IMS Common Cartridge Authorization Web Service

Version 1.0 Final Specification

Date Issued: 1 October 2008

Latest Version: http://www.imsglobal.org/cc/index.html

IPR and Distribution Notices

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

IMS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on IMS's procedures with respect to rights in IMS specifications can be found at the IMS Intellectual Property Rights web page: http://www.imsglobal.org/ipr/imsipr_policyFinal.pdf.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE CONSORTIUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Document Name: IMS Common Cartridge Authorization Web Service

Date: 1 October 2008

Executive Summary

The Common Cartridge Authorization Service is intended to provide a standardized alternative for the custom access code authorization systems publishers and LMS platforms have traditionally used to control student access to premium cartridge content. The service neither defines how the access codes are created, nor how the access codes are actually validated. It only defines the communication between the LMS and cartridge publisher. Two primary extensions to the traditional models are being added. First, cartridges may specify that only certain content items should be protected and that others may be freely accessed. This should allow publishers to create a single cartridge that contains both premium and standard content, thus simplifying the publishing process. Secondly, support is added for specifying that authorization should occur when the cartridge is imported into the LMS.

Table of Contents

1. Introduction

1.1 Scope and Context

The Content Package Authorization Service will allow publishers a standard way of describing when authorization is required for users to access the content contained in a common cartridge. Definition of the structure of the information required to perform authorization and where it appears within the common cartridge is within scope. Likewise, the definition of the communication that happens between the LMS and the cartridge publisher is also in scope. How the access codes used in the process are created and distributed is out of scope. Also out of scope are the actual rules the publisher might enforce when actually validating an access code when the request comes from the LMS. Also out of scope is any type of encryption that would protect the cartridge content from being directly manipulated outside of a compliant LMS.

1.2 Approach

A common cartridge will include the information required for the LMS to communicate with an authorization service provided by the cartridge publisher. When a user attempts to access or import protected cartridge content, the LMS will prompt the user for an access code. The LMS will then use the service to send to the cartridge publisher the access code and some unique identifier for the cartridge being accessed. The cartridge publisher’s system will attempt to validate the provided information. If the information is valid the service will respond with a success code and optionally an expiration date after which access by the user should once again require contacting the service. If the information is deemed invalid, an error code is returned along with a human-readable description of why the credentials were rejected.

1.2.1 Technology

The CC Authorization Service will be implemented as a SOAP service between the LMS and cartridge publisher.

1.3 Structure of this Document

The structure of this document is as follows:

1. Introduction	Sets the scope of what the specification covers and summarizes the authorization process.
2. Use Cases	Documents the authorization use case and the roles involved.
3. Architecture & Approach	Details the technical design of the authorization web service.
4. Authorization Model	Provides the formal representation of the authorization web service expressed in UML.
5. Implementation Guidelines & Best Practice	Offers advice on implementing a Common Cartridge authorization web service.
6. Conformance	Describes how to use the publicly available ANGEL implementation of the authorization web service for self test of an LMS implementing the service.
Appendix A WSDL	Provides the URL for downloading the WSDL xml.

1.4 References

[CC, 08a] *IMS Common Cartridge Profile (CC) v1.0 Final Specification*, K.Riley, IMS GLC, October 2008.

1.5 Definitions

Term	Definition
Access Code	A code used to authorize user access to a protected resource, in this case a Common Cartridge or a discrete component thereof.
associatedcontent	A resource type that includes a collection of files used by a specific learning application resource. Each file referenced must exist in the directory containing the descriptor file of the learning application resource with which it is associated or any subdirectory thereof. A resource of the type “associatedcontent” must comply with the following restrictions: 1. It must contain a *file* element for each file that exists in the directory that contains the associated learning application resource’s descriptor file or any of its subdirectories. 2. It must not contain any references to files above the directory containing the associated learning application resource’s descriptor file. 3. It must not contain any *dependency* elements.
Common Cartridge	A content packaging profile agreed between content providers and LMS providers, offering a common format for the distribution of both open and access protected content. The profile harnesses Content Packaging, LOM Metadata and QTI, augmented with a specification for simple access control.
Content Elements	Discrete content elements within a Learning Activity aggregate as part of a Learning Object Application Resource or module (lesson).
Course Content Package	A term for any current proprietary LMS specific, publisher developed and sourced, content package that is made commercially available via the publisher or LMS vendor to its customer base. Examples of such cartridges are the WebCT ePack, Blackboard Course Cartridge etc.
Deployment Context	Any one of the LMS deployment and learning contexts made available for online access to learning activity via learning modules, learning objects application resources and content element interaction.
Descriptor File	The file that serves as the entry point for accessing the information about a learning application resource required to import the learning application resource into the target system. Generally an XML file meeting an appropriate file specification based on the type of learning application resource. However, in some cases, such as SCORM, the file may be a zip archive or some other structured file format. The descriptor file is not intended to be displayed within the target system. Rather, it is intended to be processed by the target system upon import of the cartridge. The descriptor file is associated with a learning application resource by means of a “file” element.
Directory	A physical folder in a content package archive.
Learning Activity	A general term for describing an online learning experience and interaction with learning modules, learning objects application resources and content elements typically composed to deliver a particular outcome or experience for the Student.

