现”）必要信息的过程。

本标准可通过三种手段来完成上述发现，其相关规定见OpenID认证2.0的7.3节。

本标准定义了两种发现方法：基于XRDS的发现和基于HTML的发现。若使用的是XRI ，见OASISXRI SYNTAX V2.0或Yadis发现，则结果将为一份XRDS文档。这是一份XML文档，其中的条目所对应的服务与标识符相关，相关规定见OpenID认证2.0的7.3.2.1节。基于HTML的发现应得到各应用（依赖方）的支持。基于HTML的发现仅可用于声明标识符的发现。OP标识符应是XRI见OASIS XRI SYNTAX 2.0或支持XRDS发现的URL。要使用基于HTML的发现，应在声明标识符的URL上提供一份HTML文档，相关规定见OpenID认证2.0的7.3.3节。

本标准要求应用（依赖方）在执行发现时宜采用标识符授予 XRI 或 URL 格式。

5.4.2 认证响应

5.4.2.1 发起认证响应的相关规定

本标准中，当认证请求来自借助间接沟通的用户代理时，则宜由OP确定经授权的最终用户是否希望完成认证。若经授权的最终用户希望完成认证，则宜由OP向应用（依赖方）发出一个肯定断言（positive assertion），其相关描述见OpenID认证2.0的第10章。

本标准要求在授权请求中列入“return_to”参数。

注：识别经授权的最终用户以及获得批准以返回一个OpenID认证断言的方法已超出本标准的范围。

5.4.2.2 肯定断言（Positive Assertions）

肯定断言为间接响应，关于响应参数的信息见 OpenID 认证 2.0 的 10.1 节。

本标准规定当 OP 通过用户代理与应用（依赖方）进行间接通信时，应：

- 进行验证，以确保 return_to URL 与应用（依赖方）的一个端点匹配；
- 确定经授权的最终用户是否希望完成认证；
- 生成响应随机数；
- 对肯定响应进行签名；
- 通过用户代理向应用（依赖方）发送肯定断言。

5.4.2.3 否定断言（Negative Assertions）

若OP无法识别最终用户，或最终用户没有或不同意认证请求时，则OP向应用（依赖方）发送一个否定断言，并将其作为一种间接响应OpenID认证2.0。

若响应中收到一个“checkid_immediate”模式请求的否定断言，则应用（依赖方）使用“checkid_setup”模式构造一个新的认证请求。

5.4.2.4 对即时请求的响应

若请求为即时请求，最终用户将不能通过与OP上的网页进行交互，来提供认证凭证或对请求的批准。即时请求的否定断言应采用OpenID认证2.0的10.2.1节中规定的格式。

5.4.2.5 对非即时请求的响应

由于OP可向终端用户显示网页，并向最终用户请求获得认证凭证，因此对某一非即时请求的否定响应是确定的，且其应采用OpenID认证2.0的10.2.2节中规定的格式。

若应用（依赖方）收到“取消”响应，则表明认证不成功，且应用（依赖方）必须将最终用户视为未经认证。

5.4.3 验证断言

根据OpenID认证2.0，在收到肯定断言时，应用（依赖方）应：

- 验证返回的URL；
- 验证所发现的信息；
- 检查响应中相关随机数；
- 验证签名。

在验证断言后，若断言包含一个声明标识符，即可认为用户已通过此标识符获得认证。

5.5 安全考虑

智能型通信网络应考虑用户代理、用户界面、HTTP和HTTPS URL标识符以及协议变种等带来的相关安全问题。

以上安全问题的解决方案应符合ITU-T Y.2701（2007）第8章、ITU-T Y.2720（2009）的8.7节、ITU-T Y.2721（2010）的8.7节规定的安全要求。

