Mobile Spam Reporting Requirements

Candidate Version 1.0 – 11 Aug 2009

Open Mobile Alliance

OMA-RD-SpamRep-V1_0-20090811-C

Contents

Figures

Tables

1. Scope (Informative)

This document defines the requirements for Spam Reporting (SpamRep) functionality. A set of functional requirements is described for an enabler that allows Users to designate received Content as Spam, and send a report to an external entity containing information about that Content that may be used by the external entity to prevent further instances of unwanted Content from reaching Users.

The scope of this enabler and this document covers only the SpamRep message format and interface between User Device and the external recipient entity. The User interface is out of scope, as is any functionality of the external entity beyond the SpamRep/Device interface.

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

[OMADICT] "Dictionary for OMA Specifications", Version 2.7, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7, URL:http://www.openmobilealliance.org/

[IETF_Email_Rep] "An Extensible Format for Email Feedback Reports", draft-shafranovich-feedback-report-06, IETF, January 2, 2009, URL: http://tools.ietf.org/html/draft-shafranovich-feedback-report-06.

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

By-Fingerprint	The Spam Report contains a Fingerprint of the Spam message which can be used to identify or retrieve the Spam message Content from the operator’s database.
By-Value	The Spam Report contains the Spam message content
Content	In the context of the SpamRep Enabler, Content refers to messages, files, and/or media streams that are transmitted to a Device in an arbitrary way (i.e., via SMS, MMS, IM, Video Share, email, etc.)
Fingerprint	An arbitrary collection of one or more message descriptors that are derived from and can represent a message. Each message descriptor may represent an aspect or portion of a message. Examples of a descriptor include a hash representing a URL contained within a message, and the number of words in the fourth line of a message. An example of a Fingerprint is a collection of URL hashes and the number of words in the fourth line.
Local Spam Box	The box that contains the messages delivered to the user device even if there is a history of Spam reporting for the message Spam Sender and/or the message before. The messages may contain a Spam flag to indicate the possibility of this message being a Spam. This box may contain the messages filtered by Spam policy (e.g. Spam word).
Network Spam Box	The box that contains the blocked messages which were prohibited from being sent to the user device. The messages may expire after certain amount of time to save the server storage. For the unexpired messages, the User is able to request the current blocked message list in the Spam Box.
Reporter	The User that initiates and sends a Spam Report
Spam	In the context of the SpamRep Enabler, Spam is defined as any Content received by a User that may be considered unwanted and/or inappropriate by the message recipient and/or operator
Spam Report	A message transmitted between the SpamRep Client and SpamRep Server containing information about the Content and originator of an unsolicited and unwanted received message, as designated by a User
Spam Sender	The purported source of the Spam Content. This could be the spammer, an innocent device infected with a virus that causes it to send Spam, an individual or organization sending Content in good faith that the recipient considers Spam, or a false identity assumed by the spammer.
SpamRep Client	An entity within the SpamRep architecture that composes and transmits Spam Reports upon invocation by a User or automatically based on Service Provider policy
SpamRep Server	An entity within the SpamRep architecture that receives Spam Reports transmitted by a SpamRep Client

3.3 Abbreviations

OMA	Open Mobile Alliance

4. Introduction (Informative)

Mobile messaging abuse is rapidly increasing and is becoming a business threat to Mobile Network Operators, Service Providers, and other segments of the Mobile Network industry. Subscribers are increasingly receiving unsolicited and unwanted text and multimedia messages, commonly referred to as Spam. Various methods exist today to combat mobile Spam, including sender blacklists and network based content filters. In order to be effective, these methods require a way to identify spammers and update blacklists and content filter rules. Subscriber feedback is a very effective, proven method for identifying Spam as long as the feedback contains sufficient information to identify the message source and/or Content. At this time a parallel effort to standardise feedback for email is underway in the IETF. An Internet Draft, which is not directly applicable to many forms of mobile messaging, is described in [IETF_Email_Rep]. The IETF effort appears to primarily address inter-ISP communication of messaging abuse, whereas the OMA SpamRep effort is expected to primarily address reporting of messaging abuse from a User.

This document describes the use cases and defines the functional requirements for the SpamRep Enabler.

5. SpamRep release description (Informative)

Spam Reporting is intended to help the Mobile Network Operator to reduce the load on their network caused by Spammers sending unsolicited/unwanted messages to the operator's Users/Subscribers. The reduction in the number of Spam messages will also improve the User's/Subscriber's experience on the operator's network.

The SpamRep Enabler focuses on the Spam Report format and the interface for the delivery of this report. The user's device will be provisioned with the address of the report collection node in the operator's network, but how this provisioning is done is outside the scope of the enabler. The mechanisms used to initiate a Spam Report and the actions taken by the operator's systems based on the Spam Reports are also outside the scope of the enabler.

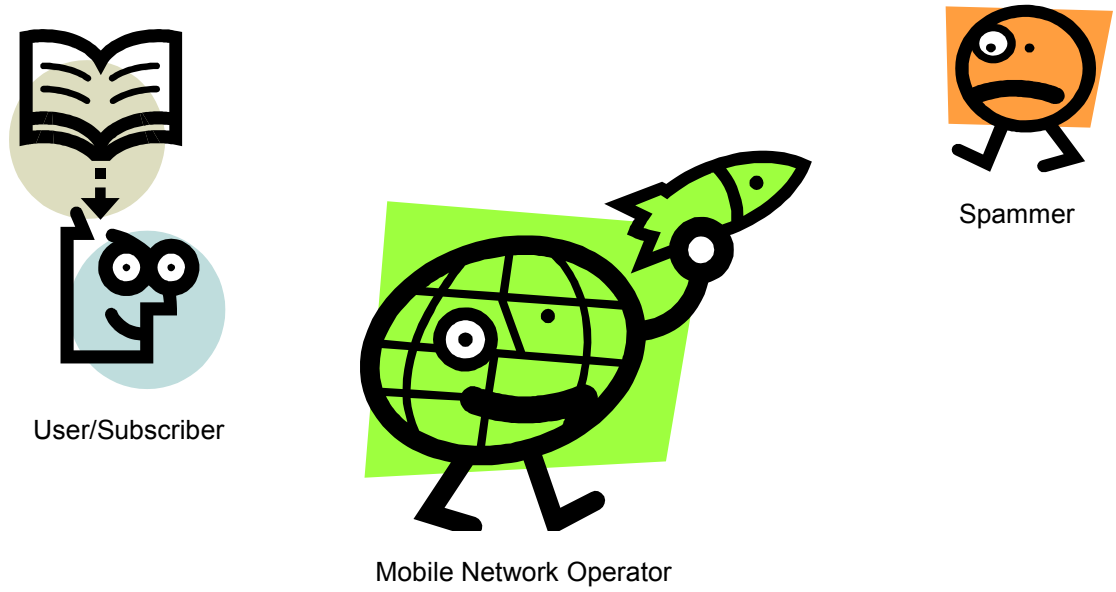

Figure 1: Actors Diagram

5.1 Version 1.0

The SpamRep 1.0 Enabler defines a standardised protocol and message format for forwarding Spam messages to a network collection point.

