IEEE 802.16 WiMax Security

Dr. Kitti Wongthavarawat
Wireless Security R&D
ThaiCERT, NECTEC

Presents at NAC 2005
March 28, 2005

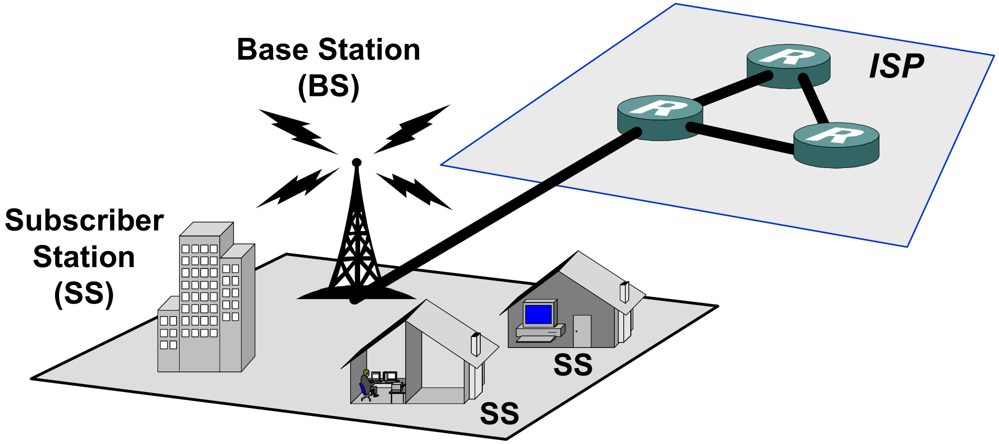
ThaiCERT
Thai Computer Emergency Response Team

ECTI-21 NECTEC
National Electronics and Computer Technology Center

Agenda

- Introduction to IEEE 802.16 WiMax
- IEEE 802.16 Security Model
- IEEE 802.16 Security Analysis
- Conclusions

