Document : ISO/IEC WAPI N 27

Date : 2005-08-18

TITLE : WAPI Technology Overview - CNB contribution for the Beijing meeting, 8-12 August

SOURCE : CNB

REQUESTED ACTION : For information

DISTRIBUTION :

Note: This revises and replaces WAPI N. 17

WAPI Technology Overview

Chinese National Body

Date: 2005-08

Abstract

This document is about the overview of WAPI, which is PART 1 of the contribution (Doc: WAPI N16) to Beijing meeting from Chinese National Body.

The contribution has been submitted to ISO/IEC on July 25th, 2005.

This document is the detailed version of PART 3 in document WAPI N17

Agenda

- Background
- Overall Architecture
- Description of WAPI Features
- Summary

Background

- ISO/IEC 8802.11 deployers want to transform commonly held resource (local unlicensed bandwidth) into a private access controlled resource.
  - ✓WEP security technology is not competent for the goal.
  - ✓New security technology is required by market.

Part 1

Overall Architecture

Overall Architecture

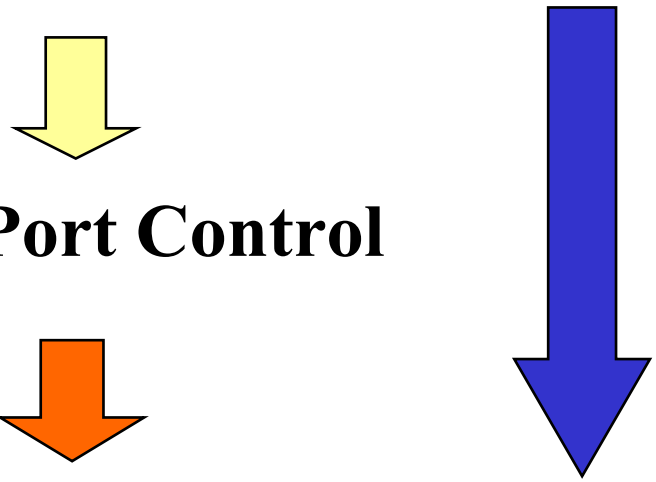
- WAPI concepts
- Security service relations
- Operation of WAPI
- WAPI architecture

WAPI Concepts

- WAPI: WLAN Authentication and Privacy Infrastructure
- WAI: WLAN Authentication Infrastructure
- WPI: WLAN Privacy Infrastructure
- Controlled Port: Passes or blocks the data traffic
- Uncontrolled Port: Passes the WAI traffic
- WAPI Security Network: A network with the WAPI security mechanism.

Security service relations

Authentication and Key Management



Peer Port Control

Data Integrity and Data Confidentiality

Operation of WAPI

STA AP ASU

Discover security policy

Select security policy

Certificate authentication and key management

Certificate Authentication

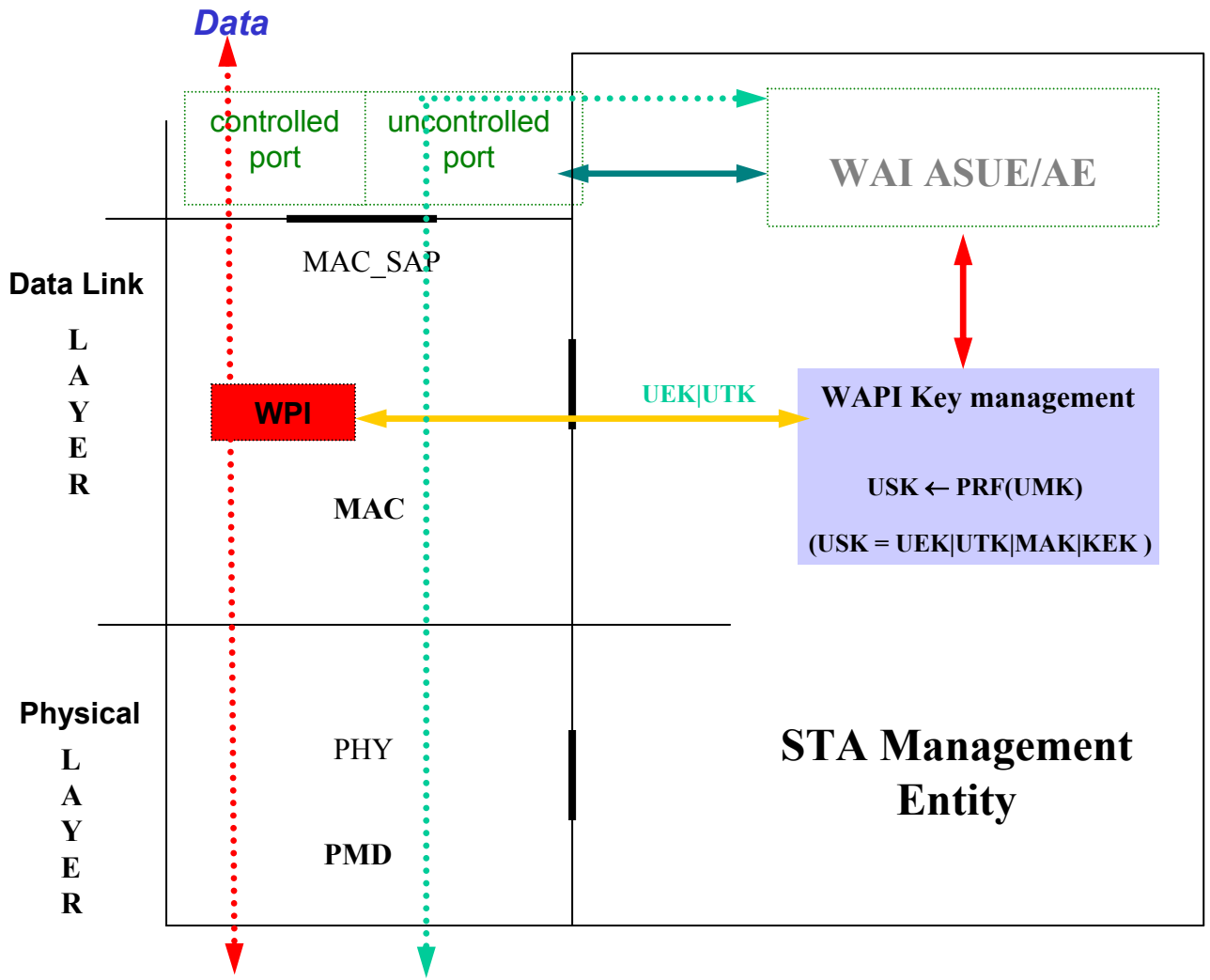
Controlled port on

Key negotiation

Controlled port on

Data protection

Architecture and Relations



Part 2

WAPI Features

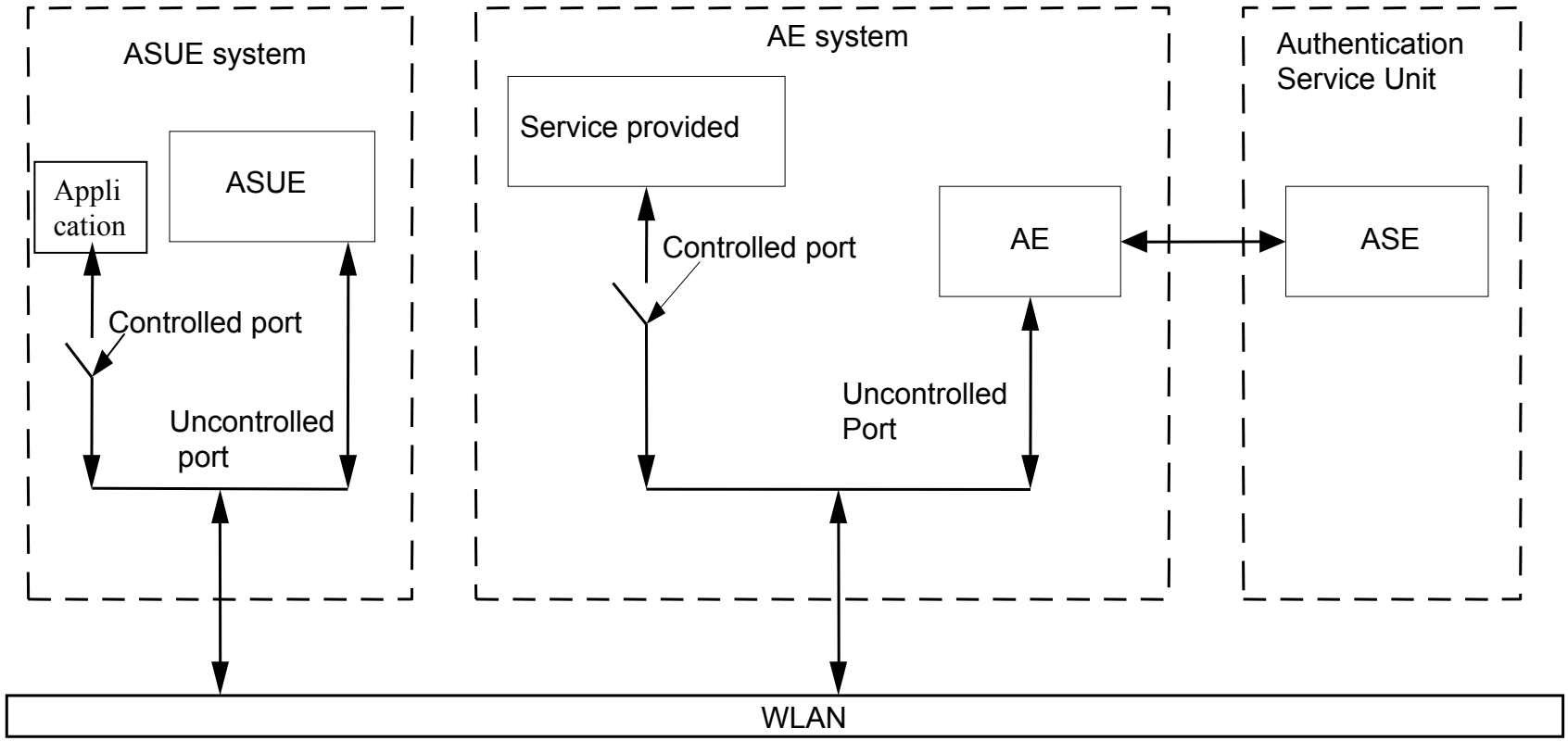
Overview

- **Peer Port Control**
- **WAI**
  - ✓**Discovery and Negotiation of security policy**
  - ✓**Authentication and key management**
- **WPI**

Concepts for Peer Port Control

- Controlled Port – for blocking/passing “normal” data traffic
- Uncontrolled Port – for WAI traffic only
- AE(Authenticator Entity): An entity that provides authentication action for the authentication supplicant before the supplicant access to the service.
- ASUE(Authentication SUpplicant Entity):An entity that requests identity authentication through any ASE (authentication service entity).
- ASE(Authentication Service Entity):An entity that provides security management for the AE and the ASUE.

