IEEE P802.21
Media Independent Handover Services

|  |
| --- |
| Requirements Document for TGd |
| Date: 2012-07-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Antonio de la Oliva | UC3M | Avda. Universidad 30,28918, Leganes, Madrid |  | aoliva@it.uc3m.es |
| Daniel Corujo | ITAv | Campus Univesirátio de Santiago, 3810-193 Aveiro, Portugal | +351 234 377 900 | dcorujo@av.it.pt |
| Carlos Guimaraes | ITav | Campus Univesirátio de Santiago, 3810-193 Aveiro, Portugal | +351 234 377 900 | cguimaraes@av.it.pt |

Abstract

This document summarizes the TGd requirements as derived from the PAR and from analyzing the TGd use cases.

# Introduction

This document defines requirements for solutions addressing functionality to be provided by the TGd amendment.

Apart from setting functional requirements, this documents specifies performance requirements and constrains for solutions addressing functionality to be provided by the TGd amendment.

## Scope

The scope for deriving requirements is set by the P802.11d PAR [1], as well as by the TGd use case document [2].

## Definitions, acronyms, and abbreviations

**Authentication:** A process that establishes the origin of information or determines an entity’s identity. [6]

**Non-repudiation**: A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (i.e., the signatory). [3].

**Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [4] [5].

**Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [4] [5].

**Availability**: Ensuring timely and reliable access to and use of information. [4][7].

## References

[1] IEEE 802.21d PAR. http://www.ieee802.org/21/802\_21d\_PAR.pdf

[2] https://mentor.ieee.org/802.21/dcn/12/21-12-0090-01-MuGM-use-case-reference-for-tgd.docx

[3] FIPS PUB 186-3: Federal Information Processing Standards Publication, Digital Signature Standard (DSS), June 2009.

[4] 44 U.S.C., SEC 3542: United States Code, 2006 Edition, Supplement 3, Title 44 - PUBLIC PRINTING AND DOCUMENTS (<http://www.gpo.gov/fdsys/pkg/USCODE-2009-title44/pdf/USCODE-2009-title44-chap35-subchapIII-sec3542.pdf>)

[5] FIPS PUB 199: Federal Information Processing Standards Publication, Standards for Security Categorization of Federal Information and Information Systems. February 2004.

[6] NIST Special Publication 800-21, Guideline for Implementing Cryptography In the Federal Government, December 2005.

[7] FIPS PUB 200: Federal Information Processing Standards Publication , Minimum Security Requirements for Federal Information and Information Systems, March 2006.

# Requirements

## Functional requirements [What the system shall do]

### Multicast Communication

 [Req2.1.1.1] The TGd amendment shall support multicast communication between a PoS, source of a multicast tree, and a group of nodes.

### Addressing

[Req2.1.2.1] The TGd amendment shall provide an addressing mechanism suitable for identifying the group.

### Multicast Transport

[Req2.1.3.1] The TGd amendment shall provide mechanisms for the MIHF to deliver information in a multicast way.

[Req2.1.3.1] The TGd amendment shall rely on already established L2, L3 or application layer multicast mechanisms to perform the multicast transport.

### Group Management

[Req2.1.4.1] The TGd amendment shall provide functionalities for managing groups of nodes. These functionalities include the creation/destruction of groups, join and leave operations and modifications to the group subscription.

### Security Requirements

[Req2.1.5.1] The TGd amendment shall provide mechanisms to perform authentication, confidentiality and integrity protection at the receiving node.

[Req2.1.5.2] The solution shall provide key management mechanisms.

## Performance requirements [How well the requirements should perform]

### Transparency to MIH Users

[Req2.2.1.1] The TGd amendment shall provide transport solutions transparent to the MIH User. The fact of using a multicast channel shall be transparent to the MIH User.

### Reduced signaling

[Req2.2.2.1] The TGd amendment shall provide mechanisms for group management incurring on lower overheads compared with unicast group management solutions.

### Scalability

[Req2.2.3.1] The mechanisms proposed in the TGd amendment shall scale from low to high capacity (in terms of computational power) devices.

[Req2.2.3.2] The mechanisms proposed in the TGd amendment for the transport of primitives, shall scale with the number of nodes.

## Constraints – [e.g. Technology, design, tools, and/or standards]

### Backward compatibility

[Req2.3.1.1] The TGd amendment shall be compatible or supersede the zero length MIHF\_ID behaviour

[Req2.3.1.2] The TGd amendment shall be compatible or supersede IEEE 802.21b mechanisms of group management.

[Req2.3.1.3] The TGd amendment shall minimize the changes introduced in the standard IEEE 802.21 protocol state machine and should clearly identify the IEEE 802.21 primitives allowed to be used in a multicast way.

# Multicast features and attributes

**(M: mandatory, O: optional, N: not supported)**

|  |  |
| --- | --- |
| **Functionality** | **Level of requirement** |
| PoS to MN multicast | M |
| PoS (or MIH non-PoS) to PoS multicast | O |
| MN-sourced multicast | N |
| Multicast Sub-groups | N |
| Multiple multicast domains | N |
| Handling of duplicate multicast MIH data | M |
| Authentication [6] | M |
| Data Integrity [4] [5] | M |
| Confidentiality [4] [5] | O |
| Availability [4] [7] | ? |
| Key management | M |

Note: Optional in previous table means “Optional to use” but the solution must provide this functionality.