6. Requirements (Normative)

6.1 Modularisation

The Spam Reporting requirements can be grouped into the following major functional modules:

1) General Enabler Requirements: These are requirements that specify basic high-level functions of the overall enabler
2) Report Characteristics: These are requirements that specify what the individual Spam Reports must contain and/or what functions the Spam Reports must perform.
3) Client Functions: These include client-side requirements as well as usability
4) Privacy: Requirements that explicitly deal with protecting information about the various SpamRep actors, such as User, Spam Sender, and Reporter
5) Policy: All requirements that support enforcement of Service Provider Policy
6) Security: Requirements dealing with authentication, authorization, data integrity, etc.
7) Charging: Requirements that enable implementation of Service Provider charging policies.

6.2 High-Level Functional Requirements

Label	Description	Release	Functional module
SPAMREP-HLF-001	The SpamRep Enabler SHALL support the creation of Spam Reports	SpamRep 1.0	General
SPAMREP-HLF-002	The SpamRep Enabler SHALL support the transfer of Spam Reports from the SpamRep Client to the SpamRep Server	SpamRep 1.0	General
SPAMREP-HLF-003	The SpamRep Enabler SHALL support SpamRep Clients reporting Spam to the SpamRep Server By-Reference in addition to By-Value.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-004	The SpamRep Enabler SHALL support a means of uniquely identifying each Spam Report as a Spam Report.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-005	The SpamRep Enabler SHALL support a means of reporting the date and time of a Spam Report's submission.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-006	The SpamRep Enabler SHALL support the inclusion of data that uniquely and consistently (i.e., with an identity that persists across multiple reports by the same Reporter) identifies the Reporter.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-007	The SpamRep Enabler SHALL support the inclusion of Content from the original message deemed abusive by the Reporter.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-008	The SpamRep Enabler SHOULD support the inclusion of data describing the delivery path of the abusive message. **Informational Note**: Spam often has spoofed sender identity; inclusion of information which supports identification of the source of Spam is helpful, but this is highly dependent on the messaging environment. This requirement is optional because this information may not be available in all cases, but if available the information SHOULD be included.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-009	The SpamRep Enabler SHALL support the inclusion of data that identifies the actual or purported originating address of the abusive message.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-010	The SpamRep Enabler SHALL support the inspection of a Spam Report by the entity that receives it..	SpamRep 1.0	Report Characteristics

SPAMREP-HLF-011	The SpamRep Enabler SHOULD NOT prevent abstraction of data from the Spam Report for ex post facto analysis and use, e.g., correlation of Spam Reports, law enforcement. **Informational Note**: Systems receiving Spam Reports may wish to abstract data for a number of reasons, such as identifying patterns of abuse. This requirement is not mandatory largely due the impracticality of anticipating all ways in which SpamRep data may be abstracted in operational environments.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-012	The SpamRep Enabler SHALL support forwarding of Spam Reports to another entity (e.g. another operator or provider) in a manner that allows the forwarder to identify both the Reporter and the forwarder.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-013	The SpamRep Enabler SHALL support a means of reporting the date and time, if available, of the original message that resulted in the Spam Report. **Informational Note**: Information such as date and time may not be available in various messaging service and operator environments, but if available the information SHOULD be included.. Moreover the date and time may be associated with different events in different transmission environments. The intent is to allow for inclusion of any information which may be helpful in identifying abuse, while not requiring inclusion of information which may not be available in certain contexts.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-0014	The SpamRep Enabler SHALL support the reporting of Spam transmitted via SMS, MMS, email, IM, and Video Share.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-0015	The SpamRep message format SHALL support extension to provide reporting of Spam for messaging services beyond those required in the SpamRep 1.0 release.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-016	The SpamRep Enabler SHALL support a request from the SpamRep Client that a list of any messages quarantined (e.g., as spam) by a messaging enabler in the network be transmitted to the mobile device	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-017	The SpamRep Enabler SHALL allow a User to send a request to the SpamRep Server to unblock the message sender (e.g., allowing messages from the unblocked sender to be recovered from the Network Spam Box or Local Spam Box, and future messages to be received)	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-018	The SpamRep Enabler SHALL support the inclusion of the following report types indicating the type of abuse: Spam, Phishing, Malware (e.g., Virus/Spyware), Not Spam, Miscategorized, Unauthorized Message (violation of a security policy), Sender Authentication Failure, Other, Unspecified.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-019	The SpamRep Enabler SHALL support the following report types indicating actions: Block Sender, Unblock Sender, Opt Out	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-020	The SpamRep Enabler SHALL support SpamRep Clients which provide only an arbitrary subset of the report types defined by the SpamRep Enabler. **Informational Note**: Several types of Spam Reports may be inappropriate in a given messaging environment, such as "Block Sender" if it is not supported by the messaging system. Additionally, MNO policies may dictate the exclusion of certain report types, such as "Unspecified," if an MNO chooses to require a reporter to specify the type of abuse.	SpamRep 1.0	General
SPAMREP-HLF-021	The SpamRep Enabler SHALL support extension of report types indicating the type of abuse beyond any initially-defined types	SpamRep 1.0	Report Characteristics

SPAMREP-HLF-022	The SpamRep Client SHOULD support inclusion of only partial Content of the message (e.g., selected body parts in a MIME formatted message) deemed Spam by the Reporter in the Spam Report. **Informational Note**: it is understood that not all clients will have this capability.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-023	The SpamRep message format SHALL support inclusion of only partial Content of the message (e.g., selected body parts in a MIME formatted message) deemed Spam by the Reporter.	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-024	The SpamRep Enabler SHALL support obtaining the Reporter's permission to share Spam Reports with third parties which reside outside of SpamRep Server's network.	SpamRep 1.0	Privacy
SPAMREP-HLF-025	The SpamRep Client SHALL support Reporter control of whether to protect or share the Reporter's personal information in the Spam Report when it is shared with third parties by the SpamRep Server.	SpamRep 1.0	Privacy
SPAMREP-HLF-026	The SpamRep Client SHALL support informing the Reporter of the list of third parties with which the SpamRep Server is allowed to share the Spam Report.	SpamRep 1.0	Privacy
SPAMREP-HLF-027	The SpamRep Enabler SHALL NOT prevent the obscuration or deletion of personal information to protect the Reporter's privacy depending on the Reporter's selection in the Spam Report when it is forwarded by the SpamRep Server to other parties.	SpamRep 1.0	Privacy
SPAMREP-HLF-028	The SpamRep Enabler SHALL be able to report Spam messages according to the Spam Report policy specified by the Service Provider.	SPAMREP 1.0	Policy
SPAMREP-HLF-029	The SpamRep Enabler SHALL support Spam report policies defining various report settings (e.g. By Value, By Reference, partial content, full content, By-Fingerprint, etc.) per abuse type (e.g. Spam, phishing, malware, etc.) and per Content or message type (e.g. SMS, MMS, email, etc.).	SpamRep 1.0	Policy
SPAMREP-HLF-030	The SpamRep Enabler SHALL support reporting Spam By-Fingerprint	SpamRep 1.0	Report Characteristics
SPAMREP-HLF-031	The SpamRep Enabler SHALL support Spam report policies defining SpamRep Client and Server behaviour regarding Reporter control of personal information in and sharing of Spam Reports with third parties (e.g. Reporter's permission, control of Reporter's personal information, and allowed third parties).	SpamRep 1.0	Policy

Table 1: High-Level Functional Requirements

6.2.1 Security

Label	Description	Release	Functional module
SPAMREP-SEC-001	The SpamRep Enabler SHOULD, support capture of information to authenticate the Reporter. **Informational Note**: An underlying authentication mechanism, such as that provided by SMS, may provide reporter authentication. Authentication may not be practical in all circumstances and over all bearers.	SpamRep 1.0	Security

SPAMREP-SEC-002	The SpamRep Enabler SHOULD, where practical, support capture of information to identify the original sender of the abusive message. **Informational Note**: Sender identity is often spoofed in Spam. This requirement is intended to facilitate the inclusion of information that may help provide the actual (as opposed to purported) sender identity. This information may not be available or practical to include in all circumstances and over all bearers.	SpamRep 1.0	Security
SPAMREP-SEC-003	The SpamRep Enabler SHOULD support mechanisms to prevent DoS attacks.	SpamRep 1.0	Security

Table 2: High-Level Functional Requirements – Security Items

6.2.1.1 Authentication

Label	Description	Release	Functional module
SPAMREP-AUTH-001	The SpamRep Enabler SHALL allow all SpamRep Clients to authenticate the SpamRep Server.	SpamRep 1.0	Security

Table 3: High-Level Functional Requirements – Authentication Items

6.2.1.2 Authorization

Label	Description	Release	Functional module
SPAMREP-AUR-001	The SpamRep Enabler SHALL support authorization of Reporters.	SpamRep 1.0	Security

Table 4: High-Level Functional Requirements – Authorization Items

6.2.1.3 Data Integrity

Label	Description	Release	Functional module
SPAMREP-INTE-001	The SpamRep Server SHALL support Spam Report message integrity protection.	SpamRep 1.0	Security
SPAMREP-INTE-002	The SpamRep Client SHOULD support Spam Report message integrity protection **Informational Note**: SHOULD is used instead of SHALL as some clients may not be able to support it.	SpamRep 1.0	Security

Table 5: High-Level Functional Requirements – Data Integrity Items

6.2.1.4 Confidentiality

Label	Description	Release	Functional module
SPAMREP-CONF-001	The SpamRep Server SHALL support confidentiality protected communication with SpamRep Client when deemed necessary (e.g., to keep report message private).	SpamRep 1.0	Security

SPAMREP-CONF-002	The SpamRep Client SHOULD support a confidentiality protected communication with the SpamRep Server when deemed necessary (e.g., to keep report message private). **Informational Note**: SHOULD is used instead of SHALL as some clients may not be able to support it.	SpamRep 1.0	Security

Table 6: High-Level Functional Requirements – Confidentiality Items

6.2.2 Charging

Label	Description	Release	Functional module
SPAMREP-CHG-001	The SpamRep Enabler SHALL support classification of a Spam Report as a chargeable or non-chargeable event.	SpamRep 1.0	Charging
SPAMREP-CHG-002	The SpamRep Enabler SHALL provide enough information in the Spam Report to allow for the correlation of Spam Reports with the original Spam message. **Informational Note**: This can be used as a basis for crediting back charges incurred by receiving or sending Spam messages.	SpamRep 1.0	Report Characteristics
SPAMREP-CHG-003	The SpamRep Enabler SHALL comply with operator policies that may restrain or condition the transmission of Spam Reports depending on the charging characteristics of the available transport networks. **Informational Note**: This is intended to allow for flexible MNO reporting policies, such as suppression of or user notification of possible charges for Spam Reports while roaming. For example, transmission of an IP-based report of SMS Spam may be prohibited while roaming.	SpamRep 1.0	Charging

Table 7: High-Level Functional Requirements – Charging Items

6.2.3 Administration and Configuration

No requirements identified

6.2.4 Usability

Label	Description	Release	Functional module
SPAMREP-USE-001	The SpamRep Enabler SHALL support User activation of the SpamRep functionality	SpamRep 1.0	Client Functions
SPAMREP-USE-002	The SpamRep Enabler SHALL provide the capability to notify the User whether a Spam Report was or was not successfully transmitted	SpamRep 1.0	Client Functions
SPAMREP-USE-003	The SpamRep Enabler SHALL support the Reporter to inquire about the status of Spam Reports.	SpamRep 1.0	Client Functions
SPAMREP-USE-004	The SpamRep Enabler SHALL support notifying the reporter about the status of a Spam Report.	SpamRep 1.0	Client Functions
SPAMREP-USE-005	The SpamRep Enabler SHALL support operator-defined Spam report policies governing whether or not to allow inquiry and/or notifications about the status of Spam Reports by the reporter.	SpamRep 1.0	Policy

SPAMREP-USE-006	The SpamRep Enabler SHOULD support automatic activation of the SpamRep functionality, based on Service Provider policy **Informational Note**: it is not a mandatory requirement for the client	SpamRep 1.0	Policy

Table 8: High-Level Functional Requirements – Usability Items

6.2.5 Interoperability

No requirements identified.