6 智能型通信网络对 OAuth 的支持

6.1 基于智能型通信网络安全要求的 OAuth 客户端类型的选择

OAuth 有两种客户端类型：机密类型的和公开类型的客户端，具体见 IETF RFC6749 的 2.1 节。

公开类型的客户端不符合智能型通信网络第三方应用提供商的认证要求，此认证要求见 ITU-T Y.2702 第 7、8 章，因为公开类型客户端不能由智能型通信网络提供商对其进行身份认证。本标准中智能型通信网络仅支持机密类型客户端，其相关认证要求见 ITU-T Y.2724 的 6.2 节。智能型通信网络支持的客户端应满足以下要求：

a）智能型通信网络的 OAuth 客户端在特定的安全保证级别应可认证，应符合 ITU-T Y.2702（2008）第 7、8 章，ITU-T X.1254（2012）第 6 章的规定；

b）智能型通信网络的 OAuth 客户端必须在授权服务器注册，应符合 IETF RFC6749 中第 2 章的规定。

智能型通信网络支持的客户端仅支持 Web 应用，其相关认证要求见 IETF RFC6749 的 2.1 节。

6.2 授权许可类型的选择

授权许可有以下 4 种类型：授权码许可、隐式的许可、资源拥有者口令凭证许可和客户端认证凭据许可。这 4 种类型的授权许可见 IETF RFC6749。此外，关于 OAuth2.0 的 SAML 2.0 断言许可类型的详细扩展见 IETFRFC 6750。当隐式许可过程中发出访问令牌时，授权服务器不需要认证客户端。在某些情况下，客户端的身份可以通过用于提供给客户端访问令牌的重定向 URI 来验证。访问令牌可能会暴露给资源拥有者或其它可访问资源拥有者的用户代理的应用，应用的相关认证见 IETF RFC6749。

因此，使用隐式许可类型的 OAuth 过程，不会产生符合智能型通信网络第三方应用提供商的认证要求，其认证要求见 ITU-T Y.2702 第 7.8 章。

智能型通信网络所支持的 Web 应用的机密型客户端能使用以下授权许可：

- 授权码（Authorization code）；
- 资源拥有者口令认证（Resource owner password credentials）；
- 客户端证书（Client credentials）；
- SAML 2.0 断言（SAML 2.0 assertion）。

6.3 智能型通信网络所支持的客户端的 OAuth 选项建议

6.3.1 客户端注册

本标准要求智能型通信网络支持的客户端向授权服务器注册其重定向的 URI，能保证客户端具有更高的安全性，具体描述见 IETF RFC6749 的 2.2 节。

6.3.2 客户端重定向端点的消息的机密性保护

当请求的应答类型是“授权码”或“令牌”时，或当重定向请求会导致敏感凭据在公开网络传输时，重定向端点应按照 IETF RFC6749 的 1.6 节所述，要求使用 TLS。本标准要求使用 TLS 传输所有敏感信息。

6.3.3 客户端身份验证

Web 应用的客户端是机密类型客户端，因此，该客户端应向授权服务器进行认证。

6.3.4 授权过程

6.3.4.1 授权许可类型

Web 应用使用以下授权许可：

- 授权码（Authorization code）；
- 资源拥有者口令凭证（Resource owner password credential）；
- 客户端证书（Client credentials）；
- SAML 扩展（SAML extension）。

6.3.4.2 授权码

本标准规定了使用授权码的机密类型客户端的授权流程，要求把参数 redirect_uri 列入到授权请求中，见 IETF RFC6749 的 4.1 节。

下列需求适用于授权服务器与使用授权码的 Web 应用客户端之间的交互。授权服务器应：

- 认证发出授权请求的客户端；
- 确保客户端的授权请求中的参数 redirect_uri 的值，与客户端的注册值相匹配；
- 仅对认证和授权成功的客户端下发授权码；
- 在下发访问令牌前，确保授权码是有效的。

6.3.4.3 资源拥有者口令认证

使用该许可类型的授权流程是对与资源所有者建立了信任的授权客户端进行了优化。客户端使用资源拥有者的口令凭证获取授权服务器发放的访问令牌。该流程能满足智能型通信网络的安全要求，具体规定见 IETF RFC6749 的 4.3 节。

