



***Society of Cable  
Telecommunications  
Engineers***

---

**ENGINEERING COMMITTEE  
Digital Video Subcommittee**

---

**SCTE 201 2013**

**Open Media Security (OMS) Root Key Derivation  
Profiles and Test Vectors**

## NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Recommended Practices (hereafter called documents) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long term reliability of broadband communications facilities.

These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members, whether used domestically or internationally.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such Standards.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2013  
140 Philips Road  
Exton, PA 19341

**Table of Contents**

1	Abstract.....	1
1.1	Background.....	1
1.2	Introduction.....	1
1.3	Normative References .....	2
1.4	Informative References.....	3
1.5	Definitions .....	4
2	Functional Diagram .....	6
3	Base Requirements.....	8
4	Additional Requirements .....	9
4.1	Preliminary SCK Manipulation Function.....	9
4.1.1	Triple-DES .....	9
4.1.2	AES Encrypt.....	9
4.1.3	AES Decrypt .....	10
4.2	Vendor Separation Function .....	10
4.2.1	Triple-DES .....	11
4.2.2	AES Encrypt.....	11
4.2.3	AES Decrypt .....	12
4.3	Final Root Key Derivation Function .....	12
4.3.1	Triple-DES .....	12
4.3.2	AES Encrypt.....	13
4.3.3	AES Decrypt .....	13
4.4	Module Key Derivation Function.....	14
4.4.1	Triple-DES .....	14
4.4.2	AES Encrypt.....	15
4.4.3	AES Decrypt .....	15
5	Profiles.....	16
5.1	Summary.....	16
5.2	Profile 0 – Base Profile.....	17
5.3	Profile 1 – Triple DES Profile .....	17
5.4	Profile 1A – Triple DES Profile with Module Key Derivation .....	17
5.5	Profile 2 – AES Profile .....	17
5.6	Profile 2A – AES Encrypt Profile with Module Key Derivation .....	18
5.7	Profile 2B – AES Decrypt Profile with Module Key Derivation .....	18
6	Test Vectors .....	19
6.1	Root Key Derivation Test Vectors.....	19
6.1.1	Profile 0 Operation .....	19
6.1.2	Profile 1 Operation .....	19
6.1.3	Profile 1A Operation .....	20
6.1.4	Profile 2 Operation .....	21
6.1.5	Profile 2A Operation .....	22
6.1.6	Profile 2B Operation .....	24
6.2	Content Descrambling (CW) Vectors.....	25
6.2.1	DVB CSA2 Operation.....	25
6.2.2	AES Vector .....	25
Appendix A	Test Vectors Python Script.....	27

**List of Tables**

Table 1	Key Ladder / Content Descrambling Algorithms .....	16
---------	--	----

**List of Figures**

Figure 1	OMS Key Ladder Functional Diagram.....	6
Figure 2	Root Key Derivation Functionality.....	7

---

# 1 Abstract

This cryptographic key ladder standard defines a set of key ladder profiles, additional requirements and test vectors for a key ladder implementation.

## 1.1 Background

This standard is an extension of the ETSI TS 103 162 [1] standard for a key ladder, by further defining certain aspects and providing test vectors to enable implementers to verify certain aspects of an implementation.

The use of a standard key ladder is part of enabling any television receiving device to receive scrambled television content from any television distribution network, independent of the network conditional access security system in use.

However, use of ETSI TS 103 162 [1], described below as Profile 0, is discouraged as it allows use of undisclosed algorithms and therefore undisclosed and unknown intellectual property. This standard specifies certain processes which are both necessary for interoperability and not specified in the ETSI standard.

## 1.2 Introduction

The key ladder is a standard for enabling and securing the delivery of content descrambling keys from a source device to a sink device. The key ladder derivation is described in this standard, and is a component of a larger system, referred to in this standard as the Open Media Security (OMS).

The basis of the key ladder standard is a three-step key ladder and challenge-response authentication scheme in which the base key derivation inputs are protected within the one-time programmable memory (OTP) of the sink device's hardware (e.g. chipset). The key ladder is used primarily for the delivery of content descrambling keys while the challenge-response mechanism is used for checking the integrity and authenticity of sink devices as well as messages arriving from a source.

The key ladder standard is designed to support dynamic substitution and replacement of either sink or source device in a manner that maintains the security and integrity of the underlying content distribution network. The standard enables the portability of sink devices between content distribution networks by permitting the field upgradeability of sink devices to work with previously unknown source devices. The standard also enhances the capability of networks to upgrade their source devices without disrupting the capabilities of already fielded sink devices.

The source device is expected to be a key management system such as a traditional CAS or DRM solution deployed by a content distribution network,