VIRGIL SECURITY

SECURE THE FUTURE

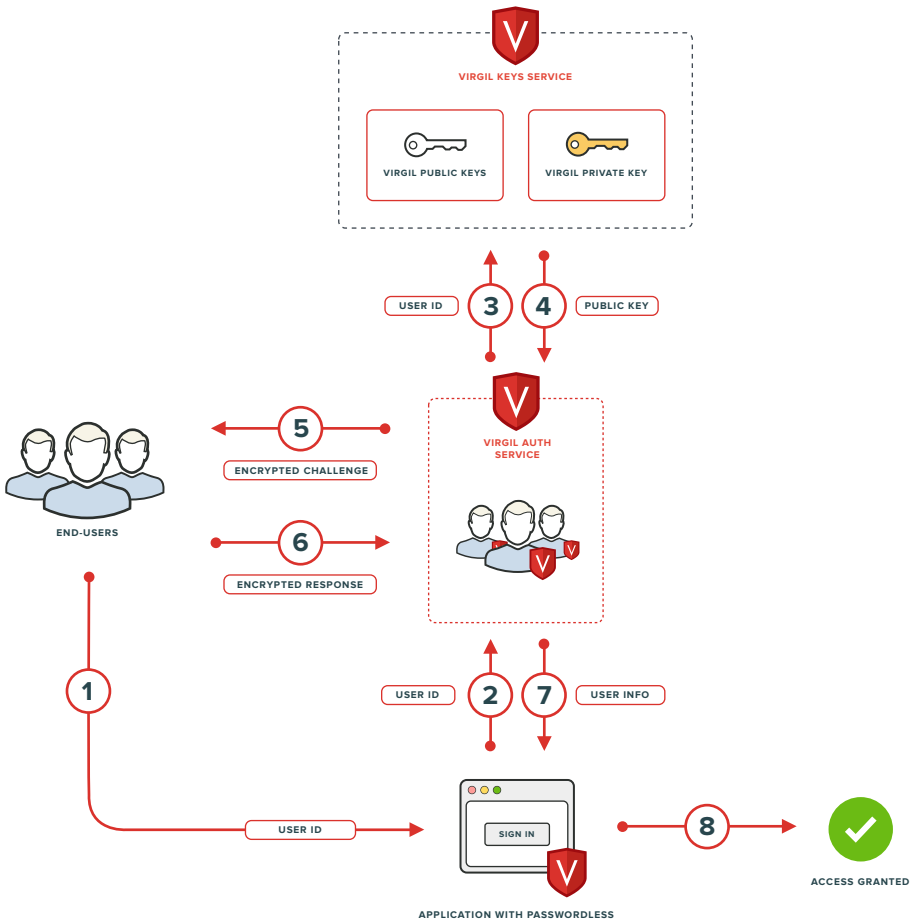
Authentificate. Encrypt. Verify. Everything.