Term	**Definition**
Learning Application Resource	Any one of a number of *resource* types that require additional processing and interpretation before they can be imported and subsequently represented within the target system. Physically, a learning application resource consists of a directory in the content package containing a descriptor file and optionally additional files and subdirectories used exclusively by that learning application resource. Each learning application resource must have a corresponding *resource* element in the manifest. Examples of learning application resources include QTI assessments, SCORM items, Discussion Forums, etc. The *type* attribute of the *resource* element is prescribed by the type of learning application resource being represented. If additional files beyond the learning application resource's descriptor file exist in the learning application resource's directory or any of its subdirectories, these files must be represented in a resource element of type "associatedcontent" which is list as a *dependency* within the learning application resource's *resource* element. A resource that represents a learning application resource has the following general restrictions: 1. It must contain a *file* element that points to the learning application resource's descriptor file. 2. It must not contain any other *file* elements. 3. If additional files exist in the directory containing the learning application resource's descriptor file, or any of its subdirectories, the resource must contain a *dependency* element that references the resource of type "associatedcontent" which contains the references to these files. 4. It must not contain any other *dependency* elements of type "associatedcontent". 5. It may contain any number of *dependency* elements that reference resources of type "webcontent".
Learning Management System	A Learning Management System (LMS) is a computer application that enables the assignment of content to learners, learning, and the reporting of learning outcomes. This is used interchangeably with Course Management System, Managed Learning Environment and a host of other terms.
Learning Module	An aggregate of content and/or application functionality that represents or is part of a learning activity.
Target System	A Learning Management System (LMS) or similar system into which a package is to be imported.
webcontent	The standard resource type for content packages. Static web resource that is generally supported on the web such as HTML files, GIF images, JPEG images, PDF documents, etc. Resources of the type "webcontent" may reference any number of *files*. Additionally, "webcontent" resources may include *dependencies* on other "webcontent" resources. A resource of the type "webcontent" must comply with the following restrictions: 1. It may contain a *file* element for any file that exists in the package so long as the file is not in a learning application resource directory or a subdirectory of any learning application resource directory. 2. It may contain *dependency* elements that reference any other resources of type "webcontent". It must not contain any *dependency* elements to resources whose type is **not** "webcontent".

2. Use Cases

2.1 Use Case Scope

2.1.1 Affected Roles and Definitions

Table 2.1 Common Cartridge User Roles.

Role	Definition
Student	LMS Learner
Instructor	LMS Faculty member leading the course/learning activity. Includes Teaching Assistants or equivalent where applicable.
Instructional Designer	LMS course/program designer responsible for creating and maintaining online learning materials/content. Often, the same person has Instructor role.
Administrator	LMS course, program, group administrator with ownership and privileges to access and maintain administrative elements of the LMS within a particular context.
LMS	Learning Management System (LMS)—as defined in Glossary.

2.1.2 High-level Use Case Scope

The following diagram summarizes the use cases considered for the framework:

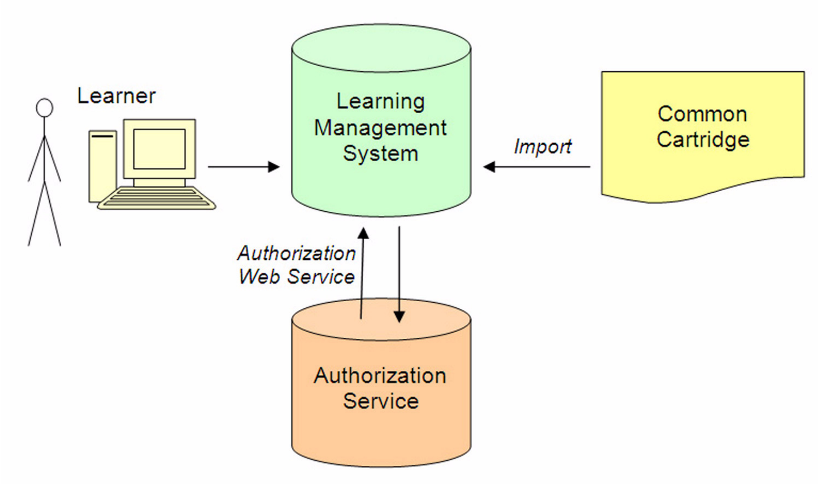


Figure 2.1 Learner Use and Authorization.

2.2 Authorization

Use Case 2	**Authorization**
Level	Summary
Primary Actor(s)	Student
Secondary Actor(s)	Instructor, LMS
Trigger	An actor requests a restricted interaction with the cartridge.
Preconditions	• Cartridge is successfully installed. • Cartridge defines one or more "restricted" items (e.g., view any cartridge material vs. view specific cartridge items). The specification must define authorization categories: "on import", "on package use", and "on item use". This use case is for "on package use". • Actor has not previously been authorized.
Success Post-conditions	• Actor is authorized for requested action, and the results of the authorization transaction potentially stored for future reference.
Failure Post-conditions	• Actor is not authorized for the requested action. • Cartridge material is not displayed.
Main Success Scenario	1. Learner navigates to LMS representation of course populated with Cartridge material. 2. LMS checks for record of previous Learner authorization. 3. If no record exists, LMS provides a prompt for entry of a simple access control token. The distribution of the tokens is out of scope for this specification. 4. LMS processes token, asserting the validity against an authorizing authority. The authorization algorithm is authorization server dependent and out of scope for this specification. The specification only defines "when" authorization is to occur, and at what level (package or for each "protected" item).
Variations	1.1 Learner navigates to a specific item that requires authorization, and is keyed to trigger "per item" authorization. 2.1 LMS evaluates any expiration rules for authorization that might be defined in the cartridge or stored with the authorization record.
Exception Conditions	• Learner-provided token is invalid. • Authorization cannot occur due to system errors (network communication to authorizing authority, etc.).

3. Architecture and Approach

Each common cartridge that implements the authorization service will contain both a cartridge ID and the URL of the Web Service to connect to for authorization. The cartridge will also specify whether authorization is required when importing the cartridge or only on student access. If authorization is required on student access, each resource that should be protected will have a flag indicating that it is protected content. The special case of all resources requiring authorization handles the current practice of requiring authorization of any student access to any content. Exactly where the required information is stored within the cartridge will be addressed as part of the common cartridge specification.

When the cartridge is imported into an LMS by either and instructor or administrator, the LMS checks for the existence of any authorization rules. If the rules indicate that authorization is required on import, the LMS prompts the user for an access code. The code, cartridge ID and URL of the LMS are then sent to the publisher’s web service which was also identified in the cartridge. The publisher’s web service performs any required validation and returns either a success code or a failure code with an error message. If a failure code is returned the import is aborted. If a success code is returned the import process continues.

If authorization rules indicate that one or more items should require authorization when accessed by students, the LMS configure these items during the import so that they honor that requirement. At a minimum this requires persisting the authorization information found in the package and associating that information with each of the protected resources. Subsequently, when a student attempts to access any of the protected items for the first time, he or she is prompted for an access code. The code is similarly validated against the publisher’s web service. The web service may either return a success code with an optional expiry date or a failure code with an error message. If a failure code is returned, the student is alerted and the content is not displayed. The student may then be allowed additional attempts to provide a valid access code. If a success code is returned, the LMS should store the fact that this user is authorized to access any of the protected resources that were imported from the cartridge and the originally requested resource should be displayed. Subsequently, when the student attempts to view the same resource or any of the other protected resources from the same package, the LMS should transparently confirm the user has been authorized take the student immediately to the requested resource so long as the authorization has not expired. If the previous authorization has since expired, the LMS should take the user through the same authorization process as before in order to obtain updated authorization information from the publisher’s web service.

The diagram in Figure 3.1 and communication flow outlined below are provided to help illustrate the process just described.

Cartridge Information
Each cartridge contains the following information

- Cartridge ID
- URL to Web Service for authorization

Web Service Communication Flow
LMS = Learning Management System
WS = Cartridge Protection Web Service

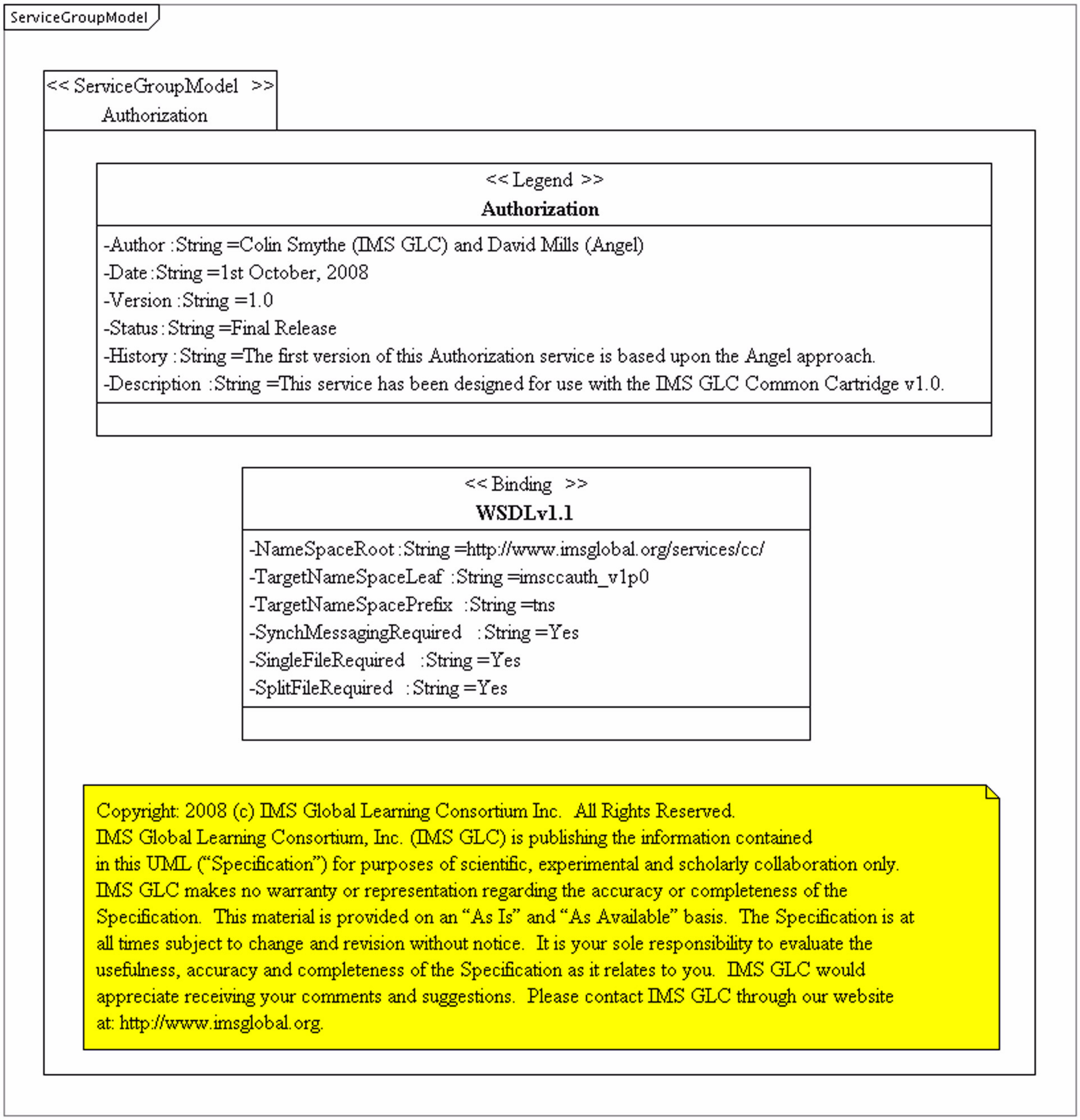
```
LMS:<auth:Validation xmlns:auth="http://www.imsglobal.org/xsd/imsccauth_ws_v1p0">
      <auth:ID>Cartridge ID</auth:ID>
      <auth:URL>The LMS’s URL</auth:URL>
   <auth:Validation>
WS:<auth:Validation>
      <auth:Show>License Agreement</auth:Show>
      <auth:Prompt>
         <auth:Message>Please enter key: </auth:Message>
         <auth:Name>Key</auth:Name>
         <auth:Type>Text</auth:Text>
      </auth:Prompt>
   </auth:Validation>
LMS:<auth:Validation>
      <auth:ID>Cartridge ID</auth:ID>
      <auth:URL>The LMS’s URL</auth:URL>
      <auth:Key> A Key </auth:Key>
   </auth:Validation>
   If Key is Valid
WS:   <auth:Validation>
         <auth:Release>
            <auth:Key>The Key passed by LMS</auth:Key>
            <auth:Exp>Expiration Date</auth:Exp>
</auth:Release>
</auth:Validation>

   If Key is Invalid
   WS:<auth:Validation>
         < auth:Invalid>
            <auth:Key> The Key </auth:Key>
            <auth:Message> A Message </auth:Message>
         </auth:Invalid>
      </auth:Validation>
```

Notes:

- LMS URL is sent for tracking purposes or only allowing Cartridges to be used at specific locations.
- Namespace http://www.imsglobal.org/xsd/imsccauth_ws_v1p0 added to uniquely identify common cartridge authentication.
- Validation\Release\Exp is optional.

4. Authorization Model



ServiceGroupModel

<< ServiceGroupModel >>
Authorization

<< Legend >>
Authorization

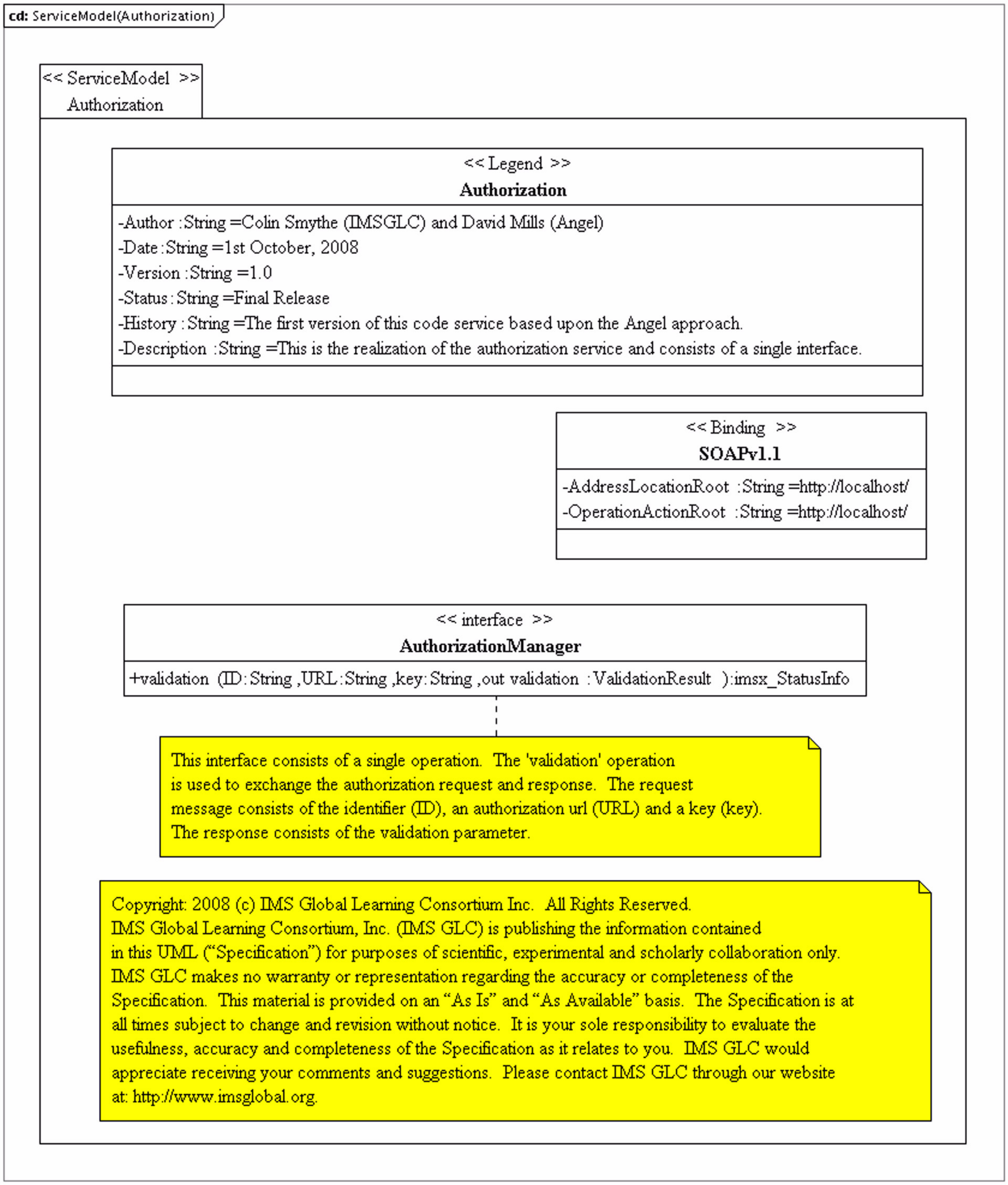
-Author :String =Colin Smythe (IMS GLC) and David Mills (Angel)
-Date :String =1st October, 2008
-Version :String =1.0
-Status : String =Final Release
-History : String =The first version of this Authorization service is based upon the Angel approach.
-Description :String =This service has been designed for use with the IMS GLC Common Cartridge v1.0.

<< Binding >>
WSDLv1.1

-NameSpaceRoot :String =http://www.imsglobal.org/services/cc/
-TargetNameSpaceLeaf :String =imsccauth_v1p0
-TargetNameSpacePrefix :String =tns
-SynchMessagingRequired :String =Yes
-SingleFileRequired :String =Yes
-SplitFileRequired :String =Yes

Copyright: 2008 (c) IMS Global Learning Consortium Inc. All Rights Reserved.
IMS Global Learning Consortium, Inc. (IMS GLC) is publishing the information contained in this UML ("Specification") for purposes of scientific, experimental and scholarly collaboration only. IMS GLC makes no warranty or representation regarding the accuracy or completeness of the Specification. This material is provided on an "As Is" and "As Available" basis. The Specification is at all times subject to change and revision without notice. It is your sole responsibility to evaluate the usefulness, accuracy and completeness of the Specification as it relates to you. IMS GLC would appreciate receiving your comments and suggestions. Please contact IMS GLC through our website at: http://www.imsglobal.org.

Figure 4.1 Service Group Model.



-Author :String =Colin Smythe (IMSGLC) and David Mills (Angel)
-Date :String =1st October, 2008
-Version :String =1.0
-Status : String =Final Release
-History : String =The first version of this code service based upon the Angel approach.
-Description :String =This is the realization of the authorization service and consists of a single interface.

-AddressLocationRoot :String =http://localhost/
-OperationActionRoot :String =http://localhost/

+validation (ID: String ,URL: String ,key: String ,out validation : ValidationResult):imsx_StatusInfo

This interface consists of a single operation. The 'validation' operation is used to exchange the authorization request and response. The request message consists of the identifier (ID), an authorization url (URL) and a key (key). The response consists of the validation parameter.

Copyright: 2008 (c) IMS Global Learning Consortium Inc. All Rights Reserved. IMS Global Learning Consortium, Inc. (IMS GLC) is publishing the information contained in this UML (“Specification”) for purposes of scientific, experimental and scholarly collaboration only. IMS GLC makes no warranty or representation regarding the accuracy or completeness of the Specification. This material is provided on an “As Is” and “As Available” basis. The Specification is at all times subject to change and revision without notice. It is your sole responsibility to evaluate the usefulness, accuracy and completeness of the Specification as it relates to you. IMS GLC would appreciate receiving your comments and suggestions. Please contact IMS GLC through our website at: http://www.imsglobal.org.

Figure 4.2 Service Model (Code Service).