注：IETF RFC6749 中的 2.1 节允许公开客户端使用本流程。本标准只考虑机密类型的客户端，即这些客户端需要向授权服务器进行身份认证。

当授权服务器与使用授权类型为资源所有者口令认证的客户端交互时，应：

- 认证客户端身份；
- 验证客户端提供的资源拥有者口令凭证的有效性；
- 如果客户端已通过授权服务器认证并出示了有效的资源拥有者凭证，发放一个访问令牌。

6.4 资源拥有者的身份认证

IETF RFC6749 没有规定授权服务器对资源拥有者（例如，最终用户）身份的认证。在智能型通信网络环境中，资源拥有者的身份认证机制，应满足 ITU-T Y.2702 第 7、8 章的要求。

6.5 安全性考虑

IETF RFC6749 的第 10 章为所有 OAuth2.0 的客户端特征——Web 应用、基于用户代理的应用、本地应用提供了安全指南。本标准对智能型通信网络的 Web 应用客户端的支持给出了建议。因此，本规范只需要考虑 Web 应用客户端带来的安全问题，具体规定及解决方案见 IETF RFC6749 的 2.1 节。此外，IETF RFC6819 的第 2 章为协议设计提供了一个全面的 OAuth 安全模型和背景介绍。在智能型通信网络中实现 OAuth 时，应考虑 IETF RFC6819 的第 5 章中与 Web 应用客户端相关的信息。

解决方案还应满足 ITU-T Y.2701 中第 8 章、ITU-T Y.2720 的 8.7 节、ITU-T Y.2721 的 8.7 节中规定的安全需求。

7 智能型通信网络支持 OAuth 和 OpenID 的消息流

7.1 消息流程涉及的实体

智能型通信网络支持 Web 应用的机密类型客户端。7.2 节、7.3 节和 7.4 节定义了实体参与 OAuth 和 OpenID 的消息流程。

根据 OpenID 认证 2.0 对 OpenID 的说明，OpenIDIdP 服务器参与整个认证工作流程，并且 OAuth 允许应用（依赖方）通过 OAuth 协议直接发送认证消息给智能型通信网络-IdP。

7.2 OAuth 和 OpenID 流程涉及的公共实体

OAuth 和 OpenID 流程均涉及到的实体如下：

- 具有 Web 客户端能力的最终用户功能（例如浏览器）；
- 应用网关功能实体见 ITU-T Y.2012 的 9.3.5 节，该功能实体应支持 OAuth 和/或 OpenID 协议。

ITU-T Y.2012 的 9.3.5 节中定义了应用网关功能实体，是使智能型通信网络的各种功能和所有外部应用服务器及业务引擎之间进行互通的实体。这使应用网关功能实体成为一个为 OpenID 和 OAuth 提供支持的合乎逻辑的选择。此外，应用网关功能实体与业务用户配置文件功能实体相连接（业务用户配置文件功能实体见 ITU-T Y.2012 的第 7 章），应用网关功能实体应支持基于 AKA 的用户设备认证，包括通用自举架构（GBA）。基于 GBA 的 OpenID 认证方法见 3GPP TR33.924 中第 4 章的详细定义。OpenID 的另一种认证方法是基于 AKA，在一些方面和 GBA 类似，见 ITU-T Y.2722 的 6.2.8 节。如何在应用网关功能实体上实现 OAuth 授权服务器和 OpenIDIdP 见 ITU-T Y.2722 的 6.2.9 节，它们通过与业务用户配置文件功能实体交互使用基于 AKA 的认证。

7.3 OpenID 流程涉及的特定实体

以下为针对 OpenID 的特定实体：

- OpenIDIdP 执行认证的应用服务器；
- OpenIDIdP 作为应用网关功能实体的一部分进行实现，为支持基于 AKA 的认证，该实体必须能够与业务用户配置文件功能实体进行通信；
- 如果智能型通信网络采用基于 AKA 的认证方法对最终用户进行认证，则需要支持 OpenID 身份认证的业务用户配置文件功能实体的具体要求见 ITU-T Y.2722 中第 7 章的规定。

