国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Y.2723

(11/2013)

Y系列：全球信息基础设施、互联网协议问题
和下一代网络

下一代网络 – 安全

在下一代网络中支持OAuth

ITU-T Y.2723 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.2723 建议书

在下一代网络中支持OAuth

摘要

ITU-T Y.2723建议书规定使用“2.0版本OAuth – 授权框架（OAuth）”的机制和程序，该框架由互联网工程任务组确定，用于OAuth授权服务器作用由下一代网络（NGN）提供商发挥的情形。

与之相互配套的文件ITU-T Y.2724建议书“在下一代网络（NGN）中支持OAuth和开放身份（OpenID）的框架”提供相关环境、架构考虑以及在NGN中使用OAuth的高层框架。

本建议书具体规定与限制OAuth选项的选择相关的要求以及使OAuth使用与NGN安全性和身份管理要求相符合的更多要求。

历史

版本	建议书	批准	研究组
1.0	ITU-T Y.2723	2013-11-15	13

前言

国际电联（国际电信联盟）是联合国在电信领域内的专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电联的常设机构。ITU-T负责研究技术的、操作的和资费的问题，并且为实现全世界电信标准化，就上述问题发布建议书。

每四年召开一次的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，然后由各研究组制定有关这些课题的建议书。

WTSA第1号决议拟定了批准ITU-T建议书的程序。

在ITU-T研究范围内的某些信息技术领域中使用的必要标准是与ISO和IEC共同编写的。

注

在本建议书中，“主管部门”一词是电信主管部门和经认可的运营机构的简称。

本建议书为自愿遵守，但建议书可能包含某些特定的强制性条款（以确保互操作性或适用性），只有满足所有此类强制性条款时，才可实现对建议书的遵守。“应”或一些其他有义务含义的语言（如“必须”）及其否定形式被用于表达特定要求。使用此类词汇不表示要求各方均遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能需要使用已申明的知识产权。国际电联对有关已申明的知识产权的证据、有效性或适用性不表示意见，无论其是由国际电联成员还是由建议书制定过程之外的其他机构提出的。

到本建议书批准之日为止，国际电联尚未收到实施本建议书时可能需要的受专利保护的知识产权方面的通知。但是，本建议书实施者要注意，这可能不代表最新信息，因此最好查询TSB专利数据库http://www.itu.int/ITU-T/ipr/。

© 国际电联 2014

版权所有。未经国际电联书面许可，不得以任何手段对本出版物的任一部分加以复制。

目录

页码

1 范围 1
2 参考文献 1
3 定义 1
3.1 其他建议书/标准机构定义的术语 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 惯例 2
6 在NGN中支持OAuth 2
6.1 根据NGN安全要求选择OAuth客户机类型 2
6.2 授权准予类型的选择 3
6.3 有关NGN支持的客户机的OAuth选项的建议 3
6.4 资源拥有方的认证 4
6.5 安全考虑 5
参考资料 6

引言

ITU-T Y.2723建议书提供在下一代网络（NGN）中支持和使用OAuth和开放身份（OpenID）的框架。本建议书以ITU-T Y.2724建议书为基础，旨在确定支持OAuth的具体方法。

注 – 本建议书不对OAuth协议做出任何更改或修改，其重点仅仅是NGN对OAuth的支持和使用。

ITU-T Y.2723 建议书

在下一代网络中支持 OAuth

1 范围

本建议书描述在下一代网络（NGN）中支持OAuth 2.0授权协议（OAuth）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及多服务提供商环境中的应用服务。本建议书假设OAuth授权服务由NGN提供。

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。本建议书中对某份文件的引用并不向作为一份单独文件的相应文件赋予建议书的地位。

[ITU-T X.1254] ITU-T X.1254建议书（2012年），实体认证保证框架

[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建议书（2013年），下一代网络（NGN）支持OAuth和开放身份的框架

[IETF RFC 6749] IETF RFC 6749（2012年），2.0版本OAuth授权框架 <http://datatracker.ietf.org/doc/rfc6749/>

3 定义

3.1 其他建议书/标准机构定义的术语

本建议书使用下列其他建议书/标准机构定义的术语：

3.1.1 接入令牌[IETF RFC 6749]：接入令牌是用以接入受保护资源的资格证书。接入令牌是一个代表向客户机发出授权的字符串，通常该字符串对客户机是非透明的。令牌代表资源拥有方准予的接入的具体范围和时长，并由资源服务器和授权服务器实施。

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。

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

3.1.4 授权准予[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）。

3.1.5 授权服务器[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。

3.1.6 客户机[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、台式机或其他装置上予以执行）。

3.1.7 秘密客户机[IETF RFC 6749]：能够保持其资格证书保密性的客户机（如在安全服务器上实施的具有客户资格证书有限接入的客户机），或使用其他手段进行安全客户机认证的客户机。

3.1.8 公共客户机[IETF RFC 6749]：无法保持其资格证书保密性的客户机（如在资源拥有方装置上执行的客户机，包括得到安装的本征应用或基于Web浏览器的应用），且无法通过任何其他手段进行安全的客户机认证的客户机。

3.1.9 资源拥有方[IETF RFC 6749]：有能力对受保护资源进行接入授权的实体。如资源拥有方是个人，则称为最终用户。

3.1.10 资源服务器[IETF RFC 6749]：托管受保护资源的服务器，能够使用接入令牌对受保护资源请求予以接受和做出响应。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

IdM 身份管理（Identity Management）

NGN 下一代网络

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）

5 惯例

无。

6 在NGN中支持OAuth

本节描述支持NGN中OAuth的一些主要方面问题。

6.1 根据NGN安全要求选择OAuth客户机类型

[IETF RFC 6749]定义了两种OAuth客户机类型：秘密和公共客户机。

公共客户机不能满足NGN第三方应用提供商[ITU-T Y.2702]的认证要求，因为公共客户机无法由NGN提供商认证 [ITU-T Y.2724] 。本建议书建议NGN仅支持秘密客户机，这类客户机必须满足下列要求：

