[MBS (Multimedia Multicast/Broadcast Service) Security Framework proposal]

Document Number: **IEEE C802.16e-04/63r1**
Date Submitted: 2004-05-17
Source:

JunHyuk Soong, Yong Chang

Samsung Electronics Co., Ltd.

Venue:

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

Base Document:**?**

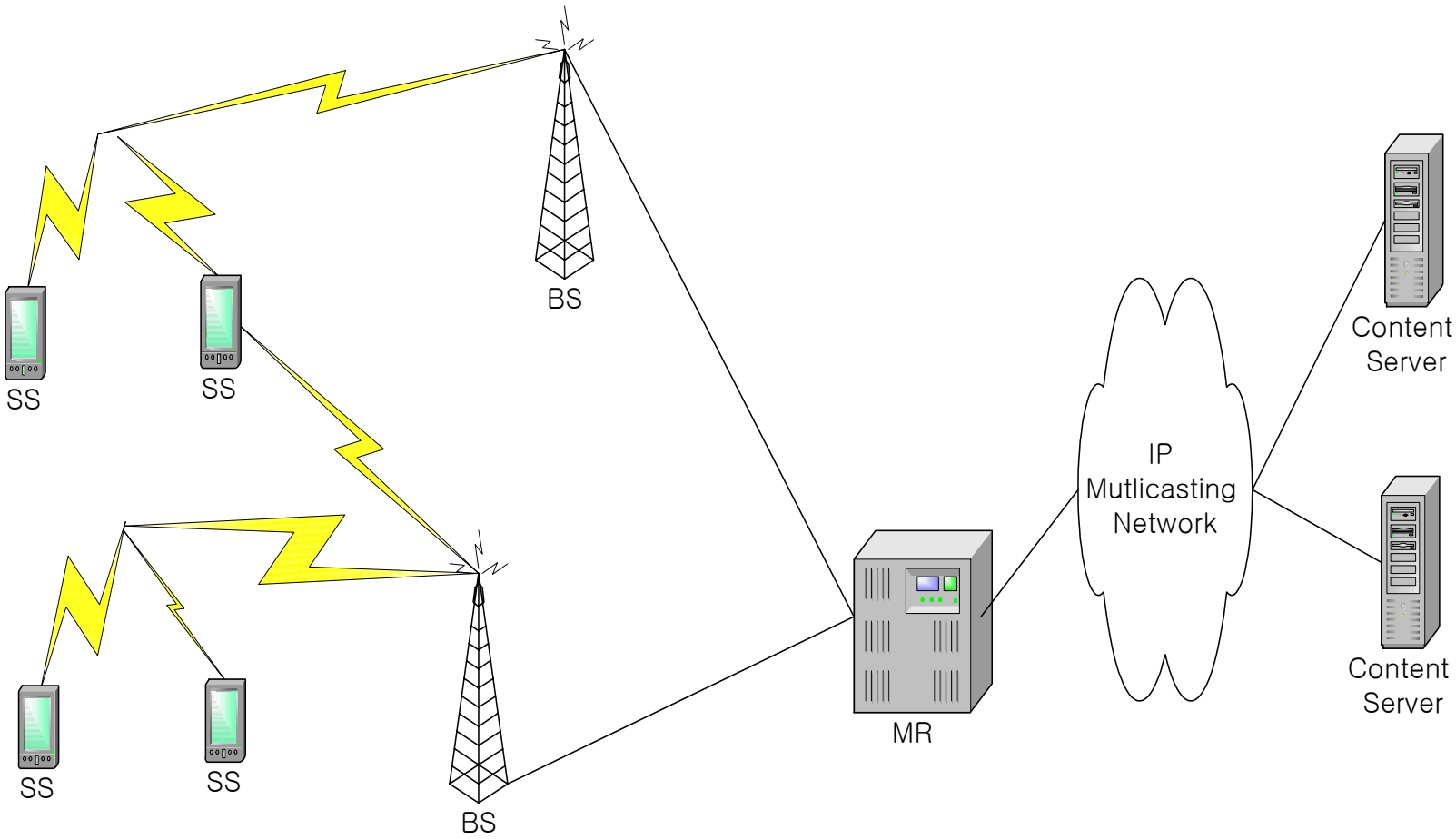
Purpose:

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

802.16e MBS (Multimedia Broadcast Service) Security Framework Proposal

JunHyuk Song,
junhyuk.song@samsung.com
Yong Chang,
yongchang@samsung.com

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*) for access control
- MBS Key Management can be supported either with PKM or without PKM
- SS shall obtain MBS Encryption keying materials and optionally obtain MBS Message Integrity Check materials from MBS Content server
- Shall support Null Message Authentication and 32/64/80bits message authentication over MBS traffic stream

MBS Key Management

- MBS Key Management can be either built in over PKM or supported in MBS stand alone mode
- PKM standalone cannot support MBS because of following reasons
  - MBS 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

PKM based MBS

- Provide robust service based on separation of access operator and third party MBS service provider
- Use both TEK and MAK for MBS link layer encryption that provide crypto binding between Link layer and application layer
- Define MBS SA shared between multiple SSs and BSs

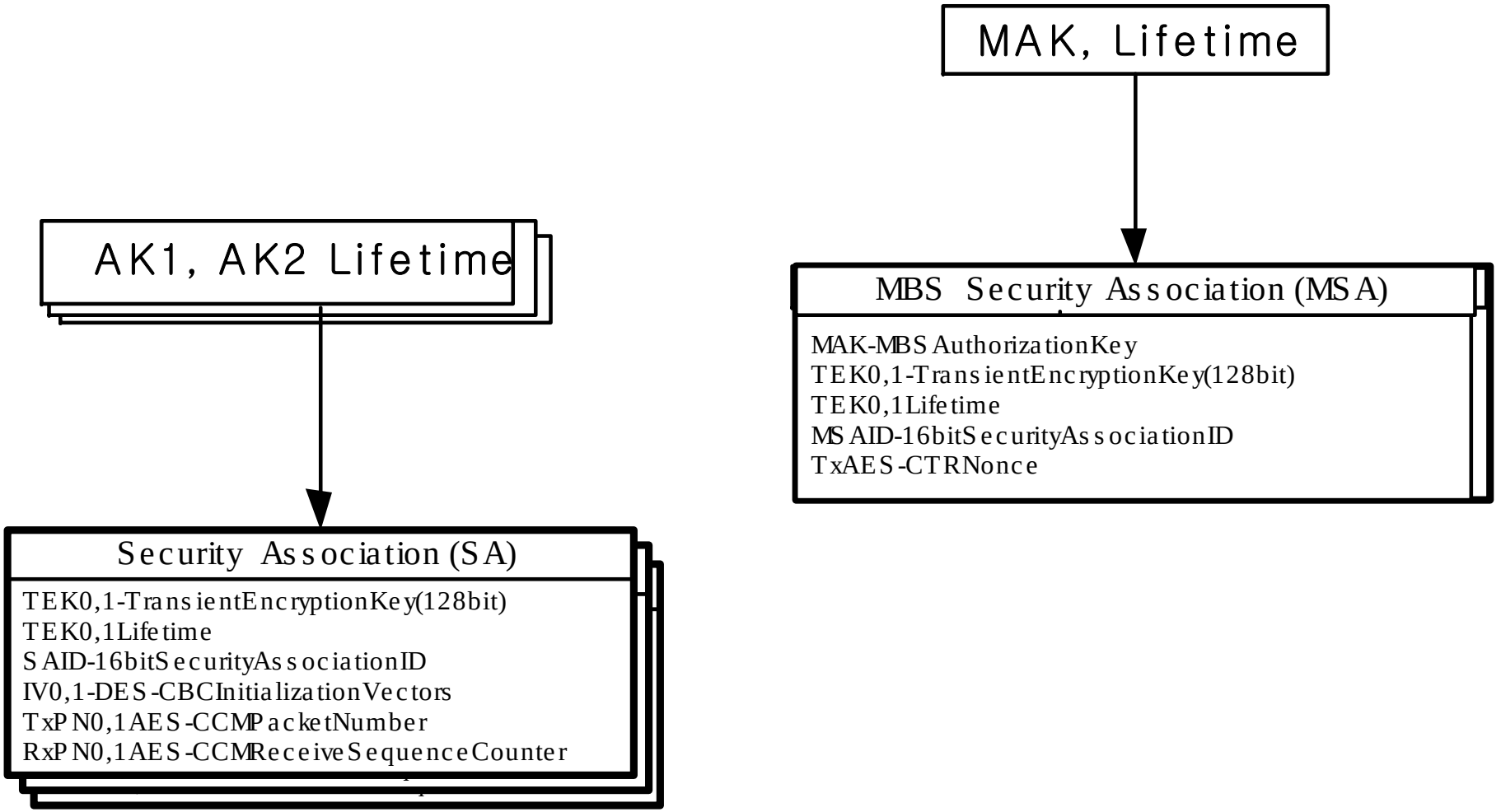
PKM based MBS Key Scheme

- MAK (MBS Authorization Key)
  - 128bits Service Authorization Token for specific Multicast IP stream used for both Application and link layer Encryption
- TEK (Traffic Encryption Key)
  - 128bits session key used toward for MBS link layer encryption with MAK. It has shorter lifetime than MAK and deliver to SS by PKM Key request and reply

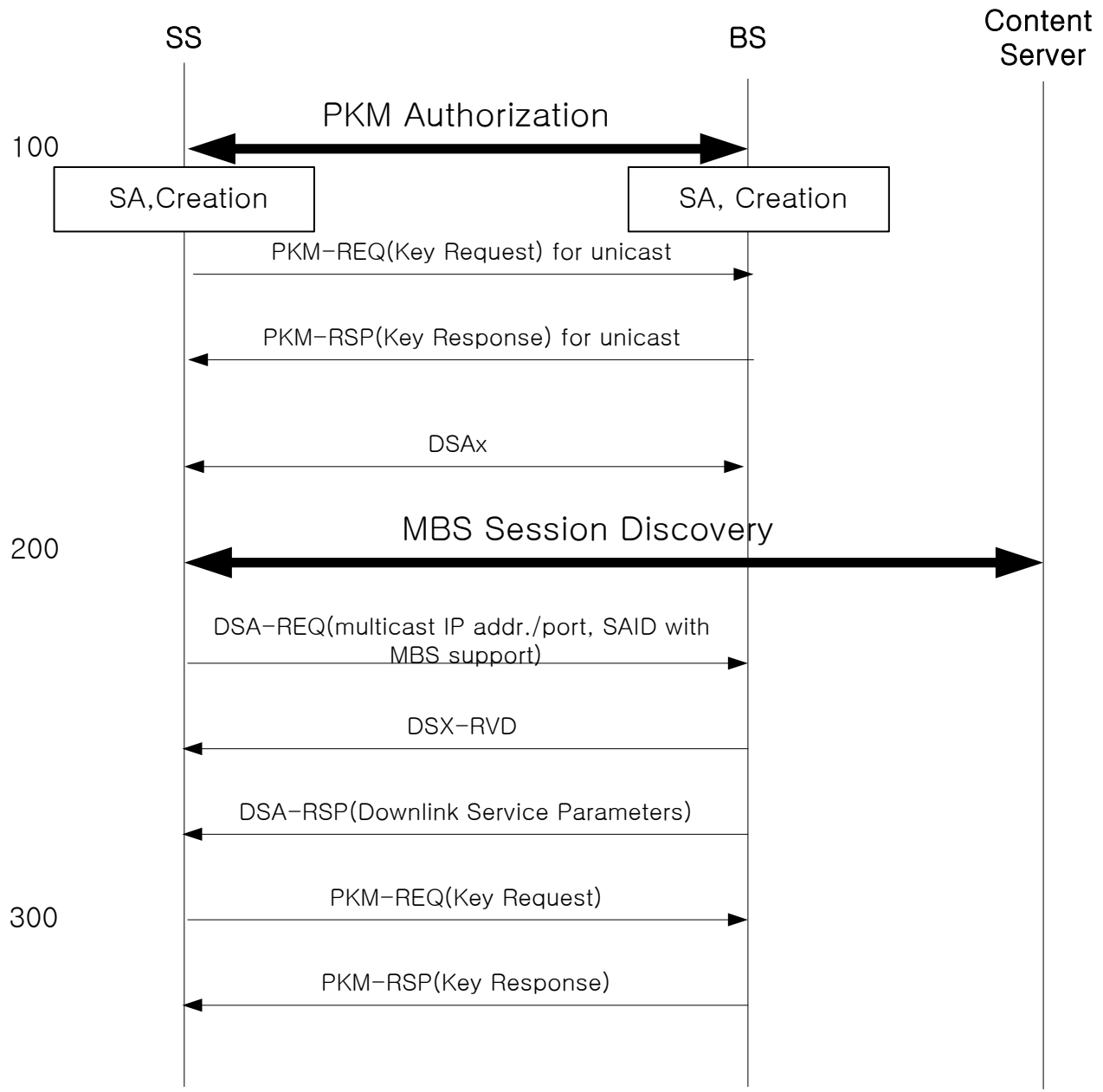
Cont.

- SS will obtain MAK and session information from content provider
- SS will obtain authorized MBS security association bind to MBS_ID during PKM Authorization
- SS will obtain TEK by Key Request and Key Reply messages, and may be further refreshed TEK by Push method or Pull method
- SS shall only be able to receive MBS packet stream if SS holds both MAK and TEK

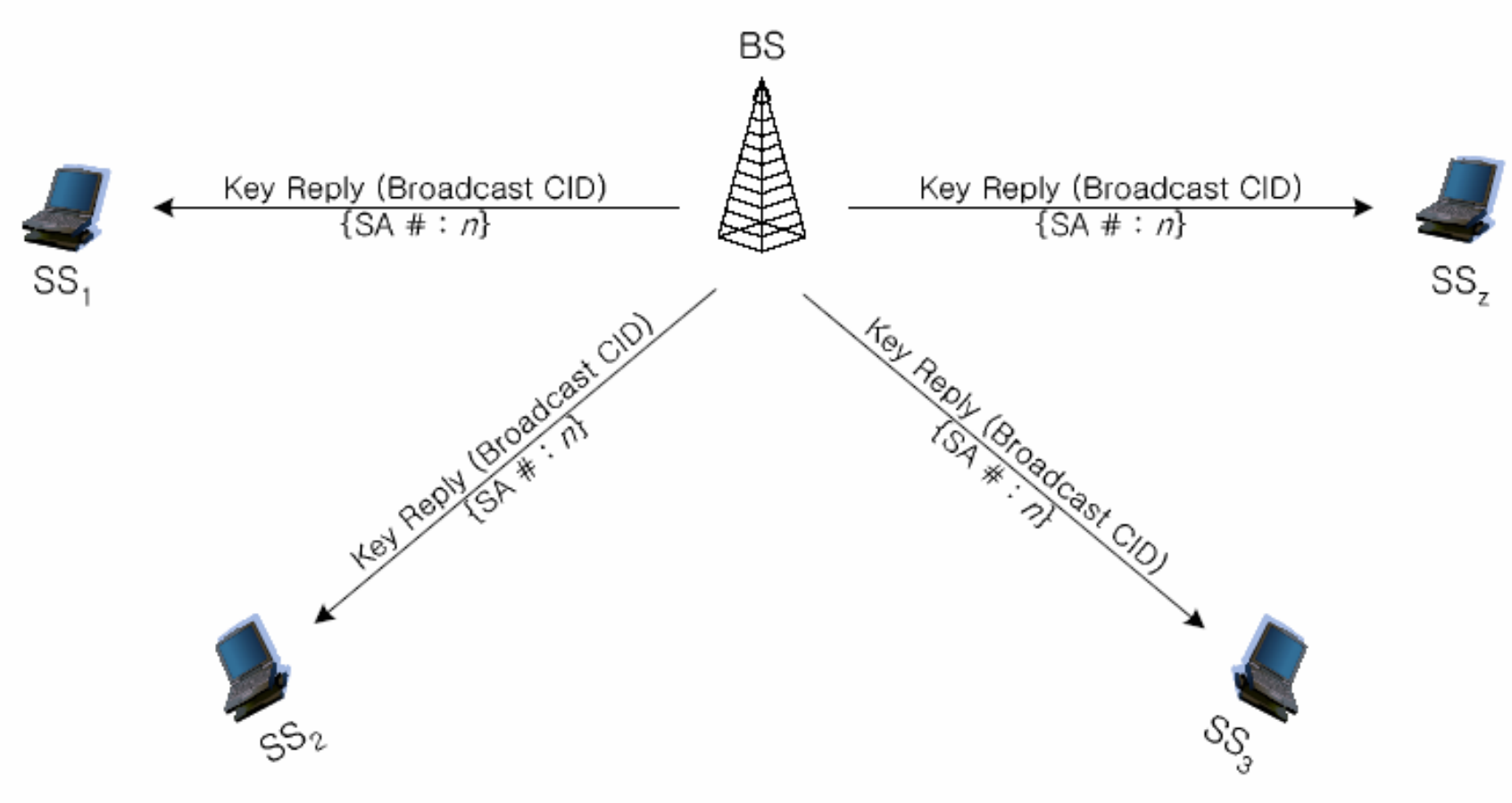
MBS SA (Security Association)



MBS Callflows



Push method for subsequent TEK delivery



Non PKM based MBS

- MBS standalone mode is not based on existing PKM
- MBS standalone mode Key Management has following advantages:
  - Can work for Idle Mode SS that doesn't have Primary Connection, SA and Key materials, since it is agonistic to PKM
  - Exiting SA based TEK cannot support Macro diversity among multiple BS because of TEK boundary in current specification is limited to BS

Non PKM based MBS Key scheme

- 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. Session Announcement Protocol)
- BS shall broadcast MBS cipher suites, mapping between MBS_ID and MBS CID over MBS Configuration messages

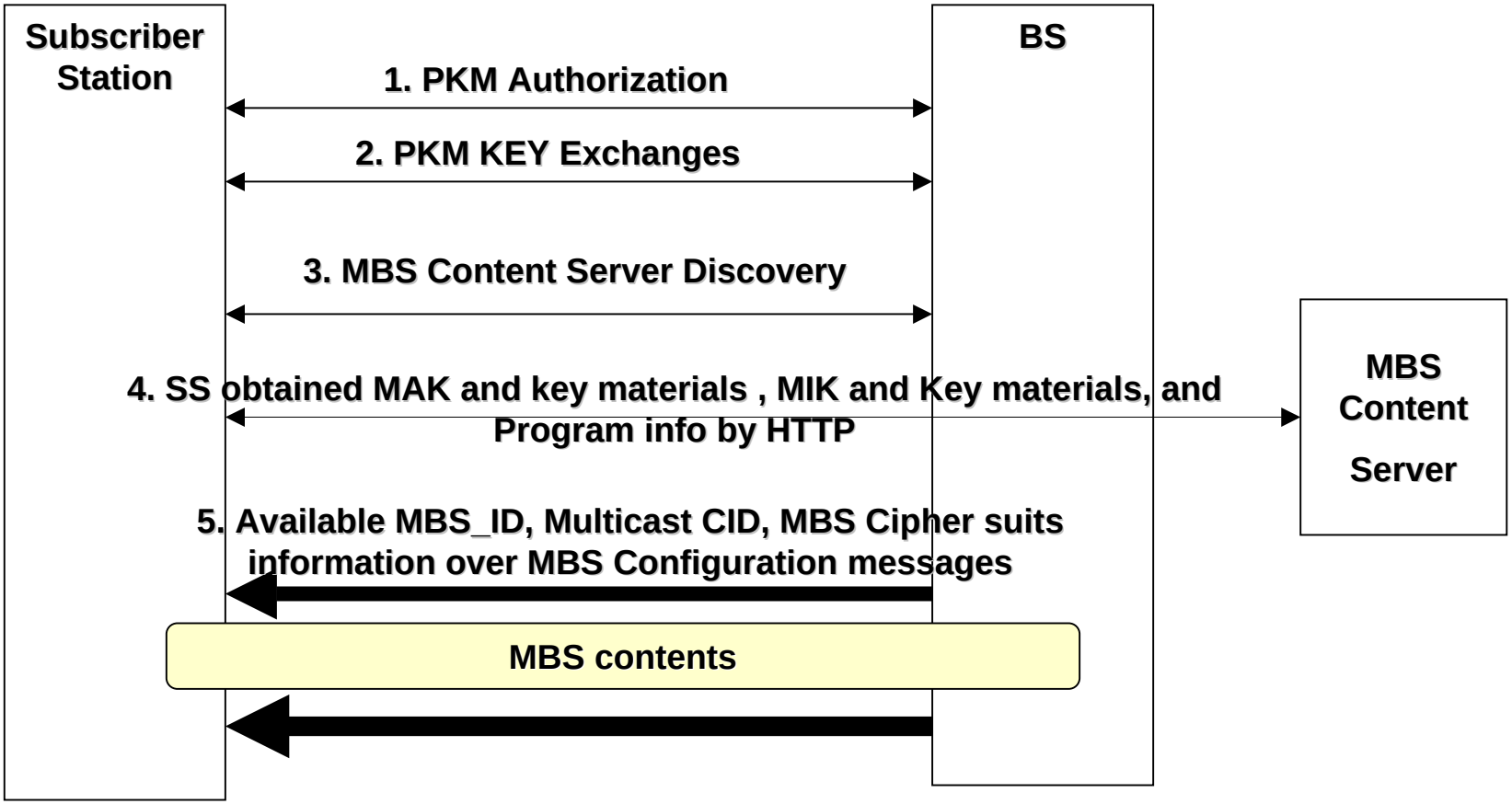
Cont.

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

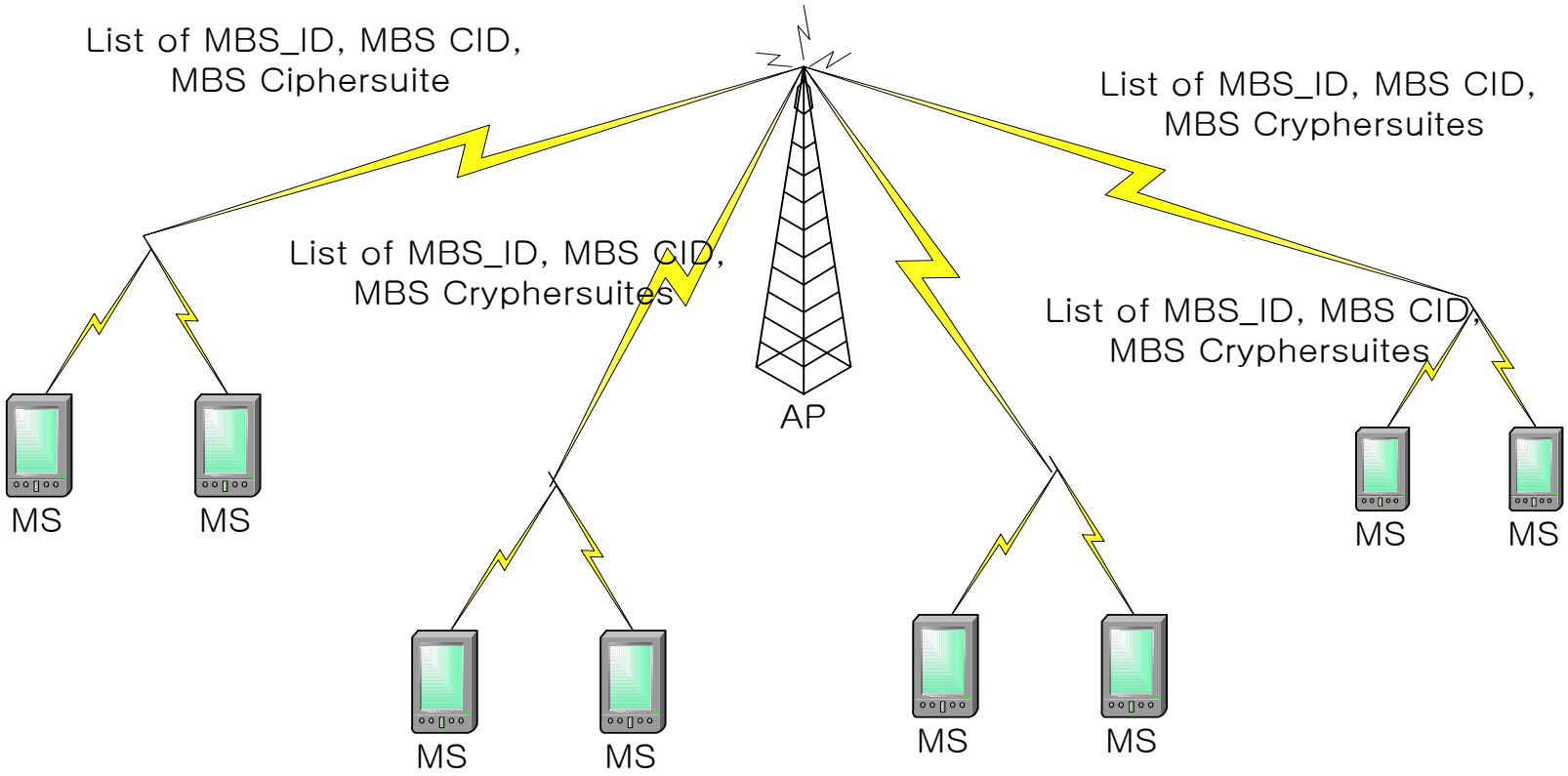
Cont.

- 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 or other appropriate key derivation algorithm
    - Delivered to SS with MAK from MBS Content Server

MAK Distribution Call flow



MBS Configuration Messages



MBS Ciphersuits in MBS configuration message

- 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 (May support other encryption mode, such as CCM)

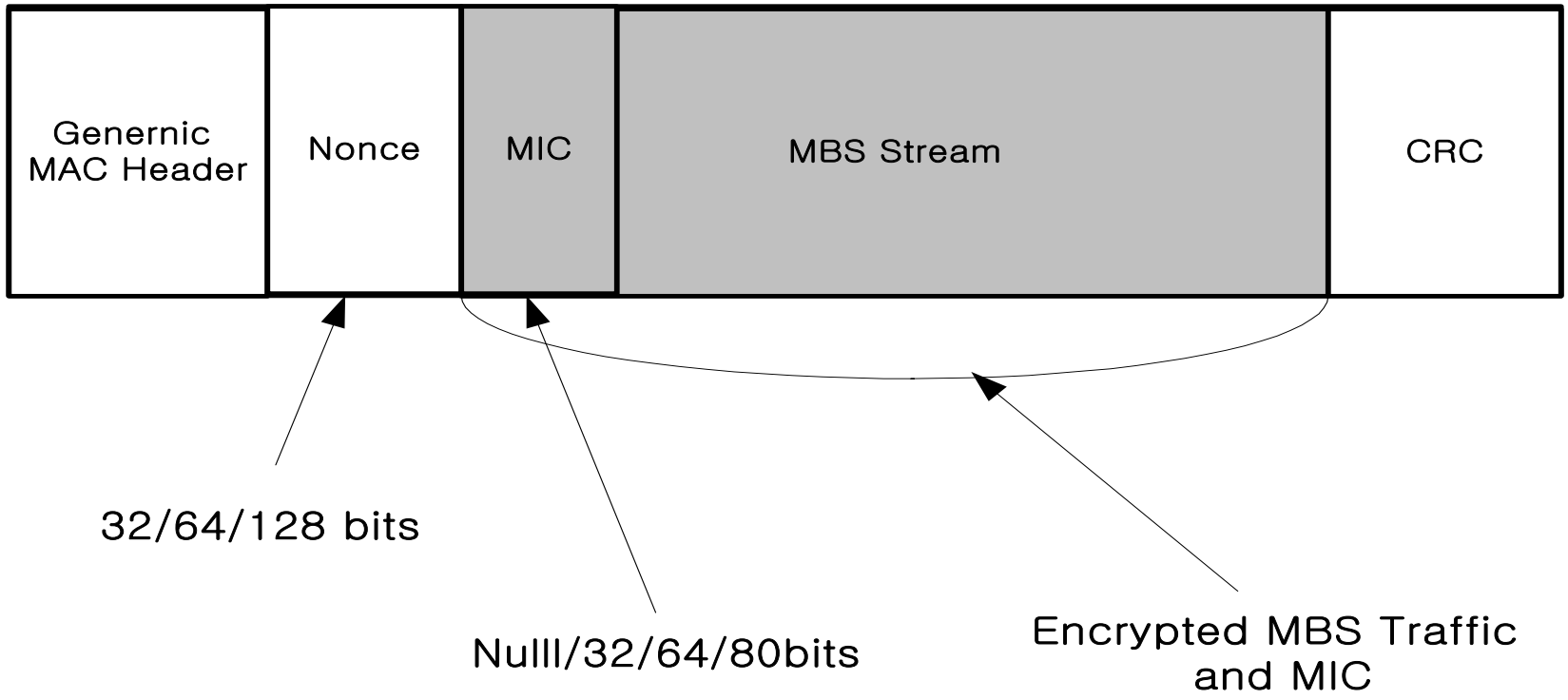
Cont.

