新闻出版重大科技工程项目管理及相关成果丛书

Collection of Standards on the National DRM R&D Project (III)

数字版权保护技术研发工程标准汇编（下）

魏玉山 主编 刘颖丽 副主编

中国书籍出版社
China Book Press

新闻出版重大科技工程项目管理及相关成果丛书

数字版权保护技术研发工程标准汇编（下）

Collection of Standards on the National DRM R&D Project（III）

中国书籍出版社
China Book Press

图书在版编目（CIP）数据

数字版权保护技术研发工程标准汇编：全3册 / 魏玉山主编. — 北京：中国书籍出版社，2016.10

ISBN 978-7-5068-5843-4

Ⅰ. ①数… Ⅱ. ①魏… Ⅲ. ①电子出版物－版权－保护－标准－汇编 Ⅳ. ① D913-65

中国版本图书馆 CIP 数据核字（2016）第 233369 号

数字版权保护技术研发工程标准汇编（下）

魏玉山　主编

统筹编辑　游　翔
责任编辑　吴化强
责任印制　孙马飞　马　芝
封面设计　楠竹文化
出版发行　中国书籍出版社
地　　址　北京市丰台区三路居路 97 号（邮编：100073）
电　　话　（010）52257143（总编室）　（010）52257140（发行部）
电子邮箱　eo@chinabp.com.cn
经　　销　全国新华书店
印　　刷　河北省三河市顺兴印务有限公司
开　　本　787 毫米×1092 毫米　1/16
印　　张　70.75
字　　数　1567 千字
版　　次　2016 年 12 月第 1 版　2016 年 12 月第 1 次印刷
书　　号　ISBN 978-7-5068-5843-4
定　　价　312.00 元（全三册）

总目录

分册目录

第五章

接口协议类标准

GC

数字版权保护技术研发工程标准

GC/BQ 19—2015

版权保护系统间通信协议

Rights management authorization protocol between systems

2015－02－03 发布　　2015－02－03 实施

新闻出版广电总局新闻出版重大科技工程项目领导小组　发布

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由新闻出版广电总局新闻出版重大科技工程项目领导小组办公室提出并归口。

本标准主要起草单位：北京方正阿帕比技术有限公司。

本标准主要起草人：黄肖俊、秦丽娇、张泽、王勤、王德胜。

版权保护系统间通信协议

1 范围

本标准给出了数字版权保护技术研发工程系统间授权通信协议的模型、消息体、协议映射和协议安全的说明。

本标准适用于数字版权保护技术研发工程。

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。

GB/T 25069 信息安全技术 术语

GC/BQ 3 数字版权保护技术研发工程术语

GC/BQ 4 数字版权管理标识

3 术语和定义、缩略语、符号

3.1 术语和定义

GC/BQ 3 界定的以及下列术语和定义适用于本文件。

3.1.1

加密密钥 cipher key

结合安全算法，用于编码和解码用户或信号数据的代码。

3.1.2

数字签名 digital sign

附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人(例如接收者)伪造或抵赖。

[GB/T 25069，定义2.2.2.176]

3.1.3

完整性 integrity

数据没有被非授权的方式所改变或破坏的特性。

3.1.4

密钥 key

一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的复合序列。

[GB/T 25069，定义2.2.2.106]

3.1.5

超级分发 superdistribution

对可公开获取的加密数字内容的一种分发手段。

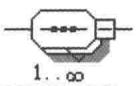
3.2 缩略语

下列缩略语适用于本文件。
XML：可扩展置标语言（Extensible Markup Language）
HTTP：超文本传输协议（Hyper Transfer Protocol）

