

---

**From:** Peter Rombouts <peter.rombouts@nxp.com>  
**Sent:** Tuesday, August 19, 2014 9:26 AM  
**To:** internal-hash  
**Subject:** Comment on Draft FIPS 202

Hi,

I would like to submit the following comment on Draft FIPS 202:

FIPS 198-1 defines how to compute a keyed-hash message authentication code based on a hash function with given input block size (B) and output block size (L). In FIPS 202 the length of the digest of the hash function (d) is clearly defined, however there is no clear definition of the input block size. I suggest adding a clarification such as the one provided in section 5.1 of the round 3 submission of Keccak (Keccak-submission-3.pdf) which states that the input block size for Keccak is equal to the rate (r).

Regards,  
Peter

The information contained in this message is confidential and may be legally privileged. The message is intended solely for the addressee(s). If you are not the intended recipient, you are hereby notified that any use, dissemination, or reproduction is strictly prohibited and may be unlawful. If you are not the intended recipient, please contact the sender by return e-mail and destroy all copies of the original message.