Enabler Release Definition for Secure Removable Media

Candidate Version 1.0 – 28 Jan 2008

Open Mobile Alliance

OMA-ERELD-SRM-V1_0-20080128-C

Contents

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of Secure Removable Media 1.0 according to OMA Release process and the Enabler Release specification baseline listed in section 6.

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

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

[OMADRMv2] "Digital Rights Management", Open Mobile Alliance™, OMA-DRM-DRM-V2_0, URL:http://www.openmobilealliance.org/

[OMADRMv2.1] "Digital Rights Management", Open Mobile Alliance™, OMA-DRM-DRM-V2_1, URL:http://www.openmobilealliance.org/

[SRM-TS] "OMA Secure Removable Media Specification", Open Mobile Alliance™, OMA-TS-SRM-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/

[SRM-AD] "OMA Secure Removable Media Architecture", Open Mobile Alliance™, OMA-AD-SRM-V1_0, URL:http://www.openmobilealliance.org/

[SRM-RD] "OMA Secure Removable Media Requirements", Open Mobile Alliance™, OMA-RD-SRM-V1_0, 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.

The formal notation convention used in sections 9 and 10 to formally express the structure and internal dependencies between specifications in the Enabler Release specification baseline is detailed in [SCRRULES].

3.2 Definitions

Device	Entity (hardware/software or combination thereof) within a user equipment that implements a DRM Agent. The Device is also conformant to the OMA DRM specifications. The Device may include a smartcard module (e.g. a SIM) or not depending upon implementation
DRM Agent	Entity in the Device that manages permissions for media objects
DRM Content	Media objects that are consumed according to a set of permissions in Rights
Enabler Release	Collection of specifications that combined together form an enabler for a service area, e.g. a download enabler, a browsing enabler, a messaging enabler, a location enabler, etc. The specifications that are forming an enabler should combined fulfil a number of related market requirements.
Minimum Functionality Description	Description of the guaranteed features and functionality that will be enabled by implementing the minimum mandatory part of the Enabler Release.
Rights	Collection of permissions and constraints defining under which circumstances access is granted to DRM Content. Rights may include the associated state information
Secure Removable Media	A removable media that implements means to protect against unauthorized access to its internal data and includes an SRM Agent (e.g. secure memory card, smart card)
SRM Agent	A trusted entity embodied in Secure Removable Media. This entity is responsible for storing and removing Rights in Secure Removable Media, for delivering Rights from/to a DRM Agent in a secure manner, and for enforcing permissions and constraints, including securely maintaining state information for stateful rights. The SRM Agent is a part of Secure Removable Media

3.3 Abbreviations

AD	Architecture Document
CRL	Certificate Revocation List
DRM	Digital Rights Management
ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
MAC	Message Authentication Code
OMA	Open Mobile Alliance
RD	Requirements Document
RI	Rights Issuer
RO	Rights Object
SD	Secure Digital
SIM	Subscriber Identity Module
S-MMC	Secure MultiMediaCard

SRM	Secure Removable Media
USIM	Universal Subscriber Identity Module

4. Introduction

This document outlines the Enabler Release Definition for Secure Removable Media (SRM) 1.0 and the respective conformance requirements for clients and servers implementing claiming compliance to it as defined by Open Mobile Alliance across the specification baseline.

Secure Removable Media is a removable media that implements means to protect against unauthorized access to its internal data and includes an SRM Agent. Example of Secure Removable Media (referred to as SRM hereinafter) may be the secure memory card and the smart card.

The secure memory card has an embedded microprocessor and is capable of storing Rights or DRM Content in a secure manner (e.g. S-MMC, SD). The smart card also has an embedded microprocessor and is capable of storing access codes, user subscription information, secret keys, DRM Content, Rights etc (e.g. SIM, USIM, R-UIM). If a user uses Devices with a physical interface to connect an SRM, the user can use the SRM as a means of increasing storage space for DRM Content and portability of Rights. Differently from the secure memory card, the smart card enables users to make a telephone call by using the Devices and is issued by a mobile network operator.

OMA DRM with SRM can provide a mechanism to write, read, delete and update Rights in SRM in a secure manner to realize the use cases defined in the OMA SRM Requirements Document [SRM-RD]. The architecture of the OMA SRM is specified in the OMA SRM architecture document [SRM-AD]. Technical details are specified in the OMA SRM technical specification [SRM-TS].

While the OMA DRM version 2.0 [OMADRMv2] and 2.1 [OMADRMv2.1] define a general framework for downloading Rights to Devices and sharing Rights in a domain, this specification defines mechanisms and protocols of the SRM to extend the OMA DRM version 2.0 or 2.1 to allow users to move Rights between Devices and SRMs and to consume Rights stored in SRMs without generating and managing complex groups of Devices in a domain.

5. Description of Differences from Previous Version

This is a new enabler release.

6. Document Listing for SRM 1.0

This section is normative.

Table 1: Listing of Documents in SRM 1.0 Enabler

Doc Ref	Permanent Document Reference	Description
Requirement Document		
[SRM-RD]	OMA-RD-SRM-V1_0-20080128-C	Requirement Document for SRM 1.0 Enabler
Architecture Document		
[SRM-AD]	OMA-AD-SRM-V1_0-20080128-C	Architecture Document for SRM 1.0 Enabler
Technical Specifications		
[SRM-TS]	OMA-TS-SRM-V1_0-20080128-C	Specification that defines the protocol for SRM 1.0 that provides control interface between the Device and SRM
Supporting Files		
n/a		

7. Minimum Functionality Description for SRM 1.0

This section is informative.

Client in the SRM specification is Device. The minimum mandatory client functionality for the SRM specification includes:

- Cryptographic algorithms: Hash, MAC, symmetric encryption, asymmetric encryption, and signature algorithms
- SRM Hello: Protocol handshaking between Device and SRM
- Mutual authentication and key exchange between Device and SRM
- Key derivation function
- Message replay protection
- CRL delivery and certificate revocation checking using CRL
- Device to SRM Rights move
- SRM to Device Rights move
- Local rights consumption
- Rights identifier list delivery from SRM
- Move replay protection

The SRM specification also defines the following optional client functionality:

- OCSP response processing
- RI certificate chain transfer between Device and SRM
- Multiple secure authenticated channels

Servers in the SRM specification are RI and SRM. The minimum mandatory server functionality for the SRM specification includes:

RI:

- Supporting Move permission and related constraints in Rights Objects

SRM:

- Cryptographic algorithms: Hash, MAC, symmetric encryption, asymmetric encryption, and signature algorithms
- SRM Hello: Protocol handshaking between Device and SRM
- Mutual authentication and key exchange between Device and SRM
- Key derivation function
- Message replay protection
- CRL store and certificate revocation checking using CRL

- Rights installation
- Rights query
- Rights removal
- REK query
- State information update
- Rights identifier list generation

The SRM specification also defines the following optional server functionality:

SRM:

- OCSP response processing and certificate revocation checking using OCSP response
- RI certificate chain store
- Multiple secure authenticated channels

8. Conformance Requirements Notation Details

This section is informative

The tables in following chapters use the following notation:

Item: Entry in this column MUST be a valid ScrItem according to [SCRRULES].

Feature/Application: Entry in this column SHOULD be a short descriptive label to the **Item** in question.

Status: Entry in this column MUST accurately reflect the architectural status of the **Item** in question.

- M means the **Item** is mandatory for the class
- O means the **Item** is optional for the class
- NA means the **Item** is not applicable for the class

Requirement: Expression in the column MUST be a valid TerminalExpression according to [SCRRULES] and it MUST accurately reflect the architectural requirement of the **Item** in question.

9. ERDEF for SRM 1.0 – Client Requirements

This section is normative.

