|  |  |
| --- | --- |
| Project | **IEEE 802.21a** **<https://mentor.ieee.org/802.21>** |
| Title | **ERP support** |
| DCN | **21-11-0165-01-0sec** |
| Date Submitted | **October 17, 2011** |
| Source(s) | Fernando Bernal-Hidalgo (University of Murcia), Rafael Marin-Lopez (University of Murcia) |
| Re: |  |
| Abstract | This document elaborates modifications 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 | 8.6.1.12 MIH\_Auth request |
| Modification type | Replace definition text |
| Text | This message is used for an MIHF in both MN and PoS to send EAP or ERP messages in an MIH service authentication. |

|  |  |
| --- | --- |
| Ref. | 002 |
| DRAFT SECTION | 8.6.1.13 MIH\_Auth response |
| Modification type | Replace definition text |
| Text | This message is used for an MIHF in both MN and PoS to send EAP or ERP messages in an MIH service authentication. |

|  |  |
| --- | --- |
| Ref. | 003 |
| DRAFT SECTION | 8.6.1.11 MIH\_Auth indication |
| Modification type | Replace definition text |
| Text | This is used for an MIHF to perform (D)TLS exchange with another MIHF to establish or terminate a (D)TLS-generated MIH SA, or to communicate with another MIHF to initiate an MIH service access authentication through EAP or ERP. In the former case, an AuthenticationContent shall be included to carry a TLS record of type handshake, change ciphersuite or alert message.  In the latter case,AuthenticationContent shall be included to carry an ERP payload message when ERP is initiated by the PoS.  This message shall not be used when EAP is initiated by a PoS or when ERP is initiated by a MN, and MIH\_Auth request message shall be used instead. |

|  |  |
| --- | --- |
| Ref. | 004 |
| DRAFT SECTION | Figure 31—Main Stages with MN Initiated Authentication |
| Modification type | Update figure |
| Text | Remove ERP from figure in MIH Service Access Authentication Phase. Update the caption to: Main Stages with MN Initiated **EAP** Authentication |

|  |  |
| --- | --- |
| Ref. | 005 |
| DRAFT SECTION | Figure 32—Main Stages with Network Initiated Authentication |
| Modification type | Update figure |
| Text | Remove ERP from figure in MIH Service Access Authentication PhaseUpdate the caption to: Main Stages with Network Initiated **EAP** Authentication |

|  |  |
| --- | --- |
| Ref. | 006 |
| DRAFT SECTION | 9.2.1 MIH service access authentication |
| Modification type | Add figure |
| Figure |  |
| Title | Main stages with MN initiated ERP re-authentication |

|  |  |
| --- | --- |
| Ref. | 007 |
| DRAFT SECTION | 9.2.1 MIH service access authentication |
| Modification type | Add figure |
| Figure |  |
| Title | Main Stages with Network Initiated ERP Re-Authentication (1) |

|  |  |
| --- | --- |
| Ref. | 008 |
| DRAFT SECTION | 9.2.1 MIH service access authentication |
| Modification type | Add figure |
| Figure |  |
| Title | Main Stages with Network Initiated ERP Re-Authentication (2) |

|  |  |
| --- | --- |
| Ref. | 009 |
| DRAFT SECTION | F.3.16 Data type for security |
| Modification type | Replace KDF\_LIST |
| Text | PRF\_LIST |
| Page | 54 |
| Line | 50 |

|  |  |
| --- | --- |
| Ref. | 010 |
| DRAFT SECTION | F.3.16 Data type for security |
| Modification type | Replace KDF\_LIST |
| Text | PRF\_LIST |
| Page | 55 |
| Line | 14 |

|  |  |
| --- | --- |
| Ref. | 011 |
| DRAFT SECTION | Annex L |
| Modification type | Replace KDF\_LIST |
| Text | PRF\_LIST |
| Page | 63 |
| Line | 43 |

|  |  |
| --- | --- |
| Ref. | 012 |
| DRAFT SECTION | F.3.16 Data type for security |
| Modification type | Update definition |
| Text | Bit 2: PRF\_HMAC\_SHA256Bit 3-7 (reserved) |
| Page | 55 |
| Line | 14 |

|  |  |
| --- | --- |
| Ref. | 013 |
| DRAFT SECTION | 9.2.3 EAP-generated MIH security association |
| Modification type | Replace KDF\_CMAC\_AES |
| Text | PRF\_CMAC\_AES |
| Page | 39 |
| Line | 53 |

|  |  |
| --- | --- |
| Ref. | 014 |
| DRAFT SECTION | 9.2.3 EAP-generated MIH security association |
| Modification type | Replace KDF\_HMAC\_SHA1 |
| Text | PRF\_HMAC\_SHA1 |
| Page | 39 |
| Line | 57 |

|  |  |
| --- | --- |
| Ref. | 015 |
| DRAFT SECTION | 9.2.3 EAP-generated MIH security association |
| Modification type | Replace KDF\_HMAC\_SHA256 |
| Text | PRF\_HMAC\_SHA256 |
| Page | 39 |
| Line | 60 |

