国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Y.2724

(11/2013)

Y系列：全球信息基础设施、
互联网的协议问题和下一代网络

下一代网络 – 安全

支持下一代网络OAuth和OpenID的框架

ITU-T Y.2724 建议书

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
服务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
服务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传送	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
NGN中的IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
服务方面：服务能力和服务体系	Y.2200–Y.2249
服务方面：NGN中服务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
分组网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
运营商级开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2724 建议书

支持下一代网络OAuth和OpenID的框架

摘要

ITU-T Y.2724建议书阐述了在下一代网络（NGN）环境下支持和采用IETF开放授权协议（OAuth）和OpenID协议的框架。现已确定，两项协议均为可通用于万维网。

下一代网络（NGN）提高了安全和身份管理要求，需要谨慎地对上述协议加以限制。本建议书对这些协议的NGN适用性做了说明，并为其使用提供了高层指导原则。

随附的题为“对下一代网络OAuth的支持”的ITU-T Y.2723建议书，提供了一系列有关NGN特性的详细信息。

历史沿革

版本	建议书	批准日期	研究组
1.0	ITU-T Y.2724	2013-11-15	13

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工委员会（IEC）合作制定的。

注

本建议书为简要扼起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2014

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1 范围 1
2 参考文献 1
3 定义 1
3.1 其他地方规定的术语 1
3.2 本建议书定义的术语 2
4 缩写词和首字母缩略语 2
5 排印惯例 3
6 支持NGN OAuth和OpenID的框架 3
6.1 参考模型 4
6.2 OAuth和OpenID流 4
附录 I 精选使用案例 9
I.1 使用案例：Web服务器 9
I.2 使用案例：客户端证书 10
I.3 使用案例：断言 11
参考资料 12

ITU-T Y.2724 建议书

支持下一代网络OAuth和OpenID的框架

1 范围

本建议书阐述了下一代网络（NGN）支持和使用OAuth和OpenID的框架。本建议书的范围包括：

- NGN支持OAuth和OpenID的功能框架
- NGN支持OAuth和OpenID的要求
- OAuth和OpenID使用案例（记录见附录I）。

注：所述技术的实施者和运营商须遵守所有现行国家和区域法律、规则和政策。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T Y.2012] ITU-T Y.2012 (2010)建议书，下一代网络（NGN）功能要求和架构。

[ITU-T Y.2720] ITU-T Y.2720 (2009) 建议书，下一代网络（NGN）身份管理框架。

[ITU-T Y.2722] ITU-T Y.2722 (2011) 建议书，下一代网络（NGN）的身份管理机制

[IETF RFC 6749] IETF RFC 6749 (2012)，OAuth2.0授权框架。
<http://tools.ietf.org/html/rfc6749>

3 定义

3.1 其他地方规定的术语

本建议书使用其他地方定义的下列术语：

3.1.1 接入令牌[IETF RFC 6749]：接入令牌是用来接入受保护资源的证书。接入令牌是一个字符串，代表向客户端发出的授权。该字符串通常对客户端是不透明的。令牌代表资源所有者授予的具体接入范围和时长，由资源服务器和授权服务器执行。

3.1.2 （实体）认证[b-ITU-T X.1252]：对实体与所介绍身份之间关联性实现充足信任的过程。

注 – 在身份管理（IdM）语境内使用术语认证是指实体认证。

3.1.3 授权[b-ITU-T X.1252]：权利的授予以及基于这些权利授权的接入。

3.1.4　授权服务器[IETF RFC 6749]：在成功授权资源所有者并获得授权后颁发接入客户端令牌的服务器。

3.1.5　客户端[b-IETF RFC 6749]：代表资源拥有方并在获得其授权的情况下发出受保护资源请求的一种应用。术语“客户端”并不具有任何特定的实施特性含义（如，应用是否在服务器、台式机或其它装置上予以执行）。

3.1.6　实体[b-ITU-T X.1252]：具有独立和独特存在并可在一定情境中识别的事务。

注 – 实体可以为真人、动物、法人、组织、主动或被动之物、设备、软件应用、服务等或上述个体的组合。在电信中，实体的例子包括接入点、订户、用户、网源、网络、软件应用、服务和设备、接口等。

