RSA BSAFE Technical Specification Comparison Tables

Algorithms

Algorithm Type	Algorithm	Mode	BSAFE C/C++ MES	CK	BSAFE CNG	TLS-J ME	BSAFE Java
Symmetric	AES	CBC, CFB, ECB, OFB, CTR, CCM, GCM	Y	Y	Y	Y	Y
	Triple DES	CBC, CFB, ECB, OFB	Y	Y	Y	Y	Y
	DES	CBC, CFB, ECB, OFB	Y	Y	Y	Y	Y
	RC2	CBC, CFB, ECB, OFB	Y	Y	Y	Y	Y
	RC4	CBC, CFB, ECB, OFB	Y	Y	Y	Y	Y
	RC5	CBC, CFB, ECB, OFB	Y	Y	N	N	Y
Asymmetric Encryption	RSA (2 primes)	ANSI X9.31	Y	Y	N	Y	Y
		Optimal Asymmetric Encryption Padding (OAEP)	Y	Y	Y	Y	Y
		PKCS #1 Block02 Padding	Y	Y	Y	Y	Y
		No Padding (Raw RSA)	Y	Y	Y	Y	Y
	RSA (3 primes)	ANSI X9.31	Y	Y	N	Y	Y
		Optimal Asymmetric Encryption Padding (OAEP)	Y	Y	Y	Y	Y
		PKCS #1 Block02 Padding	Y	Y	Y	Y	Y
		No Padding	Y	Y	Y	Y	Y

		(Raw RSA)					
	ECIES	KDF2 XOR	Y	Y	N	Y	Y
		AES	Y	Y	N	Y	Y
		Triple-DES	Y	Y	N	Y	Y
Signature	ECDSA	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	Y	Y	Y	Y	Y
	DSA	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	Y	Y	Y	Y	Y
	RSA	PKCS #1 v1.5 with SHA-1, SHA224, SHA256, SHA 384, SHA512, MD2, and MD5	Y	Y	Y	Y	Y
		Probabilistic Signature Scheme (PSS) with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Y	Y	Y	Y	Y
Parameter Generation	Diffie-Hellman (DH)	In accordance with PKCS #3 In accordance with X9.42	Y	Y	Y	N	Y
	DSA		Y	Y	Y	N	Y
	Elliptic Curve		Y	N	Y	N	Y
Asymmetric Key Generation	RSA		Y	Y	Y	Y	Y
	Diffie-Hellman		Y	Y	Y	Y	Y
	EC		Y	Y	Y	Y	Y
	DSA		Y	Y	Y	Y	Y
Key Agreement	Diffie-Hellman (DH)		Y	Y	Y	Y	Y
	ECDH		Y	Y	Y	Y	Y
	ECDHC		Y	Y	N	Y	Y
Message Digests	SHA-1		Y	Y	Y	Y	Y
	SHA-224		Y	Y	Y	Y	Y
	SHA-256		Y	Y	Y	Y	Y
	SHA-384		Y	Y	Y	Y	Y
	SHA-512		Y	Y	Y	Y	Y
	MD2		Y	Y	Y	N	Y
	MD4		N	Y	Y	Y	Y

	MD5		Y	Y	Y	Y	Y
	RIPEMD 160		N	N	N	N	Y
Message Authentication Code	HMAC/SHA-1		Y	Y	Y	Y	Y
	HMAC/SHA-224		Y	Y	Y	Y	Y
	HMAC/SHA-256		Y	Y	Y	Y	Y
	HMAC/SHA-384		Y	Y	Y	Y	Y
	HMAC/SHA-512		Y	Y	Y	Y	Y
	HMAC/MD5		Y	Y	Y	Y	Y
	HMAC/RIPEMD160		N	N	N	N	Y
	GMAC		Y	Y	Y	Y	Y
Pseudo Random Number Generator	Dual EC-DRBG		Y	Y	Y	Y	Y
	HMAC DRBG		Y	Y	Y	Y	Y
	FIPS 186-2 PRNG		Y	Y	Y	Y	Y
	SHA1 PRNG		N	N	N	N	Y
	MD5 PRNG		N	N	N	N	Y
Key Derivation Functions	PBKDF2	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	Y	Y	N	Y	Y
	SP800-56A		N	N	Y	N	N
	TLS PRF		N	N	Y	N	N
Key Wrap	AES Key Wrap	RFC 3365	N	N	Y	N	N
		RFC3394	Y	Y	N	N	Y
		RFC 5649	N	N	N	N	Y
		X9.102	Y	Y	N	N	N