6.2.6 Privacy

Label	Description	Release	Functional module
SPAMREP-PRV-001	The SpamRep Enabler SHALL be capable to provide necessary mechanisms to keep the reporting activities private upon users' request	SpamRep 1.0	Privacy
SPAMREP-PRV-002	To protect privacy, the SpamRep Enabler SHALL support full and partial suppression of the body of the Spam message which might be contained within a Spam Report.	SpamRep 1.0	Privacy

Table 9: High-Level Functional Requirements – Privacy Items

6.3 Overall System Requirements

No requirements identified.

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-SpamRep-V1_0	17 Dec 2008	1, 3.2, 4	Initial draft RD
	10 Mar 2009	9.2.2.2, 11.3	Incorporates input to committee: OMA-REQ-SpamRep-2009-0001R01-CR_Content_Blocking_Use_Case OMA-REQ-SpamRep-2009-0003-CR_Spam_Report_By_Reference.doc OMA-REQ-SpamRep-2009-0004R01-CR_Populating_introductory_sections.zip OMA-REQ-SpamRep-2009-0006R01-CR_GenReq01 OMA-REQ-SpamRep-2009-0007R02-CR_GenReq02 OMA-REQ-SpamRep-2009-0008R01-CR_GenReq03 OMA-REQ-SpamRep-2009-0010R01-CR_MsgSvc OMA-REQ-SpamRep-2009-0012-CR_Definitions OMA-REQ-SpamRep-2009-0013R01-CR_Authorization
	01 Apr 2009	2.2, 3.2, 4, 6.2, 6.2.1.1, 6.2.1.4, B.3+, B.4+	Incorporates input to committee: OMA-REQ-SpamRep-2009-0002R02-CR_Feedback_Types OMA-REQ-SpamRep-2009-0005R02-CR_Network_Spam_Box_Use_Case OMA-REQ-SpamRep-2009-0014R02-CR_Security_Requirements
	16 Apr 2009	6.2, 6.2.1.3, 6.2.6, B5.x, B6.x	Incorporates input to committee: OMA-REQ-SpamRep-2009-0015R01-CR_integrity_privacy_requirements OMA-REQ-SpamRep-2009-0017R02-CR_Report_Of_Partial_Spam_Content_Use_Case OMA-REQ-SpamRep-2009-0021R01-CR_User_Confirmed_Spam_Report_Sharing_UC OMA-REQ-SpamRep-2009-0022-CR_Policy_requirements OMA-REQ-SpamRep-2009-0023-CR_Unauth_Feedback_Type
	29 Apr 2009	3.2, 4, 6.2, 6.2.4, 6.2.6, B.7.x, B.8.x	Incorporates input to committee: OMA-REQ-SpamRep-2009-0009R05-CR_GenReq04 OMA-REQ-SpamRep-2009-0016R02-CR_Acquire_SPAM_Report_Status_Use_Case OMA-REQ-SpamRep-2009-0019R03-CR_Spam_Report_By_Fingerprint_of_Spam_Content OMA-REQ-SpamRep-2009-0024-CR_Sharing_Policy OMA-REQ-SpamRep-2009-0027R01-CR_SpamRep_Client_Invocation_Clarification OMA-REQ-SpamRep-2009-0028-CR_SpamRep_RD_Cleanup
	26 May 2009	6.1, 6.2, 6.2.1, 6.2.1.1, 6.2.1.2, 6.2.1.3, 6.2.1.4, 6.2.2, 6.2.1.4, 6.2.6	Incorporates input to committee: OMA-REQ-SpamRep-2009-0030-CR_RD_Modules Change Title of document Remove template boilerplate Remove paragraphs 5.2 and 5.2.1 Remove tables in paragraphs 6.2.3, 6.2.5, and 6.3 and add “No requirements identified” Delete Appendix C Update TOC, TOF, TOT

Document Identifier	Date	Sections	Description
	26 Jun 2009	3.2, 5.1, 6.1 6.2 6.2.2 6.2.4 B 1.1, B2, B 2.1	Incorporates input to committee: OMA-REQ-SpamRep-2009-0033R01-CR_Section_3.2 OMA-REQ-SpamRep-2009-0039R01-CR_RDRR_A011_A014_A015 OMA-REQ-SpamRep-2009-0043R01-CR_RDRR_A056_A057_A059 OMA-REQ-SpamRep-2009-0044R01-CR_RDRR_A060_A061_A063 OMA-REQ-SpamRep-2009-0045-CR_RDRR_A065_A066 OMA-RDRR-SpamRep-V1_0-20090623-D
	01 July 2009	6.2, 6.2.1, 6.2.1.3, 6.2.1.4	Incorporates input to committee: OMA-REQ-SpamRep-2009-0040R01-CR_RDRR_A021_A031_A034 OMA-REQ-SpamRep-2009-0041R01-CR_RDRR_A040_A043_A045 OMA-REQ-SpamRep-2009-0042R01-CR_RDRR_A048_A050_to_54
	16 July 2009	1, 3.2, 5, 6.1, 6.2, 6.2.1, 6.2.2, B 1.4.1, B 5.2, B7.1, B 8.1.3, B 8.1.5, plus Global	Incorporates input to committee: OMA-REQ-SpamRep-2009-0046R01-CR_Address_Various_SpamRep_RDRR_Comments_Batch_1 OMA-REQ-SpamRep-2009-0047-CR_Address_Various_SpamRep_RDRR_Comments–Batch_2 OMA-REQ-SpamRep-2009-0048-CR_RDRR_A029 Plus agreements made in email and Conference Calls
	17 July 2009	All	Editorial clean-up
Candidate Version OMA-RD-SpamRep-V1_0	11 Aug 2009	N/A	Status changed to Candidate by TP ref # OMA-TP-2009-0343-INP_SpamRep_V1_0_RD_for_Candidate_Approval

Appendix B. Use Cases (Informative)

B.1 Content Based Blocking

B.1.1 Short Description

A prankster sends an SMS messages promising $20 credit from the mobile carrier to any user who forwards the message to 10 other mobile subscribers. One SMS end user (human recipient) receives the Spam SMS and becomes suspicious. He/she identifies the message as Spam and selects "Report Spam" from device menu. The SpamRep Client, acting on end user menu navigation, composes a Spam Reportmessage and transmits to the pre-provisioned report collection node in the operator's network.

