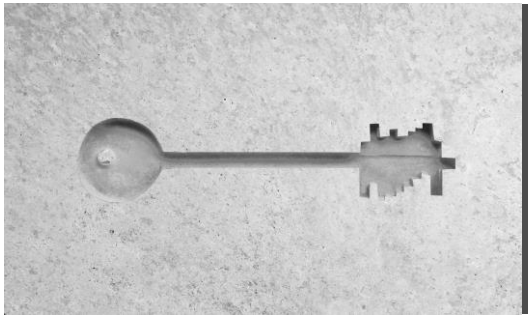


SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

1 PKCS#11 Mechanisms

The following tables are based on PKCS#11 specification version 2.20 and its amendment 3, version 2.30 draft and version 2.40. All mechanism-function-combinations defined by the standard and supported by SecurityServer 4.01 are marked with a ✓ character. All mechanism-function-combinations defined by the standard but not supported by SecurityServer 4.01 are marked with – characters. Empty mechanism-function-combinations are not defined by the standard.

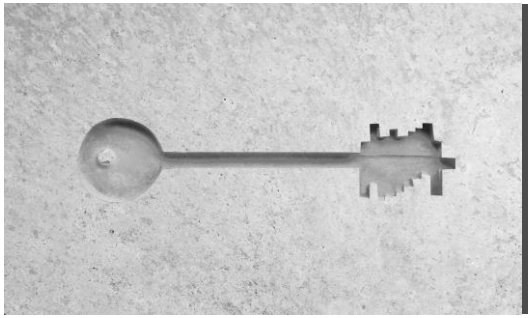
All Vendor Defined Mechanisms provided by SecurityServer 4.01 are listed on the last page of this section.

Supported mechanisms are supported by Utimaco PKCS#11 R2 implementation on all CryptoServer hardware platforms.

The list of supported mechanisms in SecurityServer 4.01 is the same as for SecurityServer 3.30/3.21/3.20.

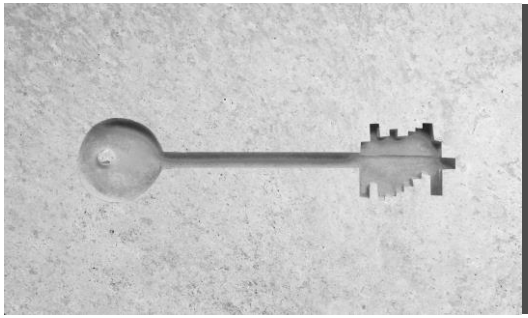
PKCS#11 v2.20

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_RSA_PKCS_KEY_PAIR_GEN					✓		
CKM_RSA_X9_31_KEY_PAIR_GEN					✓		
CKM_RSA_PKCS	✓[2]	✓[2]	✓			✓	
CKM_RSA_PKCS_OAEP	✓[2]					✓	
CKM_RSA_PKCS_PSS		✓[2]					
CKM_RSA_9796		--	--				
CKM_RSA_X_509	✓[2]	✓[2]	✓			✓	
CKM_RSA_X9_31		✓[2]					



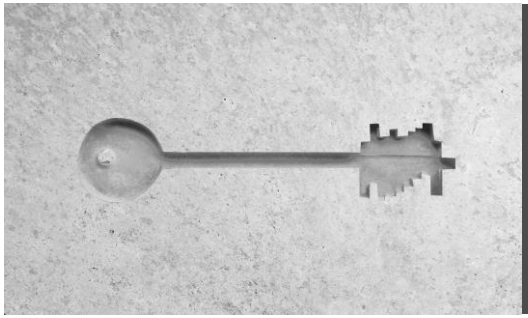
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_MD2_RSA_PKCS		--					
CKM_MD5_RSA_PKCS		✓					
CKM_SHA1_RSA_PKCS		✓					
CKM_SHA256_RSA_PKCS		✓					
CKM_SHA384_RSA_PKCS		✓					
CKM_SHA512_RSA_PKCS		✓					
CKM_RIPEMD128_RSA_PKCS		--					
CKM_RIPEMD160_RSA_PKCS		✓					
CKM_SHA1_RSA_PKCS_PSS		✓					
CKM_SHA256_RSA_PKCS_PSS		✓					
CKM_SHA384_RSA_PKCS_PSS		✓					
CKM_SHA512_RSA_PKCS_PSS		✓					
CKM_SHA1_RSA_X9_31		✓					
CKM_DSA_KEY_PAIR_GEN					✓		
CKM_DSA_PARAMETER_GEN					✓		
CKM_DSA		✓[2]					
CKM_DSA_SHA1		✓					
CKM_FORTEZZA_TIMESTAMP		--					



