802.1af Key Hierarchy Options

Joseph Salowey

Cisco Systems

jsalowey@cisco.com

Contents

1 Overview

1.1 802.1af Key Hierarchy

The ultimate goal of the 802.1af key hierarchy is to generate security association keys (SAKs) for use within 802.1AE (MACSEC) protection from the keys output from an EAP method which has executed between the EAP-peer on the supplicant and an authenticator that is providing access to the key material necessary for obtaining the correct CAK for a particular CA. One major step in this process is the generation and distribution of the connectivity association key (CAK). A CAK may be a point-to-point (PTP-CAK) association which consists of just two parties or it may be a group CAK (GRP-CAK) that can be used to protect traffic between multiple parties. A group key needs to be distributed using a key encrypting key (CAK-KEK) whereas a PTP-CAK may be distributed using a KEK or through direct key derivation. A pairwise association can be modeled as a special case of a group association so it may not be necessary to differentiate between these two cases. Since there are some differences between the two cases we will treat them as separate to see if any simplifications or optimization in some cases can be made.

In addition there currently is no confirmation that both the authenticator and supplicant have received the same keys from the EAP authentication. Since the authenticator may be physically separated from the authentication server which derives the key it would be desirable to provide key confirmation within the EAPoL exchange to verify that supplicant and authenticator agree upon the cryptographic state. A key confirmation key (KCK) may be derived for this purpose.

As with other key hierarchies the 802.1af hierarchy is designed to provide cryptographic separation between keys at the same level of the hierarchy, to prevent the knowledge of child keys from disclosing information about their parents and to prevent the reuse of a key in multiple contexts. In general, the 802.1af-CAK hierarchy should be cryptographically separated from the 802.11 key hierarchy.

Figure 1 shows an overview of the 802.1af hierarchy. A solid line indicates key derivation where the child keys are derived directly from their parents using a one way function. A dashed line indicates that child keys are generated and then transported protected under the parent key encrypting key (KEK). Once the CAK (pairwise or group) is selected then a key hierarchy showing the derivation from CAK to SAKs is needed. This figure shows a difference between the group and point-to-point hierarchies. This differentiation is not necessary in some of the options described in the following sections.

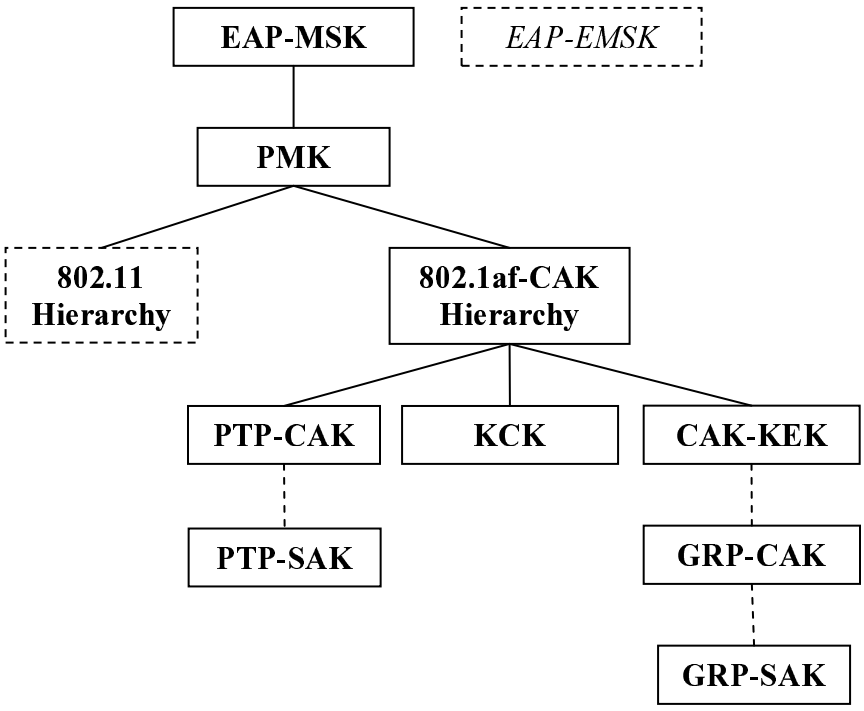

Figure 1 - 802.1af Key hierarchy Overview

2 Derivation of the 802.1af Key Hierarchy

The following sections describe the derivation of the 802.1af key derivation hierarchy. The first section makes a recommendation on the derivation of the PMK from the EAP

key material. The following sections describe several options for deriving the rest of the key hierarchy.

