2012 年第 6 期（总第 13 期）

数字图书馆标准规范
跟踪扫描

主办单位：中国科学院国家科学图书馆

2012 年 9 月

为传播科学知识，促进业界交流，特编译《标准规范跟踪扫描》，仅供个人学习、研究使用。

目　录

【标准规范报道】

1、 ISO/IEC 29363:2008 Web 服务互操作性(WS-I)简单 SOAP 绑定概要 1.0 版本

ISO（国际标准化组织）以及 IEC（国际电工技术委员会）组成了全世界范围内的标准化的专门系统。属于 ISO 或 IEC 成员的国家机构通过技术委员会参与国际标准建设。ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。其他国际组织（政府及非政府的）与 ISO 和 IEC 联络，也参与该项工作。在信息技术领域，ISO 和 IEC 已建立起了一个联合委员会，ISO/IEC JTC 1。

国际标准的起草与 ISO/IEC 指引给出的规则相一致。

联合技术委员会的主要工作是制定国际标准。被联合技术委员会所采用的国际标准草案将被转发到国家机构进行投票。国际标准的发布至少需要参与投票的 75%的国家机构通过。

值得注意的是，本文档中的一些元素可能是专利权主题。ISO 和 IEC 不负责识别这样的专利权。

ISO/IEC 29363 由 Web 服务互操作性组织(WS-I)制定，并由联合技术委员会 ISO/IEC JTC 1（信息技术）经过 PAS 程序采纳，同时得到 ISO 和 IEC 的国家机构的许可。

本国际标准定义了 Web 服务互操作性（WS-I）简单 SOAP 绑定概要 1.0 版本（以下简称“概要”），由一组非专属性的网络服务规范以及那些促进互操作性的规范的说明和详述组成。

第一部分介绍了该概要，并解释了其与其他概要的关系。

第二部分，“概要一致性”，解释了与概要一致意味着什么。

后续每个部分都是概要的一个组成部分，且由两部分组成：该组成规范及其扩展点的详细描述，以及独立组成规范的分段。注意，本国际标准与参考规范中的部分数字并无关系。

其内容纲要如下：

1. 范围与介绍：范围、与其他概要的关系、国家惯例、概要识别与版本。
2. 概要一致性：一致性要求、一致性目标、一致性范围、声明一致性。
3. 消息传送：消息序列化。
4. 描述：绑定。

(编译自：ISO/IEC 29363:2008 Information technology -- Web Services Interoperability -- WS-I Simple SOAP Binding Profile Version 1.0. http://webstore.iec.ch/preview/info_isoiec29363%7Bed1.0%7Den.pdf. [2008-06-15])

（岳增慧编译，费大羽校对）

2、NISO 和 DAISY 联盟出版了编辑和交换框架标准

2012 年 8 月 7 日，国家标准信息组织和 DAISY 联盟宣布发布新的美国国家标准编辑和交换框架标准(ANSI/NISO Z39.98-2012)。该标准定义了使用 XML 表示数字信息从而形成不同格式之间的统一转换和获取的方法。该标准是DAISY 标准(ANSI/NISO Z39.86-2005(R2012))数字有声读物规范(Specifications for the Digital Talking Book, DTB)的修订和扩展版。DAISY 联盟是该标准的维护机构。

DAISY 修订工作组技术主席、DAISY 联盟的首席技术官 Markus Gylling 说 “A&I 框架是一个创建任意数量的、表示任意信息资源特定内容模块的模块化的、可扩展的架构。该架构同时支持新的输出格式，该输出格式可以随着需求的增加而添加或使用。该标准并没有对由此创建的分布格式增加限制，电子文本、盲文、大字版本和 EPUB 的格式都是由此标准创建的。”

DAISY 联盟秘书长、DAISY 修订工作组的行政主席 George Kerscher 说：“DAISY 联盟和主流出版社的组织正在寻找一种灵活的和强大的 XML 框架，而编辑和交换框架恰好满足了这个需求，它扩展了 DAISY 图书馆用户现存团体创建的可能性，并且同时扩大了符合该标准的资源使用者和研发者的潜在人群。该标准也可用于电子杂志、数字图书、电子阅读器的语音文本文档和多媒体出版物。”

