Categorization Based Content Screening Framework Requirements

Candidate Version 1.0 – 14 Oct 2008

Open Mobile Alliance
OMA-RD-CBCS-V1_0-20081014-C

Contents

Figures

Tables

1. Scope (Informative)

The Categorization Based Content Screening (CBCS) Enabler specifies the interfaces between actors so as to apply Content Screening to content based on content categorization and Screening Rules.

The CBCS Enabler shall be applicable to any content delivery Enabler or protocol and intentionally does not restrict the definition of "content", which allows the Enabler to apply Content Screening to practically any information communicated by/to a User.

The following functions are considered to be in scope for the CBCS Enabler specification:

- Blocking of any kind of content considered "undesirable" for a certain CBCS User according to the Screening Criteria used, including illegal content, unsolicited content, malicious content and inappropriate content.
- Customer-facing warnings: these are words or symbols that are actually part of the content presented to CBCS Users such as a symbol in the corner of the screen, an announcement before a programme starts or a form of words on screen.
- Screening of previously categorized content: in this case the Content Category is defined by content meta-data that is either encoded as part of the content format, or can be requested from an external source.
- Screening of not previously categorized content.
- Screening of content from Content Providers with whom the CBCS Service Provider has a trusted relationship, and of content from Content Providers with whom the CBCS Service Provider does not have a trusted relationship.
- Screening of content sent from a Content Provider to a CBCS User, from a CBCS User to another User, or from a CBCS User to a server (including the screening of subscriptions to content and screening of service requests)

The following items have been considered to be out of scope for the CBCS Enabler specification:

- The definition or standardization of specific content categorization schemes.
- The definition or standarization of the rules used to categorize content.
- The mechanisms by which the Content Screening Authority can communicate Screening Rules to the CBCS Service Provider
- The specification or standardization of specific Screening Criteria.
- The specification or standardization of algorithms or methods for the syntactic or semantic analysis of content.
- Deployment policies for CBCS Service Providers, including which categorization schemes to apply and how, how to define permissions for CBCS Subscribers and CBCS Users, etc.

2. References

2.1 Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

2.2 Informative References

[OMA-DICT] "Dictionary for OMA Specifications", Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7 URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

For the purpose of the present requirements document, the terms and definitions in [OMA-DICT] and the following apply:

Authorized Principal	A Principal (see [OMA-DICT]) with permissions to perform specific action(s) or receive specific information
Categorization Based Content Screening Service Provider	The Service Provider (see [OMA-DICT]) that deploys the CBCS Enabler
External Service Provider	A Service Provider (see [OMA-DICT]) that is connected to the CBCS Service Provider by an external interface. The CBCS Enabler does not define the detailed functionality offered by the External Service Provider
Categorization Based Content Screening Subscriber	The entity (e.g. a User) engaged in a subscription with a Categorization Based Content Screening Service Provider
Categorization Based Content Screening User	A Principal whose receivable or transmitted Content is subject to a CBCS Enabler implementation.
Categorization Based Content Screening User Profile	The User Profile (see [OMA-DICT]) applicable to the CBCS Enabler
Categorized Content	Content for which one or more Content Categories have been assigned
Content Categorization Entity	The entity that assigns Content Categories to content.
Content Category	A category assigned to content, aiming to describe the characteristics of the content
Content Provider	The entity making content available to the Categorization Based Content Screening User
Content Scanning	The act of determining the Content Category (or Content Categories) of the content
Content Screening	The act of blocking, allowing or amending content
Content Screening Authority	An entity which defines Content Categories and/or Screening Rules. The CBCS Enabler does not define the detailed functionality offered by the Content Screening Authority
External Service Provider	A Service Provider (see [OMA-DICT]) that is connected to the CBCS Service Provider by an external interface. The CBCS Enabler does not define the detailed functionality offered by the External Service Provider
Non-Categorized Content	Content for which no Content Category has been assigned
Pre-Categorized Content	Categorized Content which includes its Content Category and the Content Provider’s identity
Screening Action	A Policy Action (see [OMA-DICT]) applicable to the CBCS Enabler
Screening Criteria	Policy Conditions (see [OMA-DICT]) applicable to the CBCS Enabler
Screening Rule	A Policy Rule (see [OMA-DICT]) that uses Screening Criteria and Screening Actions

3.3 Abbreviations

For the purpose of the present requirements document, the abbreviations in [OMA-DICT] and the following apply:

CBCS	Categorization Based Content Screening
HTML	Hyper Text Markup Language
IM	Instant Messaging
IR	Infra Red
MMS	Multimedia Messaging Service
SMS	Short Message Service
URI	Uniform Resource Identifier
WAP	Wireless Application Protocol

4. Introduction (Informative)

As the multimedia capabilities of mobile terminals improve, an increasing number of content services become available to mobile Subscribers. As a consequence, the mobile User's access to illegal, undesired or malicious content also increases. As mobile devices have become widespread among all parts of the population, this creates a new challenge of protecting Subscribers, for example minors, from inappropriate content.

The objective of the Categorization Based Content Screening (CBCS) Enabler is apply Content Screening before delivering content to the mobile User, using content categorization. A Content Category qualifies the type of content, according to a categorization scheme. Such schemes are already in existence, and can come both from public administrations and from industry groups. The CBCS Enabler can obtain the Content Category for a given piece of content from a Categorization Entity.The CBCS Enabler also relies on the CBCS User Profile for resolving its Screening Rules. The CBCS Enabler can maintain its own CBCS User Profile, or it can request User Profiles from other Service Providers. It can also use a combination of both.

The CBCS Enabler allows any Authorized Principal to create and manage Screening Rules and User Profiles, according to the deployment scheme of the CBCS Service Provider. A typical deployment scheme, for example to achieve parental control, is for the CBCS Subscriber to manage the Screening Rules and CBCS User Profiles for one or more CBCS Users. An alternative deployment scheme would allow the CBCS User itself to manage all or part of his or her own Screening Rules and CBCS User Profile. The CBCS Service Provider can even apply Screening Rules that overrule any Screening Rules set by individual Subscribers or Users, for example if the authorities require this for certain types of content. How these authorities communicate their Screening Rules to the CBCS Service Provider is outside the scope of the CBCS Enabler; for example, the CBCS Service Provider could translate legal requirements into corresponding Screening Rules. The informative figure 2 in appendix B.1 illustrates the CBCS actors and their relationships.

To screen the content, the CBCS Enabler applies Screening Rules, consisting of Screening Criteria and Screening Actions. Screening Criteria are conditions used in Content Screening, typically including the Content Category, User Profile, and possibly other parameters such as the sender of the content. Screening Actions determine what to do with the content if the condition is true, and can include decisions like "pass", "block", "pass but delete URIs to offensive content", "ask for parental permission first", or "pass and warn".

The requirements for the CBCS Enabler have been specified so as to enable the greatest possible array of implementation, deployment and usage scenarios. They allow the CBCS Enabler to be deployed in the network, on the device, or on both, and also allow the Enabler to be applied to roaming CBCS Users.

5. Use Cases (Informative)

5.1 General Content Screening

This use case describes how the CBCS Enabler filters content over multiple content delivery Enablers or protocols.