- MAC Algorithm, default value is HMAC-SHA1
- MAK_ID and MAK Sequence Number
- Size of Nonce 32/64/128bits
  - 32bits nonce will be repeated 4 times to make 128bits, 64 bits nonce will be repeated 2 times to make 128bits

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
- AES CTR mode with Traffic Inband Nonce support
- May support other AES Encryption and Authentication mode

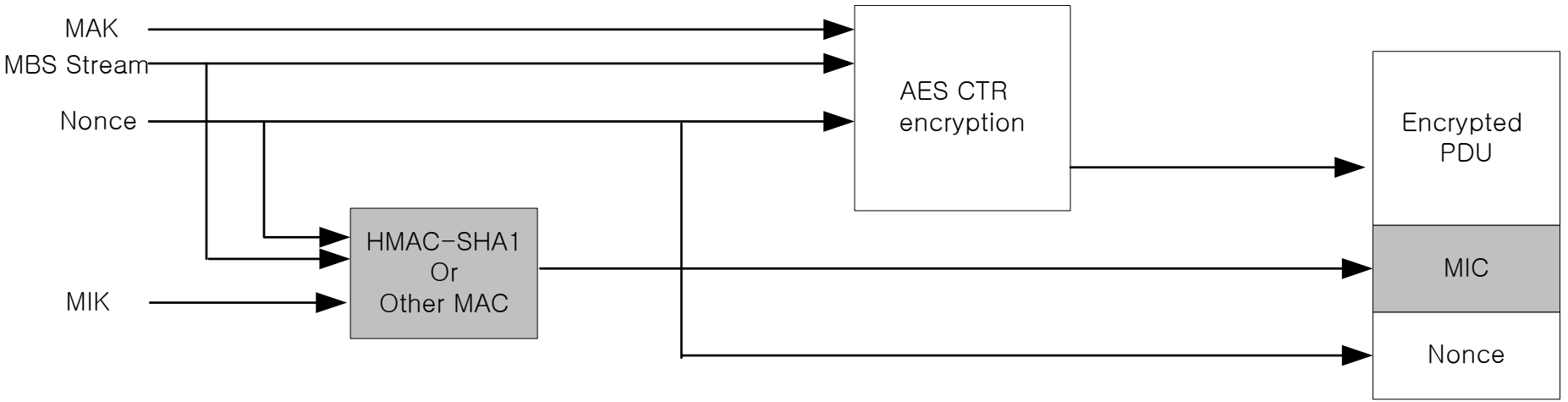
PDU Payload


Generic MAC Header
Nonce
MIC
MBS Stream
CRC
32/64/128 bits
Nulll/32/64/80bits
Encrypted MBS Traffic and MIC

MBS Message Integrity Check (MIC)

- HMAC-SHA1and other MAC shall be supported.
- 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 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, and 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 30 bytes overhead)