(Note: the following paragraph describes functionality that is out of scope of the SpamRep Enabler, but is included as narrative to provide context for use of the SpamRep Enabler):

Several additional SMS end users report similar Spam messages as above. The operator's network processors aggregate feedback reports and automatically generate an "Anti-Spam" rule to identify similar messages. The anti-Spam rule is deployed to policy-enforcement nodes in the operator's network, blocking subsequent messages and viral rate-explosion is prevented.

B.1.1.1 Actors

- User/Subscriber. The User/Subscriber possesses a mobile device that can receive SMS messages, and subscribes to an SMS messaging service from the Mobile Network Operator
- Mobile Network Operator. The MNO provides the SMS messaging service and the network entity to which the User sends the Spam Report
- Spammer. An individual who wishes to cause trouble to the MNO and/or subscribers by sending fraudulent SMS messages

B.1.1.2 Pre-Conditions

- User/Subscriber has subscribed to an SMS service
- User's device is provisioned with a SpamRep Client and the User is familiar with the use of the client
- MNO provides SMS service
- MNO has a network entity that can receive Spam reports and act on them

B.1.1.3 Post-Conditions

- User feels satisfied as an active participant in the war against Spam
- MNO has identified the Spam message and the Spammer and has blocked further proliferation of the Spam message

B.1.1.4 Normal Flow

1) The Spammer sends SMS messages to random subscribers, indicating recipients will receive $20 credit from the MNO if the message is forwarded to 10 subscribers.

2) Recipient User becomes suspicious and invokes the "Report Spam" function on her device

3) User's device creates a SpamRep message containing relevant information about the suspect SMS (e.g., originator, message body, etc.)

4) SpamRep Client sends the message to the operator's network entity, the address of which has been pre-provisioned in the device.

(Note: The remainder of this flow – steps 5 onward – are out of scope of the SpamRep Enabler but are included to illustrate a notional usage scenario.)

5) The network entity receives the User's Spam Report, along with additional reports from other recipients

6) The network entity aggregates the received reports, determines the Content of the Spam message, and traces the source back to the originating Spammer.

7) The network entity generates an update to the MNO's content filter to remove all messages with the designated text string contained in the Spam SMS messages.

8) The network entity generates an update to the MNO's blacklist to deny transmission of SMS messages from the known Spammer

.

B.1.2 Market benefits

By reducing Spam from the network the MNO derives multiple benefits. Non-revenue-generating network traffic is reduced, which leads to reduced operating costs. Billing disputes are reduced along with their associated Customer Care costs. Customer satisfaction is increased, due both to the reduction in unwanted and potentially offensive messages and also due to the fact that the Customer is able to play an active role in preventing these messages.

B.2 By Reference

B.2.1 Short Description

Copies of messages intended for the Mobile Network Operator's users are retained temporarily within the operator's servers. A message passes through the operator's servers and is received by the user (human recipient) on their handheld device. The user judges it to be Spam and selects "Report Spam" from a device menu. The SpamRep Client, acting on the user's menu navigation, composes a Spam Report message containing a reference to the original message instead of the Content of the original message and transmits to the pre-provisioned report collection node in the operator's network. The report collection node uses the reference from the Spam Report message to retrieve the Content of the original message from the database of retained messages for further processing. Retained messages which never end up being identified as Spam by their recipient users are purged from the operator's servers after an operator defined delay or when space is needed for new messages.

B.2.1.1 Actors

- User/Subscriber. The User/Subscriber possesses a mobile device that can receive messages, and subscribes to a messaging service from the Mobile Network Operator

- Mobile Network Operator. The MNO provides the messaging service and the network entity to which the User sends the Spam Report

- Spammer. An individual who sends unsolicited and unwanted messages to Users on the MNO's network.

B.2.1.2 Pre-Conditions

- User/Subscriber has subscribed to a messaging service
- User's device is provisioned with a SpamRep Client and the User is familiar with the use of the client
- MNO provides messaging service
- MNO has a network entity that can receive Spam reports and act on them

B.2.1.3 Post-Conditions

- MNO has identified the Spam message and the Spammer

B.2.1.4 Normal Flow

1) The Spammer sends unwanted messages to random subscribers.
2) The operator's messaging server retains a copy of messages going to subscribers.
3) A message from the Spammer arrives on the User's handheld.
4) Recipient User invokes the "Report Spam" function on her device for the unwanted message
5) User's device creates a SpamRep message containing a reference to the original Spam message.
6) SpamRep Client sends the message to the operator's network entity, the address of which has been pre-provisioned in the device.
7) The network entity receives the User's Spam Report and uses the reference within to retrieve the original message Content from its database of retained messages.

B.2.1.5 Alternative Flow (Original Message Unavailable)

1) The Spammer sends unwanted messages to random subscribers.
2) The operator's messaging server retains a copy of messages going to subscribers.
3) A message from the Spammer arrives on the User's handheld.
4) Time passes and the copy of the Spammer's message is discarded or replaced on the operator's server.
5) Recipient User invokes the "Report Spam" function on her device for the unwanted message
6) User's device creates a SpamRep message containing a reference to the original Spam message.

7) SpamRep Client sends the message to the operator's network entity, the address of which has been pre-provisioned in the device.

8) The network entity receives the User's Spam Report fails to retrieve the original message Content from its database of retained messages since it's no longer there.

9) The Spam Report is discarded by the network entity.

B.2.2 Market benefits

Messages identified as Spam can be quite large. Reporting Spam by reference avoids having to transmit the Content of the Spam messages back to the messaging servers, reducing the load on the operator's network. If the user takes a long time to identify a received message as Spam, such that the operator's servers remove the original message from their database, or replace it with a newer one, the report of Spam can be ignored since the opportunity to block similar messages from being sent to other subscribers has already passed.