NISO 执行董事 Todd Carpenter 解释道：“即使新的 A&I 框架标准旨在取代数字有声读物标准，但是该标准在试用期间的反馈表明内容提供商和设备制造商对于该标准中的显著变化还需要几年的过渡期。为了符合这种需求，现行的 DTB 标准(ANSI/NISO Z39.86)将会接受新的五年评议期，而 A&I 框架则作为新的标准(ANSI/NISO Z39.98)。”

A&I 框架标准适用于任何使用 XML 编辑工作流的组织、可获取的电子出版物研发者和出版者、以及创建与分布式格式（如 EPUB）的新的文档类型纲要的机构。

(编译自：NISO and DAISY Consortium Publish Authoring and Interchange Framework Standard. http://www.niso.org/news/pr/view?item_key=47de4fe39e4ee2256ce26f1438daebb19d394258. [2012-08-07])

（张琳编译，岳增慧校对）

3、NISO 和 NFAIS 发布关于期刊文章补充材料建议性实践方案草稿的第二部分寻求公众评议

2012 年 7 月 30 日，国家标准信息组织和高级信息服务国家联盟(National Federation for Advanced Information Services, NFAIS)正式宣布期刊文章补充材料在线建议性实践，B 部分：技术实践方案(Practice on Online Supplemental Journal Article Materials, Part

B: Technical Recommendations)(NISO RP-15-201x)进行公众评议，2012 年 9 月 15 日截止。尽管期刊文章越来越多的加入了补充性材料，但是至今仍未有关于补充材料的遴选、传递、发现或表示的公众认可的实践指南规范。为了弥补这一缺憾，NISO 和 NFAIS 联合创建了此领域的工作组。此工作组的目的就是为补充材料的管理者和作者提供指南并且创建最佳实践方案，从而为图书馆员、标引服务人员和存储管理人员解决相关的问题。补充材料项目先后有两个工作组：一个是强调商业实践，另一个则是关注于技术问题。目前，包括技术工作组实践方案在内的工作草案均处于公众评议阶段，商业组草案是在今年年初发布的。随着公众评议期的结束，这两个部分将合成最终的推荐性实践方案。

数字出版战略及美国化学学会的资深专家、NISO/NFAIS 期刊文章补充材料技术工作组副主席 David Martinsen 说：“技术推荐性实践方案与 A 部分中关于完全理解期刊文章的 Integral Content 和提供文章内容扩展和相关性的 Additional Content 的区分是完全一致的。完整的补充材料对于文章学术数据部分的理解是非常重要的，并且应当和文章一起保存。推荐性实践方案为这些数据和相关文章的保存提供了操作指南。”

“确保期刊文章补充材料的有效获取、使用、长期保存需要预先规划唯一标识符、元数据、文件格式和压缩包”，OSA-光学学会内容技术架构师、NISO/NFAIS 期刊文章补充材料技术工作组的副主席 Alexander Schwarzman 解释道：“技术推荐性实践方案很大程度上简化了补充材料管理的规划和决策过程，并且同时能够确保出版者和出版平台之间的标准化途径。”

“为了支持该推荐性实践方案，工作组还创建了一个元数据框架、一个标签集以及标注实例。这些辅助性文档同时接受公众评议，对于该推荐性实践方案的实施是非常有帮助的。”项目副主任 Nettie Lagace 说。

(编译自：NISO and NFAIS Issue Draft for Public Comment of Second Part of Recommended Practice on Supplemental Materials for Journal Articles. http://www.niso.org/news/pr/view?item_key=085d5c2ed191161090658d59a44c76645d96f94d. [2012-07-30])

（张琳编译，岳增慧校对）

4、知识库使用统计指南

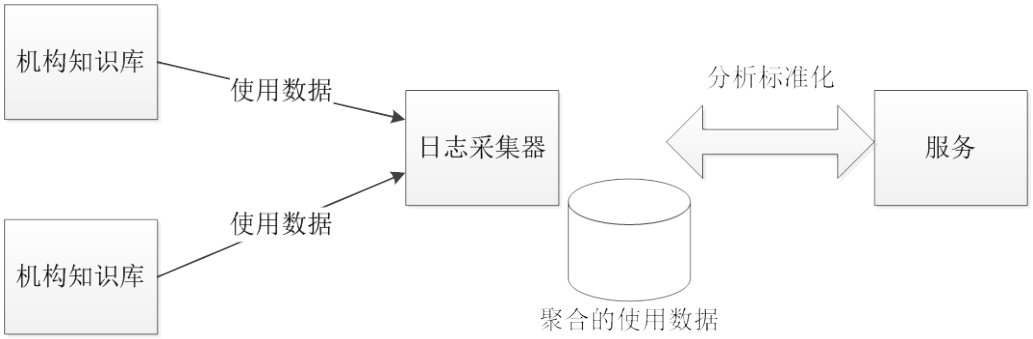
出版物能够通过网络以开放获取的方式被访问的好处之一是：能够追踪到该出版物被查看次数和被下载次数。但是往往存在着多种追踪统计的方法，你如何能够知道该出版物是被某个人查看了而不是被某个机器查看了呢？

在 SURFshare 的“SURE”（知识库使用统计）项目中，已经考虑召开关于知识库中出版物下载统计的研讨会。而且该项目已经开发了一个用于收集、分析和展示日志数据的中央数据库。这使得 NARCIS 研究门户能够针对每一个出版物显示用户使用的统计数据，从而能够

对不同种类的知识库数据进行比较。

结果：

莱顿大学、阿姆斯特丹大学、阿姆斯特丹自由大学以及荷兰皇家艺术与科学学院（KNAW）已经同意在 SURFshare 的 SURE（知识库使用统计）项目这一环境下开发一个工具。



1. 适用于所有机构知识库的通用软件。同时也是用于指导如何将知识库中的日志数据转换到中央数据库中去的指南。
2. 用于从多种不同知识库收集日志数据的中央数据库（日志收集器）软件。
3. 用于收集、分析和规范化所有日志文件并以单个出版物或文档的形式将其展示的中央数据库。
4. 提供一份基于统计分析的服务概览的服务目录。NARCIS 使用该服务为每一个出版物呈现统计数据。
5. 国际化机器过滤列表。这能够分辨普通用户还是机器所为。机器数据将会被过滤掉，这样统计数据将会被规范化从而可以比较。

该项目的结果可以在 SURF 的 Wiki（http://wiki.surf.nl/display/statistics/Home）上看到。

目的：

SURE 项目的结果使得知识库的管理者能够为研究人员和其他最终用户提供统计分析服务。

莱顿开放获取基础项目（先于 SURE 项目）的结果提供了该统计分析服务的一个实例。莱顿项目包含了一项向科学家发送使用统计数据邮件的实验。这就能够使他们看到知识库中的出版物被引用和被下载的最新频次。该服务受到广泛的好评。SURE 意味着莱顿大学的统计数据能够和马斯特里赫特大学的统计数据进行比较。

未来：

接下来的工作是让所有荷兰的大学实施这一协议并使用这一工具。如果所有的大学都实施 SURE 计划的话，NARCIS 将能够提供所有出版物的统计分析。这样的话，荷兰所有大学的研究人员都能够知道其出版物已经被查看或下载的频次。

国际化：

SURE 项目参与者将其经验介绍给知识交换环境下的可比项目。欧洲 OpenAire 项目也利用 SURE 项目的成果。

机构：格罗宁根大学、莱顿大学、阿姆斯特丹大学、阿姆斯特丹自由大学。

项目经理：P. Verhaar。

预算：20,000 欧元。

津贴：10,000 欧元。

开始时间：2009 年 6 月 1 日。

结束时间：2010 年 10 月 31 日。

(编译自：Statistics on the Usage of REpositories (SURE). http://www.surf.nl/en/projecten/Pages/SURE.aspx. [2010-10-31])

（费大羽编译，张琳校对）

5、用于管理科研数据的元数据

2012 年 8 月 22 日，将举行 NISO/DCMI 网络研讨会。

在过去的几年里，人们越来越关注数据归档与共享的国内外政策。主要动因包括数字数据的扩散以及人们对科研数据和作为学术交流框架一部分的补充信息的日益增长的兴趣。关键目标不仅包括科研数据的保存，也包括使数据能够验证研究成果，并支持数据的重新利用。

元数据在这些事业中地位显著，并对任何数据仓储以及归档活动至关重要，因此，对科研数据元数据的关注度越来越高——尤其是元数据标准开发与互操作、数据保管、元数据生成过程、数据标识符、（科学家）名称权限控制、关联数据、本体与词汇工作以及数据引用标准。

NISO/DCMI 网络研讨会将提供用于管理科研数据的元数据实践的历史回顾与当前概述，以及从操作存储库、社区驱动的数据科学活动中抽取出的实例。该会议也将讨论元数据生成、标识符、名称权限控制、关联数据以及数据引用的挑战和可能的解决方案。

