From: mike.walker@vf.vodafone.co.uk
To: AESround2@nist.gov
Cc: mike.walker@vf.vodafone.co.uk
Subject: AES comments
Date: Thu, 18 May 2000 09:41:42 +0100
X-Mailer: Internet Mail Service (5.5.2448.0)

Please find attached comments from Vodafone AirTouch to the AES selection.
My apologies for these comments being slightly late.

Regards

Michael Walker

[See attached file]

I am writing on behalf of the Vodafone AirTouch mobile communications group. We would like to state our strongly held opinion that hardware and smart card implementations should be taken very seriously in determining the AES.

In the already huge and rapidly expanding world of mobile communication and mobile commerce, smart cards (particularly SIMs - Subscriber Identity Modules) will play an enormously important role. Although it is generally accepted that digital signing should be performed on smartcards, the value of applying symmetric encryption on the smartcard is less well acknowledged. Vodafone Airtouch see considerable advantages in being able to perform symmetric encryption on the smartcard, thus allowing end to end security between a network application and a smartcard without concerns about compromise of the symmetric key in the terminal, the algorithms supported on the terminal, or security audits of terminals and terminal manufacturers.

Hardware implementations are also important, for either high speed network applications or low power mobile applications.

For these reasons we think it would be most unwise for either Mars or RC6 to be selected as the (single) AES winner. Rijndael seems to us to be by some way the best choice for smart card and hardware implementation, as well as being efficient on a variety of software platforms.

On Behalf of Vodafone AirTouch

Professor Michael Walker
Technical Executive