Introduction to IEEE 802.16 WiMax

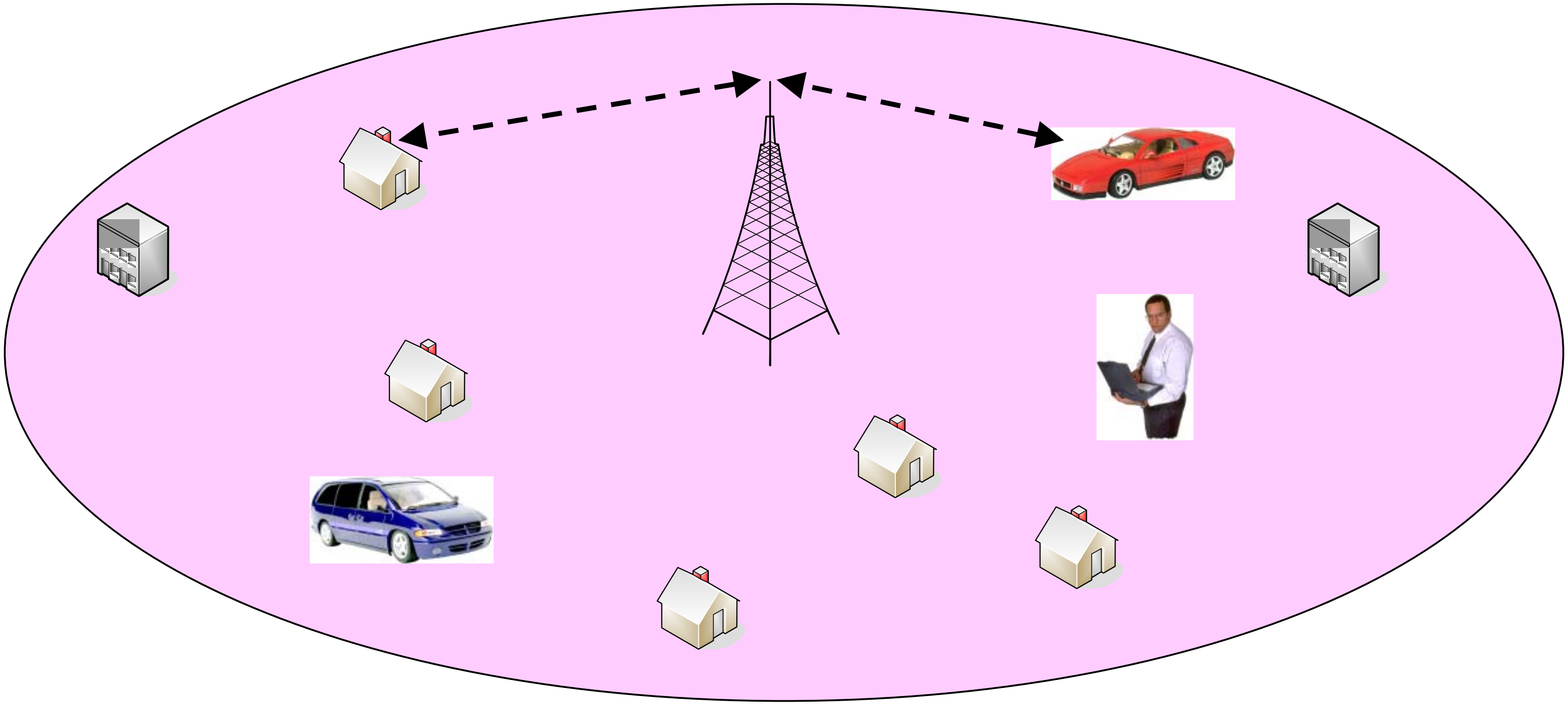


- Complement existing last mile wired networks (i.e., xDSL, Cable modem)
- Fast deployment, cost saving
- High speed data, voice and video services
- Fixed BWA, Mobile BWA

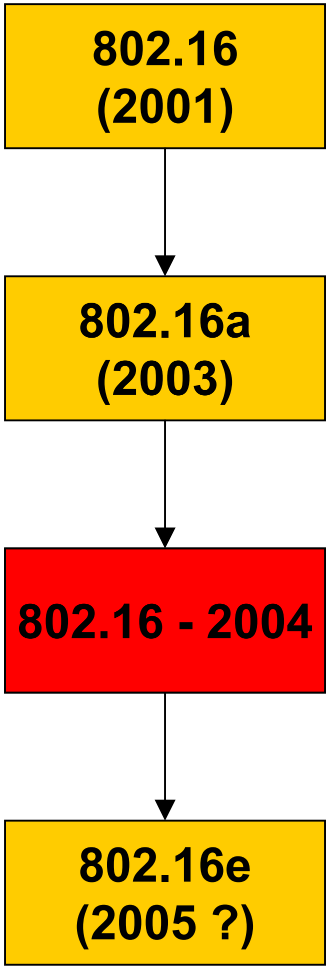
Introduction to IEEE 802.16 WiMax

Fixed BWA
(IEEE 802.16)

Mobile BWA
(IEEE 802.16e)



IEEE 802.16 Evolution



802.16 (2001)

802.16a (2003)

802.16 - 2004

802.16e (2005 ?)