3.1.7　标识符[b-ITU-T X.1252]：用来在语境中识别实体的一个或多个属性。

注–在[b-ITU-T Y.2091]定义的NGN语境内，标识符是一系列数位、字符和符号或任何用来标识订户、用户、网元、功能、提供服务/应用的网络实体或其它实体（如物理或逻辑对象）的数据。

3.1.8　身份提供方（IdP）[b-ITU-T X.1252]：见身份服务提供方（IdSP）。

3.1.9　身份服务提供者（IdSP）[b-ITU-T X.1252]：认证、维护、管理并可能创建和分配其他实体身份信息的实体。

3.1.10 刷新令牌[IETF RFC 6749]：刷新令牌是由授权服务器向客户端颁发，当前接入令牌无效或到期时，或为使用相同或更窄的范围获得附加接入令牌（接入令牌可能拥有比资源所有者授予的更短的寿命和更少的许可）时颁发的。颁发刷新令牌是授权服务器的一项选择。如授权服务器颁发刷新令牌，该令牌包含在所颁发的接入令牌中。

3.1.11 资源所有者[IETF RFC 6749]：能够授权接入受保护资源的实体。当资源所有者为个人时，该所有者被称为最终用户。

3.1.12 资源服务器[IETF RFC 6749]：托管受保护资源的服务器能够使用接收令牌接受和响应受保护资源请求。

3.2　本建议书定义的术语

无。

4　缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

AKA　认证和主要协议

ANI　应用与网络的界面

FE　功能实体

GBA　一般性自举架构

IdM　身份管理

IdP　身份提供方

IdSP　身份服务提供方

IMPI　互联网协议（IP）多媒体专用身份

IMSI　　国际移动用户身份

NGN　　下一代网络

SAML　　安全断言标记语言

SNI　　服务网络界面

UNI　　用户网络界面

5　排印惯例

在本建议书内：

关键词“须”（is required to）指必须严格遵守的要求，如果要宣称符合本文件，就不得违反。

关键词“建议”（is recommended）指建议但并非需要绝对遵守的要求。因此宣称符合本文件不需要说明已满足此要求。

关键词“禁止”（is prohibited from）指必须严格遵守的要求，如果要宣称符合本文件，就不得违反。

关键词“可作为选项”（can optionally）指允许可选的、但并非建议遵守的要求。该术语并非旨在暗示销售商的实施必须提供该选项且该功能部件可作为选项由网络运营商/业务提供商激活，而是指销售商可作为选项提供该功能部件并仍根据规范宣称符合本文件。

在本文件正文及其附件中，有时会出现“须”（shall）、“不得”（shall not）、“应”（should）、“可”（may）等词语。在这些情况下，这些词语应分别理解为“需”、“禁止”、“建议”和“可作为选项”。在附录或标为“用于通报情况”的材料中出现这些短语和关键词应理解为并非出于规范性的意向。

6　支持NGN OAuth和OpenID的框架

如[ITU-T Y.2720]所述，NGN网络包括使用实体标识符执行功能的多个功能元素，以便支持并向其他提供商推广开放认证服务。这种安排可如图1所示使用OpenID和OAuth予以支持。NGN中OpenID和OAuth的使用描述见图1。

根据[b-OpenID v.2] OpenID规范，OpenID IdP服务器参与了整个认证工作流程，可以通过OAuth协议直接向NGN-IdP发送认证消息。

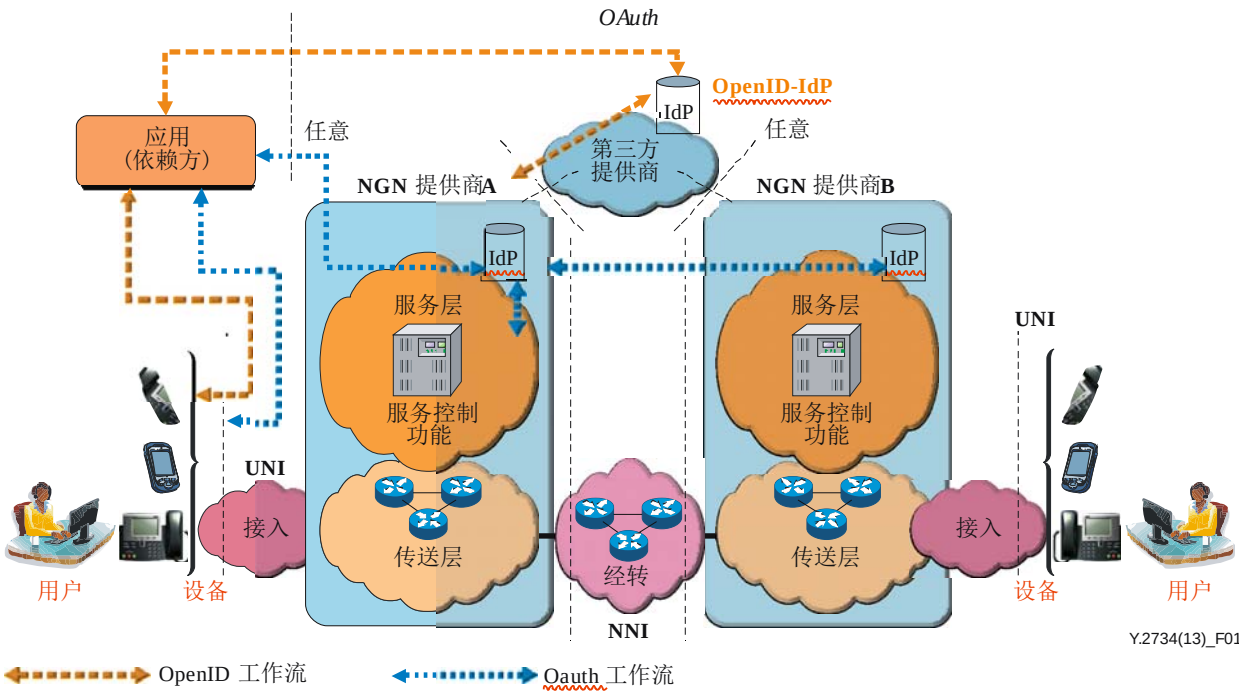

图1 – 用于NGN的OpenID和OAuth流

6.1 参考模型

图1提供了OpenID和OAuth框架概貌。

图2描述了NGN提供OAuth授权和OpenID认证服务的参考模型。NGN提供商可使用OpenID和OAuth提供IdSP服务并与内容和应用提供商以及/或其他服务提供商合作。

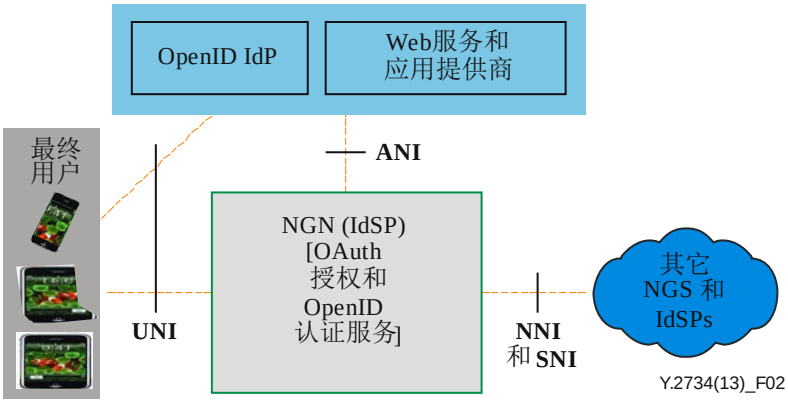

图2 – 参考模型

6.2 OAuth和OpenID流

该段对有关NGN的OAuth和OpenID的消息流进行了一般性描述。

6.2.1 信息流中的实体

该段确定了参与OAuth和OpenID信息流的实体（包括[ITU-T Y.2012]的功能实体）。

6.2.2 OAuth和OpenID流中共用实体

同时涉及OAuth和OpenID流的实体如下：

- 具有Web客户端能力（如浏览器）的最终用户功能；
- A-2：应用网关功能实体（APL-GW-FE）[ITU-T Y.2012]：该功能实体应能支持OAuth和/或OpenID协议。

如[ITU-T Y.2012]所定义的，“APL-GW-FE是NGN各种功能和所有外部应用服务器及服务使能元素之间的互连实体”。这使A-2成为提供OAuth和OpenID支持的逻辑选择。此外，由于与S-5（用户概要功能实体（SUP-FE）[ITU-T Y.2012]）的连接，A-2得以支持基于AKA的认证，包括用户设备的一般性自举架构（GBA）。基于GBA的OpenID认证方法规定见b-3GPP TS 33.220]。另一种基于在一些方面与GBA类似的AKA的OpenID认证方法描述见[ITU-T Y.2722]第6.2.8段。如果OAuth授权服务器和OpenID IdP [ITU-T Y.2722]均实施于A-2，可以通过与S-5的互动使用基于AKA的认证。

6.2.3 OAuth流的专门实体

OAuth专门实体包括：

- 为用户客户端执行服务的Web应用服务器 – 一种OAuth客户端。客户端可以但并非必须运行NGN实体。
- 授权服务器作为A-2的组成部分实施。

  授权服务器首先执行用户认证，然后对客户端请求进行授权。如果两个程序均顺利完成，OAuth通过授权服务器向客户端发布接入令牌以交换结果。为支持基于AKA的认证，授权服务器须能够与S-5互动。
- 资源服务器

  资源服务器在配有有效接入令牌时满足客户端的请求。通过使用接入令牌获得资源的两类程序已制定了规定；[b-IETF RFC 6750]负责规范此操作且IETF正在制定MAC令牌方面的规范。资源服务器可以与或不与A-2的授权服务器并置。