5.1.1 Short Description

Suppose the CBCS Subscriber has set Screening Rules appropriate for the Users managed by this Subscriber (e.g. parental control). The Subscriber now wishes to see Screening Rules uniformly applied to all delivery mechanisms (e.g. SMS, MMS, Push, IM). If content is blocked by the CBCS Enabler it will be replaced with a message explaining why the content could not be presented and whom to contact in case the User questions the appropriateness of the screening result. Results of the screening tests could be available offline for a certain period of time (e.g. the screened contents or statistics); a User can be notified periodically of the screening results.

5.1.2 Actors

The actors involved in this use case are the CBCS Service Provider, the CBCS Subscriber, the Content Categorization Entity and the CBCS User. The following subsections describe the specific issues and benefits for these actors.

5.1.2.1 Actor Specific Issues

- The CBCS Service Provider must be able to apply Content Screening to content communicated over multiple content delivery Enablers or protocols in a consistent way, yielding the same screening results regardless of the content delivery Enabler or protocol used.
- The CBCS Subscriber can securily assign Users to the CBCS Enabler and define Screening Rules for them.
- The CBCS User receives content that has been screened previously by the CBCS Enabler, on the basis of the Screening Rules defined by the CBCS Subscriber. In case content is blocked, the User may be informed through replacement of the content. The information accompanying a rejection notice could include an override or the rationale for rejection and explanation of steps the User could take if the User feels the content should not have been rejected.

5.1.2.2 Actor Specific Benefits

- The CBCS Service Provider can differentiate its service offer from other Service Providers, and can appeal to certain classes of customers, for example parents concerned about the content their children consume. In certain administrations there may be regulatory requirements that oblige a Service Provider to apply Content Screening.
- The CBCS Subscriber will have screening uniformly applied over different content delivery mechanisms. The Content Screening rigour would conform to the Screening Rules of the regulator, corporation or family.
- The CBCS User is not exposed to content that does not conform to the Screening Rules set by the CBCS Subscriber.

5.1.3 Pre-conditions

- The CBCS Service Provider uses one or more content categorization schemes that respect the Screening Rules set by the Content Screening Authority. The CBCS Service Provider may have trusted relationships with one or more Content Providers and/or Content Screening Entities.
- The CBCS Subscriber has previously assigned Users to the CBCS Enabler and has defined Screening Rules for these Users.

5.1.4 Post-conditions

- Regardless of the content delivery Enabler or protocol used, the CBCS User does not receive any content that should be blocked according to the Screening Rules defined by the CBCS Subscriber.
- Screening results may be available offline for a certain period of time (e.g. the screened contents or statistics).

5.1.5 Normal Flow

1. The Content Provider attempts to deliver content to the CBCS User via any content delivery mechanism.
2. The CBCS Enabler retrieves one or more categories for the content from one or more Content Categorization Entities.
3. The CBCS Enabler screens the content according to the Screening Rules previously defined for this User by the CBCS Subscriber.
4. Content that is not blocked will be delivered to the User using the original delivery Enabler or protocol (the one that the Content Provider used to deliver the content to the User). The CBCS User and/or CBCS Service Provider may be notified periodically of the screening results.

5.1.6 Alternative Flow

If content is blocked in step 3, then an explanatory message may be sent to the CBCS Subscriber or CBCS User.

5.1.7 Operational and Quality of Experience Requirements

If a CBCS Subscriber modifies the Screening Rules for a User, then the updated Screening Rules shall apply instantly to all content delivery mechanisms.

5.2 Content screening in a browsing session

This use case shows how content is screened by the CBCS Enabler in a mobile browsing session.

5.2.1 Short Description

Ben is a User of mobile information services. He wants to browse the web with his mobile phone. The browser will not display certain hyperlinked services, due to the Screening Rules the Subscriber of the mobile subscription being used by Ben has set (the Subscriber can be Ben himself, but can also be another person or entity). The blocked hyperlinks can include access to content (images, videos, text, audio, etc), or other services (send a form, vote, etc). The Subscriber may set the Screening Rules such that content is only partially blocked, e.g. the browser displays HTML text but not images, or shows an e-mail but without attachments.

5.2.2 Actors

The actors involved in this use case are the CBCS Service Provider, the CBCS Subscriber, the Content Categorization Entity and the CBCS User. The following subsections describe the specific issues and benefits for these actors.

5.2.2.1 Actor Specific Issues

- The CBCS Subscriber assigns Users to the CBCS Enabler, applies desired Screening Rules per User, and identifies the content delivery Enablers or protocols that the screening needs to apply to.
- The CBCS User receives content that has been screened by the CBCS Enabler, on the basis of the Screening Rules defined by the CBCS Subscriber. In case content is blocked, the User may be informed through replacement of the content.
- The CBCS Service Provider uses the The CBCS Enabler to apply Content Screening (to web pages, referenced services and media) accessed through browsing, using the Screening Rules defined by the CBCS Subscriber.
- Content Categorization Entity categorizes the content that is accessible through browsing (pictures, text, video, audio, etc.).

5.2.2.2 Actor Specific Benefits

- The CBCS User is not exposed to content that does not conform to the Screening Rules set by the CBCS Subscriber.

- The CBCS Service Provider will benefit from a higher use of the browsing services due to increased Subscriber confidence in the service.

5.2.3 Pre-conditions

- The CBCS User has a mobile device and subscription that support browsing.
- The CBCS Subscriber has previously assigned Users to the CBCS Enabler and has defined Screening Rules for these Users.
- The CBCS Service Provider applies the Screening Rules defined by the CBCS Subscriber, respecting the rules defined by the Content Screening Authority.
- The Content Categorization Entity may or may not have previously categorized content accessible through browsing.

5.2.4 Post-conditions

- The CBCS User cannot access through browsing any content that should be blocked according to the Screening Rules defined by the CBCS Subscriber.
- Screening results may be available offline for a certain period of time (e.g. the screened contents or statistics).

5.2.5 Normal Flow

1. Ben (the CBCS User) begins to browse with his mobile device and requests a web page from a Content Provider.
2. The CBCS Enabler retrieves categorization information for the page requested by Ben and its components (e.g, images) from one or more Categorization Entities. If these Categorization Entities do not provide a categorization, the CBCS Enabler may refer to a local "built-in" Categorization Entity that attempts to analyze and categorize the content on the fly.
3. The CBCS Enabler makes a decision to block or pass the requested content by applying the Screening Rules defined by the CBCS Subscriber to the categorization information obtained in step 2 (if any). If the content was not categorized in step 2, or if the Screening Rules don't produce a decision, or if conflicting Content Categorization Information was received, the CBCS Enabler will take a default action (block or pass). In this case, the CBCS Enabler may inform the CBCS User that the content he is about to receive may be not suitable for him regarding his CBCS User Profile.
4. If the requested page passes, it is delivered to Ben's browser. If it is blocked, another page may be delivered to the browser, informing the User of the blocking action.

5.2.6 Alternative Flow

As HTML (or WAP) pages typically consist of several components (text, images, hyperlinks, forms, javascript, etc), the CBCS Enabler may screen each component individually. In this case, steps 2 and 3 are applied to each component separately, and in step 4, Ben may be presented with a partially complete page, from which certain components have been blocked or replaced.

Among the page components that the CBCS Enabler can block are hyperlinks that point to content that should be blocked according to the Screening Rules used.

5.2.7 Operational and Quality of Experience Requirements

N/A

5.3 Screening of messages

This use case describes the screening of the messages.