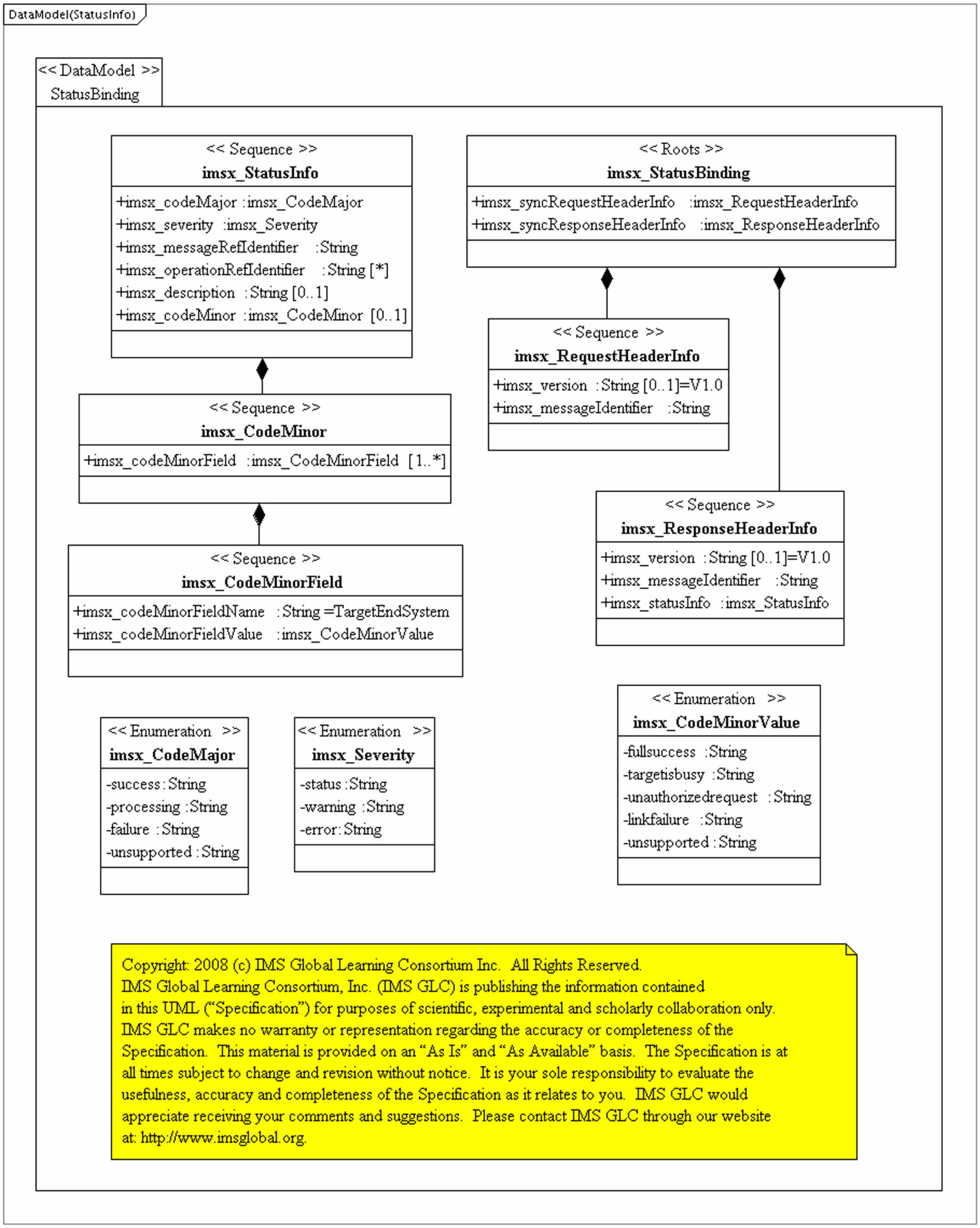
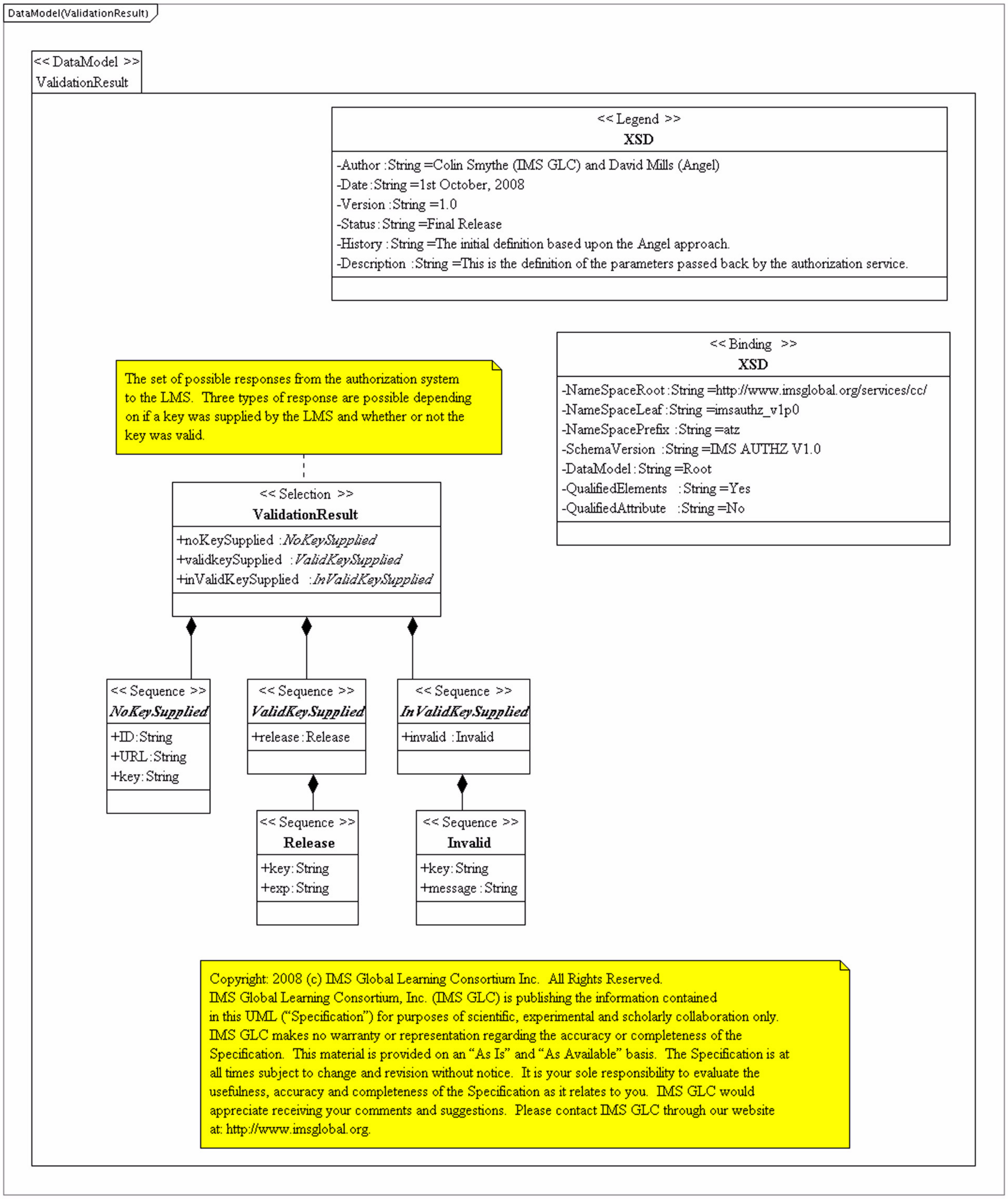