Table 2: ERDEF for SRM 1.0 Client-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-SRM-C-001	DRM 2.0 Device supporting SRM	M	OMA-ERDEF-DRMv2-C-001 AND OMA-ERDEF-SRM-C-003
OMA-ERDEF-SRM-C-002	DRM 2.1 Device supporting SRM	M	OMA-ERDEF-DRMv2.1-C-001 AND OMA-ERDEF-SRM-C-003
OMA-ERDEF-SRM-C-003	Device with SRM interface	M	SRM-CRT-C-001-M AND SRM-CRT-C-002-M AND SRM-CRT-C-003-M AND SRM-CRT-C-004-M AND SRM-CRT-C-005-M AND SRM-HEL-C-001-M AND SRM-SAC-C-001-M AND SRM-SAC-C-002-M AND SRM-SAC-C-003-M AND SRM-CRL-C-001-M AND SRM-CRL-C-002-M AND SRM-CRL-C-003-M AND SRM-CRL-C-004-M AND SRM-MOV-C-001-M AND SRM-MOV-C-002-M AND SRM-MOV-C-003-M AND SRM-MOV-C-004-M AND SRM-MOV-C-005-M AND SRM-MOV-C-006-M AND SRM-LRC-C-001-M AND SRM-LRC-C-002-M AND SRM-LRC-C-003-M AND SRM-LRC-C-004-M AND SRM-UTIL-C-001-M AND SRM-UTIL-C-002-M AND SRM-UTIL-C-004-M AND SRM-UTIL-C-005-M AND SRM-UTIL-C-006-M AND SRM-UTIL-C-007-M AND SRM-UTIL-C-009-M AND SRM-CERT-C-004-M AND SRM-LOG-C-001-M AND SRM-CAC-C-001-M

For OMA-ERDEF-DRMv2-C-001, refer to [OMADRMv2]. For OMA-ERDEF-DRMv2.1-C-001, refer to [OMADRMv.2.1].

10.ERDEF for SRM 1.0 – Server Requirements

This section is normative.

Table 3: ERDEF for SRM 1.0 Server-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-SRM-S-001	DRM 2.0 RI supporting SRM	M	OMA-ERDEF-DRMv2-S-001 AND SRM-MOV-S-001-M
OMA-ERDEF-SRM-S-002	DRM 2.1 RI supporting SRM	M	OMA-ERDEF-DRMv2.1-S-001 AND SRM-MOV-S-001-M
OMA-ERDEF-SRM-S-003	SRM	M	SRM-CRT-S-001-M AND SRM-CRT-S-002-M AND SRM-CRT-S-003-M AND SRM-CRT-S-004-M AND SRM-CRT-S-005-M AND SRM-HEL-S-001-M AND SRM-SAC-S-001-M AND SRM-SAC-S-002-M AND SRM-SAC-S-003-M AND SRM-CRL-S-001-M AND SRM-CRL-S-002-M AND SRM-CRL-S-003-M AND SRM-CRL-S-004-M AND SRM-MOV-S-002-M AND SRM-MOV-S-003-M AND SRM-MOV-S-004-M AND SRM-LRC-S-001-M AND SRM-LRC-S-002-M AND SRM-UTIL-S-001-M AND SRM-UTIL-S-002-M AND SRM-UTIL-S-004-M AND SRM-UTIL-S-005-M AND SRM-UTIL-S-006-M

For OMA-ERDEF-DRMv2-S-001, refer to [OMADRMv2]. For OMA-ERDEF-DRMv2.1-S-001, refer to [OMADRMv.2.1].

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 <current version> History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ERELD-SRM-V1_0-20070522-D	22 May 2007	All	First Draft
OMA-ERELD-SRM-V1_0-20071029-D	29 Oct 2007	6, 7, 9, 10	CR to address changes from Consistency Review OMA-DRM-2007-509
Candidate Versions OMA-ERELD-SRM-V1_0-20080128-C	28 Jan 2008	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2007-0508-INP_SRM_V1_0_ERP_for_Candidate_Approval