发言人：Jane Greenberg、Thomas Baker。

(编译自：Metadata for Managing Scientific Research Data. http://www.niso.org/news/events/2012/dcmi/scientific_data/. [2012-07-18])

（岳增慧编译，费大羽校对）

【标准规范推介】

一、OAuth 2.0 授权框架

摘要

OAuth 2.0 授权框架提供一个第三方的应用程序，用于获得访问 HTTP 服务的有限权限，可以是通过协调资源拥有者和 HTTP 服务间的批准交互代表资源拥有者，或者是通过允许第三方应用代表其自身获得访问权限。该规范替代之前编号为 RFC5849 的的 OAuth 1.0 协议。

1 介绍

在传统的基于客户端-服务器端的身份验证模型中，客户端通过使用资源拥有者的私有证书的方式进行身份验证从而访问受限制资源（受保护资源）。为了使得第三方应用能够访问受限制资源，资源拥有者必须将其私有证书共享给第三方。这就产生了一些问题和局限：

- 第三方应用需要存储资源拥有者的私有证书留作将来使用，典型的就是明文密码。
- 虽然密码验证会造成安全隐患，但是服务器仍然需要支持密码身份验证。
- 第三方应用对资源拥有者的受保护资源获得过多的使用权限，使得资源拥有者不能限制针对资源限制子集的时限或权限。
- 资源拥有者无法在不撤回所有第三方权限的情况下撤回某个特定的第三方权限，而只能通过修改密码的方式才能达到目的。
- 破解任何第三方应用将会导致终端用户密码以及被改密码所保护的数据的破解。

OAuth 通过引入身份验证层并将客户端和资源拥有者的角色进行分离来解决这些问题。在 OAuth 中，客户端请求访问由资源拥有者控制并由资源服务器托管的资源，然后能够得到一套和资源拥有者不同的私有证书。

客户端并非使用资源拥有者的私有证书去访问受保护的资源，而是获得一个访问令牌（一个代表某一特定作用域、生命周期和其他访问属性的字符串）。访问令牌由授权服务器在资源拥有者的授权下发给第三方客户端。客户端使用访问令牌访问由资源服务器托管的受保护的资源。

例如，一个用户（资源拥有者）允许一个打印服务（客户端）访问其存在另一照片共享服务（资源服务器）中的照片，而不需要将其用户名和密码告之该打印服务。她在一个被改照片共享服务所信任的身份验证服务（授权服务器）上完成验证，而该验证服务会将特定委托服务的私有证书（令牌）发给原来的打印服务。

该规范设计用于 HTTP 协议，任何其他非 HHTP 协议下使用 OAuth 都不在本规范范围内。

以信息文档的形式发布的 OAuth 1.0 协议，是一个小专业团体努力的成果。该标准跟踪规范吸取了 OAuth 1.0 的开发经验，并从 IETF 社区收集增加的用例和扩展的需求。OAuth 2.0 协议并不向后兼容于 OAuth 1.0。这两个版本协议可以同时出现在网络上，在实施的时候可

以选择同时支持这两个协议。然而，该规范的目的是新实施的项目支持本文所述的 OAuth 2.0，而 OAuth 1.0 仅仅是用于支持现有的部署。OAuth 2.0 协议和 OAuth 1.0 协议仅有很少一部分实施细节是可以共享的。熟悉 OAuth 1.0 的实施者需要处理本文档，而不要去猜想其结构和细节。

1.1 角色

OAuth 定义了四个角色：

资源拥有者

能够授权访问受保护资源的实体。当资源拥有者是一个人的时候，资源拥有者就是指最终用户。

资源服务器

受保护资源的服务器，使用令牌能够接受和响应受保护资源的请求。

客户端

代表资源拥有者及其授权产生受保护资源请求的应用。这里的术语“客户端”并不意味着任何特定的实现特征（应用在服务器、客户端或其他设备上执行）。

授权服务器

服务器在成功对资源拥有者认证并获取授权后将令牌分发给客户端。

授权服务器和资源服务器之间的交互问题不在本规范的范围之内。授权服务器也可以作为资源服务器或多资源服务器。

1.2 协议流程

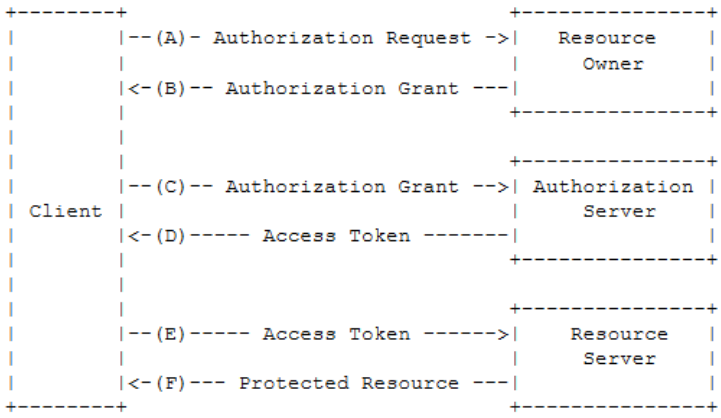


图 1 抽象协议流程

如图 1 所示的 OAuth 2.0 抽象协议流程描述了四个角色之间的交互情况，包含如下步骤：

（A） 客户端从资源拥有者那里请求授权。可以直接向资源拥有者发送授权请求（如图 1），也可以通过使用中介授权服务器间接的发送授权请求，而且后者更好。

（B） 客户端获得一份授权，该授权是代表资源拥有者授权的凭证，并以本规范所述的四类授权类型之一的方式表达，也可以使用其他扩展的授权类型。授权类型取决于客户端认证请求的方法以及认证服务器所支持的类型。

（C） 客户端使用它自己的私有证书到授权服务器上验证，并出示访问许可请求访问令牌。

（D） 授权服务器验证客户端私有证书和访问许可的有效性，如果有效的话，则分发令牌。

（E） 客户端从资源服务器请求受保护的资源，并通过出示令牌的方式进行授权。

（F） 资源服务器确认令牌有效性，如果是有效的话，则相应这个资源请求。

从资源拥有者获得访问许可(如步骤 A 和 B 所述)更好的方式是使用授权服务作为中介，这将会在图 3 中展示。

1.3 访问许可

客户端使用访问许可作为出示资源拥有者认证（用于访问受保护资源）的凭证，从而获得令牌。本文档定义了四类授权类型：授权码、隐式、资源拥有者密码凭证和客户端凭证，同时还定义了用于定义新增类型的扩展算法。

1.3.1 授权码

通过使用介于客户端和资源拥有者之间的授权服务器获得授权码。客户端不是直接向资源拥有者请求授权，而是从资源拥有者转向授权服务器（通过用户代理），然后将授权码从资源拥有者返回给客户端。

在将授权码从资源拥有者指回客户端之前，授权服务器对资源拥有者进行认证并获得授权。由于资源拥有者仅仅是和授权服务器进行了认证，所以资源拥有者的凭证不会暴露给客户端。

授权码提供了一些重要的安全益处，比如能够对客户端进行认证以及无需通过资源拥有者的用户代理直接将令牌传给客户端。而通过代理的方式存在将令牌暴露给第三方（包括资源拥有者）的隐患。

1.3.2 隐式

隐式授权是一个针对客户端优化过的简单授权码，使用脚本语言（如 JavaScript）在浏览器中实现。利用隐式授权码，不是向客户端分发授权码，而是直接分发一个令牌（这是资源拥有者授权的结果）。授权类型之所以是隐式的是因为没有分发中间凭证（如授权码），然而再获得令牌。

在隐式授权过程中分发令牌时，授权服务器不对客户端进行认证。在某些情况下，可以通过重定向 URI 来核实客户端身份，该 URI 被用于将令牌分发给客户端。令牌有可能因为要访问资源拥有者的用户代理而被暴露给资源拥有者或其他应用。

由于隐式代理减少了获取一个令牌的往返次数，其能够提供一些客户端（如以浏览器嵌入式应用的客户端）的响应能力和效率。然而，需要权衡该便利和使用隐式授权带来的安全影响（如 10.3 和 10.16 所述），尤其是当可以使用授权码许可类型的时候。