5.3.1 Short Description

A User is trying to send content which is considered undesirable for the receiving User. The CBCS Enabler screens the content in incoming messages, thus avoiding that undesirable content reaches the User via a message.

5.3.2 Actors

The actors involved in this use case are the CBCS Service Provider, the CBCS Subscriber, the Content Categorization Entity and the CBCS User.

In addition, the Sender is the entity sending a message to a CBCS User. The Sender is not necessarily a mobile Subscriber, but could also be on the Internet, for example.

The following subsections describe the specific issues and benefits for these actors.

5.3.2.1 Actor specific issues

- The CBCS User receives messages from other Users that have not been blocked by the CBCS Enabler. The CBCS User may or may not receive information about messages that were screened and blocked by the CBCS Enabler.
- The CBCS Subscriber determines whether messages should be screened and if so, using what Screening Rules.
- The Sender may or may not be informed that his/her messages are being blocked by the CBCS Enabler.

5.3.2.2 Actor specific Benefits

- The CBCS User is protected from undesired content sent via messaging.
- The CBCS Subscriber can protect its Users from undesired content sent via messaging.

5.3.3 Pre-conditions

- The CBCS Subscriber has instructed the CBCS Service Provider to apply Content Screening to incoming messages for its Users.
- The CBCS Subscriber has previously defined Screening Rules for blocking content addressed to its Users. These Screening Rules include how to deal with incoming messages.

5.3.4 Post-conditions

- Through messaging the CBCS User will not receive any content that should be blocked according to the Screening Rules defined by the CBCS Subscriber.

5.3.5 Normal flow

1. The Sender sends a message to CBCS User, with attached content (for example a picture or video).
2. Before delivering the message to the CBCS User, the CBCS Enabler may request categorization information about the message and its attachment from one or more Categorization Entities.
3. The CBCS Enabler screens the content using categorization information obtained from one or more Categorization Entities and the Screening Rules defined by the CBCS Subscriber. These Screening Rules may include messaging specific Screening Criteria such as origin of the message (white list or black list) or other messaging specific information (for example, subject, etc.).

4. If the content is considered undesirable according to the Screening Rules used in the decision, the message is not forwarded to the destination User. The CBCS Enabler may then inform the CBCS Subscriber, CBCS User and/or the sender of the Screening Action. Otherwise, the message is forwarded to the destination User.

5.3.6 Alternative Flow

N/A

5.3.7 Operational and Quality of Experience Requirements

N/A

5.4 External User Profile

This use case describes how the CBCS Enabler can retrieve the CBCS User Profile from an External Service Provider.

5.4.1 Short Description

A cellular network operator wishes for the CBCS Service Provider to be outside of the cellular operator's network, whilst maintaining the CBCS User Profile inside the cellular network operator's network. In this case, the cellular network operators acts as an External Service Provider to the CBCS Service Provider.

5.4.2 Actors

- The External Service Provider maintains the CBCS User Profile for each of its subscribers
- The CBCS Service Provider deploys and operates the CBCS Enabler.

5.4.2.1 Actor Specific Issues

- The CBCS Service Provider must be able to request the CBCS User Profile from the External Service Provider.
- The External Service Provider provides the CBCS User Profile to identify the type of content which an individual user is allowed to receive.
- The CBCS Service Provider screens content based on the content categorization and the received CBCS User Profile.

5.4.2.2 Actor Specific Benefits

- The network operator can subcontract the operation of the CBCS Service Provider to a third party, whilst maintaining the User Profile operation "in house".
- The CBCS Service Provider can focus on identifying content categorization whilst obtaining the CBCS User Profile from the External Service Provider.

5.4.3 Pre-conditions

- The External Service Provider maintains the CBCS User Profile for its subscribers.
- The External Service Provider and CBCS Service Provider are connected by an appropriate interface.

5.4.4 Post-conditions

- The CBCS User is not aware that the content is being screened by concerted activities between two different Service Provider actors.

5.4.5 Normal Flow

1. The Content Provider attempts to deliver content to the CBCS User via any content delivery mechanism.

2. The CBCS Service Provider requests the CBCS User Profile from the External Service Provider.
3. The CBCS Service Provider screens the content according to the CBCS User Profile obtained in Step 2.
4. Content that is not blocked will be delivered to the user using the original delivery Enabler or protocol (the one that the Content Provider used to deliver the content to the user). A user and/or Content Screening Authority can be notified periodically of the screening results.

5.4.6 Alternative Flow

If content is blocked in step 3, then an explanatory message may be sent to the CBCS Subscriber or CBCS User.

5.4.7 Operational and Quality of Experience Requirements

None.

5.5 Content scanning request

5.5.1 Short Description

Ben is an end-User and wants to request content form a web page using his mobile phone. He is subscribed to the CBCS Service. Ben requests the content he wants and the CBCS Enabler screens the requested content to check whether the content is appropriate for Ben. The CBCS Enabler decides that the content itself is suitable for the User and offers Ben (automatically or requesting, depending on the CBCS User Profile!) to have the content scanned to detect possible malicious software. Ben acknowledges the scan-request and after the successful scan, the CBCS Enabler delivers the scan-report to Ben. If malicious software was detected, Ben has the choice to isolate or delete the malicious software.

5.5.2 Actors

The actors involved in this use case are the CBCS Service Provider, the CBCS Subscriber and the CBCS User. The following subsections describe the specific issues and benefits for these actors.

5.5.2.1 Actor specific issues

- The CBCS User has the choice to decide whether the requested content will be scanned before delivery.
- The CBCS Service Provider has the capability to initiate content scanning for content requested by the CBCS User.
- The CBCS Subscriber decides whether content scanning is desired.

5.5.2.2 Actor specific Benefits

- The CBCS User is protected from content including malicious code or unsolicited messages.
- The CBCS Subscriber can protect its User from content including malicious code or unsolicited messages.
- The CBCS Service Provider has the capability to offer its Users protection from content includes malicious-software or the receiving of unsolicited-messages.

5.5.3 Pre-conditions

- Ben has a mobile phone that supports browsing.
- Ben is subscribed as a CBCS User.
- The CBCS User Profile contains the information that Ben wants to apply Content Scanning.
- The CBCS Enabler can have a database to store the scan-result, related with the content, in order to not have to analyze the same content again, coming from the same source.

5.5.4 Post-conditions

N/A

5.5.5 Normal flow

1. Ben makes a connection to the network operator, begins to browse and request content located on a web page via his mobile phone.
2. The CBCS Enabler determines that the content is suitable for the CBCS User based on the categorization retrieved from the Content Categorization Entity.
3. The CBCS Enabler offers the CBCS User to have the content scanned (e.g. for malicious code).
4. Ben acknowledges the scan-request and the CBCS Enabler has the content scanned.
5. The CBCS Enabler delivers the scan-result to the CBCS User
6. The scan-result includes the information whether the requested content is contaminated with malicious code or not. If the content is contaminated with malicious code, Ben decides whether the CBCS Enabler should isolate or delete the code. In the case where the content is "clean" (no contamination!) the CBCS Enabler delivers the content directly to the CBCS User without additional user interaction.

5.5.6 Alternative Flow

The CBCS User Profile can be set to enable the CBCS Enabler to have the content scanned automatically. Thus in step 3 and 4 the CBCS Enabler need not request User acknowledgment and the CBCS Enabler has the content scanned silently.