OpenID 消息流程如图 2 所示。该流程用于在 IdP 和应用服务器已经建立了一个共享秘密（secret）的情况下。该秘密用于对包含有 IdP 认证结果的信息进行签名，并让应用服务器来对签名消息进行验证。

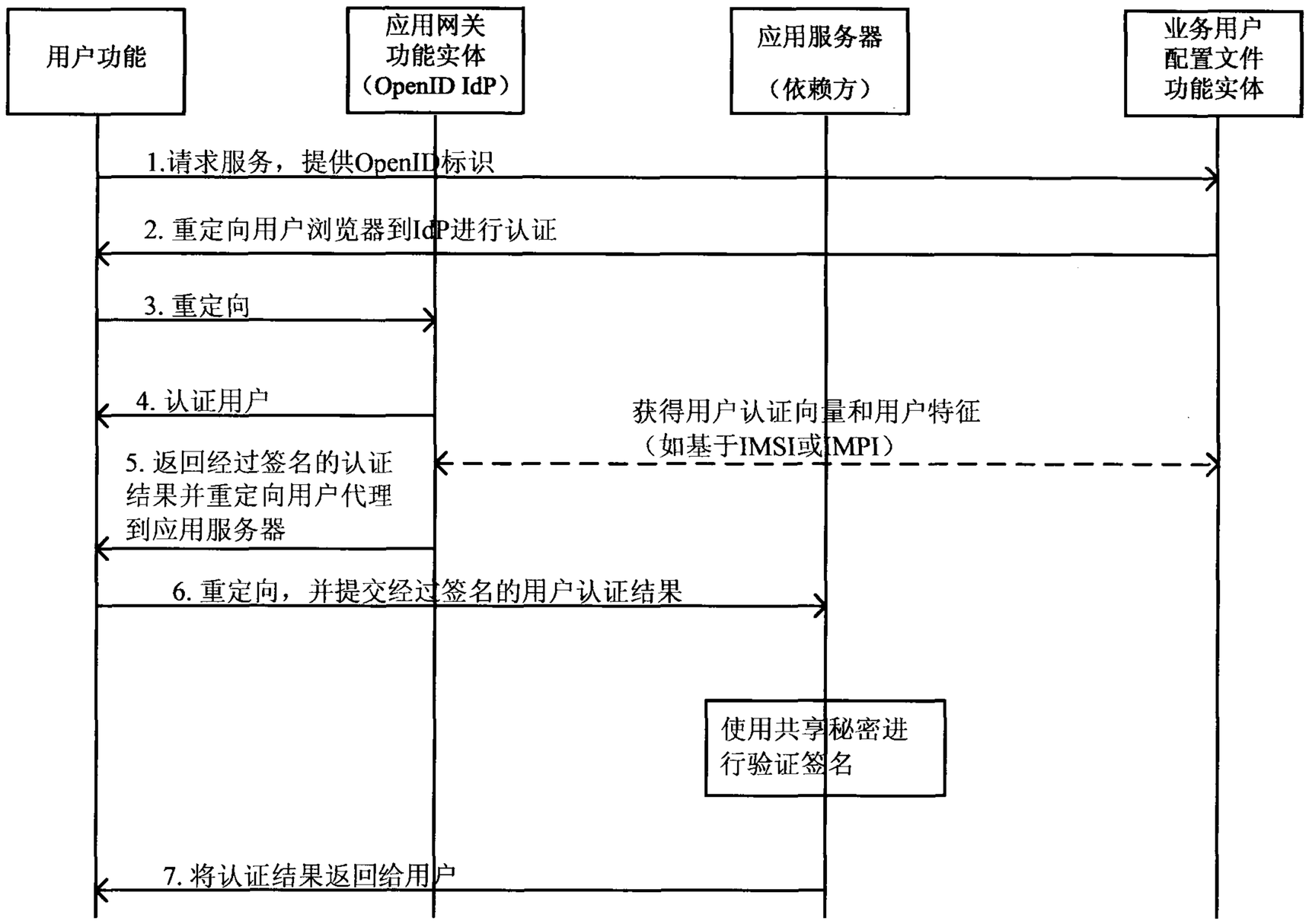

图2　OpenID 流程

该流程的详细描述如下：

1） 用户浏览器向应用服务器发送服务请求，该请求中包含用户的 OpenID 标识符；

2） 基于 OpenID 标识符，应用服务器首先找到用户的 OpenIDIdP，然后重定向用户的浏览器到 OpenIDIdP 并进行身份认证；

3） 浏览器遵循重定向请求；

4） OpenIDIdP 通过用户浏览器交互信息来认证用户，如果 OpenIDIdP 执行基于 AKA 的身份认证（见 ITU-T Y.2722），它需要与业务用户配置文件功能实体交互，这种交互由虚线箭头表示；

5） OpenIDIdP 将用户浏览器重定向回到应用服务器，响应中包含认证成功的签名消息；

6） 浏览器遵循重定向请求并传递签名消息到应用服务器。

7） 在验证签名并检查认证结果之后，应用服务器向用户通知认证是否成功。签名和验证过程见 OpenID 认证 2.0。

7.4　OAuth 流程涉及的特定实体

以下为针对 OAuth 的特定实体：

- 为用户执行服务的 Web 应用程序服务器，即一个 OAuth 客户端。该客户端可以但并不一定运行在智能型通信网络实体上。

- 授权服务器作为应用网关功能实体的一部分进行实现。授权服务器首先执行用户认证，然后进行客户端请求授权。如果这两个过程都成功，OAuth 交互的结果是授权服务器向客户端下发一个访问令牌。为了支持基于 AKA 认证，授权服务器应能够与业务用户配置文件功能实体通信。本标准第 5 章规定的智能型通信网络对 OpenID 的支持也使用在图 3 的用户认证过程中，因此本章节的 OAuth 流程实际上是智能型通信网络对 OpenID 和 OAuth 的融合支持流程。

• 资源服务器为具有有效访问令牌的客户端请求提供服务。IETF RFC 6749 中第 7 章详细规定了使用访问令牌获取资源访问的两种流程定义。资源服务器可能或可能不与应用网关功能实体中的授权服务器部署在相同的位置。

