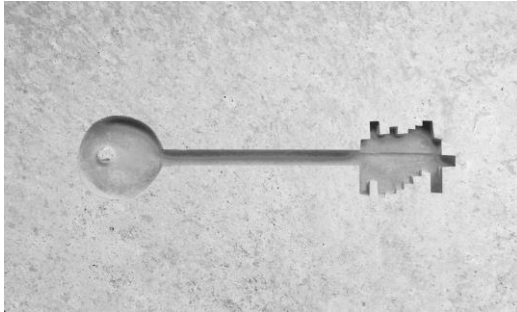# SecurityServer 4.10
Built-in Elliptic Curves

1   SecurityServer 4.10 Elliptic Curves

SecurityServer 4.10 offers a collection of built-in Elliptic Curves. Each curve is specified by its domain parameters and identified by a name. The following table lists all built-in Elliptic Curves by their name, denotes the bit size of their domain parameters (i.e. the key size) and references the specification where the respective curve and its domain parameters are defined.

Elliptic Curve calculations are implemented in firmware on CryptoServer CSe-Series models CSe10 and CSe100, and on Se-Series models Se12 and Se52. Numerous common Elliptic Curves are implemented in hardware on CryptoServer Se-Series models Se500 and Se1500, while other less common Elliptic Curves are implemented on CryptoServer Se-Series models Se500 and Se1500 in firmware as well. Elliptic Curves that are implemented in hardware on CryptoServer Se-Series models Se500 and Se1500 are marked by a ✓ in the last column of the table below.

Name	Size	Reference	HW implementation on Se500 / Se1500
secp112r1	112	[SEC2]	✓
secp112r2	112	[SEC2]	
sect113r1	113	[SEC2]	
sect113r2	113	[SEC2]	
secp128r1	128	[SEC2]	✓
secp128r2	128	[SEC2]	
sect131r1	131	[SEC2]	
sect131r2	131	[SEC2]	
brainpoolP160r1	160	[BP]	
brainpoolP160t1	160	[BP]	✓

utimaco®

SecurityServer 4.10
Built-in Elliptic Curves

Name	Size	Reference	HW implementation on Se500 / Se1500
secp160k1	160	[SEC2]	
secp160r1	160	[SEC2]	
secp160r2	160	[SEC2]	
NIST-K163 / sect163k1	163	[FIPS186-2], [ANSI-X9.62], [SEC2]	
sect163r1	163	[SEC2]	
NIST-B163 / sect163r2	163	[FIPS186-2], [ANSI-X9.62], [SEC2]	
brainpoolP192r1	192	[BP]	
brainpoolP192t1	192	[BP]	✓
NIST-P192 / secp192r1	192	[FIPS186-2], [ANSI-X9.62], [SEC2]	✓
secp192k1	192	[SEC2]	
sect193r1	193	[SEC2]	
sect193r2	193	[SEC2]	
brainpoolP224r1	224	[BP]	
brainpoolP224t1	224	[BP]	✓
NIST-P224 / secp224r1	224	[FIPS186-2], [ANSI-X9.62], [SEC2]	✓
secp224k1	224	[SEC2]	
NIST-K233 / sect233k1	233	[FIPS186-2], [ANSI-X9.62], [SEC2]	
NIST-B233 / sect233r1	233	[FIPS186-2], [ANSI-X9.62], [SEC2]	
sect239k1	239	[SEC2]	
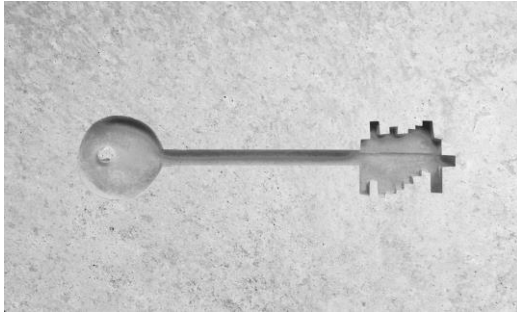
SecurityServer 4.10
Built-in Elliptic Curves

Name	Size	Reference	HW implementation on Se500 / Se1500
brainpoolP256r1	256	[BP]	
brainpoolP256t1	256	[BP]	✓
NIST-P256 / secp256r1	256	[FIPS186-2], [ANSI-X9.62], [SEC2]	✓
secp256k1	256	[SEC2]	
FRP256v1	256	[LEGIFRANCE]	
NIST-K283 / sect283k1	283	[FIPS186-2], [ANSI-X9.62], [SEC2]	
NIST-B283 / sect283r1	283	[FIPS186-2], [ANSI-X9.62], [SEC2]	
brainpoolP320r1	320	[BP]	
brainpoolP320t1	320	[BP]	✓
brainpoolP384r1	384	[BP]	
brainpoolP384t1	384	[BP]	✓
NIST-P384 / secp384r1	384	[FIPS186-2], [ANSI-X9.62], [SEC2]	✓
NIST-K409 / sect409k1	409	[FIPS186-2], [ANSI-X9.62], [SEC2]	
NIST-B409 / sect409r1	409	[FIPS186-2], [ANSI-X9.62], [SEC2]	
brainpoolP512r1	512	[BP]	
brainpoolP512t1	512	[BP]	✓
NIST-P521 / secp521r1	521	[FIPS186-2], [ANSI-X9.62], [SEC2]	✓
NIST-K571 / sect571k1	571	[FIPS186-2], [ANSI-X9.62], [SEC2]	
NIST-B571 / sect571r1	571	[FIPS186-2], [ANSI-X9.62], [SEC2]	
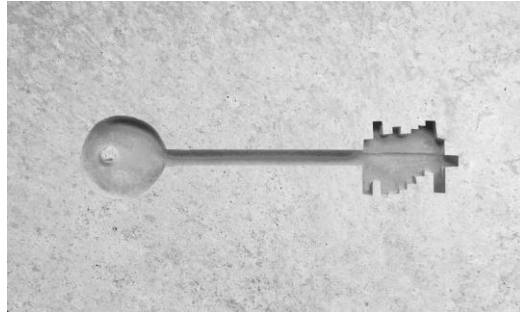
SecurityServer 4.10
Built-in Elliptic Curves

References

Reference	Title
[ANSI-X9.62]	ANS X9.62-2005: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA) / ANSI (American National Standards Institute)
[BP]	ECC Brainpool Standard Curves and Curve Generation, v1.0, 19.10.2005, www.ecc-brainpool.org
[FIPS186-2]	FIPS PUB 186-2, Digital Signature Standard / National Institute of Standards and Technology (NIST), January 2000
[SEC2]	SEC2: Recommended Elliptic Curve Domain Parameters – Certicom Research – September 20, 2000, Version 1.0
[LEGIFRANCE]	Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français (Publication of elliptic curve parameters by the French state), https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024668816