ETSI TS 104 053-4 V1.1.1 (2024-07)

TETRA Air Interface Security, Algorithms Specifications; Part 4: TETRA Authentication and Key Management Algorithms TAA2

Reference

DTS/TCCE-06214

Keywords

air interface, DMO, security, TETRA, V+D

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

The present document is part 4 of a multi-part deliverable covering the specifications of the TETRA standard encryption, authentication and key management algorithms, as identified below:

Part 1: "TETRA Encryption Algorithms Set A";

Part 2: "TETRA Encryption Algorithms TEA Set B";

Part 3: "TETRA and Authentication and Key Management Algorithms TAA1";

Part 4: "TETRA Authentication and Key Management Algorithms TAA2".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies each algorithm in the suite of authentication and key management algorithms TAA2, each designed to meet the requirements set out in the requirements specification [i.1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 100 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] TCCE(22)000038 / TCCE06(22)000018: "Requirements Specification for additions to the TETRA Authentication and Key Management Algorithm Suite, Revision 2".

[i.2] Daemen, J. and Rijmen, V. (1999): "AES proposal: Rijndael", document version 2. Submission to NIST AES competition (1999).

[i.3] Black, J., Rogaway, P. and Shrimpton, T. (2002): "Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV", in Yung, M. (ed.) Advances in Cryptology - CRYPTO 2002. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 320-335. doi:10.1007/3-540-45708-9-21.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Cipher Key (CK): value used to determine the transformation of plain text to cipher text in a cryptographic algorithm

Encryption Cipher Key (ECK): cipher key used as input to the encryption algorithm where an air interface encryption algorithm from TEA set A is in use

Extended Cipher Key (CKX): value used to determine the transformation of plain text to cipher text in a cryptographic algorithm where an air interface encryption algorithm from TEA set B is in use

Initialization Value (IV): sequence of symbols that randomize the KSG inside the encryption unit

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CCK-id	CCK identifier
CCKX	eXtended Common Cipher Key
CK	Cipher Key
CKX	eXtended Cipher Key
DCK	Derived Cipher Key

NOTE: DCK1 and DCK2 are components of the Derived Cipher Key.

DCKX	eXtended Derived Cipher Key
ECK	Encryption Cipher Key
GCK	Group Cipher Key
GCKN	Group Cipher Key Number
GCK-VN	GCK-Version Number
GCKX	Extended Group Cipher Key
GSKO	Group Session Key for OTAR
GSKO-VN	GSKO-Version Number
GSKOX	Extended Group Session Key for OTAR
IV	Initialization Value
K2	authentication Key
KS, KS'	Session authentication Key
KSG	Key Stream Generator
KSO	Session Key for OTAR
KSOX	eXtended Session Key for OTAR
MF	Manipulation Flag
MGCKX	eXtended Modified Group Cipher Key
MNI	Mobile Network Identity
RAND1	RANDom challenge 1
RAND2	RANDom challenge 2
RES	RESponse
RS	Random Seed
RSO	Random Seed for OTAR
SCCKX	Sealed Extended Common Cipher Key
SCK	Static Cipher Key
SCKN	Static Cipher Key Number
SCK-VN	SCK-Version Number
SCKX	eXtended Static Cipher Key
SGCKX	Sealed Extended Group Cipher Key
SGSKOX	Sealed Extended Group Session Key for OTAR
SSCK	Sealed Static Cipher Key
SSCKX	Sealed Extended Static Cipher Key
TAA1	TETRA Authentication Algorithm set 1
TAA2	TETRA Authentication Algorithm set 2
TEA	TETRA Encryption Algorithm

NOTE: Used with specific numeric algorithm identity e.g. TEA5.

XOR eXclusive OR

4 Introduction

4.0 General

The set of algorithms TAA2 described in the present document are the associated algorithms used for providing TETRA air interface authentication and key management as specified in detail by ETSI TS 100-392-7 [1].

The present document is organized as follows. Notations and definitions for TAA2 are covered in clauses 4.1 and 5 provides the specification of all TAA2 algorithms.

4.1 Notation and Definitions

The inputs and outputs of the TAA2 algorithms are always sequences of bits. A Boolean value is represented by single bit, with 0 denoting False and 1 denoting True.

