

7170Bis

EMU - IETF 122



TEAP: THE GIFT THAT KEEPS ON GIVING

- ▶ Many clarifications and updates to the document
 - ▶ Pending reviews from Michael Richardson and Jouni Malinen
 - ▶ But...
- ▶ The results of interop testing are up on the Wiki
 - ▶ <https://github.com/emu-wg/rfc7170bis/wiki/Interop-Testing>
- ▶ Good news? Bad news?

THE WORST NEWS

- ▶ the following combinations work for all implementations:
 - ▶ EAP-MSCHAPv2
 - ▶ EAP-MSCHAPv2 followed by EAP-MSCHAPv2
- ▶ That's it.

MAYBE SOME GOOD NEWS

- ▶ Subject to a bug fix in one implementation, the following also works:
 - ▶ EAP-TLS
 - ▶ EAP-TLS followed by EAP-MSCHAPv2
- ▶ EAP-TLS all by itself works because the derivation of the EMSK Compound MAC for the first round is clear.
- ▶ EAP-TLS following by EAP-MSCHAPv2 works because the second method uses only the MSK Compound MAC

WHAT HAPPENED?

- ▶ MSFT implemented TEAP, but did not use the EMSK Compound MAC
 - ▶ It is never sent in Crypto-Binding
 - ▶ If received, it is ignored
- ▶ All server implementations are compatible with this behavior

FURTHER DETAILS - MSFT IMPLEMENTATION

- ▶ EAP-TLS work, for both User or Machine
- ▶ EAP-MSCHAPv2 works, for both User or Machine
- ▶ Methods work alone, or in any combination (TLS/TLS, MSCHAP/TLS, etc.)
- ▶ Basic-Password is not supported
- ▶ PKCS#7 / PKCS#10 are not supported

WHERE DO WE GO FROM HERE?

- ▶ We need to decide what to do with 7170bis
- ▶ My \$0.02 is:
 - ▶ We should not break shipping products
 - ▶ We can always fix things in the future

PROPOSAL

- ▶ The simplest way forward that I can think of is the following:
 1. Declare the MSFT behaviour TEAPv1
 2. Decide what we want to do to derive the EMSK Compound MAC. Write it down. Test it with implementations.
 3. Issue TEAPv2 which defines the EMSK Compound MAC, and uses it in the Crypto-Binding TLV.

CHOICES - PICK 1 OF 2

- ▶ Crypto-Binding contains only the MSK Compound MAC, the EMSK Compound MAC is always zero
- ▶ We lose Crypto-Binding for EAP-TLS inner methods

OR

- ▶ Allow EAP-TLS, but only as the first method

FURTHER PROBLEMS

- ▶ We may also want to test PKCS#7 / PKCS#10 in TEAPv2 before shipping it
 - ▶ History shows specs without code are “special”, not “specifications”
- ▶ Clarify issues on chained methods
 - ▶ Server asks for A, supplicant supplies B
 - ▶ Is this a protocol issue, or a policy issue?

DISCUSS!