| | |
|---|---|
| Project | **IEEE 802.21a**<br>**<https://mentor.ieee.org/802.21>** |
| Title | Option II: use (D)TLS to protect MIH. |
| DCN | **21-09-0079-01-0Sec** |
| Date Submitted | **June 28, 2010** |
| Source(s) | Subir Das, Ashutosh Dutta (Telcordia), Toshikazu Kodama (Toshiba) |
| Re: | Updated version |
| Abstract | This document elaborates the use of (D)TLS to protect MIH |
| Purpose | Specific functional requirements need to be developed for the IEEE 802.21 devices to provide the necessary reliability, availability, and interoperability of communications with different operator networks. In addition, guidelines for using MIH protocol need to be developed so that vendors and operators can better understand the issues, pros, and cons of implementing IEEE 802.21 for supporting various mobility handover scenarios. |
| Notice | This document has been prepared to assist the IEEE 802.21 Working Group. 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 material 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 IEEE 802.21 may make this contribution public. |
| Patent Policy | The contributor is familiar with IEEE patent policy, as stated in Section 6 of the IEEE-SA Standards Board bylaws <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and in *Understanding Patent Issues During IEEE Standards Development* http://standards.ieee.org/board/pat/faq.pdf |

## [1] INTRODUCTION

### *Scope*

The scope of this document is to propose a solution on MIH messages can be protected with the use of (D)TLS

### *Purpose*

The purpose of this document is to describe the MIH protocol level security.

### *Definitions( Clause 3. Definitions)*

**MIH Security Association (SA):** An MIH SA is the security association between the peer MIH entities

**Main questions:**

1. **What is an MIH SA?**
2. **What is the relation between a MIH SA and the TLS ciphersuite negotiated through TLS?**

### *References (Clause 2. Normative references)*

[RFC5246] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2" , RFC 5246

[RFC4347] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security", RFC 4347

[IEEE802.21] IEEE P802.21 Std-2008, IEEE Standard for Local and Metropolitan Area Networks- Part 21: Media Independent Handover Services.

## [2] SECURING MIH PROTOCOL MESSAGES (CLAUSE 8.X. MIH PROTOCOL SECURITY)

This section proposes the MIH protocol message security using the existing protocols for authentication and key management that will greatly reduce the risk of introducing security flaws.

### *Proposed Approach*

Our proposed approach is to use TLS [RFC5246] or DTLS [RFC4347] for authentication, key establishment and ciphering. TLS handshake is carried out over MIH protocol and an MIH SA is established between two MIHF peers. (D)TLS will provide cipher suites negotiation. Once MIH SA is defined within MIH protocol, there is no need to have MIH transport level security

**MIH SECURITY (CLAUSE 8.X.2.)**

We assume that the MIH service access control is not applied through any access controller. The mutual authentication may be based on a pre-shared key or a trusted third party like certificate authority. The authentication is MIH specific. The MN and the PoS will conduct a mutual authentication and key establishment of MIH specific keys.

**Comment [LLC1]:** Here it is already pointed which credentials can be used for the mutual autehntication. See next comment.

**Call flows (Clause 8.X.2.1. Call flows)**

Figure 1 describes the MIH security call flows:

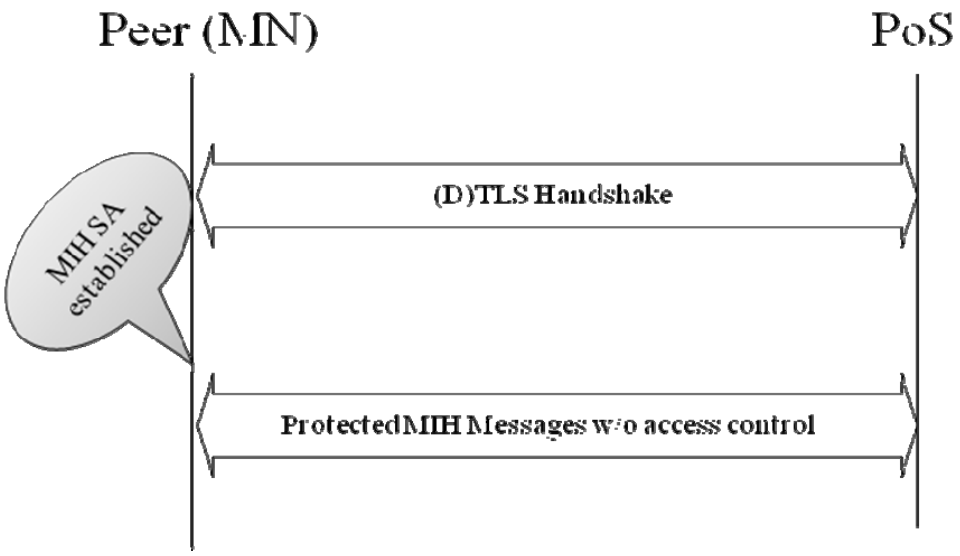



**Figure 1: MIH Security**

***Security Capability Discovery***

The following security-related capability is defined for MIH capability discovery. (Clause F.3.X. Data types security)