DataModel(StatusInfo)
<< DataModel >>
StatusBinding
<< Sequence >>
imsx_StatusInfo
+imsx_codeMajor :imsx_CodeMajor
+imsx_severity :imsx_Severity
+imsx_messageRefIdentifier :String
+imsx_operationRefIdentifier :String [*]
+imsx_description :String [0..1]
+imsx_codeMinor :imsx_CodeMinor [0..1]
<< Roots >>
imsx_StatusBinding
+imsx_syncRequestHeaderInfo :imsx_RequestHeaderInfo
+imsx_syncResponseHeaderInfo :imsx_ResponseHeaderInfo
<< Sequence >>
imsx_RequestHeaderInfo
+imsx_version :String [0..1]=V1.0
+imsx_messageIdentifier :String
<< Sequence >>
imsx_CodeMinor
+imsx_codeMinorField :imsx_CodeMinorField [1..*]
<< Sequence >>
imsx_ResponseHeaderInfo
+imsx_version :String [0..1]=V1.0
+imsx_messageIdentifier :String
+imsx_statusInfo :imsx_StatusInfo
<< Sequence >>
imsx_CodeMinorField
+imsx_codeMinorFieldName :String =TargetEndSystem
+imsx_codeMinorFieldValue :imsx_CodeMinorValue
<< Enumeration >>
imsx_CodeMinorValue
-fullsuccess :String
-targetisbusy :String
-unauthorizedrequest :String
-linkfailure :String
-unsupported :String
<< Enumeration >>
imsx_CodeMajor
-success :String
-processing :String
-failure :String
-unsupported :String
<< Enumeration >>
imsx_Severity
-status :String
-warning :String
-error:String

Figure 4.3 Data Model (Status Info).


DataModel(ValidationResult)
<< DataModel >>
ValidationResult
<< Legend >>
XSD
-Author :String =Colin Smythe (IMS GLC) and David Mills (Angel)
-Date :String =1st October, 2008
-Version :String =1.0
-Status :String =Final Release
-History :String =The initial definition based upon the Angel approach.
-Description :String =This is the definition of the parameters passed back by the authorization service.
<< Binding >>
XSD
-NameSpaceRoot :String =http://www.imsglobal.org/services/cc/
-NameSpaceLeaf :String =imsauthz_v1p0
-NameSpacePrefix :String =atz
-SchemaVersion :String =IMS AUTHZ V1.0
-DataModel :String =Root
-QualifiedElements :String =Yes
-QualifiedAttribute :String =No
<< Selection >>
ValidationResult
+noKeySupplied :NoKeySupplied
+validkeySupplied :ValidKeySupplied
+inValidKeySupplied :InValidKeySupplied
<< Sequence >>
NoKeySupplied
+ID:String
+URL:String
+key:String
<< Sequence >>
ValidKeySupplied
+release:Release
<< Sequence >>
InValidKeySupplied
+invalid :Invalid
<< Sequence >>
Release
+key:String
+exp:String
<< Sequence >>
Invalid
+key:String
+message:String

The set of possible responses from the authorization system to the LMS. Three types of response are possible depending on if a key was supplied by the LMS and whether or not the key was valid.

Figure 4.4 Data Model Validation Result.

5. Implementation Guidelines and Best Practices

5.1 General Best Practices

The CC Authorization service is intended to provide an alternative to existing proprietary models for controlling access to content via an access code redemption model. Full implementation of the CC Authorization service is not a requirement for Common Cartridge conformance. However, all systems must at least respect the implied restrictions placed on content as indicated by the CC Authorization meta-data that may exist in a cartridge. If a system that does not implement the CC Authorization service encounters a common cartridge that includes CC Authorization meta-data, the system must not import the cartridge. Instead the system should abort the import of the cartridge with an indication of the reason provided through an appropriate mechanism. If the import operation is interactive, a message should be displayed directly to the user. If the import operation is a batch or automated process, notification should be logged with any audit data provided.

In addition to the standard CC Authorization service, cartridge creators may optionally include additional information required for one or more proprietary authorization models.

However, any cartridge that includes a proprietary authorization model, must also include the standard CC Authorization model. The standard CC Authorization service must be fully implemented for the package to be considered conformant. This model should allow publishers to create a single protected cartridge that can be consumed both by new systems based on the specification and more easily work with other systems existing protection systems.

If additional proprietary authorization models are provided in a package, it is a best practice that all such authorization models validate using the same access codes interchangeably. This will significantly reduce end user confusion and associated support cost.

The CC Authorization service may be used to protect a cartridge in any one of thee ways. First, the service can be used ensure that only a user with an appropriate access code can import the cartridge into the system. This method places no restrictions on the content once it has been successfully imported. It can only be used to block the initial import of the content into a system.

The second protection model checks for authorization when any user accesses any of the content imported from the cartridge. This model is the most closely aligned to traditional authorization models implemented in most LMS systems. If all of the content in the cartridge is intended to be protected, this is the recommended model to use.

The third protection model allows mixing of protected and unprotected resources in a single package. In many cases publishers have a mix of premium and standard content associated with a text book. To make the subset of basic content available in an unprotected cartridge, publishers had to create two separate cartridges. With CC Authorization it is now possible to include both standard and premium content in a single cartridge, but require authorization only for the premium items. In this model, the authorization service meta-data is included once in the cartridge and each protected resource includes an attribute that signifies it should be protected. This model provides the most flexibility, but should only be used if there is actually a mix of protected and unprotected resources.

5.2 Future Development

No further development of the IMS Common Cartridge Authorization Web Service is as yet envisaged.

6. Conformance

6.1 Platforms and Tools

6.1.1 CC Compliance

Only platforms and tools which:

- Meet the conformance requirements identified in the CC specification [CC, 08a] and
- Fully implement the CC Authorization service

can claim CC compliance.