5.5.7 Operational and Quality of Experience Requirements

N/A

5.6 Content screening while User is roaming

5.6.1 Short Description

A User from a given network (called the Home network from now on) is visiting another network, this is, he is roaming in a Visited network. This User and/or his Subscriber has contracted CBCS in his Home network this is, the content he can receive is previously screened and/or blocked by the CBCS Enabler serving the Home network. As now he is accessing content through a Visited network, the requested content, prior to be delivered to the User has to be verified by the CBCS Enabler in the Home network and by the CBCS Enabler in the Visited network if existing. This way, the User only receives content that has the CBCS Enabler in his home network and the CBCS Enabler in the visiting network; so, for example, if the User is in another country, he could only receive content he is supposed to be allowed to receive in both countries (home and the visited).

5.6.2 Actors

The actors involved in this use case are the CBCS Service Provider, the CBCS Subscriber, the Content Categorization Entity and the CBCS User.

In addition, this use case considers a roaming scenario and makes the distinction between a CBCS User's Home Network and Visited Network.

The following subsections describe the specific issues and benefits for these actors.

5.6.2.1 Actor Specific Issues

- CBCS User is able to access a network different from the one of its operator, this is, the CBCS User is able to be roaming in a visited network.

- The content destined to the CBCS User will be screened using rules from its home network, this is its CBCS User Profile and the Screening Rules applied by the CBCS Service Provider in its Home network.
- CBCS Subscriber will be able of establishing and modifying the CBCS User Profile in its Home network.
- CBCS Service Provider must be able to decide what to do with the contents (web pages, referenced services and media) provided by the Content Provider. Different pieces of information (CBCS User Profile and additional Screening Criteria) can be used in the decision process.
- CBCS Service Provider must be able to communicate with other CBCS Service Providers and interchange information about how to apply the CBCS Enablerto a given CBCS User who is in roaming.
- Content Categorization Entity will be able to catalogue and sort the different web pages and contents (pictures, text, video, audio, etc.).

5.6.2.2 Actor Specific Benefits

- CBCS User. The User is not exposed to content that does not conform to the values or policies that are in effect since he has chosen the contents and services he/she does not want to access to even if he is roaming in a visited network.
- CBCS Service Provider will benefit from a higher use of the browsing services due to the confidence the Subscribers has on the service. Even Users in roaming can access services being sure about they are going to receive only appropriate content.

5.6.3 Pre-conditions

- The User has a mobile device that supports browsing.
- Requested content within the Content Provider may or may not have been previously categorized.
- There is a CBCS Enabler deployed in both the home network and visited network, and the CBCS Service Providers for these may be different entities.

5.6.4 Post-conditions

N/A

5.6.5 Normal Flow

1. The CBCS User is Subscriber of the Home network and is subscribed to CBCS.
2. The CBCS User tries to access contents and services through a roaming network (Visited network).
3. This Visited network also has its own CBCS Enabler (offered by a different CBCS Service Provider), which also uses Content Categorization Entities (the same or different from the ones used by the CBCS Service Provider in the Home network).
4. The CBCS User requests content.
5. Prior to delivery to the CBCS User, the content is screened by the CBCS Enabler in the Home network to assure that it is not harmful for the User according to the Screening Rules.
6. If the CBCS Enabler in the Home network considers the content suitable for the CBCS User, it is passed to the CBCS Enabler in the Visited network.
7. The CBCS Enabler in the Visited network screens the content to assure it is suitable to be delivered to the User according to the Screening Rules given by its Content Screening Authority.

8. If the content fails in any screening step, the content is not delivered to the CBCS User, who is informed of that circumstance. If the content passes the two CBCS Enablers, it is finally delivered to the CBCS User.

The following figure is given only for informational purposes and only tries to depict a general scenario. No implementation or architectural requirements or implications should be derived from this figure.

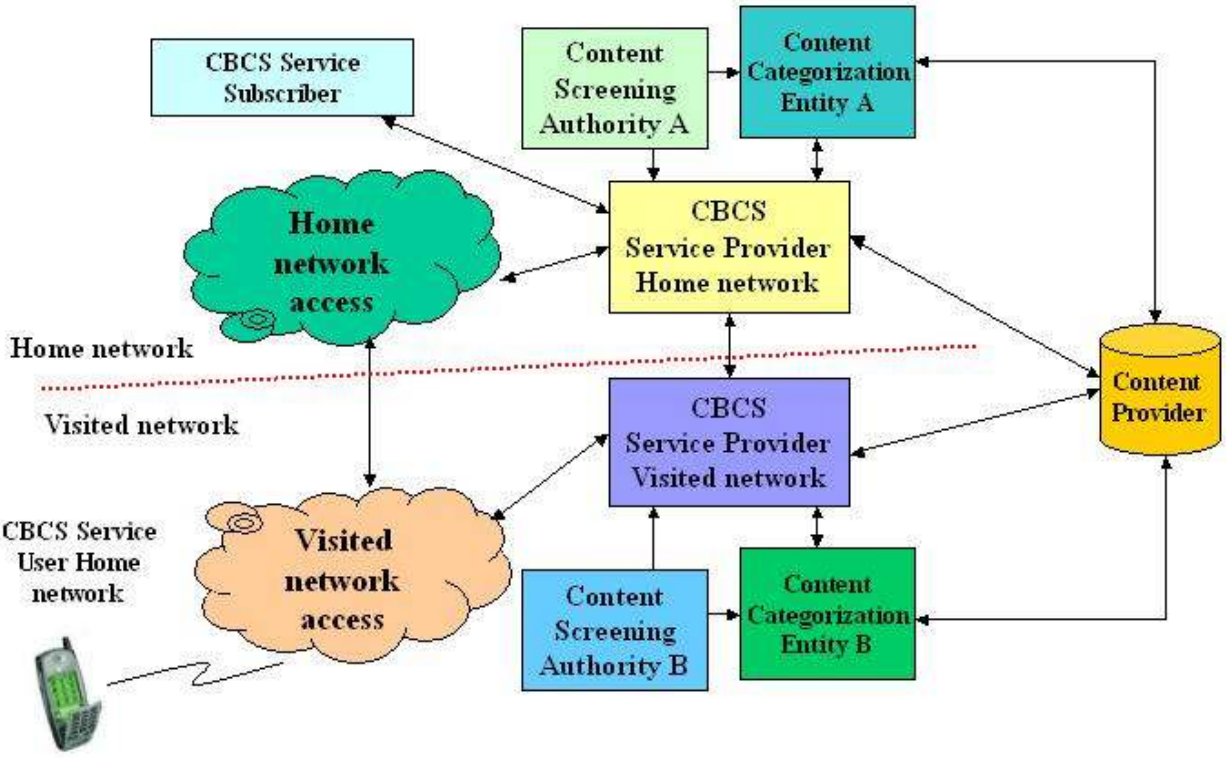

Figure 1: Roaming scenario

5.6.6 Alternative Flow

N/A

5.6.7 Operational and Quality of Experience Requirements

N/A

5.7 SMS to short number application

5.7.1 Short Description

A Content Provider is offering free content (for example, a ring tone) if the User sends a SMS with some key words to a specific short application number. The small print in the offering of the Content Provider says that doing so, the User also accepts he is going to periodically receive premium push content (content he has to pay for). The User is not aware of those conditions but he sends the SMS to the application. The User is a CBCS User so the message sent to an application goes through the CBCS Enabler who, using the CBCS User Profile (set by the CBCS Subscriber) and information regarding the

service decides that the message should not reach the application. The CBCS User is informed that the message is not delivered to the application.

