IEEE P802.21.1  
Media Independent Services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Remedy and Response for Comments #106, #107, #108 and #109 of the WG LB9 on IEEE P802.21.1/D01 draft | | | | |
| Date: 2016-02-05 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Lidong Chen | NIST | 100 Bureau Dr. Gaithersburg, MD 20898, USA | (301) 975-6974 | llchen at nist dot gov |

Abstract

This document contains proposed resolution for comments #106, #107, #108, and #109 of the WG LB9 on IEEE P802.21.1/D01 draft based on the LB9 comments file (DCN: 21-16-0008-04-SAUC).

# This is to suggest removing Clause 5.14 Proactive authentication from IEEE 802.21.1 for the reasons discussed in this contribution.

## 1. Clause 5.14 has a serious security issue

Clause 5.14 specifies a "chaining trust model" from one SPoS to next TPoS1, TPoS2, ….. Basically, SPoS will generate a key K1 and distribute it to TPoS1 and MN. K1 is used to protect the interface between TPoS1 and MN. Then TPoS1 will generate a key K2 and distribute it to TPoS2 and MN. Notice that the interface between TPoS1 and MN is protected by a key derived from K1. In this long chain, if one of the PoS is compromised, then the rest of the chain is brocken. This is very typical domino effect and should be avoid in the security design.

The comment #108 is to point this issue.

## 2. Clause 5.14 introduces inconsistencies with 21m

Even though clause 5.14 is titled "proactive authentication", it really is about establishing security associations between MN and TPoS, which is covered by Clause 9 of IEEE 802.21m Rev D01. The specified method is different from 21m and has security issues as we mentioned above.

Based on the specification of 21m, the security association between an MN and a TPoS can be established through EAP (in case of no partnership) or ERP (in case of partnership). If SPoS is involved, the interface between the MN and the SPoS is protected by the current MIS protection. The equation Payload = TPoSIdentifier, Nonce-N, [*K* ⊕ PRFSPoS (TPoSIdentifier, Nonce-N)] is unnecessary and incorrect even a key K were distributed, because it is protected through MIH security association with a well defined ciphersuite. It shall never be protected by such a "naïve" stream cipher. (At the time, comment #108 were submitted, the commenter does not understand the notations, which are not defined. See comment #106.)

The same naïve stream cipher is also used to protect the interface between SPoS and TPoS (comment #107). The interface between SPoS and TPoS can be protected by either MIH security association with a well defined ciphersuite , established using the method specified in clause 9 of 21m or transport layer protection as specified in Annex N of 21m. There is no need to define them here.

**3. Clause 5.14 is problematic and adds no value but harm to 21.1**

The aforementioned security issues and inconsistencies would the quality of 21.1 questionable.

MIH supported proactive authentication is specified in Clause 10 of IEEE 802.21m Rev D01. In 21m, it considers different situations between MIH service and media specific access. In particular, it covers the situation where MIH just provides a tunnel for the control signals to reach the target network without assuming any specific relationship of messa service provider with MIH service provider (see clause 10.1, Figure 80 and Figure 81). There is no need to specify proactive authentication for single radio handover. In fact, Clause 5.14 does not handle proactive authentication at all.

**4. Action items**

After removing clause 5.14, the other portion of single radio handover shall be checked to make sure that any reference to clause 5.14 is handled. It can refer to 21m clause 9 for MIH protection and clause 10 for proactive handover. The key distribution messages must be removed as well because they are not necessary.