Categorization Based Content Screening Framework Architecture

Candidate Version 1.0 – 12 Feb 2009

Open Mobile Alliance
OMA-AD-CBCS-V1_0-20090212-C

Contents

Figures

1. Scope (Informative)

This document provides the architecture for the Categorization Based Content Screening (CBCS) Enabler of OMA. The objective of the Categorization Based Content Screening (CBCS) Enabler is to apply Screening Rules before delivering Content to the mobile user, using Content categorization. A Content Category qualifies the type of Content, according to a categorization scheme. The CBCS Enabler can obtain the Content Category for a given piece of Content from a Categorization Entity, or from the Content itself.

There are two usage patterns for the CBCS Enabler. In the first pattern, the CBCS Enabler applies Screening Rules whenever a Resource makes a Content request or reply. In the second pattern, a Resource explicitly solicits Content Screening from the CBCS Enabler.

The architecture shown in this document is intended to facilitate the development of specifications for obtaining Content Categories and for defining, managing, evaluating, and enforcing Screening Rules in a way that is scalable and flexible yet independent of any specific implementation scheme.

Note that this Enabler does not specify individual Screening Rules, but rather addresses requirements on how to express Screening Rules. The specification of categorization schemes, CBCS User interaction (such as customer facing warnings and requests for consent), CBCS User Profile, pattern matching techniques and delegation of management rights also falls out of the scope of the Enabler specification.

2. References

2.1 Normative References

[CBCS-RD] "Categorization Based Content Screening Framework Requirements", Open Mobile Alliance™, OMA-RD_CBCS-V1_0, URL:http://www.openmobilealliance.org/

[OSE-AD] "OMA Service Environment", Open Mobile Alliance™, OMA-AD-Service-Environment-V1_0_4, URL: http://www.openmobilealliance.org/

[PEEM-AD] "Policy Evaluation, Enforcement and Management Architecture", Open Mobile Alliance™, OMA-AD_Policy_Evaluation_Enforcement_Management-V1_0, URL:http://www.openmobilealliance.org/

[PEEM-RD] "Policy Evaluation, Enforcement and Management Requirements", Open Mobile Alliance™, OMA-RD_Policy_Evaluation_Enforcement_Management-V1_0, URL:http://www.openmobilealliance.org/

[PEL-TS] "PEEM Policy Expression Language Technical Specification", Open Mobile Alliance™, OMA-TS-PEEM_PEL-V1_0, URL:http://www.openmobilealliance.org/

[PEM-1-TS] "Policy Evaluation, Enforcement and Management Callable Interface (PEM-1) Technical Specification", Open Mobile Alliance™, OMA-TS-PEEM_PEM1-V1_0, URL:http://www.openmobilealliance.org/

[PEM-2-TS] "Policy Evaluation, Enforcement and Management – Management Interface (PEM-2) Technical Specification", Open Mobile Alliance™,OMA-TS-PEEM_PEM2-V1_0 , URL:http://www.openmobilealliance.org/

[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", OMA-ORG-Dictionary-V2_7, Open Mobile Alliance™, 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 purposes of the present document, the terms and definitions given in [OMA-DICT] and the following apply:

Authorized Principal	A Principal [OMA-DICT] with permissions to perform specific action(s) or receive specific information [CBCS-RD]
Categorization Based Content Screening Service Provider	The Service Provider [OMA-DICT] that deploys the CBCS Enabler [CBCS-RD]
Categorization Based Content Screening User Profile	The User Profile [OMA-DICT] applicable to the CBCS Enabler [CBCS-RD]
Categorization Based Content Screening User	A Principal whose receivable or transmitted Content is subject to a CBCS Enabler implementation [CBCS-RD]
Categorized Content	Content for which a set of Content Categories have been assigned [CBCS-RD]
Content	Digitized work that is processed, stored, or transmitted. It includes such things as text, presentation, audio, images, video, executable files, etc. Content may have properties such as media type, mime type, etc. [OMA-DICT]
Content Categorization Entity	The entity that assigns Content Categories to Content [CBCS-RD]
Content Categorization Rule	A rule that is capable of identifying an appropriate Content Category for certain Content
Content Category	A category assigned to Content, aiming to describe the characteristics of the Content [CBCS-RD]
Content Provider	The entity making Content available to the Categorization Based Content Screening User [CBCS-RD]
Content Scanning	The act of determining the Content Category (or Content Categories) of the Content [CBCS-RD]
Content Screening	The act of blocking, allowing or amending Content [CBCS-RD]
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 [CBCS-RD}
Non-Categorized Content	Content for which no Content Category has been assigned [CBCS-RD]
Screening Action	A Policy Action [OMA-DICT] applicable to the CBCS Enabler [CBCS-RD]
Screening Criteria	Policy Conditions [OMA-DICT] applicable to the CBCS Enabler [CBCS-RD]
Screening Rule	A Policy Rule [OMA-DICT] that uses Screening Criteria and Screening Actions [CBCS-RD]

3.3 Abbreviations

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

CAMEL	Customised Applications for Mobile networks Enhanced Logic
CBCS	Categorization Based Content Screening

CBCS-1	CBCS Categorization interface
CBCS-2	CBCS Categorization Rules management interface
CBCS-3	CBCS Categorization association interface
CBCS.PEM-1	PEEM Callable interface extended for use in CBCS
CBCS.PEM-2	PEEM Management interface inherited for use in CBCS
HTTP	Hyper Text Transfer Protocol
IM	Instant Messaging
IPsec	IP Security
MMS	Multimedia Messaging Service
MSISDN	Mobile Station ISDN number
PEEM	Policy Evaluation, Enforcement, and Management
PEL	Policy Expression Language
PEM-1	PEEM Callable interface
PEM-2	PEEM Management interface
SIP	Session Initiation Protocol
SMS	Short Message Service
TLS	Transport Level Security
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 users. As a consequence, the mobile user's exposure 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 users, for example minors, from inappropriate Content. We consider Content in the broadest sense: Content can be the body of a message (request or reply), but it can also be the request itself (for example referring to a forbidden URI).

The objective of the Categorization Based Content Screening (CBCS) Enabler is to screen Content, independent of either the Resource (e.g. device [CBCS-RD]) that is used to request screening, or to which Content is being pushed, or the Enabler or protocol that is used to deliver the Content to the Resource (e.g. device [CBCS-RD]).

The screening process may use information such as:

- a Content Category,
- the Content source (for example, the URI or the Content owner),
- a CBCS User Profile (such as the user's MSISDN, age, preferred and banned type of Content),
- Screening Rules.

As a result of applying the rules, the Content may pass, be blocked, be subject to modification, be combined with a warning, or pass after consent is received from an authorized principal. The Screening Rules are managed by authorized Principals.

4.1 Planned Phases

Most of the CBCS requirements are planned to be fully met in this release [CBCS-RD]. No future releases are currently planned.

4.2 Security Considerations

The CBCS Enabler (Content Screening Component) can be deployed according to two usage patterns (callable and proxy usage pattern). In both usage patterns, interaction with the CBCS Enabler implementation may be within the same domain or across domain boundaries. For both cases appropriate security measures should be considered, such as IPsec, TLS and web service security. If the encrypted Content is to be processed by CBCS, it must be decrypted as part of the processing.

Note that different domains may imply: different administrative domains, different security domains and/or the need to traverse insecure networks between the domains.

In both usage patterns the CBCS Enabler implementation may delegate to (i.e. make a request to) other Resources such as a Charging Enabler implementation. These other (delegated to) Resources may or may not reside in different security or administrative domains and appropriate security measures should be considered for each case. Appropriate key management and selective encryption when delegating functions may be required and may be specified by the Screening Rules.

In both usage patterns the Screening Rules are managed (i.e., create, delete, modify, view Screening Rules) through the management interface. Various management actors such as network operator and end-user are supported and appropriate associated security measures need to be applied. It should be possible to authenticate requestors, (e.g., an end-user, or other principles authorised by service provider or third party) and secure the management interface exchanges for both the intra-domain and the inter-domain case.

