EBU
OPERATING EUROVISION AND EURORADIO

TECH 3292

BISS2
BASIC INTEROPERABLE SCRAMBLING SYSTEM

Version 3.0

SPECIFICATION

Geneva
March 2018

Conformance Notation

This document contains both normative text and informative text.

All text is normative except for that in the Introduction, any section explicitly labelled as ‘Informative’ or individual paragraphs which start with ‘Note:’.

Normative text describes indispensable or mandatory elements. It contains the conformance keywords ‘shall’, ‘should’ or ‘may’, defined as follows:

‘Shall’ and ‘shall not’: Indicate requirements to be followed strictly and from which no deviation is permitted in order to conform to the document.

‘Should’ and ‘should not’: Indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others.

OR indicate that a certain course of action is preferred but not necessarily required.

OR indicate that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

‘May’ and ‘need not’: Indicate a course of action permissible within the limits of the document.

Default identifies mandatory (in phrases containing “shall”) or recommended (in phrases containing “should”) presets that can, optionally, be overwritten by user action or supplemented with other options in advanced applications. Mandatory defaults must be supported. The support of recommended defaults is preferred, but not necessarily required.

Informative text is potentially helpful to the user, but it is not indispensable and it does not affect the normative text. Informative text does not contain any conformance keywords.

A conformant implementation is one which includes all mandatory provisions (‘shall’) and, if implemented, all recommended provisions (‘should’) as described. A conformant implementation need not implement optional provisions (‘may’) and need not implement them as described.

Contents

BISS2 – Basic Interoperable Scrambling System

EBU Committee	*First Issued*	*Revised*	*Re-issued*
TC	2002	2018	2018

Keywords: Security, Scrambling, Satellite, AES-128, DVB-CISSA, Contribution, encryption, CA, conditional access; BISS1, BISS2.

1. Background

This document describes the revised version of the Basic Interoperable Scrambling System (BISS). It supersedes the 2002 version of the BISS protocol, referred to as BISS1 throughout this document. The new version of the protocol, BISS2, replaces the encryption and scrambling algorithms DES and DVB-CSA with more secure and robust state of the art algorithms; AES-128 for session word encryption and DVB-CISSA for stream scrambling, respectively.

It further expands the capabilities of the protocol with a fourth conditional access mode, BISS Mode CA. The additional mode addresses the commercial requirement of in-stream key exchange with real-time addition and revocation of receivers. BISS-CA further allows the sender to enforce stream security beyond the receiver either mandating additional features such as watermarking or pre-empting stream forwarding. Due to its complexity, BISS-CA is defined in the supplement EBU Tech 3292s1 [3].

2. Introduction

The absence of standard methods for the securing and scrambling of DSNG broadcasts has spawned the development of several different proprietary security mechanisms. This situation motivated the creation of the original BISS standard (BISS1) in 2002. BISS1 enabled broadcasters to combine equipment from several vendors, while making systems more future proof.

Since then, requirements for secure media transmission have evolved. While the original BISS core components became obsolete, further requirements arose with technological disruption of the media industry. A strong demand for a software- and IP-friendly standard, the possibility for in-stream key exchange, real-time addition/revocation of receivers, royalty free, while still remaining interoperable. This BISS (BISS2) version addresses all these requirements. It supports the same modes as BISS1 (mode 0, 1 and E) with an additional Conditional Access mode (Mode CA) that addresses the key management and real-time entitlement.

The Basic Interoperable Scrambling System version 2 (BISS2) is based on the DVB-CISSA specification [1]. In BISS2 Mode 1, a fixed key called Session Word (SW) is transmitted in clear to the receivers' operator.

The BISS2 specification Mode E (BISS2 with Encrypted keys – referred to as BISS2 - E) introduces an additional mechanism to accept the insertion of Encrypted Session Words (ESWs). The session words are encrypted using the AES-128 [2] cipher. This mechanism is backward compatible with BISS specification Mode 1.

The BISS2 specification Mode CA (BISS2 with real-time conditional access – BISS2 - CA) introduces an automated mechanism to add and revoke receivers. It is based on RSA asymmetric key cryptography and use EMM and ECM messages to control the session entitlement. It is fully defined in the BISS supplement document EBU Tech 3292s1 [3].

3. Glossary

Throughout this document, the following definitions are used:

Scrambler	Overall mechanisms required to meet the DVB-CSA1 or DVB-CISSA specification.
Session Word	*Sword* assigned during a transmission by the Management Centre.
Receiver	Relates to a device for which this specification might apply.
Management Centre	Refers to an organization controlling or managing the conditional access system.
AES	Advanced Encryption Standard, fast symmetric encryption standard.
BISS	Basic Interoperable Scrambling System
BISS1	BISS version 1 with CSA1 for TS scrambling and DES for session word encryption.
BISS2	BISS version 2 with DVB CISSA replacing CSA1 and AES128 replacing DES.
BISS CA	BISS Conditional Access mode allowing secure key transmission in the MPEG transport stream.
bslbf	Bit string, left bit first
CA	Conditional Access
CAT	Conditional Access Table
CBC	Cipher Block Chaining
CISSA	DVB CISSA Common IPTV Software oriented Scrambling Algorithm
CSA	(DVB) Common Scrambling Algorithm
CW	Control Word
DES	Data Encryption Standard
DSNG	Digital Satellite News Gathering
DVB	Digital Video Broadcasting
ECM	Entitlement Control Message
EMM	Entitlement Management Message
ES	Elementary stream
ESID	Entitlement session ID
ESK	Encrypted Session Key
ESW	Encrypted Session Word
IRD	Integrated Receiver Decoder
lsb	Least Significant Bit
LSB	Least Significant Byte

MC	Management Centre
msb	Most Significant Bit
MSB	Most Significant Byte
PAT	Programme Association Table
PID	Programme Identification number
PMT	Programme Map Table.
RSA	Rivest–Shamir–Adleman asymmetric cryptosystem
SK	Session key, key transmitted through the EMM
SW	Session word, scrambling key transmitted through the ECM
Uimsbf	Unsigned integer, most significant bit first.

4. BISS2 Operational Modes

The Scrambler shall support the following four (4) modes of operation:

- **Mode 0**: No scrambling is applied.
- **Mode 1**: Components are scrambled by a Session Word (SW), and the SW is transmitted out of band in clear to the receivers.
- **Mode E**: Components are scrambled by a Session Word (SW), the SW is encrypted with a fixed Session Key (SK) and the resulting Encrypted Session Word (ESW) is transmitted out of band to the receivers.
- **Mode CA**: Components are scrambled with a Session Word (SW), the SW is encrypted with a Session Key (SK), and the resulting Encrypted Session Word (ESW), along with the key information is transmitted in-stream to receivers. Both SW and SK are dynamically changed during the live event transmission.

The scrambling mechanism, as defined in the DVB-CSA for BISS1 and DVB CISSA [2] for BISS2, shall be applied at the Transport Stream level only. A Conditional Access Table (CAT) shall be present in the TS for BISS Mode 1 and Mode E, although the table shall be empty as no Entitlement Management Message (EMM) stream will be present in these modes. The CAT table is used in conjunction with EMM and ECM messages in Mode CA.

