Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Security Context Transfer for Handoffs**
Date Submitted	**2005-09-13**

Source(s)	Mi-Young Yun	myyun@etri.re.kr
	Jung Mo Moon, PhD	jmmoon@etri.re.kr
	Jaesun Cha	jscha@etri.re.kr
	Sang Ho Lee, PhD	leesh@etri.re.kr
	ETRI	
	161, Gajeong-dong,Yuseong-gu,	Voice: 82-42-860-4821
	Daejeon, 305-700, Korea	Fax: 82-42-861-1966

Re:	Contribution on comments to IEEE 802.16g-05/008

Abstract	We define context transfer primitives for security information through the NCMS entity and describe the security information needed by a target BS. This proposal makes it possible to perform the authentication after handoffs as specified in the remainder of this document.

Purpose	Adoption

Security Context Transfer for Handoffs

Mi Young Yun, Jung Mo Moon, Jaesun Cha and Sang Ho Lee

ETRI

1. Problem Statement

The purpose of this contribution is to describe the security context for handoff in the EAP authentication only and define primitives that could be exchanged between the BS and the NCMS entities.

After handover procedure is done, the network re-entry is processed as described in [1]. For the fast handoff, a target BS needs to have an MS information served in a previous serving BS. Section 14.5.9.1.1 describes the handover context which is shared between the serving BS and the target BS for re-establishment of MS connections. However, it does not provide some specific attributes that need to be shared between the serving BS and target BS according the handover optimization.. In this contribution, we focus on the security information which is a set of parameters related to a security key which gives a way to secure communication. This information should be handled carefully and securely, so it has to be transmitted not to all candidate target BS. but to a real target BS only.

In this contribution, we define context transfer primitives for security information through the NCMS entity and describe the security information needed by a target BS. This proposal makes it possible to perform the authentication after handoffs as specified in the remainder of this document.

2. Summary of the Proposed Remedy

The security information needs to be transferred only to the actual target BS not to the all candidate target BSs. The decision to choose a target BS which an MS moves to is made in a MOB_HO-IND message.

The security information which could be required in a target BS is as follows.

- ~~PMK~~ AK context
    - ■ AK ~~PMK or MSK~~
    - ■ AK ~~PMK~~ sequence number
- TEK context
    - ■ TEK
    - ■ TEK key lifetime
    - ■ TEK sequence number
    - ■ CBC Initialize Vector
    - ■ SAID
- GTEK context
    - ■ GKEK
    - ■ GKEK lifetime
    - ■ GKEKKID
- SA descriptor

- SAID
- SA-type
- SA service type
- Cryptographic-Suite

The ~~PMK (or the MSK)~~AK which is the product of EAP exchanges could be managed at the authentication related node such as an AAA server, but the TEK and the GTEK are created and applied in a BS only. The HO process optimization TLV gives information about re-entry process management messages that may be omitted during the handover. Both TEK and GTEK could be transmitted to the target BS or not according to the HO process optimization TLV settings.

Many of scenarios are possible in order to transmit the security information according to which node provides it and which key information should be transferred.
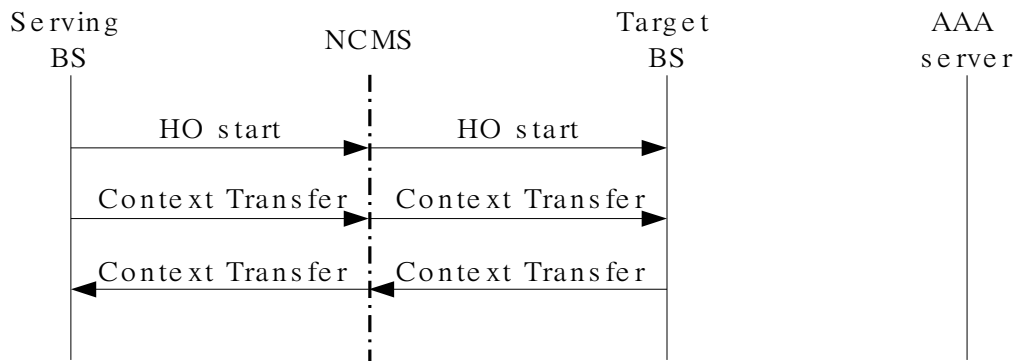We give three examples which could be occurred.