- Fixed BWA at 10-66 GHz
- Line of sight

- Fixed BWA at 2-11 GHz
- None line of sight

- Revision of 802.16
- Combine previous 802.16 standards

- Mobile BWA based on 802.16-2004 (802.16a)
- Roaming with vehicular speed

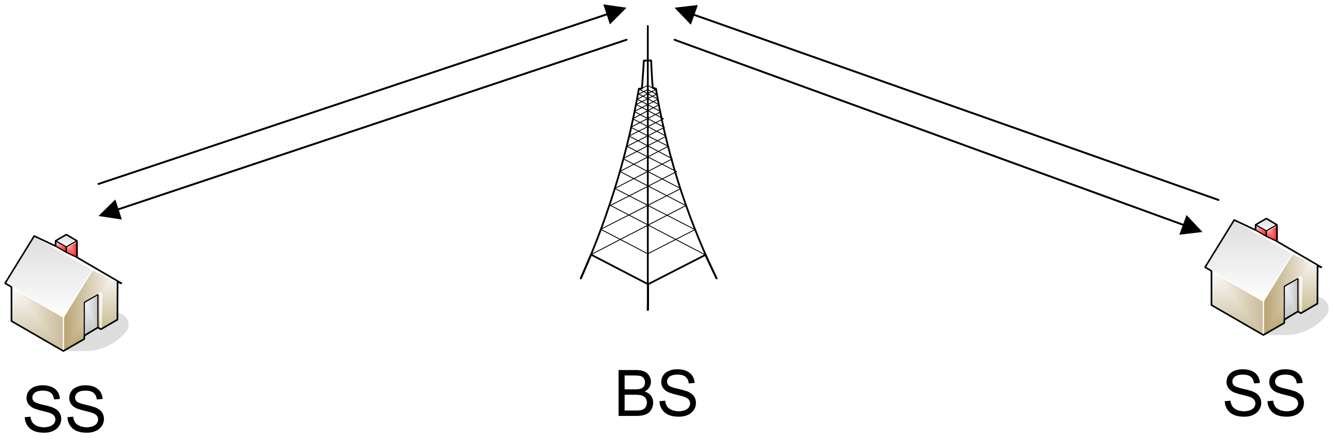
IEEE 802.16 Security Model

- Standard was adopted from DOCSIS specification (e.g. cable modem spec.)
  - □ Assumption: all equipments are controlled by the service provider
  - □ **May not be suitable for wireless environment**
- Connection oriented (i.e., Basic CID, SAID)

IEEE 802.16 Security Model

- Connection
  - □ Management connection
  - □ Transport connection
  - □ Identified by connection ID (CID)

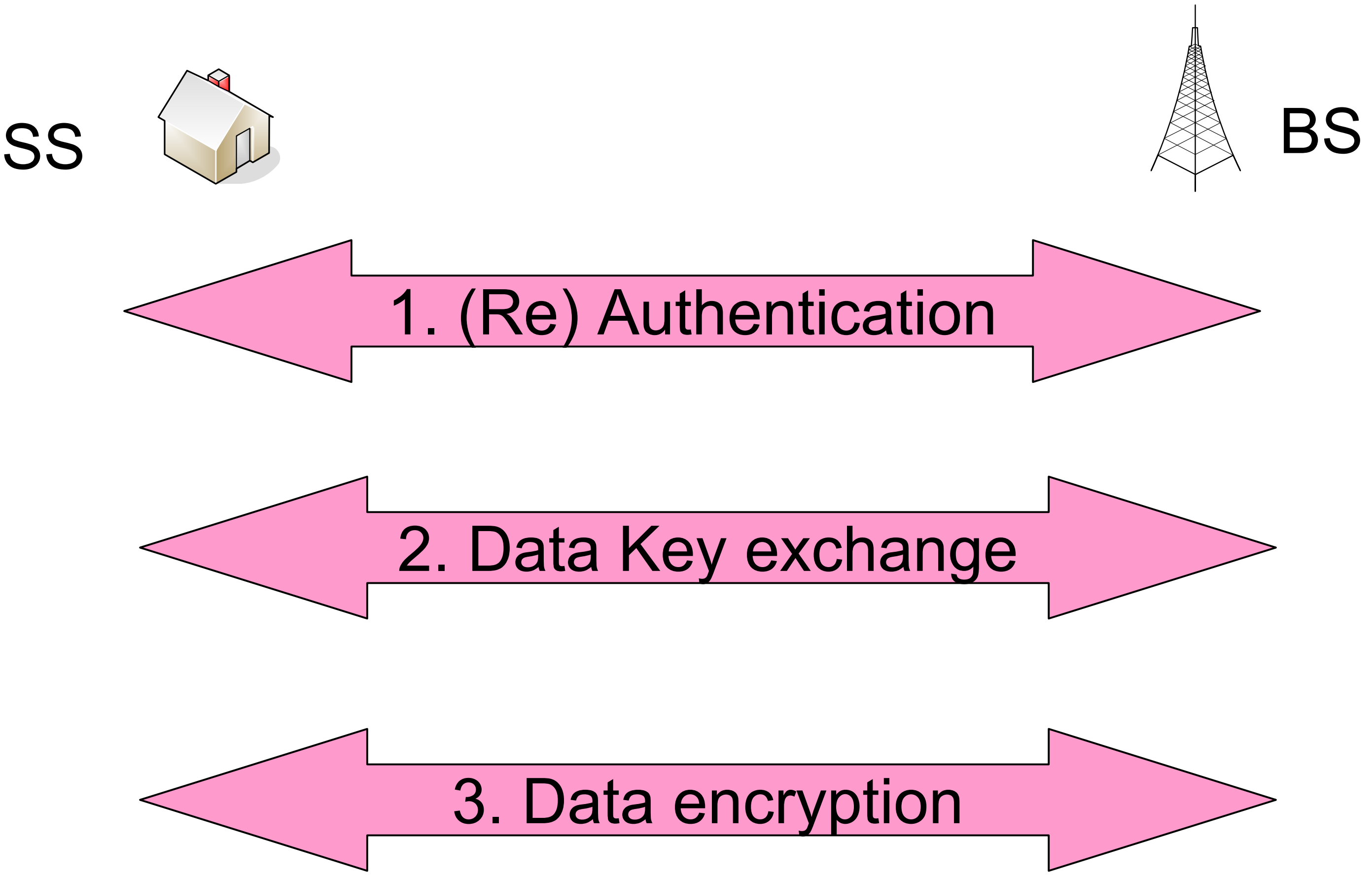
- Security Association (SA)
  - □ Cryptographic suite (i.e., encryption algorithm)
  - □ Security Info (i.e., key, IV)
  - □ Identified by SAID