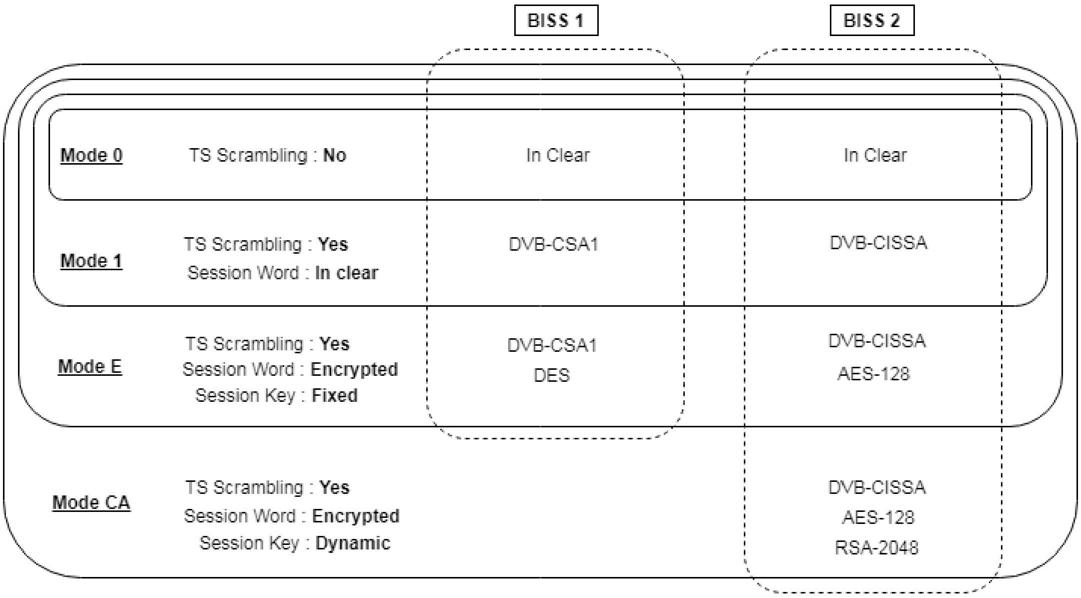

Figure 1: BISS1 and BISS2 Standards & Mode Overview

A scrambler that only supports a subset of the defined modes of operation, for BISS1 or BISS2, must do so according to an imposed hierarchy (see Figure 1). As an example, a Scrambler providing support for BISS2 Mode CA must also support BISS2 Modes 0, 1 and E.

4.1 BISS2-0

The Scrambler must be capable of disabling the scrambling operation. In this mode, there will be no CA_descriptor in the **Programme Map Table** (PMT) and no **Entitlement Control Message** (ECM) stream. The Transport_Scrambling_Control bits of the Transport Packets will be set to “00”.

4.2 BISS2-1

4.2.1 Description

This mode has been designed specifically for DSNG applications, fly-away operations, emergency situations, etc. It may also be used as a fall-back solution while using the complete BISS2-E system. In Mode 1, a fixed 32 character SW is inserted in the scrambler. The 32 character (128-bit) SW is used as a scrambling key according to the DVB-CISSA specification as defined in ETSI TS 103 127 section 6 [1].

- Manual entry of the SW shall be in hexadecimal notation, with the digits entered most-significant-nibble first, i.e. from left to right as viewed in hexadecimal notation, in sequence of 8 characters.
- Remote entry of the SW shall also be provided, although the specification of that interface is beyond the scope of this document.
- The Scrambler shall ensure that the SW cannot be changed more than ten times in a 5-minute period and that there is a minimum of 10 seconds between changes.

In this mode there will be a **CA_descriptor** in the PMT, present at programme level, but no ECM stream. A single unique **CA_System_ID (0x2602)** is assigned to identify BISS2 in mode 1 and E.

- The **Transport_Scrambling_Control** bits of the Transport Packets shall be set to “10” (even key) or "11" (odd key) as specified in [1].

4.2.2 CA Descriptor

The **CA_descriptor** which must be present in the PMT to support BISS2 is defined in Table 1.

- **CA_system_ID**: this is a 16-bit field indicating the type of CA system applicable for the associated ECM streams. The value of this field for BISS2 Mode 1 and E is **0x2602**.
- CA_PID: this is a 13-bit field indicating the Packet Identification Number (PID) of the Transport Stream packets that shall contain the ECM information. For BISS2 Modes 1 and E, no ECM information is required, so this field shall contain the value **0x1FFF**.

Table 1: Conditional Access descriptor.

Syntax	No. of bits	Mnemonic
ca_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
CA_system_ID	16	uimsbf
reserved	3	bslbf
CA_PID	13	uimsbf
}		

4.3 BISS2-E

4.3.1 Receiver identifiers

This document specifies two types of identifiers for each receiver:

- An **injected identifier (IDi)** which is a secret key embedded in the receiver. This ID is mandatory for any BISS2 compliant receiver.
- A **buried identifier (IDb)** defined by the manufacturer and linked uniquely to the device itself. This identifier is not mandatory, but if implemented it shall comply with this document.

A user shall be able to select the identifier of his choice via the front panel and the remote control interface. The selected identifier is used as the active ID to decrypt the ESW.

The injected ID is a 32-character identifier that can be entered in the BISS2 receiver by the operator at any time.

- Receivers shall support the insertion of the injected ID through its physical (e.g. front panel) virtual interfaces (e.g. web interface) and through its remote control interface.
- There shall be no mechanism for reading back part or all of the injected ID via any receiver interface.
- The same ID can be injected in more than one piece of equipment, e.g. for redundancy management.
- The manual or remote entry of the injected ID shall be in hexadecimal form; the 32 digits are entered with the most-significant nibble first (i.e. the left-most nibble) in sequences of 8 characters. For example, if the injected ID is

```
0xF09A4B3F56738AB6F09AC53F14768CB6
```

It shall be entered in the following sequence:

```
F,0,9,A,4,B,3,F then 5,6,7,3,8,A,B,6 then F,0,9,A,C,5,3,F and
1,4,7,6,8,C,B,6.
```

4.3.2 Clear Session Word (SW)

The receiver shall be compliant with BISS2 - Mode 1. It shall support the insertion of a 32-character clear SW through the front panel and through a remote control interface. It shall use the SW as specified in section 4.1 (BISS2 - Mode 1). The clear SW, once entered via the user interface or remote control port, shall not be readable through any receiver interface.

4.3.3 Encrypted Session Word (ESW)

The receiver shall support the insertion of encrypted session words (ESW) through the front panel and through a remote control interface. The definition of the remote control port is outside the scope of this document.

The ESW is a 32-character number that is decrypted by the receiver into a 32-character clear SW. The clear SW is then used by the receiver to descramble the broadcast according to § 4.2 (BISS2 - Mode 1). Once the ESW has been entered via the front panel or via the remote control interface, it shall be impossible to read it back through any receiver interface.

The manual entry of the ESW shall be in hexadecimal form; the 32 digits are entered with the most-significant nibble first (i.e. the left-most nibble) in sequences of 8 characters. For example, if the ESW is:

```
0xF76EE249BE01A286F76EE249BE01A286
```

It shall be entered in the following sequence:

```
F,7,6,E,E,2,4,9, then, B,E,0,1,A,2,8,6, then, F,7,6,E,E,2,4,9, and,
                    B,E,0,1,A,2,8 6.
```

4.3.4 Decryption process

The receiver shall include the following features:

- An **identifier**, denoted **ID**, comprising a 32-character hexadecimal word (128-bit) which shall be injected by the management centre and shall be used as the default. The injected ID is mandatory.
- Optionally, in addition, the supplier may bury an ID. In this case, the receiver operator shall actively select the buried ID.
- An **AES-128 decryption function**, as described in Figure 2.

