Enabler Test Specification for Client Side Content Screening Framework

Candidate Version 1.0 – 27 Feb 2007

Open Mobile Alliance

OMA-ETS-Client_Side_CS_FW-V1_0-20070227-C

Contents

Tables

1. Scope

This document describes in detail available test cases for Client Side Content Screening Framework (CSCSF) 1.0, http://www.openmobilealliance.com/release_program/Client_Side_CS_FW_v1_0.html.

The CSCSF specification defines technical details of interfaces and interaction mechanism necessary for implementing the OMA Client Side Content Screening Framework to screen malicious content at the mobile terminal. This document specifies conformance test cases for CSCSF. This document does not include interoperability test cases as the scope of the CSCSF technical specification excludes the necessity of such tests.

The conformance test cases are aimed to verify the adherence to normative requirements described in the technical specifications.

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

[CSCSF-RD-v1] “OMA Client Side Content Screening Framework Requirements”, Version 1.0, Open Mobile Alliance™, OMA-RD-Client_Side_CS_FW-V1_0, URL:http://www.openmobilealliance.org/

[CSCSF-AD-v1] “OMA Client Side Content Screening Framework Architecture”, Version 1.0, Open Mobile Alliance™, OMA-AD-Client_Side_CS_FW-V1_0, URL:http://www.openmobilealliance.org/

[CSCSF-TS-v1] “OMA Client Side Content Screening Framework Technical Specification”, Version 1.0, Open Mobile Alliance™, OMA-TS-Client_Side_CS_FW-V1_0, URL:http://www.openmobilealliance.org/

[CSCSF-ETR_v1] “OMA Client Side Content Screening Framework Enabler Test Requirements”, Version 1.0, Open Mobile Alliance™, OMA-ETR-Client_Side_CS_FW-V1_0, URL:http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT] “Dictionary for OMA Specifications”, Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words "SHALL", "SHALL 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", are normative, unless they are explicitly indicated to be informative.

The following numbering scheme is used:

xxx-y.z-con-number where:

xxx	Name of enabler, e.g. MMS or Browsing
y.z	Version of enabler release, e.g. 1.2 or 1.2.1
'con'	Indicating this test is a conformance test case
number	Leap number for the test case

Or

xxx-y.z-int-number where:

xxx	Name of enabler, e.g. MMS or Browsing
y.z	Version of enabler release, e.g. 1.2 or 1.2.1
'int'	Indicating this test is a interoperability test case
number	Leap number for the test case

3.2 Definitions

For the purposes of this document, the terms and definitions given in [**Error! Reference source not found.**] apply and the following also apply:

Client Side Content Screening	Content screening performed at the mobile terminal.
Client Side Content Screening Framework	An abstract conceptual structure used as the basis for constructing interaction model between OMA/non-OMA enablers and content scanning functionality through a set of interfaces with the ultimate goal of bringing forth content screening capability to the mobile terminal.
Content	Data or code delivered to an end-user and/or end-user's terminal.
Content Scanning	The actual operation of looking at the data to determine whether it is a potential candidate for screening and level of severity if found to be as such. What this operation consist of would vary according to how content scanning functionality is implemented and falls outside the scope of this document.
Content Scanning Functionality	Content scanning performed for OMA/non-OMA enabler wishing to determine whether a content under consideration is undesirable or not. This performance is accessed by a set of interfaces specified by the content screening framework.
Content Screening	The act of protecting an end-user and/or end-user's terminal from undesirable content by blocking access to the said content. This act may be in the form of warning message, confirmation of deletion, notification of deletion, silent deletion without notification, etc. Exact detail would vary according to severity level reported, I/O capability of mobile terminal, user preferences, etc.
Mobile Terminal	A device that receives content as part of its normal running operation.
Scan Engine	Component of client side content screening framework that performs content scanning service to OMA/non-OMA enablers related to end-user content delivery and/or processing.
Scan Engine Emulator	A reference implementation designed to provide an application programming interface for a Client Side Content Screening Enabler to interface with for the purpose of conducting the conformance test cases specified in the OMA Client Side Content Screening Enabler Test Specification [ETS_Client_Side_CS_FW].
Screening Action	The act of blocking an undesirable content (see 'Content Screening').

3.3 Abbreviations

OMA	Open Mobile Alliance
EICAR	European Institute for Computer Antivirus Research

4. Introduction

The purpose of this document is to provide test cases for Client Side Content Screening Framework Enabler Release 1.0. The test cases cover the inputs and outputs for CSF-1 and CSF-7. The focus of the test cases is to verify that the calling enabler is able to call the CSCSF CSF-1 to initiate a scan, pass content for scanning and handle the results returned from the CSCSF interface.

