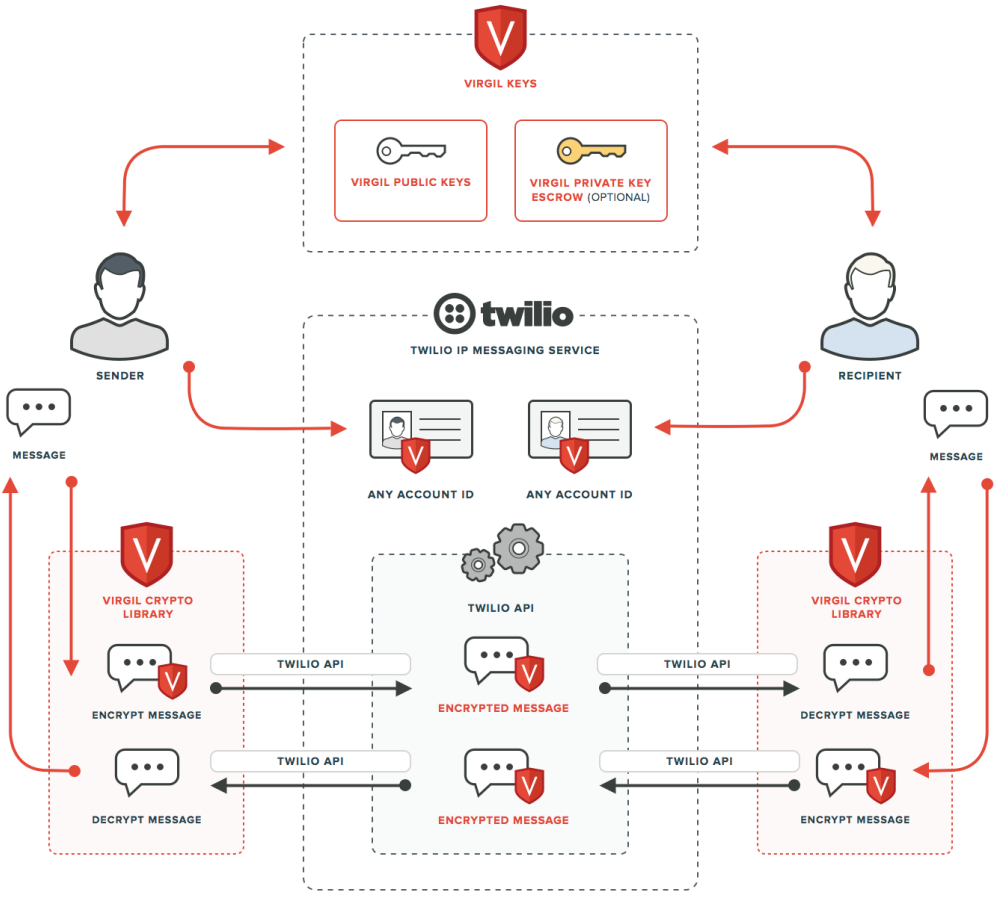
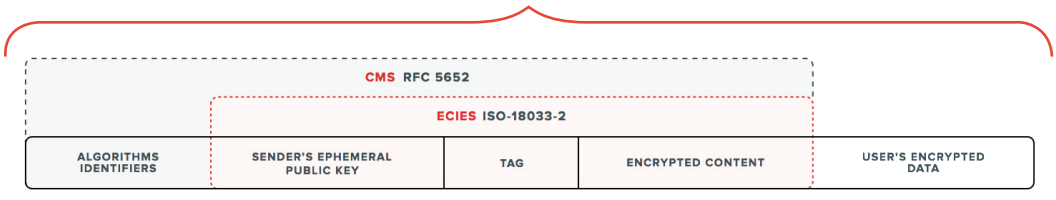
VIRGIL SECURITY

IP messaging



Virgil Cryptogram



Virgil is:

Virgil ECIES Defaults

Encryption	AES256
Elliptic Curve	Brainpool 512
Hashing	SHA512
Signature	ECDSA

NSA Suite B Compliance mode

Virgil Framework

Cryptographic Message Syntax	RFC 5652
Encryption	ISO 18033-2, SECG SEC1

Cryptography Functions

Key Generation	CTR-DRBG, NIST SP 800-90A
Key Derivation	KDF1, ISO-18033-2 Clause 6.2.2
Entropy Source	Platform dependent, multi source support
Key Exchange (EC)	ECDH, NIST SP 800-56A
Key Exchange (RSA)	NIST SP 800-56B rev 1
Signature	ECDSA, EdDSA (available soon)
Hashing	SHA2, FIPS Pub 180-4
Symmetric(AES)	AES, FIPS Pub 197, GOST 28147-89
Asymmetric(EC)	**Brainpool** bp256r1, bp384r1, bp512r1
	Koblitz secp192k1, secp224k1, secp256k1
	NIST secp192r1, secp224r1, secp256r1, secp384r1, secp521r1
	Curve 25519 (available soon)

Platforms and Languages

With more to come: