ISO 20215:2015-08 (E)

Space data and information transfer systems - CCSDS cryptographic algorithms

Contents

Page

1 INTRODUCTION **1-1**

1.1 PURPOSE OF THIS RECOMMENDED STANDARD 1-1
1.2 SCOPE 1-1
1.3 APPLICABILITY 1-2
1.4 RATIONALE 1-2
1.5 DOCUMENT STRUCTURE 1-2
1.6 NOMENCLATURE 1-2
1.7 REFERENCES 1-3

2 OVERVIEW **2-1**

2.1 GENERAL OVERVIEW 2-1
2.2 ENCRYPTION OVERVIEW 2-1
2.3 AUTHENTICATION/INTEGRITY OVERVIEW 2-2
2.4 AUTHENTICATED ENCRYPTION 2-3

3 ENCRYPTION ALGORITHMS **3-1**

3.1 ALGORITHM AND MODE 3-1
3.2 CRYPTOGRAPHIC KEY SIZE 3-1
3.3 ALGORITHM MODE OF OPERATION 3-1
3.4 AUTHENTICATED ENCRYPTION 3-1

4 AUTHENTICATION ALGORITHMS **4-1**

4.1 OVERVIEW 4-1
4.2 CCSDS HASH MESSAGE BASED AUTHENTICATION 4-1
4.3 CIPHER-BASED AUTHENTICATION 4-2
4.4 DIGITAL SIGNATURE BASED AUTHENTICATION 4-2

ANNEX A SECURITY, SANA, AND PATENT CONSIDERATIONS (INFORMATIVE) **A-1**
ANNEX B INFORMATIVE REFERENCES (INFORMATIVE) **B-1**
ANNEX C ABBREVIATIONS AND ACRONYMS (INFORMATIVE) **C-1**