Society of Cable Telecommunications Engineers

ENGINEERING COMMITTEE
Digital Video Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 52 2013

Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability 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 Standards. Such adopting party assumes all risks associated with adoption of these Standards, 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 standard may require the use of subject matter covered by patent rights. By publication of this standard, 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 standard 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.

140 Philips Road
Exton, PA 19341

TABLE OF CONTENTS

LIST OF FIGURES

1.0 SCOPE

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.

2.0 REFERENCES

2.1 Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of the standard. At the time of Subcommittee approval, the editions indicated were valid. All standards are subject to revision; and while parties to any agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents may not be compatible with the referenced version.

1. Federal Information Processing Standards Publication (FIPS PUB) 46-3[†], Data Encryption Standard (DES); specifies the use of Triple DES, available at http://csrc.nist.gov/publications/PubsFIPSArch.html
2. FIPS PUB 74[†], Guidelines for Implementing and Using the National Bureau of Standards (NBS) Data Encryption Standard, available at http://csrc.nist.gov/publications/PubsFIPSArch.html
3. FIPS PUB 81[†], DES Modes of Operation, available at http://csrc.nist.gov/publications/PubsFIPSArch.html
4. ISO/IEC 13818-1:2013 | ITU-T Rec. H.222.0 Information technology – Generic coding of moving pictures and associated audio information: Systems

2.2 Informative References

The following documents may provide valuable information to the reader but are not required when complying with this standard.

5. NBS PUB 500-20, Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard

[†] The U.S. National Institute of Standards and Technology has withdrawn this standard on May 19th, 2005, but the document is still publicly available at the given link.

3.0 DEFINITIONS

3.1 Compliance Notation

"SHALL"	This word or the adjective "REQUIRED" means that the item is an absolute requirement of this specification.
"SHALL NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighted before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

3.2 Acronyms and Abbreviations

The following acronyms and abbreviations are used within this specification:

CBC Cipher Block Chaining

CW Control Word

DES Data Encryption Standard

ECM Entitlement Control Message

EMM Entitlement Management Message

FIPS Federal Information Processing Standard

NBS National Bureau of Standards

XOR Exclusive Or

3.3 Conventions and Symbolism

The bit numbering convention used in FIPS documentation differs from the commonly used engineering notation as described below in Figure 1.

Figure 1 also depicts the symbols used in this standard. A **bold** rectangular block (labeled "DES") symbolizes the DES Encrypt Function, and a normal (or non-bold) rectangular block (labeled "DES") symbolizes the DES Decrypt Function.