Architecture of Peer Port Control

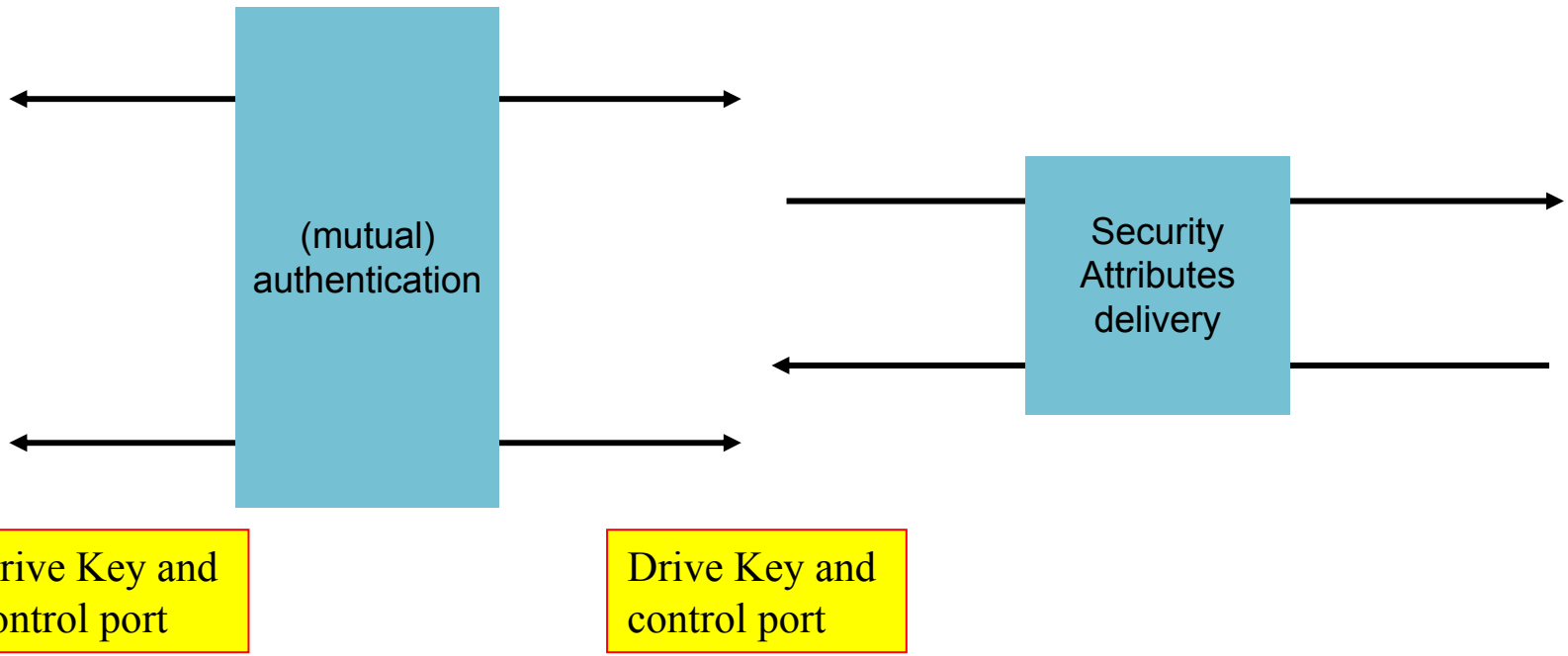


Peer Port Control Message

ASUE

AE

ASE



Peer Port Control Discussion

- Peer Port Control gets some advantages over IEEE 802.1x.
- ASUE has controlled port also
  - ✓ ASUE will be attacked in WLAN
- AE is not only a proxy of ASE. It has independent identity.
  - ✓ AE can completes authentication with ASUE directly.
- ASE is the security manager implementing the function of attributes management.
  - ✓ There is not a necessary security channel for delivering a secrete key from ASE to AE.

Peer Port Control Summary

- Peer to peer control
  - ✓ There is the controlled port in both ASUE and AE.
  - ✓ ASUE and AE are a pair in authentication procedure.
  - ✓ Each AE is discriminable to ASUE. Both AE and ASUE know that who the peer is.
- System is self-sufficient
  - ✓ ASE also is a trusted third party. Then the ASUE, AE and ASE construct the whole security system together.

Discovery and Negotiation of Security Policy

- Discovery--Find the security policy available through the Beacon and Probe Response frame
  - ✓ What Authentication and Key Management Protocol(AKMP), Unicast and Multicast Ciphersuites are available?
- Negotiation
  - ✓ Determine the policy through Association in BSS mode.
  - ✓ Determine the policy through unicast key negotiation in IBSS mode.

WAPI Parameter Set

Element ID	Length	Version
AKMS Count		AKMS
AKMS		Unicast Cipher Suite count
Unicast Cipher Suite		
Multicast Cipher Suite		
WAPI Capability Information		BKID count
BKID List		

Discovery

STA

AP/STA

Probe Request

Beacon/probe Response +WAPI Parameter Set (AP Supports WAI Certificate Authentication and Key Management, WAI Pre-shared Key Authentication and Key Management, WPI unicast, WPI multicast)

Advertises WLAN security policy. If There is not the WAPI parameter set in the frame, the WAPI security network is not supported by the AP/STA.

BSS Negotiation

STA **AP**

STA selects AKMP and Unicast Cipher suite from advertised

Association Request + WAPI parameter set (STA requests WAI Certificate Authentication and Key management, WPI unicast WPI multicast)

Association Response (Success)

IBSS Negotiation 1

STA1 **STA2**

Beacon or Probe Response +WAPI parameter set (STA2 supports WAI Certificate Authentication and Key management, WAI Preshared Key Authentication and Key management, WPI unicast,WPI multicast)

Has intersection

Beacon or Probe Response +WAPI parameter set (STA1 supports WAI Certificate Authentication and Key management, WAI Preshared Key Authentication and Key management, WPI unicast WPI multicast)

Can establish IBSS between STA1 and STA2

IBSS Negotiation 2

STA1(AE) ..... **STA2(ASUE)**

STA1 chooses the Pre-shared Key Authentication and Key management

Unicast Key Negotiation Request

Unicast Key Negotiation Response+
WAPI parameter set (…, ~~WPI unicast~~)

STA2 chooses

Unicast Key Negotiation Confirmation +
WAPI parameter set

IBSS Negotiation 3

STA1(ASUE) ..... **STA2(AE)**

STA2 chooses Certificate Authentication and Key management

Authentication Activation

Completes Certificate Authentication procedure

Completes Certificate Authentication procedure

Unicast Key Negotiation Request

Unicast Key Negotiation Response+ WAPI parameter set (…, ~~WPI unicast~~)

STA1 selects

Unicast Key Negotiation Confirmation+ WAPI parameter set

IBSS Negotiation Discussion

- STA1 and STA2 start a separate key negotiation.
  - ✓ STA1 start: STA1 selects Authentication and Key management method and multicast cipher suite. STA2 selects unicast cipher suite.
  - ✓ STA2 start: STA2 selects Authentication and Key management method and multicast cipher suite. STA1 selects unicast cipher suite.
- Unicast cipher suite: STA1 or STA2?
  - ✓ Higher MAC address wins.

Discovery and Negotiation Discussion

- Backward compatible with the existed devices
  - ✓existed devices do not recognize WAPI IE, nor do they include it in their Association messages
- Extensible: WAPI IE permits the addition of new cipher suites and AKMPs not contemplated by WAPI
- WAPI key management (below) protects against downgrade attacks

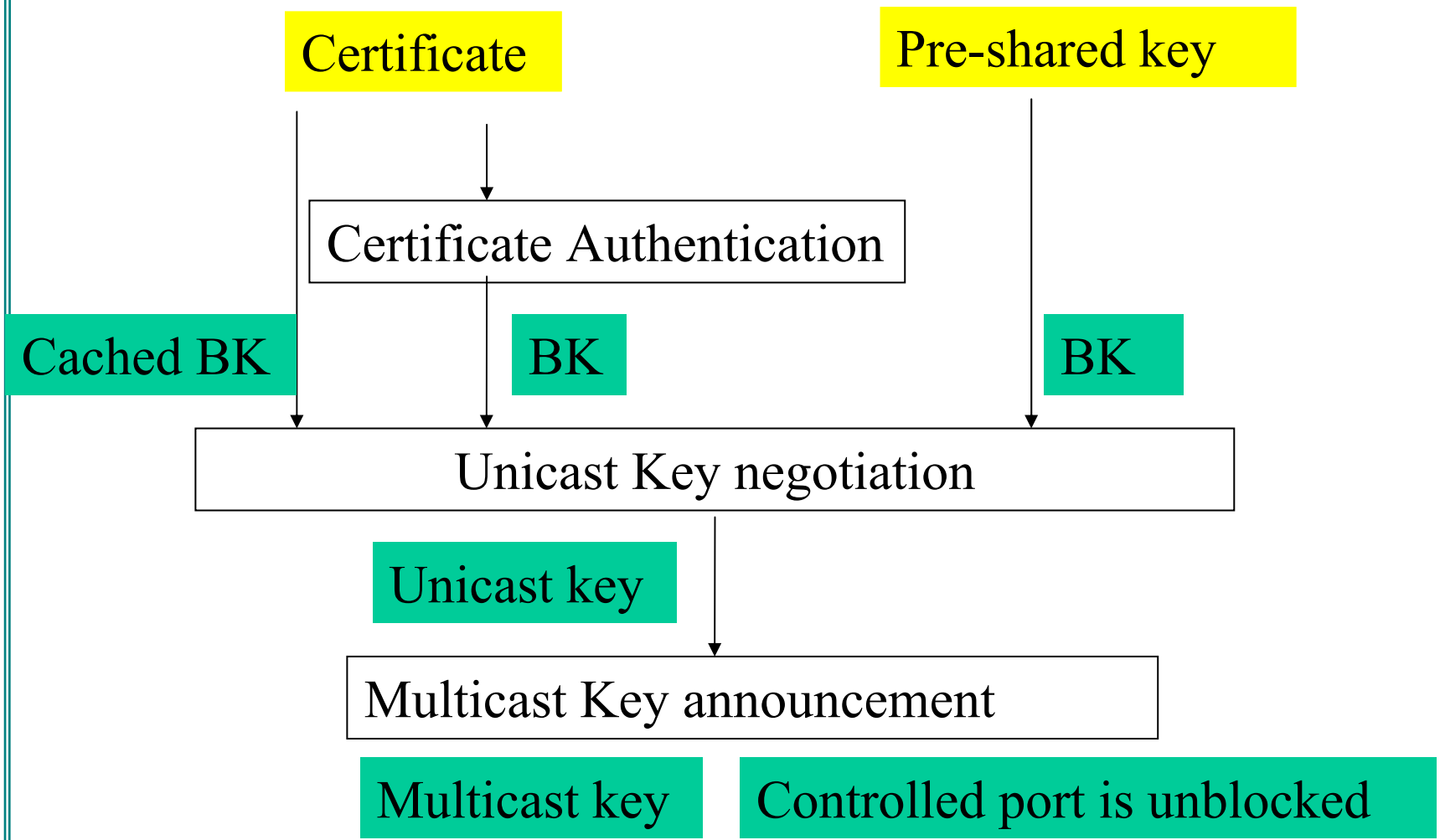
WAI

- Authentication and Key management completes the mutual authentication, establish required keys.
- Design consideration
  - ✓ Different deployment model has different requirements.
  - ✓ We should not adopt too many authentication methods in order to avoid complex implementation.
  - ✓ downgrade attacks should be protected against.
  - ✓ Meets the requirement of multiple keys

WAI design

- Two authentication methods are defined:
  - ✓ Authentication and Key management based on Certificate
  - ✓ Authentication and Key management based on pre-shared key
- Permits adding new authentication methods.
- Three procedures are introduced.
  - ✓ Certificate Authentication
  - ✓ Unicast Key Negotiation
  - ✓ Multicast Key Announcement

Overview of WAI



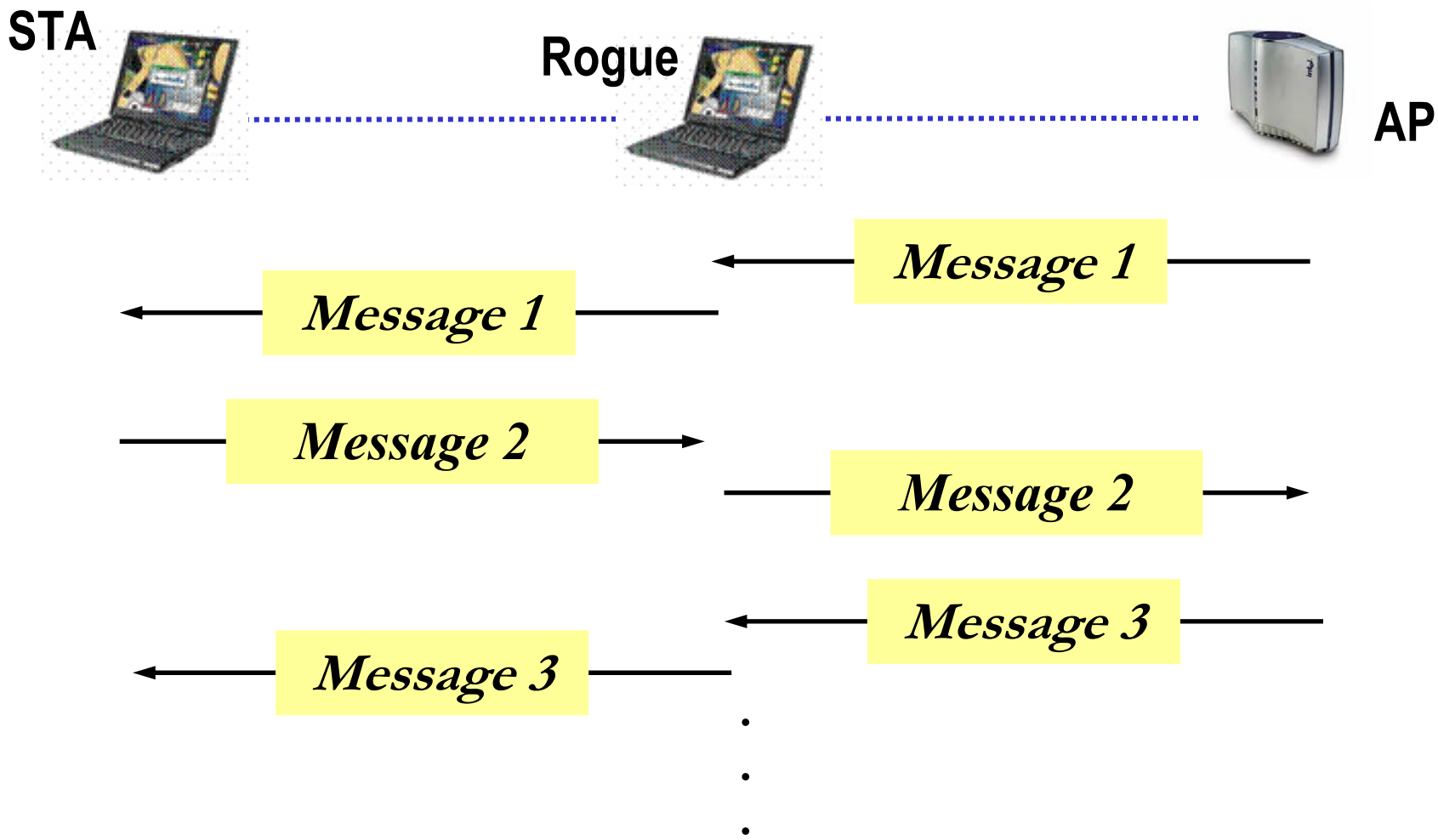
WAI discussion

- Be able to meet major deployment.
  - ✓Certificate for enterprise and operator
  - ✓Pre-shared Key for home
  - ✓Extension is supported
  - ✓avoiding complex implementation
- Separate procedure design is flexible
  - ✓Specific procedure manage specific keys
  - ✓Adopt suitable method easily

Certificate Authentication

- Goals
  - ✓Mutual Authentication
  - ✓Base Key generation
  - ✓Immunity from off-line dictionary
  - ✓Immunity from man-in-the-middle attacks
  - ✓Perfect Forward Security

MITM Attacks

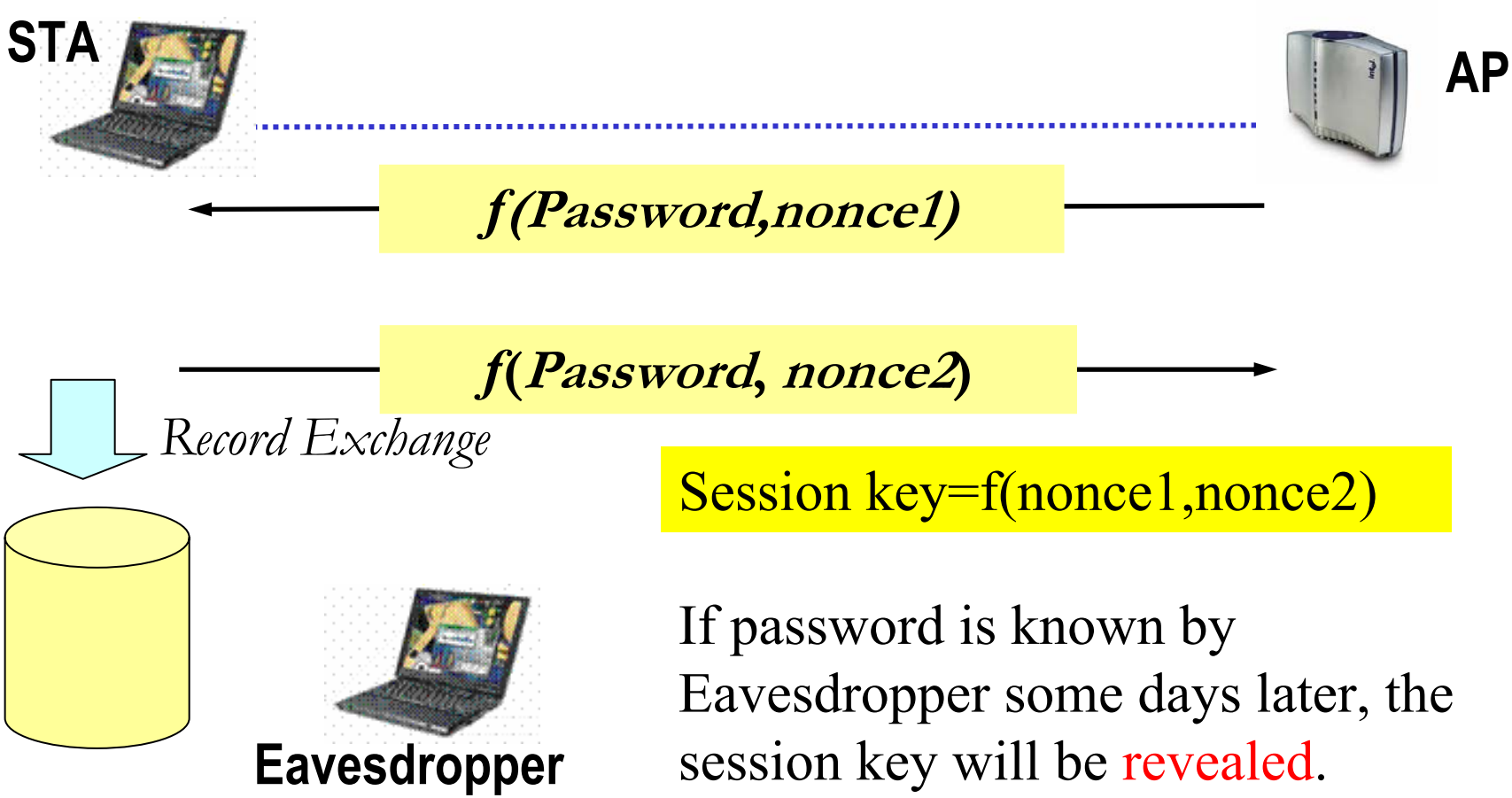


MITM Attacks

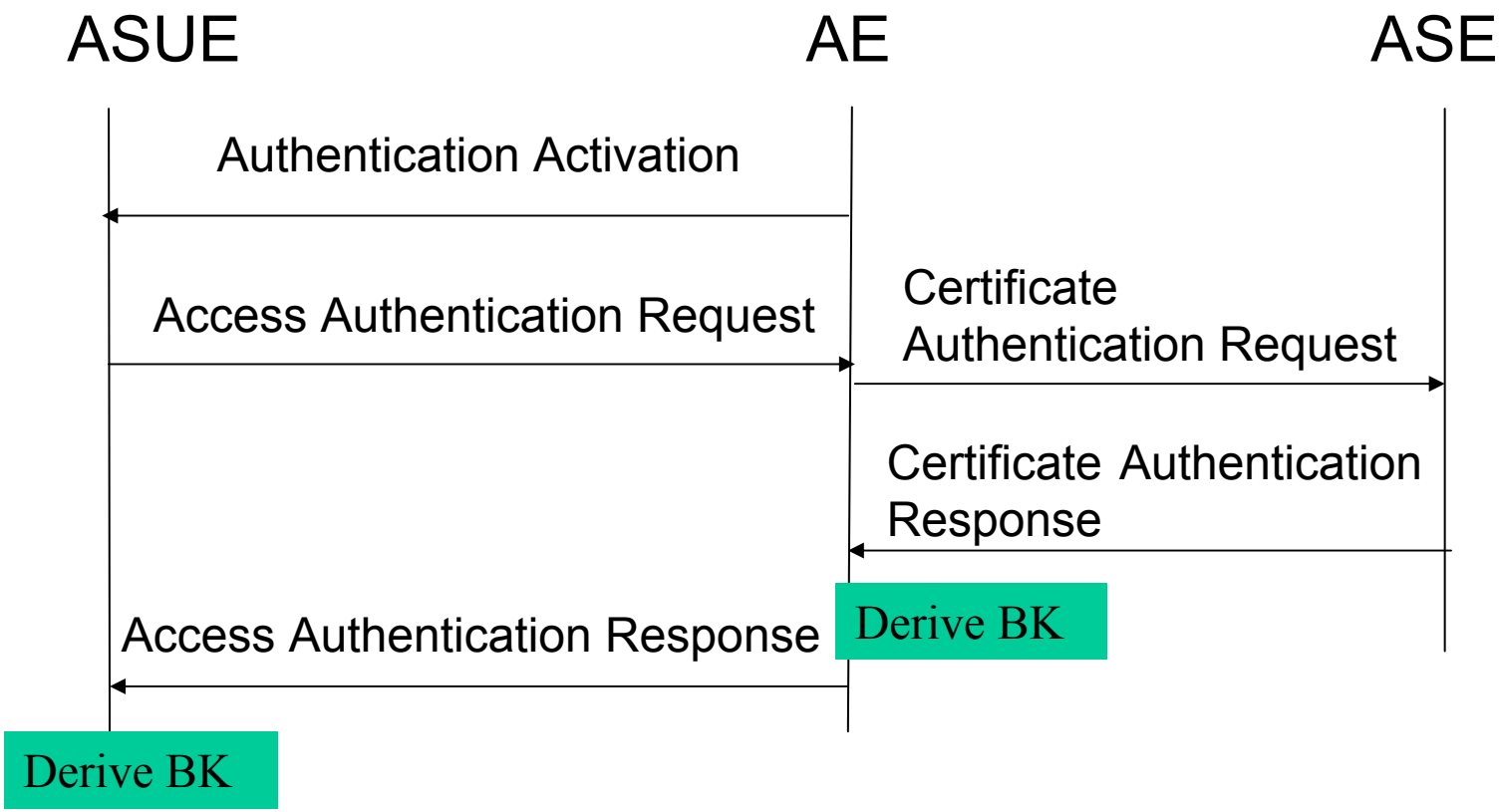
- For STA, Rogue is AP
- For AP, Rogue is STA

- How do we avoid this problem?
  - ✓Authentication with key agreement
  - ✓Mutual authentication

PFS


STA
AP
f(Password,nonce1)
f(Password, nonce2)
Record Exchange
Session key=f(nonce1,nonce2)
Eavesdropper
If password is known by Eavesdropper some days later, the session key will be revealed.

Certificate Authentication



The format of Authentication Activation

FLAG	Authentication Identifier	Local ASU Identity	STA_{AE} Certificate	ECDH Parameter

The format of Access Authentication Request

FLAG	Authentication Identifier	ASUE Challenge	ASUE Key Data	STA_{AE} Identity

STA_{ASUE} Certificate	ECDH Parameter	ASU List trusted by ASUE	ASUE Signature

The format of Certificate Authentication Request

ADDID	AE Challenge	ASUE Challenge	STA_{ASUE} Certificate	STA_{AE} Certificate	ASU List trusted by ASUE

The format of Certificate Authentication Response

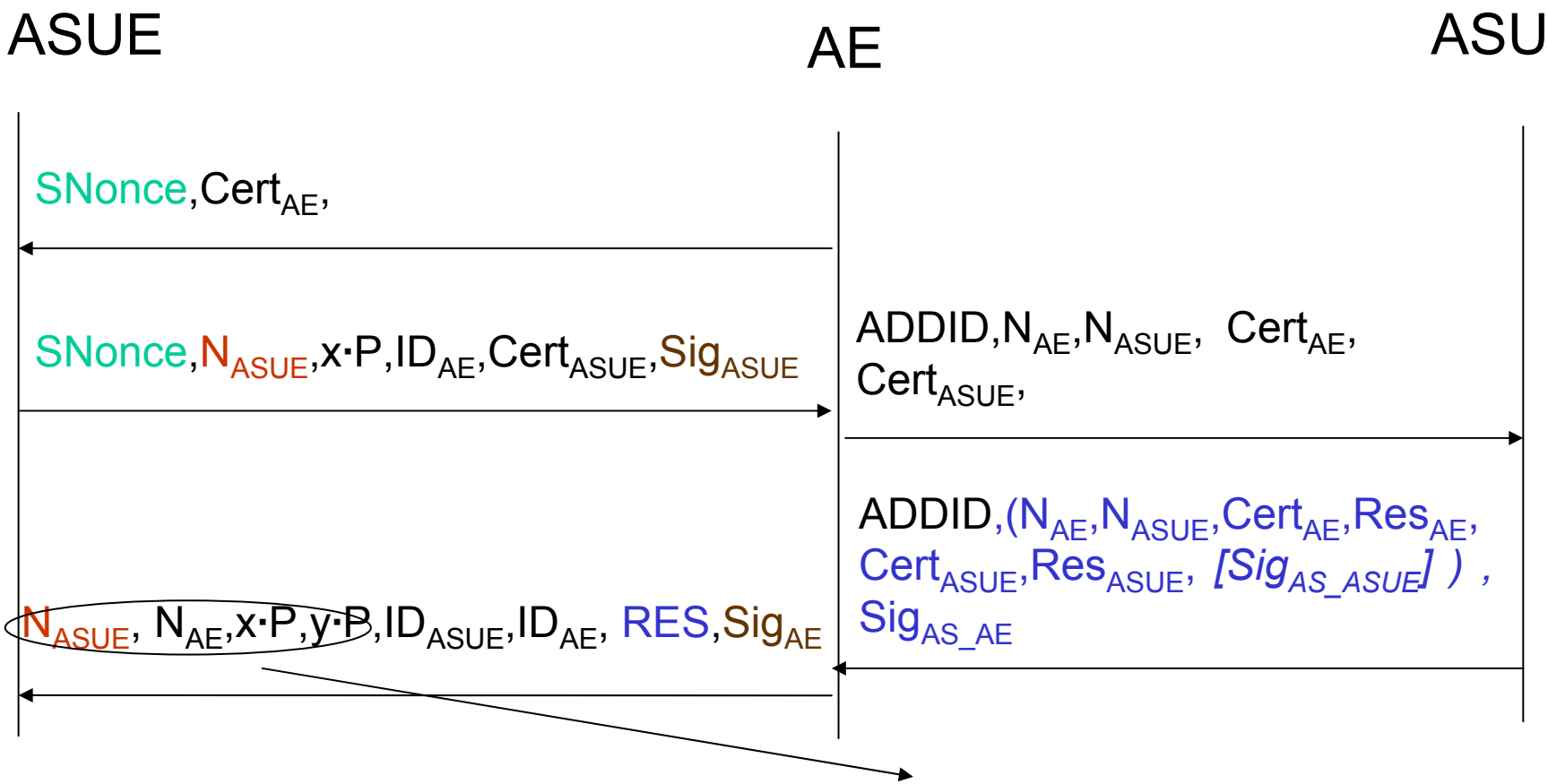
ADDID	Authentication Result of the Certificate	Server Signature trusted by ASUE	Server Signature trusted by AE

The format of Access Authentication Response

FLAG	ASUE Challenge	AE Challenge	Access Result	ASUE Key Data

AE Key Data	STA_{AE} Identity	STA_{ASUE} Identity	Multiple Certificate Verification Result	AE Signature

Certificate Authentication□DH key agreement based on signature



Message 1: Authentication Activation

- The AE sends an authentication activation packet to ASUE when:
  - ✓certificate authentication and key management method is chosen in (re)association
  - ✓ re-authentication and rekeying is required according to the local policy of the AE
  - ✓the AE receives a Pre-authentication Start packet from the ASUE.

Message 1: Authentication Activation

- After the ASUE receives the Authentication Activation packet from the AE,
  - ✓ a) If the value of bit 0 (BK Rekeying Flag) of the flag field in the packet is 1, the ASUE proceeds to Step b). Otherwise, goes to Step c).
  - ✓ b) If the Authentication Identifier of the packet dose not match the one kept in the ASUE which is negotiated in the last Certificate Authentication procedure, the ASUE silently discards the packet. Otherwise the ASUE proceeds to Step c).
  - ✓ c) The ASUE chooses the corresponding STA_{ASUE} certificate according to the ASU Identity in the Authentication Activation packet or local policies. The ASUE generates required parameters and constructs the Access Authentication Request packet and sends it to the AE.

Message 2: Access Authentication Request

- After receiving an Authentication Activation from the AE or when a BK rekeying is needed, the ASUE sends an Access Authentication Request packet to the AE.
- After the AE receives the Access Authentication Request packet from the ASUE,
  - ✓ a) If the AE has not sent an Authentication Activation packet, then it checks whether the Authentication Identification field matches the one negotiated in the last Certificate Authentication procedure. If then, the AE proceeds to Step b). Otherwise the AE silently discards the packet.

Message 2: Access Authentication Request

- ✓ b) In the following cases , the AE silently discards the packet.
  - — the Identification field of STA_{AE} does not match its own Identity,
  - — the ECDH Parameter field dose not match the one in the Authentication Activation packet,
  - — the signature of the ASUE is not valid

  In the following cases, AE constructs the Certificate Authentication Request packet and sent it to the ASU.
  - — AE or ASUE requires to verify the STA_{ASUE} certificate according to its local policy.

  In any other case, the AE proceeds to Step c).

Message 2: Access Authentication Request

- ✓ c) If the STA_{ASUE} certificate is valid, the AE computes values and constructs the Access Authentication Response packet and sent to the ASUE.

  On the other hand, if the STA_{ASUE} certificate is not valid, the AE constructs the Access Authentication Response packet and sent to the ASUE, in which Access State is set to failure. Finally, the AE delinkverifies with STA_{ASUE}.

Message 3: Certificate Authentication Request

- After receiving an Access Authentication Request packet from ASUE and sending a Certificate Authentication Request packet to the ASU.
- After the ASU receives the Certificate Authentication Request packet,
  - ✓ a) The ASU verifies the STA_{AE} certificate and the STA_{ASUE} certificate. If any of the certificate can not be verified, ASU sets the corresponding verification result to 'unknown certificate issuer', and then proceeds to Step b). If both of them can be verified, ASU verifies the state of STA_{AE} certificate and STA_{ASUE} certificate, and then proceeds to Step b).

Message 3: Certificate Authentication Request

- ✓ b) According to the result of the STA_{AE} certificate and STA_{ASUE} certificate verification, the ASU constructs a Certificate Authentication Response packet with the corresponding signature and sends it to the AE.

Message 4: Certificate Authentication Response

- When the ASU receives the Certificate Authentication Request packet, it will send the Certificate Authentication Response packet to the AE.
- After the AE receives the Certificate Authentication Response packet,
  - ✓ a) If the first nonce in the Authentication Result field in the Certificate Authentication Response packet matches the AE Challenge value in the Certificate Authentication Request packet, proceeds to Step b); otherwise, the AE discards this packet.

Message 4: Certificate Authentication Response

- ✓b) The AE verifies the signature with the signature list of its trusting ASU. If the signature is valid, proceeds to Step c). Otherwise, the AE discards this packet.

  On the other hand, if the STA_{ASUE} certificate is not valid, the AE constructs the Access Authentication Response packet and sent to the ASUE, in which Access State is set to failure, Finally, the AE delinkverifies with STA_{ASUE}.

Message 4: Certificate Authentication Response

- ✓ c) If the STA_{ASUE} certificate is valid, the AE generates a 32-octet random number N_{AE} as a challenge of AE, and computes out a 16-octet base key BK and a 32-octet Authentication Identifier used in the next Certificate Authentication procedure is obtained. Finally, the AE constructs the Access Authentication Response packet sent to the ASUE, in which Access State is set to success.

  On the other hand, if the STA_{ASUE} certificate is not valid, the AE constructs the Access Authentication Response packet and sent to the ASUE, in which Access State is set to failure. Finally, the AE delinkverifies with STA_{ASUE}.

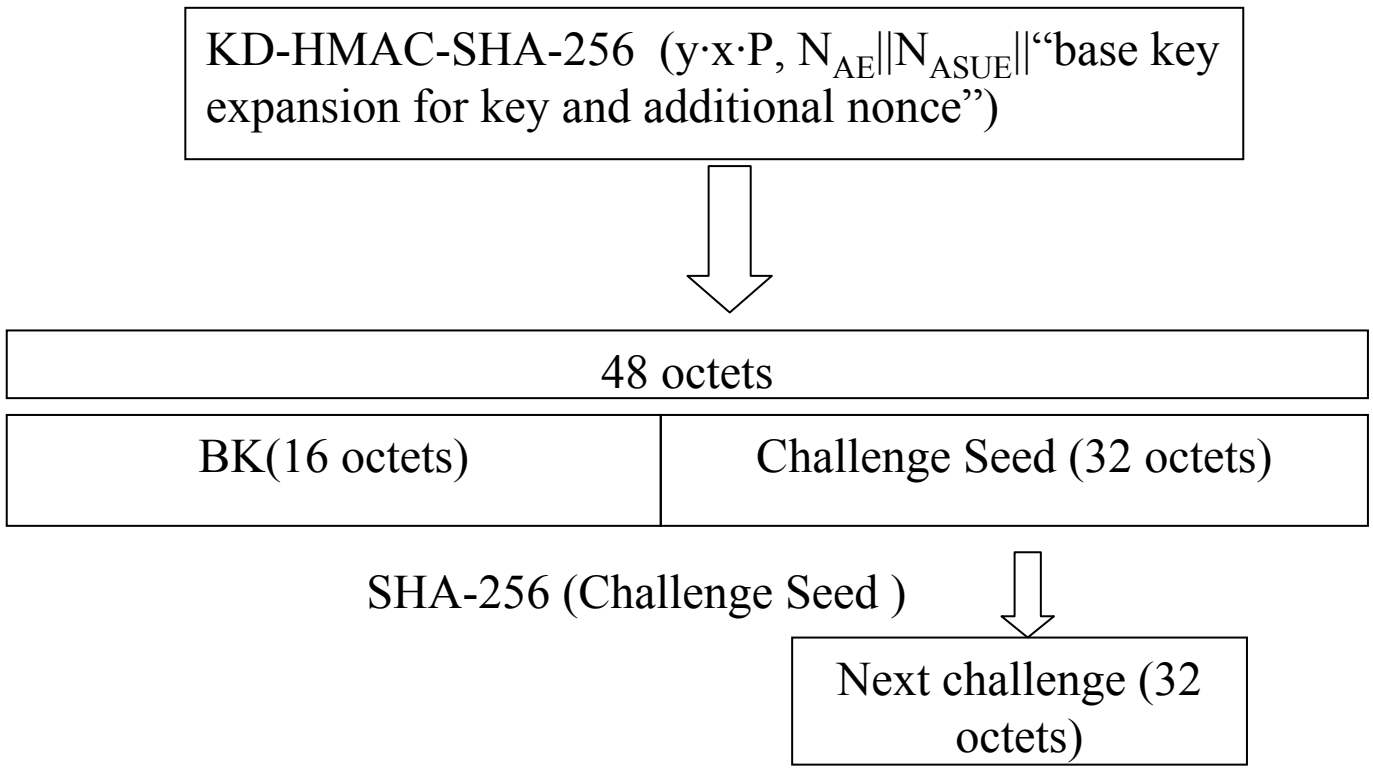
Message 5: Access Authentication Response

- When the AE receives the Certificate Authentication Responding packet or the Access Authentication request packet, it will send the Access Authentication Response packet to ASUE.
- After the ASUE receives the Access Authentication Response packet,
  - ✓ a) If the ASUE conforms that the packet corresponds to the current Access Authentication Requesting packet according to STA_{AE} Identity and STA_{ASUE} Identity, the ASUE proceeds to Step b). Otherwise the ASUE discards the packet.
  - ✓ b) If the bit 0 and bit 1 in the FLAG field match the ones in the Access Authentication Request packet respectively, the ASUE proceeds to Step c). Otherwise the ASUE discards the packet
  - ✓ c) If the ASUE Challenge field and the ASUE Key Data match those in the Access Authentication Request packet respectively, the ASUE proceeds to Step d). Otherwise the ASUE discards the packet.

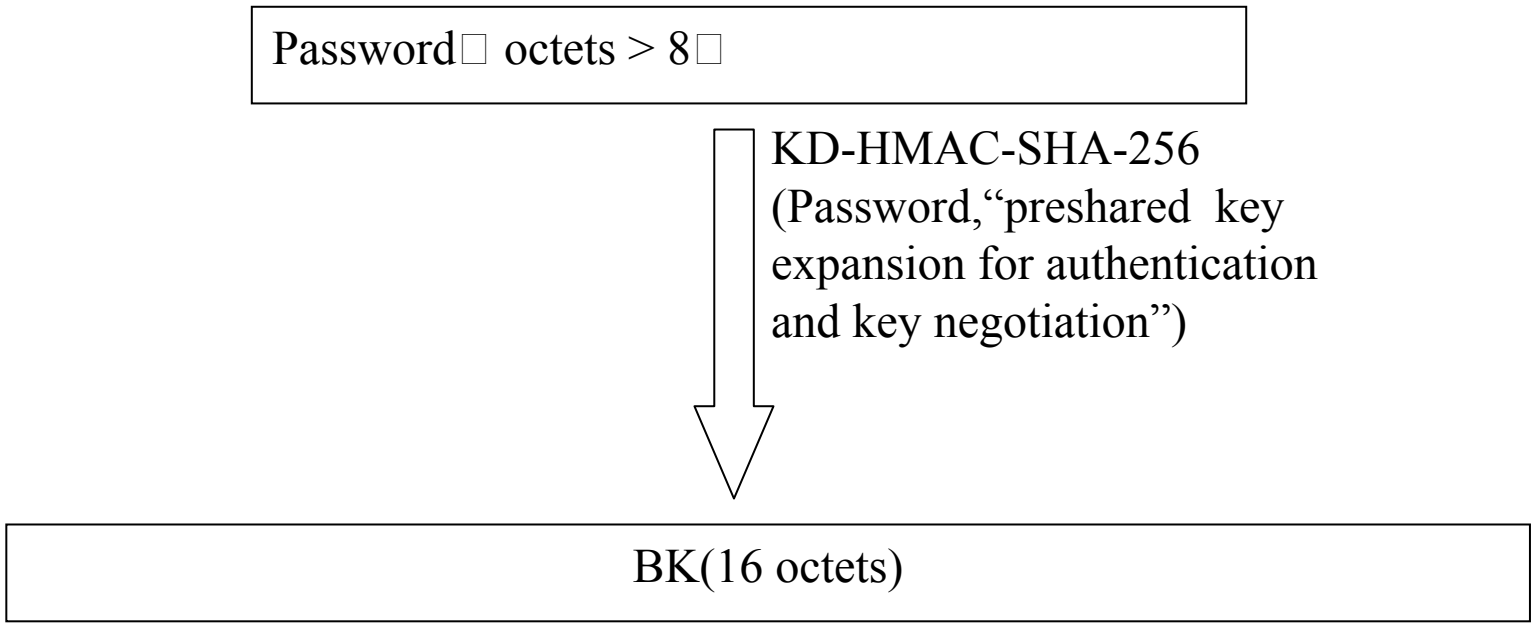
Message 5: Access Authentication Response

- ✓ d) If the ASUE does not require the certificate verification in the Access Authentication Requesting packet, the ASUE proceeds to Step e). Otherwise, the ASUE will verify corresponding signature and Access Result. If they are not valid, the ASUE terminates the linkverification with the STA_{AE}. Otherwise, the ASUE proceeds to Step e).
- ✓ e) The ASUE computes the out a 16-octet base key BK and a 32-octet Authentication Identifier used in the next Certificate Authentication procedure is obtained.

Key Derivation of BK based on Certificate



Key Derivation of BK based on pre-shared key



Unicast Key Negotiation

Given a “good” BK

- Guarantee fresh session key
- rekey with low cost
- Bind session key to the communicating AP and STA
- Protect Discovery and Negotiation from Downgrade attack
- Support the pre-shared key authentication

Unicast Key Negotiation

The format of Unicast Key Negotiation Request

FLAG	BKID	USKID	ADDID	AE Challenge

The format of Unicast Key Negotiation Response

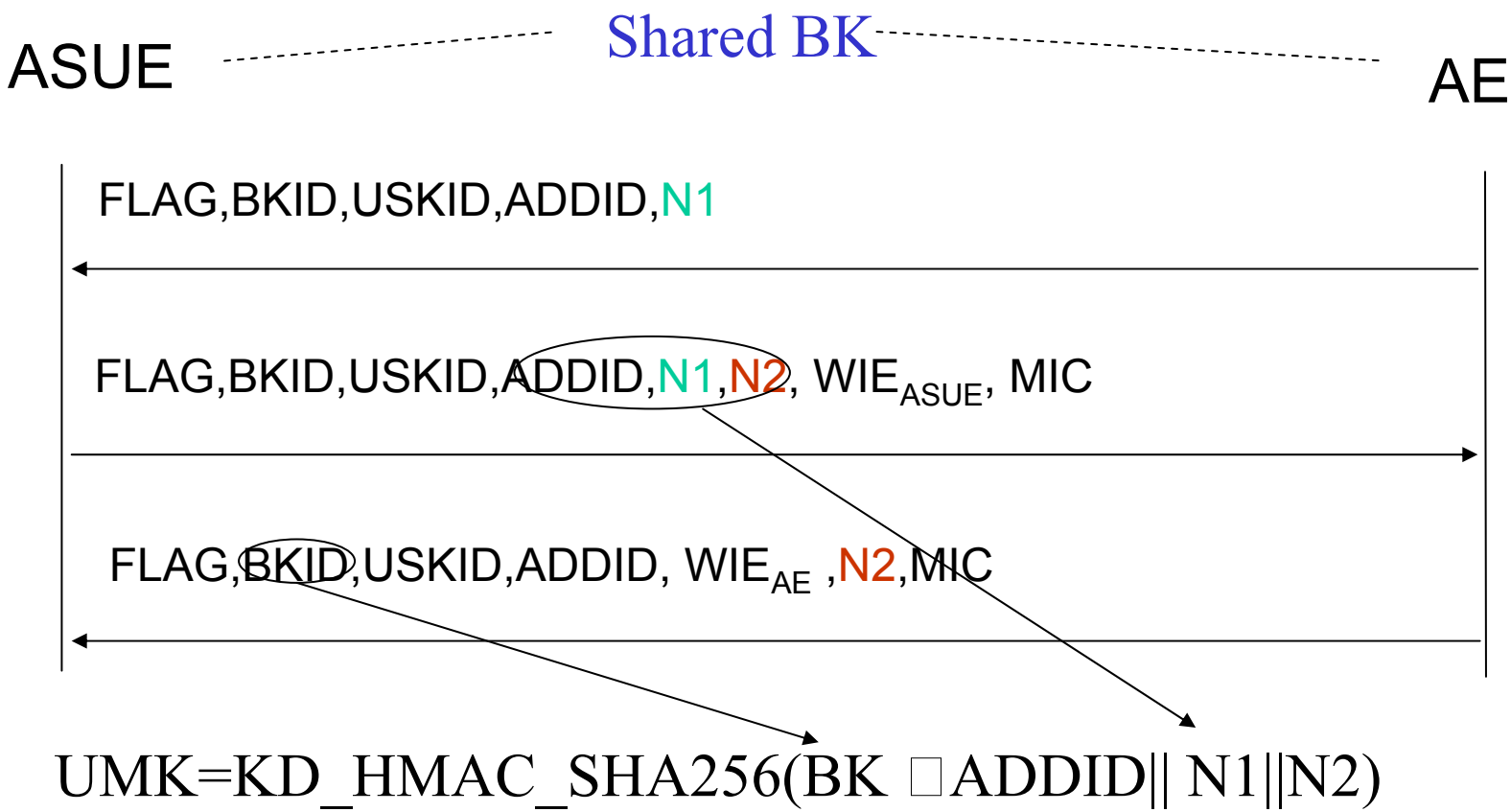
FLAG	BKID	USKID	ADDID

ASUE Challenge	AE Challenge	WIE_{ASUE}	HMAC

The format of Unicast Key Negotiation Confirmation

FLAG	BKID	USKID	ADDID	ASUE Challenge	WIE_{AE}	HMAC

Unicast Key Negotiation



Message 1: Unicast key Request

- The AE will send a unicast key negotiation request packet to ASUE and start the unicast key negotiation with ASUE in the following cases:
  - ✓After the AE completes the certificate authentication procedure and constructs the valid BKSA,
  - ✓using preshared key authentication method,
  - ✓cached BKSA is used,
  - ✓rekeying unicast key.

Message 1: Unicast Key Request

- After the ASUE receives the Unicast Key Negotiation Request packet,
  - ✓ a) If the BKSA referred by BKID is valid and bit 4 of the FLAG field (USK Rekeying Flag) is 1, the ASUE goes to Step c). If BKSA referred by BKID is valid, bit 4 of the FLAG field (USK Rekeying Flag) is 0 and USKSA referred by USKID is not valid, the ASUE proceeds to Step b). Otherwise the ASUE discards the packet.
  - ✓ b) If the AE Challenge is equal to the one negotiated in the last Unicast Key Negotiation procedure, the ASUE proceeds to Step c). Otherwise the ASUE discards the packet.

Message 1: Unicast Key Request

- ✓ c) The ASUE generates a random number as the ASUE challenge. Then the ASUE compute out the unicast session key which including the unicast encryption key, the unicast integrity check key, protocol integrity key, and key encryption key and a 32-octet AE Challenge used in the next unicast session key negotiation procedure.

Message 1: Unicast Key Request

- ✓ d) The ASUE calculates the message authentication code by the HMAC_SHA256 algorithm and constructs the Unicast Key Negotiation Response packet to send to the AE.
- ✓ e) The ASUE will install the new unicast session key when it is in BSS. When the ASUE is in IBSS, it will install the new unicast session key only if its MAC address is less than the AE's MAC address.

Message 2: Unicast Key Response

- When the ASUE rekeys, or receives the Unicast Key Negotiation Request, the ASUE sends the Unicast Key Negotiation Response packet to the AE.
- After the AE receives the Unicast Key Negotiation Response packet,
  - ✓ a) If the bit 4 (USK Rekeying Flag) of the FLAG field is 1, the AE proceeds to Step b); otherwise the AE goes to Step c).
  - ✓ b) If there is a valid USKSA and the USKSA referred by USKID in the packet is invalid, the AE proceeds to Step c); otherwise the AE discards the packet.
  - ✓ c) If the AE Challenge is correct, the AE proceeds to Step d). Otherwise the AE discards the packet.

Message 2: Unicast Key Response

- ✓ d) The AE compute out the unicast session key which including the unicast encryption key, the unicast integrity check key, protocol integrity key, and key encryption key and a 32-octet AE Challenge used in the next unicast session key negotiation procedure. The AE calculates the HMAC locally by the HMAC_SHA256 algorithm. If the calculated HMAC matches the HMAC that included in the packet, the AE proceeds to Step e); otherwise the AE discards the packet.

Message 2: Unicast Key Response

- ✓ e) the WIE_{ASUE} is verified, if not correct, the AE delinkverifies with STA_{ASUE}.
- ✓ f) The AE calculates HMAC locally by the HMAC_SHA256 algorithm, and sends the Unicast Key Negotiation Confirmation packet to the ASUE.
- ✓ g) The AE will install the new unicast session key when it is in BSS. When the AE is in IBSS, it will install the new unicast session key only if its MAC address is greater than the ASUE's MAC address.

Message 3: Unicast Key Confirmation

- After the AE receives the Unicast Key Response packet, it will send the Unicast Key Negotiation Confirmation packet to the ASUE.
- After the ASUE receives the Unicast Key Negotiation Response packet
  - ✓ a) If the ASUE challenge is equal to the value in the Unicast Key Negotiation Response packet, the ASUE proceeds to Step b). Otherwise the ASUE discards the packet.
  - ✓ b) The ASUE calculates the HMAC locally by the HMAC_SHA256 algorithm. If the calculated HMAC matches the HMAC that included in the packet, the ASUE proceeds to Step c); otherwise the ASUE discards the packet.

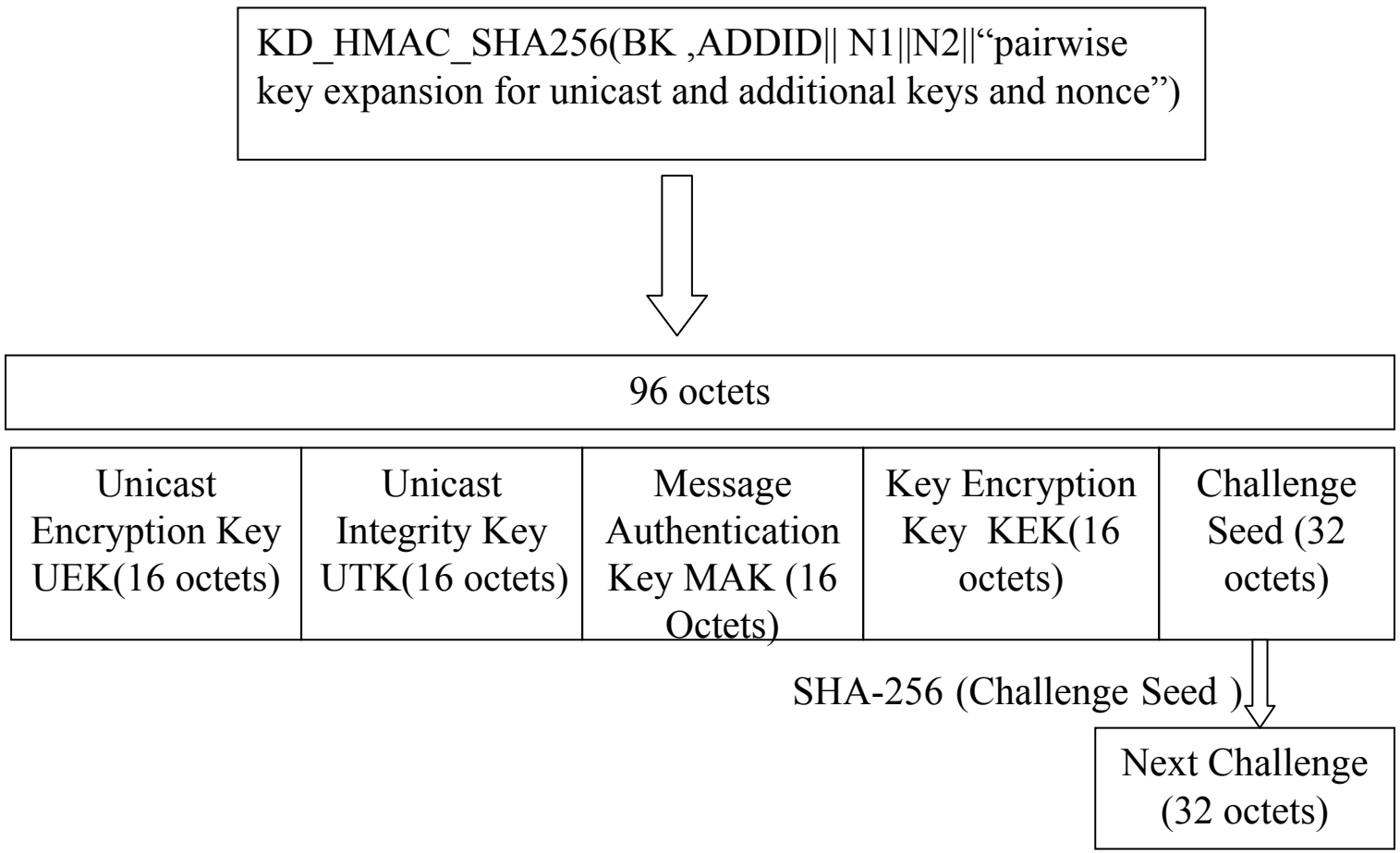
Message 3: Unicast Key Confirmation

- ✓ c) if the WIE_{AE} field is equal to the WAPI parameter set in the received Beacon and Probe Response frame, the ASUE proceeds to Step d); otherwise the ASUE delinkverifies with the STA_{AE}.
- ✓ d) The sent unicast data frame will be encapsulated with the new key. For unicast rekeying, the old key should be deleted.

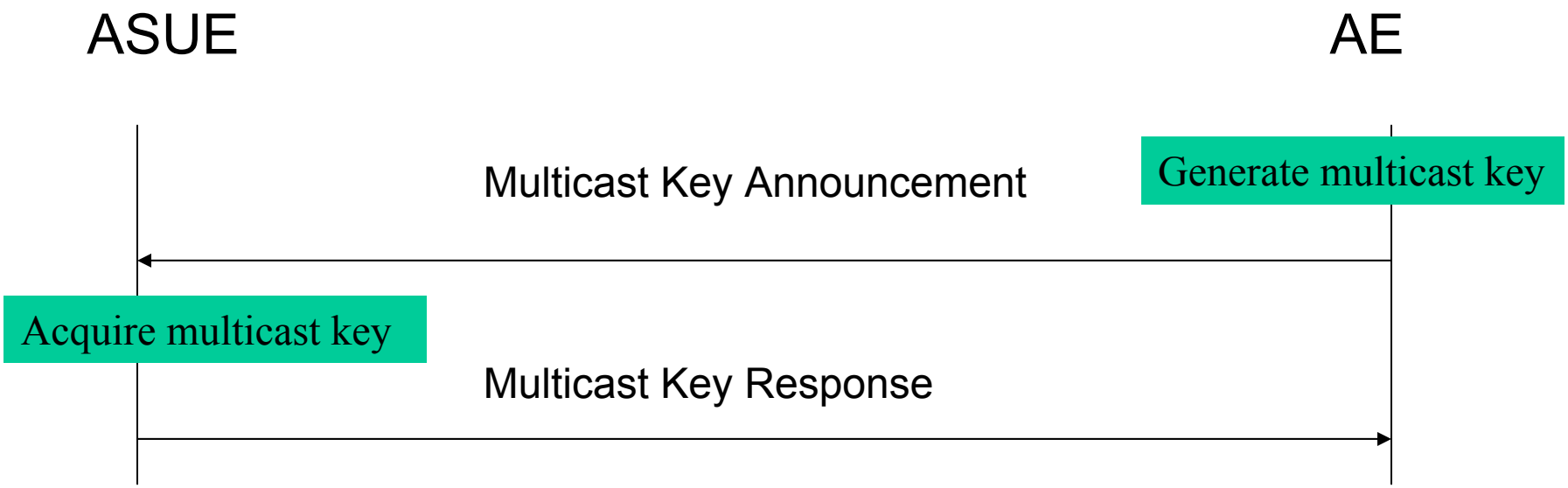
Unicast Key discussion

- It is a key agreement protocol based on shared key.
- Its another function is to verify the WAPI parameter set in order to prevent from the downgrade attacks.
- As mentioned before, this procedure also negotiate unicast cipher suite and unicast keys in IBSS network.
- The random number N1 and N2 is overloaded for key separation and message freshness.

Key Derivation of Unicast Key



Multicast Key Announcement



The format of Multicast Key Announcement

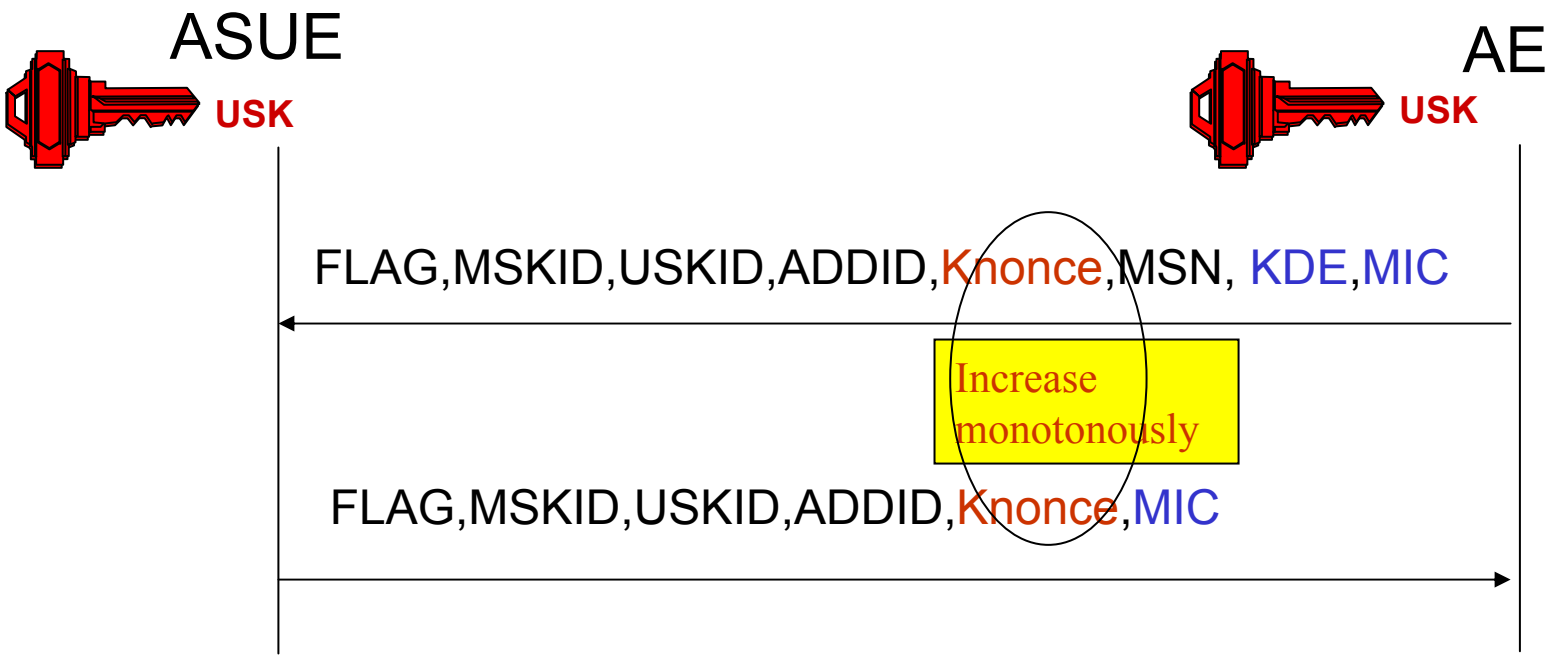
FLAG	MSKID/STAKeyID	USKID	ADDID

Data packet number	Key Announcement Identifier	Key Data	Message Authentication Code

The format of Unicast Key Negotiation Confirmation

FLAG	MSKID/ STAKeyID	USKID	ADDID	Key Announcement Identifier	Message Authentication Code

Multicast Key Announcement



Message 1: Multicast Key Announcement

- After the success of the unicast key negotiation, or when AE needs to update the multicast key, or when AE receives the STAKey request packet, AE should send ASUE the multicast key / STAKey announcement packet to announce the multicast /STAKey master key.

Message 1: Multicast Key Announcement

- After the ASUE receives the multicast key / STAKey announcement packet sent by AE it does as follows:
  - ✓ If ASUE does not support or not permit STAKey, then when bit 5 of the FLAG field (STAKey negotiation flag) is 1, this packet is discarded.

    ASUE uses the message authentication key identified by USKID field to calculate a check value, and compares it with the Message Authentication Code field value. If they are equal, goes to b). Otherwise, this packet is discarded.
  - ✓ b) Checks whether the value of the Key Announcement Identifier field value increases monotonically. If then, goes to c); otherwise, this packet is discarded.

Message 1: Multicast Key Announcement

- ✓ c) Gets a 16-octet announcement master key by decrypting the key data. Then, the ASUE uses the master key to generate a 32-octet session key.
- ✓ d) Saves the value of the Key Announcement Identifier field, then constructs the multicast key / STAKey response packet and sends it to AE.

Message 1: Multicast Key Announcement

- ✓ e) Installs or deletes the key.

If this procedure is the multicast key announcement procedure, the new MSK will be installed to receive the multicast data frame.

If this procedure is the STAKey announcement procedure, the initiator/peer will install the new key to send/receive the STA-to-STA data frame.

If this procedure is the STAKey deletion procedure, the peer will delete the corresponding STAKey.

Message 2: Multicast Key Response

- After the AE receives the multicast key response packet sent by ASUE, it does as follows:
  - ✓ a) Uses the message authentication key identified by the USKID field to calculate the check value, and then compares it with the value of the Message Authentication Code field. If they are equal, goes to b). Otherwise, discards the packet.
  - ✓ b) Compares the FLAG field, the MSKID/STAKeyID field, the USKID field, the ADDID field and the Key Announcement Identifier field with those in the multicast key/STAKey announcement packet, respectively. If every field is equal to the corresponding field in the announcement packet, then the multicast key/STAKey announcement process is successful. Otherwise,AE discards this packet.

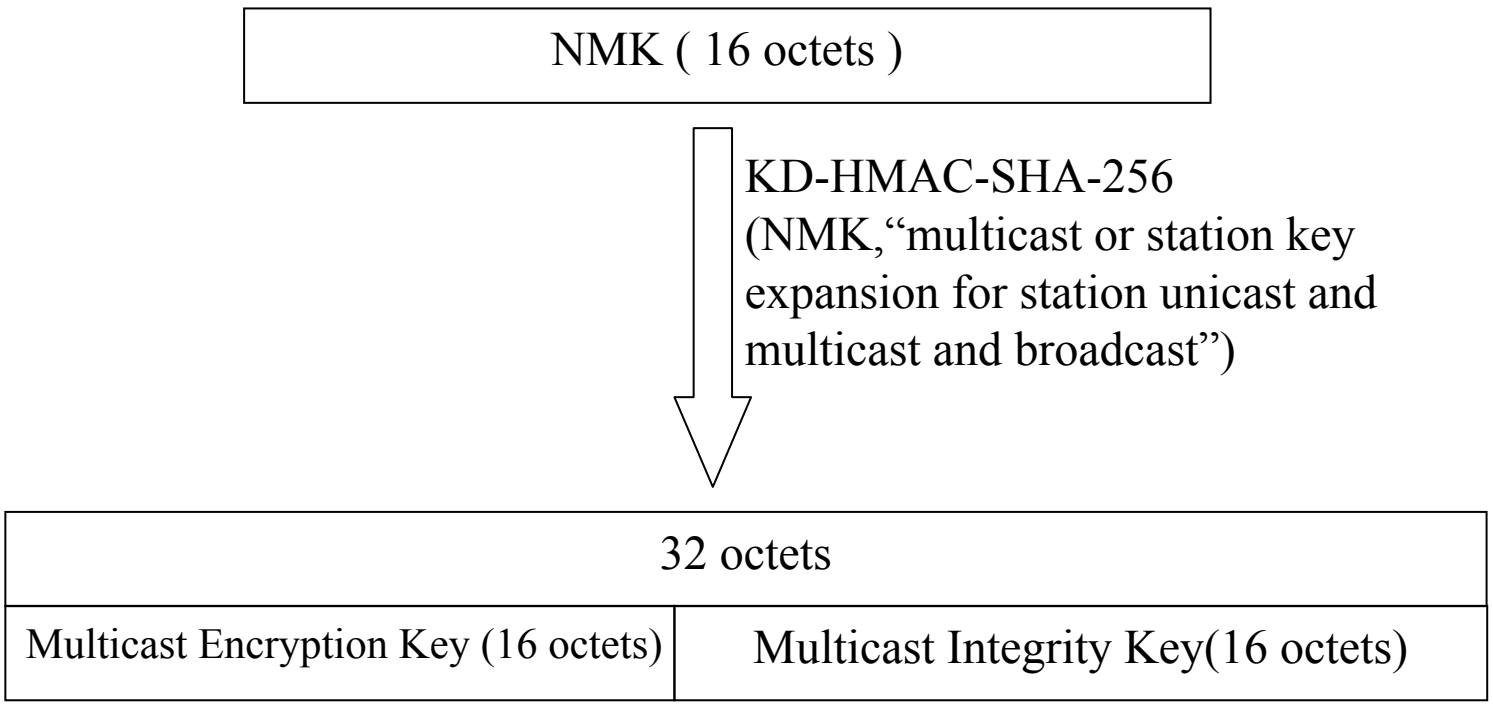
Message 2: Multicast Key Response

- ✓ c) Installs the new key when announcing successfully.

If this procedure is the multicast key announcing procedure, the AE will send multicast data frame encrypted with the new key.

If this procedure is for the STAKey initiator, the AE will relay the STA-to-STA data frame from initiator to the peer transparently without encrypting and decrypting them.

Key Derivation of Multicast Key



Other Features

- Support Station to Station key
  - ✓ When STA1 send data to STA2 in the same BSS, STA1 can establish a STAKey with STA2 to encrypt the unicast data from STA1 to STA2. The cipher algorithm used is multicast cipher suit.The AP dose not encrypt or decrypt the data from STA1 to STA2.
- Support BK, unicast key and multicast key rekeying
- Support pre-authentication

WAI Summary

- WAI is based on peer port control mechanism
- WAI design assumes authentication function blocks data traffic
- WAI executes Unicast Key Negotiation when BK becomes available
- WAI assumes authentication function unblocks data traffic after Multicast Key Announcement completes
- The uncontrolled port keeps on when rekeying
- WAI addresses known WEP problems

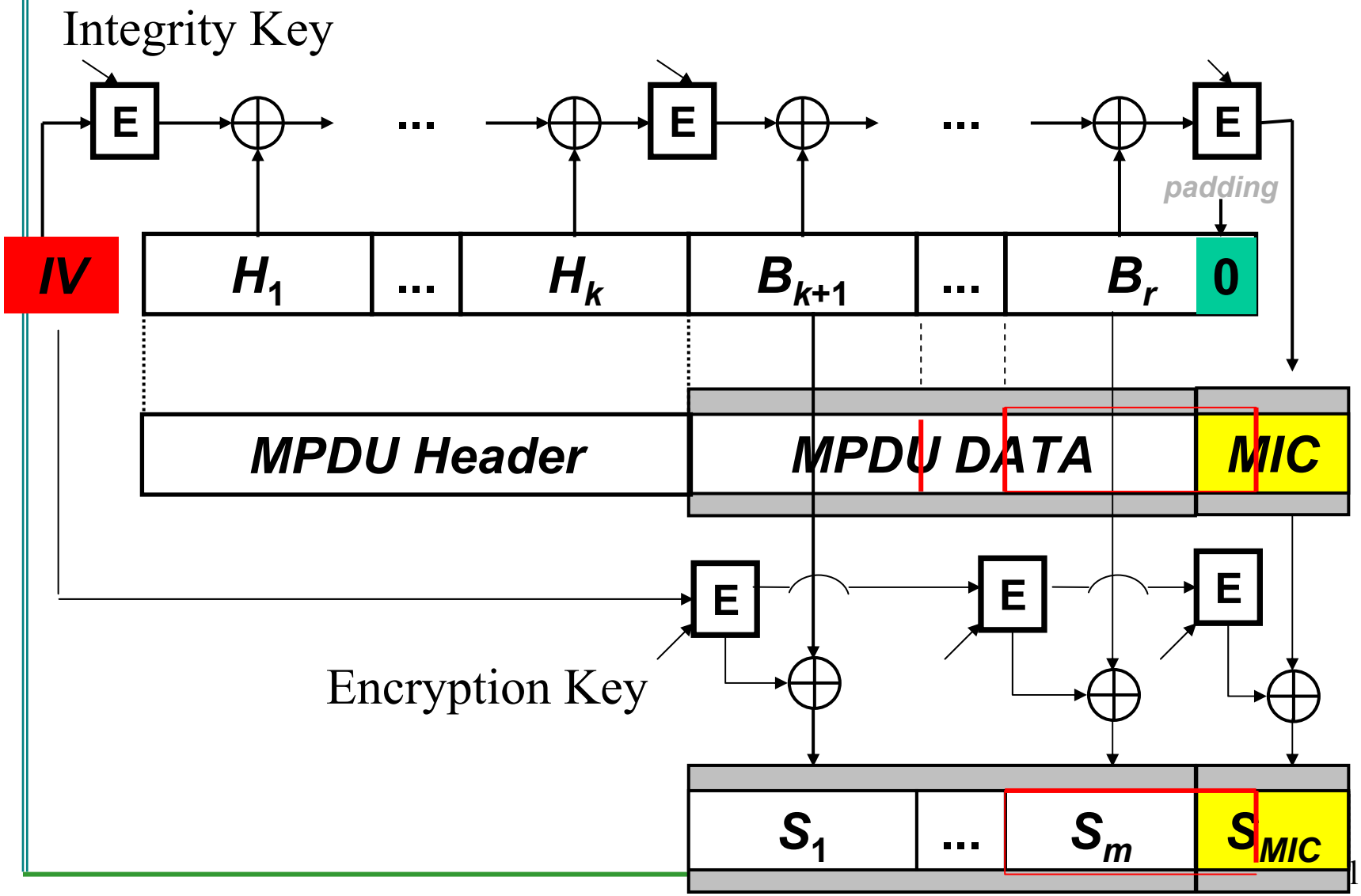
WPI

- WPI：WLAN Privacy Infrastructure
- Security goal：Address all known WEP problems
  - ✓Prevent Frame Forgeries
  - ✓Prevent Replay
  - ✓Correct WEP's misuse of encryption
  - ✓Never reuse keys

Mode in WPI

- CBC-MAC for data integrity, OFB mode for data confidentiality, with separate key
- WPI requires a block cipher with 128 bits block

WPI Mode


Integrity Key
E
...
E
...
E
padding
IV
H_1
...
H_k
B_{k+1}
...
B_r
0
MPDU Header
MPDU DATA
MIC
E
E
E
Encryption Key
S_1
...
S_m
S_{MIC}

WPI MPDU Format

PN Usage

- For each rekeying of unicast key
  - ✓ ASUE: PN=0x5C365C365C365C365C365C365C365C36
  - ✓ AE: PN=0x5C365C365C365C365C365C365C365C37
  - ✓ ASUE and AE will add 2 to the PN before encapsulate the unicast data frame.
- For each rekeying of multicast key
  - ✓ AE: PN= 0x5C365C365C365C365C365C365C365C36
  - ✓ AE will add 1 to the PN before encapsulate the multicast data frame.
- For each establishment of STAKey
  - ✓ Initiator: PN=0x5C365C365C365C365C365C365C365C36
  - ✓ The initiator will add 1 to the PN before encapsulate the unicast data frame to the peer.

WPI Summary

- Adopts general mode OFB,CBC-MAC then the security can be guaranteed.
- MIC is 128 bits, enough long
- For the same session key, IV is not reuse. Then the key stream dose not repeat.
- Prevent the replay attack by monotonously increased PN.

Part 3
Summary

Summary

- WAPI addresses all known WEP problems
- WAPI is based on peer port control mechanism
- WAPI defines two authentication and key management methods and supports extending to permit the additional new methods
- WAPI is adaptable to multiple deployment models
- WAPI is extensible to other security mechanisms(e.g. coexist with IEEE802.11i through IE)

WAPI is a mature and feasible technology

- The technology accumulation on WAPI is more than 12 years
- WAPI resolves all known WEP problems
- More than forty companies and institutes have been taking part in the WAPI process, including Chinese national standard and international standard proposal.
- WAPI has been issued and published in 2003, and there are many WAPI-compliant equipments in the market.

WAPI is the known best security mechanism in WLAN so far

- **WAPI resolves all known WEP problems**
- **WAPI is based on peer port control mechanism**
- **WAPI possesses better security and performance than the other security mechanisms, including IEEE 802.11i**

WAPI is China's Mandatory National Standard

- **WAPI standard project was approved in 2001**
- **WAPI became China's mandatory national standard in May, 2003 by AQSIQ (General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China)**

WAPI's industry chain has become mature

- **Special Test Organizations Has Been Founded**

  -- Test□State Radio Monitoring Center

  -- Certification□China Quality Certification center

  China Electromagnetism compatibility Center

  China Electronics standardization Institute

- **The Products of Many Companies in China Have Passed the Corresponding Test and been Applied in the Marketplace**

  -- Founder□Lenovo□IWNCOMM□Shenzhen minghua company, etc.

- **WAPI Chip**

  -- **BeiJing LHWT Company, Beijing HED, IWNCOMM**

  Huawei Technology, ZTE Corporation

  Xian Jiaotong University, etc.

Integrated Industrial Chain Has Been Established in China

WAPI has been implemented widely in China

- **Many WAPI-compliant equipments has entered into consumer market, including Wireless adapter, Access point, and Authentication server**
- **Some chip manufacturer can provide WAPI compliant chip**
- **WAPI-compliant equipments have been applied in many places**
  - **-- Many companies and industry application**
  - **-- large football games, such as Real Madrid versus China Dragon team**
  - **-- preparing for Olympic games coverage**
  - **-- … …**

WAPI has wide application beyond WLAN

- **WAPI can take WLAN industry out of the security marsh**
- **WAPI provides security IP network access**
- **WAPI technology can also be used in other fields, such as WMAN, WPAN, etc.**
- **Some company begin to develop WAPI compliant products of WMAN.**

WAPI has 1.3 billion people consumer base

- WAPI has been adopted and implemented in China
- China has a population of over 1.3 billion people
- The market in China is open to the companies from different countries and regions.

WAPI became standard one year earlier than 11i

- **WAPI has became Chinese National standard since May, 2003.**
- **IEEE 802.11i became the published standard in June, 2004.**
- **It is earlier that WAPI become standard than IEEE 802.11i.**

WAPI was submitted to ISO earlier than 11i

- **In May 2004, Chinese NB voted "negative" on ISO/IEC DIS 8802.11, because the document still adapt WEP as the security mechanism. It is numbered "6N12687".**
- **In July 2004, Chinese NB submitted WAPI proposal to JTC1 & SC6, and it is numbered "1N7506"**
- **In Sep. 2004, UK NB submitted IEEE 802.11i to JTC1, and it is numbered "1N7537".**
- **It is earlier that WAPI was submitted to international standard organization than IEEE 802.11i.**

WAPI provide technologies which is urgently needed by the international community

- WEP has many well-known security problems, and it has been the obstacles to the development of international WLAN industry
- With the development of WLAN, the security problem would be even serious and destructive
- WAPI is feasible and mature
- China NB has the responsibility to provide urgently needed technology

WAPI is a contribution of Chinese NB to international community

- **WAPI has been adopted and implemented in China more than one year before it was submitted to ISO/IEC, and it is fully feasible**
- **WAPI is a contribution of Chinese NB to international community**
- **China NB is eager to advance the industry development both in China and in other countries with advanced technology**

WAPI is a sign of Chinese NB's duty as a member of ISO/IEC

- China is JTC1 P-member and SC6 P-member
- China has adopted many international standards in different fields
- China has submitted some proposals to ISO/IEC
- Some proposals have became international standards
- Chinese NB regards WAPI as the sign of Chinese NB's duty as a member of ISO/IEC
- Chinese NB has the right and responsibility to proceed WAPI into international standard in ISO/IEC

WAPI fully satisfied with ISO/IEC requirements for international standardization

- **The process of submitting WAPI fully complies with ISO/IEC directives**
- **WAPI accords with requirements for international standardization**
- **As a P-member, China has right to submit WAPI to ISO/IEC directly and proceed WAPI within ISO/IEC frame**

WAPI has been modified to help reach objective set by Geneva meeting

- Geneva resolution specifies that the objective of Beijing meeting is "develop a single technical solution acceptable to all parties"
- WAPI has been modified to make it coexist with IEEE 802.11i
- It shows Chinese NB's great efforts to reach objective set by Geneva meeting

WAPI has been modified to preserve ISO/IEC consensus tradition

- **WAPI has been submitted to ISO/IEC firstly, and it was the only proposal when submitted**
- **Chinese NB has received some comments on WAPI**
- **To be international standard, WAPI should get consensus; So WAPI is modified to adequately take comments into account**
- **The action of Chinese NB shows that Chinese NB tries best to preserve ISO/IEC consensus tradition**

Conclusion

WAPI deserves to become an international standard!

Thanks