SCTE · ISBE

STANDARDS

Digital Video Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 201 2018

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

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational 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•ISBE 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•ISBE members.

SCTE•ISBE 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 documents.

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•ISBE 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•ISBE web site at http://www.scte.org.

140 Philips Road
Exton, PA 19341

Table of Contents

List of Tables

List of Figures

1 Abstract

This document is identical to SCTE 201 2013 except for informative components which may have been updated such as the title page, NOTICE text, headers and footers. No normative changes have been made to this document.

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