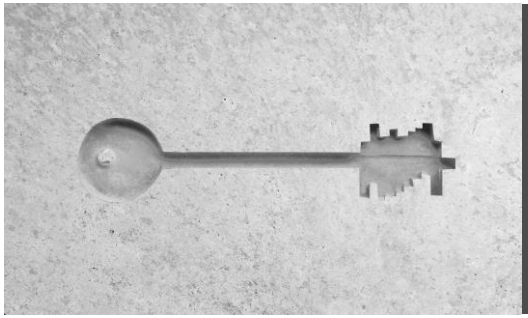
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_EC_KEY_PAIR_GEN (CKM_ECDSA_KEY_PAIR_GEN)					✓		
CKM_ECDSA		✓[2]					
CKM_ECDSA_SHA1		✓					
CKM_ECDH1_DERIVE							✓
CKM_ECDH1_COFACTOR_DERIVE							✓
CKM_ECMQV_DERIVE							--
CKM_DH_PKCS_KEY_PAIR_GEN					✓		
CKM_DH_PKCS_PARAMETER_GEN					--		
CKM_DH_PKCS_DERIVE							✓
CKM_X9_42_DH_KEY_PAIR_GEN					✓		
CKM_X9_42_DH_PKCS_PARAMETER_GEN					✓		
CKM_X9_42_DH_DERIVE							✓
CKM_X9_42_DH_HYBRID_DERIVE							--
CKM_X9_42_MQV_DERIVE							--
CKM_KEA_KEY_PAIR_GEN					--		
CKM_KEA_KEY_DERIVE							--
CKM_GENERIC_SECRET_KEY_GEN					✓		
CKM_RC2_KEY_GEN					--		



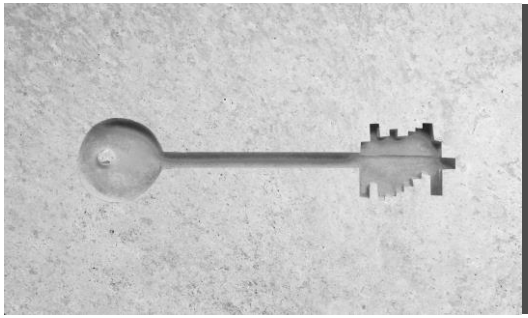
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_RC2_ECB	--					--	
CKM_RC2_CBC	--					--	
CKM_RC2_CBC_PAD	--					--	
CKM_RC2_MAC_GENERAL		--					
CKM_RC2_MAC		--					
CKM_RC4_KEY_GEN					--		
CKM_RC4	--						
CKM_RC5_KEY_GEN					--		
CKM_RC5_ECB	--					--	
CKM_RC5_CBC	--					--	
CKM_RC5_CBC_PAD	--					--	
CKM_RC5_MAC_GENERAL		--					
CKM_RC5_MAC		--					
CKM_AES_KEY_GEN					✓		
CKM_AES_ECB	✓					✓	
CKM_AES_CBC	✓					✓	
CKM_AES_CBC_PAD	✓					✓	
CKM_AES_MAC_GENERAL		✓					



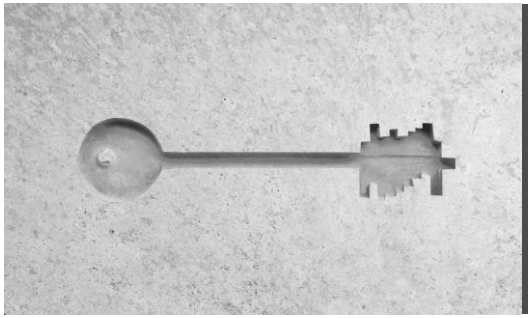
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_AES_MAC		✓					
CKM_DES_KEY_GEN					✓		
CKM_DES_ECB	✓					✓	
CKM_DES_CBC	✓					✓	
CKM_DES_CBC_PAD	✓					✓	
CKM_DES_MAC_GENERAL		✓					
CKM_DES_MAC		✓					
CKM_DES2_KEY_GEN					✓		
CKM_DES3_KEY_GEN					✓		
CKM_DES3_ECB	✓					✓	
CKM_DES3_CBC	✓					✓	
CKM_DES3_CBC_PAD	✓					✓	
CKM_DES3_MAC_GENERAL		✓					
CKM_DES3_MAC		✓					
CKM_CAST_KEY_GEN					--		
CKM_CAST_ECB	--					--	
CKM_CAST_CBC	--					--	
CKM_CAST_CBC_PAD	--					--	



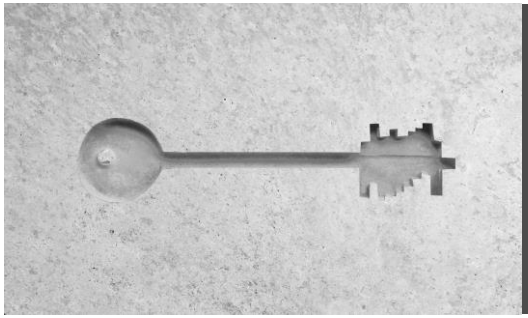
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_CAST_MAC_GENERAL		--					
CKM_CAST_MAC		--					
CKM_CAST3_KEY_GEN					--		
CKM_CAST3_ECB	--					--	
CKM_CAST3_CBC	--					--	
CKM_CAST3_CBC_PAD	--					--	
CKM_CAST3_MAC_GENERAL		--					
CKM_CAST3_MAC		--					
CKM_CAST128_KEY_GEN (CKM_CAST5_KEY_GEN)					--		
CKM_CAST128_ECB (CKM_CAST5_ECB)	--					--	
CKM_CAST128_CBC (CKM_CAST5_CBC)	--					--	
CKM_CAST128_CBC_PAD (CKM_CAST5_CBC_PAD)	--					--	
CKM_CAST128_MAC_GENERAL (CKM_CAST5_MAC_GENERAL)		--					
CKM_CAST128_MAC (CKM_CAST5_MAC)		--					
CKM_IDEA_KEY_GEN					--		
CKM_IDEA_ECB	--					--	
CKM_IDEA_CBC	--					--	
CKM_IDEA_CBC_PAD	--					--	



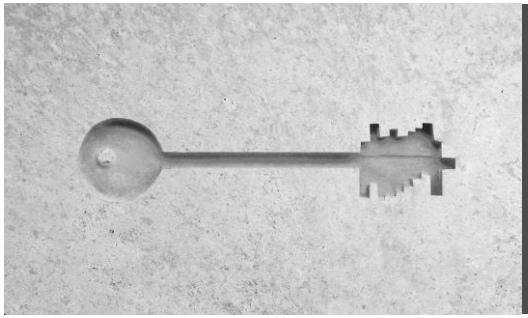
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_IDEA_MAC_GENERAL		--					
CKM_IDEA_MAC		--					
CKM_CDMF_KEY_GEN					--		
CKM_CDMF_ECB	--					--	
CKM_CDMF_CBC	--					--	
CKM_CDMF_CBC_PAD	--					--	
CKM_CDMF_MAC_GENERAL		--					
CKM_CDMF_MAC		--					
CKM_DES_ECB_ENCRYPT_DATA							✓
CKM_DES_CBC_ENCRYPT_DATA							✓
CKM_DES3_ECB_ENCRYPT_DATA							✓
CKM_DES3_CBC_ENCRYPT_DATA							✓
CKM_AES_ECB_ENCRYPT_DATA							✓
CKM_AES_CBC_ENCRYPT_DATA							✓
CKM_SKIPJACK_KEY_GEN					--		
CKM_SKIPJACK_ECB64	--						
CKM_SKIPJACK_CBC64	--						
CKM_SKIPJACK_OFB64	--						