|  |  |
| --- | --- |
| Ref. | 016 |
| DRAFT SECTION | 9.2.2 Key derivation and key hierarchy |
| Modification type | Update text |
| Text | Upon a successful MIH service access authentication, the authenticator, PoS, obtains a master session key (MSK) or a re-authentication master session key (rMSK). From the MSK or rMSK, based on the ciphersuite agreed upon between an MN and a PoS, the session keys used for MIH message protection can consist of an encryption key (MIEK) only, an integrity key (MIIK) only, or both an encryption key (MIEK) and an integrity key (MIIK).**Moreover, an authentication key (MIAK) is used to provide integrityprotection to the MIH\_Auth messages and the length of this key must be 128 bits**. The length, L, of the derived keying material, called media independent session key (MISK), depends on the ciphersuite, which are specified in Clause 9.2.3. |
| Page | 37 |
| Line | 51 |

|  |  |
| --- | --- |
| Ref. | 017 |
| DRAFT SECTION | 9.2.2 Key derivation and key hierarchy |
| Modification type | Update text |
| Text | MISK = MIAK || MIIK ||MIEK |
| Page | 38 |
| Line | 47 |

|  |  |
| --- | --- |
| Ref. | 018 |
| DRAFT SECTION | 9.2.2 Key derivation and key hierarchy |
| Modification type | Update figure 33 |
| Text |  |
| Page | 39 |
| Line | 1 |

|  |  |
| --- | --- |
| Ref. | 019 |
| DRAFT SECTION | 10.2.1.2 Derivation of media specific pairwise master keys (MSPMKs) |
| Modification type | Update figure 44 |
| Text |  |
| Page | 51 |
| Line | 1 |

|  |  |
| --- | --- |
| Ref. | 020 |
| DRAFT SECTION | 4. Abbreviations and acronyms |
| Modification type | Add text |
| Text | MIAK media independent authentication key |
| Page | 5 |
| Line | 22 |

|  |  |
| --- | --- |
| Ref. | 021 |
| DRAFT SECTION | 9.2.1 MIH serviceaccessauthentication (line 64-65, page 35; line 1-4 page 36) |
| Modification type | Update text |
| Text | Figure 31 and Figure 32 illustrate the EAP authentication when it isstarted by the MN (MN initiated EAPauthentication) and when it is started by the network (networkinitiatedEAP authentication), respectively. In both figures, onlytheprotocol interface betweenan EAPpeer and an EAP authenticatorisdescribed. The interface within EAP server isnotincluded. The messages for MIH service access authentication are defined in 8.6.1.11, 8.6.1.12, and 8.6.1.13. The messages for termination are defined in 8.6.1.14 and 8.6.1.15.Similarly, Figure 33 illustratesthe ERP re-authentication in a MN initiated re-authentication case. Figure 34 and Figure 35 show anetworkinitiation ERP re-authentication, whenthe ERP re-authentication is started by sending an EAP Request/Identity or by sending ERP-Initiate/Re-auth-Start, respectively. |
| Page | 35 |
| Line | 64 |

|  |  |
| --- | --- |
| Ref. | 022 |
| DRAFT SECTION | 9.3.1 MIH\_Auth PDU protection procedure |
| Modificationtype | New section |
| Text | The MIH\_Auth messages are no protected using the MIH SA established after a successful Media Independent Service Access Authentication. They are only integrity protected by using an AUTH TLV and the MIAK derived from the MSK or rMSK(as described in section 9.2.2). When a MIAK is available, the MIH\_Auth messages must be protected with AUTH TLV.How the AUTH TLV is generated is shown in the following formula, which defines the different parameters needed.*AUTH TLV value = PRF(K, “AUTH\_TLV” | MIH\_Auth message| MNCiphersuite | PoSCiphersuite)*Parameters:* K: represents the MIAK (Media-Independent Authentication Key)
* MIH\_Auth message: represents the MIH\_Auth request /OR response to be protected including the AUTH TLV filled with 0s
* MNCiphersuite: represents the ciphersuite sent by the MN
* PoSCiphersuite: represents the ciphersuite sent by the PoS
* PRF function is one of the negotiated ones
	+ PRF\_CMAC\_AES
	+ PRF\_HMAC\_SHA1
	+ PRF\_HMAC\_SHA256

The PRF output length must be 128-bit. If the PRF output length is more than 128-bits, the 128 leftmost bits of the output must be used as the AUTH TLV value. |

|  |  |
| --- | --- |
| Ref. | 023 |
| DRAFT SECTION | 8.6.1.12 MIH\_Auth request |
| Modification type | Replace Auth TLV |
| Text | AUTH TLV |
| Page | 29 |
| Line | 12 |

|  |  |
| --- | --- |
| Ref. | 024 |
| DRAFT SECTION | 8.6.1.13 MIH\_Auth response |
| Modification type | Replace Auth TLV |
| Text | AUTH TLV |
| Page | 29 |
| Line | 42 |