IEEE 802.16 Security Analysis

- IEEE 802.16 security process
- Security mechanisms
  - Authentication
  - Access control
  - Message encryption
  - Message modification detection (Integrity)
  - Message replay protection
  - Key management
    - Key generation
    - Key transport, Key protection
    - Key derivation
    - Key usage

IEEE 802.16 Security Process



SS

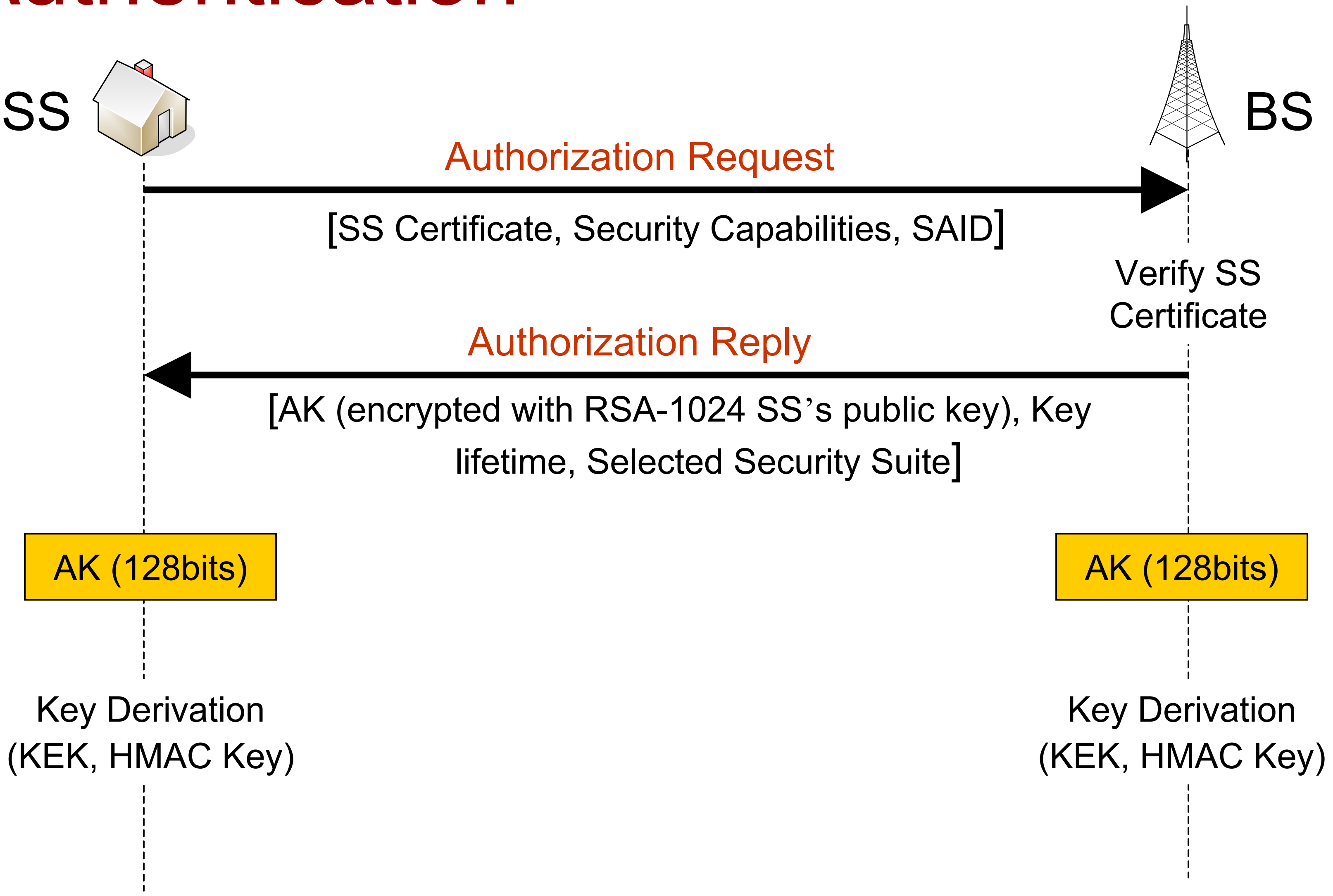
BS

1. (Re) Authentication

2. Data Key exchange

3. Data encryption

Authentication



SS

BS

Authorization Request

[SS Certificate, Security Capabilities, SAID]

Verify SS Certificate

Authorization Reply

[AK (encrypted with RSA-1024 SS's public key), Key lifetime, Selected Security Suite]

AK (128bits)

AK (128bits)

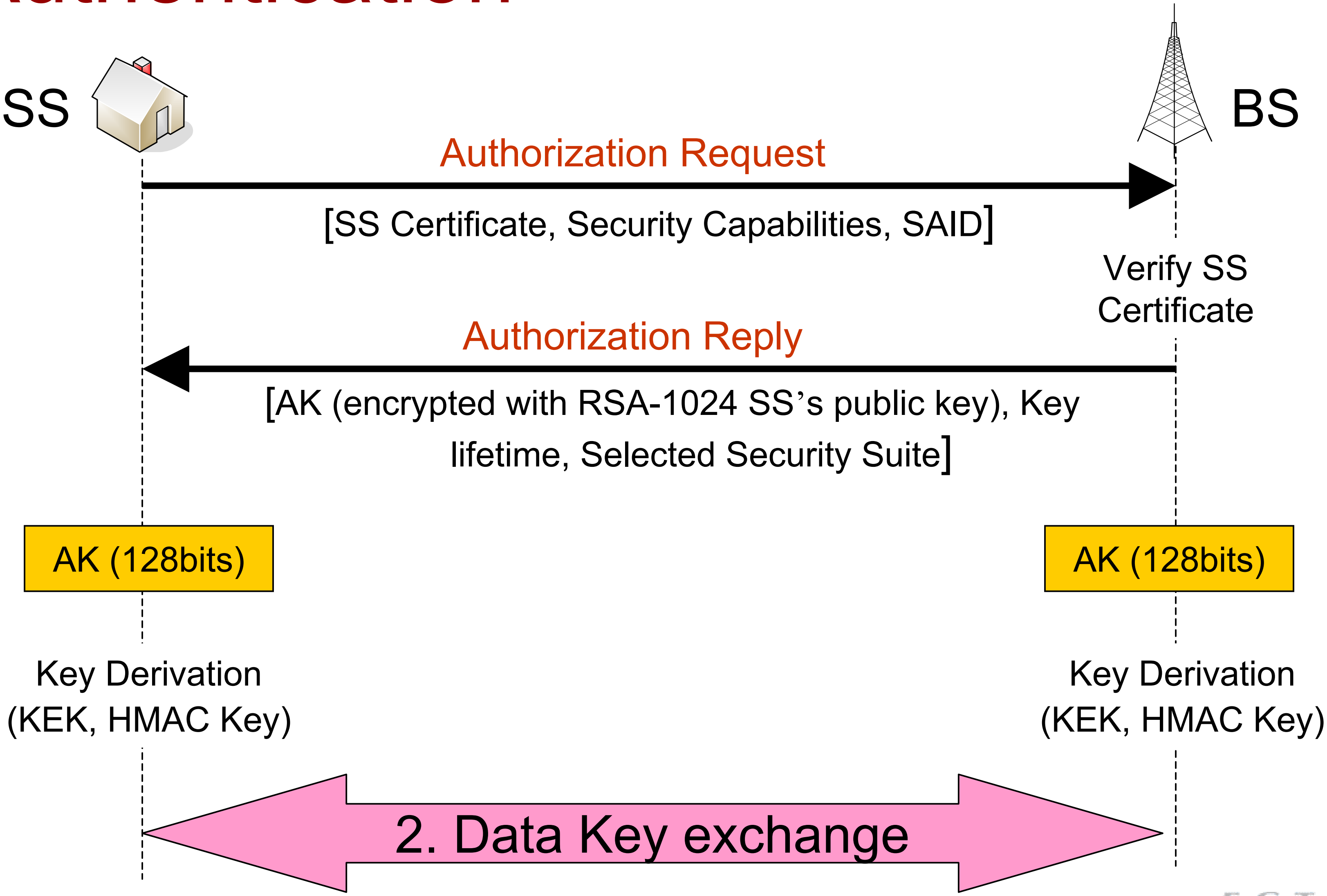
Key Derivation (KEK, HMAC Key)

Key Derivation (KEK, HMAC Key)

Authentication – Vulnerabilities

- No mutual authentication – Rogue BS
- Limited authentication method – client certification
- New authentication method requires changing the authentication message

Authentication



SS

BS

Authorization Request

[SS Certificate, Security Capabilities, SAID]

Verify SS Certificate

Authorization Reply

[AK (encrypted with RSA-1024 SS’s public key), Key lifetime, Selected Security Suite]

AK (128bits)

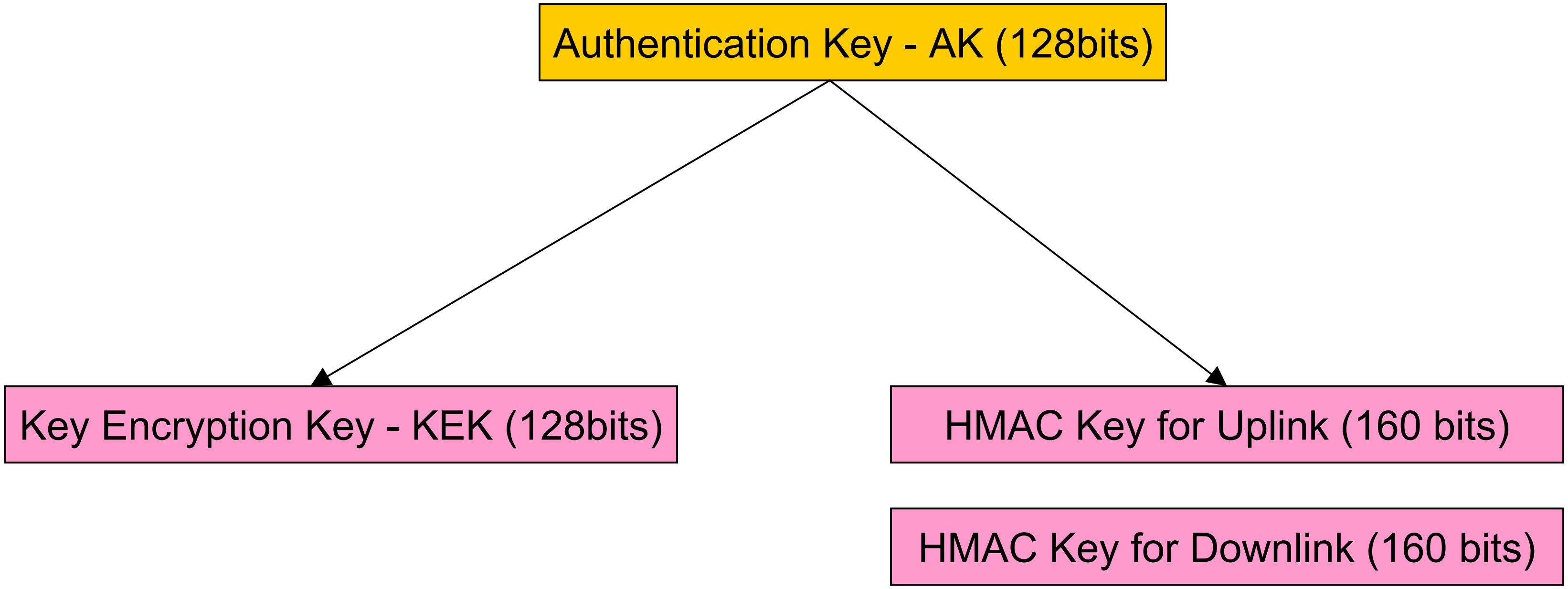
AK (128bits)

Key Derivation (KEK, HMAC Key)

Key Derivation (KEK, HMAC Key)

