IEEE P802.21.1
Media Independent Services

|  |
| --- |
| Proposed text change for 5.14 based on Remedy 1 for Comments #106, #107, #108 and #109 of the WG LB9 on IEEE P802.21.1/D01 draft |
| Date: 2016-02-19 |
| 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 text changes for Clause 5.14 based on remedy 1 proposed in 21-15-00-0036-00-SAUC to resolve 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).

**5.14 PoS facilitated proactive authentication for single radio handover service**

The PoS is a convenient and natural place to locate security services, and roaming partners have in place agreements that can be used to beneficially establish the needed security agreements between different PoS modules in partner networks.

**5.14.1 Establishing MIS Security Association between roaming partners**

It is expected that the PoS functions in partner networks must often communicate by data paths that traverse the external Internet; in such cases, a secure communication channel must exist or must be established between the partners. It is out of scope for this document to specify exactly how the secure communication channel should be established, but this can be done by configuration when the partners enter into their roaming agreement. It can also be done on demand by using IKEv2 (RFC 7296) [B36]. The following overview describes in more detail the circumstances enabling dynamic establishment of security association between the SPoS and the TPoS.



1. **—MN handover signaling for preregistration using SPoS.**

MIS\_Prereg\_Xfer and MIS\_N2N\_Prereg\_Xfer messages exchanged between the SPoS and the TPoS may require security protection. Furthermore, the TPoS may reject these messages from an unauthorized source network PoS. To protect the link between the SPoS and the TPoS, several approaches are possible.

An MIS SA (Security Association) (see 8.4.2 of IEEE Std 802.21-XXXX) can be used for protecting the communications between an SPoS and a TPoS. In this case, the SPoS acts as the initiating end-point of an MIS SA and a TPoS as the other end-point of the MIS SA. The MIS SA can be established using (D)TLS over MIS or EAP over MIS (see 9.2 of IEEE Std 802.21-XXXX).

Other mechanisms for providing message integrity and confidentiality, such as IPSec and TLS over TCP, can also be used for protecting the communications between SPoS and TPoS.

Except for the initial network attachment, by the time an MN enters a network, it can also have a security relationship with the PoS in that network by using MIS\_Prereg\_Xfer commands. For each newly visited network, this security relationship can be created on demand, enabled by signaling from another PoS. The PoS creating the visited security relationship can either be the MN's home PoS (HPoS, a PoS in MN's home network) or the PoS in the network previously visited by the MN. When the MN first attaches to one of the partner networks of the roaming partners, it is either the MN's home network or a visited network. If the first attachment is to the MN's home network, the MN is expected to already have a security association with HPoS; otherwise, the MN can bootstrap this security association with the assistance of the HPoS, IKEv2, standard AAA mechanisms, or other proprietary means.

After initial attachment, there is signaling defined so that at all times the MN has a security association with the PoS in the network at its current point of attachment, i.e., the SPoS. As the MN moves from one partner network to the next target network, the MN establishes or renews a security association with the PoS in the target network, i.e. the TPoS. When handover is completed, the TPoS ~~naturally~~ begins to play the role of the MN’s serving PoS, and subsequently when a handover is required the TPoS plays the role of the SPoS.

In order to enable a wider application of handovers and in particular preregistration signaling, security must be guaranteed for the control traffic. As described above, this signaling traffic is mediated by the PoS in each target network, which may be unknown to the MN until the need for handover has been determined. In such cases, for secure signaling, the MN needs to establish a security association with the TPoS. In Clause 9 of Draft IEEE IEEE Std 802.21-XXXX, an MIH SA can be established through (D) TLS or EAP. The methods specified there shall be used to establish an MIH SA between an MN and a TPoS so that TPoS can provide security service, in particular, can facilitate proactive authentication for an MN in a handover event. For single radio handover, an optimized MIH SA establishment mechanism is introduced to speed up when the home networks of SPoS and TPoS have an existing trust relationship through partnership agreement.

**5.14.2 Optimized MIH SA establishment for single radio handover service**

This clause specifies one optimized MIH SA establishment for single radio handover service. It allows a TPoS to obtain a key derivation key *K* from SPoS or from a higher level entity. The key derivation key *K* is then used to derive other keys such as the media independent session key (MISK) as described in 9.2.1 of IEEE Std 802.21-XXXX between the MN and the TPoS, enabling further secure preregistration activities.

Because of previous protocol operations (e.g., derivation of MIAK upon arrival in the source network), the MN has a current security association with the SPoS. As discussed in 5.14.1, the protection mechanisms applied between SPoS and TPoS are out of the scope of this specification. If the key *K* is distributed by SPoS to MN and to TPoS, the key distribution is protected by MIH SA between MN and SPoS and by out of scope mechanisms between SPoS and TPoS.

In order to establish an SA between the MN and the TPoS, they need to exchange Nonce-N and Nonce-T through messages MIS\_Prereg\_Xfer Request and MIS\_Prereg\_Xfer Response. They also need to agree on a cipher suite coded as c. With the information, MN and TPoS can derive the media independent session key (MISK) as specified in 9.2.1 of IEEE Std 802.21-XXXX.

Note:

1. The optimized MIH SA establishment is allowed only when a trust relationship has established between the network domains of SPoS and TPoS. It shall fall back to an SA establishment mechanism as specified in IEEE Std 802.21-XXXX whenever it is possible, or if any of the MN or TPoS requests so.
2. If protocol of establishing SAs between an MN and a TPoS is EAP, the optimized MIH SA etsblishment applies. In this case, the MN and the TPoS use key derivation key *K* as it is obtained through an EAP or ERP execution.
3. If protocol of establishing SAs between an MN and a TPoS is TLS, then the optimized SA establishment method does not apply, because the MN and the TPoS cannot use key derivation key *K* in TLS.
4. If any SPoS is compromised, the generated key *K* is compromised and so is the remaining of the PoS chains assuming that a TPoS will become a SPoS. To prevent such domino effect, the chain shall be limited. That is, after certain number of executions of the optimized SA establishment, it shall force an SA establishment through the methods specified in 21m.

**5.14.3 TPoS selection by the SPoS**

It is possible for the SPoS to take a more active role to promote smooth handover. When the MN determines the need for handover, but does not already know the address of the TPoS for the intended target network, the MN can start the preregistration sequence by sending all the known information to the SPoS. If the SPoS has access to information about each surrounding network and information about the MIS PoS in each such surrounding network, the SPoS can make a determination about which target network may best be able to provide connectivity and service to the MN. This also depends on the SPoS having access to location and configuration information about the MN—for example which radio access technologies (RATs) are configured for operation on the MN. When the candidate TPoS is in another operator’s network, it may be also important that the SPoS should have a security relationship with a candidate TPoS in order to avoid interference from malicious nodes. This would typically mean that the operators are also roaming partners.

Subsequently, the SPoS will provide the address of the TPoS to the MN along with *K*, as described above. The exact nature of the information about TPoS provided by the MN is dependent on the radio access technology type (RAT) of the target network and is outside the scope of this document.

*Add following Table to Draft IEEE P802.21.1/D01.*

**Table** Error! No text of specified style in document.**.1—Data type for security**

|  |  |  |
| --- | --- | --- |
| **Data type** | **Derived from** | **Definition** |
| ID\_TYPE | EUMERATED | The type of security association.0: TLS-generated;1: EAP-generated;2: GKB-generated;3: SPoS-generated |