2.1 Derivation of the PMK

The pairwise master key (PMK) is derived from the output of the EAP exchange. Specifically, the PMK is taken as the first 256 bits (bits 0-255) of the EAP-MSK. The use of the remaining 256 bits of the EAP-MSK is reserved and not used in this specification. This specification also does not currently make use of any keys derived from the EAP-EMSK. This derivation of the PMK is consistent with the derivation for the PMK in 802.11i.

The PMK is named the same way as in 802.11i and the definition is given below:

A PMK identifier is defined as

PMKID = HMAC-SHA1-128(PMK, "PMK Name" || AA || SPA)

Here, HMAC-SHA1-128 is the first 128 bits of the HMAC-SHA1 of its argument list.

2.2 CAK Distribution Options

The following sections outline some distribution options for the CAK.

2.2.1 802.11i Approach

This section describes an approach which provides maximum reuse of 802.11i. In the pairwise case it is basically the same as 802.11i and in the group case the CAK is distributed in the same manner as the GTK in 802.11i. The basic key hierarchy is given in Figure 2.

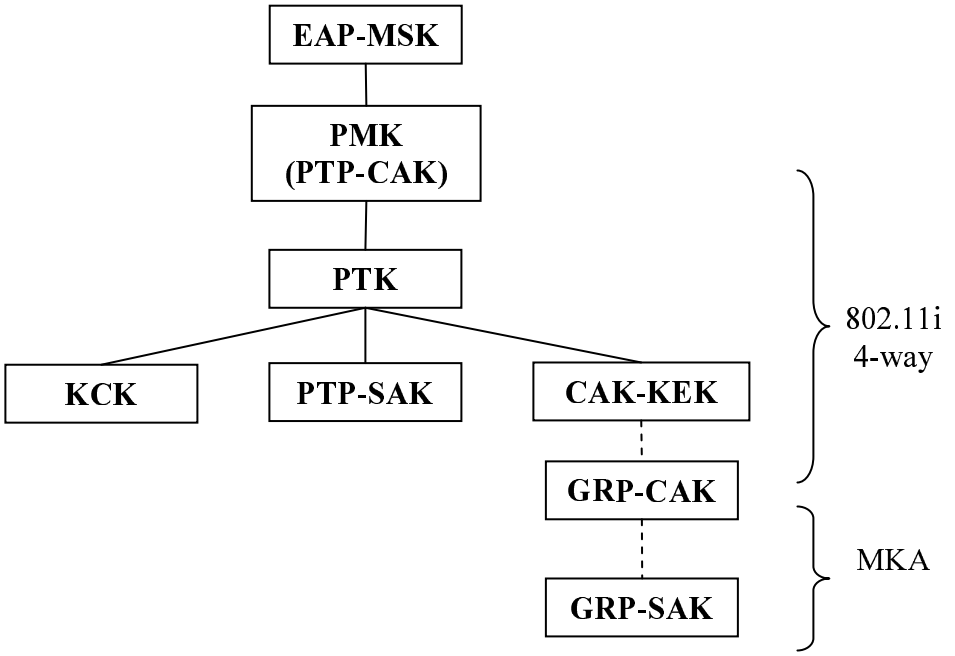

Figure 2 - 802.11i Centric Approach

This approach is highly asymmetric between the pairwise point-to-point case and the group multi-point case. In this approach the PMK is treated as a PTP-CAK in that it is used directly to derive PTP-SAK for use in 802.1AE through the 4-way handshake. If it is desired to use a group CAK instead then the authenticator may distribute a group CAK during the 4-way handshake. Re-keying for the point-to-point case would be handled through the use of the 4-way handshake and re-keying in the group case would be handled through a special MACSEC key agreement (MKA) protocol.

One advantage of this approach is that it is possible to reuse much the 802.11 specification and possibly the 802.11 implementation. This could also make it possible to reuse much of the security analysis and NIST evaluation done for 802.11 especially in the point-to-point case. The approach provides separation between the 802.11i hierarchy and the 802.1af hierarchy. This could allow the same PMK to be used as an 802.11i PMK and an 802.1af PTP-CAK. The 4-way handshake also provides for key confirmation and a well defined way to insert external data integrity protected which allows for binding to the key exchange.

The disadvantage to this approach is that there is a strong asymmetry between the point-to-point case and the group case. Implementers are forced to implement both the 802.11i 4-way handshake and MACSEC key agreement protocol to derive SAKs. In addition the re-keying protocol is different in both cases so it essentially requires a point-to-point mode and a group mode.

2.2.2 802.11i Group Only Approach

In the 802.11i group only approach the PTP-CAK case is removed and everything is treated as a group with the point-to-point case being a degenerate group case. This simplifies the key hierarchy as shown in Figure 3.

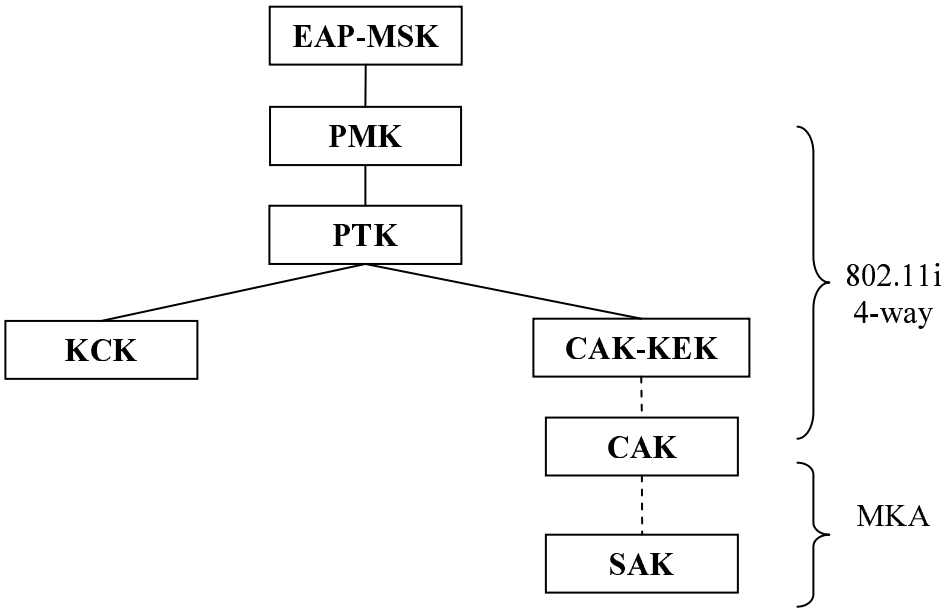

Figure 3 - 802.11i Group Only Approach

This case is more symmetric with respect to the point-to-point and multipoint cases. The CAK is always distributed through the 4-way handshake. The re-key and SAK derivation are always done through MKA. An advantage here is that there may not need to be any differentiation between the point-to-point case and the group case.

This approach still has the advantage that much of the 802.11 4-way handshake is used which may help in specification and implementation. The approach provides separation between the 802.11i hierarchy and the 802.1af hierarchy. Caching of the PMK could still be done, however it is more likely that the CAK would be more useful to cache in the 802.1af case. The 4-way handshake also provides for key confirmation and a well defined way to insert external data integrity protected which allows for binding to the key exchange.

This approach still has the disadvantage of having to implement 802.11i 4-way handshake and MKA. In addition since MKA is used during SAK generation and re-key it may require additional FIPS evaluation.

2.2.3 MKA Only Approach

It may be possible that MKA could be used to distribute the CAK. In this approach the pairwise CAK for MKA (PMK-MKA) is derived directly from the PMK. Since MKA is in the progress of being it is a little hard to describe in detail how this would work. Since the 4-way handshake is not used, care is required to ensure that this usage of the PMK to derive the PMK-MKA does not conflict with other uses of the PMK. The hierarchy may look something like the following in Figure 4.

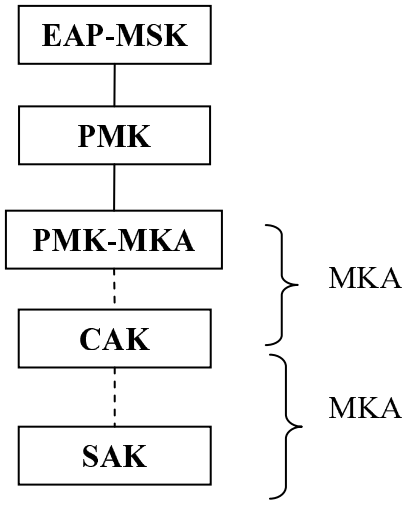

Figure 4 - MKA Only Approach

This case provides simplicity in that MKA is the only scheme used, however it is difficult to know if there will be differences in the MKA protocol between the pairwise case and the group case. In the MKA only case there is no confirmation that both parties have possession of the correct PMK before the MKA protocol starts.
This approach limits what can be done within 802.1X EAPoL since there is no pairwise key established for key confirmation within EAPoL. In addition the use of the PMK would have to be examined carefully to ensure it does not conflict with other uses and that fresh keys can be derives.

2.2.4 Abbreviated Handshake Group Case

Using an alternative mechanism to the 4-way handshake to derive the CAK-KEK may have advantages. This mechanism could possibly be similar to MKA executed within EAPoL frames. Care would be necessary to ensure that this usage of the PMK does not conflict with other uses of the PMK. The hierarchy in this case is shown in Figure 5.

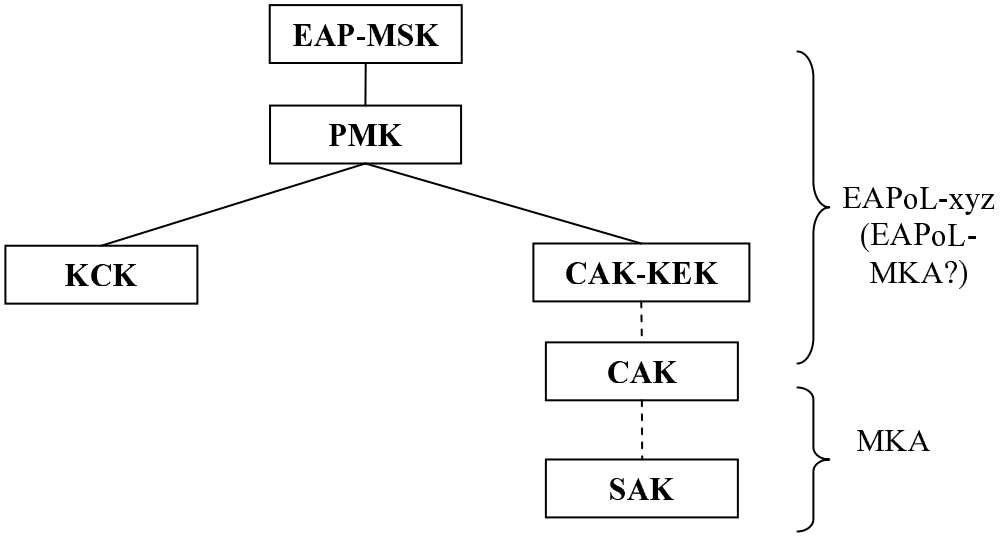

Figure 5 - Abbreviated Group Only Approach

The message exchange can provide key confirmation of possession of the PMK as well as distributing the CAK. Note that the PMK key confirmation could be done within EAPoL messages as part of 802.1X. It may be necessary to add an additional message to fit the exchange nicely into the state machine.

This approach has the advantage that implementers are not required to implement the 802.11 4-way handshake. If the abbreviated handshake can be based on MKA this would simplify implementation as well. This approach allows for key conformation to occur within EAPoL and creates a pairwise association that can be used to protect EAPoL messages for other purposes.

This approach has the disadvantage of differing from the existing 802.11i mechanism. The use of the PMK would have to be examined carefully to ensure that it did not conflict with other uses and that fresh keys could be derived. If freshness cannot be guaranteed then caching of the PMK would probably not be recommended.