5.7.2 Actors

The actors involved in this use case are the CBCS Service Provider, the Content Provider, the CBCS Subscriber, the Content Categorization Entity and the CBCS User. In this use case, the Content Provider provides content through a messaging shortcode application. The following subsections describe the specific issues and benefits for these actors.

5.7.2.1 Actor Specific Issues

- CBCS User has the ability to send a SMS to a shortcode application.
- CBCS Subscriber is able of establishing and modifying the CBCS User Profile.
- Content Provider is the entity that will receive the request (the SMS) from the CBCS User and provides premium rate content through messaging.
- CBCS Service Provider can screen SMS sent to short number applications and decide if the receiving application is adequate for the CBCS User or not.
- Content Categorization Entity is able to categorize the content offered through short number applications.

5.7.2.2 Actor Specific Benefits

- CBCS User will be protected from fraud applications delivering unsolicited premium push content he has to pay for.
- CBCS Service Provider can control short number applications offered by Content Providers so it (CBCS Service Provider) will benefit from offering a higher level of protection and a higher use of its services.

5.7.3 Pre-conditions

- The CBCS Subscriber has to contract any Network Operator to be able to access the web.
- The CBCS User Profile must be able of storing all the information about the User.
- The CBCS Enabler must be able to categorize contentservices offered through short number applications by different Content Providers.

5.7.4 Post-conditions

N/A

5.7.5 Normal Flow

1. The CBCS Subscriber sets the CBCS User Profile to not allow CBCS User to send messages with certain keywords to certain short codes.
2. The CBCS User sends a SMS to a short number application.
3. The CBCS Enabler detects the CBCS User has sent a SMS to a short number application so it has to check if he is allowed to do that.
4. The CBCS Enabler retrieves information from the Content Provider to determine some characteristics (type of content, periodicity, etc.) of the application serving the receiving short number. This information can be previously given by the Service/Content Provider to the CBCS Service (for example, during the deployment process of the application).
5. The CBCS Enabler finds that the application is offering premium push content to Users.

6. If the CBCS User Profile indicates the CBCS User is not allowed to send messages to this kind of services the SMS is not delivered to the short number application and the CBCS User is informed of that.
7. If the CBCS User Profile is not preventing from sending messages to this kind of service, the SMS is delivered to the short number application.

5.7.6 Alternative Flow

N/A

5.7.7 Operational and Quality of Experience Requirements

N/A

5.8 Reporting failed screening

This use case is about a CBCS User providing feedback to the CBCS Enabler about content that should have been blocked but wasn't (false positives), and content that was blocked but shouldn't have been (false negatives).

5.8.1 Short description

A CBCS User receives content that has been screened but not blocked by the CBCS Enabler.

The CBCS User perceives that the received content should have been blocked by the CBCS Enabler according to the CBCS Subscribers preferences and decides to report failure of screening.

The CBCS User utilizes a special feature of the content rendering component of the device (e.g., browser, MMS client, etc.) with which the User consumes the content in order to quickly and easily report the screening failure. Thereby, the device sends information to the CBCS Service Provider that allows the CBCS Service Provider to uniquely identify the content (e.g. checksum or some sort of fingerprint) and sender's identity (e.g., of the Content Provider or of an individual sending a message).

Optionally, the CBCS User can indicate (e.g., through an HTML form using the browser) which part of the Screening Rules have not correctly been taken into account. This could indicate seemingly wrong categorization of one or more categories.

The CBCS Service Provider acts upon the received report of failure for the given content and sender's identity. This step is not part of the requirements and open to the CBCS Service Provider deploying the Enabler.

5.8.2 Actors

The actors involved in this use case are the CBCS Service Provider, the CBCS Subscriber and the CBCS User. The following subsections describe the specific issues and benefits for these actors.

5.8.2.1 Actor specific issues

- The CBCS User will be able to provide feedback to the CBCS Service Provider about Screening Actions he or she considers inappropriate.
- The CBCS Service Provider will have to process this feedback to improve the effectiveness of the CBCS Enabler for a given CBCS User.

5.8.2.2 Actor specific benefits

- CBCS User will take part in a self-regulating content ecosystem and receive less spam or unwanted content.
- CBCS Service Provider can recognize small volume spam (from a single party to few recipients at a time).
- CBCS Service Provider can instruct their Categorization Entities about possible mis-categorization of content and help to improve the categorization mechanisms.

5.8.3 Pre-conditions

- The sender of the content can be reliably identified by the CBCS Service Provider.
- The device can send information to the CBCS Service Provider.
- Easy reporting of screening failure by the CBCS User requires a client side component of the CBCS Enabler.

5.8.4 Post-conditions

N/A

5.8.5 Normal flow

1. A CBCS User receives content that has been screened (but not blocked) by the CBCS Service Provider.
2. The CBCS User reports screening failure by sending information to the CBCS Service Provider that allows the CBCS Service Provider to uniquely identify the content and sender's identity.

5.8.6 Alternative flow

(Extends step 2 compared to Normal Flow)

2. The CBCS User reports screening failure by sending information to the CBCS Service Provider that allows the CBCS Service Provider to uniquely identify the content and sender's identity. Also, the CBCS User specifies which part of the Screening Rules have been violated (e.g., certain categories).

5.8.7 Operational and Quality of Experience Requirements

N/A

5.9 Online screening of local content

This use case is about a CBCS User receiving content on his/her device through transport mechanisms that cannot be intercepted by or on behalf of the CBCS Service Provider. One could think of content transfer through removable media or using short range networks such as Bluetooth or IR. Upon reception of the content on the device Content Screening would be requested and the result applied before the content could be used in any way by the User of the device.

5.9.1 Short description

A CBCS User receives content on his/her device that has not been screened yet by the CBCS Service Provider.

The received content (whether or not on a removable storage medium or within the device) is from now on referred to as local content in the context of this use case.

Content Screening is requested for the local content, either explicitely upon User request or initiated by (a CBCS client side component of) the device according to the CBCS Subscribers' preferences. The request contains a fingerprint of the content and other parameters useful for identifying the piece of content and its origin, possibly also indications of content categories set by the content issuer. Request to and response from the CBCS Enabler in the network is sent online and will possibly be delayed until network connectivity to the CBCS Enabler is available. The local content cannot be used in any way (played, stored, forwarded, etc.) until it is allowed as a result of the CBCS screening.

If the screening result is blocking of the content then the content will not be accessible for the Users of the device, otherwise it can be used normally. If the local content was stored temporarily in the internal (not removable) memory of the device then the content will be removed from the internal memory.

According to the CBCS Subscribers preferences (a CBCS client side component of) the device could be instructed to always block content that has not been screened by the network side component of the CBCS Enabler, without requesting online CBCS.

5.9.2 Actors

The actors involved in this use case are the CBCS Service Provider, the CBCS Subscriber, the Content Categorization Entity and the CBCS User.

The following subsections describe the specific issues and benefits for these actors.

