|  |  |
| --- | --- |
| Project | **IEEE 802.21a**  **<https://mentor.ieee.org/802.21>** |
| Title | **LB comments** |
| DCN | 21-10-0255-00-0sec |
| Date Submitted |  |
| Source(s) | Fernando Bernal-Hidalgo (University of Murcia), Rafael Marin-Lopez (University of Murcia) |
| Re: |  |
| Abstract | This document elaborates comments that need to be carried out in the draft |
| Purpose | Proposes changes in the current draft |
| 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/opman/sect6.html#_blank) <[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://127.0.0.1:4664/cache?event_id=757737&schema_id=1&s=5X0vID10lu_E6yrIkWkNd4Wz2H8&q=hancock#_blank)> and in *Understanding Patent Issues During IEEE Standards Development* [http://standards.ieee.org/board/pat/faq.pdf](http://standards.ieee.org/board/pat/faq.pdf#_blank) |

|  |  |
| --- | --- |
| Ref. | 001 |
| DRAFT SECTION | 3. DEFINITION |
| Modification type | ADD |
| Text | **PoS:** acts as authenticator for the service authentication. Moreover, it is the entity that interacts with PoAs to facilitate key distribution services.  **MIH Service AS:** It is a backend authentication server for the MIH service authentication.  **Candidate PoS:** A PoS that is a potential target to the MN’s movement  **Serving PoS:** A PoS that is the current PoS which provides access to the supported network services.  **Candidate PoA:** A PoA that is a potential target to the MN’s network attachment.  **Target PoA:** A PoA that is the PoA selected to perform a key distribution  **Serving PoA:** A PoA that is the current PoA where the MN is attached. Moreover, it provides network access to the MN. |

|  |  |
| --- | --- |
| Ref. | 002 |
| DRAFT SECTION | 4. ABBREVIATIONS AND ACRONYMS |
| Modification type | ADD |
| Text | **PoS:** Point of Service  **PoA:** Point of Attachment  **MN:** Mobile Node  **MIH PDU:** MIH Packet Data Unit |

|  |  |
| --- | --- |
| Ref. | 003 |
| DRAFT SECTION | 10.2.2.3 Proactive pull key distribution |
| Modification type | Replace  Section name to Optimized Proactive Pull Key distribution |
| Text | This mechanism allows the MN to perform a proactively media-specific authentication with the target PoA without being directly connected to the wireless link of the target PoA by means sending link-layer frames through the PoS to the target PoA. The key hierarchy shared between the MN and the PoS is used in order to derive a shared key to be used in the key distribution process, where the PoS will be acting as a local AAA and using the identity provided during the Media Independent Service Authentication phase the PoS could be contacted to perform the key distribution mechanism. To perform this key distribution mechanism the primitives provided in section 7.4.34 and the MIH messages in section 8.6.1.21 and 8.6.1.22. |

|  |  |
| --- | --- |
| Ref. | 004 |
| DRAFT SECTION | 7.4.34 MIH\_Pro\_Auth and subsections |
| Modification type | REPLACE  The new section must be named MIH\_LL\_Auth |
| TEXT | This section provides the primitives needed in order to carry out the MN authentication using link layer frames over MIH between the MN and the PoS where the authenticator will be the target PoA. MIH\_LL\_Auth.requestFunction This primitive is used to perform an authentication based on link-layer frames. Semantics of service primitive MIH\_LL\_Auth.request (  DestinationIdentifier,  PoAIndentifier,  LLInformation,  )   |  |  |  | | --- | --- | --- | | Name | Data type | Description | | DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this request. | | PoAIdentifier | PoA\_ID | This identifies a PoA. | | LLInformation | LL\_FRAMES | This contains link-layer frames |  When generated This primitive is generated by a MIH User to start the authentication process based on link-layer frames. Effect on receipt The local MIHF shall generate a MIH\_LL\_Auth request message to the remote MIHF. MIH\_LL\_Auth.indicationFunction This primitive is used by the remote MIHF to notify the corresponding MIH user about the reception of a MIH\_LL\_Auth request message. Semantics of service primitive MIH\_LL\_Auth.indication (  SourceIdentifier,  PoAIndentifier,  LLInformation,  )   |  |  |  | | --- | --- | --- | | Name | Data type | Description | | SourceIdentifier | MIHF\_ID | This identifies the invoker, which is a remote MIHF. | | PoAIdentifier | PoA\_ID | This identifies a PoA. | | LLInformation | LL\_FRAMES | This contains link-layer frames. |    When generated This primitive is generated by remote MIHF after receiving a MIH\_LL\_Auth request message. Effect on receipt The MIH user must generate a MIH\_LL\_Auth.response primitive. MIH\_LL\_Auth.responseFunction This primitive is used by a MIH user to provide the link-layer frames to the local MIHF. Semantics of service primitive MIH\_LL\_Auth.response (  DestinationIdentifier,  PoAIndentifier,  LLInformation,  Status  )   |  |  |  | | --- | --- | --- | | Name | Data type | Description | | DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this request. | | PoAIdentifier | PoA\_ID | This identifies a PoA. | | LLInformation | LL\_FRAMES | This contains link-layer frames both the MN and the PoA in other to perform a proactive authentication. | | Status | STATUS | Status of the authentication |  When generated This primitive is generated after receiving a MIH\_LL\_Auth.indication primitive. Effect on receipt The local MIHF must generate a MIH\_Proact\_Pull response in order to provide the required information until the authentication is finished. MIH\_LL\_Auth.confirmFunction This primitive is used to notify the corresponding MIH user about the reception of a MIH\_Proact\_Pull response. Semantics of service primitive MIH\_LL\_Auth.confirm (  LLInformation,  Status  )   |  |  |  | | --- | --- | --- | | Name | Data type | Description | | LLInformation | LL\_FRAMES | This contains link-layer frames both the MN and the PoA in other to perform a proactive authentication. | | Status | STATUS | Status of the authentication |    When generated This primitive is generated by the remote MIHF after receiving a MIH\_LL\_Auth response message. Effect on receipt The MIH user must generate a MIH\_LL\_Auth.request primitive until the authentication is completed. |

|  |  |
| --- | --- |
| Ref. | 005 |
| DRAFT SECTION | NEW SUBSECTION |
| Modification type | NEW  10.1.3 Proactive Pull Key Distibution Mechanism. |
| Text | Proactive pull key distribution mechanism allows a MN to perform a proactively media-specific authentication with the target PoA without being directly connected to the wireless link of the target PoA by means sending link-layer frames through the PoS to the target PoA. The target PoA upon receiving the frames contact with the Media Specific AS in order to authenticate the MN. Once the MN has been authenticated a key is distributed to the target PoA and this key is shared with the MN. Therefore, when the MN moves to the target PoA the security association can be established. |

|  |  |
| --- | --- |
| Ref. | 006 |
| DRAFT SECTION | 8.6.1.21 |
| Modification type | REPLACE  Section name must be update to MIH\_LL\_Auth request |
| Text | |  | | --- | | **MIH Header Fields (SID = 1, Opcode = 1, AID = 12)** | | Destination Identifier = receiving MIHF ID  (Destination MIHF ID TLV) | | Source Identifier = sending MIHF ID  (Source MIHF ID TLV) | | PoAIdentifier  (PoA Identifier TLV) | | LLInformation  (Pull Information TLV) | |

|  |  |
| --- | --- |
| Ref. | 007 |
| DRAFT SECTION | 8.6.1.22 |
| Modification type | REPLACE  Section name must be update to MIH\_LL\_Auth response |
| Text | |  | | --- | | **MIH Header Fields (SID = 1, Opcode = 2, AID = 12)** | | Destination Identifier = receiving MIHF ID  (Destination MIHF ID TLV) | | Source Identifier = sending MIHF ID  (Source MIHF ID TLV) | | PoAIdentifier  (PoA Identifier TLV) | | LLInformation  (Pull Information TLV) | | Status (optional)  (Status TLV) | |

|  |  |
| --- | --- |
| Ref. | 008 |
| DRAFT SECTION | NEW section (Data types definition) |
| Modification type | NEW |
| Text | |  |  |  | | --- | --- | --- | | **Data Type Name** | **Derived from** | **Definition** | | KEY\_DIST\_LIST | BITMAP(8) | A list of key distribution methods available.  Bitmap values:  Bit 0: Push Key distribution.  Bit 1: Proactive Pull Key Distribution.  Bit 2: Optimized Proactive Pull Key Distribution.  Bit 3: Reactive Pull Key Distribution.  Bit 4-7: (Reserved) | | INT\_ALG\_LIST | BITMAP(8) | A list of integrity algorithms available.  Bitmap values:  Bit 0: INTR\_HMAC\_SHA\_96  Bit 1: INTR\_CMAC\_AES  Bit 2: INTR\_NULL  Bit 3-7: (Reserved) | | CIPH\_ALG\_LIST | BITMAP(8) | A list of encryption algorithms available.  Bitmap values:  Bit 0: ENCR\_AES\_CBC  Bit 1: AUTH\_ENC\_AES\_CCM  Bit 2 : ENCR\_NULL  Bit 3-7: (Reserved) | | KDF-List | BITMAP(8) | A list of Key Derivation Functions available.  Bitmap values:  Bit 0: PRF\_CMAC\_AES  Bit 1: PRF\_HMAC\_SHA1  Bit 2-7: (Reserved) | | ID\_OPT | OCTET\_STRING | Represents a new identity provided for optimization purposes. | | NONCE\_VALUE | UNSIGNED\_INT(2) | Represents a random value. | | AUTH\_INFO\_VALUE | OCTET\_STRING | Represents the authentication information used to authenticate. | | AUTH\_VALUE | OCTET\_STRING | Represent an integrity string to verify data integrity. | | INTEGRITY\_DATA | OCTET\_STRING | Represents the integrity data of a message. | | KEY | OCTET\_STRING | Represents a key | | LL\_FRAMES | OCTET\_STRING | Represents the information needed to carry out a key installation. | | STATUS | ENUMERATED | This is an extension of STATUS TLV defined in IEEE 802.21, it must be updated to support:  5: Authentication Failure | | LIFETIME | UNSIGNED\_INT(2) | Represents the period of time that a key is valid for being used. | | POA\_ID | LINK\_ADDR | A data type to represent an address of any link layer | | SECURITY | CHOICE(TLS\_RECORD,MIH\_SPS\_RECORD) | Data type to represent information which is carried in the SECURITY TLV. | | TLS\_RECORD | OCTECT\_STRING | Represent a TLS record. | | MIH\_SPS\_RECORD | SEQUENCE(CHOICE(ENCR\_BLOCK,PLAINTEXT\_BLOCK),CHOICE(INTG\_BLOCK,NULL)) | Represent data protected or not by a MIH security association. | | PLAINTEXT\_BLOCK | OCTECT\_STRING | Represent unencrypted data. | | ENCR\_BLOCK | OCTECT\_STRING | Represent encrypted data. | | INTG\_BLOCK | OCTECT\_STRING | Represent integrity data. | |