Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Security Context Transfer for Handoffs**	
Date Submitted	**2005-09-09**	
Source(s)	Mi-Young Yun Jung Mo Moon, PhD Jaesun Cha Sang Ho Lee, PhD ETRI 161, Gajeong-dong,Yuseong-gu, Daejeon, 305-700, Korea	myyun@etri.re.kr jmmoon@etri.re.kr jscha@etri.re.kr leesh@etri.re.kr Voice: 82-42-860-4821 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	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate text contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.	

Security Context Transfer for Handoffs

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

ETRI

1. Problem Statement

The purpose is to describe the security context for handoff 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 the specific attributes which should be transferred. 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 candidate target BSs 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 not to candidate target BSs but to actual target BS. 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 context
  - ■ PMK or MSK
  - ■ 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 MSK which is the product of EAP exchange could be managed the authentication related node such as an AAA server, but the TEK and GTEK is 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.

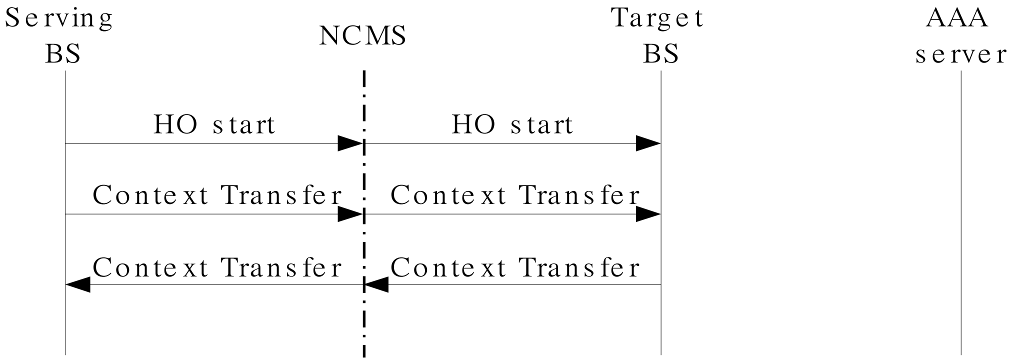

Figure 1. the security information provided by the serving BS

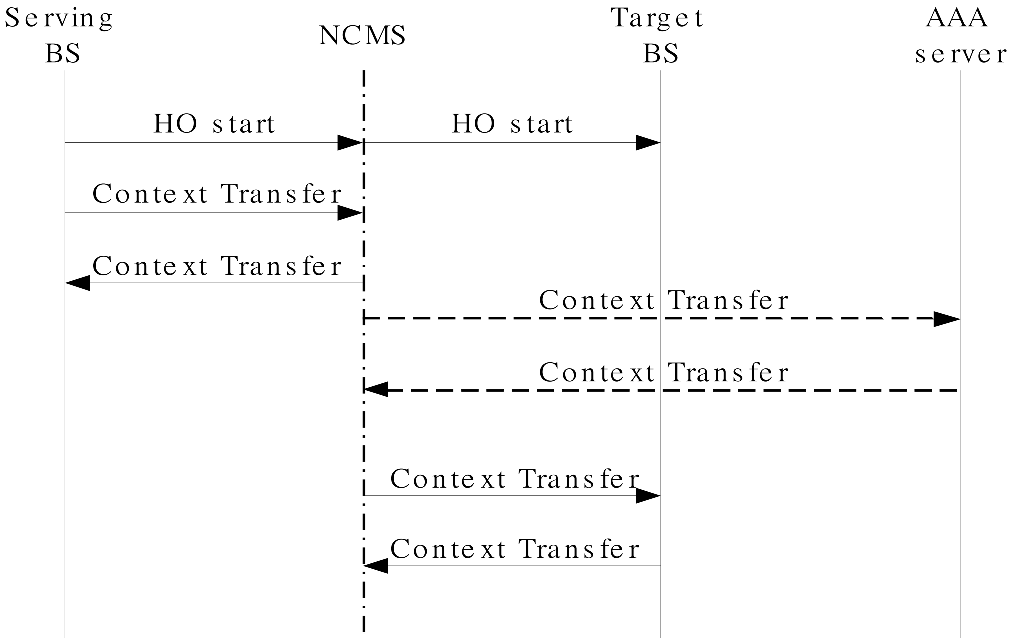

Figure 2. The security information provided by an AAA server

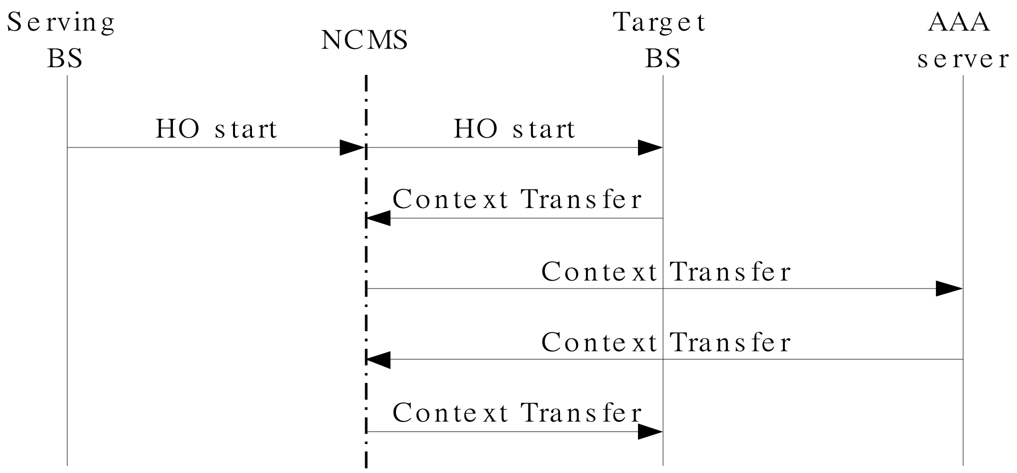

Figure 3. The security information requested by a target BS

In this contribution, we define 4 primitives to support security context transfer for handoffs between BS and 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

3. Proposed Text Changes

14.5.5 Security Management

[*Insert section 14.5.5.4 as follow*]

14.5.5.4 Security for Handoffs

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 NAS entity in NCMS as follows

