Annex C: Contradictory specification quotes relative to the derivation of a 256-bit MSK for HMACs with an output size of 256-bit or more

- ITU-T G.9804.2 Annex C “Secure mutual authentication”: “This is the same as Annex C of [ITU-T G.987.3].”. So ITU-T G.987.3 is the reference.
- ITU-T G.987.3 Annex C “Secure mutual authentication”: “This method employs the enhanced security control managed entity (ME) defined in clause 9.13.11 of [ITU-T G.988] to perform a three-step hash-based authentication. ”. We also follow ITU-T G.988 then.
- ITU-T G.9804.2 clause 9.13: “When the key derivation is triggered by the success of secure mutual authentication, the procedure to obtain the MSK depends on the specific authentication mechanism. (see clauses 9.13.11 of [ITU-T G.988] for OMCI-based mutual authentication). ITU-T G.9804.2 clause 9.13 also confirms the use of ITU-T G.988.
- ITU-T G.988: “If the selected hash function generates more than 128 bits, the result is truncated to the leftmost (most significant) 128 bits.”. While this sentence is under the *Master session key name* equation, the MSK equation is just above and it is unclear if it applies to both.
- ITU-T G.987.3 Annex C “Secure mutual authentication”: “Leaving this mutual authentication, the MSK is ready to be used in the key derivation specified in clause 15.3.”. According to ITU-T G.988, MSK is 128 bits. Except the “MSK is ready” sentence is just after the equation, the 128 bits truncation is only mentionned indirectly through ITU-T G.988.
- ITU-T G.9804.2 clause 9.13: “In case the length of the cipher is shorter than the length of the MSK, the MSK is truncated to its leftmost (most significant) bits as needed to match the cipher length.”. We either have a 128 bits value at this point (following ITU-T G.988) or a 256 or 512 bits one if we use the ITU-T G.987.3 formula directly. In the first case, we always have to use the AES-128-ECMAC method, in the second case we have to truncate the value.