2. Data Key exchange

Key Derivation



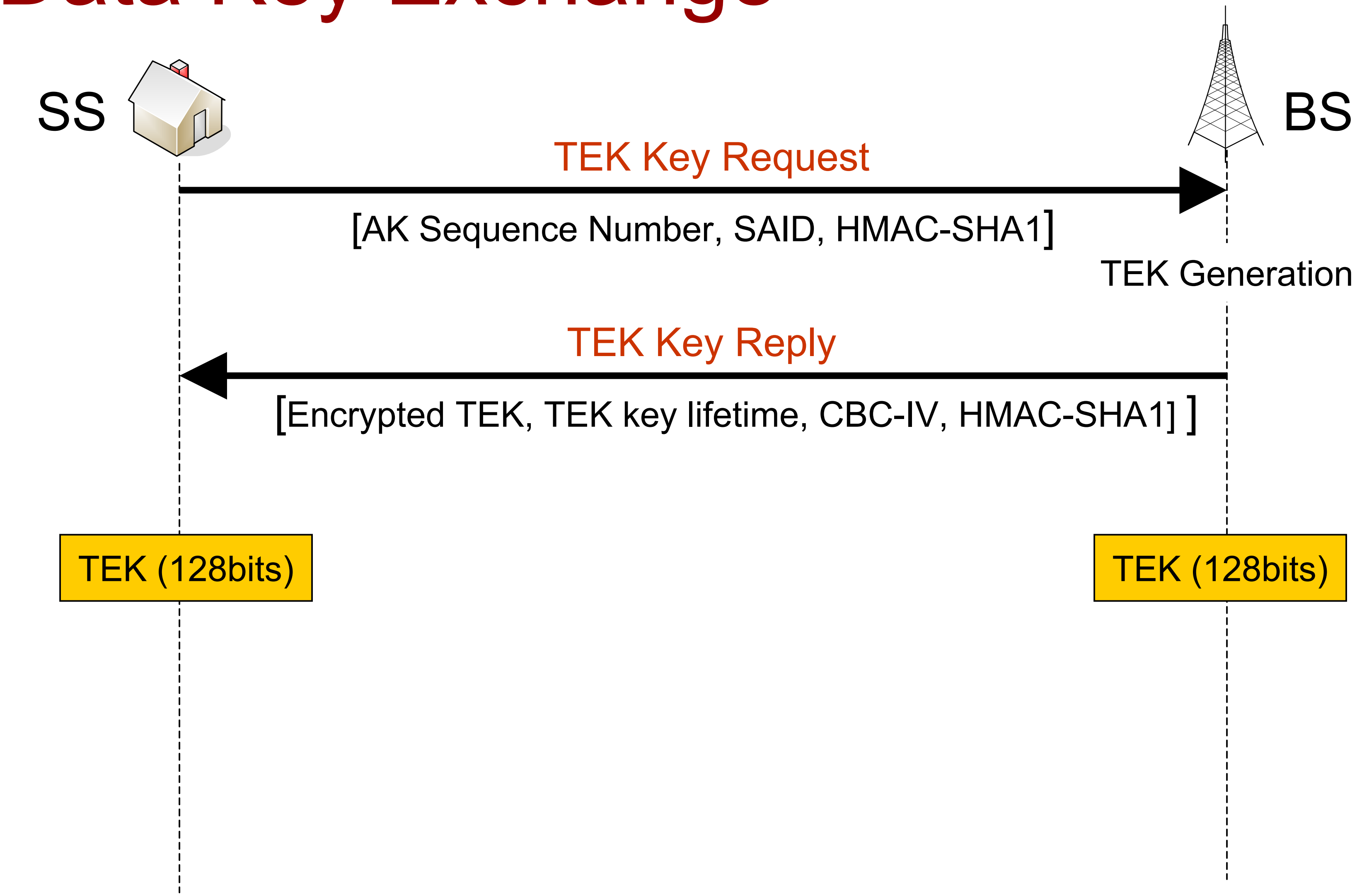
Authentication Key - AK (128bits)

Key Encryption Key - KEK (128bits)

HMAC Key for Uplink (160 bits)

HMAC Key for Downlink (160 bits)

Data Key Exchange



SS

BS

TEK Key Request

[AK Sequence Number, SAID, HMAC-SHA1]

TEK Generation

TEK Key Reply

[Encrypted TEK, TEK key lifetime, CBC-IV, HMAC-SHA1]]