1.3.3 资源拥有者密码证书

资源拥有者密码证书（例如用户名和密码）可以直接用作访问许可来获取访问令牌。这种私有证书只应在如下情况使用：当在资源拥有者和客户端之间有很强的信任关系的时候

（例如客户端是设备操作系统的一部分或具有很高权限的程序时），以及当其它访问许可类型（如授权码）不可以使用的时候。

即使这种许可类型需要客户端直接访问资源拥有者的私有证书，资源拥有者的私有证书也只是在一个请求中使用并且被交换为访问令牌。通过使用长生命周期的访问令牌或刷新令牌的方式交换私有证书，该许可类型不再需要客户端存储资源拥有者将来要用的私有证书。

1.3.4 客户端私有证书

当授权作用域限制在客户端所控制的受保护资源或之前与授权服务器商定好的受保护资源时，客户端私有证书（或客户端授权的其他形式）可被用作访问许可。客户端私有证书用作访问许可的典型例子是当客户端代表其自身执行操作时（客户端同时也是资源拥有者），或者当客户端请求访问基于之前与授权服务器商定好的受保护资源时。

1.4 访问令牌

访问令牌是用于访问受保护资源的私有凭证。访问令牌是分发给客户端用于代表授权的字符串。字符串通常不会对客户端透明。令牌由资源拥有者授权，由资源服务器和授权服务器执行，说明特定的访问范围和期限。令牌可以使用可验证的方法来表示用于检索或自包含授权信息的标识符（比如包含一些数据和签名的令牌字符串）。有可能需要另外的授权私有证书用于客户端使用令牌，但这已经超出了本规范的范围。

访问令牌提供了一个抽象层，用能被资源服务器理解的单一令牌取代不同的授权概念（如用户名和密码）。该抽象是的分发访问令牌比用于获取它们的访问许可更加具备约束力，同时移除资源服务器理解更广泛授权方法的需求。

基于资源服务器安全需求，访问令牌可以有不同的格式、结构和正则化方法（如密码属性）。用于访问受保护资源的访问令牌属性和方法超出本规范的范围，其会在同系列规范中进行定义。

1.5 刷新令牌

刷新令牌是用于获得访问令牌的私有许可。刷新令牌通过授权服务器被分发给客户端，并且当现有访问令牌失效或过期时被用于获取一个新的访问令牌，或者用于以同样或更小的范围来获取另外的访问令牌（访问令牌可以比资源拥有者授权的拥有更短的生命周期和更少的权限）。在授权服务器处理的时候是否分发刷新令牌是一个可选项。如果授权服务器分发了一个刷新令牌，则当分发访问令牌时（如步骤 D）刷新令牌会被包含在图 1 内。

刷新令牌是一个代表资源拥有者授予客户端的授权字符串。该字符串通常对客户端是透明的。令牌表示一个用于检索授权信息的标识符。和访问令牌不同，刷新令牌目的是仅仅和授权服务器一起使用而绝不向资源服务器发送刷新令牌。

