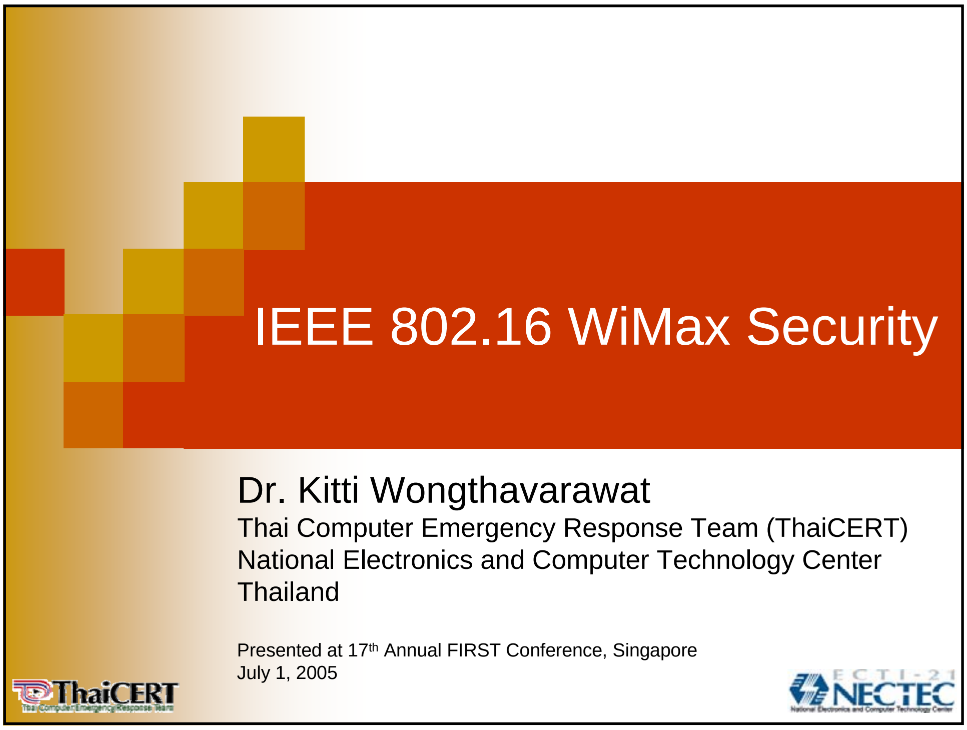
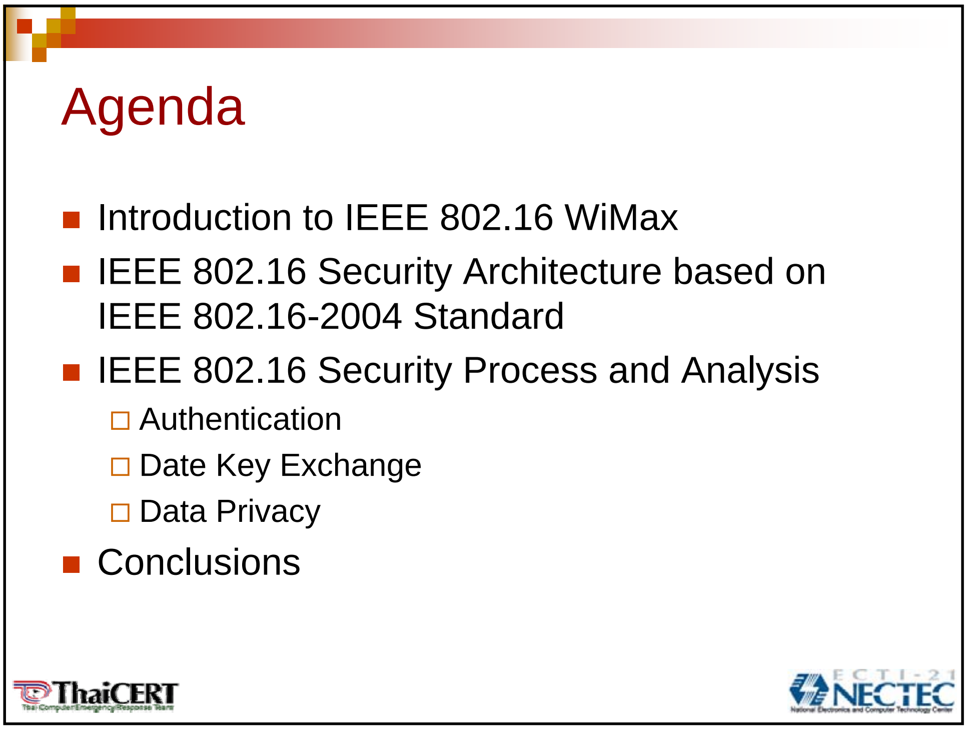


IEEE 802.16 WiMax Security

Dr. Kitti Wongthavarawat
Thai Computer Emergency Response Team (ThaiCERT)
National Electronics and Computer Technology Center
Thailand

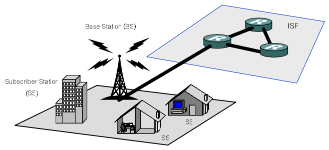
Presented at 17th Annual FIRST Conference, Singapore
July 1, 2005



Agenda

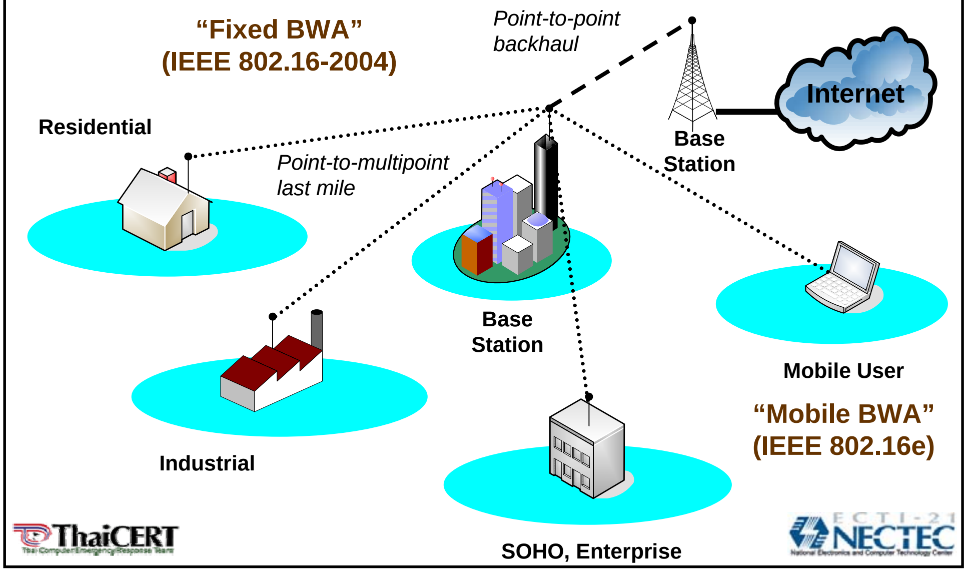
- Introduction to IEEE 802.16 WiMax
- IEEE 802.16 Security Architecture based on IEEE 802.16-2004 Standard
- IEEE 802.16 Security Process and Analysis
  - □ Authentication
  - □ Date Key Exchange
  - □ Data Privacy
- Conclusions

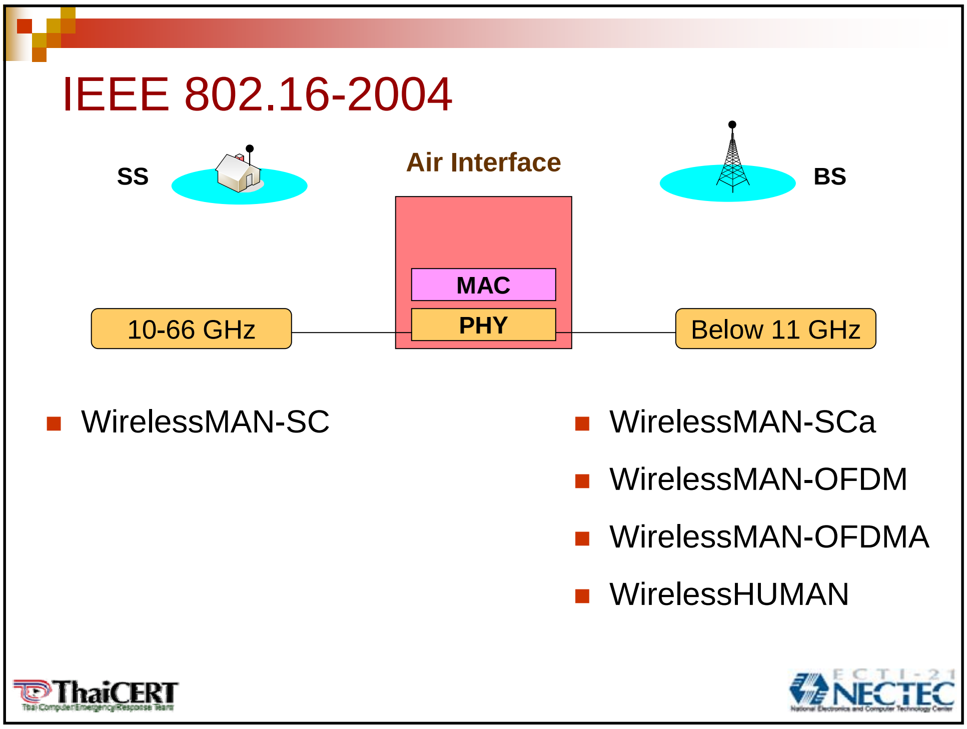
IEEE 802.16 WiMAX



- Wireless Metropolitan Area Network (WMAN) Standard, Broadband Wireless Access (BWA)
- Last mile connectivity
- Range up to 50 km.
- Provide high speed connectivity that supports data, voice and video
- Fast deployment, cost saving

IEEE 802.16 Applications





IEEE 802.16-2004

SS

Air Interface

BS

MAC

PHY

10-66 GHz

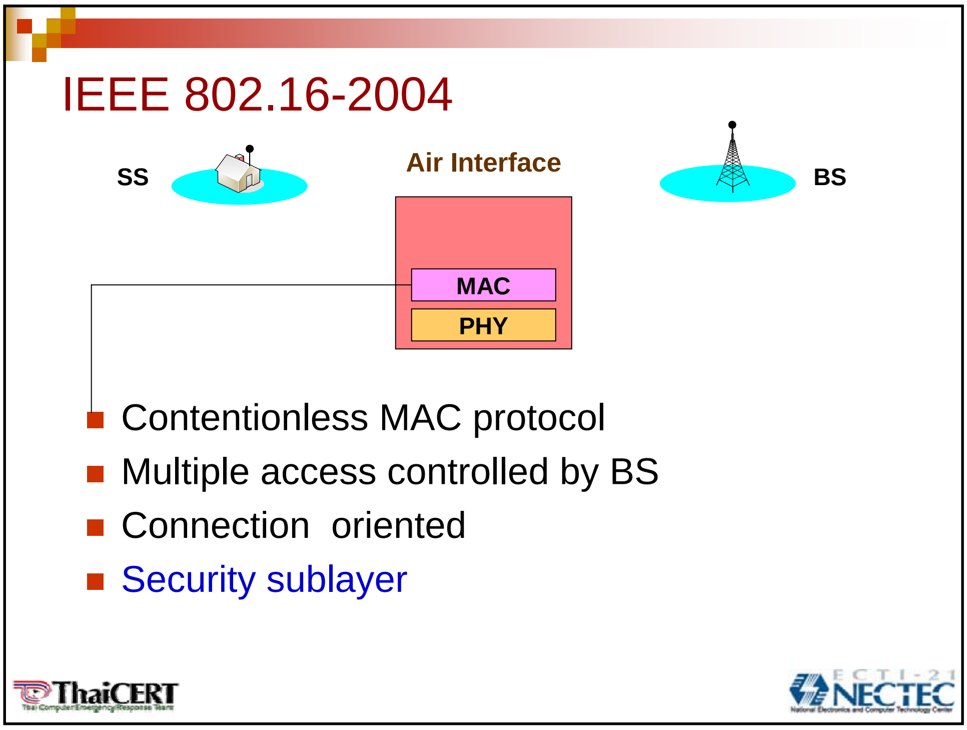
Below 11 GHz

- WirelessMAN-SC

- WirelessMAN-SCa
- WirelessMAN-OFDM
- WirelessMAN-OFDMA
- WirelessHUMAN

ThaiCERT

NECTEC



IEEE 802.16-2004

SS

Air Interface

BS

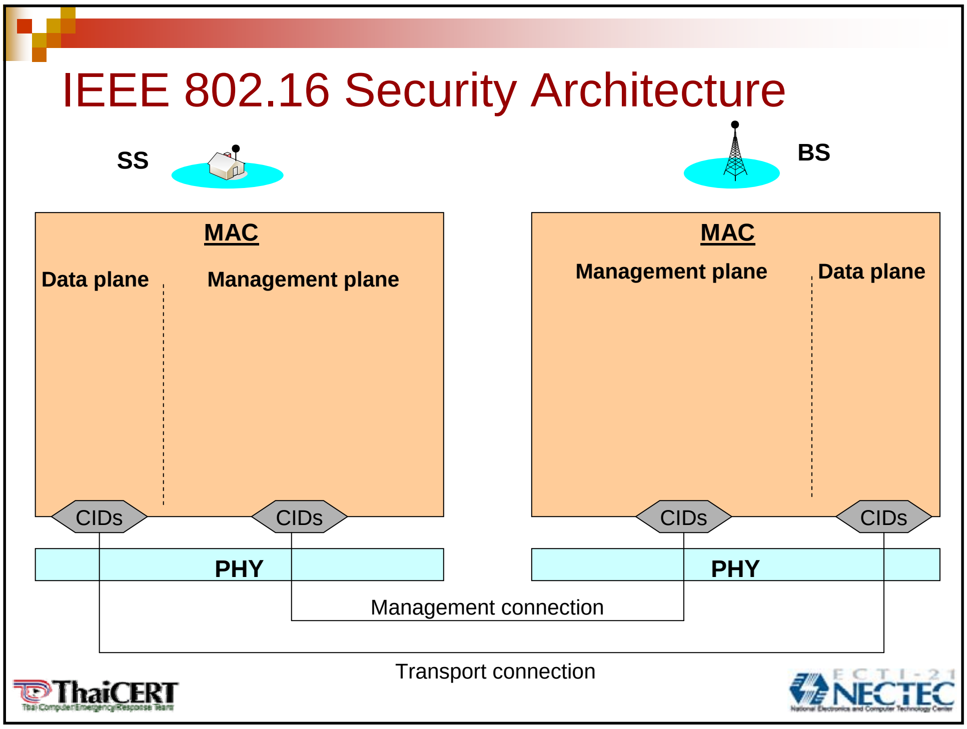
MAC

PHY

- Contentionless MAC protocol
- Multiple access controlled by BS
- Connection oriented
- Security sublayer

ThaiCERT

NECTEC



IEEE 802.16 Security Architecture

SS

BS

MAC

Data plane

Management plane

CIDs

CIDs

PHY

MAC

Management plane

Data plane

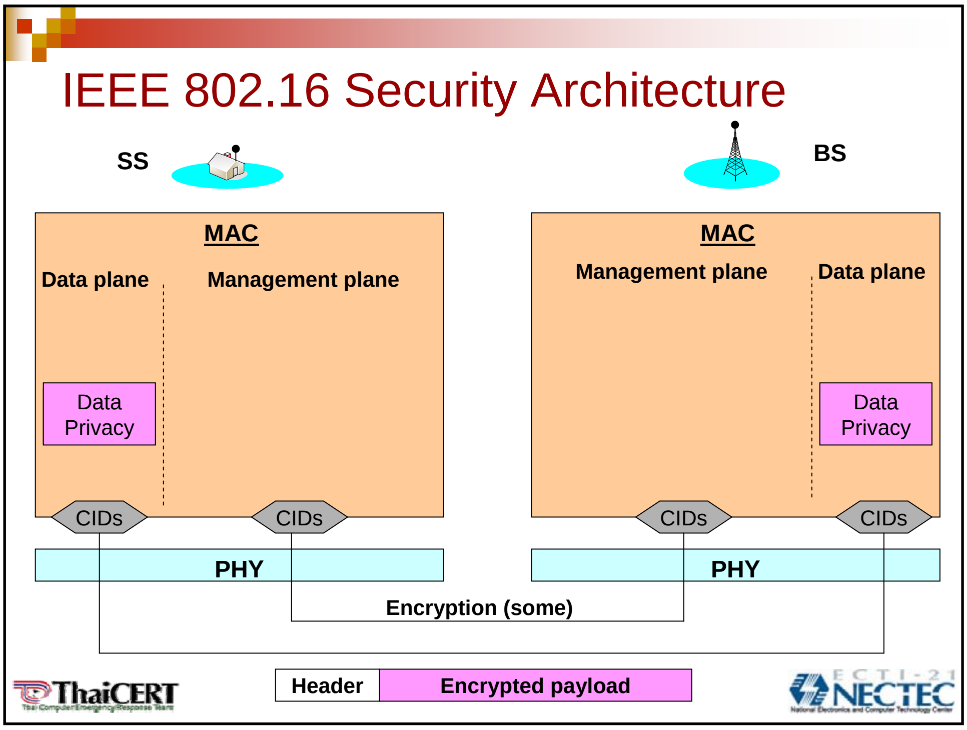
CIDs

CIDs

PHY

Management connection

Transport connection



IEEE 802.16 Security Architecture

SS

BS

MAC

Data plane

Management plane

Data Privacy

CIDs

CIDs

PHY

MAC

Management plane

Data plane

Data Privacy

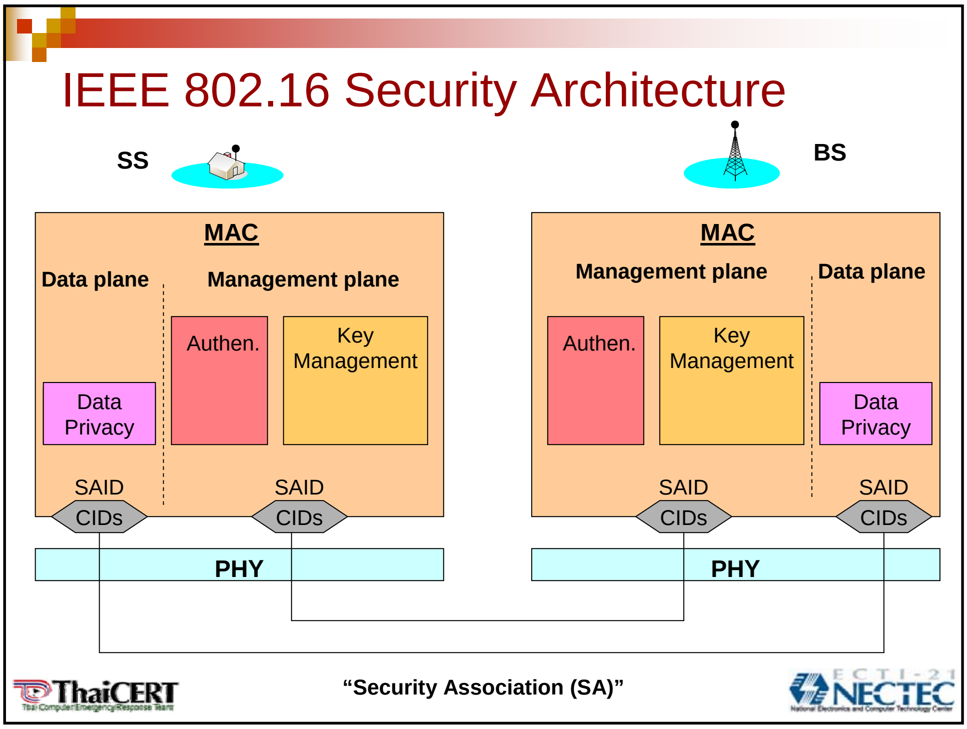
CIDs

CIDs

PHY

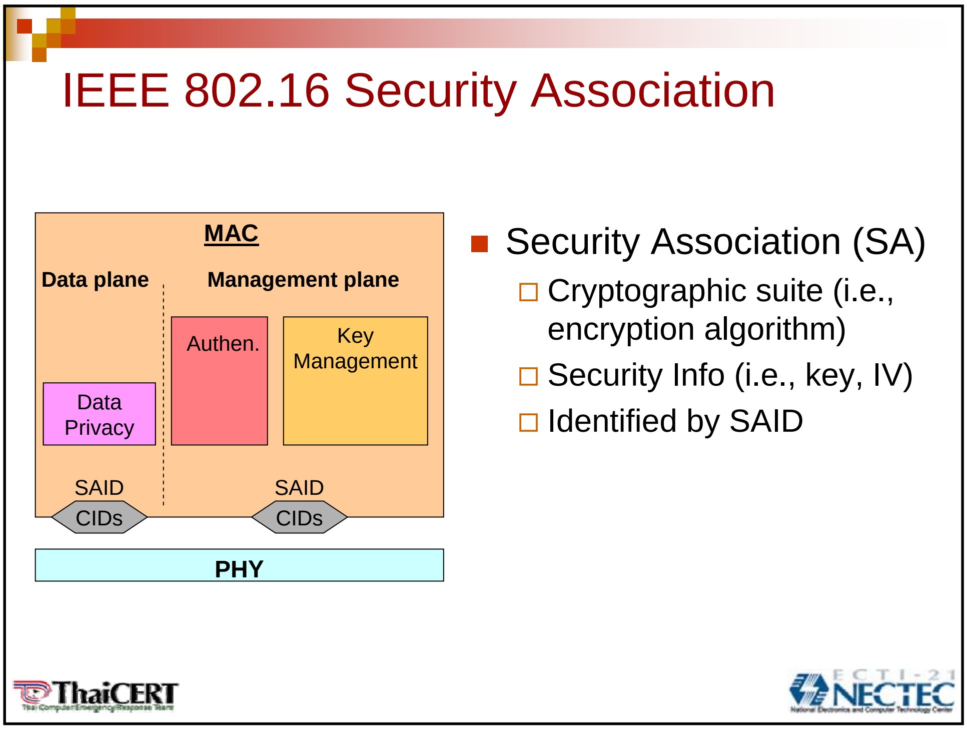
Encryption (some)

Header	Encrypted payload



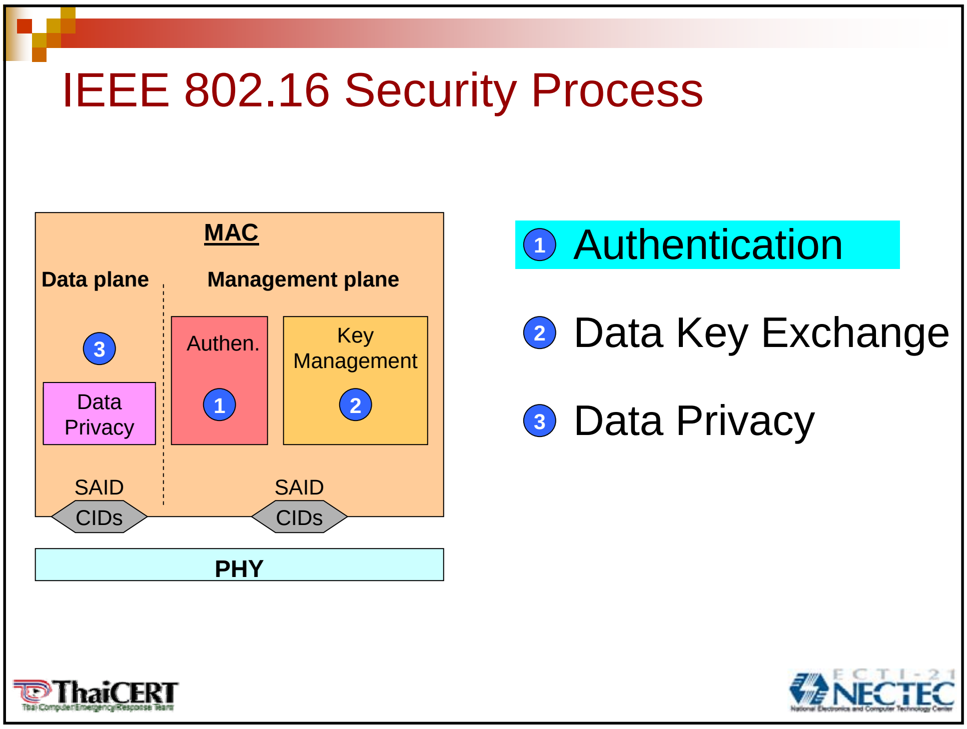
IEEE 802.16 Security Architecture

"Security Association (SA)"



IEEE 802.16 Security Association

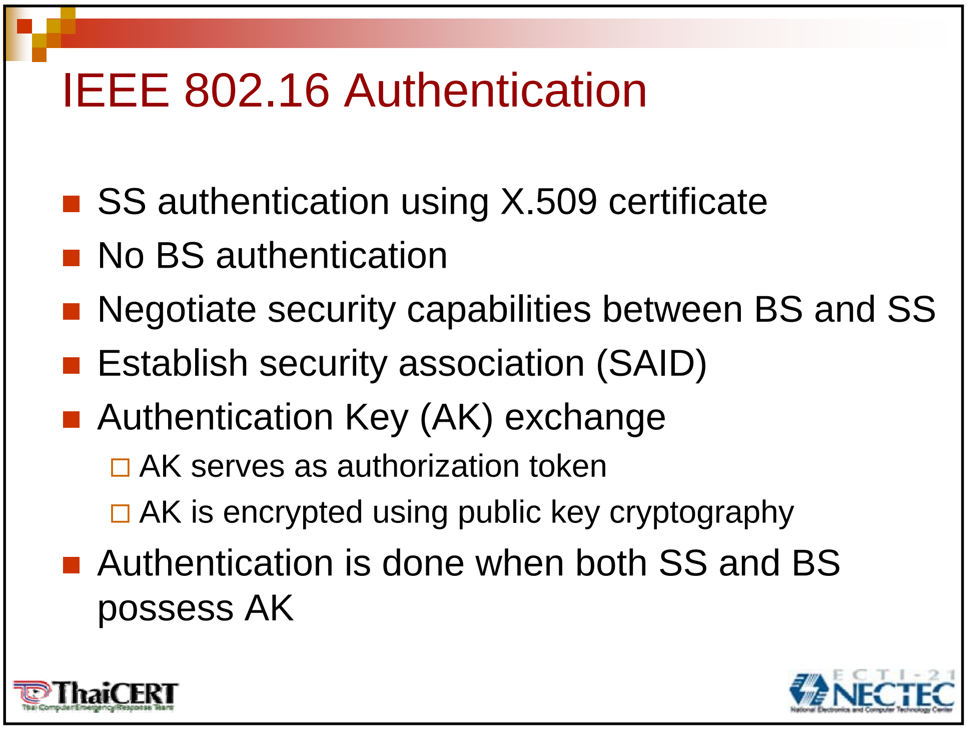
- Security Association (SA)
  - Cryptographic suite (i.e., encryption algorithm)
  - Security Info (i.e., key, IV)
  - Identified by SAID



IEEE 802.16 Security Process

MAC
Data plane
Management plane
3
Data Privacy
Authen.
1
Key Management
2
SAID
CIDs
SAID
CIDs
PHY

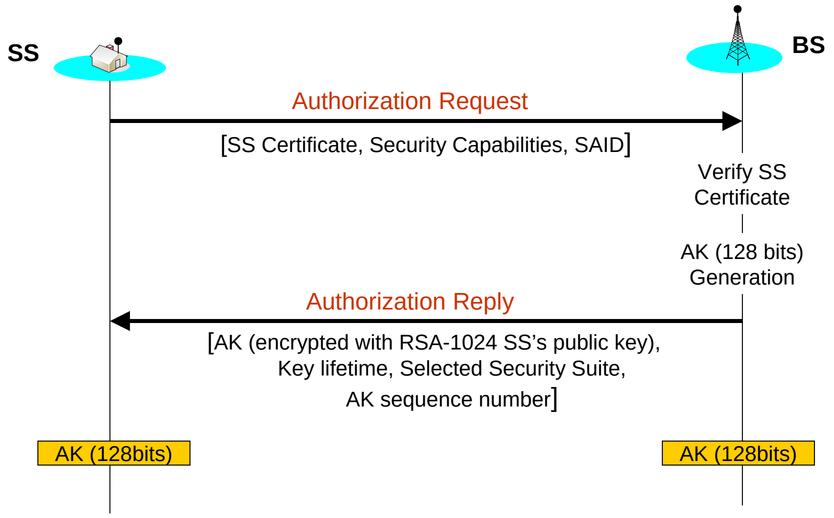
1. Authentication
2. Data Key Exchange
3. Data Privacy



IEEE 802.16 Authentication

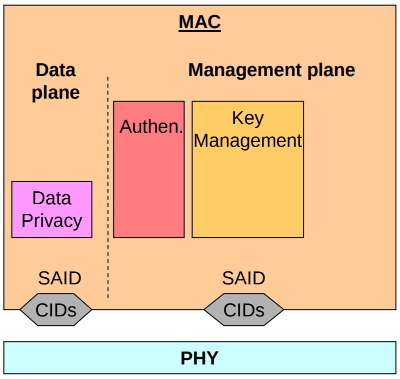
- SS authentication using X.509 certificate
- No BS authentication
- Negotiate security capabilities between BS and SS
- Establish security association (SAID)
- Authentication Key (AK) exchange
  - AK serves as authorization token
  - AK is encrypted using public key cryptography
- Authentication is done when both SS and BS possess AK

IEEE 802.16 Authentication


SS
BS
Authorization Request
[SS Certificate, Security Capabilities, SAID]
Verify SS Certificate
AK (128 bits) Generation
Authorization Reply
[AK (encrypted with RSA-1024 SS's public key), Key lifetime, Selected Security Suite, AK sequence number]
AK (128bits)
AK (128bits)

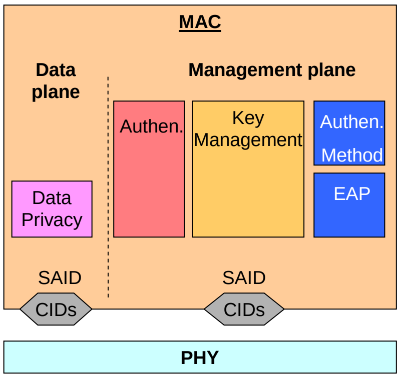
Key lifetime = 1 day to 70 days

IEEE 802.16 Authentication Analysis



- No mutual authentication – Rogue BS
  - □ Man-in-the-middle attack
- Limited authentication method – SS certification
- New authentication method requires adding new type of authentication message

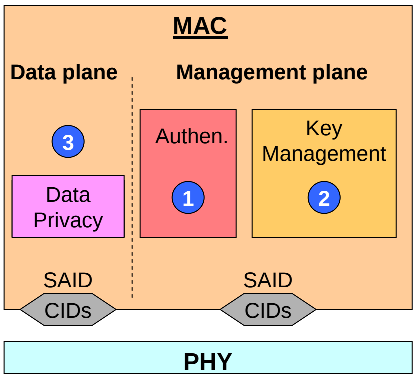
IEEE 802.16 Authentication Analysis



Solution

- EAP-based Authentication
- Authentication methods (i.e., EAP-TLS, EAP-TTLS, PEAP, EAP-SIM)
- Extend the authentication to AAA Server
- Proposed in draft IEEE 802.16e

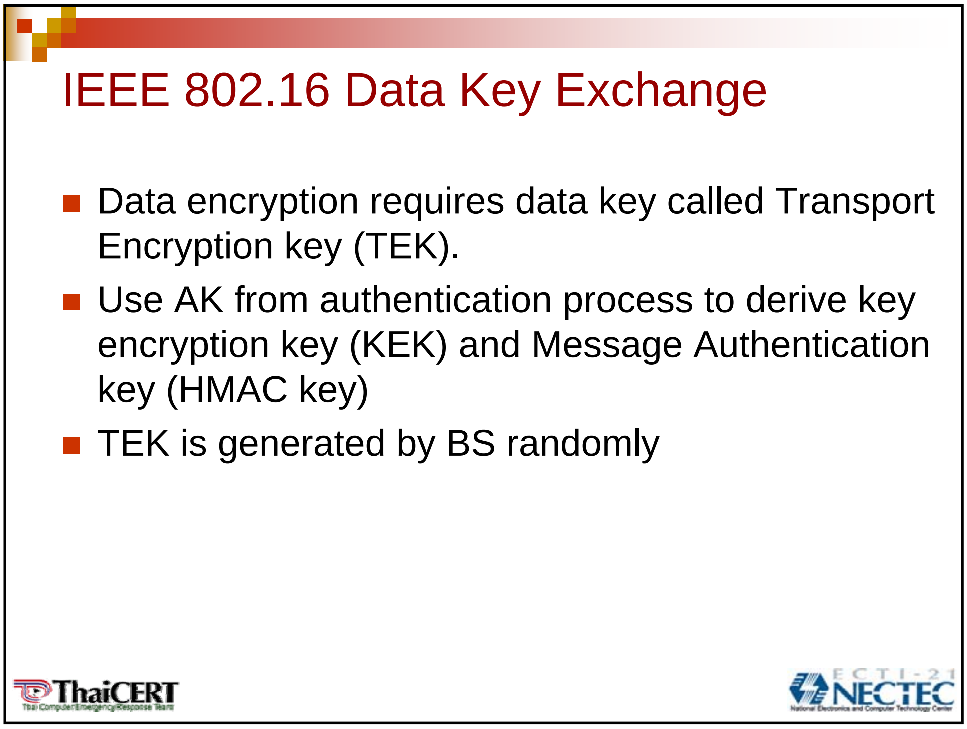
IEEE 802.16 Security Process



1 Authentication

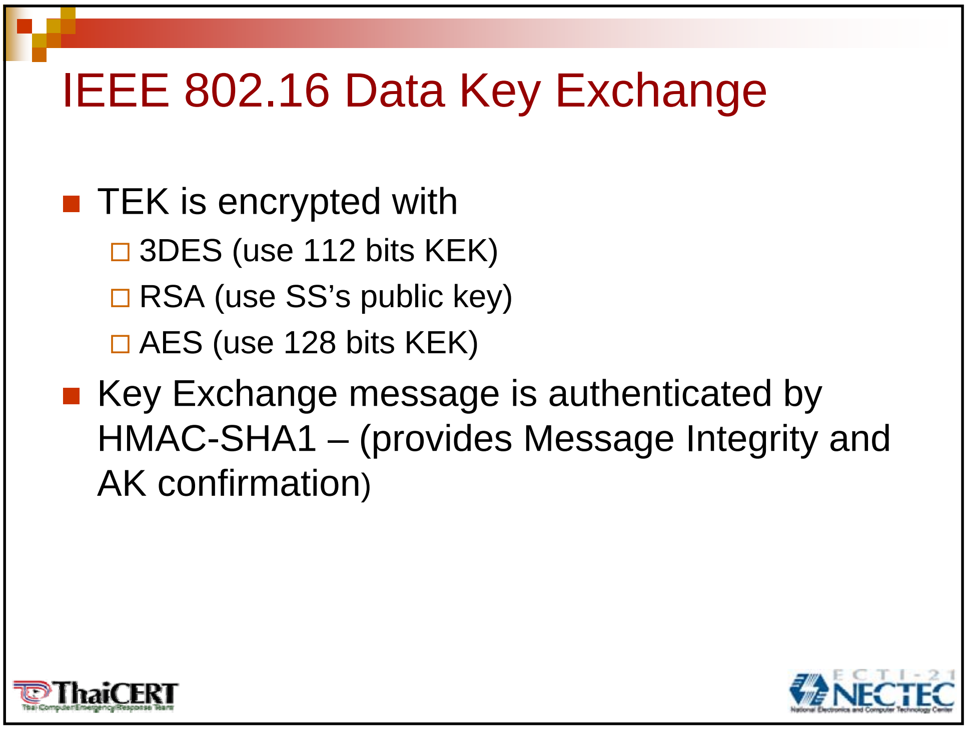
2 Data Key Exchange

3 Data Privacy



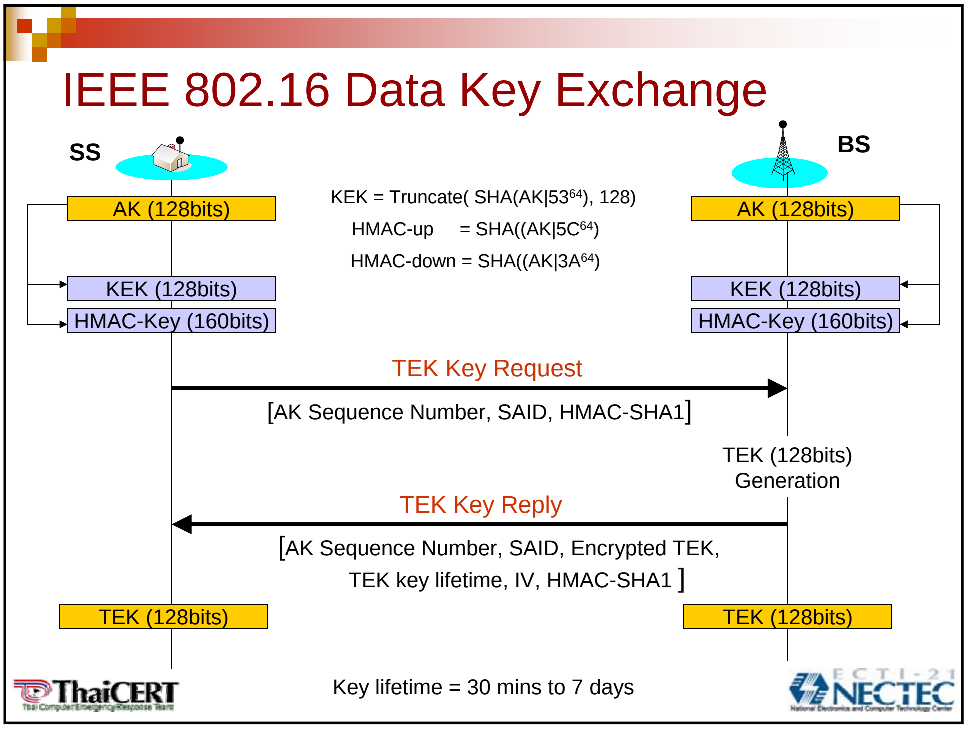
IEEE 802.16 Data Key Exchange

- Data encryption requires data key called Transport Encryption key (TEK).
- Use AK from authentication process to derive key encryption key (KEK) and Message Authentication key (HMAC key)
- TEK is generated by BS randomly



IEEE 802.16 Data Key Exchange

- TEK is encrypted with
  - □ 3DES (use 112 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)



IEEE 802.16 Data Key Exchange

SS

BS

AK (128bits)

AK (128bits)

KEK = Truncate(SHA(AK|53^{64}), 128)

HMAC-up = SHA((AK|5C^{64})

HMAC-down = SHA((AK|3A^{64})

KEK (128bits)

HMAC-Key (160bits)

KEK (128bits)

HMAC-Key (160bits)

TEK Key Request

[AK Sequence Number, SAID, HMAC-SHA1]

TEK (128bits)
Generation

TEK Key Reply

[AK Sequence Number, SAID, Encrypted TEK,
TEK key lifetime, IV, HMAC-SHA1]

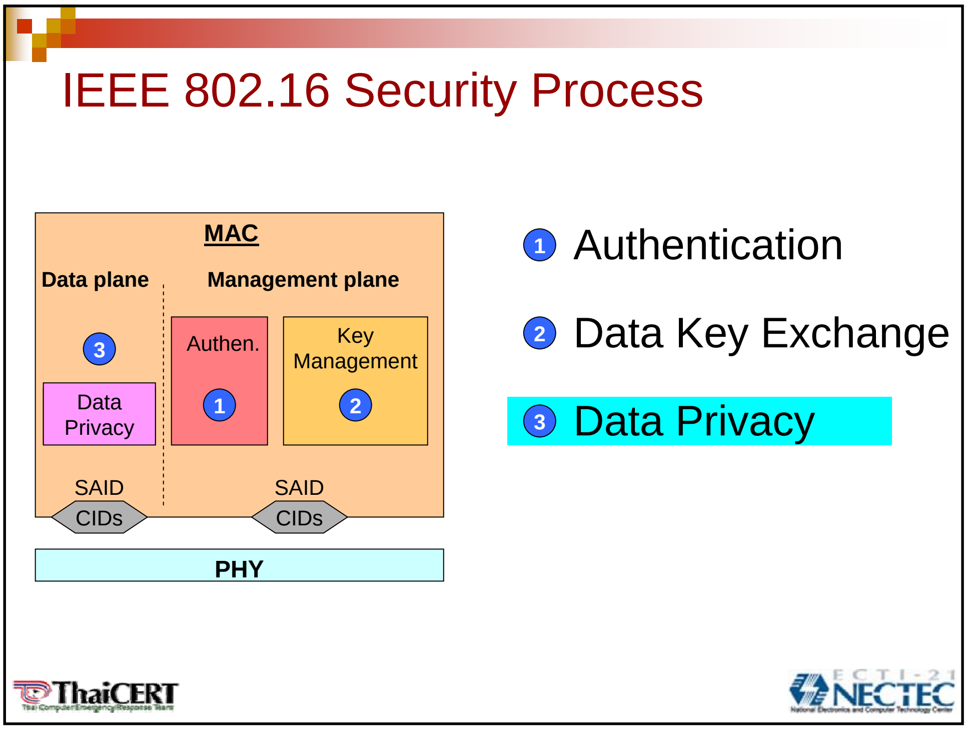
TEK (128bits)

TEK (128bits)

Key lifetime = 30 mins to 7 days

ThaiCERT

ECTI-21 NECTEC



IEEE 802.16 Security Process

MAC

Data plane

Management plane

3

Data Privacy

Authen.