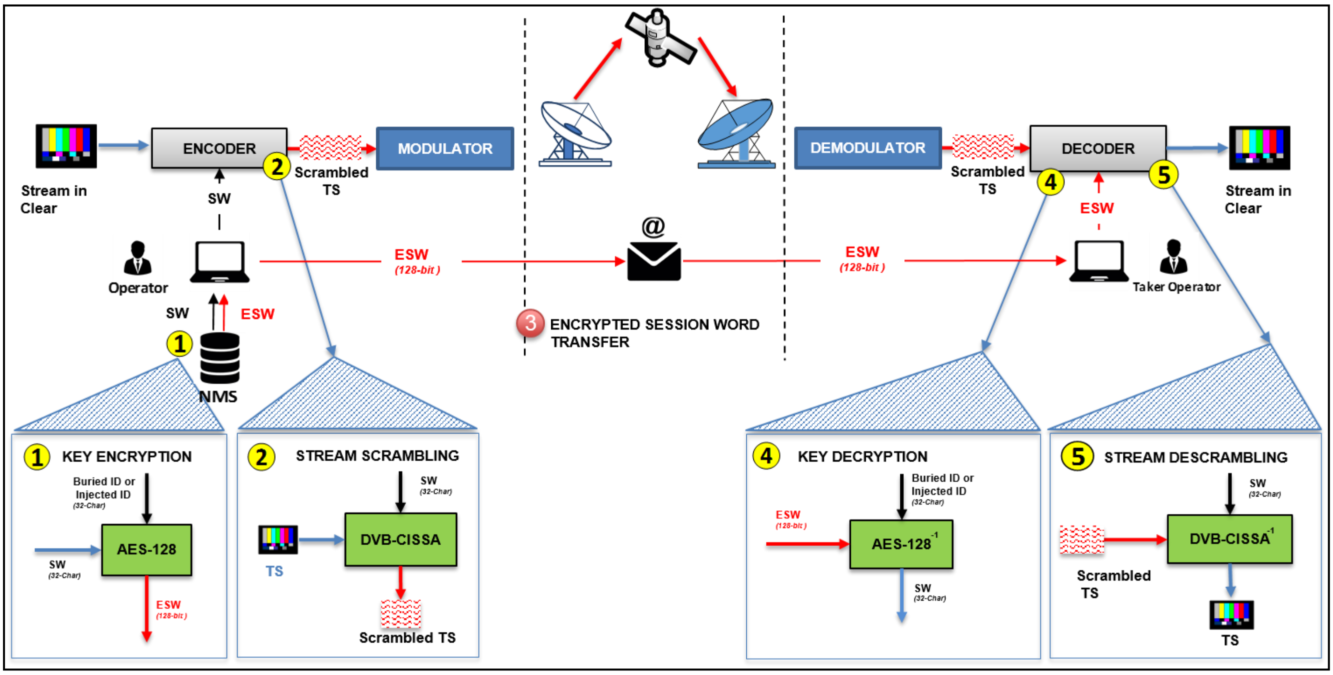

Figure 2: BISS-E process description.

The Management Centre generates the ESW by encrypting the SW using either the 128bit injected ID or buried ID as a cipher key in accordance with the **Advanced Encryption Standard (AES)** specified in [4]. AES-128 should be used in ECB mode. The ESW is then transmitted to the receiver operators via a channel deemed secure by the management centre.

The specification of the ESW transfer channel is outside the scope of this specification. The processing of the ESW in the receiver to provide the clear SW is illustrated in Figure 2. The ESW is entered in the receiver via the available user interface (physical or virtual).

The operator shall select the relevant active ID (injected ID or buried ID) as indicated by the management centre. The active ID is used as a de-cipher key with the AES-128 decryption function to decrypt the Session Word (SW).

4.4 BISS2-CA

4.4.1 Description

BISS-CA is a conditional access mode of the BISS protocol defined in Tech 3292s1. This section provides an overview of the CA mode. For further details please refer to Tech3292s1 [3].

The BISS2-CA conditional access mode is based on open cryptographic standards. It uses a combination of symmetric and asymmetric ciphers (see figure 3) to protect the transmitted content and entitle or revoke, in real-time any targeted receivers in an interoperable manner. It is registered as a DVB service owned by the EBU, with the **CA_SYSTEM_ID 0x2610**.