图3和下文描述了用于Web服务器的高层OAuth信息流案例（描述见附录1）。

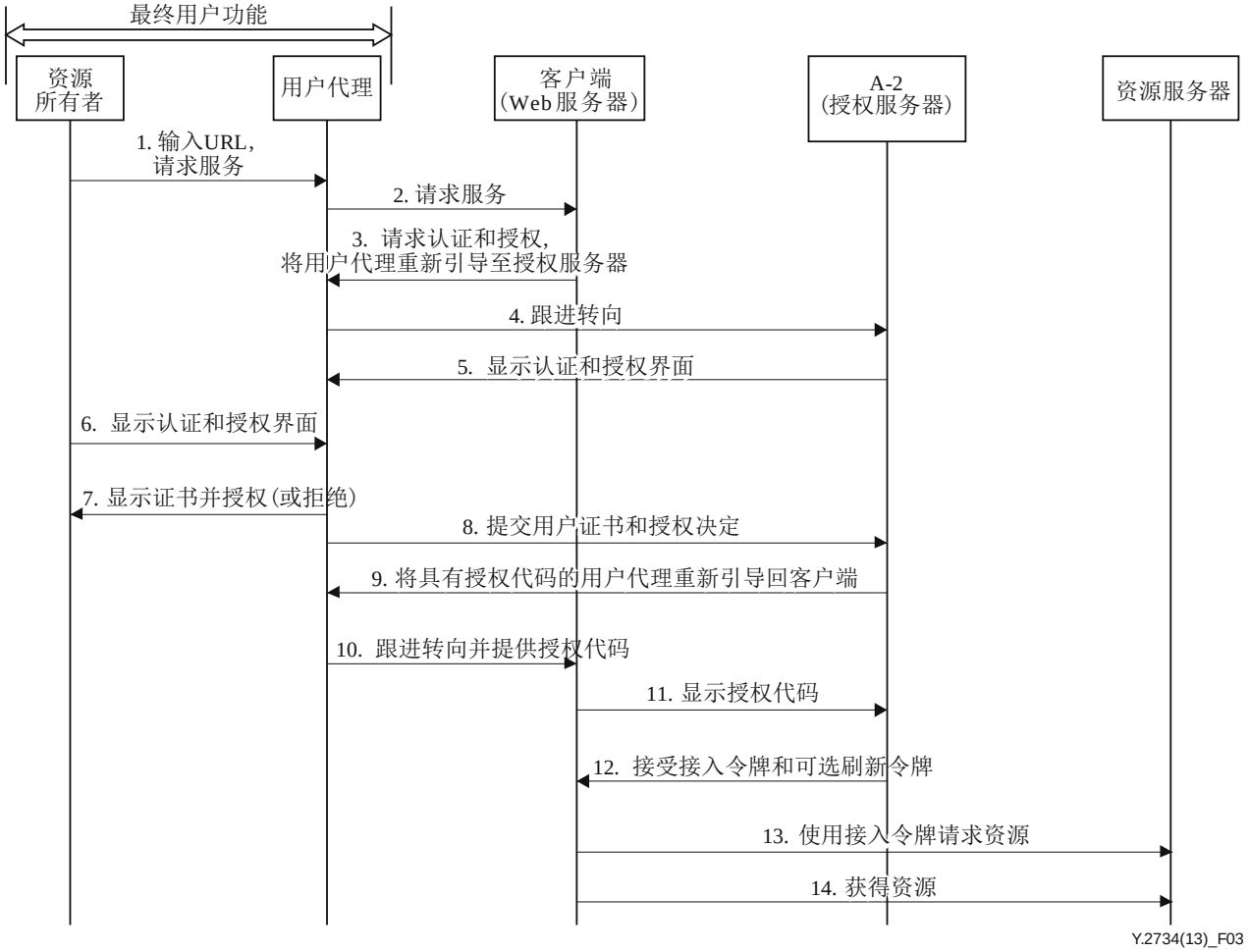

图3 用于Web服务器的OAuth流使用案例

1 用户引导用户代理（如浏览器）从客户端请求服务。

2 用户代理向客户端提交请求。

3 客户端做出响应并将用户代理重新引导至授权服务器，以便进行客户端请求的用户认证和授权。

4 用户代理跟进转向。

5 授权服务器做出响应，向用户代理提供认证和授权界面。

6 用户代理向用户（资源所有者）显示认证和授权界面。

7 用户使用用户代理提供认证证书并说明授权决定。

8 用户代理向授权服务器发送用户提供的数据。

9 授权服务器，在认证用户和确保用户已授权了客户端请求后将用户代理重新引导回客户端。响应包括授权代码。

10 用户代理在重新引导后，将授权代码提供给客户端。

11 客户端向授权服务器发送授权代码。

12 授权服务器用可选刷新令牌响应接入令牌。

13　　客户端向资源服务器发送请求并显示接入令牌。

14　　资源服务器提供所请求的资源。

6.2.4　OpenID流专用实体

OpenID专用实体包括：

- 依赖于OpenID IdP执行的认证的应用服务器。
- OpenID IdP作为A-2的组成部分予以实施，以便支持基于AKA的认证。该实体须能够与S-5互动。
- S-5，如NGN按照[ITU-T Y.2722]的规定执行基于AKA的最终用户认证功能，参与OpenID认证。

OpenID信息流描述见图4及下文。文本和图表描述了当IdP和应用服务器建立了共享秘密后，OpenID程序的使用案例。该秘密用于签署IdP认证结果消息并由应用服务器加以确认。