1

Key Management

2

SAID

CIDs

SAID

CIDs

PHY

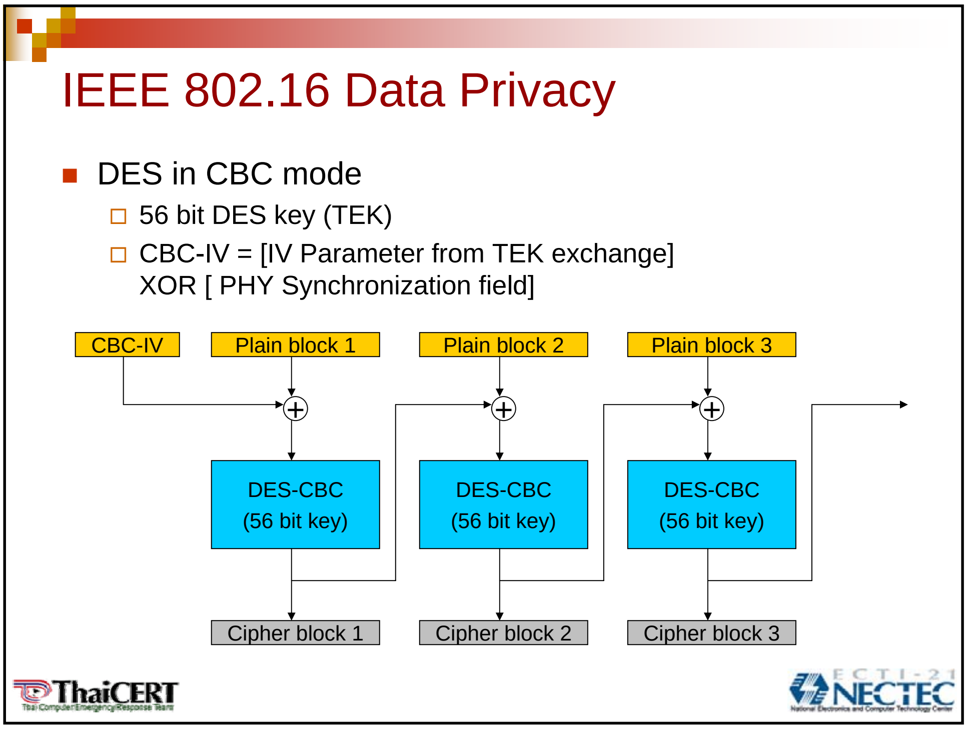
1 Authentication

2 Data Key Exchange

3 Data Privacy

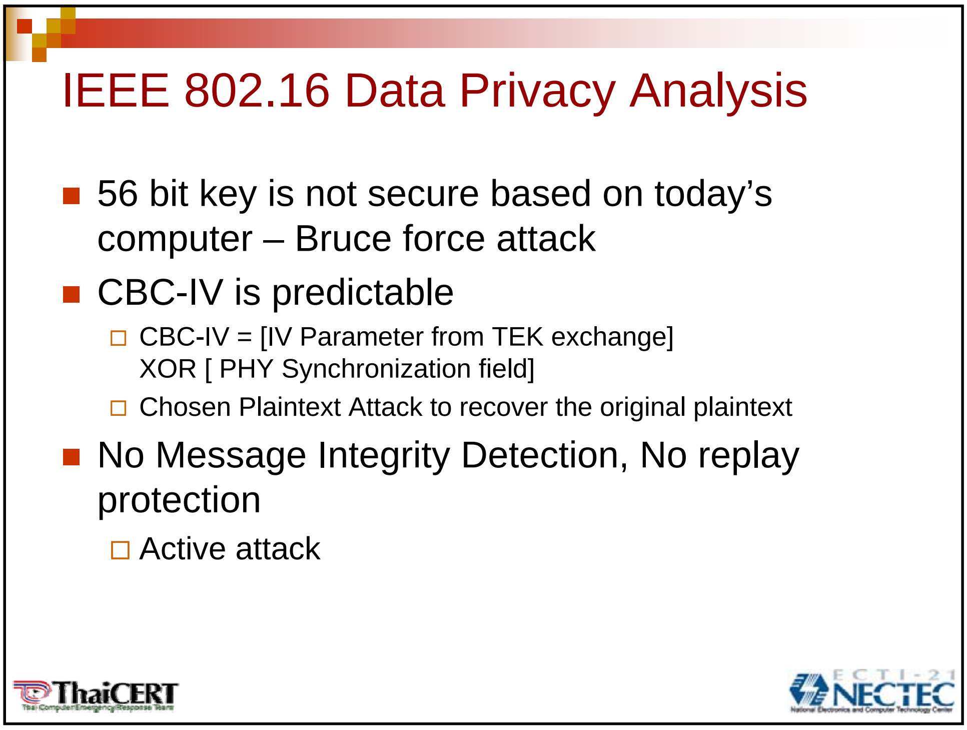
ThaiCERT

ECTI-21 NECTEC



IEEE 802.16 Data Privacy

- DES in CBC mode
  - □ 56 bit DES key (TEK)
  - □ CBC-IV = [IV Parameter from TEK exchange]
    XOR [PHY Synchronization field]



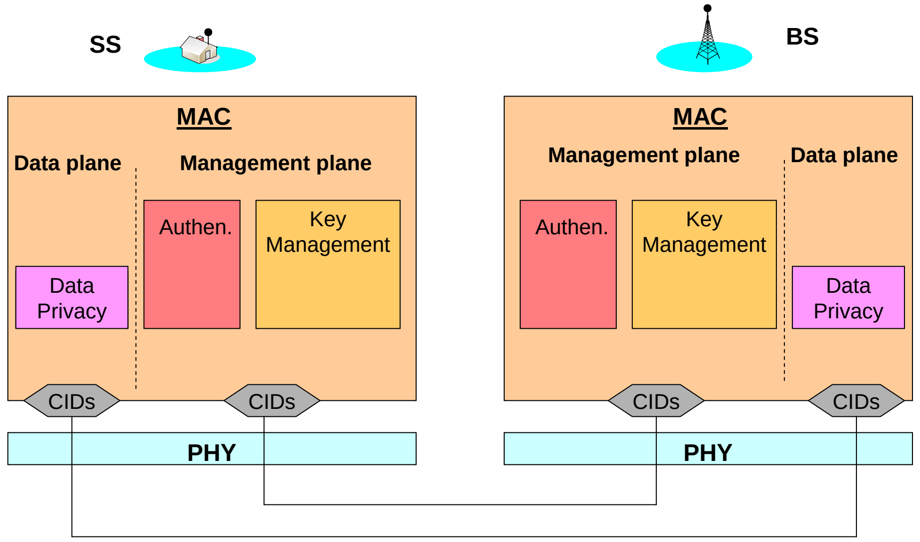
IEEE 802.16 Data Privacy Analysis

- 56 bit key is not secure based on today's computer – Bruce force attack
- CBC-IV is predictable
  - □ CBC-IV = [IV Parameter from TEK exchange]
    XOR [PHY Synchronization field]
  - □ Chosen Plaintext Attack to recover the original plaintext
- No Message Integrity Detection, No replay protection
  - □ Active attack

IEEE 802.16 Data Privacy

- AES in CCM Mode
  - □ 128 bit key (TEK)
  - □ Message Integrity Check
  - □ Replay Protection using Packet Number

IEEE 802.16 Security Architecture



SS

BS

MAC

Data plane

Management plane

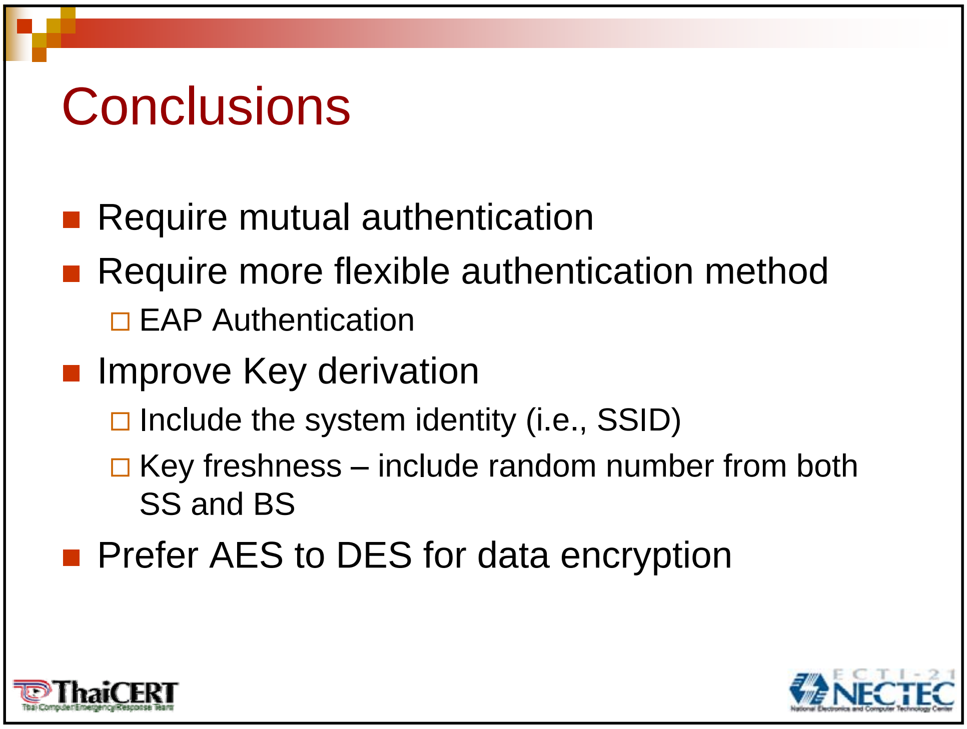
Authen.

Key Management

Data Privacy

CIDs

PHY



Conclusions

- Require mutual authentication
- Require more flexible authentication method
  - □ EAP Authentication
- Improve Key derivation
  - □ Include the system identity (i.e., SSID)
  - □ Key freshness – include random number from both SS and BS
- Prefer AES to DES for data encryption