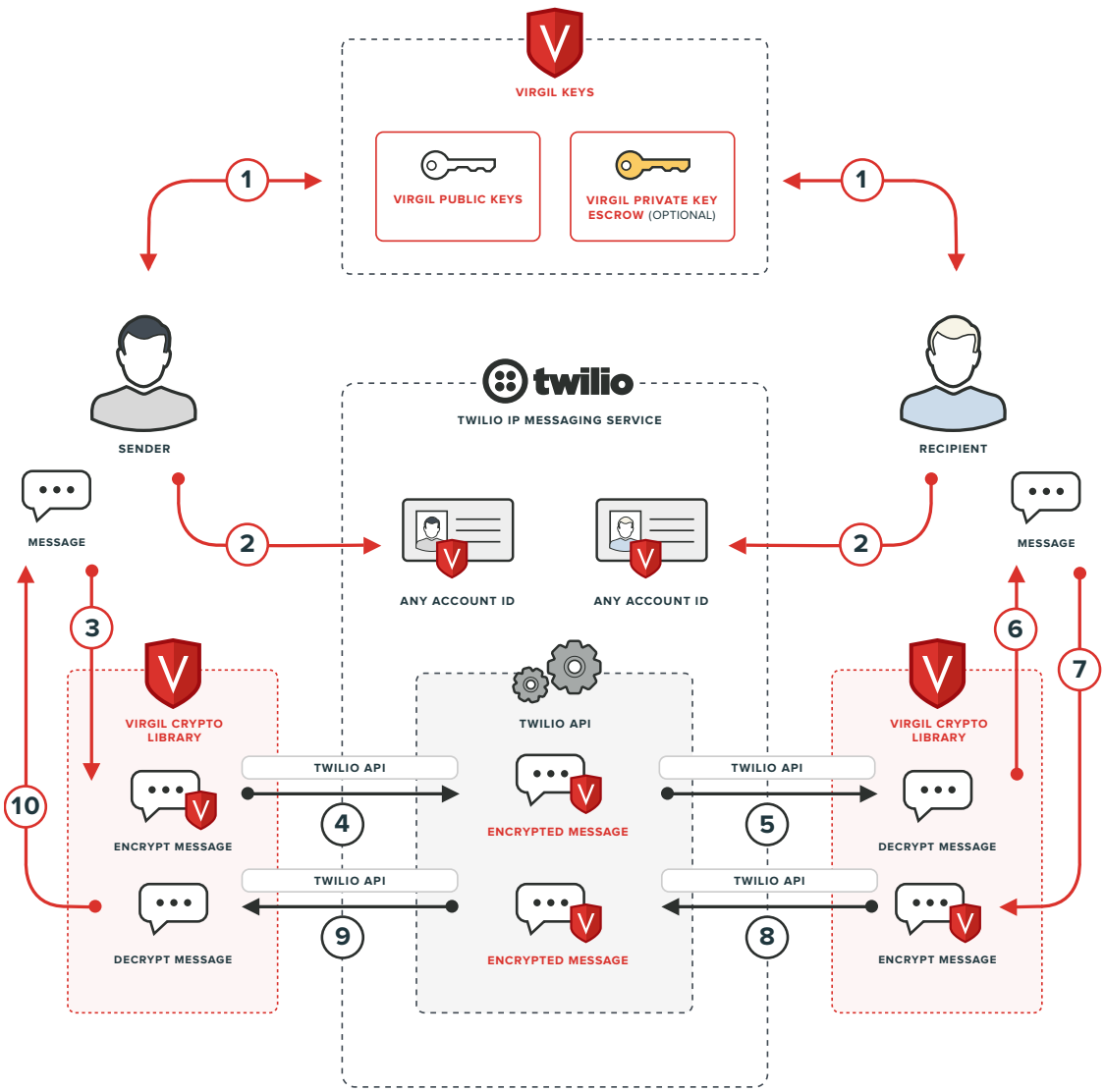
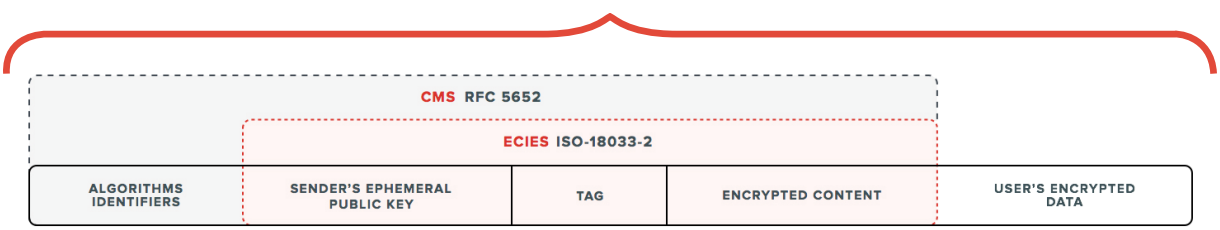
VIRGIL SECURITY + twilio

Twilio IP Messaging with Virgil Security



Virgil Cryptogram



Virgil Uses

Virgil ECIES Defaults

DESCRIPTION	AES256
ELLIPTIC CURVE	Brainpool 512
HASHING	SHA384
SIGNATURE	ECDSA

NSA Suite B Compliance mode

Virgil Framework

CRYPTOGRAPHIC MESSAGE SYNTAX	RFC 5652
ENCRYPTION	ISO 18033-2, SECG SEC1

Crytography 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	SHA-2, 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 & Languages

WITH MORE TO COME: