Amendment 2:2012 to
SMPTE 430-3-2008

SMPTE STANDARD

D-Cinema Operations — Generic Extra-Theater Message Format — Amendment 2

Table of Contents

Page

Approved
August 22, 2012

Foreword

SMPTE (the Society of Motion Picture and Television Engineers) is an internationally-recognized standards developing organization. Headquartered and incorporated in the United States of America, SMPTE has members in over 80 countries on six continents. SMPTE's Engineering Documents, including Standards, Recommended Practices, Engineering Guidelines and Registered Disclosure Documents, are prepared by SMPTE's Technology Committees. Participation in these Committees is open to all with a bona fide interest in their work. SMPTE cooperates closely with other standards-developing organizations, including ISO, IEC and ITU.

SMPTE Engineering Documents are drafted in accordance with the rules given in Part XIII of its Administrative Practices.

SMPTE Amendment 2 to SMPTE 430-3 was prepared by Technology Committee 21DC.

1 Scope

Since the publication of SMPTE 430-3-2008, “D-Cinema Operations Generic Extra-Theater Message Format”, the following amendments have been identified:

The amendments have also been incorporated into SMPTE ST 430-3:2012.

2 Amendment of Section 7.1.1

7.1.1 EncryptionMethod

The last paragraph of this section:

> All ETMs shall use the mode for RSA called Optimal Asymmetric Encryption Padding (OAEP), which is specified in [PKCS1]. However, the OAEP Parameter is omitted, which causes OAEP to use a default ciphertext redundancy value. This choice was made to simplify the implementation and to avoid features that are not widely supported in an interoperable manner.

Shall be replaced by:

> All ETMs shall use the mode for RSA called Optimal Asymmetric Encryption Padding (OAEP), which is specified in [PKCS1]. The OAEP Parameter shall be omitted, causing OAEP to use a default ciphertext redundancy value. The OAEP digest algorithm shall be limited to SHA-1. The DigestMethod element shall be present and the Algorithm attribute shall be set to the URI value "***http://www.w3.org/2000/09/xmldsig#sha1***". These choices were made to simplify the implementation and to avoid features that are not widely supported in an interoperable manner.