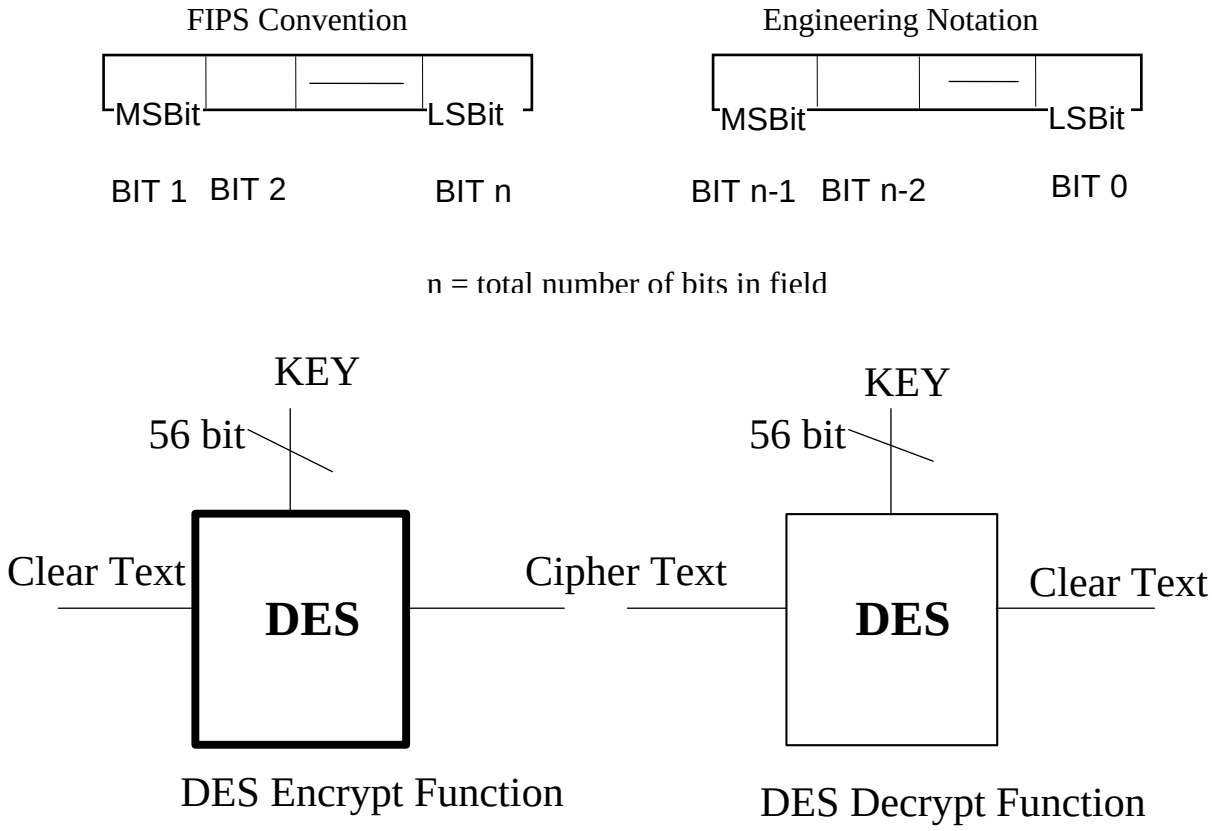

Figure 1 – Notation and Symbolism

4.0 PACKET ENCRYPTION SPECIFICATION

4.1 Use of DES CBC for MPEG-2 Transport Stream Packet Payloads

The DES CBC packet encryption methods explained in this standard, and used for MPEG-2 transport stream packets SHALL comply with the scrambling requirements defined in ISO/IEC 13818-1 [5]. Of primary importance in [5] for this standard is the requirement that only MPEG-2 transport stream packet payloads are to be encrypted (or decrypted). That is, the MPEG-2 transport packet header and the adaptation field of the packet, when present, are not to be encrypted (or decrypted).

4.2 Basic DES Cipher Block Chaining

DES packet encryption permits the encryption and decryption of packet data such as audio, video, or data. This is performed using DES Cipher Block Chaining, as specified in [2], pg. 16 and [3], pg. 5. Figure 2 shows basic DES CBC, which SHALL be used to encrypt and decrypt packet payloads that contain an integer number of 8-byte blocks.

