AAA Mobile IP

Protocol Purpose

```
                  {{K_MnFa,K_MnHa}_K_MnAAAH,
                   {{K_MnFa,K_MnHa}_K_MnAAAH}_K_MnHa
                  }_K_AAAHHa
7. AAAH -> AAAL: N_FA,
                  {K_MnFa,K_FaHa}_K_AAAHAAAL,
                  {K_MnFa,K_MnHa}_K_MnAAAH,
                  {{K_MnFa,K_MnHa}_K_MnAAAH}_K_MnHa,
                  {N_FA,
                   {K_MnFa,K_FaHa}_K_AAAHAAAL,
                   {K_MnFa,K_MnHa}_K_MnAAAH,
                   {{K_MnFa,K_MnHa}_K_MnAAAH}_K_MnHa
                  }_K_AAAHAAAL
8. AAAL -> FA:   N_FA,
                  {K_MnFa,K_FaHa}_K_FaAAAL,
                  {K_MnFa,K_MnHa}_K_MnAAAH,
                  {{K_MnFa,K_MnHa}_K_MnAAAH}_K_MnHa,
                  {N_FA,
                   {K_MnFa,K_FaHa}_K_FaAAAL,
                   {K_MnFa,K_MnHa}_K_MnAAAH,
                   {{K_MnFa,K_MnHa}_K_MnAAAH}_K_MnHa
                  }_K_FaAAAL
9. FA   -> MN:   {K_MnFa,K_FaHa}_K_FaAAAL,
                  {K_MnFa,K_MnHa}_K_MnAAAH,
                  {{K_MnFa,K_MnHa}_K_MnAAAH}_K_MnHa
```

```
role aaa_MIP_AAAH (AAAH,AAAL,HA,FA,MN : agent,
```

```
role session(MN,FA,AAAL,AAAH,HA: agent,
             Kmn3ah,Kfa3al,K3ah3al,Kha3ah: symmetric_key) def=

   local     MNs,MNr,
             FAs,FAr,
             Ls, Lr,
```

```
goal

  %secrecy_of K_MnFa, K_FaHa, K_MnFa
  secrecy_of secFAHA, secFAMN, secMNHA
  %AAA_MIP_FA weakly authenticates AAA_MIP_AAAH on k_faha1
  weak_authentication_on k_faha1
  %AAA_MIP_FA weakly authenticates AAA_MIP_AAAH on k_mnfa1
  weak_authentication_on k_mnfa1
  %AAA_MIP_HA weakly authenticates AAA_MIP_AAAH on k_faha2
  weak_authentication_on k_faha2
  %AAA_MIP_HA weakly authenticates AAA_MIP_AAAH on k_mnha1
  weak_authentication_on k_mnha1
  %AAA_MIP_MN weakly authenticates AAA_MIP_AAAH on k_mnha2
  weak_authentication_on k_mnha2
  %AAA_MIP_MN weakly authenticates AAA_MIP_AAAH on k_mnfa2
  weak_authentication_on k_mnfa2

end goal

environment()
```

References

[CJP03]