图 3 所示为用于 Web 服务应用案例（参见附录 A）的 OAuth 消息流程。

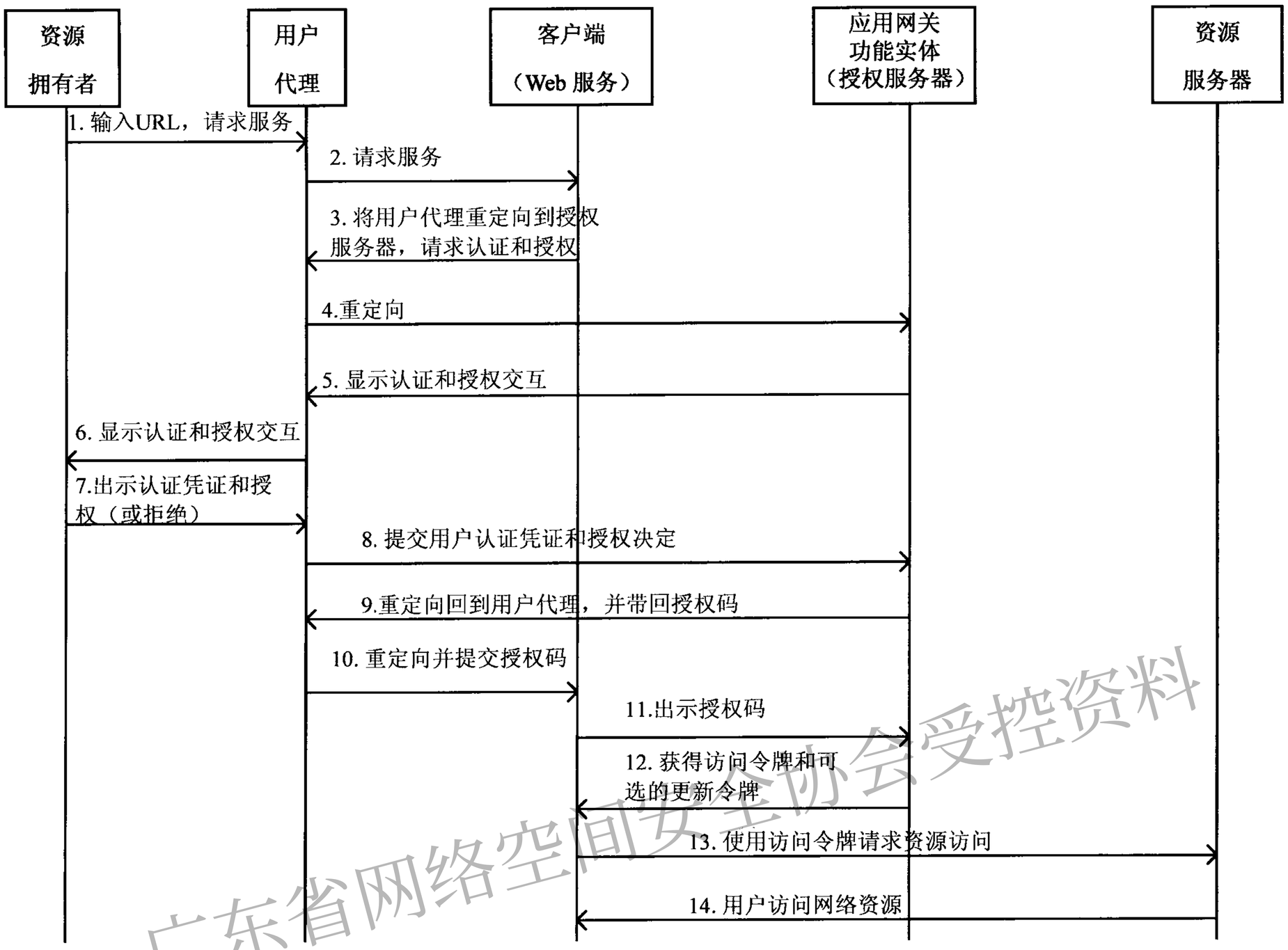

图3　Web 服务器应用案例的 OAuth 流程

该流程的详细描述如下：

1） 用户指示用户代理（如浏览器）从客户端请求服务；

2） 用户代理向客户端递交请求；

3） 客户端给出响应，并重定向用户代理到授权服务器来进行客户端请求的用户身份认证和授权；

4） 用户代理遵照该重定向；

5） 授权服务器响应，提供认证和授权接口给用户代理；

6） 用户代理显示认证和授权接口给用户（资源拥有者）；

7） 用户提供身份认证凭证，并使用用户代理表明授权决定；

8） 用户代理将用户提供的数据发送到授权服务器；

9） 授权服务器在认证用户身份并确保用户已经授权客户端的请求后，将用户代理重定向回客户端，该响应包括授权代码；

10） 用户代理遵从重定向将授权码交付到客户端；

11） 客户端发送授权码到授权服务器；

12） 授权服务器返回访问令牌和可选的更新令牌；

13） 客户端发送请求到资源服务器并提供访问令牌；

14） 资源服务器提供请求的资源。

附 录 A
（资料性附录）
应用案例

A.1 应用案例Web服务器

A.1.1 应用案例Web服务器的描述

Alice在WWW.X printphotos.example上访问运行在Web服务器上的应用，并指示它来打印存储在服务器WWW.X storephotos.example上的她的照片。Alice与智能型通信网络服务提供商进行签约，该智能型通信网络服务提供商在WWW.X carrier.example运行OAuth授权服务器。WWW.X-printphotos.example上的应用接收Alice的授权后通过WWW.X storephotos.example或WWW.X carrier.example去访问Alice的照片时，不需要知道Alice的认证凭证。