5.9.2.1 Actor specific issues

N/A

5.9.2.2 Actor specific benefits

- CBCS User can benefit from CBCS even for content received through networks or mechanisms not controllable by the CBCS Service Provider.
- CBCS Subscriber can be sure that a CBCS User only consumes content that has passed CBCS screening. (Think of parents subscribing to CBCS for their kids' mobile phones).

5.9.3 Pre-conditions

- The device can send information to the CBCS Service Provider and receive information.

5.9.4 Post-conditions

N/A

5.9.5 Normal flow

1. A CBCS User receives content on his/her device that has not been screened yet by the CBCS Service Provider.
2. Content Screening is requested for the local content. The request contains a fingerprint of the content or the content itself and other parameters useful for identifying the piece of content and its origin, possibly also indications of content categories set by the content issuer. Request to and response from the CBCS Enabler in the network is sent online and possibly delayed until network connectivity to the CBCS Enabler is available. There are two options for the invocation of the CBCS Enabler:
    a. Explicitely upon User request, e.g. for content that the User considers as "suspicious"
    b. Forced by (a CBCS client side component of) the device
3. The local content cannot be used in any way (played, stored, forwarded, etc.) until allowed as a result of the CBCS screening.
4. The CBCS screening response is received by the device. If the screening result demands blocking of the content then the content will not be accessible for the User of the device, otherwise it can be used normally. If the local content was stored temporarily in the internal (not removable) memory of the device then the content will be removed from the internal memory.

5.9.6 Alternative flow

(Replaces steps 2 to 4 compared to Normal Flow)

2. The (CBCS client side component of the) device blocks all content that has been received through mechanisms that by-passed the CBCS Enabler in the network. No online CBCS screening is requested.

5.9.7 Operational and Quality of Experience Requirements

N/A

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
CBCS-FUNC-001	The CBCS Enabler MUST include the possibility to apply Content Screening on a per CBCS User basis.	CBCS V1.0
CBCS-FUNC-002	The CBCS Enabler MUST be able to retrieve categorization information from the Content Categorization Entity	CBCS V1.0
CBCS-FUNC-003	The CBCS Enabler MAY use information from multiple Content Categorization Entities.	CBCS V1.0
CBCS-FUNC-004	The CBCS Enabler SHALL be able to apply Content Screening if the categorization information from a Content Categorization Entity is missing.	CBCS V1.0
CBCS-FUNC-005	The CBCS Enabler SHALL be able to extract Content Categories and the Content Provider's identity from Pre-Categorized Content.	CBCS V1.0
CBCS-FUNC-006	The CBCS Enabler SHALL be able to verify the integrity of Pre-Categorized Content (i.e. verifying Content Categories and Content Provider identity provided with the Pre-Categorized Content)	CBCS V1.0
CBCS-FUNC-007	The CBCS Enabler SHALL be able to treat Pre-Categorized Content as Categorized Content	CBCS V1.0
CBCS-FUNC-008	The CBCS Enabler MUST allow an authorized CBCS Service Provider to securely retrieve the CBCS User Profile from an External Service Provider. (Note: This does not imply that the CBCS Service Provider can modify a CBCS User Profile stored at an External Service Provider.)	CBCS V1.0
CBCS-FUNC-009	The CBCS Enabler MUST be able to use Screening Rules when applying Content Screening.	CBCS V1.0
CBCS-FUNC-010	The Content Screening Criteria MAY be composed of information from different sources, including public (public bodies, governments, etc.) and private sources.	CBCS V1.0
CBCS-FUNC-011a	The CBCS Enabler SHALL provide the CBCS Service Provider the ability to create, modify or delete Screening Rules.	CBCS V1.0
CBCS-FUNC-011b	The CBCS Enabler SHALL provide the CBCS Service Provider the ability to delegate permissions to create, modify or delete Screening Rules to Authorized Principal(s).	Future
CBCS-FUNC-012	The CBCS Enabler SHALL be able to apply Screening Criteria based on the source of content (for example, the URI or the content owner).	CBCS V1.0
CBCS-FUNC-013	In addition to Content Categories and CBCS User Profiles, the CBCS Enabler MAY use any additional information such as the origin of a message in its Screening Rules.	CBCS V1.0
CBCS-FUNC-014	For content or services explicitly requested by the User, the CBCS Enabler MUST be able to always give a response to the CBCS User (previous advice, blocking information, requested content, etc.).	Future
CBCS-FUNC-015	For content not explicitly requested by the User (Push contents, alerts, spam, etc.) the CBCS Enabler SHOULD be able to generate a register (a log file, for example) with related information without advising the User.	CBCS V1.0
CBCS-FUNC-016	The CBCS Enabler MUST be able to warn an Authorized Principal about content not blocked, but potentially undesirable for the CBCS User.	Future
CBCS-FUNC-017	The CBCS Enabler MUST be able to apply Content Screening to content delivered via browsing, including (but not limited to) HTTP, and incoming messaging, including (but not limited to) SMS, MMS, IM or mobile e-mail.	CBCS V1.0
CBCS-FUNC-018	The CBCS Enabler MUST provide a mechanism to allow a Service Provider to control whether Content Scanning is performed (e.g. using service	CBCS V1.0

	subscription, service type)	
CBCS-FUNC-019	The CBCS Enabler MUST be able to initiate Content Scanning independently of the protocol used to deliver the content to the User.	CBCS V1.0
CBCS-FUNC-020	The CBCS Enabler MUST be able to apply Content Screening to User-originated content (e.g. HTTP requests, SMS).	CBCS V1.0
CBCS-FUNC-021	The CBCS Enabler MUST provide the mechanisms to allow CBCS Service Provider offer its service when the User is roaming in a visited network.	CBCS V1.0
CBCS-FUNC-022	The CBCS Enabler SHOULD give the CBCS User the possibility to inform the CBCS Service Provider about the reception of a particular piece of unwanted content that the CBCS User expected to be blocked by the CBCS Service Provider.	CBCS V1.0
CBCS-FUNC-023	The feedback information about failed screening SHOULD allow the CBCS Service Provider to identify at least the CBCS Subscriber, the Content and the origin of the Content. It MAY contain information about why the CBCS User perceives that the Content should not have been delivered.	CBCS V1.0
CBCS-FUNC-024	It MUST be possible to apply the CBCS Enabler to content that reaches the device through Bluetooth, Infrared, WiFi, USB, removable media or other mechanisms that cannot be controlled by the CBCS Enabler before the content arrives at the device	CBCS V1.0
CBCS-FUNC-025	The CBCS Enabler SHALL be able to present to the CBCS User information (e.g. parental advice or Content Category) about content not blocked	Future
CBCS–FUNC-026	The CBCS Enabler MUST provide a mechanism for Authorized Principals to give feedback to the CBCS Service Provider regarding the decisions made (for example, reporting false positives, false negatives, etc.).	Future
CBCS–FUNC-027	The CBCS Enabler MUST provide a mechanism to allow Authorized Principals to review blocked content and/or get informed about Screening Actions. In order to avoid malicious Content Providers from abusing information about Screening Actions, by default a Content Provider SHOULD NOT be an Authorized Principal to get information about Screening Actions.	Future
CBCS–FUNC-028	The Screening Actions supported by the CBCS Enabler SHALL include the action of asking an Authorized Principal for consent before delivering content to the CBCS User.	Future
CBCS–FUNC-029	The CBCS Enabler SHALL be able to apply Content Screening to all devices employed by a CBCS User	CBCS V1.0
CBCS–FUNC-030	The CBCS Enabler SHALL allow the application of the same or different Screening Rules to different devices employed by a CBCS User	CBCS V1.0
CBCS-FUNC-031	The CBCS Enabler MAY support Screening Criteria which depend on information contained in earlier messages that the CBCS Enabler implementation processed, or the interval between particular screening checking requests.	CBCS V1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
CBCS–SEC–001a	The CBCS Enabler SHALL permit only Authorized Principals to create, modify and access, permissions for Screening Rules.	CBCS V1.0
CBCS–SEC–001b	The CBCS Enabler SHALL permit only Authorized Principals to delegate permissions for Screening Rules.	Future