In CSCSF the scan engine works (interacts) with the implementation of the CSCSF Enabler (the Enabler from now and on) through an interface (CSF-1), which is identified as one of the main elements to be tested in this ETS. The CSCSF conformance test cases are designed to verify the interface calls, and not the content analysis function that a CSCSF scan engine provides. The test tool should analyse the request from the Enabler implementation and return an expected result. to check the process and the implementation is succesful in both ways:

1. The input content received in the Enabler triggers the scanning proccess depending on the content type (the request to the engine/test tool could be different if the content is an e-mail, a HTML document, an executable file, etc.).
2. The result of the scanning process (in fact, the result given by the test tool) must be understood by the Enabler which should take an action with the received content:
    a. Do nothing if the content is correct;
    b. Or request the scan engine (the test tool) for more information and (optionally) give the user the chance to abort or continue the process.

Evidently, the test tool acting as the scan engine does not have to effectively analyse the content; the returned result given to the Enabler can be configured for each test case. Finally, this test tool may generate a log file with the result of the perfomed tests for checking purposes.

The features in the Client Side Content Screening Framework enabler are implemented in mobile devices. The following items are needed to test the enabler:

- Client side content screening framework test harness containing

➢ A Scan Engine Emulator (SEE) that provides the CSCSF interface to the invoking enabler

➢ Test content samples

➢ Test Content Detection Logic (TCDL)

There is no interoperability tests defined for the Client Side Content Screening Framwork due to the fact that the specification defines the API calls between an enabler and the CSCSF interface, both of which will be implemented in the client terminal.

5. Client Side CS FW Conformance Test Cases

5.1 CSCSF-1.0-con001-Invoking the CSFScanData (CSF-1) to scan content

Test Case ID	CSCSF-1.0-con001-Invoking the CSFScanData (CSF-1) to scan content
Test Object	CSCSF invoker e.g. OMA enabler
Test Case Description And Purpose	Verify that the CSCSF invoker can call CSFScanData interface to scan content.
Specification Reference	[CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-004
Tool	CSCSF test harness, Scan Engine Emulator
Test Code/Files	Valid test document
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect test content flagged as benign. The invoker SHALL select benign flagged test content for passing to through the interface.
Test Procedure	1. The CSCSF invoker passes a valid test document, which is flagged as benign, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. The status code is 0, and the scan result is 0.

Table 1: Test Information for Invoking the CSFScanData (CSF-1) to scan content test case

5.2 CSCSF-1.0-con002-Invoking the CSFScanData (CSF-1) to scan content of unknown type

Test Case ID	CSCSF-1.0-con001-Invoking the CSFScanData (CSF-1) to scan content of unknown type
Test Object	CSCSF invoker e.g. OMA enabler
Test Case Description And Purpose	Verify that the CSCSF invoker can call CSFScanData interface to scan content and receive the result.
Specification Reference	[CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF test harness, Scan Engine Emulator
Test Code/Files	Valid test document flagged as benign

Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect test content flagged as benign. The invoker SHALL select benign flagged test content of unknown type for passing to through the interface.
Test Procedure	1. The CSCSF invoker passes a valid test document, which is flagged as benign, through the interface. The CSCSF invoker sets the content type as 0. 2. The interface returns a status code and scan result
Pass-Criteria	2. The status code is 0, and the scan result is 0.

Table 2: Test Information for Invoking the CSFScanData (CSF-1) to scan content of unknown type.

5.3 CSCSF-1.0-con003-Invoking the CSFScanData (CSF-1) to scan a HTML document that is benign

Test Case ID	CSCSF-1.0-con002-Invoking the CSFScanData (CSF-1) to scan an HTML document that is benign
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid HTML document that is flagged as benign
Specification Reference	[CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect HTML test content. The invoker SHALL select benign flagged content for passing through to the interface.
Test Code/Files	Valid HTML test content, flagged as benign
Preconditions	
Test Procedure	1. The CSCSF invoker passes a valid HTML test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. The status code is 0, and the scan result is 0.

Table 3: Test Information for Invoking the CSFScanData (CSF-1) to scan an HTML document that is benign

5.4 CSCSF-1.0-con004-Invoking the CSFScanData (CSF-1) to scan a HTML document that is flagged malicious

Test Case ID	CSCSF-1.0-con004-Invoking the CSFScanData (CSF-1) to scan an HTML document that is malicious
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid HTML document that is flagged as malicious, and receive the returning code.
Specification Reference	[CSCSF-AD] Section 6.4.1 [CSCSF-AD] Section 6.4.2 [CSCSF-TS] Section 5.1.1

SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid HTML test content flagged as malicious
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect HTML test content. The invoker SHALL select malicious flagged content for passing through to the interface.
Test Procedure	1. The CSCSF invoker passes a valid HTML test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. Status code is 0, and scan result is 1.

Table 4: Test Information for Invoking the CSFScanData (CSF-1) to scan an HTML document that is flagged malicious

5.5 CSCSF-1.0-con005-Invoking the CSFScanData (CSF-1) to scan a URL that is benign

Test Case ID	CSCSF-1.0-con005-Invoking the CSFScanData (CSF-1) to scan a URL that is benign
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid URL that is flagged as benign
Specification Reference	[CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect HTML test content. The invoker SHALL select benign flagged content for passing through to the interface.
Test Code/Files	Valid URL test content flagged as benign
Preconditions	
Test Procedure	1. The CSCSF invoker passes a valid URL test content, which is flagged as benign, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. The status code is 0, and the scan result is 0.

Table 5: Test Information for Invoking the CSFScanData (CSF-1) to scan a URL that is benign

5.6 CSCSF-1.0-con006-Invoking the CSFScanData (CSF-1) to scan a URL that is flagged malicious

Test Case ID	CSCSF-1.0-con006-Invoking the CSFScanData (CSF-1) to scan a URL that is malicious
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid URL that is flagged as malicious, and receive the returning code.
Specification Reference	[CSCSF-AD] Section 6.4.1 [CSCSF-AD] Section 6.4.2 [CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid URL test content flagged as malicious
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect URL test content. The invoker SHALL select malicious flagged content for passing through to the interface.
Test Procedure	1. The CSCSF invoker passes a valid URL test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. Status code is 0, and scan result is 1.

Table 6: Test Information for Invoking the CSFScanData (CSF-1) to scan a URL that is flagged malicious

5.7 CSCSF-1.0-con007-Invoking the CSFScanData (CSF-1) to scan an email that is benign

Test Case ID	CSCSF-1.0-con007-Invoking the CSFScanData (CSF-1) to scan an email that is benign
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid email that is flagged as benign
Specification Reference	[CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect email test content. The invoker SHALL select benign flagged content for passing through to the interface.
Test Code/Files	Valid email test content flagged as benign

Preconditions	
Test Procedure	1. The CSCSF invoker passes a valid email test content, which is flagged as benign, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. The status code is 0, and the scan result is 0.

Table 7: Test Information for Invoking the CSFScanData (CSF-1) to scan an email that is benign

5.8 CSCSF-1.0-con008-Invoking the CSFScanData (CSF-1) to scan an email that is flagged malicious

Test Case ID	CSCSF-1.0-con008-Invoking the CSFScanData (CSF-1) to scan an email that is malicious
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid email that is flagged as malicious, and receive the returning code.
Specification Reference	[CSCSF-AD] Section 6.4.1 [CSCSF-AD] Section 6.4.2 [CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid email test content flagged as malicious
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect email test content. The invoker SHALL select malicious flagged content for passing through to the interface.
Test Procedure	1. The CSCSF invoker passes a valid email test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. Status code is 0, and scan result is 1.

Table 8: Test Information for Invoking the CSFScanData (CSF-1) to scan an email that is flagged malicious

5.9 CSCSF-1.0-con009-Invoking the CSFScanData (CSF-1) to scan a phone number that is benign

Test Case ID	CSCSF-1.0-con007-Invoking the CSFScanData (CSF-1) to scan a phone number that is benign
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid phone number that is flagged as benign
Specification Reference	[CSCSF-TS] Section 5.1.1

SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect phone test content. The invoker SHALL select benign flagged content for passing through to the interface.
Test Code/Files	Valid phone number test content flagged as benign
Preconditions	
Test Procedure	1. The CSCSF invoker passes a valid phone number test content, which is flagged as benign, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. The status code is 0, and the scan result is 0.

Table 9: Test Information for Invoking the CSFScanData (CSF-1) to scan a phone number that is benign

5.10 CSCSF-1.0-con0010-Invoking the CSFScanData (CSF-1) to scan a phone number that is flagged malicious

Test Case ID	CSCSF-1.0-con008-Invoking the CSFScanData (CSF-1) to scan a phone number that is malicious
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid phone number that is flagged as malicious, and receive the returning code.
Specification Reference	[CSCSF-AD] Section 6.4.1 [CSCSF-AD] Section 6.4.2 [CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid phone number test content flagged as malicious
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect phone number test content. The invoker SHALL select malicious flagged content for passing through to the interface.
Test Procedure	1. The CSCSF invoker passes a valid phone number test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. Status code is 0, and scan result is 1.

