From: Babbage, Steve, Vodafone Group <Steve.Babbage@vodafone.com>
Sent: Friday, July 18, 2014 8:46 AM
To: internal-hash
Subject: Comment on Draft FIPS 202

ETSI is the European Telecommunications Standards Institute. Within ETSI, TC SAGE is the Technical Committee "Security Algorithms Group of Experts", which specifies many of the cryptographic algorithms for mobile and other telecoms standards.

ETSI TC SAGE would like to express its support for the inclusion of the Extendable-Output Functions SHAKE-128 and SHAKE-256 in the SHA-3 standard (although we prefer the word "Extensible" …). We believe that these add genuine value.

In particular we would like to draw attention to the TUAK algorithm set (http://www.3gpp.org/DynaReport/35231.htm, together with http://www.3gpp.org/DynaReport/35232.htm and http://www.3gpp.org/DynaReport/35233.htm), an authentication and key generation algorithm standardised by 3GPP for mobile telephony. The TUAK functions can all be defined very straightforwardly in terms of SHAKE-256, so that a TUAK implementation could directly and quickly be built from a SHAKE-256 implementation.

Steve Babbage, Vodafone
Chair of ETSI SAGE