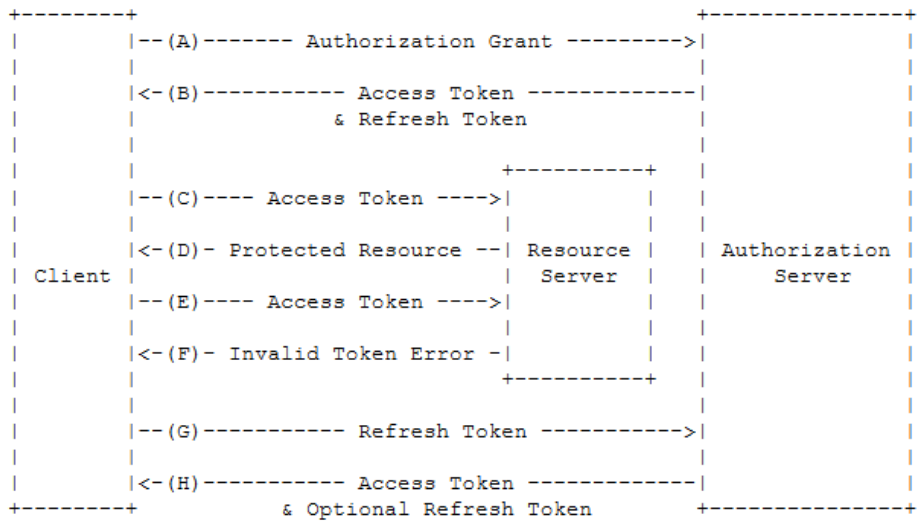


图 2 刷新失效的访问令牌

接下来具体阐述图 2 所示的各个步骤：

（A） 客户端通过使用授权服务器进行验证请求一个访问令牌，并出示一个访问许可。

（B） 授权服务器验证客户端以及访问许可的有效性，如果通过的话，则分发一个访问令牌和刷新令牌。

（C） 客户端通过出示访问令牌向资源服务器请求受保护资源。

（D） 资源服务器验证访问令牌的有效性，如果通过的话，则响应这个请求。

（E） 不停重复步骤（C）和步骤（D）直到访问令牌过期。如果客户端知道访问令牌过期则跳到步骤（G),否 则它会再请求一次受保护资源。

（F） 因为访问令牌是无效的，资源服务器则返回一个无效令牌错误。

（G） 客户端通过使用授权服务器进行验证请求一个新的访问令牌，并出示刷新令牌。客户端授权需求基于客户端类型和授权服务器的政策。

（H） 授权服务器验证对客户端进行验证以及刷新令牌的有效性，如果通过的话，则分发一个新的访问令牌（也可能还有一个刷新令牌）。

步骤 C、D、E 和 F 超出了本规范的范围。

(编译自：The OAuth 2.0 Authorization Framework..
http://www.ietf.org/id/draft-ietf-oauth-v2-31.pdf. [2012-06-19])

（费大羽编译，张琳校对）

二、有效 XML 交换(EXI)概要

1 介绍

许多类别的设备和用例都希望使用 EXI 作为交换格式。由于各种限制，这些应用不能或者不被允许在运行期间任意存储。此领域的内容中的 EXI 的某些评估遇到一些挑战，即使用

各自有限阈值时尝试限制内存使用量。

该 EXI 纲要文件指定了确保与 EXI1.0 规范兼容的情况下，重视内存限制的规则。第 2 部分语法限制(Grammar Capping)定义了限制语法学习定义的机制和参数，第 3 部分本地值限制(Local Value Capping)定义了简化值索引的机制，第 4 部分参数表示(Parameters representation)定义了本纲要中定义的参数在 EXI 标头中的表示方法。

为了标识 EXI 1.0 的兼容性，EXI 纲要并没有提供用于名称列表的内存绑定机制。该工作组讨论了允许 EXI 处理器克服这些问题策略和规则。

2 语法限制(Grammar Capping)

为了禁止语法学习，xsi:type 属性可能从展开的内置语法向合并的框架通知(schema-informed)语法转变。尤其是，xsd:anyType 复杂类型可以用来表示任意 XML 元素。

注意 EXI 纲要只能限制框架通知(schema-informed)EXI 流而不是无模式（schema-less）EXI 流限制语法学习。在没有获取任何框架的情况下，“schemaId”可能设置为空值，从而使所有由内置 XML 框架类型的语法，尤其是符合 xsd：anyType 复杂类型的语法，都可通过“xsi:type”语法进行转换。

以下两个前缀用于在本文档中设置某个命名空间。下面显示的绑定均为假设，但是如果任何前缀都正确的和命名空间绑定，那么这些前缀就可以在实践中使用。

Prefix	Namespace Name
xsd	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

2.1 语法学习禁用机制(Grammar Learning Disabling Mechanism)

对于一个已知元素 E，禁用语法学习是通过嵌入带有 xsd:anyType 值的 xsi:type 属性事件作为元素 E 的 SE 事件之后的第一个事件完成的。如果元素 E 已经有了 xsi:type 属性并且对于元素 E 的语法表示来说，已经禁用了语法学习，那么 xsi:type 属性值必须指向一个可以表示指定元素的已知框架通知(schema-informed)语法。

如果在新的内置元素语法 G 的用例中，要禁用元素 E 语法学习，就要遵循以下规则：

- 如果一个 xsi:type 事件尚未表示，则和 xsd:anyTye 值一起插入到 SE 事件中表示该元素。xsi:type 属性事件必须用事件编码长度为 2 的 AT(*)表示。
- 对于 EXI 流中的 E 元素之后的所有元素，与 E 元素具有相同的 QName，并且使用内置元素语法表示，如果一个 xsi:type 事件尚未表示，则和 xsd:anyTye 值一起插入到 SE 事件响应之后表示该元素。xsi:type 属性事件必须用事件编码长度为 2 的 AT(*)表示。

如果在指定语法 G 的用例中，要禁用语法学习，就要遵循以下规则：

- 指定元素 E 的所有事件有待表示的均使用事件编码长度为 2 的 AT(*)表示。在这种例子中，EXI 处理器必须确保事件代码增量符合 EXI 1.0 规范中的 8.4.3 部分定