B.3 Recovery of Spam message

B.3.1 Short Description

A User finds she is unable to receive messages from a suspect that the message sender is on the black list of the Mobile Network Operator. The User wishes to browse her blocked messages to determine if some expected messages are blocked or further if any message senders are being erroneously blocked. Using the terminal, she sends a SpamRep message containing a request for obtaining the blocked messages in her Network Spam Box. The User peruses the blocked messages and sees that a certain message was erroneously blocked by the Mobile Network Operator as Spam. Using the terminal, she sends the SpamRep message to the SpamRep Server with indicating a request to unblock the identified erroneously blocked messages. From then on she is able to receive messages from her friend.

In case that some messages from a certain message Sender with indication of possible Spam were received by the terminal and those messages were saved in the Local Spam Box, the user may want to send a SpamRep request message to unblock the message sender or recover the messages.

B.3.1.1 Actors

- User. The User possesses a mobile device that can browse blocked message list, and send the recover message for the blocked message

- Mobile Network Operator (MNO). The MNO provides the blocked message list and the network entity to which the User requests the blocked message list in the Network Spam Box and the network entity to which the User sends the report for the erroneously blocked message.

B.3.1.2 Pre-Conditions

- The User could not get the expected message from the family or friend who is blocked user.

- The User's device is provisioned with a SpamRep Client and the User is familiar with the use of the client.

- The MNO is able to store the blocked message list in the Network Spam Box.

- The MNO has a network entity (i.e. Spam Rep Server) that can receive Spam reports and act on them.

B.3.1.3 Post-Conditions

- The User gets the expected messages from the family or friend who was blocked before but not now.
- The MNO has managed the black list and/or blocked messages based on the recovery report.

B.3.1.4 Normal Flow

1) A User finds she is unable to receive messages from a suspect that the message sender is on the black list of the Mobile Network Operator. Using the terminal, she sends a SpamRep message containing a request for obtaining the blocked messages in her Network Spam Box to the SpamRep Server.

2) The SpamRep Server makes the list of the unexpired message in her Network Spam Box and sends it to the User's terminal.

3) The User peruses the blocked messages and sees that a certain message from her friend was erroneously blocked by the Network Operator as Spam. (Note: This step is out of scope of the SpamRep Enabler but is included to illustrate a notional usage scenario.)

4) She sends the SpamRep report to the SpamRep Server indicating "Unblock Sender" in device.

5) The SpamRep Server gets the report for the erroneously blocked message sender from the User and unblocks the identified messages from the Network Spam Box.

6) Based on the received report from the User, the SpamRep Server can consider removing the message sender from the black list or anti-spam rule. Also, the SpamRep Server can adjust the report from the User whether it is requested by the spammer himself. (Note: This step is out of scope of the SpamRep Enabler but is included to illustrate a notional usage scenario.)

7) The User is able to get the expected message from her friend.

B.3.2 Market benefits

By supporting the Network Spam Box, the MNO would not send messages to the User's terminal, which are firmly suspected to be Spam messages and stored in the Network Spam Box. By supporting the Local Spam Box, the message is still delivered to the device allowing the User to review the spam filtered message locally, where spam filtered messages are stored not in the inbox but in the separated box. This will increase User benefit by allowing the User to check whether the blocked messages are erroneously classified by the MNO or not. Further by supporting the unblocking mis-categorized message from the Network Spam Box and/or Local Spam Box, the MNO will benefit from opening the channel for User's complaining and giving chance for the User to review blocked messages.

B.4 Subscriber SMS Feedback – Report Types

B.4.1 Short Description

A subscriber receives an SMS message which appears to be Spam, phishing, viral, misclassified, of an undesired message subscription, unwanted, or has some other issue. To improve his own and/or other users' experiences, he selects an appropriate "feedback message" from a device menu. The type of report may be a Spam feedback, a request to block all future messages from this specific Spam Sender, or several other types. An SMS user agent, acting on end user menu navigation, composes a feedback message and transmits to the pre-provisioned report collection node in the operator's network.

(Note: The following paragraph describes functionality that is out of scope of the SpamRep Enabler, but is included as narrative to provide context for use of the SpamRep Enabler):

Based on this and possibly other feedback messages, an MNO may wish to modify its message delivery policies and/or take legal, civil or other actions to manage the abuse.

(Note: Only steps 5 through 7 below are within the formal scope of the SpamRep Enabler. The remaining steps are included to illustrate a notional usage scenario.)

Normal flow:

1) The Abuser sends an abusive SMS message to a User/Subscriber.

2) User/Subscriber becomes aware of an issue related to the message and or its classification. Any message classification indications and any reasons for the subscriber's identification of an issue are outside of the formal scope of this use case.

3) User/Subscriber invokes the "Report Spam" function on her device.

4) User/Subscriber selects a specific type of Spam Report conveying one or more of the following statements related to the received message:

    a. Abusive "spam" message

    b. Fraudulent message – indicates phishing or similar abuse

    c. Virus

    d. Message miscategorized as Spam (e.g., indicated as Spam, but not Spam)

    e. Opt-out – indicates recipient's desire to receive no more of a subscribed message

    f. Block Sender – indicates recipient's instruction to block future messages from Spam Sender

    g. Unblock Sender – indicates recipient's instruction to unblock future messages from Spam Sender

    h. Sender Authentication Failure – indicates a failure of a Sender authentication mechanism (Note: The "Sender Authentication Failure" report type covers cases where the SpamRep Client is informed that the sender authentication mechanism has failed. An expected use case is a DKIM authentication failure. Depending on the network architecture, this could happen in the network and/or in the device. A report might be sent automatically. Other use cases include other mechanisms (including human) of Spam Sender spoofing detection. We should, for generality, not assume that SpamRep Clients will be human-activated and device based. Although we expect most Spam Reports to be initiated by a User via a SpamRep Client inside a mobile device, there are other use cases. Nothing in the SpamRep Enabler limits its use to human-initiated reports from a device. A device-based SpamRep Client could automatically detect issues, such as sending or receiving messages at a high rate (a DOS attack).

    i. Other – indicates some other (unspecified) reason for reporting the message

j. Unspecified – indicates some type of issue of an unspecified nature; however, its type MAY be one of the above types

5) User's device creates a SpamRep message containing relevant information about the suspect SMS (e.g., originator, message body, time stamp, SMSC, MSC).

6) SpamRep Client sends the message to the SpamRep Server, the address of which has been pre-provisioned in the device.

7) The SpamRep Server receives the User's Spam Report, possibly also receiving other correlated reports from other SpamRep Clients.

8) A network entity aggregates the received reports. For example, in the case of correlated SpamRep Spam Reports,

   a. A policy engine determines that messages with the reported "Spam" Content should be blocked, and

   b. A network entity generates an update to the MNO's content filter to block all SMS messages containing the reported "spam" Content.

   Other actions, such as billing adjustments, address-based block list management and abuse alerting, may be taken.

B.4.2 Market benefits

Indicating the type of report (e.g., opt-out, spam) allows an MNO to more effectively manage abuse, reducing costs and increasing subscriber satisfaction.

B.5 Reporting Partial Spam Content

B.5.1 Short Description

A multimedia message (MM) which includes an advertisement audio clip is received by the user (human recipient) on his handheld device. For the user, only the audio clip is unwanted and unsolicited, so he/she decides to report only the advertisement audio clip.

B.5.1.1 Actors

- User/Subscriber. The User/Subscriber possesses a mobile device that can receive MM messages (MIME formatted), and subscribes to MMS (Multimedia Messaging Service) from the Mobile Network Operator (MNO)

- Mobile Network Operator. The MNO provides MMS and the network entity to which the User sends the Spam Report

- Spammer. An individual who sends unsolicited and unwanted messages to Users on the MNO's network.

B.5.1.2 Pre-Conditions

- User/Subscriber has subscribed to MMS

- User's device is provisioned with a SpamRep Client
- MNO provides MMS
- MNO has a network entity that can receive Spam Reports and act on them

B.5.1.3 Post-Conditions

- It is convenient and flexible for Users to report partial Spam content.
- The SpamRep message processing overhead of MNO has been reduced. Communication efficiency and processing effectiveness are also improved.

B.5.1.4 Normal Flow

1) The Spammer sends a MM (MIME formatted) to random subscribers.

2) The message arrives at the User's handheld.

3) The User considers an advertisement audio clip in the message as Spam , while the rest of the message is considered useful , so the User decides to report only the audio clip and invokes the " Partial Report" function on his/her device.

4) SpamRep Client extracts the partial Content of message that the User has selected to report (i.e., the audio clip).

5) SpamRep Client creates a SpamRep message containing the extracted partial content.

6) SpamRep Client sends the Spam Report to the operator's network entity, the address of which has been pre-provisioned in the device.

B.5.2 Market benefits

By reporting partial message Content which is considered as Spam, MNO enjoys multiple benefits. The processing overhead of SpamRep messages of MNO is reduced, as a result of the reduction of the size of the report message, and network traffic is also reduced. As User specifies which part of the message is Spam, efficiency and effectiveness of SpamRep message processing are improved. By reporting partial message Content instead of the whole message Content, non-revenue-generating network traffic is reduced, which leads to reduced operating costs.

B.6 User Confirmed Spam Report Sharing

B.6.1 Short Description

The Mobile Network Operator can forward the Spam Report or processed one to another Mobile Network Operator or third party (e.g. the government department, a vaccine company). The device should notify the User of this sharing before sending the Spam Report to the Mobile Network Operator. The User allows/disallows that the Mobile Network Operator's sharing the Spam Report with other parties. If the User wants to protect the privacy information included in the Spam Report when it is shared with other parties, the User can request the privacy protection to be applied.

B.6.1.1 Actors

- User/Subscriber. The User/Subscriber possesses a mobile device that can receive messages, and subscribes to the messaging service from the Mobile Network Operator
- Mobile Network Operator. The MNO provides the messaging service and the network entity to which the User sends the Spam Report
- Spammer. An individual who wishes to cause trouble to the MNO and/or subscribers by sending fraudulent or virus like messages

B.6.1.2 Pre-Conditions

- User/Subscriber has subscribed to the messaging (e.g. SMS, MMS, email) service
- User's device is provisioned with a SpamRep Clientep Client and the User is familiar with the use of the client
- MNO provides the messaging service
- MNO has a network entity that can receive Spam Reports, act on them and forward them

B.6.1.3 Post-Conditions

- User feels satisfied as an active participant in the war against Spam
- User knows that her Spam Report is shared with which party including which information
- MNO has identified the Spam message and the Spammer and has blocked further proliferation of the Spam message
- MNO forwards the Spam Reports to the other parties for the valuable process in the Spam protection

B.6.1.4 Normal Flow

1) The Spammer sends email messages to random subscribers, indicating a virus like document.
2) Recipient User becomes suspicious about the virus and invokes the "Report Spam" function on her device.
3) User's device creates a Spam report message containing relevant information about the suspect message (e.g. originator, message body, receiver phone number etc.).
4) Before sending the Spam Report, the User's device notifies that the Spam Report will be shared with other parties (e.g. the government department, a vaccine company) and the preview of the created Spam Report.
5) User recognizes the sharing of Spam Report and requests sending the Spam Report
6) The SpamRep Clientep Client sends the Spam report message to the operator's network entity, the address of which has been provisioned in the device.

(Note: The remainder of this flow – steps 7 onward – are out of scope of the SpamRep Enabler but are included to illustrate a notional usage scenario.)

7) The network entity receives the User's Spam Report.

8) Following the addressed notification for sharing, the MNO forwards the Spam Report to the other party.

B.6.1.5 Alternative Flow

1) The Spammer sends email messages to random subscribers, indicating a virus like document.

2) Recipient User becomes suspicious about the virus and invokes the "Report Spam" function on her device.

3) User's device creates a Spam Report message containing relevant information about the suspect message (e.g. originator, message body, receiver phone number etc.).

4) Before sending the Spam Report, the User's device notifies that the Spam Report will be shared with other parties (e.g. the government department, a vaccine company) and the preview of the created Spam Report.

5) User recognizes the sharing Spam Report and requests sending the Spam Report.

6) User doesn't want that MNO shares the Spam Report with other parties and withdraws the sending the Spam Report.

7) Consequently, the Spam Report won't be sent to the SpamRep Server.

B.6.1.6 Alternative Flow

1) The Spammer sends email messages to random subscribers, indicating a virus like document.

2) Recipient User becomes suspicious about the virus and invokes the "Report Spam" function on her device.