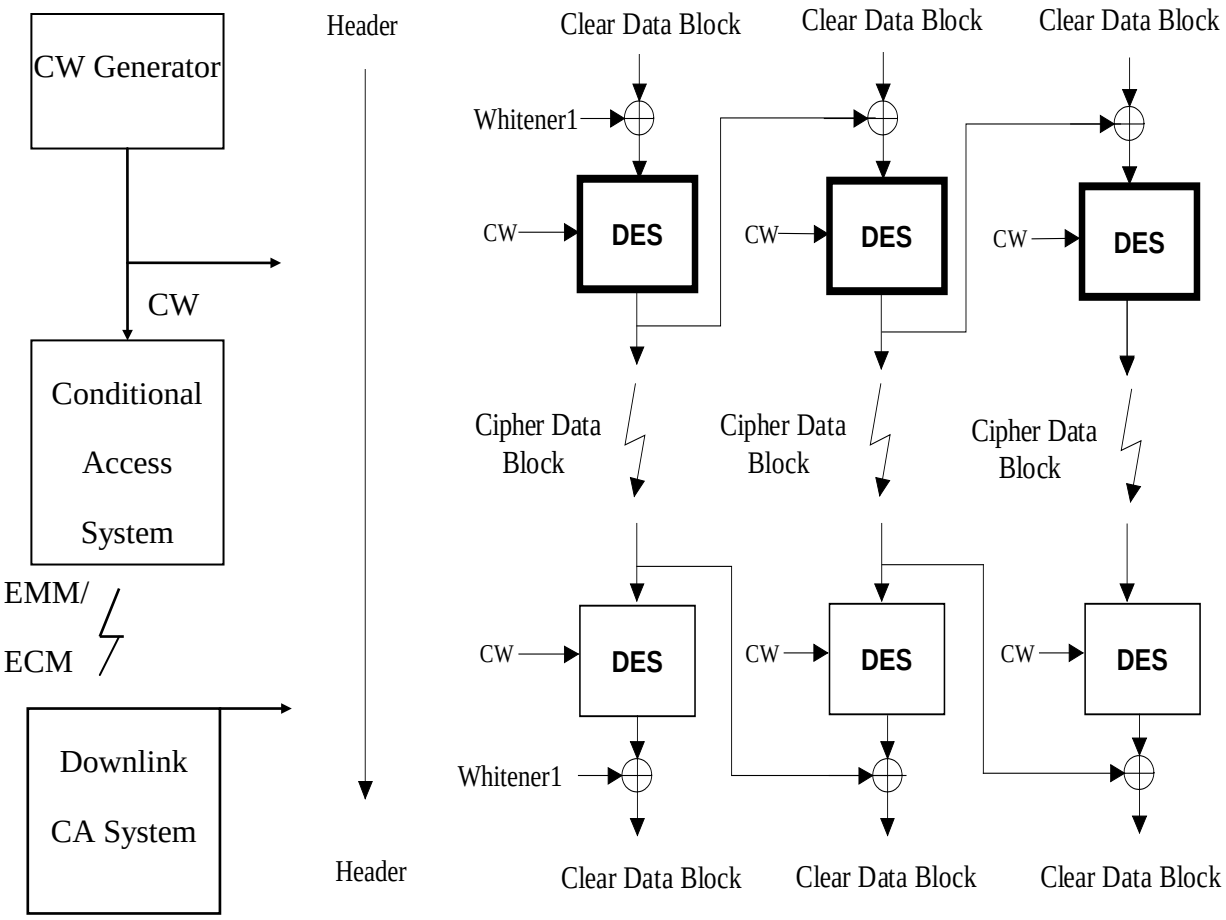

Figure 2 – Basic DES CBC

Notes: The Whitener1 is a fixed 64-bit random value. The CW (Control Word) is a fixed or a programmable value.