5. Architectural Model

5.1 Dependencies

The CBCS Enabler depends on PEEM [PEEM-AD] for its callable interface (a.k.a. CBCS.PEM-1 [PEM-1-TS]) and management interface (a.k.a. CBCS.PEM-2 [PEM-2-TS]). The CBCS Enabler specifications will define how to apply the CBCS.PEM-1 and CBCS.PEM-2 interfaces to achieve Categorization Based Content Screening. The CBCS Enabler may be realized using PEEM proxy and callable usage pattern.

5.2 Architectural Diagram

This section contains the CBCS architectural diagram using some PEEM nomenclature [PEEM-AD].

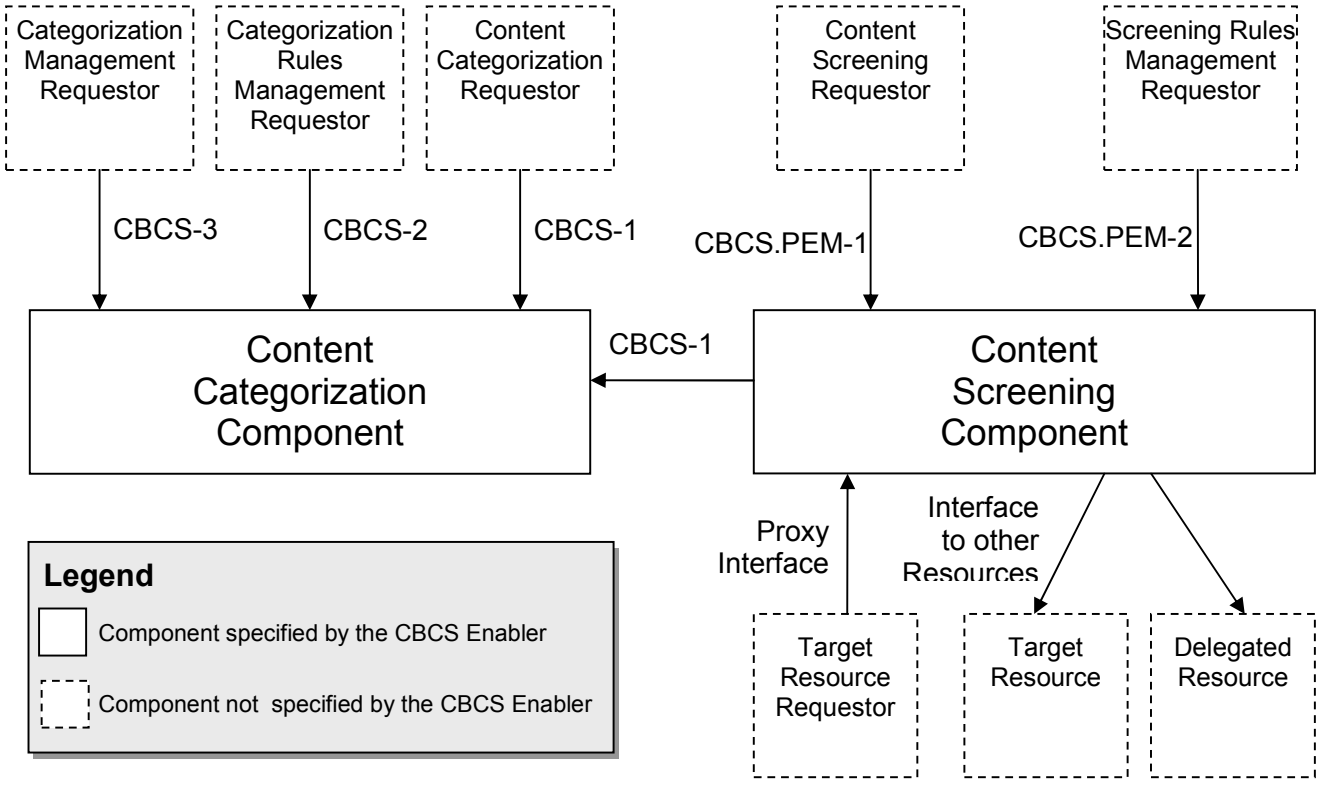

Figure 1 CBCS Enabler architecture

The CBCS Enabler consists of two independent functional components, the Content Categorization Component and the Content Screening Component:

- Content Screening Component: processes Content according to Screening Rules, CBCS User Profile information and Content Category/other characteristics (see also Section 5.3.1), and
- Content Categorization Component: The Content Categorization Component is responsible for mapping Content and/or Content references (e.g., URI) in the incoming request to a set of Content Categories. This component can be called directly by any Resource or by the Content Screening Component. (see also Section 5.3.2). This component can also be called in order to manage categories related to Content.

The two components can be used together or separately. The Content Screening Component can be deployed in the proxy usage pattern [PEEM-AD: Section 5.2] and/or in the callable usage pattern [PEEM-AD: Section 5.2]. Also, it is evident from the CBCS Requirements Document [CBCS-RD] that an interface is required for the purposes of managing Screening Rules ,

and since Screening Rules are Policy Rules specific to CBCS, the PEEM interface for Policy Rules management (PEM-2) may be re-used [PEEM-AD: Section 5.3.4] to create interface CBCS.PEM-2.

The Content Screening Component may use the "Interface to other Resources" to access the CBCS User Profile, but the specification of this interface and the definition of the CBCS User Profile itself are out of the scope of the CBCS Enabler specification.

The functional components and interfaces are further described in section 5.3.

5.3 Functional Components and Interfaces

5.3.1 Content Screening Component

The Content Screening Component has the following features:

- Identifies the Screening Rules associated with the incoming request (proxy or callable usage pattern). This phase may include:
    - The identification of the relevant fields which compose the "Content" in the request ("Content" part but also fields like sender information may be relevant)
    - The identification of Content Category. This information about Content Category may be present in the request. The information may not be used in case the sender is an untrusted source. In this case, or if no information about the Content Category is available, the Content Category may be determined using the CBCS-1 interface to the Content Categorization Component.
- Processes the Screening Rules:
    - The processing of the Screening Rules may use Content Category/other information received and/or use context information obtained through other means.
    - The screening rules may use information from the CBCS User Profile which may include the following:
        - User information :
            - User identification (communications addresses, e.g. MSISDN, email address, etc.)
            - Date of birth
            - Type of user (e.g. teenager, adult...)
            - Country of residence
        - Willingness to be asked for consent before receiving the Content
        - User preferences
            - Preferred and banned type of Content
    - As determined by the Screening Rules, processing may depend on the results of other functions (e.g., pattern matching). Note that specification of the interface to these functions is not in scope of CBCS.
    - The Content Screening Component may determine a decision:
        - in the proxy usage pattern the Screening Rules processing may complete by enforcing the resulting decision, or
        - in the callable usage pattern: the Screening Rules processing may complete by returning a decision to the requesting Resource or perform enforcement itself. If a decision is returned to a Resource, that Resource uses the rendered decision.
- Provides the management functions of creating, deleting, modifying and viewing of Screening Rules.
- To support roaming, the Screening Rules can be applied in CBCS Enablers in different domains, or can be combined and applied in one of them. In the former case, when there is a need for communication, the Enablers interact via

CBCS.PEM-1. In the latter case, the Screening Rules in one CBCS Enabler may be made available in the other domain using a CBCS.PEM-2 interface.

The Screening Rules are expressed as PEEM rules [PEL-TS].

5.3.2 Content Categorization Component

The Content Categorization Component has the following features:

- Upon request made via the CBCS-1 interface, this component maps Content/other information (e.g., reference to the Content) to a set of Content Categories which are returned. Internal functions (e.g. pattern recognition) that may be involved during the determination of the Content Categories to be returned are not directly exposed through the CBCS-1 interface.