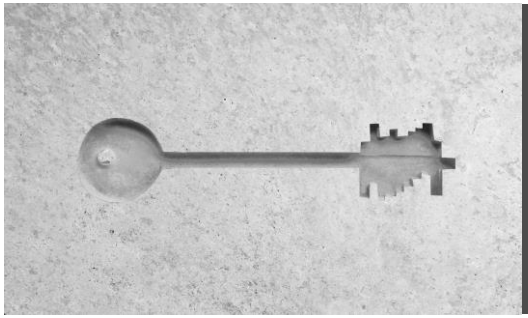
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_SKIPJACK_CFB64	--						
CKM_SKIPJACK_CFB32	--						
CKM_SKIPJACK_CFB16	--						
CKM_SKIPJACK_CFB8	--						
CKM_SKIPJACK_WRAP						--	
CKM_SKIPJACK_PRIVATE_WRAP						--	
CKM_SKIPJACK_RELAYX						--	
CKM_BATON_KEY_GEN					--		
CKM_BATON_ECB128	--						
CKM_BATON_ECB96	--						
CKM_BATON_CBC128	--						
CKM_BATON_COUNTER	--						
CKM_BATON_SHUFFLE	--						
CKM_BATON_WRAP						--	
CKM_JUNIPER_KEY_GEN					--		
CKM_JUNIPER_ECB128	--						
CKM_JUNIPER_CBC128	--						
CKM_JUNIPER_COUNTER	--						



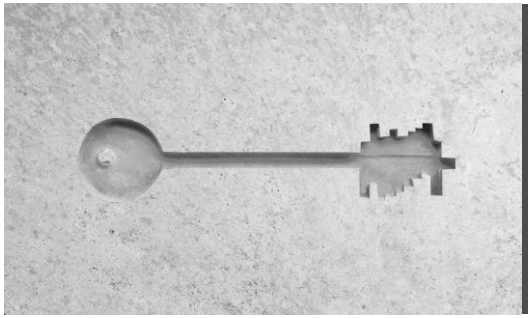
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_JUNIPER_SHUFFLE	--						
CKM_JUNIPER_WRAP						--	
CKM_MD2				--			
CKM_MD2_HMAC_GENERAL		--					
CKM_MD2_HMAC		--					
CKM_MD2_KEY_DERIVATION							--
CKM_MD5				✓			
CKM_MD5_HMAC_GENERAL		✓					
CKM_MD5_HMAC		✓					
CKM_MD5_KEY_DERIVATION							✓
CKM_SHA_1				✓			
CKM_SHA_1_HMAC_GENERAL		✓					
CKM_SHA_1_HMAC		✓					
CKM_SHA1_KEY_DERIVATION							✓
CKM_SHA256				✓			
CKM_SHA256_HMAC_GENERAL		✓					
CKM_SHA256_HMAC		✓					
CKM_SHA256_KEY_DERIVATION							✓



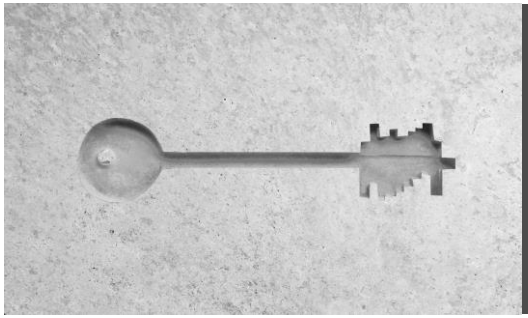
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_SHA384				✓			
CKM_SHA384_HMAC_GENERAL		✓					
CKM_SHA384_HMAC		✓					
CKM_SHA384_KEY_DERIVATION							✓
CKM_SHA512				✓			
CKM_SHA512_HMAC_GENERAL		✓					
CKM_SHA512_HMAC		✓					
CKM_SHA512_KEY_DERIVATION							✓
CKM_RIPEMD128				--			
CKM_RIPEMD128_HMAC_GENERAL		--					
CKM_RIPEMD128_HMAC		--					
CKM_RIPEMD160				✓			
CKM_RIPEMD160_HMAC_GENERAL		✓					
CKM_RIPEMD160_HMAC		✓					
CKM_FASTHASH				--			
CKM_PBE_MD2_DES_CBC					--		
CKM_PBE_MD5_DES_CBC					--		
CKM_PBE_MD5_CAST_CBC					--		