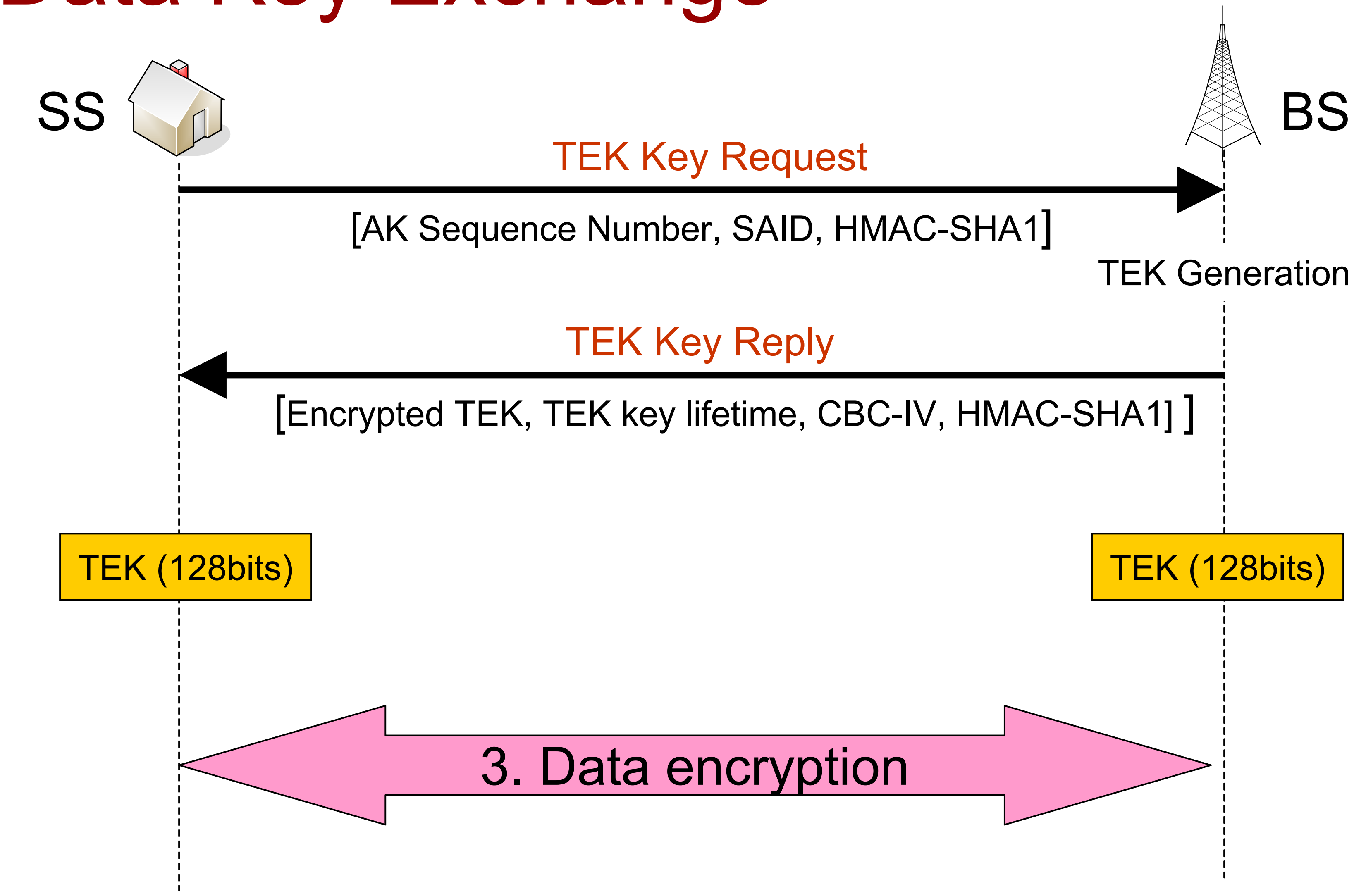
TEK (128bits)

TEK (128bits)

Data Key Exchange

- Transport Encryption Key (TEK)
- TEK is generated by BS randomly
- TEK is encrypted with
  - 3DES (use 128 bits KEK)
  - RSA (use SS's public key)
  - AES (use 128 bits KEK)
- Key Exchange message is authenticated by HMAC-SHA1 – (provides Message Integrity and AK confirmation)

Data Key Exchange



SS

BS

TEK Key Request

[AK Sequence Number, SAID, HMAC-SHA1]

TEK Generation

TEK Key Reply

[Encrypted TEK, TEK key lifetime, CBC-IV, HMAC-SHA1]]

TEK (128bits)

TEK (128bits)

3. Data encryption

Data Encryption

- Encrypt only data message not management message
- DES in CBC Mode
  - 56 bit DES key (TEK)
  - No Message Integrity Detection
  - No Replay Protection
- AES in CCM Mode
  - 128 bit key (TEK)
  - HMAC-SHA1
  - Replay Protection using Packet Number

Conclusions

- Require mutual authentication
- Require more flexible authentication method
- Prefer AES to DES for data encryption