- Provides the management functions of creating, deleting, modifying and viewing of
    - Content Categorization rules.
    - Content references (e.g., URIs) and associated Content Categories.

As two CBCS-1 arrows are represented in figure 1, this component can be used either by the Content Screening Component or another requestor.

The Categorization Rules are expressed as PEEM rules [PEEM-AD].

5.3.3 CBCS.PEM-1 Interface

The CBCS.PEM-1 interface to invoke the processing of Screening Rules is derived from PEM-1 [PEM-1-TS]. It is used to perform Content Screening in the callable usage pattern. The request passed over this interface may include the following parameters:

- Identification of the target principal for Content,
- Content or a Content reference (e.g., URI),
- Other information (e.g., Content metadata and categorization information)
- Content source (e.g. URI) and associated information

The response passed over this interface may include the following parameters:

- The decision resulting from the processing of the screening rules
- Additional explanatory information related to the decision (e.g. justification of a decision to not allow access to Content)

If needed, CBCS specific input and/or output parameter may be added to extend the CBCS.PEM-1 interface

5.3.4 CBCS.PEM-2 Interface

The CBCS.PEM-2 management interface to the Content Screening Component is derived from PEM-2. It is used to create, delete, modify and view Screening Rules.

5.3.5 CBCS-1 Interface

Using this interface a Resource may obtain the Content Category (or Categories) for given Content.

Input parameters in the request may include:

- the Content itself or a Content reference (e.g. URI)

- Content related information (e.g. Content metadata and categorization information)
- Content source (e.g. URI) and associated information.
- A request identifier.

Output parameters in the response may include:

- A set of Content Categories (i.e. zero or more)
- Metadata associated with the Content Categories (e.g. for a sport category: type of sport, etc)
- The request identifier of the request to which this is the response.

5.3.6 CBCS-2 Interface

The CBCS-2 interface is used to create, delete, modify and view Content Categorization Rules.

5.3.7 CBCS-3 Interface

The CBCS-3 interface is used to associate (create, delete, modify and view) Content references (e.g., URIs or the Content itself) with Content Categories.

5.3.8 Interfaces Not Defined by CBCS Enabler (Informative)

Proxy Interface

While CBCS can be deployed in proxy pattern, a proxy interface is not specified by CBCS; this is because specifying such an interface depends on the protocols being proxied (e.g. Browsing, HTTP, Messaging, etc), which is out of scope for CBCS.

Interfaces to Other Resources

The Interface to other Resources is not specified by CBCS; it is a shorthand standing for all interfaces that CBCS may have to use for exchanges with delegated Resources, in the process of evaluating and/or enforcing Screening Rules or Content Categorization Rules. The Interface to other Resources may also be used to ask for consent to receive the Content. The CBCS Enabler has to ensure the correlation between the request and its response, but this is outside the scope of this enabler.

The user notifications may be performed by existing mechanisms. These mechanisms may involve: SMS, MMS, WAP PUSH and SIP Push, etc. Protocols for these deliveries are not specified in this specification.

The function of subscribing to the notification of specific event (e.g. subscribe to notifications of management operations performed on permissions rule they manage) can be performed by existing mechanisms, for example a web-page or a message (e.g. SIP SUBSCRIBE), which are not specified in this specification.

5.4 Flows

5.4.1 Flows on CBCS-1 Interface

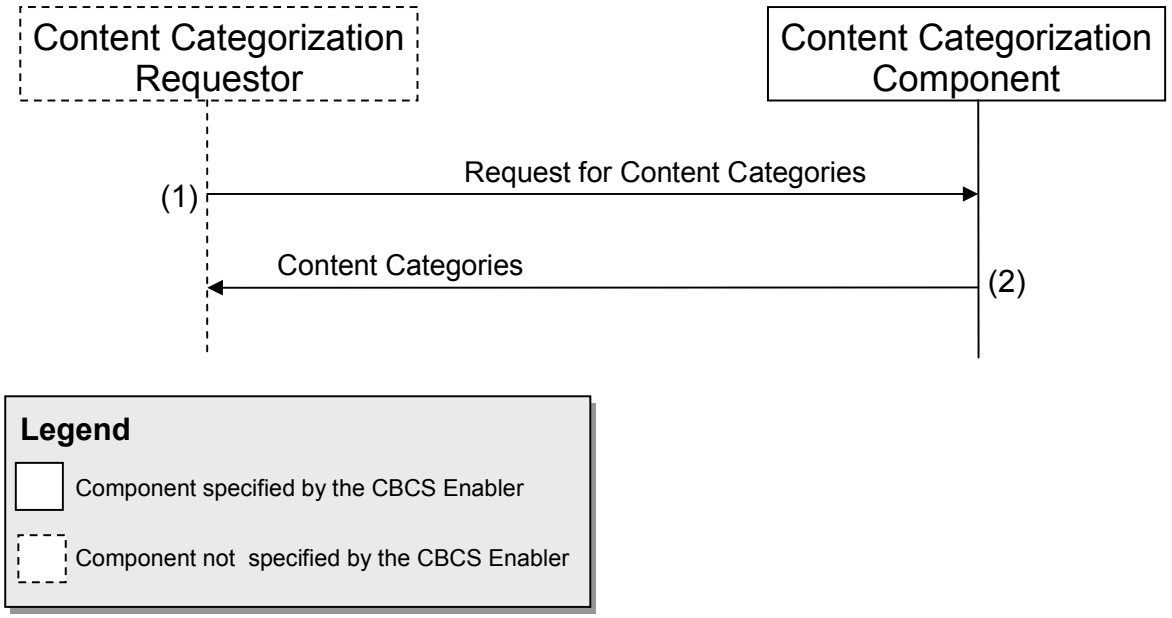

Figure 2 Logical flow for the Content Categorization callable usage pattern

Figure 2 shows how the Content Categorization Requestor interacts with Content Categorization Component via CBCS-1 interface. Any Resource including the CBCS Screening Component may use the CBCS-1 interface to request a Content Category (flow #1), and then receive a result carrying the Content Categories that the Content is associated with (flow #2).

5.4.2 Flow in the Callable Usage Pattern of the Content Screening Component

The CBCS Enabler can be deployed in a callable usage pattern (see Figure 3).