CBCS–SEC–002	The CBCS Enabler MUST be able to authenticate Content Categorization Entities.	CBCS V1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.2 Charging

Label	Description	Enabler Release
CBCS–CHAR–001	The CBCS Enabler SHALL NOT limit charging models.	CBCS V1.0
CBCS–CHAR–002	The CBCS Enabler MUST be able to provide Charging Enablers with the information for charging the use of the Enabler.	CBCS V1.0

Table 3: High-Level Functional Requirements – Charging Items

6.1.3 Administration and Configuration

Label	Description	Enabler Release
CBCS-ADM-001	The CBCS Enabler MUST be able to be deployed as a subscription-based service.	CBCS V1.0
CBCS-ADM-002	The CBCS Enabler MUST be able to create and manage CBCS User Profiles.	Future
CBCS-ADM-003	The CBCS Enabler MUST be able to create and manage CBCS User Profiles of arbitrary granularity (e.g. per User, per group of Users, for all Users,..)	Future
CBCS–ADM–004	The administration of the CBCS Enabler MAY include configuration, provisioning and maintenance of the Enabler.	CBCS V1.0
CBCS–ADM–005	The CBCS Enabler MAY be able to generate and make available information about Enabler activity (e.g. for statistics, monitoring, reporting, etc.).	CBCS V1.0
CBCS–ADM–006	The CBCS Enabler SHOULD allow a CBCS Subscriber to securely configure the Screening Rules applied to its CBCS Users.	CBCS V1.0
CBCS–ADM–007	The CBCS Enabler SHOULD allow a CBCS Subscriber to customize the responses returned or behaviour when content is blocked.	CBCS V1.0

Table 4: High-Level Functional Requirements – Administration and Configuration Items

6.1.4 Usability

Label	Description	Enabler Release
CBCS–USA-001	For content originating from the CBCS User, the CBCS User SHOULD be informed of the decision made by the CBCS Enabler when the content is blocked.	Future
CBCS-USA-002	For content explicitly requested, the CBCS User SHOULD be informed of the decision made by the CBCS Enabler when the content is blocked.	Future
CBCS–USA-003	The perceived User experience in terms of time to get requested contents SHOULD NOT be significantly affected by the application of the CBCS Enabler.	CBCS V1.0
CBCS–USA-004	The CBCS Enabler SHOULD give the CBCS User the possibility to provide feedback to the CBCS Service Provider without the need to enter the address of the CBCS Service Provider (phone number, email address, HTTP URI, SIP URI, etc.) and with automatic reference to the Content in question.	Future

Table 5: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

Label	Description	Enabler Release
CBCS–IOP–001	The CBCS Enabler MUST provide interfaces to ensure interoperability with other Enablers.	CBCS V1.0
CBCS–IOP–002	The CBCS Enabler MUST be technology agnostic.	CBCS V1.0
CBCS–IOP–003	The CBCS Enabler MUST NOT impact the functionality of other Enablers and MUST NOT impact protocols used to deliver the content.	CBCS V1.0
CBCS–IOP–004	The CBCS Enabler MUST be interoperable across different Network Operators or Content Providers or Service Providers.	CBCS V1.0

Table 6: High-Level Functional Requirements – Interoperability Items

6.1.6 Privacy

Label	Description	Enabler Release
CBCS–PRV-001	The CBCS Enabler MUST be able to keep the CBCS Subscriber identity secret to Content Providers.	CBCS V1.0
CBCS–PRV-002	The CBCS Enabler MUST be able to keep the CBCS User identity secret to Content Providers.	CBCS V1.0
CBCS–PRV-003	The CBCS Enabler MUST be able to keep the Screening Rules secret to Content Providers.	CBCS V1.0
CBCS-PRV-004	Mechanisms SHOULD be provided to allow the protection and avoid the disclosure of CBCS Subscriber information (for example, identity, preferences, policies, blocked content, etc.).	CBCS V1.0

Table 7: High-Level Functional Requirements – Privacy Items

6.2 Overall System Requirements

Label	Description	Enabler Release
CBCS-SYS–001	The CBCS Enabler MUST be defined in an execution environment neutral manner.	CBCS V1.0
CBCS-SYS–002	Any interface defined in the CBCS Enabler MUST be access technology neutral.	CBCS V1.0
CBCS-SYS–003	The interfaces used to access to or interact with the CBCS Enabler from external entities MUST be access technology neutral.	deleted

Table 8: High-Level System Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-CBCS-V0_1	28 Jul 2005		First draft.
	16 Aug 2005		Comments from 3rd Aug CC.
	22 Aug 2005		Comments from revision in Montreal meeting.
	20 Oct 2005		Introduction: Text agreed in Sydney F2F meeting and modified in managed email discussions. Definitions and abreviations: Definition of actors agrred in Sydney Appendix B: Informative figure.
	16-Nov-2005		3 use cases agreed in previous conference calls and meetings (Browsing, multiple sources and messaging). Requirements derived from these 3 use cases. Enhancements in introduction.
	1-Dec-05		Additions in scope section Complete revision of use cases and requirements for consistency
	7-Dec-05		Some editorials corrections during the 20051207 conference call
	17-Jan-06		OMA-REQ-CBCS-2005-0050R01 included. OMA-REQ-CBCS-2005-0052 included. Some minors editorials errors fixed.
	30-Jan-06		Figure 1 in Appendix B has been modified. Some comments from 20060125 conference call included. Some minor editorial errors fixed.
	14-Feb-06		Some changes agreed during Paris F2F. Use case OMA-REQ-CBCS-2006-0006R01 added. Use case OMA-REQ-CBCS-2006-0011R01 added. Different amends to address comments included in OMA-REQ-CBCS-2006-0013.
	31-Mar-06		Changes in Definitions section proposed in the 20060214 version (some of them not formally agreed). Changes in agreed use cases proposed in the 20060214 version (within normal flow of use cases 5.2 and 5.3). Use case OMA-REQ-CBCS-2006-0018R01 added. Use case OMA-REQ-CBCS-2006-0025R01 added. Input contribution OMA-REQ-CBCS-2006-0034R01 added. Implemented all changes in document OMA-REQ-CBCS-2006-0038 Updated use of the terms “screening criteria”, “screening rules” and “CBCS User Profile” according to agreed definitions Changes in Annex B: No difference between Trusted and Untrusted Content Providers (changes in figure and relationships description).
	4-Apr-06		Implemented all changes in document OMA-REQ-CBCS-2006-0039 Implemented all changes in document OMA-REQ-CBCS-2006-0009R05 Implemented revisions agreed in the Vancouver face to face meeting Clean-up of English and typing errors
	5-Apr-06		Implemented all changes in document OMA-REQ-CBCS-2006-0037R02 Implemented all changes in document OMA-REQ-CBCS-2006-0045 Re-arranged the order of some definitions and requirements for readability (without modifying them) Implemented additional revisions agreed in the Vancouver face to face meeting Further clean-up of formatting, English and typing errors
	18-May-06		Revision according to the comments in the RD Review Report, document OMA-RDRR-CBCS-V1_0-20060518-D