6.1.2 CC Lite Compliance

Full implementation of the CC Authorization service is not a requirement for ‘CC lite’ compliance. However, only platforms and tools which meet the conformance requirements identified in the CC specification [CC, 08a] and which either:

- Routinely deny import of protected cartridges and deny any access to protected content, or
- Are able to process the additional proprietary authorization information included in a cartridge

can claim ‘CC lite’ compliance. It should be noted that systems which only support proprietary authorization will not be able to run cartridges which only include the open CC Authorization meta-data, hence their designation as being ‘CC lite’ compliant.

All systems must at least respect the implied restrictions placed on content as indicated by the CC Authorization meta-data that may exist in a cartridge. If a system that does not implement the CC Authorization service encounters a common cartridge that includes CC Authorization meta-data, the system must not import the cartridge. Instead the system should abort the import of the cartridge with an indication of the reason provided through an appropriate mechanism. If the import operation is interactive, a message should be displayed directly to the user. If the import operation is a batch or automated process, notification should be logged with any audit data provided.

The CC Authorization service is intended to provide an alternative to existing proprietary models for controlling access to content via an access code redemption model. However, the Common Cartridge specification also allows the inclusion of additional proprietary authorization information so that proprietary authorization models may be implemented alongside the standard CC Authorization model.

6.2 Cartridges

6.2.1 Unprotected Cartridges

Use of CC Authorization for content protection is entirely optional for publishers and content providers. Therefore unprotected cartridges which meet the conformance requirements identified in the CC specification [CC, 08] can claim CC compliance.

6.2.2 Protected Cartridges

In addition to meeting the conformance requirements identified in the CC specification [CC, 08], protected cartridges must meet the following requirements in order to achieve CC compliance:

- Protected cartridges must include the standard CC Authorization meta-data. Optionally, they may also include proprietary authorization meta-data.
- The web service indicated in the standard CC Authorization meta-data must be a fully functioning standard CC Authorization web service.

- A user with a valid license must be able to obtain permission to access the protected resources in a cartridge by passing a valid access code to the standard CC Authorization web service (i.e. the referenced standard CC Authorization service may not be used simply to block access in the non-proprietary use case).

Appendix A – WSDL

The schema for the Common Cartridge authorization web service is located at:
http://www.imsglobal.org/services/cc/wsdl/AuthorizationSyncSingle.wsdl

About This Document

Title	IMS Common Cartridge Authorization Web Service
Editors	Kevin Riley, David Mills
Co-Leads	Erik Unjhem, David Mills
Version	v1.0
Version Date	1 October 2008
Status	Final Specification v1.0
Summary	This document contains the authorization web service for Common Cartridge, an open format for the distribution of rich, web-based content.
Revision Information	16 July 2008
Purpose	This document has been approved by the IMS Technical Advisory Board and is made available for pubic adoption.
Document Location	http://www.imsglobal.org/cc/index.html

List of Contributors

The following individuals contributed to the development of this document:

Name	Organization	Name	Organization
Adam Cooper	JISC	Kellan Wampler	ANGEL Learning
Alan Aikens	Pearson Education	Kevin Riley (editor)	IMS Global Learning Consortium
Anthony Whyte	University of Michigan	Kim Cetrone	Pearson Education
Bob Alcorn	Blackboard Inc.	Lou Mersereau	Pearson Central Media Group
Brent Bailey	Elsevier	Mark Norton	University of Michigan
Brian Cepuran	Desire2Learn	Martin Bayly	Blackboard Inc.WebCT
Chris Darroch	Pearson Central Media Group	Mike Farnesi (co-chair)	Pearson Education
Chris Chung	Harcourt	Mike Jones	Cengage
Chris Moffatt	Microsoft Inc.	Mladen Maljkovic	Pearson Education
Chris Vento (co-chair)	WebCT Blackboard Inc.	Nilesh Shinde	LearningMate
Christian Kaefer	McGraw-Hill Education	Paul Lewis	Horizon Wimba
Chuck Severance	University of Michigan	Prasad Mohare	LearningMate
Colin Smythe	IMS Global Learning Consortium	Sarah Currier	Intrallect Ltd
Dan Rinn	Cengage	Scott Criswell	McGraw-Hill
Dave Dusthimer	Cisco	Stefan Gerstmann	Digital Spirit
David Mills (co-chair)	ANGEL Learning	Stuart Sim	Moodle
Erik Unhjem (co-chair)	Pearson Education	Tom Grega	Cengage

Name	Organization	Name	Organization
Ingo Dahn	University of Koblenz-Landau	Warwick Bailey	Icodeon
Jan Posten Day	Blackboard Inc.	Wilbert Kraan	JISC
Jeff Bradley	Blackboard Inc.	Yong-Sang Cho	KERIS

Revision History

Version No.	Release Date	Comments
Base Document 1.0	6 April 2006	The internal project group draft of the specification.
CM/DN Draft 1.0	19 March 2007	The CM/DN Draft of the specification.
Public Draft Specification 1.0	22 July 2008	The Public Draft of the CC v1.0 specification.
Final Specification 1.0	1 October 2008	The first formal version of the CC v1.0 specification.

IMS Global Learning Consortium, Inc. ("IMS GLC") is publishing the information contained in this IMS Common Cartridge Authorization Web Service *("Specification") for purposes of scientific, experimental, and scholarly collaboration only.*

IMS GLC makes no warranty or representation regarding the accuracy or completeness of the Specification.

This material is provided on an "As Is" and "As Available" basis.

The Specification is at all times subject to change and revision without notice.

It is your sole responsibility to evaluate the usefulness, accuracy, and completeness of the Specification as it relates to you.

IMS GLC would appreciate receiving your comments and suggestions.

Please contact IMS GLC through our website at http://www.imsglobal.org

Please refer to Document Name: IMS Common Cartridge Authorization Web Service

Date: 1 October 2008