RFC 3748bis

Jari Arkko and John Mattsson
Ericsson Research

https://datatracker.ietf.org/doc/html/draft-arkko-emu-rfc3748bis-00

https://arkko.com/ietf/eap/draft-arkko-emu-rfc3748bis-from-rfc3748.diff.html

Motivation

DON'T PANIC

There's nothing fundamentally wrong with RFC 3748 as is

And we're not changing the protocol

However …

Some Reasons for Updates

- Fold in errata or other issues observed over the years
- We think about security in very different way today than in 2001; opportunity to improve security considerations, document the properties we expect, references to methods etc.
- Several core EAP protocol documents published after RFC 3748; opportunity to put in the references
- Terminology — personal preference for better terminology
- Reference updates
- Nothing earth shattering, but several opportunities to clean up & provide more information

  “Yearly maintenance”

Updates

1. Ivo Sedlacek's errata on a reference to Section 7.12 rather than Section 7.2
2. Noting the deficiencies in legacy EAP methods and refer to more modern ones
3. The security claim perfect forward secrecy has been added
4. Refer to state machine, network discovery/selection, keying, man-in-the-middle attacks
5. MSK is now expanded as “Main Session Key”. Same for EMSK.
6. References have been updated to their most recent versions.
7. Discuss 3GPP usage, not only IEEE
8. SHOULD omit the peer-name portion of the NAI in EAP identity response.
9. IANA rules have been updated to comply with RFC 8126 and current allocations

Open Questions

- Likely more to say about security considerations
- Is there a reason for some of the sections to be reduced in light of references to other core EAP RFCs that now exist?
- Newer IEEE references?
- SASLprep reference validity?

Next Steps

- What did we miss?
- Where did we go too far?
- Discuss doing an update