Document Identifier	Date	Sections	Description
	31-May-06		Revision of section 5.5 according to document OMA-REQ-CBCS-2006-0058R01 to align the use of the term "content scanning". Minor (editorial) revisions according to comments on conference call.
	12-Jun-06		Added CBCS V1.0 in the "Enabler Release"columns of the normative requirements tables in section 6.
	22 Jun-06		DSO editorial changes (frontpage, footers and IPR) prior to TP approval
Candidate Version: OMA-RD-CBCS-V1_0	11 Jul 2006		TP approval: OMA-TP-2006-0252- INP_INP_CBCS_V1_0_RD_for_Candidate_Approval
Draft Version: OMA-RD-CBCS-V1_0	05 Nov 2007	6.1	Editorial updates: 2007 template/copyright Table of content: added Figures and Tables (missing from previous version) Implemented class 2 change: OMA-REQ-2007-0049R02-INP_Class_2_change_CBCS_RD (requirement FUNCT_018)
Candidate Version: OMA-RD-CBCS-V1_0	11 Dec 2007	N/A	Editorial fix: Tables sorted in Content TP Notified: OMA-TP-2007-0454-INP_CBCS_V1_0_RD_for_Notification BoD Ratified
Candidate Version: OMA-RD-CBCS-V1_0	18 Aug 2008	2.2, 3.2, 3.3, 4, 5.4.5, 6.1, 6.1.1, 6.1.3, 6.1.4, 6.1.5, 6.2	Revision according to the agreed comments accumulated in consistency review report OMA-CONRR-CBCS-V1_0-20080812-D
Draft Version: OMA-RD-CBCS-V1_0	28 Aug 2008	All	Back to –D as changes were applied to previous version Editorial fixes: Footer and copyright updated Definitions and abbreviations sorted
	29 Aug 2008	6.2	Reinstated deleted row and marked CBCS_SYS_003 as deleted
Candidate Version: OMA-RD-CBCS-V1_0	14 Oct 2008	All	Status changed to Candidate by TP: OMA-TP-2008-0377- INP_CBCS_V1_0_ERP_for_Candidate_Approval

Appendix B. CBCS Actors (Informative)

B.1 Relationships between actors

This informative appendix includes a figure with the proposed relationships between the identified actors in the CBCS scene. This is included only as an informative example and it does not imply or suppose any architectural decision or assumption. The doted lines are for relationships that may or may not be needed in the complete CBCS scene. Even if every relationship is showed in the figure as one-to-one, some of them can be intended also as an one-to-many relationship (for example, there can be several Content Screening Authorities related with the CBCS Service Provider).

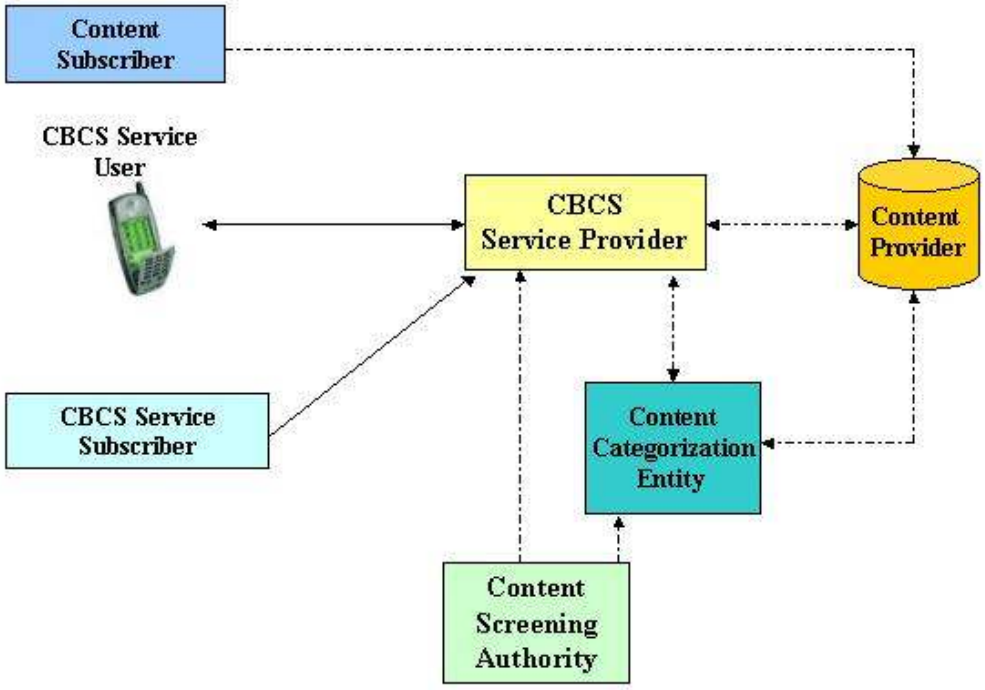

Figure 2: Relationships between CBCS actors

The description of each one of these relationships is the following:

Content Subscriber – Content Provider

The relationship between a Content Subscriber and a Content Provider usually includes a subscription model between the Subscriber and the entity providing the content (this is, the Content Providers). This kind of relationship can be related with any content delivery protocol or mechanism (for example, contents delivered via text messaging, multimedia messaging, WAP Push indications, etc.). This kind of subscription and the delivery of content through any of these involved mechanisms does not imply the use (not even the existence) of a CBCS Service.

CBCS Service Provider – Content Provider

The Content Provider is considered the source of the content requested by or offered to the Users through different access services or delivery mechanisms (MMS; WAP/Web browsing, etc.). This content is screened by the CBCS Service Provider prior to be delivered to the CBCS User.

CBCS User – CBCS Service Provider

The CBCS Service Provider is in charge of, through the offering of the CBCS Service, screen the content received and/or sent by the CBCS User. This relationship also includes the delivery channels that allow the CBCS Service Provider to receive content from and forward content to the CBCS User (for example, MMS bearers, WAP bearer, etc.).

CBCS Subscriber – CBCS Service Provider

The CBCS Subscriber is the entity engaged in a subscription with the CBCS Service Provider. Usually, the CBCS Subscriber may have permissions to manage the CBCS User Profile.

Content Screening Authority – CBCS Service Provider

The Content Screening Authorities gives the CBCS Service Provider information regarding some general rules and/or guidelines affecting the whole service. These guidelines are not about the way the service has to be implemented or deployed.

Content Screening Authority – Content Categorization Entity

The Content Screening Authorities give the Content Categorization some rules and guidelines regarding the categorization schemas to be used.

Content Categorization Entity – CBCS Service Provider

The communication between the CBCS Service Provider and the Content Categorization Entity can be used to retrieve Content Categories. This may also be done online regarding a given content (previously categorized or not).

Content Categorization Entity – Content Provider

Content Providers can use the services offered by the Content Categorization Entities to retrieve the assigned categorization information to its content. This way, Content Providers can offer previously categorized content.