4.3 Residual Termination Block Processing

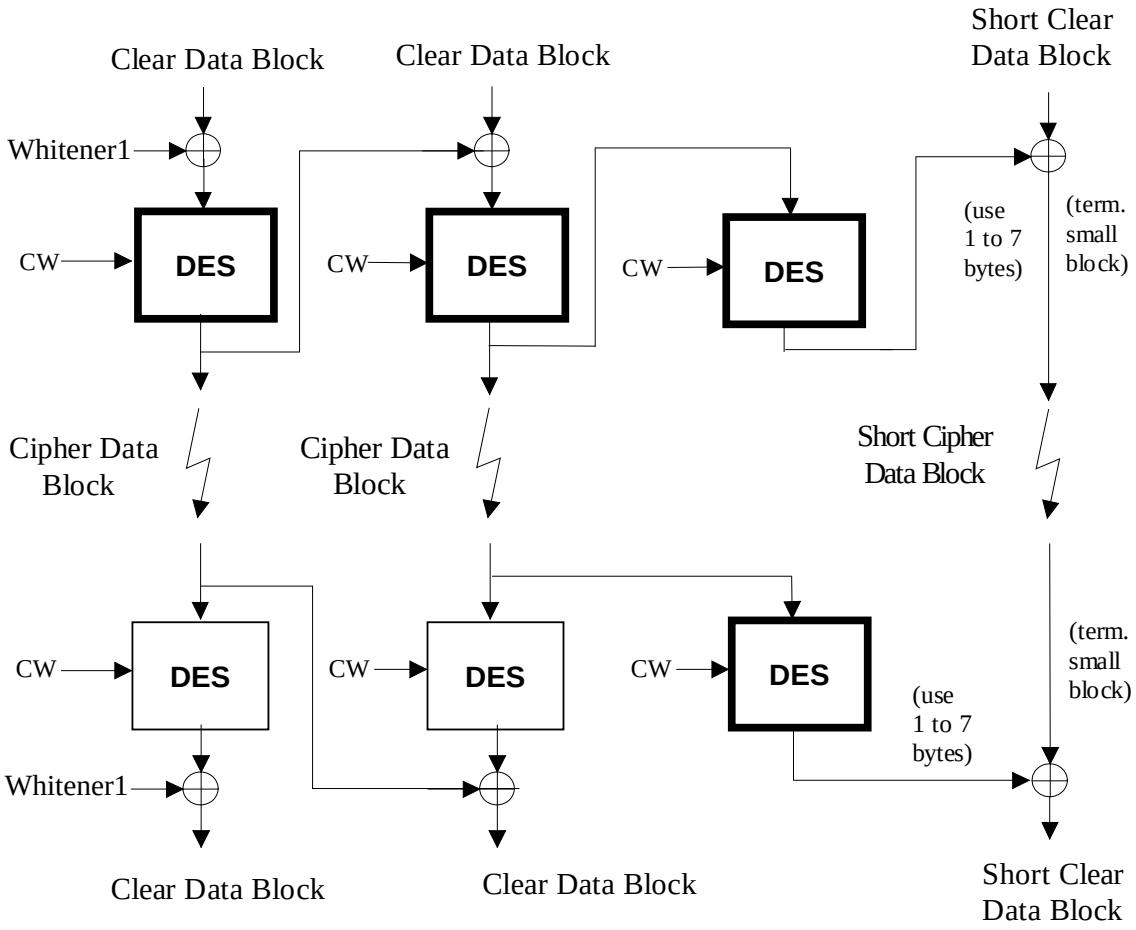

Figure 3 - Residual Termination Block Processing

Note the exception handling of a small block of data less than 8 bytes, following a non-zero number of 8-byte blocks might occur with a packet payload not equal to an integer number of 8-byte blocks such as a payload of an odd length. This is called "termination block processing." Note that this is not encryption of packet data, but XOR of packet data with a quantity generated by encryption. The 1 to 7 bytes (of the quantity generated by encryption) used for XOR with packet data SHALL be the leftmost. It is similar to Output Feedback Processing in that regard, in that the Encoder and Decoder form identical quantities to XOR on the packet data. This differs from non-termination block (basic DES) CBC, where packet data is encrypted at the encoder and decrypted at the decoder. The DES operation for this mode is encryption in both Encoder and Decoder, not decrypt in one and encrypt in the other. The Residual Termination Block Processing as explained above and illustrated in Figure 3 SHALL be used for packet payloads containing a residual termination block, with less than 8 bytes of data, following a non-zero number of 8-byte blocks.

