To: DraftFips201@nist.gov
From: "Eric Wagner" <wagnerec@nv.doe.gov>
Subject: Comments on Public Draft FIPS 201

I believe making the digital signature key optional would be a mistake. Everyone at some point is required to sign documents even if it is just a time sheet.

The digital signature key should allow batch signing. I.e. several data points may be presented to the user at once, each requiring an independent signature. Allow one entry of the PIN to sign all the selected data points.

Given the specification on page 29 that the digital signature key shall not be exported what is meant by the signature only being accessible via the contact interface. I assume it means that the key can't be used at all in a contactless manner. This should be clarified.

I believe there should be an option to use the cryptographic keys on a contactless interface over an encrypted connection. The standard mentions that its not suitable for quick access points due but some devices that may not be able to support a contact interface could still use the digital signature key if the card is held to it for the entire processing time.

Eric Wagner, Ph.D., CHP
Senior Scientist, Science and Technology Section
Remote Sensing Laboratory
PO Box 98521; M/S RSL-11
Las Vegas, NV 89193-8521
Phone: 702-295-8828
Fax: 702-794-1038