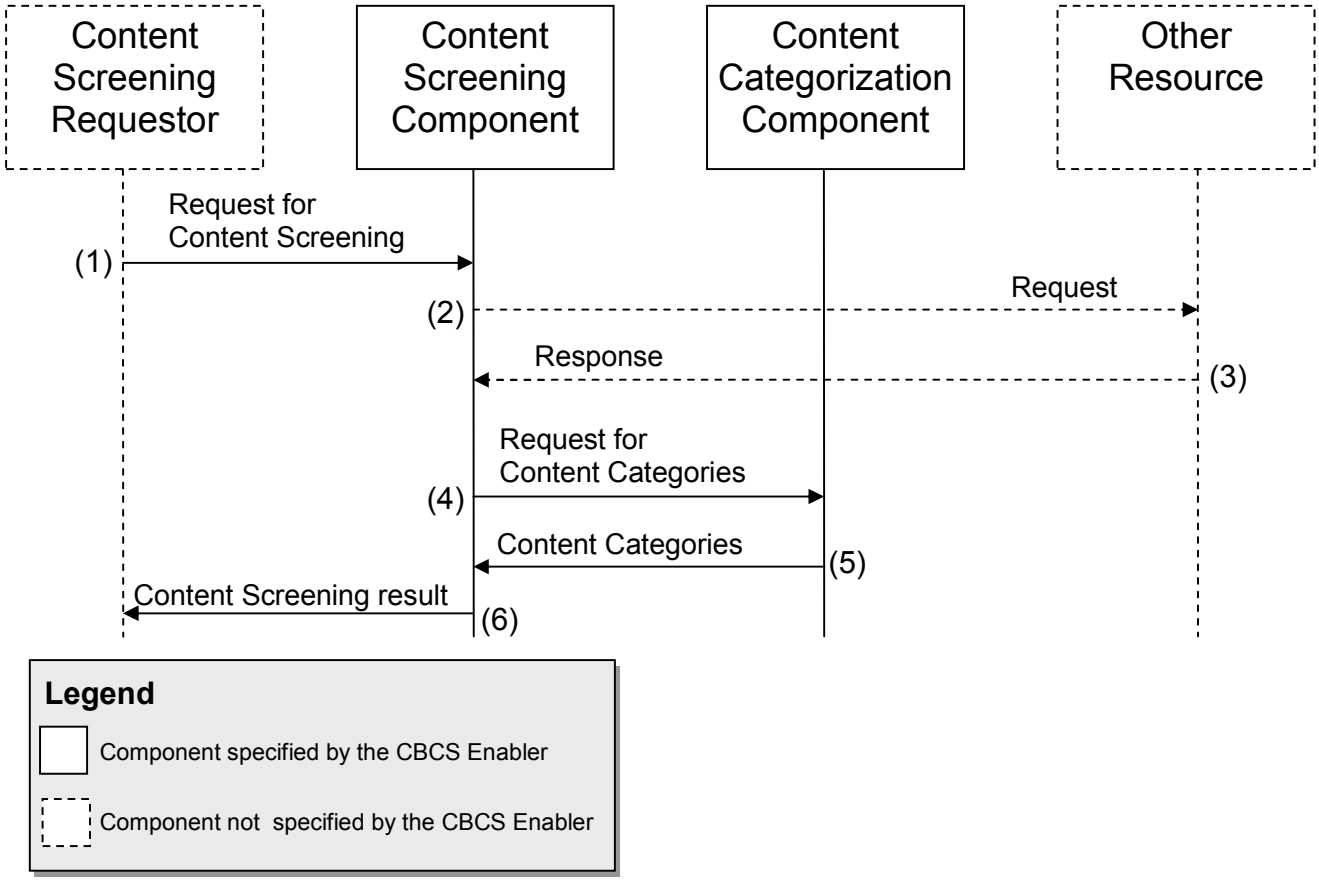

Figure 3 Logical flows for the Content Screening Component callable usage pattern

The Content Screening Requestor uses CBCS.PEM-1 to send a request for Content Screening to the Content Screening Component (flow #1). Upon reception of the content screening request the Content Screening Component may or may not interact with Other Resources (flow #2 and #3) and this may be decided through processing of screening rules. The Content Screening Component then requests the Content Category of the Content to the Content Categorization component (flow #4) by means of CBCS-1. The Content Categorization component determines the Content Categories and returns the result (flow #5). The Content Screening component continues processing the Screening Rules and returns (flow #6) the outcome to the Content Screening Requestor.

An example of an interaction with Other Resources in flows #2 and #3 is a request to an identity management system to resolve the identity of the end-user. The details of such interactions with Other Resources fall out of the scope of the CBCS Enabler specifications.

5.4.3 Flow in the Proxy Usage Pattern

The CBCS Enabler can be applied in proxy usage pattern (see Figure 4).

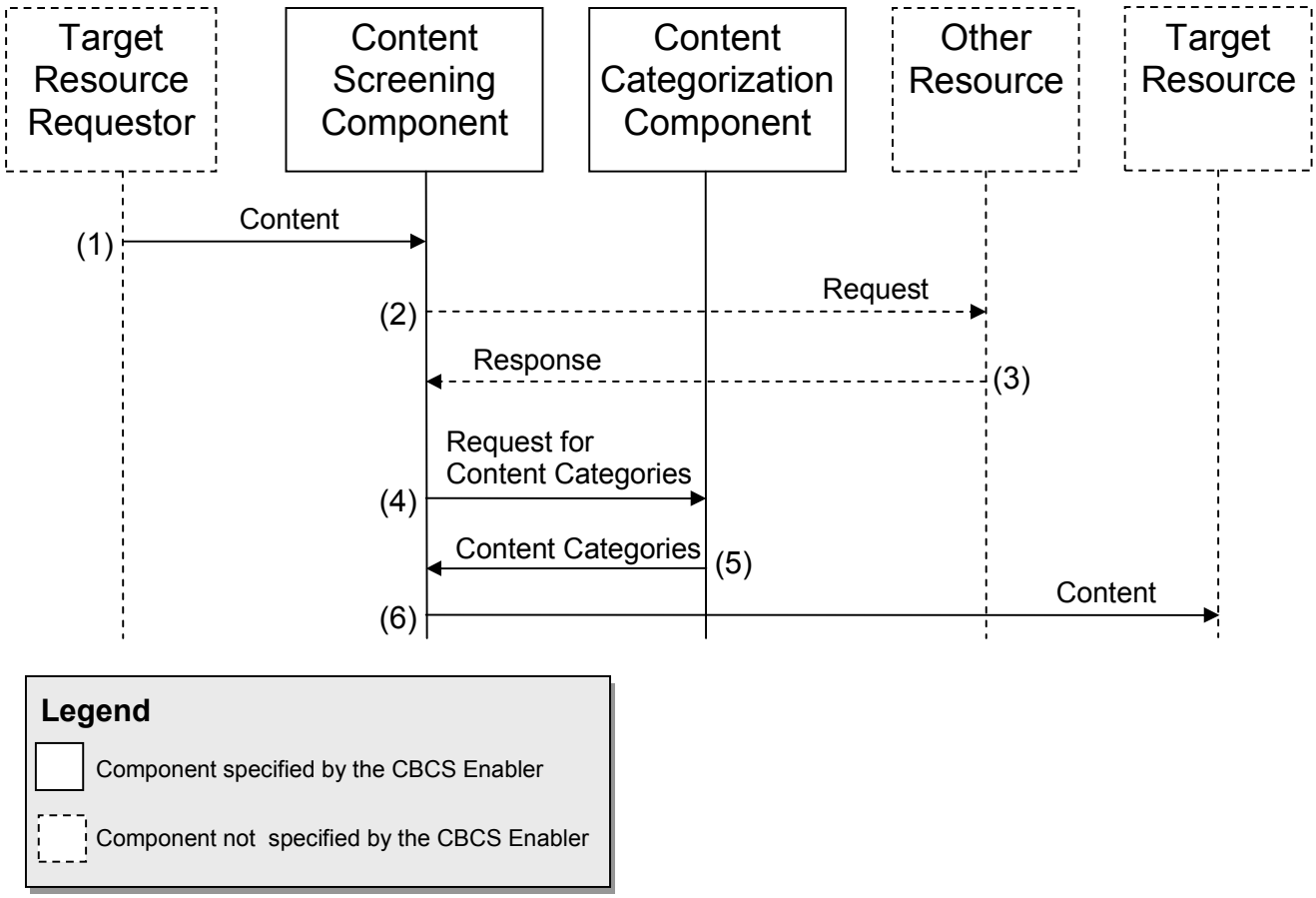

Figure 4 Logical flows for the Content Screening Component proxy usage pattern

In Figure 4 the Target Resource Requestor sends Content (e.g., requests or responses that carry Content) to its Target Resource. That Content is intercepted by the Content Screening component (flow#1). Flows #2, #3, #4 and #5 are similar to the ones explained for the callable usage pattern in Figure 3. The Content Screening component processes the Screening Rules and applies the associated Screening Actions to the Content intercepted from the Target Resource Requestor. The Content Screening Component sends on the resulting Content (which may be equal to the original Content or not) to the Target Resource (flow #6).

5.4.4 Flow on the CBCS.PEM-2 Interface for the Screening Rules Management

In the Screening Rules management flows the Screening Rules Management Requestor issues a request for Content Screening Rules Management (flow #1 in Figure 5) to the Content Screening component, through the CBCS.PEM-2 interface. Upon reception of the request the Content Screening component identifies the type of Screening Rules management request (e.g., create, delete, modify, view), executes the appropriate function and returns the results to the Screening Rules Management Requestor (flow #2).

