1. **IEEE P802.21 Media Independent Handover Services**

|  |
| --- |
| **Solution for LB7 Cmt#121** |
| **Date:** 2013-08-23 |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Yoshikazu Hanatani | Toshiba | 1 Komukai-Toshiba-cho, Saiwai-ku, Kawasaki, 212-8582 Japan |  | yoshikazu.hanatani@toshiba.co.jp |

Abstract

This is a contribution to solve the comment #121 in 802.21-13-0113-12-MuGM-lb7-commentary-file.

1. Overview
	1. Scope
	2. Purpose
2. Normative references
3. Definitions
4. Abbreviations and acronyms
5. General Architecture
6. MIHF services
7. Service access points (SAPs) and primitives
	1. Introduction
	2. SAPs
	3. MIH\_LINK\_SAP primitives
	4. MIH\_SAP primitives
		1. MIH\_Capability\_Discover
		2. MIH\_Register
		3. MIH\_DeRegister
		4. MIH\_Event\_Subscribe
		5. MIH\_Event\_Unsubscribe
		6. MIH\_Link\_Up.indication
		7. MIH\_Link\_Down.indication
		8. MIH\_Link\_Parameters\_Report.indication
		9. MIH\_Link\_Going\_Down.indication
		10. MIH\_Link\_Handover\_Imminent.indication
		11. MIH\_Link\_Handover\_Complete.indication
		12. MIH\_Link\_PDU\_Transmit\_Status.indication
		13. MIH\_Link\_Get\_Parameters
		14. MIH\_Link\_Configure\_Thresholds
		15. MIH\_Link\_Actions
		16. MIH\_Net\_HO\_Candidate\_Query
		17. MIH\_MN\_HO\_Candidate\_Query
		18. MIH\_N2N\_HO\_Query\_Resources
		19. MIH\_MN\_HO\_Commit
		20. MIH\_Net\_HO\_Commit
		21. MIH\_N2N\_HO\_Commit
		22. MIH\_MN\_HO\_Complete
		23. MIH\_N2N\_HO\_Complete
		24. MIH\_Get\_Information
		25. MIH\_Push\_Information
		26. MIH\_Push\_key
		27. MIH\_LL\_Auth
		28. MIH\_Net\_HO\_Bcast\_Commit
		29. MIH\_Configuration\_Update
		30. MIH\_MN\_Group\_Manipulate
			1. MIH\_MN\_Group\_Manipulate.request
			2. MIH\_MN\_Group\_Manipulate.indication
			3. MIH\_MN\_Group\_Manipulate.response
				1. Function

This primitive is generated by an MIH User to acknowledge result of an MIH\_MN\_Group\_Manipulate request from an MN.

* + - * 1. Semantics of service primitive

MIH\_MN\_Group\_Manipulate.response (

DestinationIdentifier,

GroupIdentifier,

MulticastAddress,

SubgroupRange,

VerifyGroupKey,

AuxData,

CompleteSubtree,

GroupKeyData,

SAID,

GroupStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MIHF\_ID | Specifies the MIHF ID of the destination of the primitive |
| GroupIdentifier | MIHF\_ID | The target group identifier for the group operation. |
| MulticastAddress | TRANSPORT\_ADDR | (Optional) Multicast address corresponding with the target group identifier. |
| SubgroupRange | SUBGROUP\_RANGE | (Optional) Subgroup to process the command |
| VerifyGroupKey | VERIFY\_GROUP\_KEY | (Optional) Verification data for group key. |
| AuxData | OCTET\_STRING | (Optional) Auxiliary data. |
| CompleteSubtree | COMPLETE\_SUBTREE | (Optional) Complete Subtree data. |
| GroupKeyData | GROUP\_KEY\_DATA | (Optional )Encrypted group key. |
| SAID | ID\_VALUE | (Optional) ID of GKB\_generated SA. |
| GroupStatus | GROUP\_STATUS | Status of the group operation |

* + - * 1. When generated

An MIH User at the PoS generates this primitive after receipt and processing of MIH\_MN\_Group\_Manipulate request. This primitive returns the status of the action asked in the request. Optionally, it may respond with the security mechanisms required by the group.

* + - * 1. Effect on receipt

MIH\_MN\_Group\_Manipulate response message is sent back to the requester.

