Supported Curves (ECDSA and ECGOST)

Supported ECDSA Curves

The following ECDSA curves are currently supported by the Bouncy Castle APIs:

F_p

X9.62

Curve	Size (in bits)
prime192v1	192
prime192v2	192
prime192v3	192
prime239v1	239
prime239v2	239
prime239v3	239
prime256v1	256

SEC

Curve	Size (in bits)
secp192k1	192
secp192r1	192
secp224k1	224
secp224r1	224
secp256k1	256
secp256r1	256
secp384r1	384
secp521r1	521

NIST (aliases for SEC curves)

Curve	Size (in bits)
P-224	224
P-256	256
P-384	384
P-521	521

F_{2m}

X9.62

Curve	Size (in bits)
c2pnb163v1	163
c2pnb163v2	163
c2pnb163v3	163
c2pnb176w1	176
c2tnb191v1	191
c2tnb191v2	191
c2tnb191v3	191
c2pnb208w1	208
c2tnb239v1	239
c2tnb239v2	239
c2tnb239v3	239
c2pnb272w1	272
c2pnb304w1	304
c2tnb359v1	359
c2pnb368w1	368
c2tnb431r1	431

SEC

Curve	Size (in bits)
sect163k1	163
sect163r1	163
sect163r2	163
sect193r1	193
sect193r2	193
sect233k1	233
sect233r1	233
sect239k1	239
sect283k1	283
sect283r1	283
sect409k1	409
sect409r1	409
sect571k1	571
sect571r1	571

NIST (aliases for SEC curves)

Curve	Size (in bits)

B-163	163
B-233	233
B-283	283
B-409	409
B-571	571

Teletrust

Curve	Size (in bits)
brainpoolp160r1	160
brainpoolp160t1	160
brainpoolp192r1	192
brainpoolp192t1	192
brainpoolp224r1	224
brainpoolp224t1	224
brainpoolp256r1	256
brainpoolp256t1	256
brainpoolp320r1	320
brainpoolp320t1	320
brainpoolp384r1	384
brainpoolp384t1	384
brainpoolp512r1	512
brainpoolp512t1	512

Supported ECGOST (GOST3410-2001) Curves

The following ECGOST curves are currently supported by the Bouncy Castle APIs:

Curve
GostR3410-2001-CryptoPro-A
GostR3410-2001-CryptoPro-XchB
GostR3410-2001-CryptoPro-XchA
GostR3410-2001-CryptoPro-C
GostR3410-2001-CryptoPro-B