virgilsecurity.com

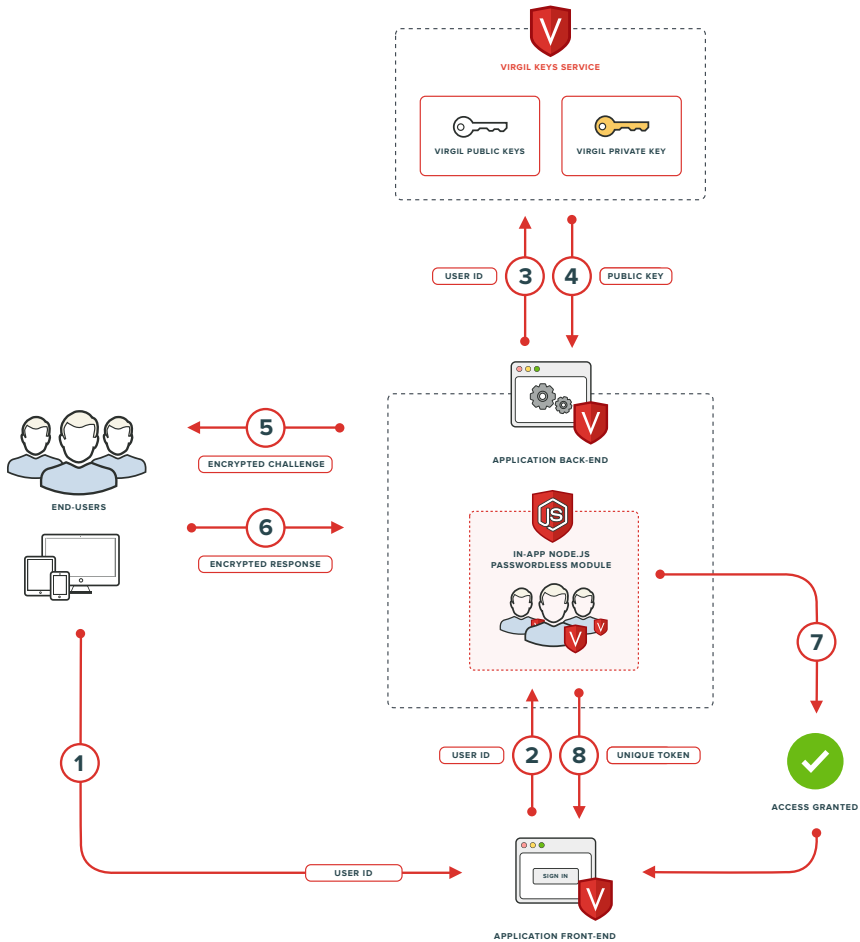
support@virgilsecurity.com

@virgilsecurity

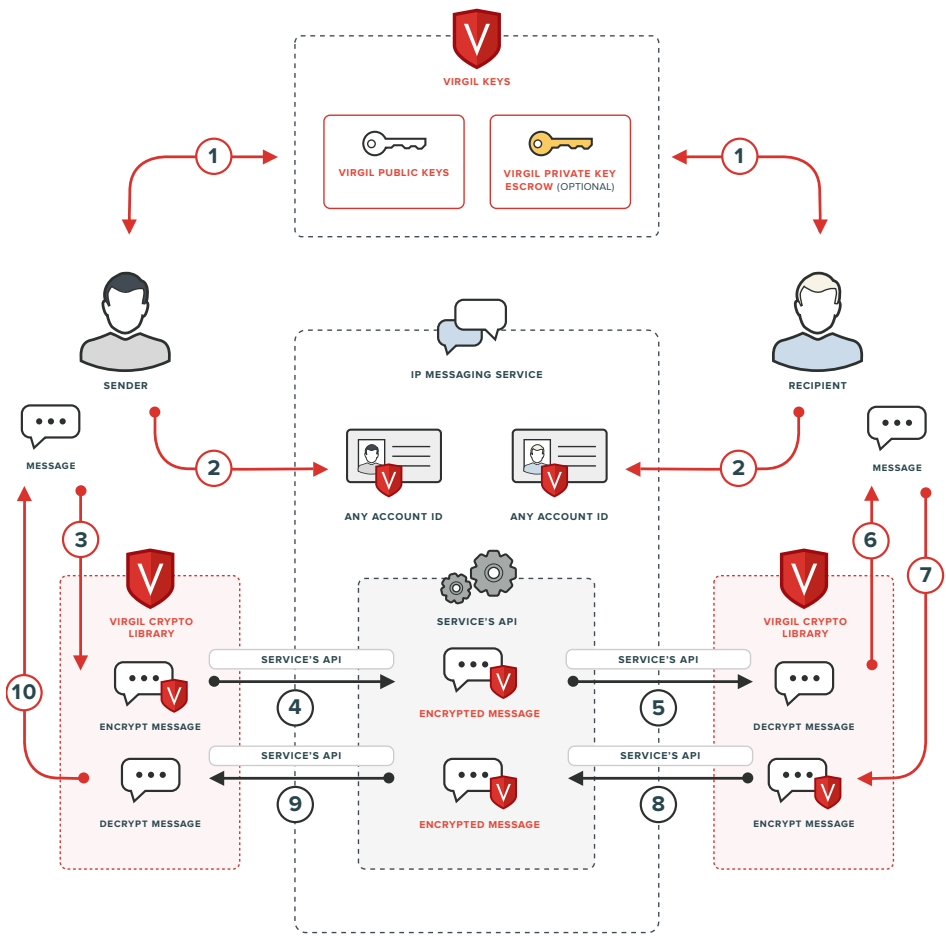
Passwordless Authentication with Virgil Security