A.1.2 应用案例Web服务器的前置条件

前置条件如下：

- Alice 已在 WWW.X carrier.example 上注册以启用身份认证；
- WWW.X-printphotos.example 上的应用已在 WWW.X carrier.example 上的 OAuth 授权服务器注册，并建立了身份认证凭证；
- WWW.X-storephotos.example 上的应用能够验证在 WWW.X-carrier.example 上的授权服务器下发的访问令牌的有效性。

A.1.3 应用案例Web服务器的后置条件

一个成功过程的结果是 WWW.X-printphotos.example 上的应用从 WWW.X-carrier.example 获得授权码。该授权码同时绑定到 WWW.X-printphotos.example 上的应用和由应用提供的回传 URL。WWW.X-printphotos.example 上的应用使用授权码来从 WWW.X-carrier.example 获得访问令牌。WWW.X-carrier.example 上的应用认证 WWW.X-printphotos.example 上的应用并验证提交的授权码的有效性后，下发访问令牌。WWW.X-printphotos.example 上的应用使用访问令牌来访问在 WWW.X-storephotos.example 上的 Alice 的照片。

当访问令牌过期时，WWW.X-printphotos.example 上的服务需要重复 OAuth 过程以获得 Alice 的授权去访问她在 WWW.X-storephotos.example 的照片。另外，如果 Alice 想许可一个应用长期访问她在 WWW.X-storephotos.example 的资源，WWW.X-carrier.example 的授权服务器可以下发长生命周期的令牌。这些令牌可以转换为访问 WWW.X storephotos.example 上的资源所必需的短生命周期访问令牌。

A.1.4 应用案例Web服务器的要求

要求如下：

- 运行 OAuth 客户端的服务器 WWW.X-printphotos.example，应能将 HTTP 重定向请求发送到 Alice 的用户代理，即浏览器。
- WWW.X carrier.example 上的授权服务器应能认证 Alice，具体认证方法不在规范 OAuth 中定义。
- 在 WWW.X-carrier.example 上的应用应获得 Alice 的授权，使得 WWW.X-printphotos.example 上应用能访问到她的照片。
- 在 WWW.X-carrier.example 上的应用可识别 Alice 的访问范围，该范围值是在要求 Alice 授权时 WWW.X printphotos.example 上应用已请求获得的。

• WWW.X-carrier.example 上的授权服务器在下发访问令牌前，应能认证 WWW.X-printphotos.example 的应用并能验证授权码的有效性。在 WWW.X-printphotos.example 的应用应提供一个回传 URL 给 WWW.X-carrier.example 的授权服务器。其中，URL 应预先在 WWW.X-carrier.example 上注册。

• WWW.X-carrier.example 的授权服务器应能保存一个记录，该记录是保留授权码与 WWW.X-printphotos.example 的应用以及由该应用提供的回传 URL 的关联。

• 访问令牌是 Bearer's Token（这些令牌不与 WWW.X-printphotos.example 的特定应用相关联），且有效时间短。

• WWW.X-carrier.example 的授权服务器应能在授权码第一次使用后，撤销其授权许可。

• Alice's manual involvement in the OAuth authorization procedure (e.g., entering an URL or a password) should not be required. (Alice's authentication to WWW.X-carrier.example is not in the OAuth scope) 不应该要求 Alice 人工参与 OAuth 授权过程（如，输入一个 URL 或口令），Alice 向 WWW.X-carrier.example 的认证，不在 OAuth 规范中定义。

A.2 应用案例客户端认证凭证

A.2.1 应用案例客户端认证凭证的描述

Good-X-Pay 公司为 Good-X-Work 公司的雇员管理工资清单。为了做到这一点，WWW.Good-X-Pay.example 上的应用，通过认证访问存储在 WWW.Good-X-Work.example 的员工考勤数据。授权服务器执行身份认证，其中授权服务器是 URL 为 WWW.X-carrier.example 的智能型通信网络的一部分。