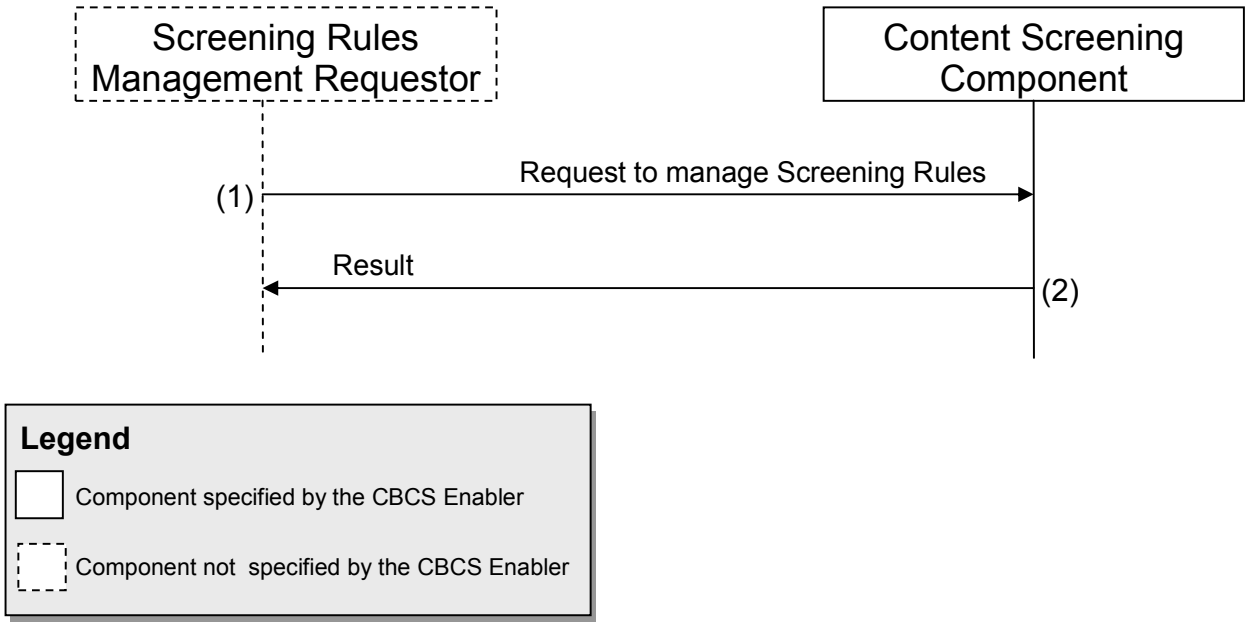

Figure 5 Management of Screening Rules

5.4.5 Flows to Manage Content Categories and Rules

In the Content Categorization Component management flows the Categorization Rules Management Requestor issues a request to manage Content Categorization Rules using CBCS-2 (flow #1 in figure 6a) or a request to associate Content references (e.g., URIs) with Content Categories using the CBCS-3 interface (flow #1 in figure 6b). Upon reception of the request the Content Categorization component identifies the type of management request (e.g., create, delete, modify, view), executes the appropriate function and returns the results to the Categorization Rules Management Requestor (flow #2 in figure 6a and figure 6b).

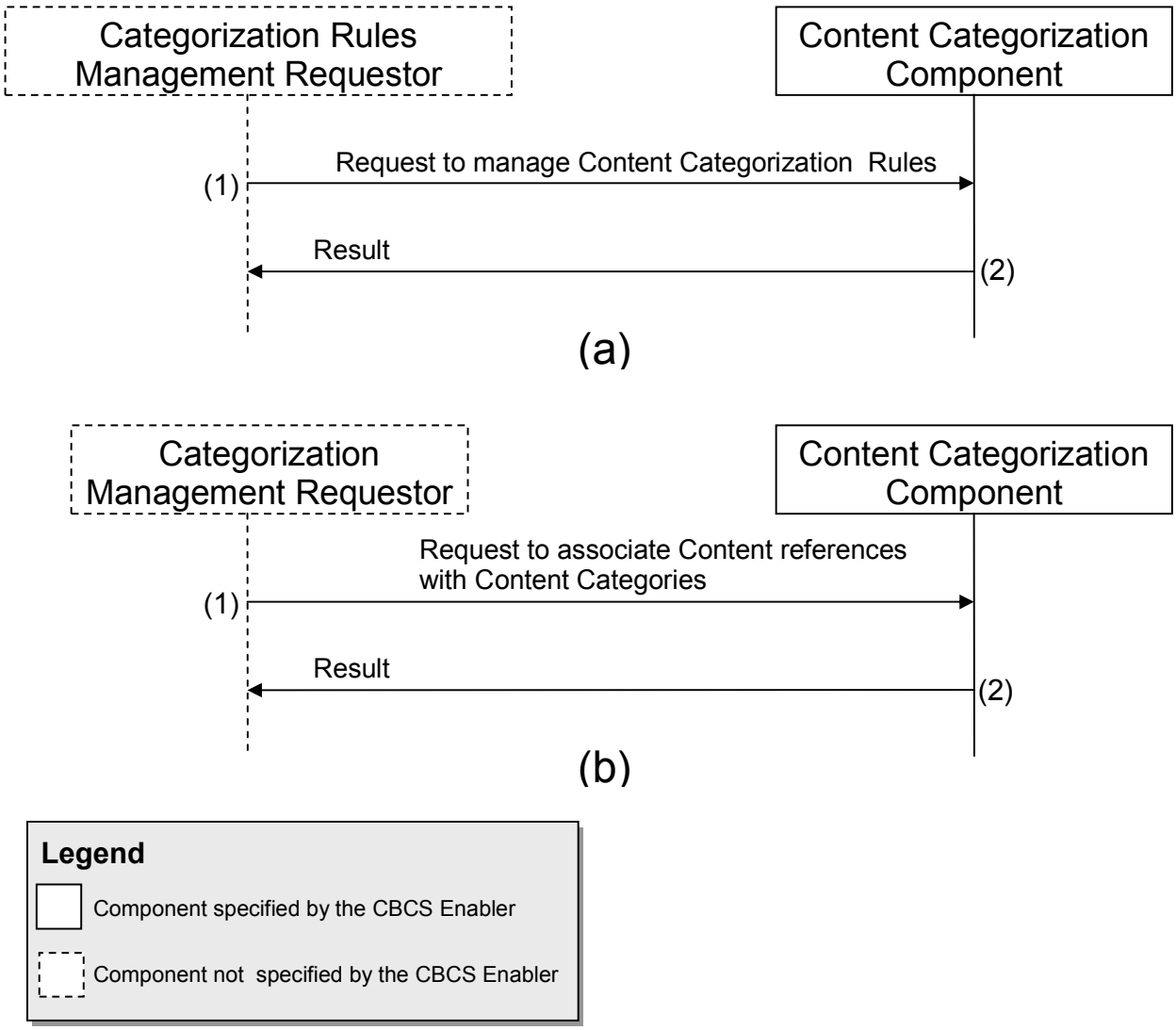

Figure 6 Management interactions with the Content Categorization Component

5.4.6 Roaming scenarios (Informative)

The CBCS Enabler MUST support roaming, however how to apply the CBCS Enabler to roaming users is essentially a deployment issue. This section explains how the CBCS Enabler MAY be used to screen content for roaming users.

The following scenarios have been identified for the use of the CBCS Enabler in roaming situations:

- *Home network only screening* (section 5.4.6.1): a Content Screening Requestor in the Visited network makes a CBCS.PEM-1 call to the CBCS Enabler in the Home network to screen the Content before delivery to the roaming user.
- *Independent screening in Home and Visited networks* (section 5.4.6.2): a Content Screening Requestor in the Visited network makes independent CBCS.PEM-1 calls to the CBCS Enabler in the Home and Visited networks to screen the Content before delivery to the roaming user.
- *Combined screening in Home or Visited network* (sections 5.4.6.3and 5.4.6.4): the content is screened in the Home or Visited network, combining the Screening Rules from both networks. A CBCS.PEM-2 request is used to fetch the external Screening Rules from the other network.
- *PEM-1 delegation* (sections 5.4.6.5 and 5.4.6.6): the Home or Visited network delegates the CBCS.PEM-1 request to the other network, exporting the Screening Rules it wants the other network to evaluate.