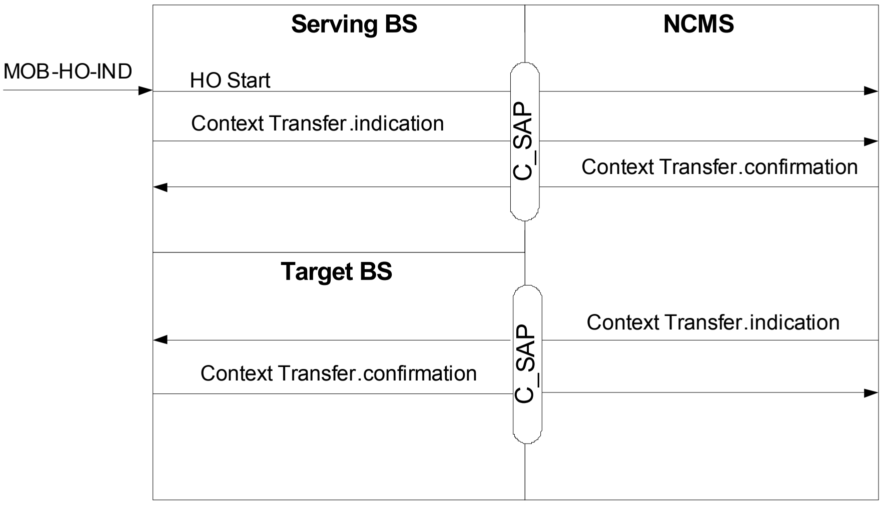
Serving BS
NCMS
MOB-HO-IND
HO Start
Context Transfer.indication
C_SAP
Context Transfer.confirmation
Target BS
Context Transfer.indication
Context Transfer.confirmation
C_SAP

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 primitive is issued by the serving BS in order to request the NCMS entity that the security context of the MS be forward to the target BS in order to re-establish the existed connection in the target BS. In addition, this primitive is forwarded from the NCMS to the target BS in order to give it the MS information.

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 sequence number, TEK, TEK key lifetime, TEK sequence number, CBC Initialize Vector, 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 when the handover procedure is successfully processed and after the HO start primitive is forwarded by the BS or the NCMS entity forwards the security context to the target BS.

14.5.5.4.1.1.4 Effect of receipt

The NCMS entity forwards the Context Transfer.indication to the target BS or another NCMS entity. Or the target BS could communicate securely with the MS which moves from other BSs.

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 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 when the Context Transfer.indication is successfully completed.

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 to request the NCMS entity of the MS's handoff context information.

14.5.5.4.1.3.4 Effect of receipt

The NCMS entity returns the context information of the requested MS.

14.5.5.4.1.4 Context Transfer.response

14.5.5.4.1.4.1 Function

This primitive is issued by the target BS in order 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 sequence number, SAID, SA-type, SA service type and Cryptographic-Suite

14.5.5.4.1.4.3 When generated

This primitive is issued by the NCMS entity when the context transfer is successfully completed.

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