4.4 Solitary Termination Block Processing

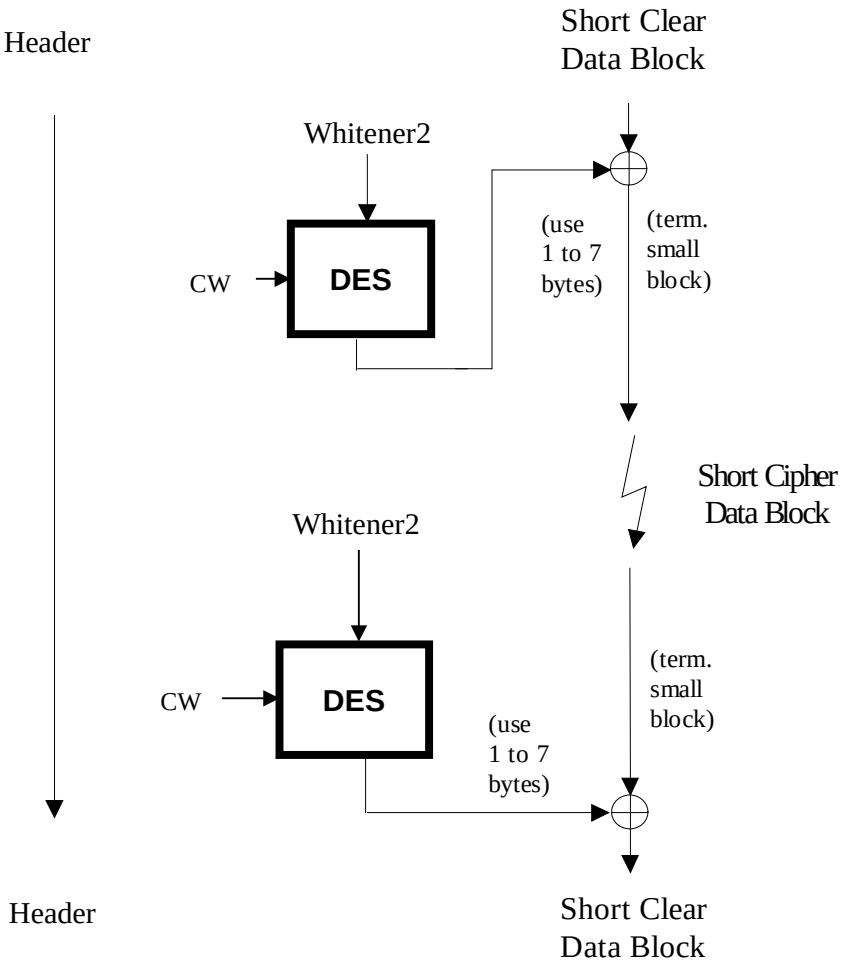

Figure 4 - Solitary Termination Block Processing

Note: The Whitener2 is not equal to Whitener1 in value, and is a fixed 64-bit random value.

There is another special case of termination block processing that is not covered in the FIPS documents. An MPEG-2 packet can have an adaptation header that can allow arbitrary amounts of undefined information to be part of a packet header, which may result in a very small actual data payload that could be less than 8 bytes. This special case could result in the termination block of less than 8 bytes being the only data in the packet - the termination block would be the first and last block in that case. Note that no DES operation is performed on packet data but XOR of packet data is performed with the same quantity generated by encryption in both Encoder and Decoder. The 1 to 7 bytes (of the quantity generated by encryption) used for XOR with packet data SHALL be the leftmost. The Solitary Termination Block Processing as explained above and illustrated in Figure 4 SHALL be used for packet payloads containing less than 8 bytes.

APPENDIX A: EXAMPLES OF DIFFERENT CIPHER BLOCK PROCESSING METHODS

This appendix provides example data which MAY be used to confirm the understanding of the three different cipher block processing methods illustrated in the standard. Note that the data strings in the below examples use hex digits and follow the FIPS convention described in section 3.3.