5.4.6.1 Screening in Home network only

Before delivering Content to a roaming CBCS User, a Content Screening Requestor in a Visited network SHOULD make a screening request to the CBCS Enabler in the CBCS User's Home network. This should be possible even if the Visited network has no CBCS Enabler deployed, or if the CBCS Enabler in the Visited network does not screen content for visiting CBCS Users. Figure 7 illustrates this scenario.

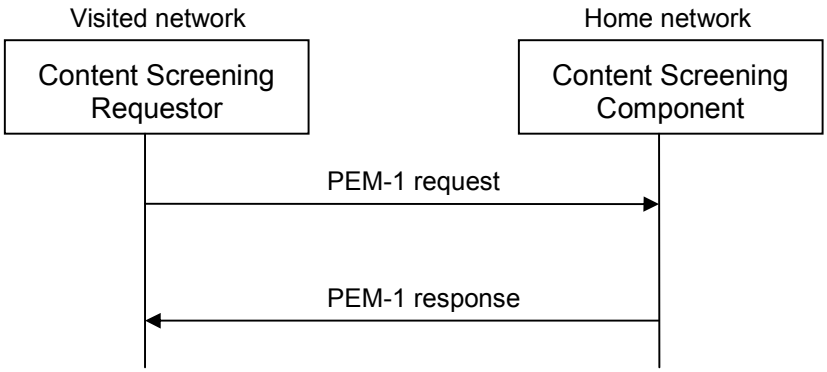

Figure 7 Screening in the Home network of a roaming CBCS User

5.4.6.2 Independent screening in Home and Visited networks

If the Visiting network requires content to be screened for roaming users, then a Content Screening Requestor MAY make independent screening requests to the CBCS Enabler in the Home network and the CBCS Enabler in the Visiting network. The Content Screening Requestor SHOULD deliver the Content to the visiting CBCS User only if the response from both the Home and Visited CBCS Enabler indicate that the Content can be delivered to the User. Figure 8 illustrates this scenario.

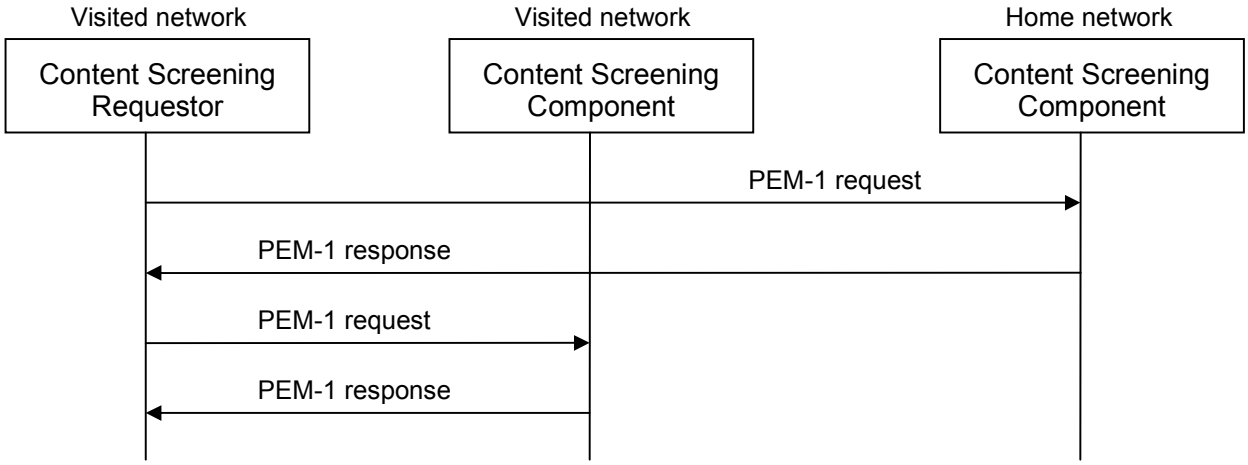

Figure 8 Subsequent screening in Home and Visited network

5.4.6.3 Combined screening in Visited network

Although the scenario in section 5.4.2 is straightforward and simple, it has two important disadvantages:

- It involves two independent CBCS.PEM-1 requests which are processed separately in two servers, which can lead to considerable delay. This is particularly inefficient if the screening rules in CBCS Enablers of the Home and Visited networks are very similar.
- It can cause the Content Screening Requestor to receive conflicting responses from the CBCS Enablers in the Home and Visited networks. The fact that the Content Screening Requestor must resolve such conflicting responses means that it must have some decision capacity itself, which cannot be assumed in general.

Figure 9 shows an alternative scenario that addresses these two disadvantages. In this scenario the Content Screening Requestor in the Visited network makes a single CBCS.PEM-1 screening request to the CBCS Enabler in the Visited network. This CBCS.PEM-1 request MAY contain a reference to an external Policy, in this case the Screening Rules held by the CBCS Enabler in the user's Home network.

The CBCS Enabler in the Visited network fetches the external Screening Rules from the Home network with a CBCS.PEM-2 request. It then evaluates both the Screening Rules obtained from the Home network and its own Screening Rules to determine the response to be sent back to the requesting Enabler.

The following points explain this scenario further:

- The CBCS.PEM-2 interface (for Policy Management) SHOULD be used to request Screening Rules from the CBCS Enabler in the Home network.
- The Screening Rules from the CBCS Enabler in the Home network MAY have to be adapted for processing by the CBCS Enabler in the Visited network.
- The CBCS Enabler in the Visited network MAY combine the Screening Rules from the CBCS Enabler in the Home network with its own Screening Rules to form one set of Screening Rules, or it MAY process the Screening Rules separately.
- The request for Screening Rules MAY also be triggered as a result of mobility management, for example when a roaming CBCS User attaches to the Visiting network for the first time.

- The CBCS Enabler in the Visited network MAY delete the Screening Rules for the visiting CBCS User as a result of mobility management (e.g. when the CBCS User detaches from the Visited network) or after a certain time has passed without the Screening Rules having been used.
- If the CBCS Enabler in the Visited network caches external Screening Rules for visiting users, then the CBCS Enabler in the Home network SHOULD use the CBCS.PEM-2 interface to notify the CBCS Enabler in the Visited network if any of the Screening Rules for the visiting CBCS User are modified.