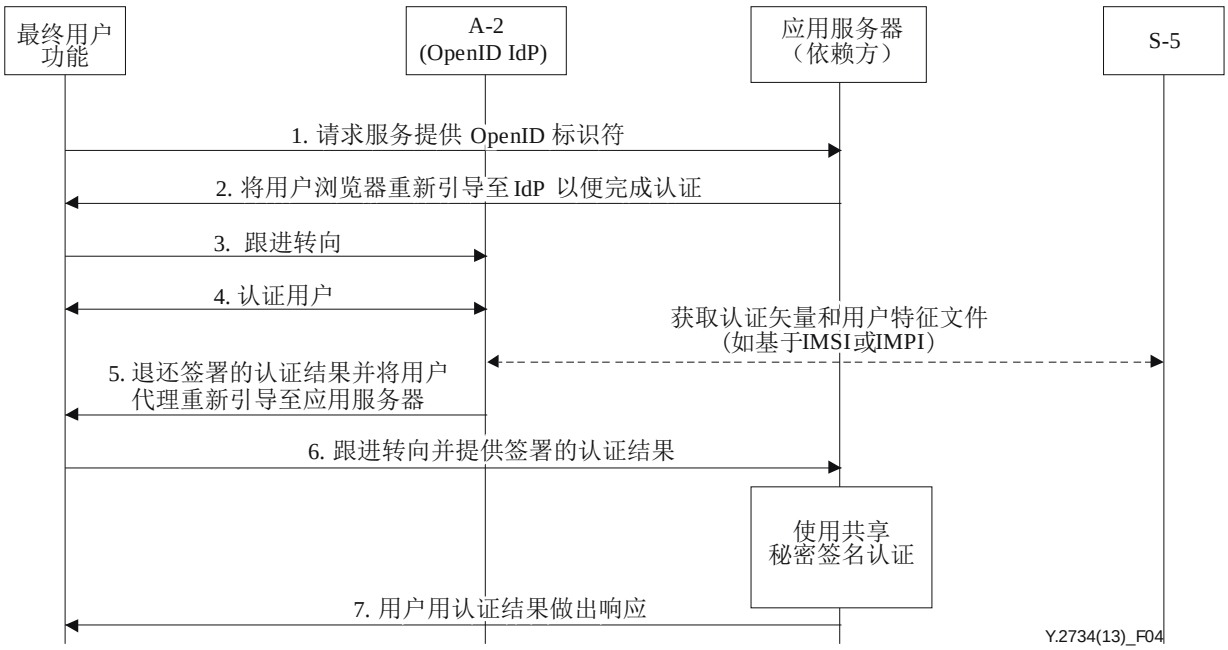

图4 – OpenID流

1.　　浏览器将服务请求发送至应用服务器，请求包含用户OpenID标识符。

2　　基于OpenID标识符，应用服务器发现用户OpenID IdP之后，应用服务器将用于认证的用户浏览器重新引导至OpenID IdP。

3　　浏览器跟进转向请求。

4　　OpenID IdP通过与用户浏览器交流信息认证用户。

5　　如OpenID IdP执行基于AKA的认证（如[ITU-T Y.2722]所述），需与S-5互动。这种互动用虚线箭头表示。

6　　OpenID IdP通过响应将用户浏览器重新引导回应用服务器。该响应包含签名的认证结果消息。

7　　浏览器跟进转向请求并将签名消息提供给应用服务器。

8 应用服务器在确认签名和核对认证结果后通知用户认证是否成功。签名和确认程序规定见[b-OpenID v.2]。

附录 I

精选使用案例

（本附录并非此建议书不可分割的组成部分）

I.1 使用案例：Web服务器

描述

Alice接入运行在www.X-printphotos.example的网络服务器上的应用并指示该应用打印其存储在www.X-storephotos.examplele服务器上的照片。Alice是NGN服务提供商的订户。与Alice签约的该提供商在www.X-carrier.example运行OAuth授权服务器。www.X-printphotos.example应用收到Alice使用其照片的授权，但无需了解其在www.X-storephotos.example或www.X-carrier.example上的认证证书。

前期条件

- Alice已在www.X-carrier.example中注册以便进行认证。
- www.X-printphotos.example应用通过www.X-carrier.exampleOAuth授权服务器已确定了认证证书。
- www.X-storephotos.example应用可以确认www.X-carrier.example授权服务器发布的接入令牌。

后续条件

成功的程序将在www.X-printphotos.example应用接收到从www.X-carrier.example中获得的授权代码。该代码与www.X-printphotos.example应用和应用所提供的回叫URL绑定。www.X-printphotos.example应用使用授权代码从www.X-carrier.example获得接入令牌。www.X-carrier.example应用在认证了www.X-printphotos.example应用并确认了所提交的授权代码后发布接入令牌。www.X-printphotos.example应用使用该接入令牌获得www.X-storephotos.example中Alice的照片。

注– 当接入令牌到期时，www.X-printphotos.example中的服务需重复OAuth程序，以便获得Alice有关接入其在www.X-storephotos.example中的照片的授权。换言之，如Alice希望向该应用授予获取其在www.X-storephotos.example中的资源的长期接入时，www.X-carrier.example中的授权服务器可发布长期有效令牌。这些令牌可以与接入www.X-storephotos.example所需要的短期接入令牌相交换。

要求

- 托管OAuth客户端的www.X-printphotos.example服务器必须得以向Alice用户代理（浏览器）发布HTTP转向请求。
- www.X-carrier.example中的授权服务器必须能够认证Alice。认证方法不在OAuth范围内。
- www.X-carrier.example应用必须获得Alice有关通过www.X-printphotos.example接入其照片的授权。
- www.X-carrier.example应用可向Alice确认www.X-printphotos.example在寻求Alice授权时所请求的接入范围。

