PKCS#11 v3.0 Statement of Use

Document Version: 1.0.0

Date: February 20, 2020

Author: Jonathan Schulze-Hewett, Director of Development

General Statement

Information Security Corporation (ISC) has successfully used or implemented selected mechanisms of the OASIS PKCS#11 Cryptographic Token Interface Base Specification [1], [2], [3] in accordance with OASIS policy. The implementation has been successfully used in interoperation with other implementations.

Detailed Statement

ISC has successfully implemented the core set of data types, objects, and functions defined in the OASIS PKCS #11 Cryptographic Token Interface Base Specification [1] in our Acala softHSM. Acala v2.1 supports numerous mechanisms defined in the PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0 [2]. Further objects, functions and mechanisms newly introduced in [1] and [2] will become available in future releases of Acala.

PKCS#11 consumer implementations by Oracle and Mozilla have successfully been used in interoperation with ISC's Acala PKCS#11 provider implementation.

[1] PKCS #11 Cryptographic Token Interface Base Specification Version 3.0, Committee Specification 01, approved 19 December 2019, http://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/pkcs11-base-v3.0.docx
[2] PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0, Committee Specification 01, approved 19 December 2019, http://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/pkcs11-curr-v3.0.docx
[3] PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 3.0, Committee Specification 01, approved 19 December 2019, http://docs.oasis-open.org/pkcs11/pkcs11-hist/v3.0/pkcs11-hist-v3.0.docx