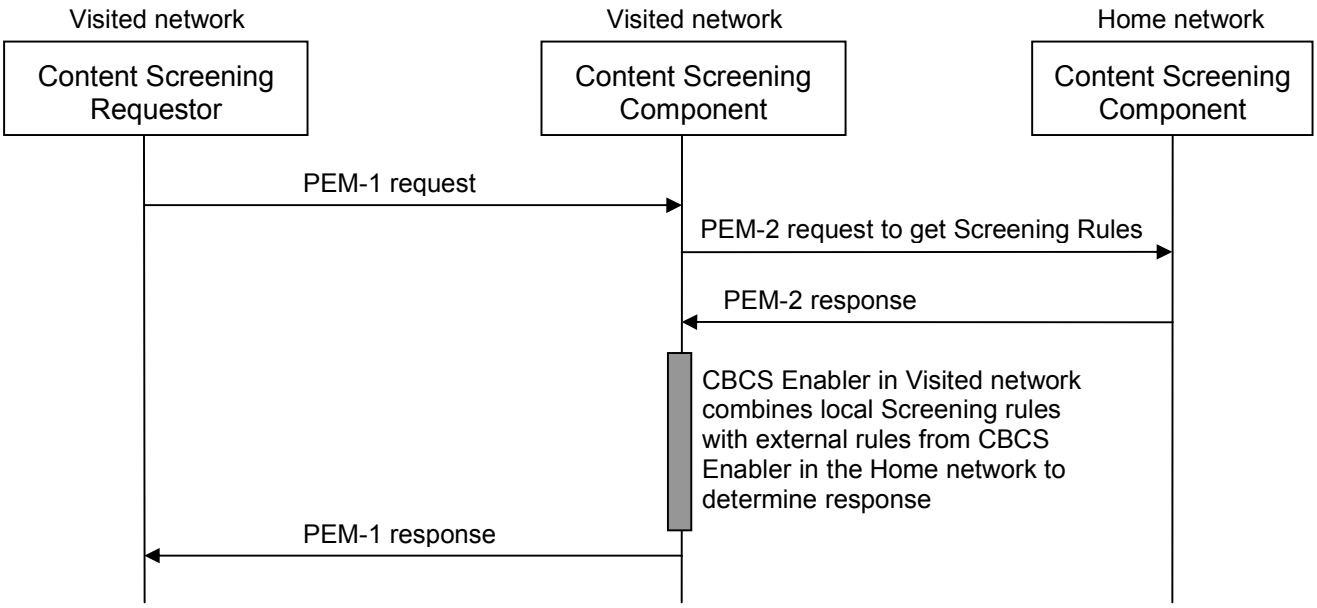

Figure 9 Combined screening in Visited network

5.4.6.4 Combined screening in Home network

This scenario is similar to the scenario in section 5.4.6.3, except that the roles of the CBCS Enabler in the Home and Visited networks are reversed.

The difference between the scenarios in figures 9 and 10 is essentially a difference in deployment strategy. The scenario in Figure 10corresponds to a Home network centric approach to service control, as is common in current cellular networks and CAMEL. The scenario in Figure 9 could apply in situations where Content screening is required in the Visited network.

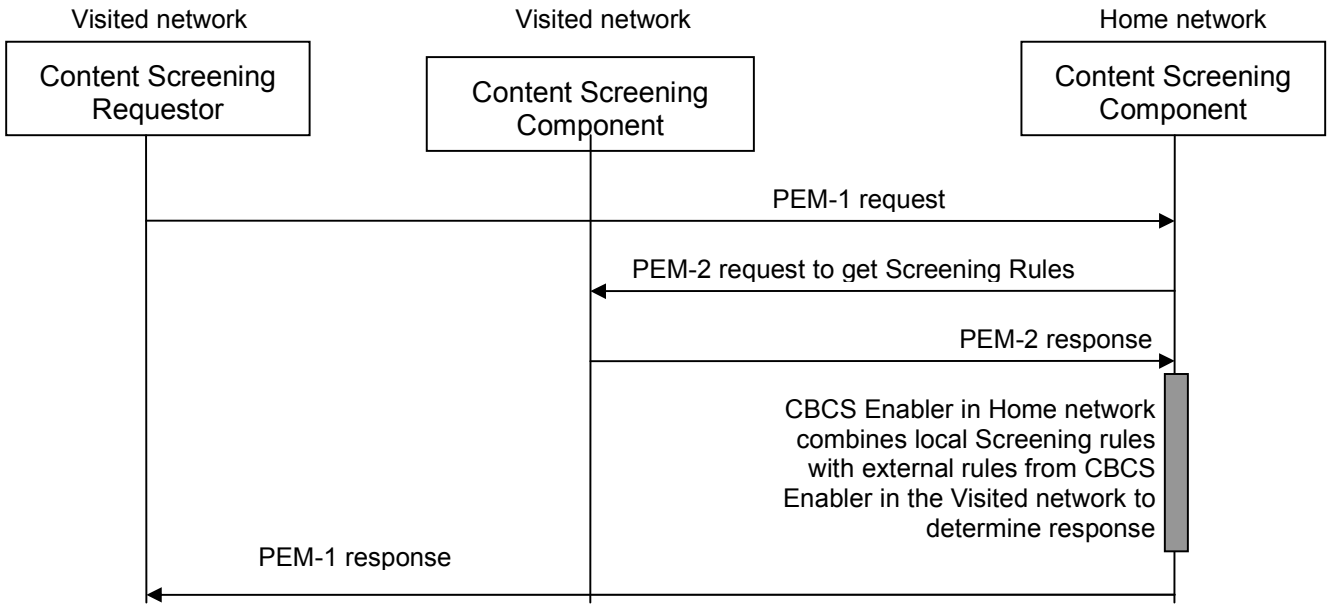

Figure 10 Combined screening in Home network

5.4.6.5 PEM-1 delegation to Home network

In the scenarios of sections 5.4.6.3 and 5.4.6.4, an external Policy is passed *by reference* in the CBCS.PEM-1 request.

The CBCS.PEM-1 protocol also allows external Policies to be passed *by value*. This gives rise to an alternative scenario called *PEM-1 delegation*. Figure 11 illustrates this scenario.

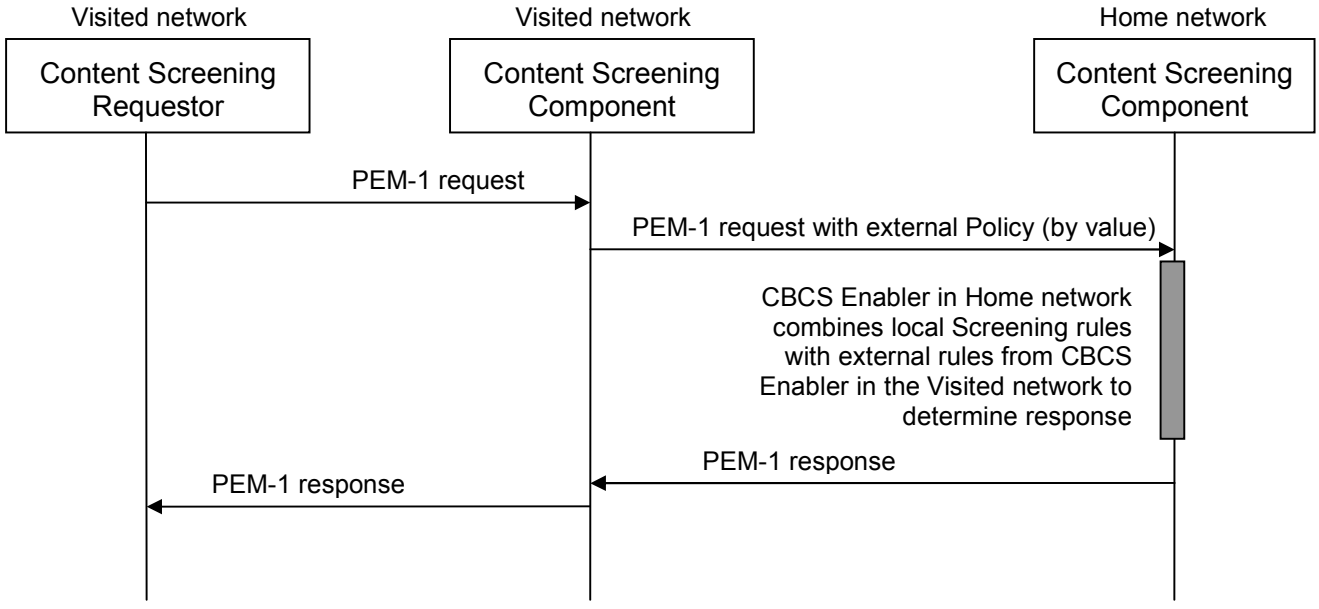

Figure 11 PEM-1 delegation to Home network

In the scenario of Figure 11, when the CBCS Enabler of the Visited network receives a CBCS.PEM-1 request, it delegates the request to the CBCS Enabler of the Home network. In the delegated request it adds an external Policy consisting of the Screening Rules it wants the CBCS Enabler in the Home network to execute.