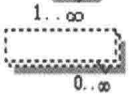
3.3　符号

下列符号适用于本文件。

 　按顺序出现的子元素

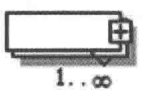


重复出现的一个或无穷多个子元素



可出现多个的可选元素

 　必选元素



至少有一个，可多个的元素

4　版权保护系统间通信协议模型

授权方服务器向授权接受方服务器进行授权的通信协议模型见图1。

图1　授权通信协议模型

授权方服务器撤销授权接受方服务器的授权通信协议模型见图2。

图2　撤销授权通信协议模型

版权保护系统间通信协议的XML Schema见附录A，示例参见附录B。

5　协议消息体

5.1　授权协议

5.1.1　协议流程

授权协议的流程如图3所示。

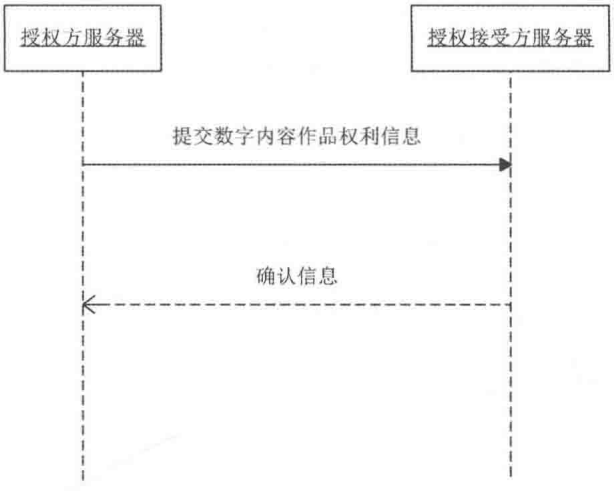


图3　授权协议流程

授权协议的步骤如下：

a)　提交数字内容作品的权利信息给授权接受方；

b)　授权接受方在接收到权利信息后向授权方进行确认。

5.1.2　协议消息

授权协议主要包括以下两类消息：

a)　数字内容作品权利信息

数字内容作品权利信息的结构如图4所示。

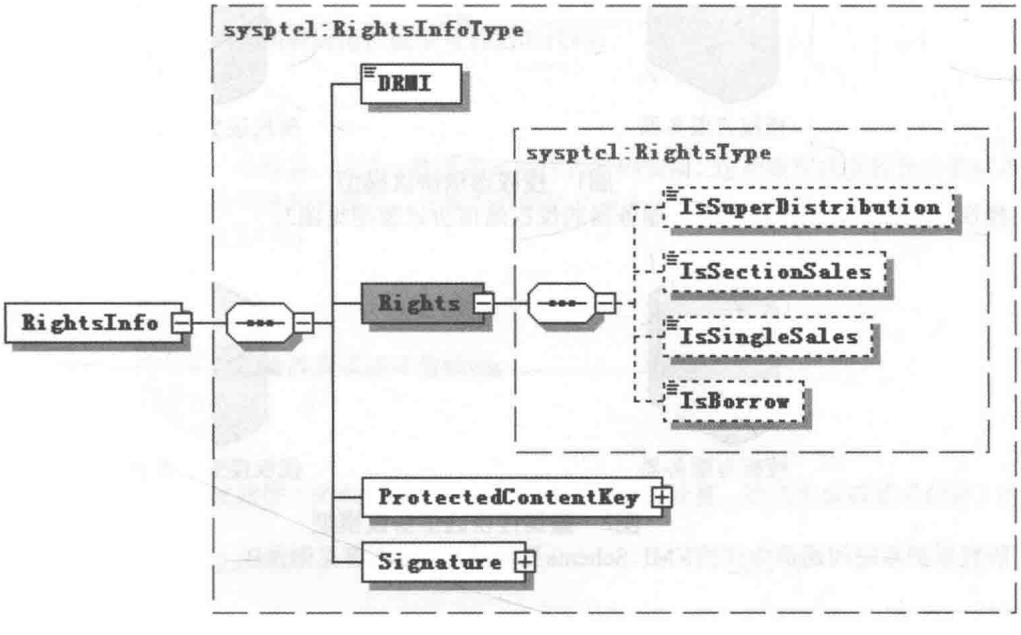


图4　数字内容作品权利信息结构

数字内容作品权利信息包括数字版权管理标识、权利、加密的内容密钥、签名，具体见表1。

表1　数字内容作品权利信息

序号	中文名称	英文标签	类型	长度	取值	选择性	说明	示例
1	数字版权管理标识	DRMI	字符串	22 个字符	定长	必选	数字版权管理标识，遵循 GC/BQ 4 要求	
2	权利	Rights	复合型	不定长	不定	必选	申请获取的数字内容权利，包括是否超级分发，是否章节销售，是否单本销售，是否可借阅等权利	
3	加密的内容密钥	ProtectedContentKey	复合型	不定长	不定	必选	用授权接受方公钥加密的内容密钥	
4	签名	Signature	复合型	不定长	不定	必选	授权方服务器端对发送消息的签名，签名范围为 Signature 部分之前的所有数据，遵循 XML Signature	

b)　确认信息

授权接受方的确认信息结构如图5所示。

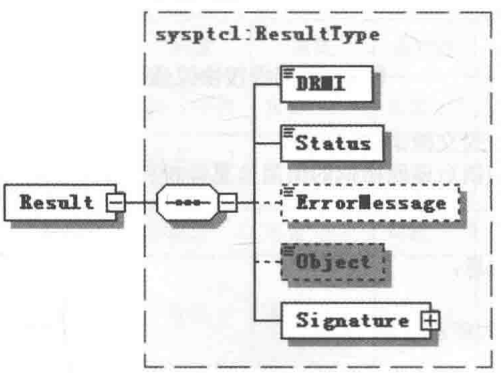


图5　授权接受方的确认信息结构

授权接受方的确认信息包括数字版权管理标识、状态、错误信息、扩展项、签名，具体见表2。

表2　授权接受方的确认信息

序号	中文名称	英文标签	类型	长度	取值	选择性	说明	示例
1	数字版权管理标识	DRMI	字符串	不定长	不定	必选	数字版权管理标识，遵循 GC/BQ 4 要求	
2	状态	Status	布尔型	定长，1 个字符	0，1，2，3	必选	0 为成功；1 为参数错误；2 为签名错误；3 为其他错误	
3	错误信息	ErrorMessage	字符串	不定长	不定	可选	错误描述	
4	扩展项	Object		不定长	不定	可选	描述一些扩展信息，对扩展信息的使用和定义在本协议中没有明确的规定，可以根据不同的情况自己定义	
5	签名	Signature	复合型	不定长	不定	必选	授权接受方服务器端对发送消息的签名，签名范围为 Signature 部分之前的所有数据，遵循 XML Signature	

