|  |  |  |
| --- | --- | --- |
| Project | **IEEE 802.21m Media Independent Services Framework: 802.21-2008 Revision Project** | |
| Title | **Differences in 802.21m definitions between Sep. 2013 and Jan. 2014** | |
| DCN | **21-14-0022-00-REVP-Definitions-Diff-Sep2013-Jan2014** | |
| Date Submitted | **January 22, 2014** | |
| Source(s) | Farrokh Khatibi,  Charles Perkins | Voice:+1 408-330-4586  Mailto: charliep@computer.org |
| Abstract | This document displays differences between definitions in 21-13-0210-03-REVP-802.21-2008\_include (January 2014) compared to the original definitions in 802.21-2008, 802.21a, and 802.21b Microsoft Word files, as received from IEEE document support in September 2013 | |
| Purpose | To elicit approval for the revised definitions | |
| 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 802.2 may make this contribution public. | |
| Patent Policy | The contributor is familiar with IEEE patent policy, as outlined in [Section 6.3 of the IEEE-SA Standards Board Operations Manual](http://standards.ieee.org/guides/opman/sect6.html#6.3) <<http://standards.ieee.org/guides/opman/sect6.html#6.3>> and in *Understanding Patent Issues During IEEE Standards Development* <*http://standards.ieee.org/board/pat/pat-material.html* >. | |

This document displays differences between definitions in 21-13-0210-03-REVP-802.21-2008\_include (January 2014) compared to the original definitions in 802.21-2008, 802.21a, and 802.21b Microsoft Word files, as received from IEEE document support in September 2013.

**authenticated encryption**: An algorithm to convert plaintext data to ciphertext and generate a message authentication code with a cryptographic key as a parameter to provide confidentiality, integrity, and authen- ticity of the data. See also: encryption; MIC algorithm.

**authentication process**: A process to assure that the claimed identity belongs to the entity. It is also called entity authentication. In this standard, an access authentication is an entity authentication with the identity used to access a specific network or a media independent service (MIS).

**authentication server**: A server used for authentication purposes. When EAP is used as an authentication protocol, the authentication server is an EAP server.

**authenticator**: A network entity to execute EAP with a MN called a peer. An authenticator can use a backend server to conduct EAP execution. Syn: EAP authenticator.

**bidirectional network**: A general communication network providing bidirectional transmission such as 802.3, 802.11, 802.16, 3GPP and 3GPP2.

**candidate authenticator**: An authenticator that is associated with a candidate PoA. candidate network: A network that is a potential target to the MN's movement candidate PoS: A potential PoS that can serve the MNs after movement.

**candidate point of attachment (candidate PoA)**: A point of attachment (PoA) under evaluation to which the link may be switched.

**decryption**: An algorithm to convert ciphertext of data to plaintext with a cryptographic key as a parameter. It is an inverse operation of encryption.

**downlink-only (DO) network**: A broadcasting network providing unidirectional transmission from the PoA to the user device, such as DVB, T-DMB and ATSC-M/H.

**dual-radio operation**: In this mode a dual radio device can receive and transmit simultaneously on both the radios. See also: single-radio operation.

**EAP authenticator**: See: authenticator.

**EAP peer**: The entity that responds to the EAP authenticator.

**EAP Re-authentication**: An authentication protocol using a key established in a previous EAP execution as defined in IETF RFC 5296.5

**EAP Server**: The entity that terminates the EAP execution with the EAP peer. In the case where no back- end authentication server is used, the EAP server is a part of the EAP authenticator. In the case where a backend authentication server is used, the EAP server is located on the backend authentication server.

**encryption**: An algorithm to convert plaintext data to ciphertext to provide confidentiality with a crypto- graphic key as a parameter.

**extensible authentication protocol (EAP)**: An access authentication framework specified in IETF RFC 3748. It can support different authentication methods, called EAP methods.

**home subscriber network**: Network managed by an operator with whom the subscriber has a business relationship (subscription). See also: visited network; serving network.