* + - 1. MIH\_MN\_Group\_Manipulate.confirm
		1. MIH\_Net\_Group\_Manipulate
			1. MIH\_Net\_Group\_Manipulate.request
				1. Function

This primitive is generated by the MIH User of a PoS to manipulate group membership of one or more MN(s) or other PoS(es).

* + - * 1. Semantics of service primitive

MIH\_Net\_Group\_Manipulate.request (

DestinationIdentifier,

ResponseFlag,

GroupKeyUpdateFlag,

GroupIdentifier,

MulticastAddress,

SubgroupRange,

VerifyGroupKey,

AuxData,

CompleteSubtree,

GroupKeyData,

SAID

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MIHF\_ID | Specifies group MIHF-ID of the remote MIHF peers. DestinationIdentifier may be different from GroupIdentifier. |
| ResponseFlag | RESPONSE\_FLAG | Flag which represents whether or not a response is needed. |
| GroupKeyUpdateFlag | GROUP\_KEY\_UPDATE\_FLAG | Flag which represents whether or not a group key in GroupKeyData is updated. |
| GroupIdentifier | MIHF\_ID | The target group identifier for the group operation. |
| MulticastAddress | TRANSPORT\_ADDR | (Optional) Multicast address corresponding with the target group identifier. |
| SubgroupRange | SUBGROUP\_RANGE | (Optional) Subgroup to process the command |
| VerifyGroupKey | VERIFY\_GROUP\_KEY | (Optional) Verification data for group key. |
| AuxData | OCTET\_STRING | (Optional) Auxiliary data. |
| CompleteSubtree | COMPLETE\_SUBTREE | Complete Subtree data. |
| GroupKeyData | GROUP\_KEY\_DATA | (Optional) Encrypted group key. |
| SAID | ID\_VALUE | (Optional) ID of GKB\_generated SA. |

* + - * 1. When generated

The MIH user generates this primitive to create, delete or modify group membership.

* + - * 1. Effect on receipt

Upon receipt of this primitive, MIHF on the PoS sends the corresponding MIH\_Net\_Group\_Manipulate indication message or MIH\_Net\_Group\_Manipulate request message to the MN(s) or other PoS(es). The ResponseFlag TLV indicates which message shall be sent.

* + - 1. MIH\_Net\_Group\_Manipulate.indication
			2. MIH\_Net\_Group\_Manipulate.response
			3. MIH\_Net\_Group\_Manipulate.confirm
		1. MIH\_Pull\_Credential
		2. MIH\_Push\_Credential
		3. MIH\_Revoke\_Credential
	1. MIH\_NET\_SAP primitives
1. Media independent handover protocol
	1. Introduction
	2. MIH protocol description
	3. MIH protocol identifiers
	4. MIH protocol frame format
	5. Message parameter TLV encoding
	6. MIH protocol messages
		1. MIH messages for service management
			1. MIH\_Capability\_Discover request
			2. MIH\_Capability\_Discover response
			3. MIH\_Register request
			4. MIH\_Register response
			5. MIH\_DeRegister request
			6. MIH\_DeRegister response
			7. MIH\_Event\_Subscribe request
			8. MIH\_Event\_Subscribe response
			9. MIH\_Event\_Unsubscribe request
			10. MIH\_Event\_Unsubscribe response
			11. MIH\_Auth indication
			12. MIH\_Auth request
			13. MIH\_Auth response
			14. MIH\_Termination\_Auth request
			15. MIH\_Termination\_Auth response
			16. MIH\_Push\_key request
			17. MIH\_Push\_key response
			18. MIH\_LL\_Auth request
			19. MIH\_LL\_Auth response
			20. MIH\_Configuration\_Update indication
			21. MIH\_MN\_Group\_Manipulate request
			22. MIH\_MN\_Group\_Manipulate response

The corresponding MIH primitive of this message is defined in 7.4.31.3.