1 NGN OAuth客户机必须能够在具体保障层面得到认证[ITU-T Y.2702]、[ITU-T X.1254]。

2 NGN OAuth客户机必须按照[IETF RFC 6749]第2节的规定，与授权服务器进行注册。

2.0版本OAuth [IETF RFC 6749]定义了下列客户机应用程序（profile）：网络应用、基于用户代理的应用和本征应用。网络应用是一种专用客户机应用程序，而后两者则是公共客户机应用程序。本建议书描述NGN仅对网络应用应用程序客户机的支持。

6.2 授权准予类型的选择

[IETF RFC 6749]定义了下列类型的授权准予：授权代码、隐含、资源拥有方密码资格证书以及客户机资格证书。此外，IETF目前正在着手定义一种延伸，该延伸具体规定2.0版本OAuth的SAML 2.0断言准予类型。

[IETF RFC 6749]解释道，在隐含准予流程中发放接入令牌时，授权服务器并不对客户机进行认证。有些情况下，可通过重新确定用以向客户机提供接入令牌的URI方向，核实客户机的身份。接入令牌可由资源拥有方或能够接入资源拥有方“用户代理”的其他应用看到。

因此，OAuth的流程是，使用隐含准予类型不会带来满足NGN第三方应用提供商认证要求的认证[ITU-T Y.2702]。

本建议书重点描述NGN支持的网络应用应用程序的秘密客户机，且使用下列授权准予：

- 授权代码
- 资源拥有方密码资格证书
- 客户机资格证书
- SAML 2.0断言。

6.3 有关NGN支持的客户机的OAuth选项的建议

[IETF RFC 6749]定义的流程是两种类型客户机的若干客户机应用程序的优化流程。RFC具体规定了选择授权准予类型、参数和安全要求的选项。

本款提出支持网络应用应用程序秘密客户机的若干建议，重点是对于NGN支持的*OAuth*至关重要的要求和可选参数的选择。

6.3.1 客户机注册

[IETF RFC 6749]第2.2节建议，客户机经重新确定方向的URI与授权服务器进行注册，因为带有注册URI的客户机具有更高的安全性。

本建议书要求NGN支持的客户机将其改变方向的URI与授权服务器进行注册。

6.3.2 信息对客户机改变方向后端点的保密

[IETF RFC 6749]第3.1.2.1节提出下列建议：改变方向的端点应要求，按照第1.6节描述，在所要求资源类型为“代码”或“令牌”的情况下，使用TLS，或在重新改变方向将导致在开放网络上传输敏感资格证书时如此行事。本建议书要求在传送任何敏感信息时都使用TLS。

6.3.3 客户机认证

网络应用应用程序定义的客户机是秘密客户机，因此，要求授权服务器对客户机进行认证。

6.3.4 授权程序

本建议书涵盖使用下列授权准予类型授权程序的网络应用应用程序秘密客户机：

- 授权代码
- 资源拥有方密码资格证书
- 客户机资格证书
- SAML扩展

6.3.4.1 授权代码

[IETF RFC 6749]第4.1节具体规定了使用授权代码的秘密客户机的授权程序。本建议书要求在授权请求中包含*redirect_uri*这一参数。

下列要求适用于与使用授权代码网络应用应用程序客户机进行互动的授权服务器。授权服务器必须：

- 对发出授权请求的客户机进行认证
- 确保客户机授权请求中的*redirect_uri*参数数值与客户机注册的数值相匹配
- 只为经过认证和授权的客户机发放认证代码
- 在发放接入令牌前，确保授权代码有效。

6.3.4.2 资源拥有方密码资格证书

使用该准予类型的授权程序对于业已与资源拥有方建立信任的客户机是优化的。客户机使用资源拥有方的密码资格证书从授权服务器处获得接入令牌。[IETF RFC 6749]第4.3节规定的程序满足NGN的安全要求。

注 – [IETF RFC 6749]允许公共客户机使用这一程序。本建议书认为，只有被要求由授权服务器进行认证的秘密客户机才可使用这一程序。

按照[IETF RFC 6749]，当授权服务器与使用准予类型资源拥有方密码资格证书的客户机进行互动时，必须：

- 对客户机进行认证
- 核实客户机提交的资源拥有方密码资格证书
- 如果客户机已由授权服务器认证并提出有效的资源拥有方资格证书，则发放接入令牌。

6.4 资源拥有方的认证

OAuth规范[IETF RFC 6749]并未具体规定授权服务器对资源拥有方（如最终用户）的认证。在NGN环境中，资源拥有方的认证机制必须符合[ITU-T Y.2702]的要求。

6.5 安全考虑

2.0版本OAuth规范[IETF RFC 6749]的“安全考虑”一节中提出了所有2.0版本OAuth客户机应用程序 – 网络应用、基于用户代理的应用和本征应用 – 的安全导则。本建议书建议在NGN环境中支持网络应用客户机，因此，在此仅适用与网络应用客户机相关的[IETF RFC 6749]的安全考虑。此外，[b-IETF RFC 6819]提供了全面的OAuth安全模式和协议设计背景。与网络应用客户机相关的[b-IETF RFC 6819]中的资料应在实施在NGN中支持OAuth时得到考虑。

这些解决方案还应符合[ITU-T Y.2701]、[ITU-T Y.2720]、[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-IETF RFC 6819] IETF RFC 6819, *OAuth 2.0 Threat Model and Security Considerations*.
http://datatracker.ietf.org/doc/rfc6819/

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
2014年，日内瓦