

# SCTE • ISBE<sup>®</sup>

## S T A N D A R D S

---

**Digital Video Subcommittee**

---

**AMERICAN NATIONAL STANDARD**

**ANSI/SCTE 52 2018**

**Data Encryption Standard – Cipher Block Chaining  
Packet Encryption Specification**

ANSI/SCTE 52 2018

## 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>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2018  
140 Philips Road  
Exton, PA 19341

ANSI/SCTE 52 2018

**TABLE OF CONTENTS**

1.0	SCOPE .....	4
2.0	REFERENCES .....	5
3.0	DEFINITIONS .....	6
4.0	PACKET ENCRYPTION SPECIFICATION .....	8
	APPENDIX A: EXAMPLES OF DIFFERENT CIPHER BLOCK PROCESSING METHODS .....	12

**LIST OF FIGURES**

FIGURE 1 – NOTATION AND SYMBOLISM	7
FIGURE 2 – BASIC DES CBC	9
FIGURE 5 - BASIC DES CBC EXAMPLE	12
FIGURE 6 - RESIDUAL TERMINATION BLOCK PROCESSING EXAMPLE	13
FIGURE 7 - SOLITARY TERMINATION BLOCK PROCESSING EXAMPLE	14

## ANSI/SCTE 52 2018

### 1.0 SCOPE

This document is identical to SCTE 52 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.

#### 1.1 Purpose

This document defines a method for encrypting MPEG-2 transport stream packets using the Data Encryption Standard (DES) Cipher Block Chaining (CBC) encryption standard.

#### 1.2 Organization

The sections of this document are organized as follows:

- **Section 1** — Provides this general introduction.
- **Section 2** — Lists applicable documents.
- **Section 3** — Provides a list of acronyms and abbreviations used in this document.
- **Section 4** — Discusses packet encryption.
- **Appendix A** — Provides examples of different Cipher Block termination methods.