- Data Type: MIH_SEC_CAP
- Derived from BITMAP(16)
    - Bit 0: TBD
    - Bit 1: TBD
    - Bit 2: TBD

- Bit 4: MIH SA with access control (TBD)
- Bit 5: MIH SA without access control
- Bit 6-15: Reserved

The following parameter is added to MIH_Capability_Discover.{request,response} primitives. (Clause 7.4.1.1 **MIH_Capability_Discover.request** and 7.4.1.3 **MIH_Capability_Discover.response**)

| Name | Data type | Description |
|---|---|---|
| SupportedSecurityCapList | MIH_SEC_CAP | List of supported MIH security capabilities on the local MIHF. |

The following parameter is added to MIH_Capability_Discover.{indication,confirm} primitives. (Clause 7.4.1.2 **MIH_Capability_Discover.indication and 7.4.1.4 MIH_Capability_Discover.confirm)**

| Name | Data type | Description |
|---|---|---|
| SupportedSecurityCapList | MIH_SEC_CAP | List of supported MIH security capabilities on the remote MIHF. |

**TLS Identity**

Either Pre-configured TLS credentials or a key established through other manner (e.g., EAP) is used for (D)TLS handshake to mutually authenticate the MIHF peers and establish (D)TLS key material for protecting MIH messages using (D)TLS.

**Comment [LLC2]:** Here the mutual authentication credentials are discussed again. Is this different from the previous statement. Especially, EAP is an authentication protocol. Can we recommend to use keys established through EAP to conduct TLS authentication? It is more likely, an TLS can be used as an EAP mehod. Do we need to recommend the authentication credentials. Can we assume that a MN and PoS have credentials to condut a TLS authentication.

**MIH Protocol Extensions (Clause 8.X.3. Securing MIH protocol messages)**

TLS or DTLS is used for securing the MIH protocol. The transport protocol for (D)TLS in this case is the MIH protocol itself. When the MIH protocol transport is reliable, TLS is used. Otherwise, DTLS is used. The transport protocol entities to be associated with a TLS session are MIHF peers and identified by MIHF identifiers. Therefore, the transport address of an MIHF can change over the lifetime of a TLS session as long as the mapping between the transport address and MIHF identifier of an MIHF is maintained. The following subsections describe extensions to the MIH protocol for use of (D)TLS.

**Comment [LLC3]:** I do not think we can recommend TLS or (D) TLS based on whether MIH is reliable. Can we? We keep DTLS as an option since MIH may be carried over UDP. (At least, this is the answered provided at July meeting.)

**Comment [LLC4]:** How to maintain this mapping? Is this in the scope of 21a? Do we need add some more details here?

**TLS TLV (Annex L Table L.2 - Type values for TLV encoding)**

TLS (Transport Layer Security) TLV is a new TLV of type OCTET_STRING carrying a (D)TLS message. Once an MIH SA is established, the entire raw MIH PDU excluding Source and Destination MIHF Identifier TLVs, must be

**Comment [LLC5]:** This is very confusing. If an MIH SA is established, then we need to distinguish this SA with SA in EAP MIH authentication case.

protected with the TLS key material of the MIH SA and carried in the payload of the TLS TLV as the TLS application data.

**Session ID TLV (Annex L Table L.2 - Type values for TLV encoding)**

Session ID (Identifier) TLV is a new TLV of type OCTET_STRING carrying a (D)TLS session identifier [RFC 5246] that is assigned as a result of a TLS handshake.

**Security Capability TLV (Annex L Table L.2 - Type values for TLV encoding)**

Security Capability TLV is a new TLV of type MIH_SEC_CAP carrying security capabilities of an MIHF. This TLV is carried in MIH_Capability_Discover request and response messages.

**MIH Security PDU (Clause 8.4.X : Frame format with Security)**

An MIH Security (MIHS) PDU is an MIH PDU that has an MIHS header, followed by followed by optional Source and Destination MIHF-ID TLVs, followed by an optional Session ID TLV, followed by a TLS TLV. An MIHS header is an MIH protocol header containing the following information.

- Version: the version of MIH protocol
- Ack-Req: 0
- Ack-Rsp: 0
- UIR: 0
- M:0
- FN:0
- SID: 5 (Security Service)
- Opcode: 2 (Indication)
- TID: 0

A Session ID TLV is associated with the pair of MIHFs associated with the MIH SA. Therefore, Source and Destination MIHF Identifier TLVs do not need to be carried in an MIHS PDU in existence of an MIH SA, and a Session ID TLV is carried instead. Source and Destination MIHF Identifier TLVs are carried in a MIHS PDU in absence of an MIH SA or when the sender's transport address has been changed. In the latter case, the mapping between the sender's transport address and the MIHF identifier shall be updated, and an MIH Registration request or response message may be contained in the TLS TLV.

**Comment [LLC6]:** Again, this must be specified. Is this bootstrap TLS key to establish a MIH SA or use the record layer to protect MIH messages?