5.4.6.6 PEM-1 delegation to Visited network

It is also possible to reverse the roles of the CBCS Enabler in Home network and Visited network in the PEM-1 delegation scenario of section 5.4.6.5. Doing so results in the PEM-1 delegation scenario shown in Figure 12.

The difference between the scenarios in figures 11 and 12 is mainly a question of deployment. The scenario of Figure 11 puts control of the content screening activity in the Home network, while the scenario of Figure 12 puts the Visited network in control. However, both scenarios use the same delegation mechanism.

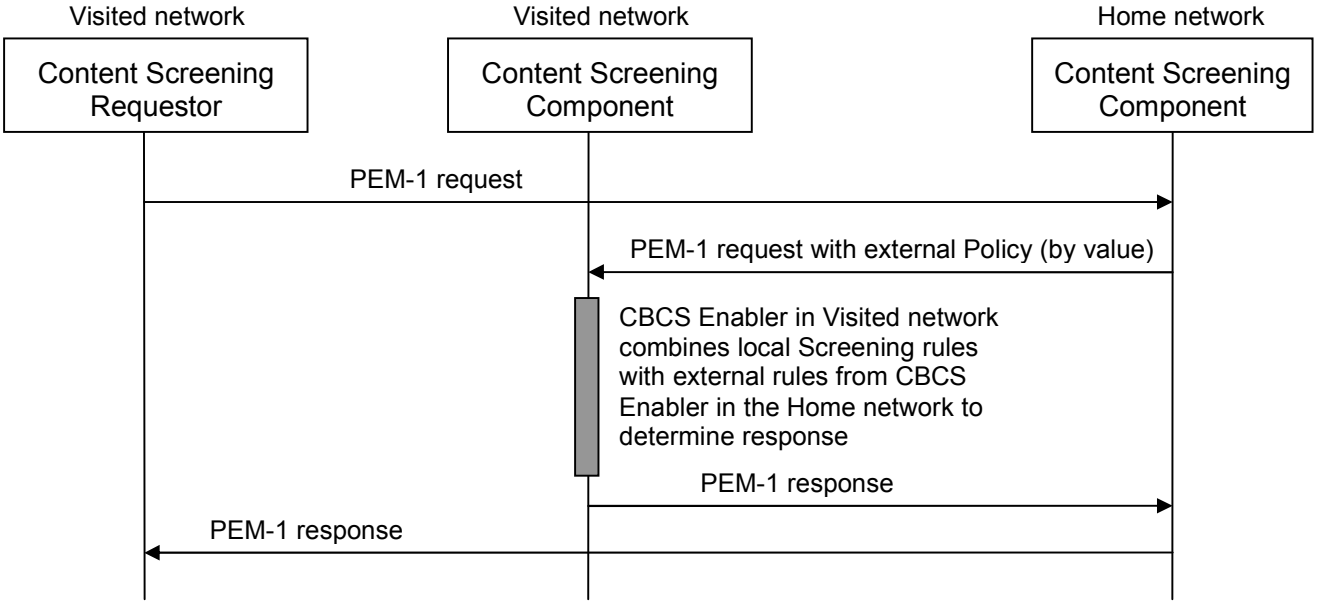

Figure 12 PEM-1 delegation to Visited network

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 Version OMA-AD-CBCS-V1_0_0	4 Jan 2006	n/a	Initial version using template OMA-Template-ArchDoc-20050929-I
	7 Apr 2006	2.1, 3.2, 3.3, 5.1, 5.2, 5.3	Implementation of OMA-ARC-2006-0098R03-CBCS-PEEM-dependency, update of references and implementation of OMA-Template-ArchDoc-20060405-D.
	8 Aug 2006		Implementation of OMA-ARC-2006-0168R02-CBCS-AD-introduction-diagram, OMA-ARC-2006-0211R06-CBCS-AD-introduction-diagram, OMA-ARC-2006-0244R02-Alternative_to_split_non_split_issues.
	23 Aug 2006		Implementation of OMA-ARC-2006-0280R04-INP_CBCS_Flows (incl. agreed change of 'policy' into 'rules' in Figure 5), OMA-ARC-2006-0275R01-INP_CBCS_AD_Cleanup, OMA-ARC-2006-0274R01-INP_CBCS_AD_Security, OMA-ARC-2006-0273-INP_CBCS_AD_Planned-Phases, OMA-ARC-2006-0272R01-INP_CBCS_AD_Scope
Draft Version OMA-AD-CBCS-V1_0_1	28 Aug 2006		Re-implementation of OMA-ARC-2006-0287-INP_CBCS_AD_Further_clean_up. Note that version OMA-AD-CBCS-V1_0_1-20060823-D should be ignored due mix up in file naming, versioning issues, and lack of change marks
	5 Jan 2007		OMA-ARC-2006 – 0318R02 – Editorial fixes as per ADDR OMA-ARC-2006 – 0373R05 – management interaction with Content Categorization Component OMA-ARC-2006 – 0381R01 – example to resolve identity of end user OMA-ARC-2006 – 0388 Section 5 reorganized OMA-ARC-2006-0390R2 – text for figure 1 OMA-ARC-2006-0421R01 – CBCS roaming
	12 Jan 2007		OMA-ARC-2007-0001 – text for PEM-2 interface Deletion of heading 5.4.5 that was introduced as an editorial (not shown in change marks)
	16 Jan 2007		History table updated to align with issued ADs
	16 Mar 2007	all	Update according to ADRR resolutions made at the OMA San Francisco meeting and conference calls up to March 20th 2007, as documented in OMA-ADRR-CBCS-V1_0_0-20070313-D
Draft Version OMA-AD-CBCS-V1_0	13 Apr 2007	5.3.4, 5.4.2, 5.4.3	Update according to ADRR resolutions made in the conference calls of February 20, March 6, 13, 20, 27 and April 3, 2007.
	17 Apr 2007	5.2, 5.3, 5.4.5	Updated according to the revisions approved during the ARC meeting in Frankfurt on 16-19th April 2007. Rolled back the renaming of CBCS-3 to CBCS-2 and the renaming of CBCS-2 to PEM-2.
	4 May 2007	3.3, 5.2, 5.3.5, 5.4.5	Corrected definition of "URI" in section 3.3, corrected figures 1 and 8, minor spelling corrections
	26 Jun 2007		Clean version without revision marks, after re-review and agreement of the ADRR.
	30 Aug 2007	5.2, 5.3.1, 5.3.2, 5.3.5, 5.3.8, 5.4.4; all figures	Update according to agreed change request OMA-ARC-2007-0185-CR_CBCS_AD_editorial, which requested mostly editorial fixes. All figures re-drawn as embedded Microsoft Word picture objects.
	5 Feb 2008	5.4.5	Figure 6 corrected as per comments made on the conference call of January 8th 2008
	26 Feb 2008	5.4.6	Addition of section 5.4.6 according to agreed change request OMA-ARC-CBCS-2008-0003-CR_Roaming_Scenarios_for_AD, with some syntactic corrections to align terminology and figure captions

Document Identifier	Date	Sections	Description
	18 Aug 2008	1, 2.1, 3.3, 4.1, 5.1, 5.2, 5.3.1, 5.3.3, 5.3.6, 5.3.7, 5.3.8, 5.4.2, 5.4.5, 5.4.6	Revision according to the agreed comments accumulated in consistency review report OMA-CONRR-CBCS-V1_0-20080812-D
	08 Sep 2008	All	Editorial fixes: 2008 copyright References and definitions sorted alphabetically Cross-references fixed History boxfixed.
Candidate Version: OMA-AD-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
Draft Version: OMA-AD-CBCS-V1_0	03 Feb 2009	All	Editorial fix: 2009 copyright Implemented agreed change: OMA-ARC-CBCS-2009-0001-CR_change_interface_names_in_AD_for_reuse
Candidate Version: OMA-AD-CBCS-V1_0	12 Feb 2009	All	Re-approved as Candidate by TP: OMA-TP-2009-0079-INP_CBCS_V1_0_ERP_for_Candidate_re_Approval