Named Curves

Elliptic Curve Type	**BSAFE C/C++ MES**	**CK**	**BSAFE CNG**	**TLS-J ME**	**BSAFE Java**
Binary Curve B-163	Y	Y	N	N	Y
Koblitz Curve K-163	Y	Y	N	N	Y
Prime Curve P-192	Y	Y	N	N	Y
Binary Curve B-233	Y	Y	N	N	Y
Koblitz Curve K-233	Y	Y	N	N	Y
Prime Curve P-224	Y	Y	N	N	Y
Binary Curve B-283	Y	Y	N	N	Y
Koblitz Curve K-283	Y	Y	N	N	Y
Prime Curve P-256	Y	Y	Y	Y	Y
Binary Curve B-409	Y	Y	N	N	Y
Koblitz Curve K-409	Y	Y	N	N	Y
Prime Curve P-384	Y	Y	Y	Y	Y
Binary Curve B-571	Y	Y	N	N	Y
Koblitz Curve K-571	Y	Y	N	N	Y
Prime Curve P-521	Y	Y	Y	Y	Y

Supported Standards

Standard Type	Standard	BSAFE C/C++ MES	BSAFE CNG	TLS-J ME	BSAFE Java
Key Storage	PKCS #12	Y	N	Y	Y
	PKCS #15	N	N	N	Y
Cryptographic Message Syntax	PKCS #7	Y	N	N	Y
	CMS RFC 5652, RFC 3852, RFC 3369, RFC 2630, RFC 3211	Y	N	N	Y
	Authenticated Enveloped Content RFC 5083	N	N	N	Y
Certificate Request	PKCS #10	Y	N	Y	Y
	Certificate Management Protocol (CMP) RFC 4210	N	N	N	Y
	Certificate Request Message Format (CRMF) RFC 4511	N	N	N	Y
Certificate Revocation	CRL	Y	N	Y	Y
	OCSP	Y	N	Y	Y
Certificate Path Validation	RFC 5280 / RFC 3280	Y	N	Y	Y
	Suite B Profile	Y	N	Y	Y
Transport Layer Security	SSL v3	Y	Y	N	Y
	TLS 1.0 RFC 2246	Y	Y	Y	Y
	TLS 1.1 RFC 4346	Y	Y	Y	Y
	TLS 1.2 RFC 5246	Y	Y	Y	Y
	TLS Extensions RFC 3546	Y	Y	Y	Y
	ECC Cipher Suites RFC 4492	Y	Y	Y	Y
	GCM Cipher Suites RFC5289	Y	Y	Y	Y
	Suite B TLS RFC 5430	Y	Y	Y	Y
	Renegotiation Protection RFC 5746	Y	Y	Y	Y

TLS Cipher Suites

Cipher Suite	BSAFE C/C++ MES	BSAFE CNG	TLS-J ME	BSAFE Java
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Y	Y	N	Y
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Y	Y	N	Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Y	Y	N	Y
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	Y	N	N	Y
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Y	N	N	Y
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	Y	N	N	Y
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	Y	N	N	Y
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Y	Y	N	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Y	N	N	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Y	Y	N	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y	N	Y
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	Y	Y	N	Y
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	Y	Y	N	Y
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	N	Y
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	Y	N	N	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	Y	N	N	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	Y	N	N	Y
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	Y	N	N	Y
TLS_ECDHE_RSA_WITH_RC4_128_SHA	Y	N	N	Y
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	Y	N	N	Y
TLS_ECDH_RSA_WITH_RC4_128_SHA	Y	N	N	Y
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Y	N	Y	Y
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	Y	Y	N	Y
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Y	N	Y	Y
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Y	Y	N	Y
TLS_RSA_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_RSA_WITH_AES_256_CBC_SHA256	Y	Y	N	Y
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	N	N	N	Y
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	N	N	N	Y
TLS_RSA_WITH_AES_256_CBC_SHA	Y	Y	N	Y
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	N	N	N	Y
TLS_DH_RSA_WITH_AES_256_CBC_SHA	N	N	N	Y
TLS_DH_DSS_WITH_AES_256_CBC_SHA	N	N	N	Y

