国　际　电　信　联　盟

ITU-T

Y.2725

(07/2014)

国际电信联盟
电信标准化部门

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 – 框架和功能结构模型

在下一代网络（NGN）中支持OpenID

ITU-T Y.2725 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
业务、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
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传输	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
运行于NGN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
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业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
智能泛在网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
电信级开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T Y.2725 建议书

在下一代网络（NGN）中支持OpenID

摘要

ITU-T Y.2725建议书针对由NGN提供商来担任*OpenID*提供商的场景规定了支持和使用*OpenID*的机制和程序。

ITU-T Y.2725建议书提供了支持和使用*OAuth*和*OpenID*的NGN框架。ITU-T Y.2725建议书基于Y.2722和ITU-T Y.2724来定义支持*OpenID*的特定机制。

注 - ITU-T Y.2725不对*OpenID*协议进行任何更改或修改，且仅涉及NGN对*OpenID*的支持和使用。

历史沿革

版本	建议书	批准日期	研究组	唯一 编号*
1.0	ITU-T Y.2725	2014-07-18	13	11.1002/1000/12079

* 欲查阅建议书，请在您网络浏览器的地址字段内先输入URL http://handle.itu.int/，然后再输入该建议书的唯一编号，例如，http://handle.itu.int/11.1002/1000/11830-en。

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）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“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”等其它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它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，这可能并非最新信息，因此特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/。

目录

ITU-T Y.2725 建议书

在下一代网络（NGN）中支持OpenID

1 范围

本建议书描述在下一代网络中支持*OpenID*的机制和程序。本建议书阐明的机制和程序可用于支持多服务提供商环境中的应用服务。本建议书假设NGN提供商为*OpenID*提供商。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，由于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。本建议书对自成一体的文件的引用，不能给予它建议书的地位。

[ITU-T Y.2701] ITU-T Y.2701建议书（2007年）：第1版本下一代网络（NGN）的安全性要求。

[ITU-T Y.2702] ITU-T Y.2702建议书（2008年）：第1版本下一代网络（NGN）的认证和授权要求。

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

[ITU-T Y.2721] ITU-T Y.2721建议书（2010年）：下一代网络（NGN）的身份管理要求和使用案例。

[ITU-T Y.2724] ITU-T Y.2724（2013年）：下一代网络（NGN）中支持OAuth和OpenID的框架。

[OASIS XRI SYNTAX] 可扩展资源标识符（XRI）语法V2.0。

3 定义

3.1 他方定义的术语

本建议书使用下列他方定义的术语：

3.1.1 （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。

3.1.2 授权[b-ITU-T X.800]：权利的授予，包括根据接入权授予的接入。

3.1.3 授权准予[b-IETF RFC 6749]：授权准予是一种资格证书，代表客户机为获得接入令牌而使用的资源拥有方授权（以接入其受保护资源）。

3.1.4 授权服务器[b-IETF RFC 6749]：在成功对资源拥有方进行认证并获得授权后发放接入令牌的服务器。

3.1.5 客户机[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“客户机”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）。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用了以下缩写词和首字母缩略语：

FE 功能实体（Functional Entity）

FRA 功能要求和架构（Functional Requirements and Architecture）

IdM 身份管理（Identity Management）

IdP 身份提供方（Identity Provider）

IETF 互联网工程任务组(Internet Engineering Task Force)

IP 互联网协议（Internet Protocol）

OAuth OAuth 2.0版本OAuth授权协议（OAuth 2.0 Authorization Protocol）

SAML 安全断言标记语言（Security Assertion Markup Language）

URI 统一资源标识符（Uniform Resource Identifier）

WS Web服务器（Web Server）

5 惯例

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。

6 在NGN中支持OpenID

本节介绍在NGN中支持OpenID所涉及的主要内容。

6.1 参考模型

根据OpenID的规范[b-OpenID v.2]，OpenID IdP服务器参与整个认证工作流程，请参照[ITU-T Y.2724]中有关OAuth和OpenID框架的一般概述。

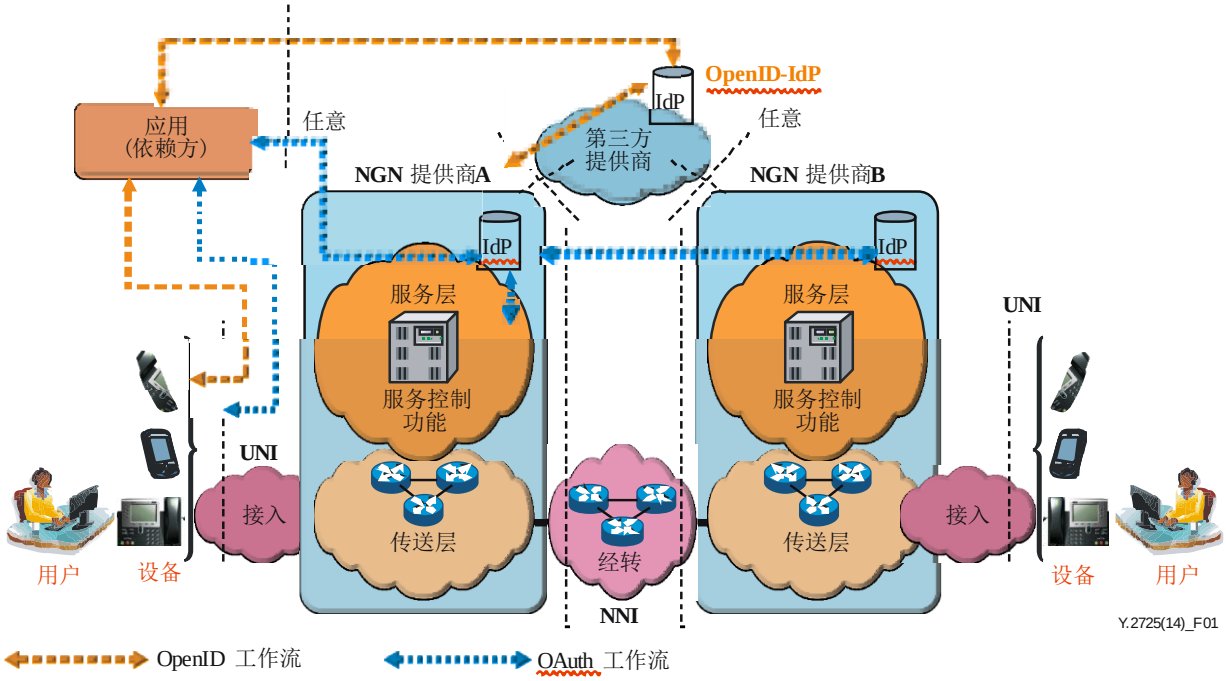

图1 – 用于NGN的OpenID和OAuth流

6.2 NGN环境中的协议消息格式

[b-OpenID v.2]定义了两种协议消息格式类型：

- 键值形式编码，
- HTTP编码。

[b-OpenID v.2]的第4.1.1节指出，键值形式编码被用于签名计算和向依赖方做出的直接响应。

关于HTTP编码，[b-OpenID v.2]的第4.1.2节指出，“这种模式适用于从用户代理到依赖方和OP的消息，以及从依赖方到OP的消息。”

由NGN支持的实体须在发送一个协议消息时符合相关要求。

6.3 通信类型

[b-OpenID v.2]定义了两种通信类型：

- 直接通信，
- 间接通信。

[b-OpenID v.2]第5.1节指出，直接通信由依赖方向OP终点URL发起，用于建立关联及验证认证断言。

[b-OpenID v.2]的第5.2节指出，在间接通信中，消息经由用户代理传送。这可以通过依赖方或OP发起。间接通信被用于认证请求和认证响应。

由NGN支持的实体须在发起通信上下文时符合这些要求。

6.4 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

本款建议使用HMAC- SHA256。生成[b-OpenID v.2] 第6.1节中规定的消息签名的程序已满足NGN的安全要求。

6.5 NGN中的OpenID认证程序

6.5.1 认证请求

[b-OpenID v.2]的第13节建议，建议依赖方使用Yadis协议来发布其有效的“返回到”（return_to）URL。依赖方可作为选项在任何URL发布此信息，并建议在域内发布此信息，以令提供商得以验证return_to URL。

本建议书要求建议依赖方在NGN中使用Yadis协议来发布其有效的return_to URL消息。

有关认证请求的规定见[b-OpenID v.2]的第9节。

下列要求适用于依赖方与最终用户的交互。依赖方须：

- 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。

6.5.1.1 发起OpenID认证

[b-OpenID v.2]的第7.1节提出如下建议：要发起OpenID认证，建议依赖方向最终用户呈现一份表单，且表单中的一个字段可用于输入用户提供的标识符。

建议表单字段的“名称”属性的取值为“openid_identifier”，以令用户代理得以自动确定这是否为一份OpenID表单。若此属性未得到正确设置，则支持OpenID认证的浏览器扩展或其他软件可能无法检测到依赖方的支持。