This message is used by the MIHF to supply the group status of MIH node(s) identified by the Source Identifier.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=2, AID=11 ) |
| **Source Identifier** = sending MIHF ID(Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID(Destination MIHF ID TLV) |
| GroupIdentifier(Group Identifier TLV) |
| SequenceNumber (conditional)ª(Sequence Number TLV) |
| MulticastAddress (Optional)(Multicast Address TLV) |
| SubgroupRange (Optional)(Subgroup\_Range TLV) |
| VerifyGroupKey (Optional)(Verify Group Key TLV) |
| AuxData (Optional)(Aux Data TLV) |
| CompleteSubtree (Optional)(Complete Subtree TLV) |
| GroupKeyData (Optional)(Group Key Data TLV) |
| SAID (Optional)(SAID TLV) |
| GroupStatus(Group Status TLV) |

ª This parameter is only used in the case CCM encryption method is used and the group key is not updated.

* + - 1. MIH\_Net\_Group\_Manipulate request

The corresponding MIH primitive of this message is defined in 7.4.32.1.

This message is used by the MIHF to manipulate group membership of MIH node(s) identified by the Destination Identifier.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=1, AID=12 ) |
| **Source Identifier** = sending MIHF ID(Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID(Destination MIHF ID TLV) |
| GroupKeyUpdateFlag(Group Key Update Flag TLV) |
| GroupIdentifier(Group Identifier TLV) |
| SequenceNumber (Optional)(Sequence Number TLV) |
| MulticastAddress (Optional)(Multicast Address TLV) |
| SubgroupRange (Optional)(Subgroup Range TLV) |
| VerifyGroupKey (Optional)(Verify Group Key TLV) |
| AuxData (Optional)(Aux Data TLV) |
| CompleteSubtree(Complete Subtree TLV) |
| GroupKeyData (Optional)(Group Key Data TLV) |
| SAID (Optional)(SAID TLV) |

* + - 1. MIH\_Net\_Group\_Manipulate indication

The corresponding MIH primitive of this message is defined in 7.4.32.2.

This message is used by the MIHF to manipulate group membership of MIH node(s) identified by the Destination Identifier.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=3, AID=12 ) |
| **Source Identifier** = sending MIHF ID(Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID(Destination MIHF ID TLV) |
| GroupIdentifier(Group Identifier TLV) |
| GroupKeyUpdateFlag(Group Key Update Flag TLV) |
| SequenceNumber (Optional)(Sequence Number TLV) |
| MulticastAddress (Optional)(Multicast Address TLV) |
| SubgroupRange (Optional)(Subgroup Range TLV) |
| VerifyGroupKey (Optional)(Verify Group Key TLV) |
| AuxData (Optional)(Aux Data TLV) |
| CompleteSubtree(Complete Subtree TLV) |
| GroupKeyData (Optional)(Group Key Data TLV) |
| SAID (Optional)(SAID TLV) |

* + - 1. MIH\_Net\_Group\_Manipulate response
			2. MIH\_Pull\_Credential request
			3. MIH\_Pull\_Credential response
			4. MIH\_Push\_Credential request
			5. MIH\_Push\_Credential response
			6. MIH\_Revoke\_Credential request
			7. MIH\_Revoke\_Credential response
		1. MIH messages for event service
		2. MIH messages for command service
		3. MIH messages for information service
1. MIH protocol protection
2. Proactive authentication

