Mr. Mike Cooper

NIST CMVP

US Department of Commerce

Dear Mr. Cooper,

We are writing because the CMVP’s recent FIPS 140-2 implementation guidance for AES GCM IV generation has major implications for any PKCS #11 based cryptographic module.

Many cryptographic module vendors make PKCS #11 the basis of their FIPS 140-2 cryptographic boundary, while others present their cryptographic implementation to applications through PKCS #11 (even if their formal cryptographic boundary is on their hardware). As such, the FIPS 140-2 validation of those vendors’ products is heavily dependent on the state of the PKCS #11 specification.

PKCS #11 is the primary cross-platform standard for embedding hardware cryptographic modules into applications and providing cryptographic services in software. PKCS #11 is used by, or in, multiple operating systems, programming languages, secure applications, databases, hardware security modules, smart cards and other security devices. The PKCS #11 standard was originally developed under the leadership of RSA, but as of early 2013, is actively maintained within the OASIS standards body. A list of the member companies involved in the OASIS PKCS#11 technical committee is available at <https://www.oasis-open.org/committees/documents.php?wg_abbrev=pkcs11>. These member companies provide, either directly or indirectly, the implementations in a substantial portion of the validated cryptographic modules under the CMVP.

The PKCS #11 standard currently only permits application-supplied IV's, and does not provide a mechanism to allow for token-generated IV's. PKCS #11, as an API, is designed to allow for a broad range of devices, many of which are simply unable to provide the necessary internal persistent storage to meet the changed implementation guidance.

The impact of the changed FIPS 140-2 implementation guidance, as we understand it, is that any cryptographic module that interfaces with PKCS #11 will be considered FIPS 140-2 non-compliant for AES GCM mode, including all PKCS #11 based HSMs.

As a technical committee, we have recognized the challenges that the changed FIPS 140-2 implementation guidance creates and have commenced work to enable additional APIs within PKCS #11 to handle these new requirements in a manner that will enable us to address this requirement for the broad range of devices which PKCS#11 supports.

We believe that a standards based approach for token-generated IV’s for PKCS #11 based modules is preferable to each PKCS #11 vendor implementing a vendor-specific mechanism. A vendor-specific mechanism would require that every application must correspondingly be changed to support every vendor-specific implementation in order to meet the changed FIPS 140-2 implementation guidance.

Standards development takes time (generally measured in a number of years) as the members of the standard body work through the standards process. Once the standard itself is finalized, vendor implementations have to be designed, developed, and deployed through the normal software development lifecycle. All of these activities are necessary to achieve a common standard approach for handling such requirements for PKCS #11 based cryptographic modules.

Respectfully, we request that you consider allowing a transition period for conformance with the updated implementation guidance for any PKCS #11 based cryptographic module until such time as we have an updated standard and vendors have had an opportunity to adjust their implementations to conform to the new standard.

It would also be helpful if the PKCS #11 technical committee could designate an official liaison on the CMUF and CMVP working groups to enable more timely review of future implementation guidance updates via the CMUF and CMVP working groups prior to implementation guidance being formally adopted by the CMVP.

We look forward to your response.

Thank you for your consideration,

Valerie Fenwick & Robert Relyea

Co-Chairs, OASIS PKCS #11 Technical Committee