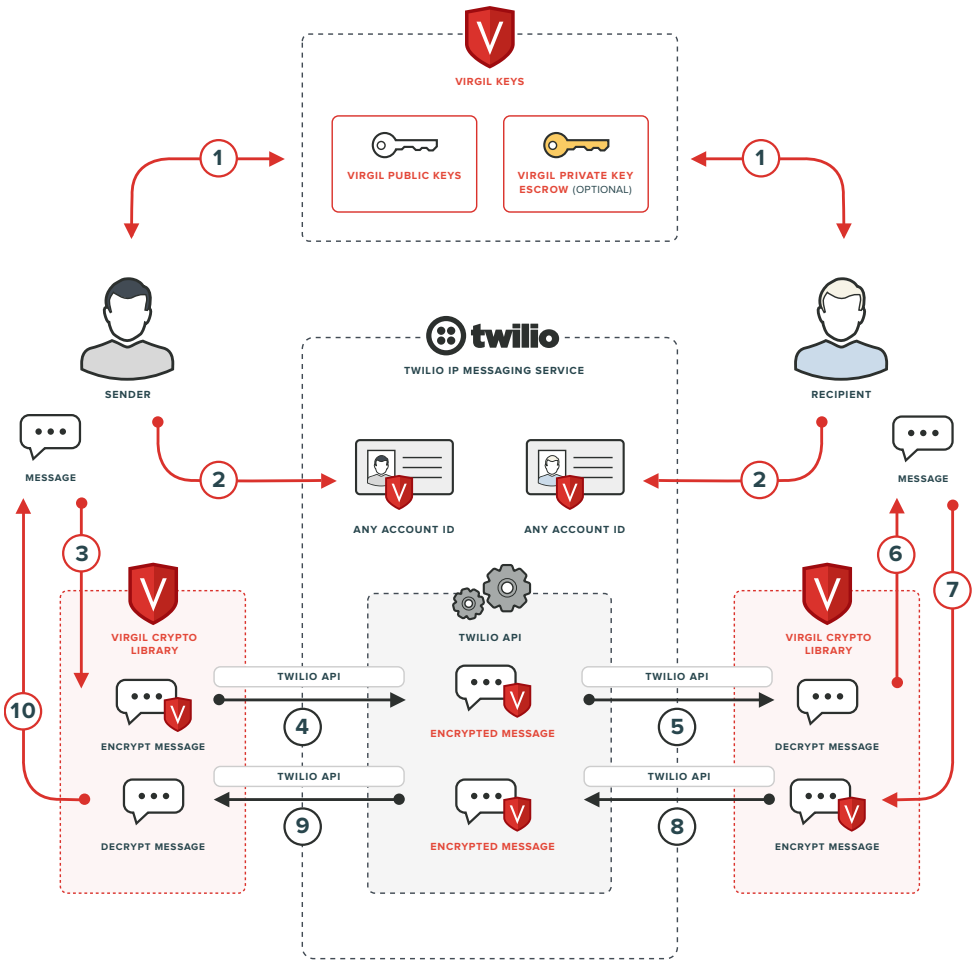
Passwordless Module for Your Application



IP Messaging with Virgil Security



Twilio Chat with Virgil Security



Virgil Uses

Virgil ECIES Defaults

DESCRIPTION	AES256
ELLIPTIC CURVE	Brainpool 512
HASHING	AES256
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	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 & Languages

WITH MORE TO COME:

Thanks for Attention!

www.virgilsecurity.com

support@virgilsecurity.com

@virgilsecurity

github.com/virgilsecurity

virgilsecurity.com