5.2 撤销授权协议

5.2.1 协议流程

撤销授权协议的流程如图6所示。

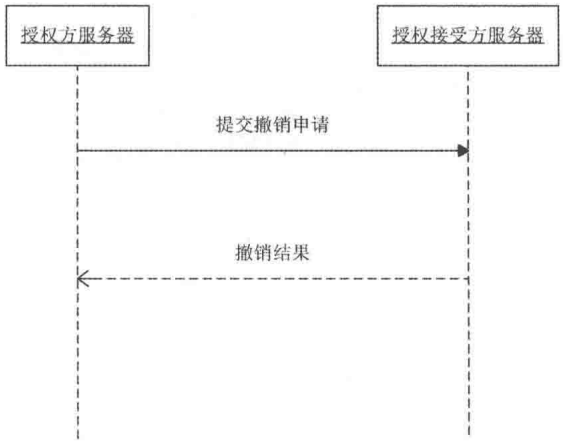


图6 撤销授权协议流程

撤消授权的步骤如下：

a) 授权方向授权接受方提交撤销的申请；

b) 授权接受方在完成撤销后返回撤销的结果信息给授权方。

5.2.2 协议消息

撤销授权主要包括以下消息：

a) 撤销申请

撤销申请的结构如图7所示。

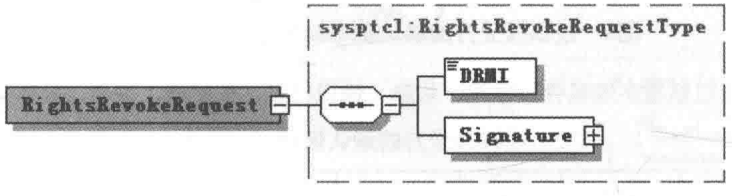


图7 撤销申请结构

撤销申请信息包括数字版权管理标识、签名，具体见表3。

表3 撤销申请信息

序号	中文名称	英文标签	类型	长度	取值	选择性	说明	示例
1	数字版权管理标识	DRMI	字符串	22 个字符	定长	必选	数字版权管理标识，遵循 GC/BQ 4 要求	
2	签名	Signature	复合型	不定长	不定	必选	授权方服务器端对发送消息的签名，签名范围为 Signature 部分之前的所有数据，遵循 XML Signature	

b)　撤销结果

撤销反馈的结果信息结构如图8所示。

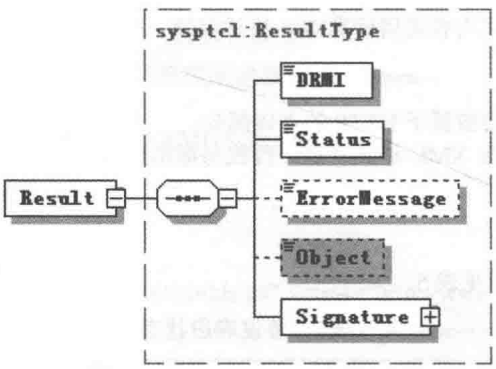


图8　撤销反馈结果结构

撤销反馈结果信息包括数字版权管理标识、状态、错误信息、签名、扩展项，具体见表4。

表4　撤销反馈结果信息

序号	中文名称	英文标签	类型	长度	取值	选择性	说明	示例
1	数字版权管理标识	DRMI	字符串	22 个字符	定长	必选	数字版权管理标识，遵循 GC/BQ 4 要求	
2	状态	Status	布尔型	定长，1 个字符	0，1，2，3	必选	0 为成功；1 为参数错误；2 为签名错误；3 为其他错误	
3	错误信息	ErrorMessage	字符串	不定长	不定	可选	错误描述	
4	签名	Signature	复合型	不定长	不定	必选	授权接受方服务器对确认消息的数字签名。签名范围为 Signature 部分之前的所有数据，遵循 XML Signature	
5	扩展项	Object		不定长	不定	可选	描述一些扩展信息，对扩展信息的使用和定义在本协议中没有明确的规定，可以根据不的情况自己定义。	

5.3　协议的触发

协议的触发应由授权方服务器的推送过程来完成，即授权方服务器将数字内容作品包括数字内容作品的元数据信息、内容资源文件及其权利信息主动推送给授权接受方，授权接受方按照定义的接口接受元数据及内容文件。

6　协议映射

6.1　概述

本标准描述了数字版权保护系统间协议数据如何通过HTTP传输协议进行传输，但是可扩展支持其他映射。

本标准范围内联网设备和服务器都应支持HTTP的传输协议，遵循HTTP规范。

6.2　HTTP 协议映射

6.2.1　协议请求