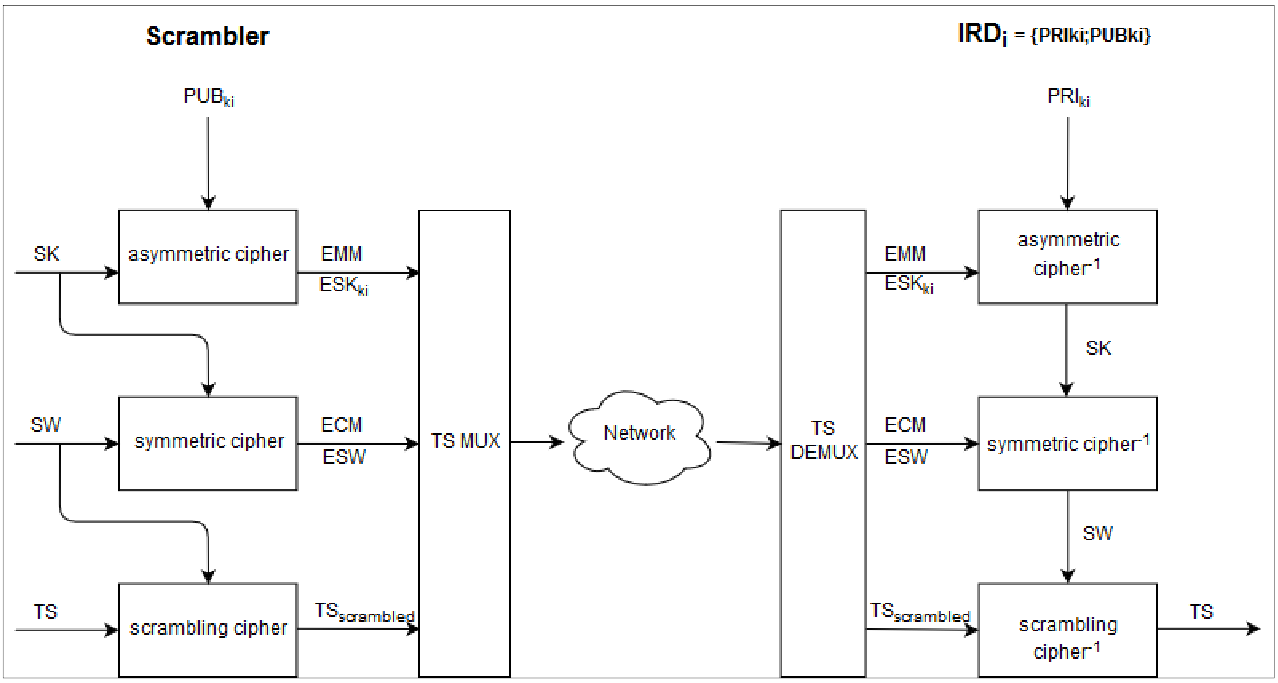

Figure 3: BISS-CA overview

In BISS-CA, each receiver (IRD_i) eligible to descramble the stream has an asymmetric key pair: a public key, and a private key { PRI_{ki} , PUB_{ki} }. The public keys of entitled receivers are transported to the scrambler out of band. The method of transporting the public keys are out of scope of this document. An accurate entitlement list is maintained, consisting of a collection of entitled receivers with their corresponding public keys. The list is used by the scrambler to generate the entitlement management messages (EMMs).

A Session Word (SW) is used as an input to the Transport Stream (TS) scrambling algorithm DVB-CISSA, to scramble individual service components in the TS. The Session Word is then encrypted with a symmetric cipher (AES-128) using a Session Key (SK). The resulting Encrypted Session Word (ESW) is transmitted to the entitled receivers' in-band in the TS via Entitlement Control Messages (ECMs).

The Session Key (SK), which is required to decrypt the ESW, is encrypted individually with an asymmetric cipher (RSA-2048) [7] [8] using the public key of each entitled receiver (PUB_{ki} for IRD_i). Only the receiver having the corresponding Private Key (PRI_{ki}) will be able to decrypt that Encrypted Session Key (ESK_{ki}). The set of individual ESK_{ki} are transmitted to receivers' in-band in the TS via Entitlement Management Messages (EMMs).

The scrambled TS, the ECM and EMM tables are multiplexed in the same TS. The EMM and ECM table structures are not scrambled.

To maintain security of the BISS-CA session, Session Words and Session Keys shall be automatically generated using a cryptographically secure random number generator by the sender/scrambler. The exact method of creating random numbers is outside the scope of this document, but an example method using a Deterministic Random Bit Generator (DRBG) and a random or secret seed is described in NIST Special Publication 800-90A [9].

5. References

[1] ETSI TS 103 127 V1.1.1 (2013-05) - Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams : http://www.etsi.org/deliver/etsi_ts/103100_103199/103127/01.01.01_60/ts_103127v010101p.pdf

[2] Federal Information Processing Standards, Publication 197 - ADVANCED ENCRYPTION STANDARD (AES) https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[3] BISS CA : Basic Interoperable Scrambling Systems Conditional Access Mode – Tech 3292-1 https://tech.ebu.ch/tech3292-1.pdf

[4] Recommendation for random Number Generation Using Deterministic Random Bit Generators; https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final

[5] ISO/IEC 13818-1:2018 Generic coding of moving pictures and associated audio information – Part1:Systems; https://www.iso.org/standard/74427.html

[6] ETSI EN 300 468 v1.13.1 ; DVB document A038 ; Specification for Service information (SI in DVB Systems); https://www.dvb.org/resources/public/standards/a38_dvb-si_specification.pdf

[7] NIST 800-56b; Recommendation for pairwise Key-Establishment schemes Using Integer factorization cryptography; https://csrc.nist.gov/publications/detail/sp/800-56b/rev-1/final

[8] RFC 8017 : PKSC#1 RSA cryptography specifications Version 2.2; https://tools.ietf.org/html/rfc8017

[9] Recommendation for random Number Generation Using Deterministic Random Bit Generators; https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final

Annex A: Protocol Component Examples

```
AES-128 (Nk=4, Nr=10):

Injected ID / Buried ID:         000102030405060708090a0b0c0d0e0f

Session word (SW):               00112233445566778899aabbccddeeff
Encrypted Session Word (ESW):    69c4e0d86a7b0430d8cdb78070b4c55a
```