#

#

#

#

#

# (normative)Data type definition

## Derived data types

### Data type for security

***Change Table F.24 as follows:***

Table F.24—Data type for security

|  |  |  |
| --- | --- | --- |
| Data type name  | Derived from | Definition |
| CERTIFICATE | OCTET\_STRING | Provides a X.509 Certificate |
| CERT\_SERIAL\_NUMBER | OCTET\_STRING | Provides X.509 formatted certificate serial number which are unique by certificate authority. |
| CERT\_STATUS | ENUMERATED | This indicates the status of the certificate being pushed or revoked0: Not Present – indicates that certificate is not present 1: Certificate Valid – indicates that certificate is present and that the associated public key is being used to verify signatures2: Certificate Revoked3: Certificate Expired |
| COMPLETE\_SUBTREE | LIST (GKB\_INDEX) | The data type for the complete subtree part of a GKB. See 9.4.2.1 for the details. |
| ENCRYPTED\_GROUP\_KEY | OCTET(16) | This is the base data type for GROUP\_KEY\_DATA. This store a group key of 16 octets encrypted with an AES key of 16 octets. |
| ID\_TYPE | ENUMERATED | The type of security association.0: TLS-generated;1: EAP-generated2: GKB-generated |
| GKB\_INDEX | SEQUENCE( NODE\_BIT\_LENGTH, NODE\_INDEX) | This is the base data type for COMPLETE\_SUBTREE. |
| GROUP\_KEY\_DATA | LIST (ENCRYPTED\_GROUP\_KEY) | The data type for the key data part of a GKB. See 9.4.2.1 for the details. |
| GROUP\_KEY\_UPDATE\_FLAG | ENUMERATED | This indicates if the group key is to be updated0: Key is not to be updated1: Key is to be updated |
| GROUP\_MGT\_ACTION | ENUMERATED | This indicates a manipulation command.0: Join the group.1: Leave the group. |
| GROUP\_STATUS | ENUMERATED | This indicates a status of group manipulation command.0: Join operation successful1: Unauthorized to join the group2: Leave operation successful3: Unchanged |
| MIH\_SEC\_CAP | SEQUENCE(TLS\_CAP,EAP\_CAP,MULTICAST\_CAP,) | Represents the MIH security capabilities. |
| MULTICAST\_CAP | UNSIGNED\_INT(2) | A multicast ciphersuite. Available multicast ciphersuites are defined in 9.4.6.  |
| NODE\_BIT\_LENGTH | UNSIGNED\_INT(1) | This stores the bit length of the following NODE\_INDEX. |
| NODE\_INDEX | CHOICE ( UNSIGNED\_INT(1), UNSIGNED\_INT(2), UNSIGNED\_INT(3), UNSIGNED\_INT(4) ) | This stores the index of a node of the binary tree. See 9.4.2.1 for the details. |
| RESPONSE\_FLAG | ENUMERATED | This indicates if an answer is required0: No response is needed1: Response is needed |
| SIGNATURE | OCTET\_STRING | A digital signature data. |
| SUBGROUP\_RANGE | CHOICE( SEQUENCE( UNSIGNED\_INT(1), UNSIGNED\_INT(1)),SEQUENCE( UNSIGNED\_INT(2), UNSIGNED\_INT(2)),SEQUENCE( UNSIGNED\_INT(3), UNSIGNED\_INT(3)),SEQUENCE( UNSIGNED\_INT(4), UNSIGNED\_INT(4))) | A range of valid leaf identifiers in a complete subtree of a GKB. The first integer indicates the lowest value of the range. The second integer indicates the highest value of the range. |
| VERIFY\_GROUP\_KEY | SEQUENCE ( OCTETS(16), OCTETS(16)) | The first OCTET(16) is arbitrary data, which is an input message to AES-CMAC (defined in RFC-4493). The second OCTET(16) is the MAC value for the first OCTET(16) to be verified. |

#

#

#

#

#

# (normative)MIH protocol message code assignments

***Change Table L.2 as follows:***

Table L.2 —Type values for TLV encoding

|  |  |  |
| --- | --- | --- |
| TLV type name | TLV type value | Data Type |
| Aux Data | 79 | OCTET\_STRING |
| Configuration Data | 80 | OCTET\_STRING |
| Credential Revocation Signature | 81 | SIGNATURE |
| Credential | 82 | CERTIFICATE |
| Credential Serial Number | 83 | CERT\_SERIAL\_NUMBER |
| Credential Status | 84 | CERT\_STATUS |
| Complete Subtree | 85 | COMPLETE\_SUBTREE |
| Encrypted Credential | 86 | ENCR\_BLOCKDATA |
| Group Action  | 87 | GROUP\_MGT\_ACTION |
| Group Identifier | 88 | MIHF\_ID |
| Group Key Data | 89 | GROUP\_KEY\_DATA  |
| Group\_Status | 90 | GROUP\_STATUS |
| Multicast Address | 91 | TRANSPORT\_ADDRESS |
| Multicast Ciphersuite | 92 | MULTICAST\_CAP |
| Multicast Link Action List | 93 | LIST(MULTICAST\_ACTION\_REQ) |
| Multicast Link Identifier | 94 | NET\_TYPE\_INC |
| Response Flag  | 95 | RESPONSE\_FLAG |
| Sequence Number | 96 | OCTET\_STRING |
| Signature | 97 | SIGNATURE |
| Subgroup Range | 98 | SUBGROUP\_RANGE |
| Verify Group Key | 99 | VERIFY\_GROUP\_KEY |

#

#

#

#