Table 10: Test Information for Invoking the CSFScanData (CSF-1) to scan a phone number that is flagged malicious

5.11 CSCSF-1.0-con011-Invoking the CSFScanData (CSF-1) to scan a text document that is benign.

Test Case ID	CSCSF-1.0-con011-Invoking the CSFScanData (CSF-1) to scan a text document that is benign
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid text document that is flagged as benign
Specification Reference	[CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect text document test content. The invoker SHALL select benign flagged content for passing through to the interface.
Test Code/Files	Valid text document test content flagged as benign
Preconditions	
Test Procedure	1. The CSCSF invoker passes a valid text document test content, which is flagged as benign, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. The status code is 0, and the scan result is 0.

Table 11: Test Information for Invoking the CSFScanData (CSF-1) to scan a text document that is benign

5.12 CSCSF-1.0-con012-Invoking the CSFScanData (CSF-1) to scan a text document that is malicious.

Test Case ID	CSCSF-1.0-con0012-Invoking the CSFScanData (CSF-1) to scan a text document that is malicious
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid text document that is flagged as malicious, and receive the returning code.
Specification Reference	[CSCSF-AD] Section 6.4.1 [CSCSF-AD] Section 6.4.2 [CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid text document test content flagged as malicious
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect text document test content. The invoker SHALL select

	malicious flagged content for passing through to the interface.
Test Procedure	1. The CSCSF invoker passes a valid text document test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. Status code is 0, and scan result is 1.

Table 12: Test Information for Invoking the CSFScanData (CSF-1) to scan a text document that is malicious

5.13 CSCSF-1.0-con013-Receive severity threat level (OPTIONAL)

Test Case ID	CSCSF-1.0-con0013-Receive severity threat level
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid text document that is flagged as malicious, and receives the appropriate severity level code
Specification Reference	[CSCSF-TS] Section 5.1.1
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid test content flagged as malicious
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect test content. The invoker SHALL select malicious flagged content for passing through to the interface. The scan emulator SHALL return a severity level code of the same level as the test content.
Test Procedure	1. The CSCSF invoker passes a valid test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. Status code is 0, and scan result is 1. The severity code is the same as the code of the test code.

Table 13: Test information for receiving a security threat level (optional)

5.14 CSCSF-1.0-con014-Receive the name of the threat (OPTIONAL)

Test Case ID	CSCSF-1.0-con0014-Receive the name of the threat
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler passes a valid test content that is flagged as malicious, and receives the appropriate name of the threat
Specification Reference	[CSCSF-AD] Section 6.4.1 [CSCSF-AD] Section 6.4.2 [CSCSF-TS] Section 5.1.1

SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid test content flagged as malicious
Preconditions	The Scan Engine Emulator SHALL be present and SHALL contain signature definitions to detect test content. The invoker SHALL select malicious flagged content for passing through to the interface. The scan emulator SHALL return the name of the threat to the invoker.
Test Procedure	1. The CSCSF invoker passes a valid test content, which is flagged as malicious, through the interface. 2. The interface returns a status code and scan result
Pass-Criteria	1. Status code is 0, and scan result is -1. The expected name of threat is returned.

Table 14: Test information for receiving the name of the threat (optional)

5.15 CSCSF-1.0-con015-Retrieve Set Error (OPTIONAL)

Test Case ID	CSCSF-1.0-con0015-Invoke CSF-7 to retrieve last error code
Test Object	CSCSF invoker
Test Case Description and Purpose	Verify that the enabler invokes CSF-7 GetLastError to retrieve the last set error.
Specification Reference	[CSCSF-TS] Section 5.1.2
SCR Reference	CSCSF-CE-001 CSCSF-CE-003 CSCSF-SE-001 CSCSF-SE-003 CSCSF-SE-004
Tool	CSCSF invoker, scan engine enabler, test harness
Test Code/Files	Valid test content flagged as setting an error
Preconditions	The Scan Engine Emulator SHALL be present and SHALL set an error if the status code is -1.
Test Procedure	1. The CSCSF invoker invokes CSF-7 to retrieve last error set. 2. The interface returns an error code.
Pass-Criteria	1. Interface returns one of the error codes specificed in CSCSF TS.

Table 15: Test information for receiving set error

6. CSCSF Interoperability Test Cases

There is no interoperability tests defined for the Client Side Content Screening Framework due to the fact that the specification defines the API calls between an enabler and the CSCSF interface, both of which will be implemented in the client terminal.

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-ETS-Client Side CS-FW-V1_0	18 Dec 2006	1,2,3,4,5,	First draft
	05 Feb 2007	3,4,5,6	Editorial changes (clarification of terms, capitalization of terms, complete incomplete fields)
	08 Feb 2007	n/a	IOP WG Agreed
Candidate Version OMA-ETS-Client Side CS-FW-V1_0	27 Feb 2007	n/a	Status changed to Candidate (TP R&A 2007-02-14 to 2007-02-27) TP ref # OMA-TP-2007-0094-INP_OMA_ETS_CSCSF_V1_0_for_Candidate_Approval