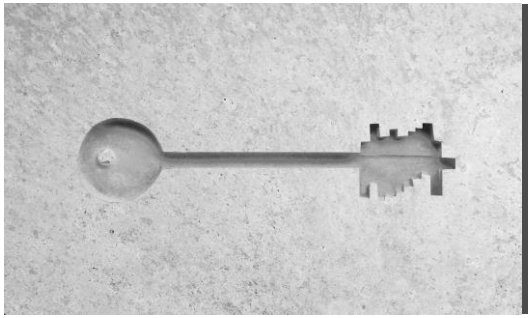
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_PBE_MD5_CAST3_CBC					--		
CKM_PBE_MD5_CAST128_CBC (CKM_PBE_MD5_CAST5_CBC)					--		
CKM_PBE_SHA1_CAST128_CBC (CKM_PBE_SHA1_CAST5_CBC)					--		
CKM_PBE_SHA1_RC4_128					--		
CKM_PBE_SHA1_RC4_40					--		
CKM_PBE_SHA1_DES3_EDE_CBC					--		
CKM_PBE_SHA1_DES2_EDE_CBC					--		
CKM_PBE_SHA1_RC2_128_CBC					--		
CKM_PBE_SHA1_RC2_40_CBC					--		
CKM_PBA_SHA1_WITH_SHA1_HMAC					--		
CKM_PKCS5_PBKD2					--		
CKM_KEY_WRAP_SET_OAEP						--	
CKM_KEY_WRAP_LYNKS						--	
CKM_SSL3_PRE_MASTER_KEY_GEN					--		
CKM_SSL3_MASTER_KEY_DERIVE							--
CKM_SSL3_MASTER_KEY_DERIVE_DH							--
CKM_SSL3_KEY_AND_MAC_DERIVE							--
CKM_SSL3_MD5_MAC		--					



SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

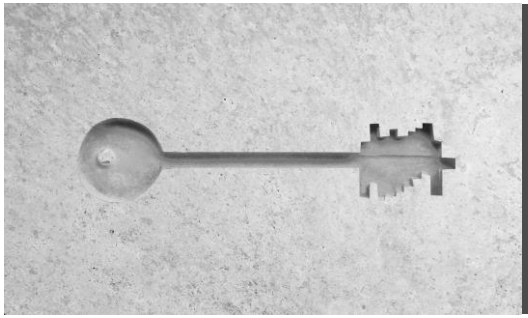
Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_SSL3_SHA1_MAC		--					
CKM_TLS_PRE_MASTER_KEY_GEN					--		
CKM_TLS_MASTER_KEY_DERIVE							--
CKM_TLS_MASTER_KEY_DERIVE_DH							--
CKM_TLS_KEY_AND_MAC_DERIVE							--
CKM_TLS_PRF							--
CKM_WTLS_PRE_MASTER_KEY_GEN					--		
CKM_WTLS_MASTER_KEY_DERIVE							--
CKM_WTLS_MASTER_KEY_DERIVE_DH_ECC							--
CKM_WTLS_SERVER_KEY_AND_MAC_DERIVE							--
CKM_WTLS_CLIENT_KEY_AND_MAC_DERIVE							--
CKM_WTLS_PRF							--
CKM_CMS_SIG		--	--				
CKM_CONCATENATE_BASE_AND_KEY							✓
CKM_CONCATENATE_BASE_AND_DATA							✓
CKM_CONCATENATE_DATA_AND_BASE							✓
CKM_XOR_BASE_AND_DATA							✓
CKM_EXTRACT_KEY_FROM_KEY							✓



SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

PKCS#11 v2.20 Amendment 3

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_SHA224				✓			
CKM_SHA224_HMAC		✓					
CKM_SHA224_HMAC_GENERAL		✓					
CKM_SHA224_RSA_PKCS		✓					
CKM_SHA224_RSA_PKCS_PSS		✓					
CKM_SHA224_KEY_DERIVATION							✓
CKM_AES_CTR	✓					--	
CKM_CAMELLIA_KEY_GEN					--		
CKM_CAMELLIA_ECB	--					--	
CKM_CAMELLIA_CBC	--					--	
CKM_CAMELLIA_CBC_PAD	--					--	
CKM_CAMELLIA_CTR	--					--	
CKM_CAMELLIA_MAC_GENERAL		--					
CKM_CAMELLIA_MAC		--					
CKM_CAMELLIA_ECB_ENCRYPT_DATA							--
CKM_CAMELLIA_CBC_ENCRYPT_DATA							--

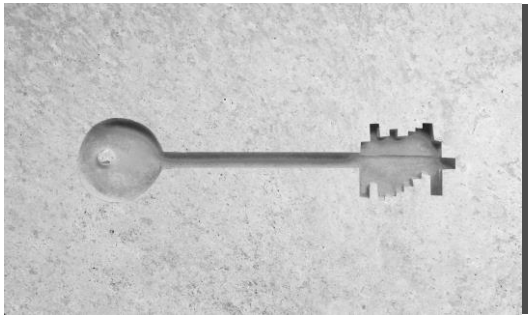


SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_ARIA_KEY_GEN					--		
CKM_ARIA_ECB	--					--	
CKM_ARIA_CBC	--					--	
CKM_ARIA_CBC_PAD	--					--	
CKM_ARIA_MAC_GENERAL		--					
CKM_ARIA_MAC		--					
CKM_ARIA_ECB_ENCRYPT_DATA							--
CKM_ARIA_CBC_ENCRYPT_DATA							--

PKCS#11 v2.40

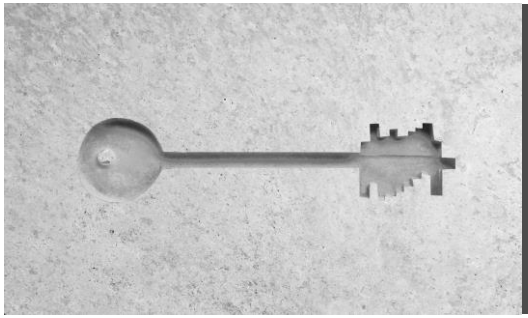
Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_AES_GCM	✓						
CKM_AES_OFB	✓					✓	



SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

PKCS#11 Vendor Defined Mechanisms

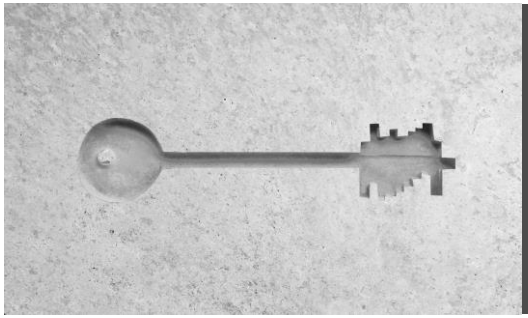
Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_ECDSA_SHA224		✓					
CKM_ECDSA_SHA256		✓					
CKM_ECDSA_SHA384		✓					
CKM_ECDSA_SHA512		✓					
CKM_ECDSA_RIPEMD160		✓					
CKM_ECKA		✓[4]					
CKM_DSA_SHA224		✓					
CKM_DSA_SHA256		✓					
CKM_DSA_SHA384		✓					
CKM_DSA_SHA512		✓					
CKM_DSA_RIPEMD160		✓					
CKM_DES3_RETAIL_MAC		✓					
CKM_AES_CMAC		✓					
CKM_RSA_PKCS_MULTI		✓[4,5]					
CKM_RSA_X_509_MULTI		✓[4,5]					
CKM_DES_CBC_WRAP						✓	



SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Mechanism	Function						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key (Pair)**	**Wrap & Unwrap**	**Derive**
CKM_AES_CBC_WRAP						✓	
CKM_ECDSA_ECIES	✓[2]						
CKM_ECDSA_MULTI		✓[4,5]					

[1] SR = SignRecover, VR = VerifyRecover
[2] Single-part operations only
[3] Mechanism can only be used for wrapping, not unwrapping
[4] Single-part sign operations only
[5] Mechanism can only be used for signing, not for verification

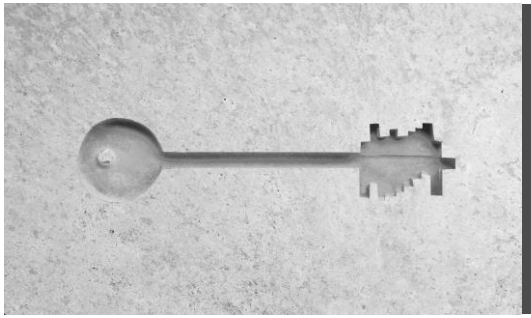


SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

PKCS#11 Functions

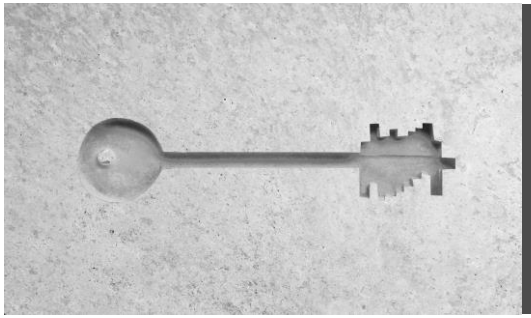
The following table is based on PKCS#11 specification version 2.20. It lists all functions as defined by the standard. Functions supported by SecurityServer 4.01 are marked with a ✓ character. Functions not supported by SecurityServer 4.01 are implemented as function stub which returns CKR_FUNCTION_NOT_SUPPORTED; they are marked with a -- character.

Function	Description	Supported
General purpose functions		
C_Initialize	initializes Cryptoki	✓
C_Finalize	clean up miscellaneous Cryptoki associated resources	✓
C_GetInfo	obtains general information about Cryptoki	✓
C_GetFunctionList	obtains entry points of Cryptoki library functions	✓
Slot and token management functions		
C_GetSlotList	obtains a list of slots in the system	✓
C_GetSlotInfo	obtains information about a particular slot	✓
C_GetTokenInfo	obtains information about a particular token	✓
C_WaitForSlotEvent	waits for a slot event (token insertion, removal, etc.) to occur	--
C_GetMechanismList	obtains a list of mechanisms supported by a token	✓
C_GetMechanismInfo	obtains information about a particular mechanism	✓
C_InitToken	initializes a token	✓
C_InitPIN	initializes the normal user's PIN	✓
C_SetPIN	modifies the PIN of the current user	✓



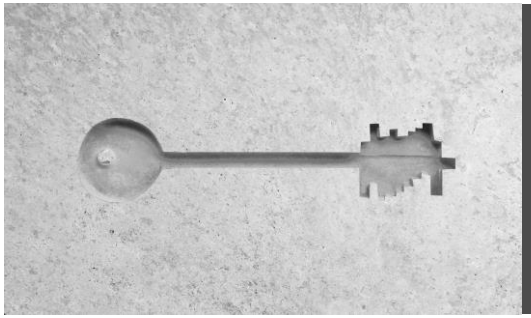
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Function	Description	Supported
Session management functions		
C_OpenSession	opens a connection between an application and a particular token or sets up an application callback for token insertion	✓
C_CloseSession	closes a session	✓
C_CloseAllSessions	closes all sessions with a token	✓
C_GetSessionInfo	obtains information about the session	✓
C_GetOperationState	obtains the cryptographic operations state of a session	--
C_SetOperationState	sets the cryptographic operations state of a session	--
C_Login	logs into a token	✓
C_Logout	logs out from a token	✓
Object management functions		
C_CreateObject	creates an object	✓
C_CopyObject	creates a copy of an object	✓
C_DestroyObject	destroys an object	✓
C_GetObjectSize	obtains the size of an object in bytes	✓
C_GetAttributeValue	obtains an attribute value of an object	✓
C_SetAttributeValue	modifies an attribute value of an object	✓
C_FindObjectsInit	initializes an object search operation	✓
C_FindObjects	continues an object search operation	✓
C_FindObjectsFinal	finishes an object search operation	✓