Figure 1. The security information provided by the serving BS
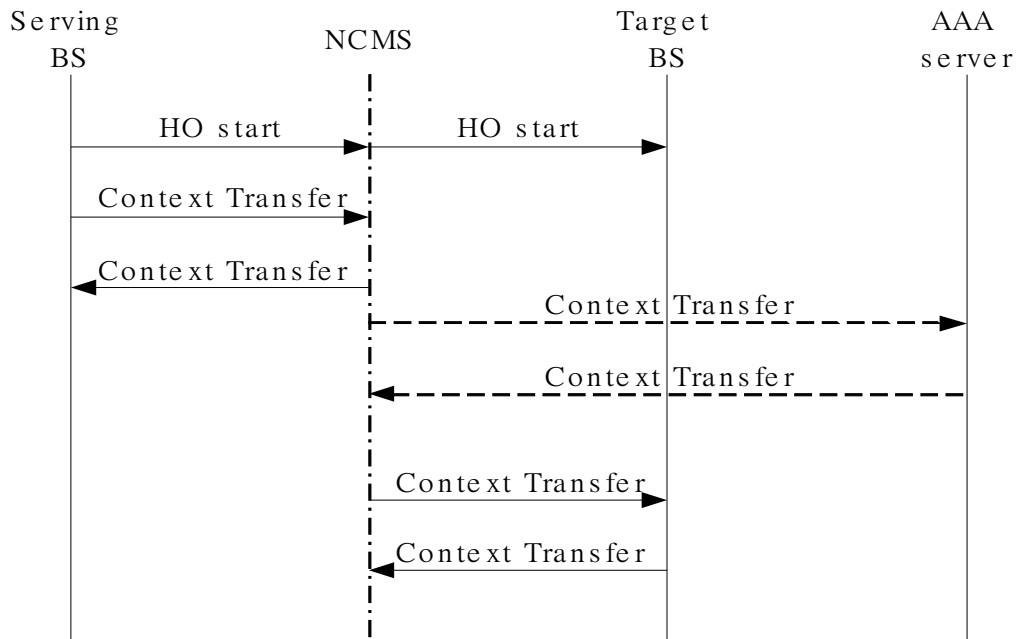
Figure 2. The security information provided by an AAA server
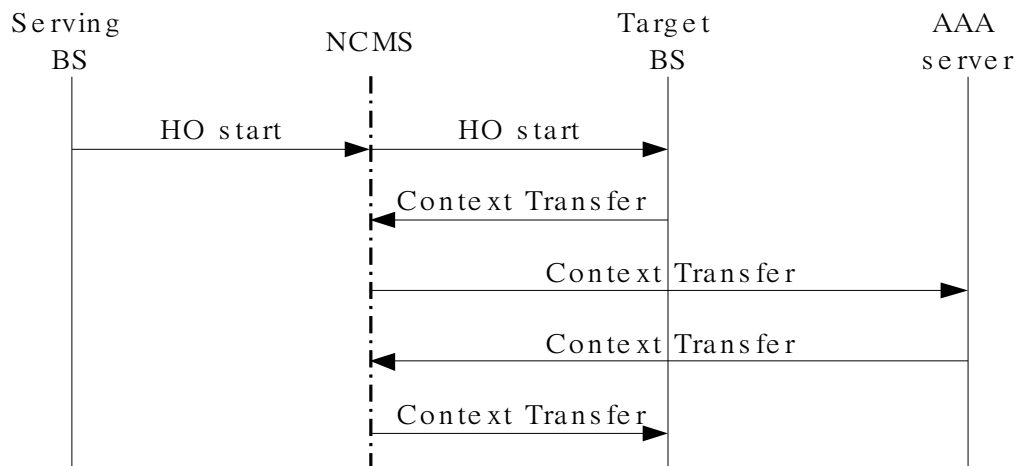
Figure 3. The security information requested by a target BS

In this contribution, we define 4 primitives to support security context transfer for handoffs between the BS and the access network (NCMS) which could be applied to various security context transfer scenarios.

