|  |  |
| --- | --- |
| Project | **IEEE 802.21a** **<https://mentor.ieee.org/802.21>** |
| Title | 802.21a Issue List |
| DCN | **21-10-0187-08-0sec** |
| Date Submitted | **November 3, 2010** |
| Source(s) | Yoshihiro Ohba (Toshiba) |
| Re: | 802.21a Issue List |
| Abstract | This document contains summary of 802.21a issues |
| 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/opman/sect6.html#6.3) <[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)> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/faq.pdf> |

The following list is created from the following contributions as well as email conversations.

* 21-10-0171-00-0sec, 21-10-0079-02-0sec (WI#2 option II)
* 21-10-0078-04-0sec , 21-10-0120-03-0sec (WI-option-iii)
* 21-10-0123-01-0sec (WI#1 option A)
* 21-10-0172-00-0sec (Aug 17 teleconference minutes)
* 21-10-0174-00-0sec (Aug 31 teleconference-minutes)

Issues are not listed if they are recognized as non-issues after discussion.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Assignee | Description | Proposed Resolution | Status |
| 1 | Subir | MIH SA definition should cover both (D)TLS and EAP based key establishment. | MIH SA definition has been revised to cover both types of key establishment schemes. | Closed |
| 2 | Subir | There are redundant text about mutual authentication and its credentials. | * Definition on “TLS credential” was added.
* Definition on TLS Identity was removed.
* Redundant text was cleaned up.
 | Closed |
| 3 | Subir | Is maintaining a mapping between transport address and TLS session in the scope of 802.21a? | * Yes, it is in scope.
* Added one sentence “A Session TLV is defined [Clause XXX] to maintain the mapping.”
 | Closed |
| 4 | Subir | Service Id field should not be used to indicate that MIH security is used. | * Used one reserved bit to indicate MIH security.
* Removed AID for MIH security
 | Closed |
| 5 | Rafa | What are the ciphersuites  | * For confidentiality, AES-CBC, null
* For integrity, HMAC-SHA-96, CMAC-AES, null
* For confidentiality and integrity, AES-CCM
* For KDF, CMAC-AES, HMAC-SHA1
 | Closed |
| 6 | Rafa | The terms KDF and PRF+ are confusing. | * Replaced PRF+ with KDF.
* Added reference to RFC 5246 for KDF.
 | Closed |
| 7 | Rafa | MIH\_Capability\_Discover extension needs to have .request, .indicate, .response and .confirm primitives. | * Add the four primitives.
 | Closed |
| 8 | Rafa | Are the same random numbers used for generating MIEK, MIIK and MI-PMK? | * Yes.
* MI-PMK was removed and make MS-ROOT as a child of MSK/rMSK.
 | Closed |
| 9 | Rafa | How is MIH PDU protected with MIH-specific ciphering processed? | Detailed processing rule is provided. For encrypted message authentication, only MIEI is used. | Closed |
| 10 | Rafa | MIH\_Start\_Auth.request primitive generated by MIH user is used for sending an indication message. | Use of MIH\_Start\_Auth.request primitive to send MIH\_Start\_Auth indication message is ok.Needs some consideration on race condition (i.e., both MN and PoS initiates authentication simultaneously). | Closed |
| 11 | Rafa | MIH\_Start\_Auth and MIH\_Finish\_Auth primitives have both Source and Destination identifier. | One of the identifiers should be removed from each primitive. | Closed |
| 12 | Rafa | Extended MIH\_Capability\_Discover primitives do not have the attributes originally defined in 802.21-2008. | The security related attributes are only additions and the original capability attributes must be kept as it is. | Closed |
| 13 | Rafa | Are reactive key distribution messages MIH messages or not? | They are not MIH messages. Reactive key distribution call flow has been updated to distinguish them from MIH messaging. | Closed |
| 14 | Dapeng | Which IE container structures should be used, having a separate container for all security related IEs or add security related IEs to each existing container. | It is simpler and natural to add security related IEs to each existing container. | Closed |
| 15 | Dapeng | What are the data types for SuggestedNewLinkCandidateAuthenticatorList and PreferedCandidateAuthenticator? | PreferedCandidateAuthenticator data type is: LINK\_ADDRSuggestedNewLinkCandidateAuthenticatorList data type is: LIST(LINK\_ADDR) | Closed |
| 16 | Lily | For AES-CCM, what are the counter generation function and formatting function and what is the nonce generation rule?  | * Use counter generation and formatting functions defined in Appendix of NIST SP800-38C.
