

PKCS #11 v3.0 Statement of Use

General Statement

Utimaco has successfully implemented selected mechanisms of the OASIS PKCS #11 Cryptographic Token Interface Base Specification [2], [3], [4] in accordance with the OASIS policy. The implementation has successfully been used in interoperation with other implementations.

Detailed Statement

Utimaco has successfully implemented the core set of data types, objects, and functions defined in the OASIS PKCS #11 Cryptographic Token Interface Base Specification [2] in our SecurityServer PKCS #11 provider and administration tools. The PKCS #11 provider in the current SecurityServer 4.3x releases supports numerous mechanisms defined in the PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40 Errata 01 [5] and selected mechanisms newly introduced with the PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0, Committee Specification 01 [3]. Further objects, functions and mechanisms newly introduced in [2] and [3] will become available with our PKCS #11 provider in the next SecurityServer 4.4x releases.

PKCS #11 consumer implementations by Cryptsoft and Primekey have successfully been used in interoperation with Utimaco's SecurityServer PKCS #11 provider implementation.

[1] PKCS #11 Cryptographic Token Interface Profiles Version 3.0, Committee Specification 01, approved 19 December 2019, <http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v3.0/pkcs11-profiles-v3.0.docx>

[2] 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>

[3] 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>

[4] 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>

[5] PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40 Errata 01, OASIS Standard Incorporating Approved Errata 01, 13 May 2016, <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/pkcs11-curr-v2.40-errata01-complete.pdf>

Dieter Bong

Head of HSM Product Management

Utimaco IS GmbH

Germanusstraße 4
52080 Aachen
Tel +49 241 1696-0
Fax +49 241 1696-199
utimaco.com

Registergericht:
Aachen HRB 18922
Sitz: Aachen
USt.-IdNr.: DE 815 496 496

Deutsche Bank AG, Köln
BLZ: 370 700 60
Konto-Nr.: 1 135 912 00
BIC: DEUTDE33XXX
IBAN: DE14370700600113591200

Geschäftsführer:
Stefan Auerbach
Malte Pollmann
Martin Stamm