**link**: A communication channel through which nodes communicate for the exchange of L2 protocol data units. Each link is associated with two endpoints and has a unique identifier.

**link indication**: Link state information provided by the link layer to higher layers.

**link layer**: Conceptual layer of control or processing logic that is responsible for maintaining control of the data link. The data link-layer functions provide an interface between the higher-layer logic and the data link.

**link switch**: The process by which a MN changes the link that connects it to the network. Changing a link implies changing the remote link endpoint and therefore the point of attachment of the MN.

**link**:**lower layers**: The layers located at OSI Level 2 and below across different link-layer technology standards supported by this standard. For example, the IEEE 802.11 Lower Layers are the MAC sublayer and the PHY, while the 3GPP Lower Layers are L1/MAC/radio link control (RLC)/packet data convergence protocol (PDCP) in the case of wideband code division multiple access (W-CDMA) frequency division duplex (FDD)/time division duplex (TDD), L1/LAPDm in the case of GSM CS, and L1/MAC/RLC in the case of general packet radio service (GPRS)/ Enhanced GPRS (EGPRS), respectively. The term “Lower Layers” also includes Logical Link Control Layers such as IEEE 802.2 Logical Link Control (LLC) or 3GPP Radio Link Control (RLC). The MISF uses the services provided by these layers.

**media independent service (MIS) discovery protocol**: A protocol for discovering media independent service (MIS) entities.

**media independent service (MIS) network entity**: Network entity with at least one media independent service function (MISF).

**media independent service (MIS) node**: An entity providing a MISF (MN or network).

**media independent handover (MIllservice (MIS) non-PoS**: An MIS network entity that can directly exchange MIS messages with other MIS network entities but cannot directly exchange MIS messages with any MIS enabled MN.

**media independent service (MIS) transport protocol**: A protocol for transporting MIS protocol messages between a pair of MIS entities.

**media independent service (MIS) users**: Entities that use the services provided by the MISF. MIS users use the MIS\_SAP to interact with the MISF.

**media independent service function (MISF)**: A function that realizes media independent service.

**media independent service function (MISF) pairing**: The communication relationship that exists between different MISF instances when they exchange MIS messages.

**media independent service function (MISF) transaction**: A combination of an MIS Request message and MIS Response message, MIS Indication, or MIS Response message and any associated MIS Acknowledgement messages.

**media independent point of service (MIS PoS)**: Network-side MISF instance that exchanges MIS messages with an MN-based MISF. The same MIS Network Entity includes an MIS PoS for each MIS-enabled MN with which it exchanges MIS messages. A single MIS PoS can host more than one MIS service. The same MIS Network Entity can include multiple MIS Points of Service that can provide different combinations of MIS services to the respective MNs based on subscription or roaming conditions. Note that for a network entity comprising multiple interfaces, the notion of MIS PoS is associated with the network entity itself and not with just one of its interfaces. For MIS service access authentication, a PoS serves as an authenticator. Moreover, when a service access authentication establishes keys for proactive authentication, a PoS provides key distribution service for media specific authenticators.

**media specific authentication server**: An authentication server used for media specific access authentication.

**media specific authenticator**: An authenticator used for a media specific network access authentication.

**media specific network access authentication**: An authentication protocol for media access purpose specified for a specific media access. It may establish keys to be used in media specific protection mechanisms.

**media specific protection mechanism**: A mechanism that is applied to media specific layers to protect the data traffic using an encryption algorithm, an integrity protection algorithm, an authenticated encryption algorithm, or a combination of an encryption algorithm and an integrity protection algorithm.

**message authentication code (a.k.a. message integrity code)**: A data string generated over a message with a symmetric key by an algorithm, called message authentication code algorithm. It is used to verify the integrity of the message and to authenticate the origin of the message.

**message authentication code algorithm**: An algorithm to generate a message authentication code on a data message with a symmetric key to provide integrity protection and message origination authentication. See: message authentication code.