3) User's device creates a Spam report message containing relevant information about the suspect message (e.g. originator, message body, receiver phone number etc.).

4) Before sending the Spam Report, the User's device notifies that the Spam Report will be shared with other parties (e.g. the government department, a vaccine company) and the preview of the created Spam Report.

5) User recognizes the sharing of Spam Report and requests sending the Spam Report.

6) User wants to protect privacy in the sharing process. For example, user doesn't want to include her personal information like phone number or name in the Spam Report to be shared.

(Note: The remainder of this flow – steps 7 onward – are out of scope of the SpamRep Enabler but are included to illustrate a notional usage scenario.)

7) The SpamRep Clientep Client sends the Spam report message to the operator's network entity, the address of which has been provisioned in the device.

8) The network entity receives the User's Spam Report.

9) Following the addressed notification for sharing, the MNO forwards the Spam Report protecting the User privacy to the other party.

B.6.2 Market benefits

The MNO forwards the Spam Report after the sharing notification to the User and also gets the Spam Report from the other parties to improve the Spam protection. Since the User can recognize that the Spam Report will be shared before the sending the Spam Report, the MNO provides the transparent sharing mechanism and also the User can control her privacy.

B.7 Report Anonymisation

B.7.1 Short Description

The SpamRep Enabler is designed to allow Spam Reports to be sent from mobile operator subscribers to the mobile operator, for purposes such as remediating future Spam with similar Content, or from similar sources.

As part of this process, the operator may choose to keep all such Spam Reports within their administrative domain; however, there are many use case where the operator would like to forward these Spam Reports to a third-party domain.

Example reasons for forwarding a Spam Report to a third-party domain include:

1. Sending Spam Reports to an Anti-Spam Filtering vendor for automatic update of filtering rules or definitions.
2. Sending Spam Reports to other mobile operators to alert them about Spam being sent from their domain.
3. Sending Spam Reports to third-party Content senders, for removal from their sending lists.
4. Etc

In order to safely send such Spam Reports outside the operator's administrative domain without violating privacy laws and/or policies, it may be necessary for the operator to anonymise aspects of the Spam Report before sending to a third-party domain. There are thus several requirements that the SpamRep Enabler to take no action that would prevent such anonymisation.

Additionally, subscribers may wish some of the Content of a message to be anonymised or removed before sending a Spam Report to their operator; this may be for reasons of personal privacy, or some other reason such as the fact that for some Spam Report types, the Content of the original message may not be required (for example blocking a Spam Sender). It is recognised that modification or removal of message Content may cause some Spam Reports to be disregarded by the SpamRep Server (depending on the Spam Report type), due to a lack of actionable information.

Normal flow:

1) An abuser, having illegally gained access to a phone number and bank account database, sends a phishing SMS message containing a partial bank account identifier to a User/Subscriber.

2) User/Subscriber becomes suspicious of this message. Any message classification indications and any reasons for the subscriber's suspicion are outside of the formal scope of this use case.

3) User/Subscriber invokes the "Report Spam" function on his device.

4) User/Subscriber selects a 'phishing' type of Spam Report.

5) User's device creates a SpamRep message containing relevant information about the suspect SMS (e.g., originator, message body, time stamp, SMSC, MSC).

6) SpamRep Client sends the message to the SpamRep Server, the address of which has been pre-provisioned in the device.

7) The SpamRep Server within an MNO network receives the User's Spam Report.

(Note: The remainder of this flow – steps 8 onward – are out of scope of the SpamRep Enabler but are included to illustrate a notional usage scenario.)

8) An MNO network entity sanitises the information from the Spam Report, removing Content identifying the bank account of the User/Subscriber, and forwards the sanitised Spam Report to a 3rd-party content filter provider located outside of the MNO network.

9) 3rd party content filter provider develops and deploys (within MNO network) rules blocking similar phishing messages.

B.7.2 Market benefits

Spam, phishing and other types of attacks are minimised, while protecting subscriber privacy and remaining within legal subscriber privacy guidelines.

B.8 Acquire the Status of Spam Report

B.8.1 Short Description

A user receives a Spam message and becomes suspicious. He/she sends a Spam Report to the pre-provisioned report collection node in the operator's network. Two days later, he/she wants to know how the MNO processes the Spam Report, and inquires about the status of the Spam Report to the MNO. The MNO notifies the user the Spam Report's status.

B.8.1.1 Actors

- User/Subscriber. The User/Subscriber possesses a mobile device that can receive messages, and subscribes to a messaging service from the Mobile Network Operator
- Mobile Network Operator. The MNO provides the messaging service and the network entity to which the User sends the Spam Report
- Spammer. An individual who wishes to cause trouble to the MNO and/or subscribers by sending fraudulent messages

B.8.1.2 Pre-Conditions

- User/Subscriber has subscribed to a messaging service
- User's device is provisioned with a SpamRep Client
- MNO provides messaging service
- MNO has a network entity that can receive Spam Reports and responds to the user's Spam Report inquiry, or notify the user the Spam Report's status.

B.8.1.3 Post-Conditions

- User receives the status of the Spam Report that he reported previously.
- MNO has identified the Spam message and the Spammer and has blocked further proliferation of the Spam Message, and MNO has notified the user the status of the Spam Report.

B.8.1.4 Normal Flow

1) The Spammer sends messages to random subscribers, indicating recipients will receive $20 credit from the MNO if the message is forwarded to 10 subscribers.

2) Recipient User becomes suspicious and SpamRep Client reports the SPAM message to the operator's network entity.

3) Several days later, Recipient User wants to know the status of the Spam Report that he has reported, and SpamRep Client sends a request to the operator's network entity, and inquires about the status of the Spam Report.

4) The network entity receives the User's inquiry, and replies that the MNO's blacklist has been updated to deny transmission of messages from the known Spammer.

B.8.1.5 Alternative Flow

1),2) Same as normal flow

3) The network entity may automatically (i.e. without an explicit action of the User) notify the user about the status of the Spam Report one hour later.

B.8.2 Market benefits

A user can know the status of the Spam Report (e.g., whether a reported Spam is really a Spam or a false alarm, whether it has been blocked, etc.), and has a peace of mind and good user experience. Quick and relevant feedback from MNO will encourage uses to keep reporting. This is beneficial to the MNO as well.