A.1 Basic Cipher Block Chaining Example

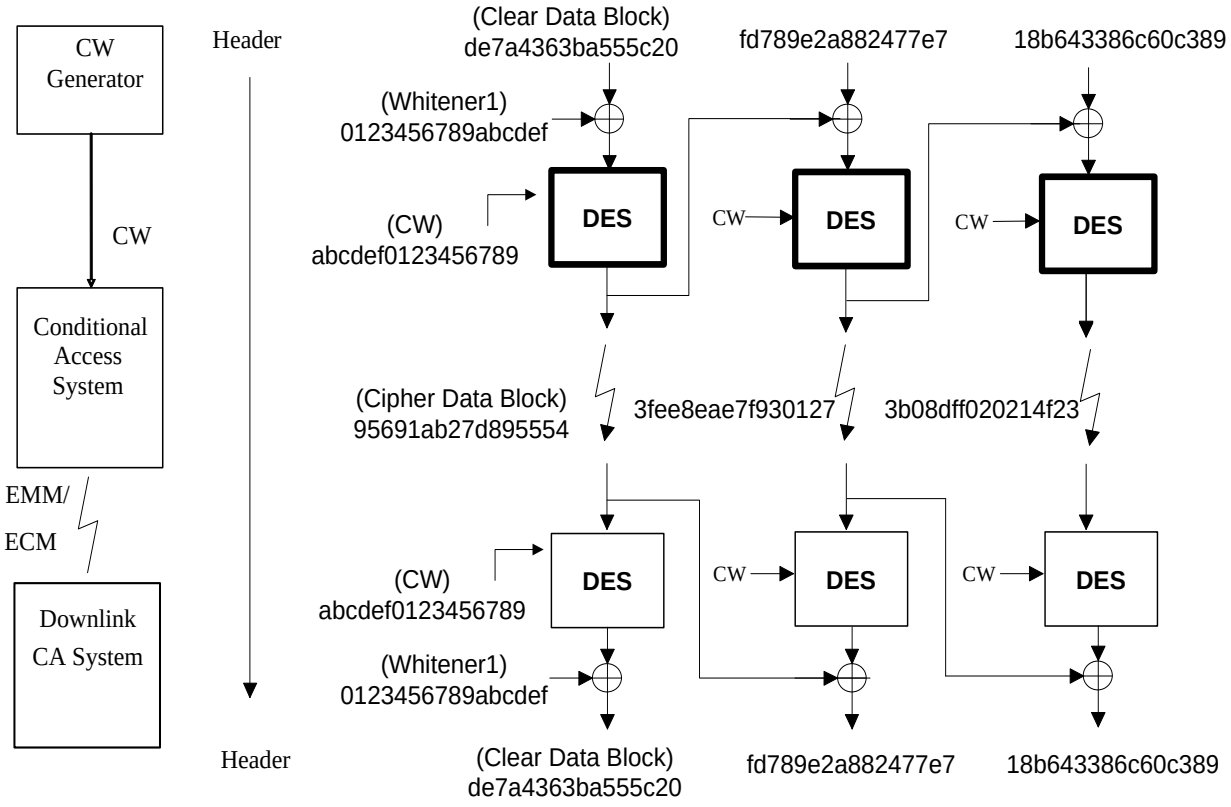

Figure 5 - Basic DES CBC Example

A.2 Residual Termination Block Processing Example

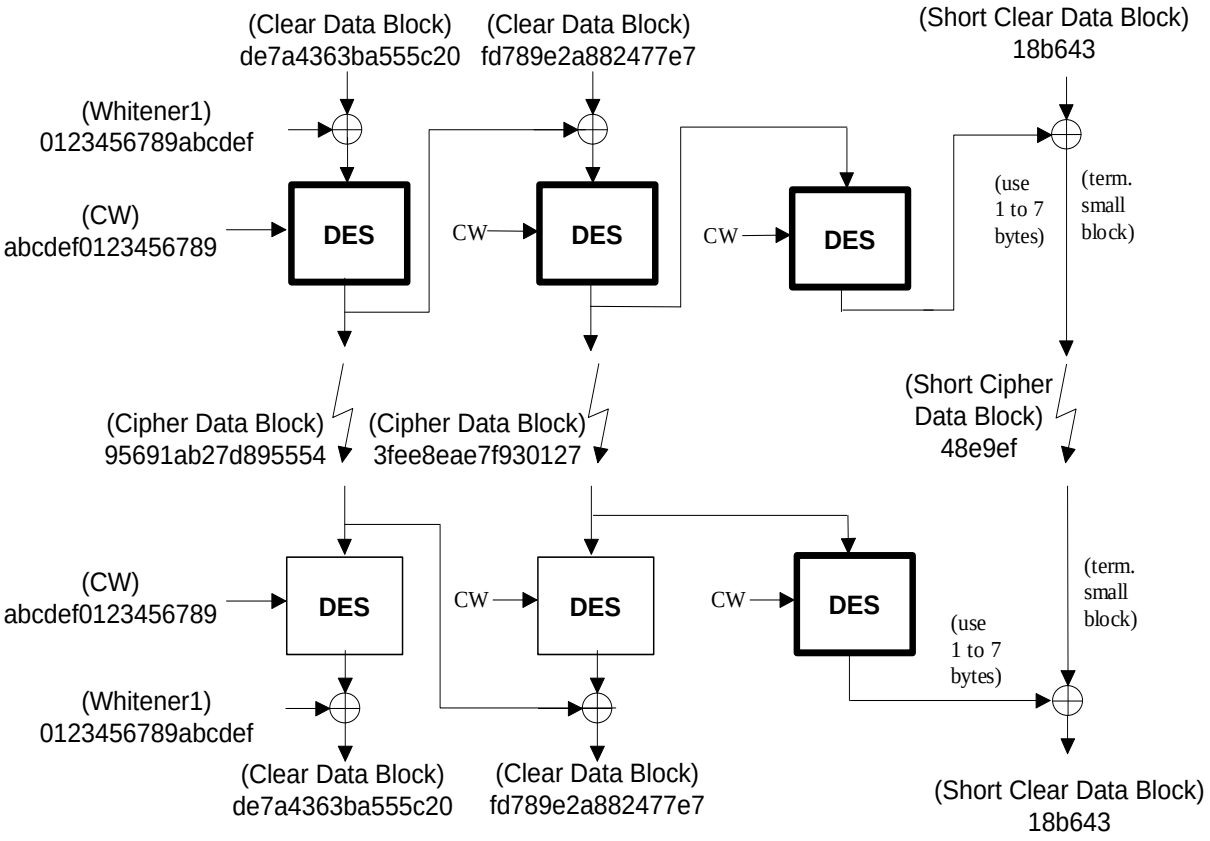