Primitive	Direction	Primitive Contents
Context Transfer.indication	BS <-> NCMS	Serving BS ID, Target BS ID, MS ID, Security Information
Context Transfer.confirmation	BS <-> NCMS	Serving BS ID, Target BS ID, MS ID, Result Code
Context Transfer.request	BS <-> NCMS	Serving BS ID, Target BS ID, MS ID
Context Transfer.response	BS <-> NCMS	Serving BS ID, Target BS ID, MS ID, Security Information, Result Code

The main purpose of this contribution is to make the sharing of the security information between the serving BS and the target BS possible regardless of the aforementioned sharing scenarios by providing the above primitives. The type and the order of the messages exchanged through backbone network is not our concern.

3. Proposed Text Changes

14.5.5 Security Management

[*Insert section 14.5.5.4 as follow*]
14.5.5.4 Security for Handoffs (EAP only)

In the handover procedure, if an MS tries to process the network re-entry to a target BS, but the target BS has not an MS information, then the target BS may request the MS information to a serving BS and the serving BS may give a response of it.
Figure 1 shows the context transfer primitives initiated by a serving BS between a BS and an NCMS entity.

Figure 1. Context transfer primitives initiated by a serving BS

If an MS tries to process the network re-entry to a target BS, but the target BS has not an MS information, then the target BS may request the MS information to a serving BS and the serving BS may give a response of it. Figure 2 shows the context transfer procedure initiated by a target BS between a BS and an NCMS entity as follows
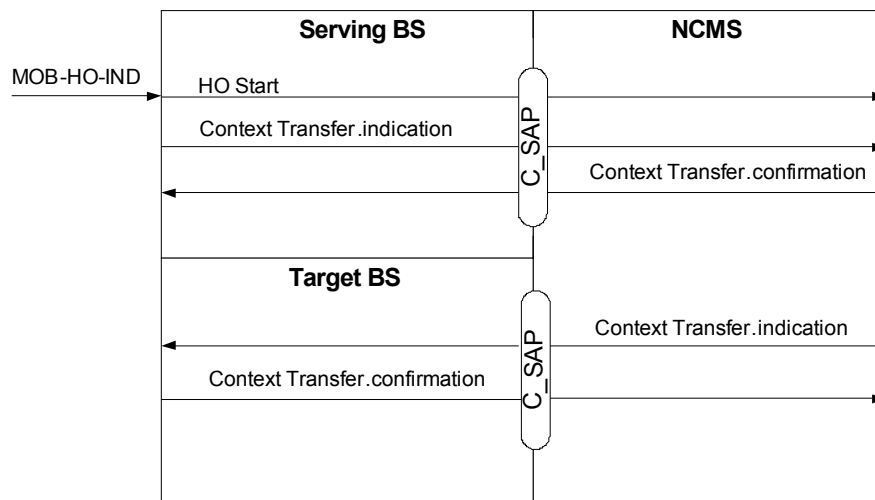
Figure 2. Context transfer primitives initiated by a target BS

14.5.5.4.1 Service Primitives

14.5.5.4.1.1Context Transfer.indication

14.5.5.4.1.1.1 Function
This primitives is issued by the serving BS or the NCMS entity in order to give the target BS the security context information of the MS. It is transmitted only to the real target after the handover procedure. The MS information what they have could be included.

14.5.5.4.1.1.2 Semantics of the Service Primitives

The parameters of the primitives are as follows:
  Context Transfer.indication
  {
  Serving BS ID
  Target BS ID
  MS ID
  Security Information
  }

  MS ID
      48-bit unique identifier used for user identification between BS and NCMS
  Serving BS ID
      Base station unique identifier of the serving BS (same as in the DL-MAP)
  Target BS ID
      Base station unique identifier of the target BS (same as in the DL-MAP)
  Security Information
      The information negotiated during PKM procedure. It presents when the information could be provided.
      ~~PMK or MSK, PMK~~ AK and AK sequence number transmitted by NCMS, TEK, TEK key lifetime, TEK sequence number, CBC Initialize Vector (the reuse of IV is TBD because of the security issue), SAID, GKEK, GKEK lifetime, GKEKKID, SAID, SA-type, SA service type and Cryptographic-Suite

14.5.5.4.1.1.3 When generated
This primitive is issued by a BS or the NCMS when the handover procedure is successfully processed. The actual trigger point may be different according to the security sharing policy. One example is a serving BS issues this primitive after it generates HO start primitive.