A.2.2 应用案例客户端认证凭证的前置条件

前置条件如下：

• WWW.Good-X-Pay.example 的应用在 WWW.X-carrier.example 的授权服务器进行注册，并获得一个身份标识符和一个共享秘密；

• 定义好 WWW.Good-X-Pay.example 上的应用对存储在 WWW.Good-X-Work.example 上的数据的访问范围。

A.2.3 应用案例客户端认证凭证的后置条件

一个成功过程的结果是：WWW.Good-X-Pay.example 的应用通过 WWW.X-carrier.example 的授权服务器的身份验证后，会获得一个访问令牌。WWW.Good-X-Pay.example 的应用使用该访问令牌访问 WWW.Good-X-Work.example 的考勤数据。

A.2.4 应用案例客户端认证凭证的要求

要求如下：

• WWW.Good-X-Pay.example 的应用应向 WWW.X-carrier.example 的授权服务器进行认证；

• 应基于身份标识符和共享秘密进行身份认证，其中该身份标识和共享秘密由运行在 WWW.Good-X-Pay.example 的应用在最初的 HTTP 请求中，提交给 WWW.X-carrier.example 的授权服务；

• 因为该流程的结果需要访问 Good-X-Work 公司的敏感数据，因此 Good-X-Work 应与 Good-X-Pay 公司及在 WWW.X-carrier.example 的授权服务器建立信任关系。

A.3 应用案例断言

A.3.1 应用案例断言的描述

Good-X-Pay 公司为 Good-X-Work 公司雇员管理工资清单。为了做到这一点，WWW.Good-X-Pay.

example 的应用，获得认证访问存储在 WWW.Good-X-Work.example 的员工的考勤数据。WWW.Good-X-Work.example 的服务器，使用由 WWW.X-carrier.example 的授权服务器下发的一个访问令牌，访问 WWW.Good-X-Pay.example 的应用。WWW.X-carrier.example 的授权服务器通过验证由 WWW.Good-X-Pay.example 所提交断言的有效性，来认证 WWW.Good-X-Pay.example 的应用。

该应用案例描述了一个可替代客户端认证凭证所描述的方案的解决方案。

A.3.2 应用案例断言的前置条件

前置条件如下：

- WWW.Good-X-Pay.example 的应用已从 WWW.X-carrier.example 的授权服务器所信任的一方处获得认证断言；
- 定义好 WWW.Good-X-Pay.example 的应用对存储在 WWW.Good-X-Work.example 的数据的访问范围；
- WWW.X-carrier.example 的授权服务器已与断言方建立信任关系并能够验证它所发放的断言的有效性。

A.3.3 应用案例断言的后置条件

一个成功的流程结果是 WWW.Good-X-Pay.example 的应用，通过提交断言（例如 SAML 断言）到 WWW.X-carrier.example 的授权服务器进行成功认证以后，会获得一个访问令牌。通过使用该访问令牌，WWW.Good-X-Pay.example 的应用访问雇员的考勤数据。

A.3.4 应用案例断言的要求

要求如下：

- WWW.X-carrier.example 的授权服务器认证 WWW.Good-X-Pay.example 的应用；
- WWW.X-carrier.example 的授权服务器应能验证由断言方下发的、由运行在 WWW.Good-X-Pay.example 上的应用呈现的断言的有效性；
- Good-X-Work 应与 Good-X-Pay 公司及 WWW.X-carrier.example 的授权服务器建立信任关系。

中华人民共和国
通信行业标准

智能型通信网络
支持开放标识（OpenID）和开放认证（OAuth）的技术要求

YD/T 2917-2015

*

人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷

*

开本：880×1230　1/16　　2015 年 12 月第 1 版
印张：1.25　　2015 年 12 月北京第 1 次印刷
字数：32 千字

15115・836
定价：15 元

本书如有印装质量问题，请与本社联系　电话：(010)81055492