义的规则，但是不需要创建和插入顶级产品(top-level productions)。尤其是，EXI 处理器可能需要是否追踪已插入的 CH 产品(CH production)或者不在语法 G 中来保持顶级产品(top-level)符合在 EXI1.0 规范中的 8.4.3 部分定义的规则。

- 对于所有 EXI 流中的元素 E 之后的所有元素以及使用语法 G 的元素来说，xsi:type 属性事件必须用事件编码长度为 2 的 AT(*)表示。

对于一个给定的语法一旦有产品插入，语法使用就会受到限制，从而只有产品已插入并且顶级水平产品的数量需要存储在语法中。应该指出的是，即使对于一个给定的语法的生产插入式禁用的，在产品插入之间插入的产品对于语法是禁用的，并且该语法在整个文档中适用的。

2.2 语法学习禁用参数

为了限制由于语法学习产生的日益增加的内存消耗，EXI 纲要确保限制展开内置语法和插入产品的数量。并且 w 为该目的定义了两个参数：

[定义：maximumNumberOfBuiltInElementGrammars 选择是内置元素语法的最大数量，增加动态产品而不是 AT(xsi:type)产品]

[定义：maximumNumberOfBuiltInProductions 选择是顶级水平产品的最大数量，能够动态插入除 AT(xsi:type)产品外的内置元素语法]

如果以下的条件是正确的，要禁用语法学习的元素 E 就需要创建新的内置元素语法 G：

- 对于动态产品而不是 AT(xsi:type)产品的内置元素语法数量已经增加等于或者更多的 maximumNumberOfBuiltInElementGrammars 值。

如果以下条件是正确的话，产品插入用例的语法学习禁用：

- 动态插入所有内置元素的顶级水平产品的数量总和等于或大于 maximumNumberOfBuiltInProductions 值。

一旦设定参数，MUST 的规则必须恰当应用。参数有可能是在语法学习禁用机制的应用中需要定义一个未指定的优化存取控制的。在这个用例中，EXI 处理器不应该设定两个定义的参数，并且应当使用 out-of-band 机制来承载使用中的精确语法禁用。

3 本地值限制

EXI 处理器的某些类别可能承担起本地值列表表示的消耗。本纲要定义了一个能够禁用本地值参考的参数。全局值索引可能使用 EXI1.0 规范中定义的选项。

[定义：localValuePartitions 是一个用于指示是否使用本地值分割的布尔逻辑。]值“0”表明当“1”表示 EXI 1.0 规范中的行为时，没有本地值分割。

当 localValuePartitions 值设置为“0”时，表示参考字串值对本地值分割的引用错误。

有些处理器可能会决定在本地值列表构建和使用中采用细粒度策略。

4 参数表示

EXI 纲要的使用是由在 EXI 六种的 EXI 可选项中用户定义的元数据部分中编码以下 XML

元素的：

```
<p xmlns="http://www.w3.org/2009/exi"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                              xsi:type="xsd:decimal">
                              ...
                          </p>
```

该元素的内容显示纲要三个参数值，这三个参数值是由单一的十进制值编码的。每个纲要参数如下表示：

1. localValuePartitions 参数编码作为十进制值的标识：当十进制值为正时，参数为 0，十进制值为负时参数为 1。

2. maximumNumberOfBuiltInElementGrammars 参数这代表了第一个无符号整数对应于积分部分的十进制值:如果 maximumNumberOfBuiltInElementGrammars 参数是无限的，则无符号的整型值为 0，否则为-1。

3. maximumNumberOfBuiltInProductions 参数代表了第二个无符号整数对应小数部分以相反的顺序的十进制值:如果 maximumNumberOfBuiltInProductions 参数是无限的，则无符号整型值为 0，否则为-1。

为了声明 EXI 纲要中没有声明的每一个参数值，编码了没有任何内容的 exi:p 元素：

```
<p xmlns="http://www.w3.org/2009/exi"/>
```

在这种用例中，实际的纲要参数值（或细粒度限制策略）应当由 out-of-bound 机制定义。

(编译自：Efficient XML Interchange (EXI) Profile. http://www.w3.org/TR/2012/WD-exi-profile-20120731/. [2012-07-31])

（张琳编译，岳增慧校对）