本建议书要求依赖方实体在NGN中呈现的表单内列入openid_identifier字段。

6.5.1.2 规范化用户提供的标识符

[b-OpenID v.2]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”），或*XRI* [b-OASIS XRI SYNTAX 2.0]。

最终用户的输入须被规范化为一个标识符，[b-OpenID v.2]的第7.2节所规定的程序已满足NGN的规范化要求。

6.5.1.3 为发起请求发现必要信息

[b-OpenID v.2]指出，“发现是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”。

OpenID认证可通过三种手段来完成上述发现，相关规定见[b-OpenID v.2]的第7.3节。

[b-OpenID v.2]定义了两种发现方法：

- 基于XRDS的发现
- 基于HTML的发现

若使用的是XRI [b-OASIS XRI SYNTAX 2.0]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[b-OpenID v.2]的第7.3.2.1节。

基于HTML的发现必须得到各依赖方的支持。基于HTML的发现仅可用于声明标识符的发现。OP标识符必须是XRI [b-OASIS XRI SYNTAX 2.0]或支持XRDS发现的URL。要使用基于HTML的发现，必须在声明标识符的URL上提供一份HTML文档，相关规定见[b-OpenID v.2] 的第7.3.3节。

本建议书要求依赖方在执行发现时须符合相关要求，且建议由标识符授予XRI或URL格式。

6.5.2 认证响应

[b-OpenID v.2]的第10节建议，当认证请求来自借助间接沟通的用户代理时，则建议由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，则建议OP向依赖方发出一个正断言。

本建议书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规范的范围。

6.5.2.1 正断言

正断言为间接响应，关于响应参数的信息，请参见[b-OpenID v.2] 的第10.1节。

根据[b-OpenID v.2]，当OP通过用户代理与依赖方进行间接通信时，须：

- 确认return_to URL可与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
- 签署正响应
- 通过用户代理向依赖方发送正断言。

6.5.2.2 负断言

若OP无法识别最终用户，或最终用户没有或不能批准认证请求，则建议OP向依赖方发送一个负断言，并将其作为一种间接响应，亦见[b-OpenIDv.2] 的第10.2节。

若在回应一个“checkid_immediate”模式请求时收到一个负断言，则建议依赖方使用“checkid_setup”模式构造一个新的认证请求。

6.5.2.2.1 对即时请求的负断言

若请求为直接请求，则在提供鉴定证书或对请求予以批准时，最终用户将无机会在OP上与网页交互。直接请求的负断言需采用[b-OpenID v.2] 的第10.2.1节中规定的形式。

6.5.2.2.2 对非即时请求的负断言

由于OP可向终端用户显示网页，并向最终用户请求获得证书，因此对某一非即时请求的负响应是决定性的，且其需采用[b-OpenID v.2] 第10.2.2节中规定的形式。

若依赖方收到“取消”响应，则表明认证不成功，且依赖方须将最终用户视为未经认证。

6.5.3 验证断言

根据[b-OpenID v.2]，在收到正断言时，依赖方须：

- 验证返回URL
- 验证所发现的信息
- 检查相关响应
- 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。

6.6 安全考虑

OpenID 2.0规范[b-OpenID v.2]第15节（安全考虑）提供的安全导则涉及攻击防范、用户代理、用户界面、HTTP和HTTPS URL标识符以及协议变种等内容。本建议书建议支持NGN中的各类安全方面的考虑。

这些解决方案亦应符合[ITU-T Y.2701]、[ITU-T Y.2720]和[ITU-T Y.2721]具体规定的NGN和IdM安全要求。

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-OpenIDv.2] OpenID Authentication 2.0
http://openid.net/specs/openid-authentication-2_0.html

[b-Yadis] Yadis协议
http://infogrid.org/trac/wiki/Yadis

[b-IETF RFC 6749] IETF RFC 6749 (2012)，OAuth 2.0 *Authorization Framework*
http://tools.ietf.org/html/rfc6749

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、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、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	电话传输质量、电话设施及本地线路网络
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
2015年，日内瓦