The notation A || B has been used to denote concatenation of two sequences of bits A and B, meaning a sequence of bits consisting of the bits of sequence A followed by those of the sequence B.

Many algorithm definitions involve interpreting a sequence of bits, of length 8n for some n, as a sequence of bytes of length n, and vice versa. In this correspondence the first bit appears as the most significant bit of the first byte, the second bit as the second most significant bit of the first byte, …, and the last bit as the least significant bit of the last byte. More precisely, a bit sequence B[1], …, B[8n] corresponds to the byte sequence b[1], …, b[n],

where $b[i] = 2^7B[8i-7] + 2^6B[8i-6] + \ldots + B[8i]$ for i = 1, …, n

When the length of a sequence of bits is not a multiple of 8, it is represented by the sequence of bytes corresponding to the sequence of bits padded with the smallest number of 0s required to make its length a multiple of 8.

C(i) is used to denote the sequence of 8 bits corresponding to the single byte with integer value i, using the correspondence just defined: so, for example, C(5) is the 8-bit sequence 0, 0, 0, 0, 0, 1, 0, 1. The argument i is written in decimal.

For any m in the set {128, 192, 256} and n in the set {128, 192, 224, 256}, the notation Rijndael(Km, Bn) is used to denote the variant of Rijndael [i.2] with m-bit key and n-bit block size. Rijndael with block size n = 224 is defined in section 12.1 of [i.2].

In [i.2], the Rijndael plaintext block, ciphertext block and key are all expressed as arrays of bytes. In this specification, Rijndael plaintext blocks, ciphertext blocks and keys are referred to as arrays of bits. The correspondence mentioned above applies here, interpreting sequences of bits as sequences of bytes and vice versa.

For any two sequences A and B of bits of the same length, A ⊕ B is defined as the bit sequence whose bit in any position is the XOR of the bits from A and B in the corresponding position. This also defines an operation a ⊕ b on byte sequences, via our identification of a byte sequence with a corresponding bit sequence.

The notation Z(n) denotes a sequence of n bits, each with value 0.

For some algorithms a function H(M, n) is used to produce an n-bit sequence which is the hash of an m-bit message M, for m ≥ 1 and n ≥ 256. H is calculated as follows:

Write M || Z = M_1 || … || M_r, where r = ⌈m/256⌉, the smallest integer ≥ the floating-point quotient m / 256; Z is the sequence of 256r-m bits, each 0; and M_1, …, M_r are each 256 bits long. (In our applications, r will be either 1 or 2. In each particular application, the length of M will be fixed.)

1) Set X to be the sequence of 256 bits, each 0.

2) For i := 1 to r do:

   a) Let C be the result of encrypting the block X under Rijndael (K256, B256) with key M_i.

b) Set X := C ⊕ X.

3) Return the first n bits of X as the function result.

Note that this is construction f5 from [i.3], also widely referred to as the Davies-Meyer scheme.

The function H(M,n) is illustrated in figure 1.

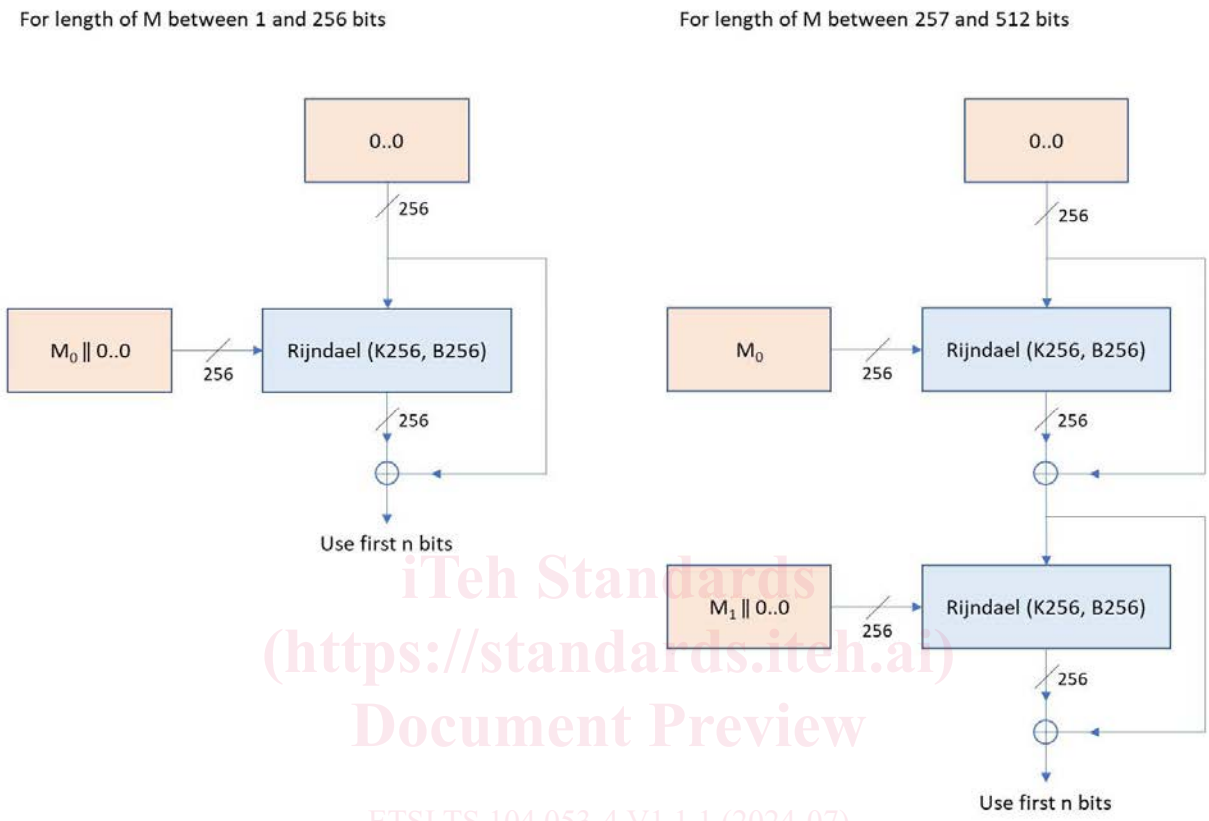

Figure 1: The Function H(M,n)

5 Specifications

5.1 TA13

5.1.1 Inputs and Outputs

- Input 1: K2, a sequence of bits of length 256
- Input 2: RS, a sequence of bits of length 80
- Output 1: KS, a sequence of bits of length 128
- Output 2: KS', a sequence of bits of length 128

5.1.2 Algorithm Definition

- Encrypt the block RS || Z(168) || C(13) under Rijndael (K256, B256) with key K2.

Take the first 128 bits of the ciphertext to be KS and the latter 128 bits to be KS' TA13 is illustrated in figure 2.