- www.X-carrier.example授权服务器必须能够认证www.X-printphotos.example应用并在发布接入令牌时确认授权代码。www.X-printphotos.example应用必须向www.X-carrier.example向授权服务器提供回叫URL（注：URL应在www.X-carrier.example中提前注册）。
- www.X-carrier.example授权服务器需保留与www.X-printphotos.example应用相关的授权代码记录以及应用所提供的回叫URL。
- 接入令牌为承载令牌（这些与具体的应用，如www.X-printphotos.example无关），有效期应较短。
- www.X-carrier.example授权服务器须在第一次使用后废除授权代码的有效性。
- 不需要Alice人为参与OAuth授权程序（如输入URL或密码）。（Alice对www.X-carrier.example的认证不在OAuth范围内）。

I.2 使用案例：客户端证书

描述

Good-X-Pay公司为Good-X-Work公司准备了员工工资单。为完成这项工作，www.Good-X-Pay.example应用获得经认证的接入www.Good-X-Work.example中存储的员工出勤数据。认证是由认证服务器进行的。该服务器使用作为NGN的一部分，其URL为：www.X-carrier.example

前提条件

- www.Good-X-Pay.example应用通过在www.X-carrier.example应用服务器中注册建立一个标识符和一共享秘密。
- www.Good-X-Pay.example应用接入存储于www.Good-X-Work.example内数据的范围已然定义。

后续条件

该程序成功在 www.Good-X-Pay.example 应用中获得 www.X-carrier.example 授权服务器认证后收到的接入令牌。www.Good-X-Pay.example 应用在此之后使用该接入令牌获得www.Good-X-Work.example 中的出勤数据。

要求

- www.Good-X-Pay.example应用必须在www.X-carrier.example授权服务器得到认证。
- 认证方法必须基于运行在 www.Good-X-Pay.example 中的应用向 www.X-carrier.example授权服务器在HTTP首次请求后提交的标识符和共享秘密。
- 由于该程序可接入Good-X-Work敏感数据，Good-X-Work须在www.X-carrier.example授权服务器上与Good-X-Pay建立信任。

I.3 使用案例：断言

描述

Good-X-Pay公司为Good-X-Work公司制作工资单。为完成该项工作，www.Good-X-Pay.example应用获得了经认证的，获取存储于www.Good-X-Work.example的员工出勤数据的权利。应用在收到www.X-carrier.example授权服务器发布的接入令牌后，www.Good-X-Work.example服务器向www.Good-X-Pay.example授予接入。www.X-carrier.example授权服务器负责认证www.Good-X-Pay.example的应用，其方式为确认www.Good-X-Pay.example显示的断言。

该使用案例描述了“客户端证书”使用案例的另一种解决方案。

前提条件

- www.Good-X-Pay.example应用从www.X-carrier.example授权服务器所信任的一方获得认证断言。
- www.Good-X-Pay.example应用接入存储在www.Good-X-Work.example中的数据范围得到确定。
- www.X-carrier.example授权服务器与断言方确定信任关系并能确认断言。

后续条件

成功的程序使 www.Good-X-Pay.example 应用在向 www.X-carrier.example 授权服务器通过显示断言（如 SAML 断言）进行认证后收到接入令牌，由此利用接入令牌获取员工出勤数据。

要求

- www.Good-X-Pay.example应用需要获得www.X-carrier.example授权服务器认证。
- www.X-carrier.example授权服务器必须能够确认断言方发布的、由运行在www.Good-X-Pay.example上的应用显示的断言。
- Good-X-Work须与Good-X-Pay在www.X-carrier.example上的授权服务器建立信任。

参考资料

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks.*

[b-IETF RFC 6750] IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*.

[b-OpenID v.2] OpenID Authentication 2.0
< http://openid.net/specs/openid-authentication-2_0.html>

[b-3GPP TS 33.220] 3GPP TS 33.220 (2013) *Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, Release 12*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	终端和主观与客观评估方法
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网的协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2014年，日内瓦