**message integrity code (MIC)**: See: message authentication code.

**MIS security association (SA)**: An MIS security association is a set of cryptographic attributes established between the peer MIS entities for protecting MIS messages at the MIS protocol layer. An MIS SA is established via TLS handshake or EAP execution, where both the TLS handshake and EAP execution take place over the MIS protocol. When an MIS SA is established via TLS handshake, the TLS master key and its child keys, TLS random values and the TLS cipher suite negotiated in the TLS handshake are a part of the MIS SA. When an MIS SA is established via EAP execution, an MSK or rMSK and its child keys, MIS random values and the MIS cipher suite negotiated between the peer MIS entities are associated with the MIS SA.

**MIS access authentication**: An authentication process that authorizes the access to media indepen- dent services.

**MIS access authentication server**: An authentication server used to execute the MIS service access authentication

**mobile node (MN)**: Communication node that can change its point of attachment from one link to another.

**multimedia program (MMP)**: An instance of certain content (e.g., voice, data or video) with some specific attributes, e.g., chapter 2 of a TV series.

**multimedia service (MMS)**: A sequence of MMPs under the control of a content aggregator and provider, e.g., TV Channel One, TV Channel Two, etc.

**network detection**: The process by which a MN collects information on networks in its locality, identifies the different points of attachment, and ascertains the validity of link-layer configuration.

**network entity**: A communication node inside the network.

**network neighborhood**: The area of interest in which the network discovery and selection entity seeks to determine the available coverage of a wired/wireless network with identical or different link-layer technologies.

**network point of attachment (network PoA, or PoA)**: The network side endpoint of a layer 2 link that includes a MN as the other endpoint. See also: candidate PoA; serving PoA; target PoA.

**network selection**: The process by which a MN or a network entity makes a decision to connect to a specific network (possibly out of many available) based on a policy configured in the MN and/or obtained from the network.

**network selector**: The entity that undertakes the network selection decisions..

**operator identifier (operator ID)**: An identifier of the access or core network provider.

**PICS Proforma**: A normative document to express in compact form the static conformance requirements of a specification. As such, it serves as a reference to the static conformance review.

**proactive authentication**: A media specific authentication with a candidate network executed via the serving network.

**protection mechanisms for MIS messages**: A protection mechanism that is applied to MIS PDU using an encryption algorithm, an integrity protection algorithm, an authenticated encryption algorithm, or a combi- nation of an encryption algorithm and an integrity protection algorithm.

**security association identifier (SAID)**: An identifier of an MIS security association. When an SA is estab- lished through TLS, it is the TLS session ID. When an SA is generated through an EAP execution, it is assigned by the authenticator and the ID value is an octet string unique for a pair of MIS functions.

**serving authenticator**: The authenticator which is associated with the serving PoA.

**serving network**: A network that provides services to the user. The serving network can be a home subscriber network or a visited network. See also: visited network; home subscriber network.

**serving point of attachment (serving PoA)**: The PoA of the current link being used by the MN.

**serving PoS**: An MIS PoS that is currently providing a media independent service to the MN.

**single-radio operation**: In this mode, a dual radio device can receive and transmit on only one radio at a time. This is usually the mode of operation when radio frequencies of the two radios are close to each other (e.g., in IMT 2000 bands). See also: dual-radio operation.

**static conformance requirement**: One of the requirements that specify the limitations on the combinations of implemented capabilities permitted in a real open system, which is claimed to conform to the relevant specification(s).

**static conformance review**: A review of the extent to which the static conformance requirements are claimed to be supported by the system under test, by comparing the answers in the implementation conformance statement(s) and the system conformance statement with the static conformance requirements expressed in the relevant specifications.

**target point of attachment (target PoA)**: A candidate PoA that has been selected to become the new serving PoA.

**uniform resource identifier (URI)**: A compact sequence of characters that identifies an abstract or physical resource including video.

**visited network**: A network managed by an operator other than the subscriber’s home operator and in which the subscriber is receiving service. See also: home subscriber network; serving network.