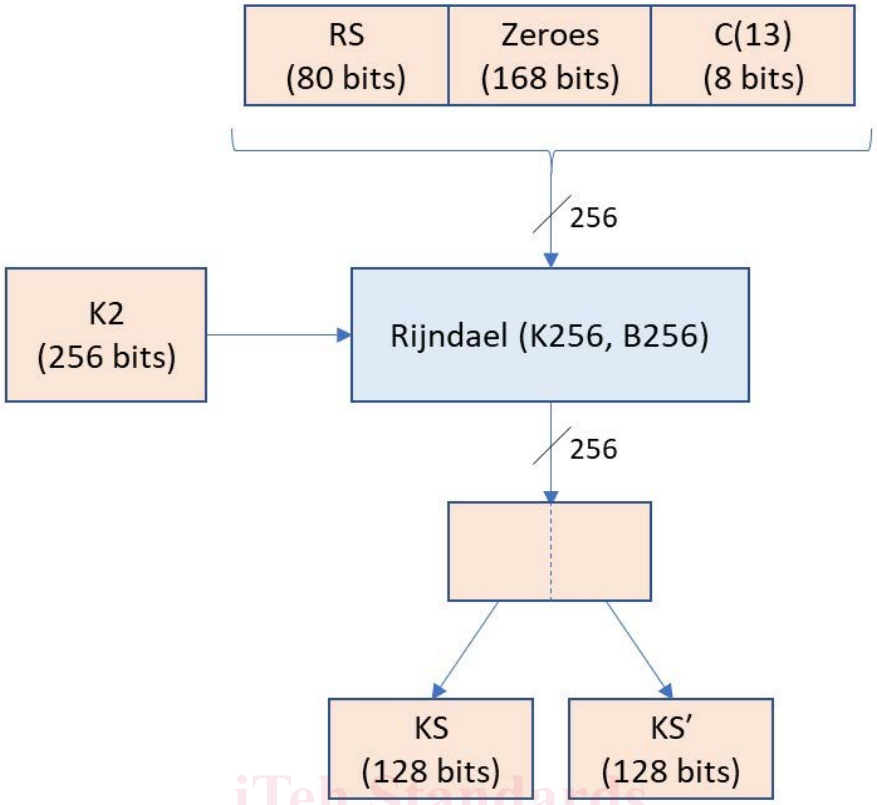

Figure 2: TA13

5.2 TA14

5.2.1 Inputs and Outputs

- Input 1: KS, a sequence of bits of length 128
- Input 2: KS', a sequence of bits of length 128
- Input 3: RAND1, a sequence of bits of length 80
- Input 4: RAND2, a sequence of bits of length 80
- Output: DCKX, a sequence of bits of length 192

5.2.2 Algorithm Definition

1) Encrypt the block RAND1 || RAND2 || Z(88) || C(14) under Rijndael (K256, B256) with key KS || KS'.
2) Take the first 192 bits of the ciphertext to be DCKX.

TA14 is illustrated in figure 3.

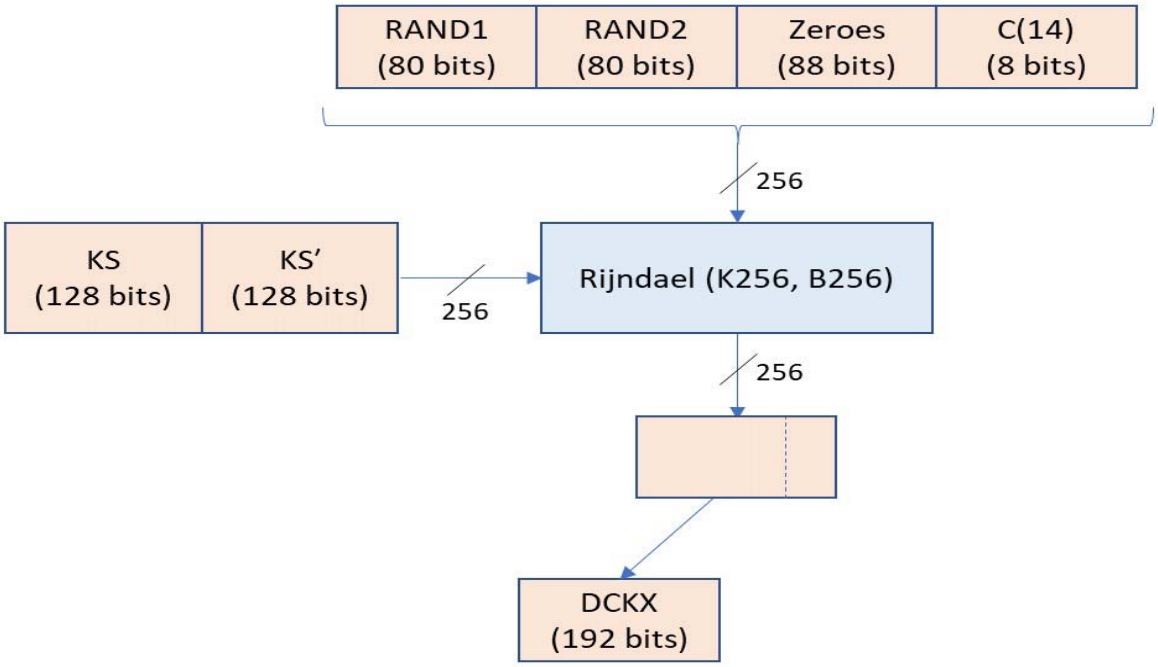

Figure 3: TA14

5.3 TA15

5.3.1 Inputs and Outputs

- Input 1: KS, a sequence of bits of length 128
- Input 2: KS', a sequence of bits of length 128
- Input 3: RAND1, a sequence of bits of length 80
- Output: (X)RES1, a sequence of bits of length 32

5.3.2 Algorithm Definition

1) Encrypt the block RAND1 || Z(168) || C(15) under Rijndael (K256, B256) with key KS || KS'.
2) Take the first 32 bits of the ciphertext to be (X)RES1.

TA15 is illustrated in figure 4.