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Y	N	N	Y
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	Y	N	N	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Y	N	Y	Y
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	Y	N	N	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Y	N	N	Y
TLS_RSA_WITH_AES_128_GCM_SHA256	Y	Y	N	Y
TLS_RSA_WITH_AES_128_CBC_SHA256	Y	Y	N	Y
TLS_RSA_WITH_AES_128_CBC_SHA	Y	N	N	Y
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	N	N	N	Y
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	N	N	N	Y
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	N	N	N	Y
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	N	N	N	Y
TLS_DH_RSA_WITH_AES_128_CBC_SHA	N	N	N	Y
TLS_DH_DSS_WITH_AES_128_CBC_SHA	N	N	N	Y
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
SSL_RSA_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA	N	N	N	Y
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA	N	N	N	Y
SSL_RSA_WITH_RC4_128_SHA	Y	N	N	Y
SSL_RSA_WITH_RC4_128_MD5	Y	N	N	Y
SSL_DHE_RSA_WITH_DES_CBC_SHA	Y	N	N	Y
SSL_DHE_DSS_WITH_DES_CBC_SHA	Y	N	N	Y
SSL_RSA_WITH_DES_CBC_SHA	Y	N	N	Y
SSL_DH_DSS_WITH_DES_CBC_SHA	N	N	N	Y
SSL_DH_RSA_WITH_DES_CBC_SHA	N	N	N	Y
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	Y	N	N	Y
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	Y	N	N	Y
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	Y	N	N	Y
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	N	N	N	Y
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	N	N	N	Y
SSL_RSA_EXPORT_WITH_RC4_40_MD5	Y	N	N	Y
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	Y	N	N	Y
SSL_DH_anon_WITH_DES_CBC_SHA	Y	N	N	Y
TLS_ECDH_anon_WITH_AES_256_CBC_SHA	Y	N	N	Y
TLS_DH_anon_WITH_AES_256_GCM_SHA384	Y	N	N	Y
TLS_DH_anon_WITH_AES_256_CBC_SHA256	Y	N	N	Y
TLS_DH_anon_WITH_AES_256_CBC_SHA	Y	N	N	Y
TLS_ECDH_anon_WITH_AES_128_CBC_SHA	Y	N	N	Y
TLS_DH_anon_WITH_AES_128_CBC_SHA256	Y	N	N	Y
TLS_DH_anon_WITH_AES_128_CBC_SHA	Y	N	N	Y
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	Y	N	N	Y
TLS_ECDH_anon_WITH_RC4_128_SHA	Y	N	N	Y
SSL_DH_anon_WITH_RC4_128_MD5	Y	N	N	Y

SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	Y	N	N	Y
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	Y	N	N	Y
TLS_ECDHE_ECDSA_WITH_NULL_SHA	Y	N	N	Y
TLS_ECDHE_RSA_WITH_NULL_SHA	Y	N	N	Y
TLS_ECDH_ECDSA_WITH_NULL_SHA	Y	N	N	Y
TLS_ECDH_RSA_WITH_NULL_SHA	Y	N	N	Y
TLS_RSA_WITH_NULL_SHA256	Y	Y	N	Y
SSL_RSA_WITH_NULL_SHA	Y	Y	N	Y
SSL_RSA_WITH_NULL_MD5	Y	Y	N	Y
TLS_ECDH_anon_WITH_NULL_SHA	Y	N	N	Y
SSL_NULL_WITH_NULL_NULL	Y	N	N	Y