

Product Details

u.trust Anchor FIPS 140-3

Elliptic Curves



u.trust Anchor FIPS 140-3 - Elliptic Curves

Built-in Elliptic Curves

The CXI firmware module of your device can use elliptic curves for ECDSA signature creation, EdDSA signature creation and ECDH key agreement. Each curve is specified by elliptic curve domain parameters and is identified by a name.

The following table lists curves actually approved/allowed for FIPS 140-3. The table shows what is blocked in FIPS mode and what is not implemented. Built-in elliptic curves are listed by their name, denotes the bit size of their domain parameters (i.e. the key length), references the specification where the curve and its domain parameters are defined, and shows what they can be used for.

On high-performance HSM models, numerous common elliptic curves are implemented in hardware.

✓	approved / allowed
—	blocked
✗	Not implemented

Type	Curve	Size	sign	verify	deriveKey	agreeSecret	ECDSA user authentication	generateKey (pair)	Defined in
Weierstrass Curves	P-224 P-256 P-384 P-521	224 256 384 521	✓	✓	✓ in FIPS mode only ECDH_COF with kdf	—	✓	✓	[FIPS186-4], [ANSI-X9.62], [SEC2] [FIPS186-4], [ANSI-X9.62], [SEC2] [FIPS186-4], [ANSI-X9.62], [SEC2] [FIPS186-4], [ANSI-X9.62], [SEC2]
	P-192 K-163 B-163	192 163 163	—	✓	—	—	—	—	[FIPS186-4], [ANSI-X9.62], [SEC2] [FIPS186-4], [ANSI-X9.62], [SEC2] [FIPS186-4], [ANSI-X9.62], [SEC2]

u.trust Anchor FIPS 140-3 - Elliptic Curves

Type	Curve	Size	sign	verify	deriveKey	agreeSecret	ECDSA user authentication	generateKey (pair)	Defined in
Weierstrass Curves	K-233	233	⊖	✓	⊖	⊖	⊖	⊖	[FIPS186-4], [ANSI-X9.62], [SEC2]
	K-283	283							[FIPS186-4], [ANSI-X9.62], [SEC2]
	K-409	409							[FIPS186-4], [ANSI-X9.62], [SEC2]
	K-571	571							[FIPS186-4], [ANSI-X9.62], [SEC2]
	B-233	233							[FIPS186-4], [ANSI-X9.62], [SEC2]
	B-283	283							[FIPS186-4], [ANSI-X9.62], [SEC2]
	B-409	409							[FIPS186-4], [ANSI-X9.62], [SEC2]
	B-571	571							[FIPS186-4], [ANSI-X9.62], [SEC2]
Montgomery Curves	curve25519 curve448	255 448	✗	✗	⊖	⊖	✗	⊖	[RFC 7748] with Errata ID 4730 [RFC 7748] with Errata ID 4730
Twisted Edwards Curves	Edwards25519 Edwards448	255 448	✓ only EdDSA	✓ only EdDSA	✗	✗	✗	✓	[RFC 7748] with Errata ID 4730 [RFC 7748] with Errata ID 4730
Brainpool Curves	brainpoolP224r1	224	✓	✓	✓	⊖	✓	✓	[BP]
	brainpoolP256r1	256							[BP]
	brainpoolP320r1	320							[BP]
	brainpoolP384r1	384							[BP]
	brainpoolP512r1	512							[BP]
	+ twisted variants								
	brainpoolP224t1	224							[BP]
	rainpoolP256t1	256							[BP]
	brainpoolP320t1	320							[BP]
	brainpoolP384t1	384							[BP]
	brainpoolP512t1	512							[BP]

u.trust Anchor FIPS 140-3 - Elliptic Curves













Type	Curve	Size	sign	verify	deriveKey	agreeSecret	ECDSA user authentication	generateKey (pair)	Defined in
	assuming the module verifies the domain parameter validity to ensure the correct curves are used (i.e., not its quadratic twist)*								
Curve secp256k1 (Koblitz, security strength of 128 bits)	secp256k1	256	 only for use with blockch ain applicati ons	 only for use with blockchai n applicatio ns				 only for use with blockchain applicatio ns	[SEC2]
French Curve	FRP256v1	256							[ANSSI]

Table 1: List of built-in elliptic curves

u.trust Anchor FIPS 140-3 - 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)
[ANSSI]	ANSSI (Agence nationale de la sécurité des systèmes d'information): "Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français", Journal officiel de la République française (JORF), n° 0241 du 16 octobre 2011 page 17533 text n° 30 (Announcement about elliptic curve parameters set by the French government). NOR: PRMD1123151V. Available: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024668816
[BP]	RFC 5639, ECC Brainpool Standard Curves and Curve Generation, March 2010
[FIPS186-4]	FIPS PUB 186-4, Digital Signature Standard / National Institute of Standards and Technology (NIST), July 2013
[RFC7748]	RFC 7748 Elliptic Curves for Security, January 2016
[SEC2]	SEC2: Recommended Elliptic Curve Domain Parameters – Certicom Research – January 27, 2010, Version 2.0