#

# From barbican.plugin.crypto.p11

#

# Path to vendor PKCS11 library (string value)

library\_path = {{ plugin.get('library\_path', '/usr/lib/libCryptoki2\_64.so') }}

# Password to login to PKCS11 session (string value)

login = {{ plugin.login }}

# Master KEK label (used in the HSM) (string value)

mkek\_label = {{ plugin.mkek\_label }}

# Master KEK length in bytes. (integer value)

mkek\_length = {{ plugin.get('mkek\_length', 32) }}

# HMAC label (used in the HSM) (string value)

hmac\_label = {{ plugin.hmac\_label }}

# HSM Slot ID (integer value)

#slot\_id = 1

# Flag for Read/Write Sessions (boolean value)

#rw\_session = true

# Project KEK length in bytes. (integer value)

#pkek\_length = 32

# Project KEK Cache Time To Live, in seconds (integer value)

#pkek\_cache\_ttl = 900

# Project KEK Cache Item Limit (integer value)

#pkek\_cache\_limit = 100

# Secret encryption algorithm (string value)

#algorithm = VENDOR\_SAFENET\_CKM\_AES\_GCM

# File to pull entropy for seeding RNG (string value)

#seed\_file =

# Amount of data to read from file for seed (integer value)

#seed\_length = 32

# User friendly plugin name (string value)

#plugin\_name = PKCS11 HSM

# Flag for plugin generated iv case (boolean value)

#generate\_iv = false