14.5.5.4.1.1.4 Effect of receipt
The entity receiving this primitive shall response with Context Transfer.confirmation primitive. In addition, if the serving BS issues this primitive for the MS security information, the NCMS entity shall forwards the MS information to the target BS or another NCMS entity using Context Transfer.indication primitive.

14.5.5.4.1.2 Context Transfer.confirmation

14.5.5.4.1.2.1 Function

This primitive is issued by the target BS or the NCMS in order to response the Context Transfer.indication.

14.5.5.4.1.2.2 Semantics of the Service Primitives
The parameters of the primitives are as follows:

> Context Transfer.confirmation
> {
> Serving BS ID
> Target BS ID
> MS ID
> Result Code
> }

> **MS ID**
>> 48-bit unique identifier used for user identification between BS and NCMS
> **Serving BS ID**
>> Base station unique identifier of the serving BS (same as in the DL-MAP)
> **Target BS ID**
>> Base station unique identifier of the target BS (same as in the DL-MAP)
> **ResultCode**
>> The result of context transfer procedure

14.5.5.4.1.2.3 When generated
This primitive is issued by the target BS or the NCMS when the Context Transfer.indication is successfully processed.

14.5.5.4.1.2.4 Effect of receipt
This primitive informs the result of context transfer for the handover

14.5.5.4.1.3 Context Transfer.request

14.5.5.4.1.3.1 Function
After the successful handover procedure, the Target BS can re-establish the session information of MS in old BS.

14.5.5.4.1.3.2 Semantics of the Service Primitives
The parameters of the primitives are as follows:
> Context Transfer.request
> {
> Serving BS ID
> Target BS ID
> MS ID
> }

> **MS ID**
>> 48-bit unique identifier used for user identification between BS and NCMS
> **Serving BS ID**
>> Base station unique identifier of the serving BS (same as in the DL-MAP)

Target BS ID
        Base station unique identifier of the target BS (same as in the DL-MAP)

14.5.5.4.1.3.3 When generated
This primitive is issued by the target BS or the NCMS entity to request the MS's security context information.

14.5.5.4.1.3.4 Effect of receipt
The NCMS entity or the BS receiving this primitive provides the security context information using Context Transfer.response primitive.

14.5.5.4.1.4 Context Transfer.response

14.5.5.4.1.4.1 Function

This primitive is issued by the serving BS or the NCMS to response the Context Transfer.request.

14.5.5.4.1.4.2 Semantics of the Service Primitives
The parameters of the primitives are as follows:

    Context Transfer.response
    {
    Serving BS ID
    Target BS ID
    MS ID
    Result Code
    }

MS ID
        48-bit unique identifier used for user identification between BS and NCMS
Serving BS ID
        Base station unique identifier of the serving BS (same as in the DL-MAP)
Target BS ID
        Base station unique identifier of the target BS (same as in the DL-MAP)
ResultCode
        The result of context transfer procedure
Security Information
        The information negotiated during PKM procedure
        ~~PMK or MSK, PMK~~ AK and AK sequence number transmitted by an NCMS, TEK, TEK key lifetime, TEK sequence number, CBC Initialize Vector (the reuse of IV is TBD because of the security issue), SAID, SA-type, SA service type and Cryptographic-Suite

14.5.5.4.1.4.3 When generated
This primitive is issued by the serving BS or the NCMS entity after receiving Context Transfer.request primitive.

14.5.5.4.1.4.4 Effect of receipt

This primitive informs the result of context transfer for the handover

[Reference]
[1] IEEE P802.16e/D10
[2] IEEE-Std 802.16-2004
[3] IEEE 802.16g-05/008