2.2.5 Summary

The first approach in section 2.2.1 makes maximum reuse of 802.11. It requires implementers to implement both 802.11 4-way and 802.1af MKA. It requires explicit differentiation between the point-to-point association and the group association. Note that it would probably be useful to profile the usage of the 4-way handshake for its use in 802.1af. This approach might be more attractive if pairwise associations were expected to dominate the use cases. This would probably make FIPS approval easiest in the point-to-point case.

The second approach in section 2.2.2 makes reuses of 802.11, but it also requires implementation of MKA in both the point-to-point and group cases. This approach does not require point-to-point to be a special case.

The third approach which uses MKA in section 2.2.3 only does not rely upon 802.11 implementation. It does not allow for any key confirmation or other extensions of EAPoL and any features that they provide.

The fouth approach in section 2.2.4 is essentially a combination of the previous case in which the 4-way handshake is replaced with a simpler exchange that could be based on MKA. This is new and still needs to be specified. The risk is that it may turn out to be more complicated the 4-way handshake from 802.11. This mechanism could provide key confirmation within EAPoL and allow for further extensions based on the pairwise association.

The first approach would be preferred if the pairwise case is expected to dominate and if leveraging 802.11 is considered desireable. The second approach is architecturally cleaner than the first approach while still reusing much of 802.11. The third approach makes maximum use of MKA with a loss of key confirmation in EAPoL. The fourth approach could provide a compromise where much of MKA could be reused and key confirmation with message protection could still be provided within EAPoL.

Appendix A 802.11i approach

In the 802.11i approach a 4-way handshake is executed using EAPoL key descriptor messages to generate keys for authentication and encryption. A similar approach could be used to generate connectivity association keys. The basic 802.11 key hierarchy is shown in figure 2.

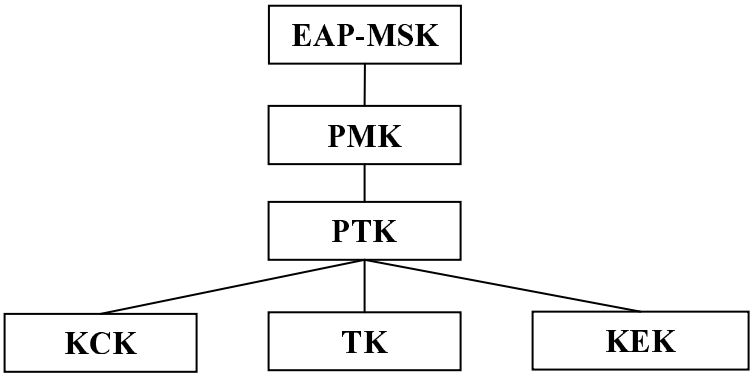

Figure 6 – Part of the 802.11i hierarchy

The PMK is used to generate a Pairwise Transient Key (PTK) which is in turn segmented into a key confirmation key (KCK), a key encrypting key (KEK) used to distribute group

keys for multicast and broadcast, and a temporal key for pairwise encryption (TK). The derivation of the PTK is as follows:

PTK ← PRF-X(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) ||
Min(ANonce,SNonce) || Max(ANonce,SNonce))

The transient nature of the keys comes from the use of nonces (single use random values) in the key derivation. In addition the key derivation of the PTK incorporates the identities (MAC addresses) of the participating stations. The nonces are exchanged as part of the 4-way handshake. The 4-way handshake uses the KCK to integrity protect the last 2 messages of the exchange which ensures that both sides have synchronized key state. The multicast group key (GTK) may be exchanged encrypted under the KEK along with the 3rd message of the 4-way handshake.

The 4-way handshake generates a fresh PTK from the PMK every time it is run. This is especially important in 802.11i since the PMK may be a static pre-shared key, but it is also useful to perform re-keying without have to execute EAP. The 4-way exchange also provides a way to bind external data to the key exchange. 802.11i uses this to bind the advertised RSNIE information to the exchange. The exchange also allows the exchange of group keys encrypted under a key encrypting key. It should also be noted that the 802.11i 4-way handshake has passed NIST evaluation.