Figure 6 - Residual Termination Block Processing Example

A.3 Solitary Termination Block Processing Example

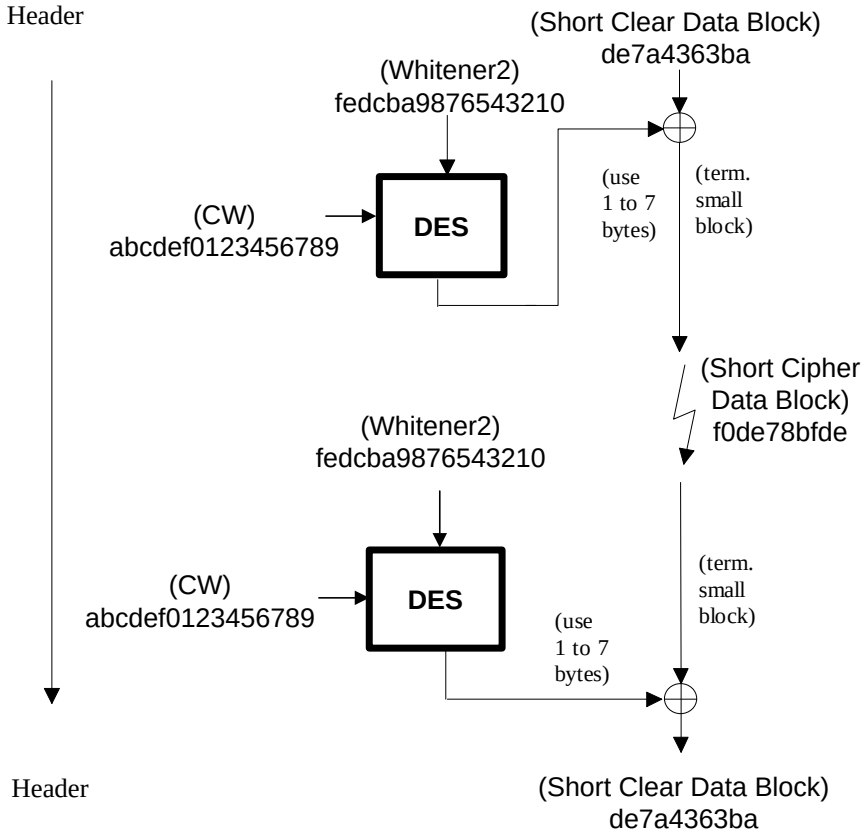

Figure 7 - Solitary Termination Block Processing Example