* Check 802.11 specification for nonce usage.
 | Text Needed |
| 17 | Dapeng | Detailed text is needed for MIH\_Pro\_Auth\_start. | Detailed text provided in DCN 123-02. | Closed |
| 18 | Dapeng | Is it true that MIH\_Pro\_Auth\_Start is the only primitive without extensions, such as .request, response, indication, and confirm? How to use this primitive? In which messages? |  Detailed text provided in DCN 123-02. | Closed |
| 19 | Dapeng | Detailed text is needed for MIH\_Pro\_Auth.request and .response. | Detailed text provided in DCN 123-02. | Closed |
| 20 | Dapeng | IE\_POA\_POS\_IP\_ADDR appears twice, i.e., in PoA specific IEs and PoS specific higher layer service IEs. | It should appear in PoS specific higher layer service IEs only. | Closed |
| 21 | Rafa | Several new data types are used without definition, such as KEY\_DIST, {INT,CIPH,KDF}\_ALG, ID\_OPT, INTREGRITY\_DATA, SESSION\_ID and KEY. | Detailed text provided in DCN 78-07. | Text Provided |
| 22 | Subir, Rafa, Dapeng | Are authentication messages defined as service management or command service? | Since authentication is related to all services, authentication messages are defined as service management. | Closed |
| 23 | Subir | Can all different authentication options (i.e, TLS, EAP and proactive EAP) be defined as a single message type or separate message types? | For the time being, define as separate messages.For TLS, use an indication message under service management category. | Closed |
| 24 | Rafa | .confirm primitive is missing in MIH\_Push\_Key and MIH\_Proact\_Pull\_Key. | Detailed text provided in DCN 78-07. | Text Provided |
| 25 | Rafa | What is session lifetime of MIH SA? | Define session lifetime parameter. Detailed text provided in DCN 78-07.  | Text Provided |
| 26 | Rafa | General message flow figure should be explicit about MIH\_Start\_Auth is an indication message.Also, MIH\_Auth request with “EAP-Succ” needs to be responded by MN with MIH\_Auth response message. | Revise the figure as follows:Add “indication” to MIH\_Start\_Auth message.Add MIH\_Auth response message below MIH\_Auth request (EAP Succ).Detailed text provided in DCN 78-07. | Revised Figure Provided |
| 27 | Rafa | Clarification is needed on Figure 16 of DCN 0078 “scenario using a PoA as a bridge” as to why the proposed approach is more suitable than PANA.  | Detailed text provided in DCN 78-07. | Revised Text Provided |
| 28 | Lily, Rafa | Capability discovery may not need to contain detailed ciphersuite parameters. | Detailed ciphersuite parameters will be included for MIH-specific ciphering for both capability discovery primitives and messages and MIH\_Auth messages (but not MIH\_Auth primitives). IEs for ciphesuite parameters also need to be defined. | Text Needed |
| 29 | Rafa/Lily | For MIIK and MIEK derivation, KDF is called twice. | Derive MIIK and MIEK from one KDF call.Lily to provide text. | Text Needed |
| 30 | Lily | Do we want to use all 512 bits for MSK and do we need to support only HMAC or CMAC?  | We should use HMAC-SHA1 or HMAC-SHA2 that does not need to truncate key before computing hash.802.11 uses HMAC-SHA-1 but uses only 256 bits of MSK before computing hash. This came from historic usage of MPPE-Recv-Key as PMK based on RFC2716 which is obsolete now. 802.16e uses CMAC or SHA-1 but it also truncate MSK before computing hash.So both 802.11 and 802.16 are not good practices for KDF. | Text Needed |
| 31 | Rafa | Is there any way both peers will know if there is a bundle or non-bundle case? | Text added to indicate that if the KeyDistMechList TLV is not present the bundle option is not going to be used. | Text Needed |
| 32 | Rafa/Dapeng | MIH\_Pro\_Auth primitives and MIH\_Auth primitives are semantically different but have similar structures. | Rafa will work with Dapeng to harmonize this. | Text Needed |
| 33 | Rafa/Subir | Can we move P and F- bits by defining a generic security TLV? | * Bit P is represented on position 0 in RESERVED2 field in MIH Header.
* Bit F is replaced by adding a STATUS TLV in MIH\_AUTH.
 | Text Needed |
| 34 | Subir/Rafa/Fernando | A new Security TLV should be used for both TLS-based ciphering and MIH-specific ciphering. | A generic TLV: SECURITY TLV must be defined on subir’s proposal instead of TLS TLV to merge both proposals in order to use MIHS header. | Text Needed |