

MBS (Multimedia Multicast/Broadcast Service) Security Framework proposal

Document Number: **IEEE C802.16e-04/63**

Date Submitted: 2004-05-07

Source:

JunHyuk Soong, Yong Chang

Samsung Electronics Co., Ltd.

Venue:

[Cite the specific meeting and any known agenda details.]

Base Document:?

Purpose:

Proposing MBS (Multimedia Multicast/Broadcast Service) Security Framework proposal

Notice:

This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Release:

The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.

IEEE 802.16 Patent Policy:

The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <<http://ieee802.org/16/ipr/patents/policy.html>>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <<mailto:chair@wirelessman.org>> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <<http://ieee802.org/16/ipr/patents/notices>>.

802.16e MBS (Multimedia Broadcast Service) Security Framework Proposal

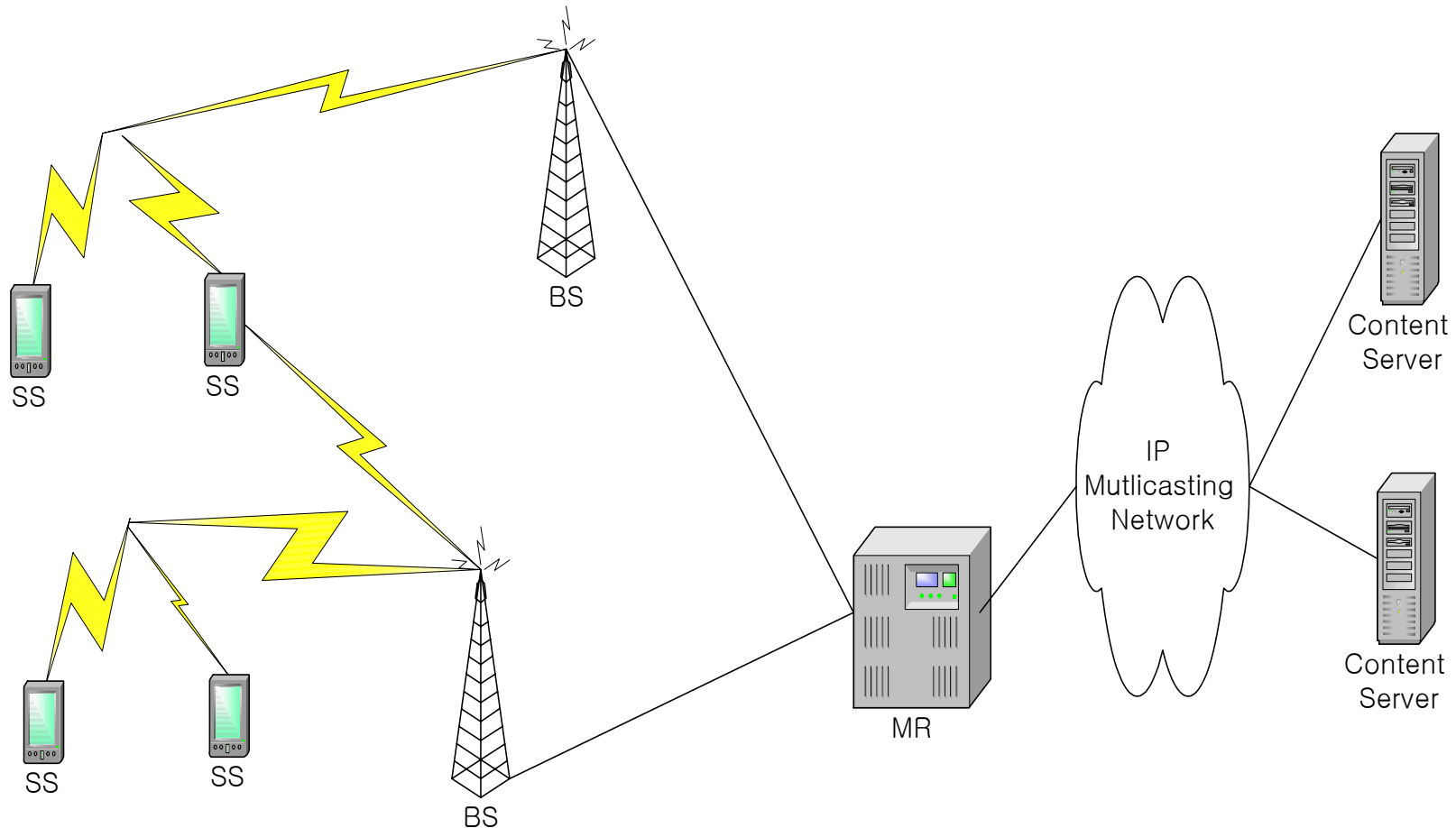
JunHyuk Song,
junhyuk.song@samsung.com

Yong Chang,
yongchang@samsung.com

Table of Contents

- Architectural Overview
- MBS Security Overview
- MBS Key Management
- MBS Ciphersuits
- MAK Distribution call flows
- MBS Configuration messages
- MBS Link Layer Encryption
- MBS Message Integrity Check Support
- Risk Evaluation of MBS Null Authentication

MBS Architecture Overview



MBS Security Overview

- Shall support either Link Layer Encryption and Application Layer Encryption (Support of Application Layer Encryption is outside scope of 802.16e and *only Link Layer Encryption shall be defined*)
- MBS Security shall not use PKM messages for key delivery and key management
- SS shall obtain MBS Encryption keying materials and optionally obtain MIK materials for message integrity check from MBS Content server
- Shall support high speed Link Layer Encryption for Access Control
- May support Null Message Authentication and 32/64/80bits message authentication

MBS Key Management

- PKM is not optimized for MBS because of the following reasons:
 - Service Authorization is only possible through MBS content server, since BS is agonistic to Application Service Information such as MBS contents
 - Key Materials and Key Management for MBS will be unique for each MBS Channel, which is service provider dependent
 - Idle Mode SS will not have valid SA and Key materials
 - Exiting TEK cannot support Macro diversity among multiple AP because of TEK boundary in current specification is limited to BS

Cont.

- MBS Traffic Encryption Key Management
 - 128 bits MAK (MBS Authorization Key) shall be used for both Link layer and Application layer encryption
 - MAK shall be delivered to SS with MBS session information, upon successful Service Authorization from MBS content server
 - Delivery of MAK to BS from Content Server for Link Layer Encryption is outside of this standard (ex. SAP (Session Announcement Protocol))
 - BS shall broadcast MBS cipher suites, mapping between MBS_ID and MBS CID over MBS Configuration messages

Cont.

- MAK Keying Materials
 - MAK
 - MAK ID
 - MAK Sequence Number
 - MAK Lifetime

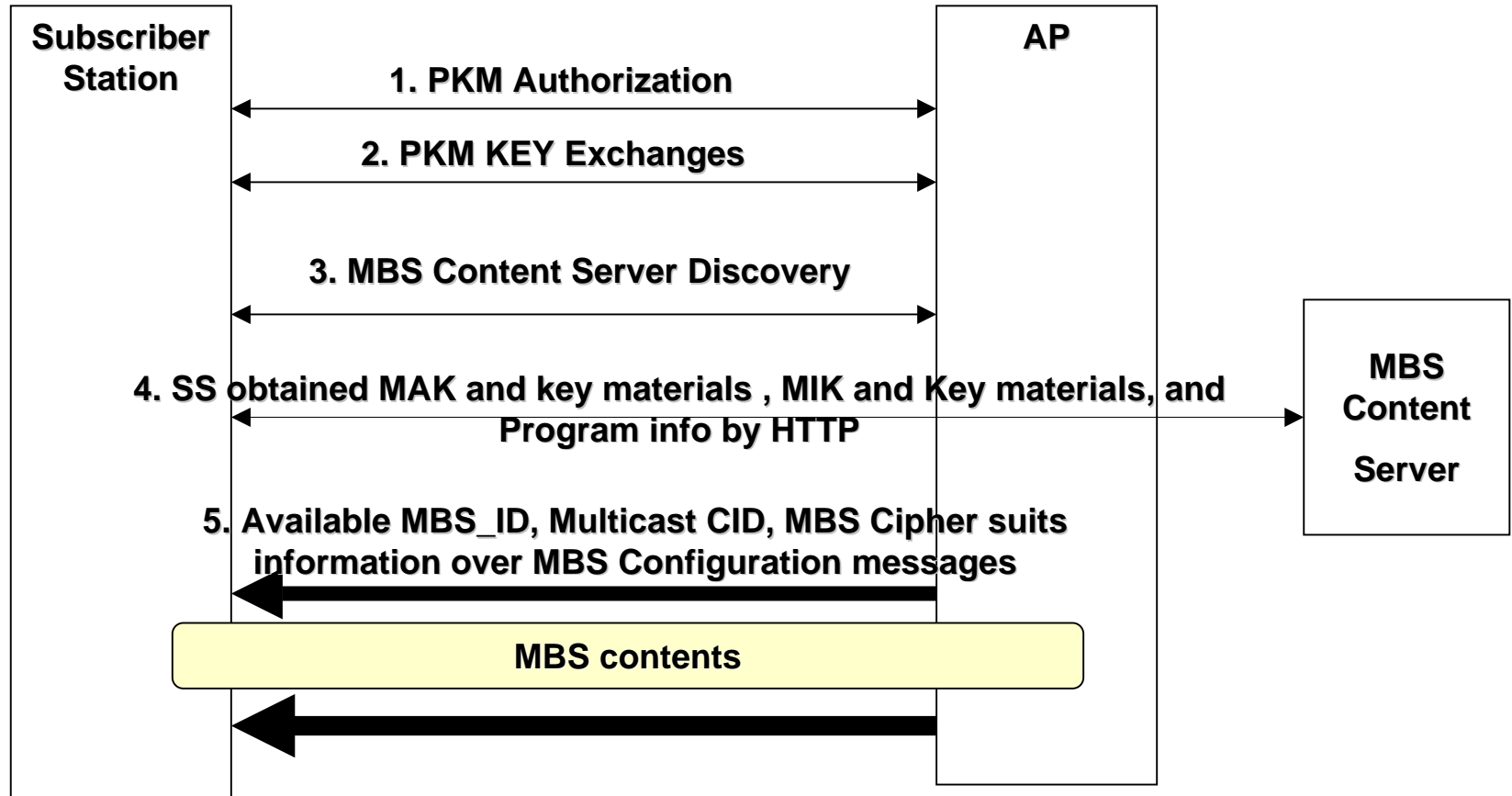
Cont.

- MBS Traffic Message Integrity Check Key Management
 - 160 bits MIK (MBS Message Integrity Key) shall be given to SS by one of the following method:
 - Derived from MAK by SHA-1 algorithm
 - Delivered to SS with MAK from MBS Content Server

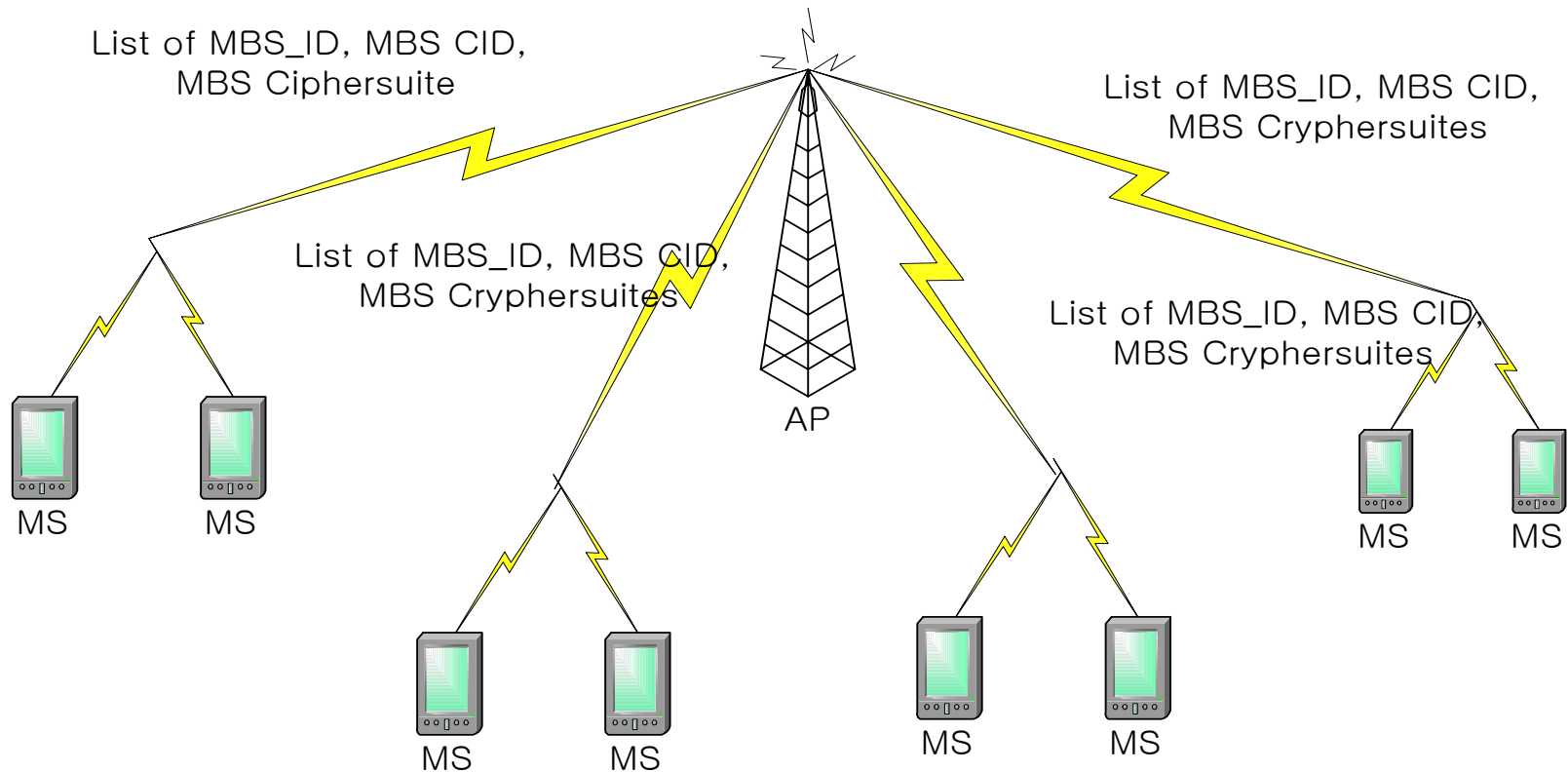
MBS Ciphersuits

- MBS ID and MBS CID
- Support of Link Layer Encryption or Application Layer Encryption
- Support of MBS Message Integrity support (Null Authentication, 32/64/80/bits Authentication)
- Encryption Algorithm, default value is AES Counter mode
- MAC Algorithm, default value is HMAC-SHA1
- MAK_ID and MAK Sequence Number
- Size of Nonce 32/64/128bits

MAK Distribution Call flow



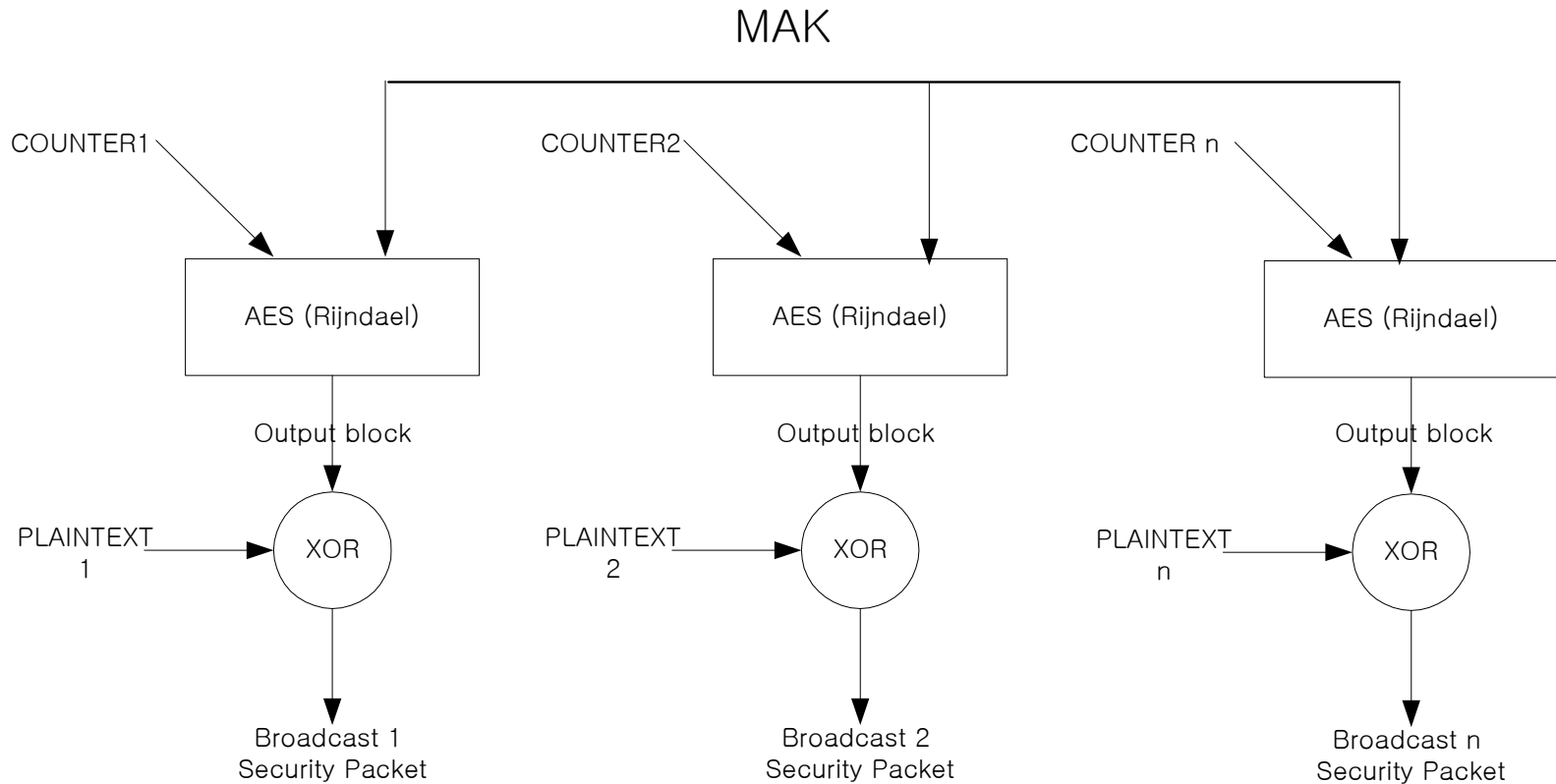
MBS Configuration Messages



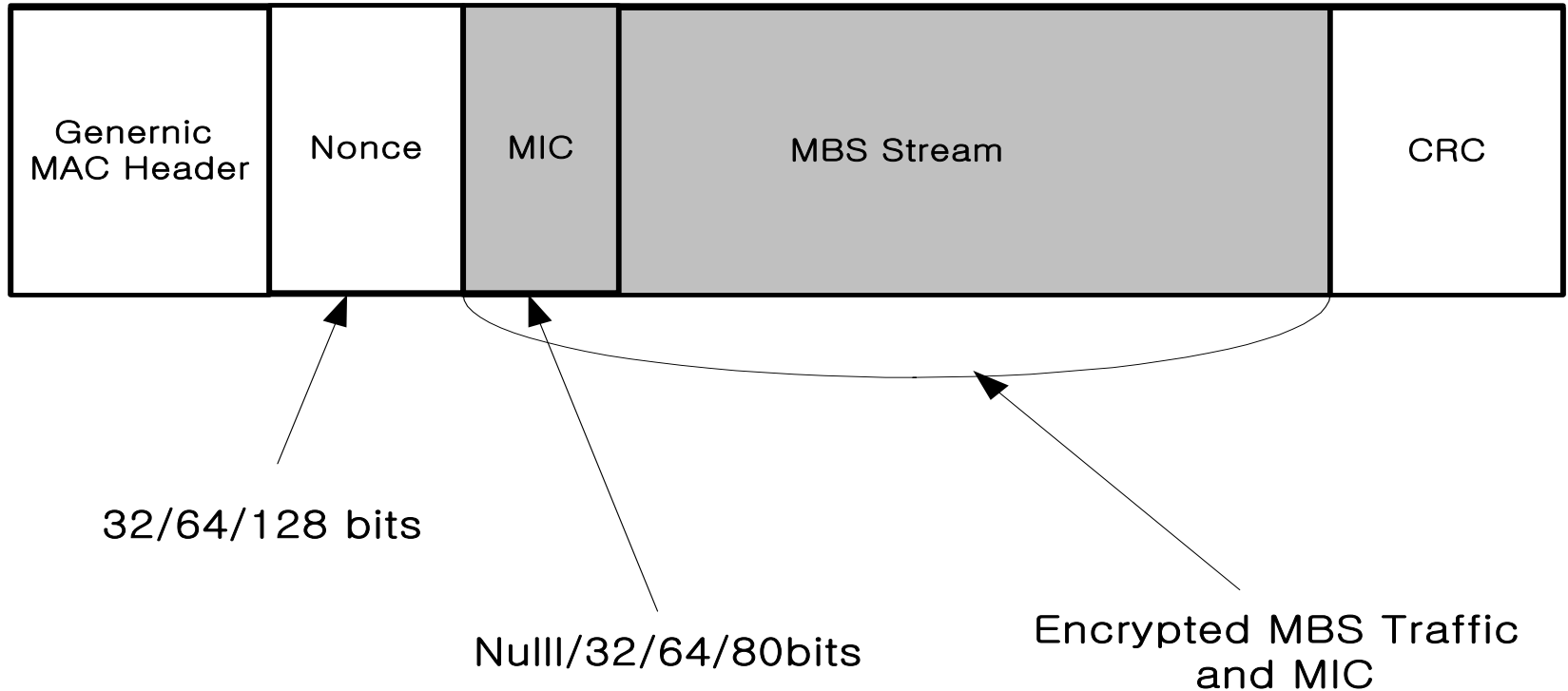
MBS Link Layer Encryption

- Based on 128bits key and block size AES Encryption algorithm
- Federal standard based algorithm, CTR mode defined in NIST Special Publication 800–38A is recommended because of high speed data encryption
- Traffic Inband Nonce support

CTR mode Encryption



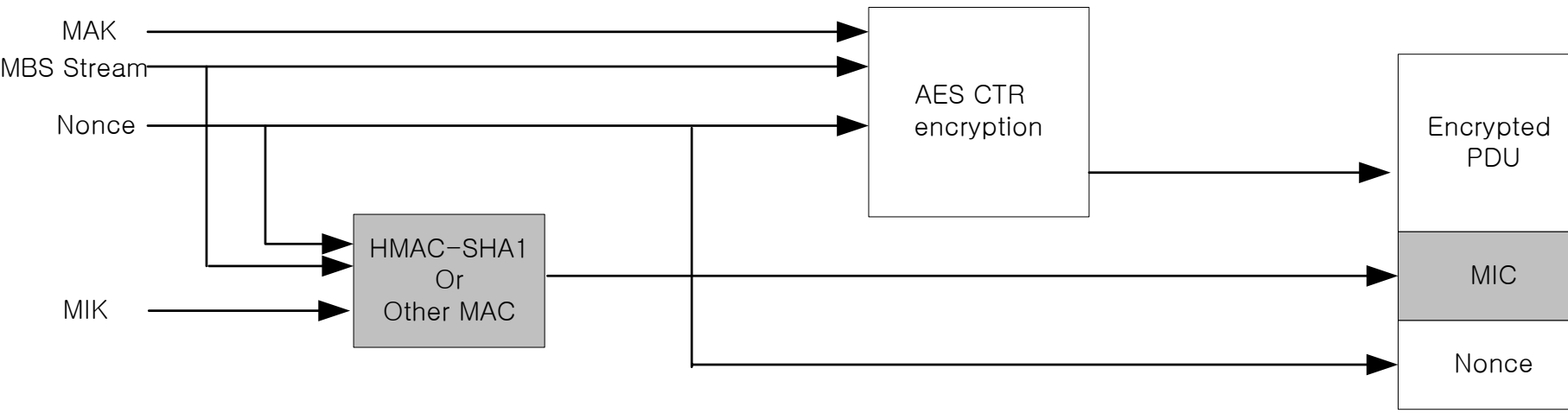
PDU Payload



MBS Message Integrity Check (MIC)

- HMAC-SHA1 shall be the default message authentication code.
- The default session authentication key is 160bits
- MIC length is variable to null/32/64/80bits
- Secure HASH over Nonce, MBS traffic
- Encrypted MAC support

MBS AES CTR with HMAC-SHA1 MAC Encapsulation Block Diagram



Risk Evaluation of Null Authentication

- It is unlikely that an adversary can broadcast forged MBS traffic stream with same physical, MAC, Transport, Applications information (Encoding scheme and session information)
- It is unlikely that an adversary can modify MBS traffic stream so that SS decrypts to an intelligible value
- Bandwidth saving is imperative in Wireless environment (With nonce 160bits and MIC 80bits, will have 26 bytes overhead)