**Comment [LLC7]:** Here whether it is TLS which carries MIH or MIH carries TLS?

The structure of MIHS PDU during TLS handshake is shown in **Error! Reference source not found.**. The structure of MIHS PDU in existence of an MIH SA is shown in Figure 3. The structure of MIHS PDU upon Transport Address Change is shown in Figure 4.


Figure 2: MIHS PDU during TLS handshake

**Comment [LLC8]:** If this is the handshake, then it uses MIH messages to carry TLS TLV. We assume that the messages (MIH messages) are not protected yet. Do we really need MIHS header or a regular MIH header?

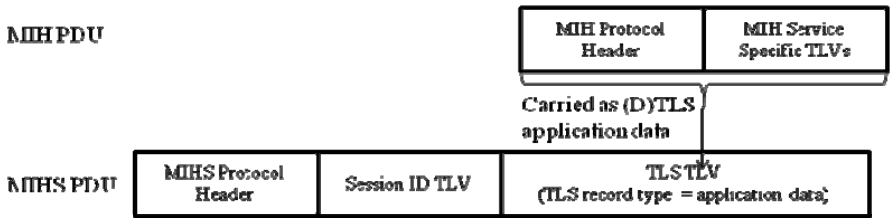


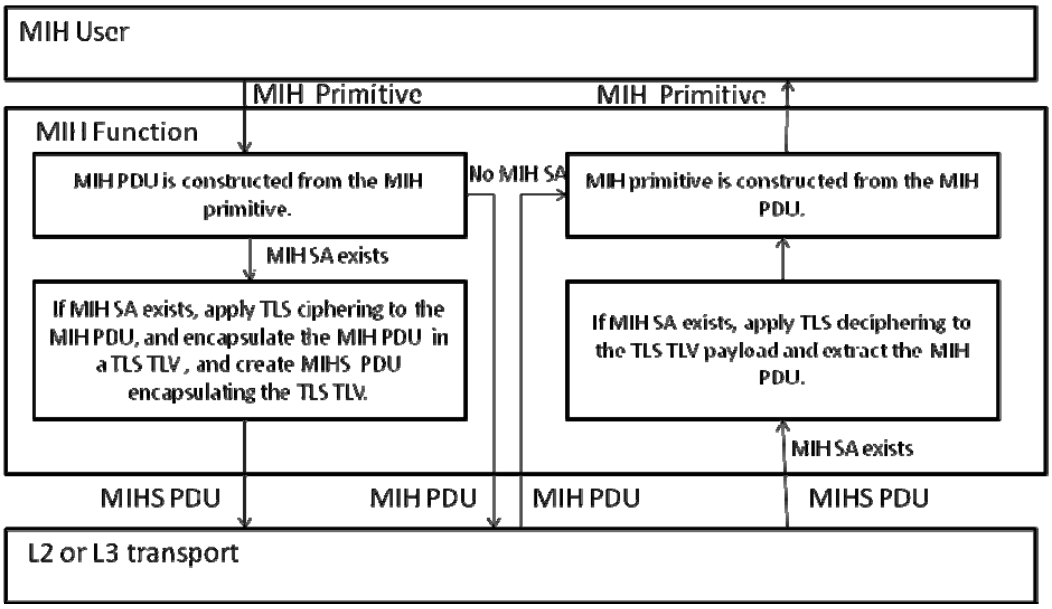

Figure 3: MIHS PDU in existence of MIH SA

**Comment [LLC9]:** Are we assuming that MIH protocol header together with MIH service specific TLVs are application data for TLS? Why do we still need MIHS header?


Figure 4: MIHS PDU upon Transport Address Change

**Comment [LLC10]:** Where are the protected portion?

**Interaction between MIH User, MIHF and Transport (This section should go to Annex X if necessary)**




[2] **MIH PROTOCOL MESSAGES**

**Message Types (Annex L (Normative) Table L.1—AID assignment)**

Table 1 lists the new MIH messages types [IEEE802.21]

**Table 1: MIH New Message Types**

| Message name | Action ID |
|---|---|

| | |
|---|---|
| MIH_Security Indication | JJ |

Table 2 lists the messages that need extension

**Table 2: MIH Message Extension**

| Message Name | Action ID |
|---|---|
| Capability_Discover_Request | 1 |
| Capability_Discover_Response | 1 |

**(Clause 8.6.X MIH messages for security)**

For the messages in Table 5, an additional Supported Security Cap List parameter is carried in a Security Capability List TLV of type MIH_SEC_CAP.

**MIH_Security Indication (Clause 8.6.X.6 MIH_Security Indication )**

| |
|---|
| MIH Header Fields (SID=5, Opcode=2, AID-xx) |
| Source Identifier = sending MIHF ID (optional)<br><br>(Source MIHF ID TLV) |
| Destination Identifier = receiving MIHF ID (optional)<br><br>(Destination MIHF ID TLV) |
| Session Identifier = session id (optional)<br><br>(Session ID TLV) |
| TLS = transport layer security<br><br>(TLS TLV) |

**Comment [LLC11]:** Is this an MIH header or an MIHS header?

**Comment [LLC12]:** IS it true that the data after this indication will be protected using the ciphersuite as negotiated in TLS or (D) TLS?

**Security Policies**

TBD