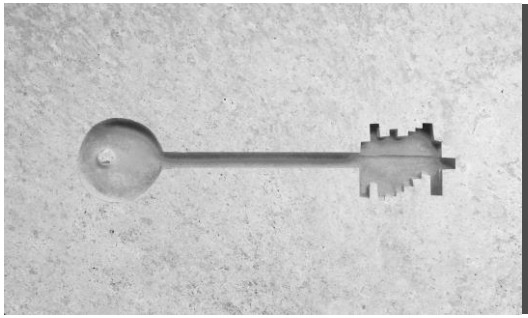
SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Function	Description	Supported
Encryption functions		
C_EncryptInit	initializes an encryption operation	✓
C_Encrypt	encrypts single-part data	✓
C_EncryptUpdate	continues a multiple-part encryption operation	✓
C_EncryptFinal	finishes a multiple-part encryption operation	✓
Decryption functions		
C_DecryptInit	initializes a decryption operation	✓
C_Decrypt	decrypts single-part encrypted data	✓
C_DecryptUpdate	continues a multiple-part decryption operation	✓
C_DecryptFinal	finishes a multiple-part decryption operation	✓
Message digesting functions		
C_DigestInit	initializes a message-digesting operation	✓
C_Digest	digests single-part data	✓
C_DigestUpdate	continues a multiple-part digesting operation	✓
C_DigestKey	digests a key	✓
C_DigestFinal	finishes a multiple-part digesting operation	✓
Signing and MACing functions		
C_SignInit	initializes a signature operation	✓
C_Sign	signs single-part data	✓



SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Function	Description	Supported
C_SignUpdate	continues a multiple-part signature	✓
C_SignFinal	finishes a multiple-part signature operation	✓
C_SignRecoverInit	initializes a signature operation, where the data can be recovered from the signature	✓
C_SignRecover	signs single-part data, where the data can be recovered from the signature	✓
Functions for verifying signatures and MACs		
C_VerifyInit	initializes a verification operation	✓
C_Verify	verifies a signature on single-part data and MACs	✓
C_VerifyUpdate	continues a multiple-part verification operation	✓
C_VerifyFinal	finishes a multiple-part verification operation	✓
C_VerifyRecoverInit	initializes a verification operation where the data is recovered from the signature	✓
C_VerifyRecover	verifies a signature on single-part data, where the data is recovered from the signature	✓
Dual-purpose cryptographic functions		
C_DigestEncryptUpdate	continues simultaneous multiple-part digesting and encryption operations	✓
C_DecryptDigestUpdate	continues simultaneous multiple-part decryption and digesting operations	✓
C_SignEncryptUpdate	continues simultaneous multiple-part signature and encryption operations	✓
C_DecryptVerifyUpdate	continues simultaneous multiple-part decryption and verification operations	✓
Key management functions		
C_GenerateKey	generates a secret key	✓
C_GenerateKeyPair	generates a public-key/private-key pair	✓



SecurityServer 4.01
PKCS#11 R2 Mechanisms and Functions

Function	Description	Supported
C_WrapKey	wraps (encrypts) a key	✓
C_UnwrapKey	unwraps (decrypts) a key	✓
C_DeriveKey	derives a key from a base key	✓
Random number generation functions		
C_SeedRandom	mixes in additional seed material to the random number generator	✓
C_GenerateRandom	generates random data	✓
Parallel function management functions		
C_GetFunctionStatus	legacy function which always returns CKR_FUNCTION_NOT_PARALLEL	--
C_CancelFunction	legacy function which always returns CKR_FUNCTION_NOT_PARALLEL	--