A Successful Full Authentication Session/A Successful FIL Re-authentication Session

1. EAP-Request/Identity
   (Fast_ID(i)+realm)
   1) The AP recognizes the Fast_ID(i)+1 identity and agrees on using a FIL Re-authentication protocol.

2. EAP-Response/Identity
   (Fast_ID(i)+1)
   Identity Authentication

3. EAP-Request/AKA/FIL Re-authentication
   (AT_MAC(i), AT_IV(i), * AT_Counter_A(i), * AT_Nonce_A(i), * AT_Encr_Data(i))
   (1) Decrypt *AT_Nonce_A(i) and *AT_Counter_A(i) with K_encr(i-1) key to acquire the Nonce_A(i) and Counter_A(i) attributes
   (2) Generate Nonce_A(i) and Counter_A(i)
   (3) Calculate AT_XMAC(i) and AT_RES(i)
   (4) Calculate AT_MAC(i)=HMAC-SHA1-128(K_auth(i)|Nonce_A(i)|EAP message)
   (5) Generate next Fast_ID(i)
   (6) New generating AVs are stored to database
   (7) New generating AVs are stored to database

4. EAP-Response/AKA/synchronization-error
   (Initiate a new conventional full authentication)

5. EAP-Response/AKA/synchronization-error
   (Initiate a new conventional full authentication)

6. EAP-Response/AKA/FIL Re-authentication
   (AT_RES(i), AT_IV(i), *AT_Encr_Data(i))
   1) Decrypt *AT_Encr_Data(i) with K_encr(i) key to acquire the Counter_A(i) attribute
   2) Check AT_RES(i) = AT_XRES(i)?
   3) New generating AVs are stored to database
   4) New generating AVs are stored to database

7. EAP-Request/AKA/Client-error
   (Initiate a new conventional full authentication)

8. Ciphering mode
   (802.11i Encryption)
   Next FIL Re-authentication