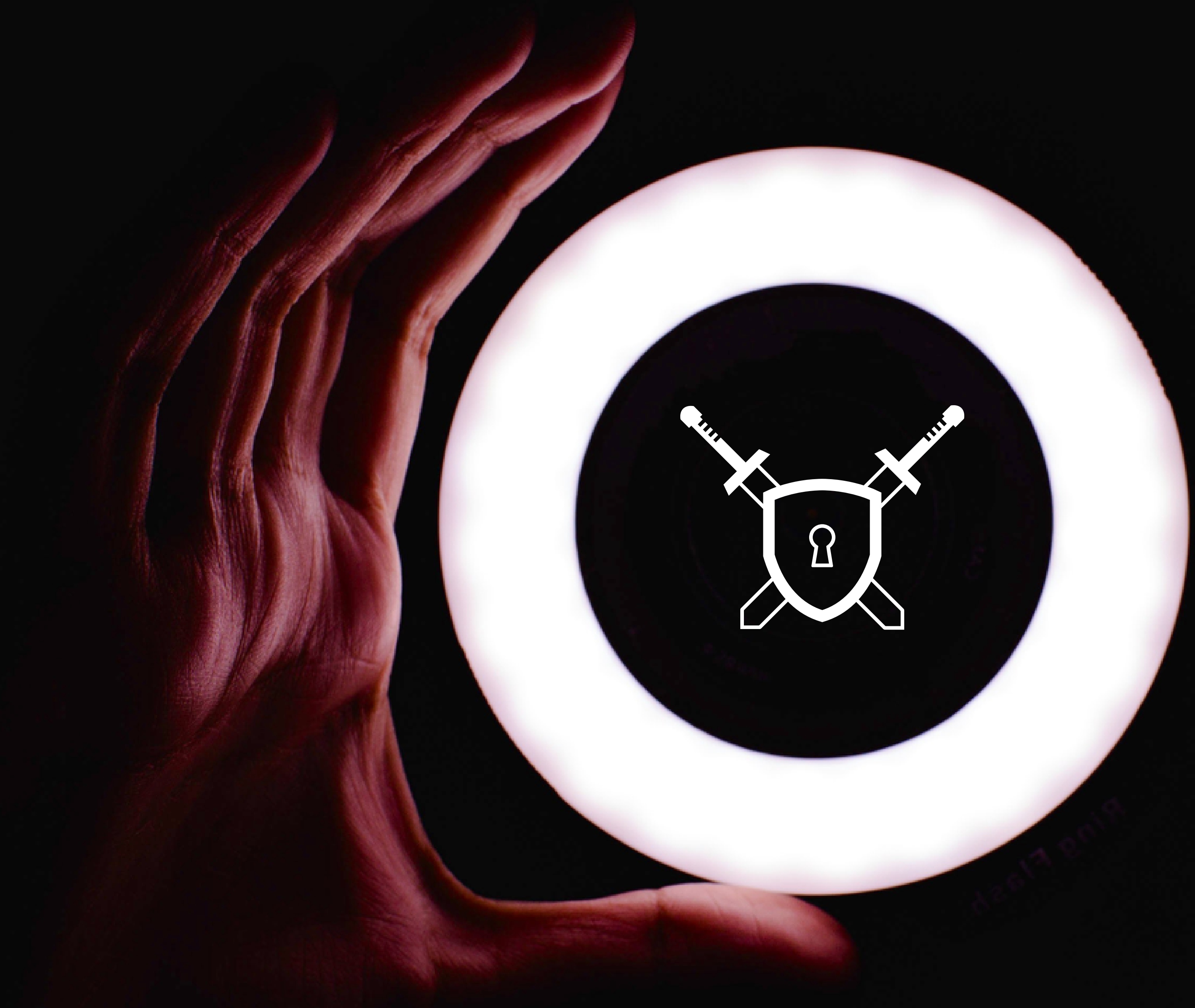




VIRGIL SECURITY

A distributed trust system. Apps. Devices. Users.

We provide full transparency in everything from crypto libraries to application trust. You have full control of trust between you and your customers.

 VirgilSecurity.com

 passwOrd.io

 github.com/VirgilSecurity

DMYTRO MATVIIV

dmytro.matviiv@virgilsecurity.com

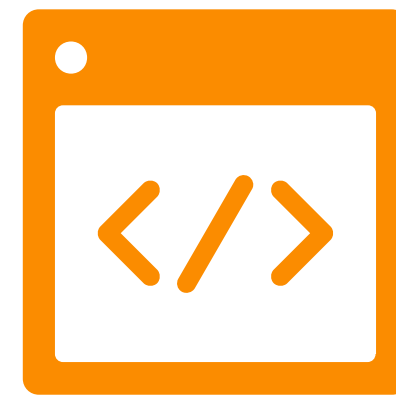
2

Virgil: Crypto Library

High-level open source cryptographic library that allows you to perform the all necessary operations for securely storing and transferring data with everything needed to become HIPAA and GDPR compliant.



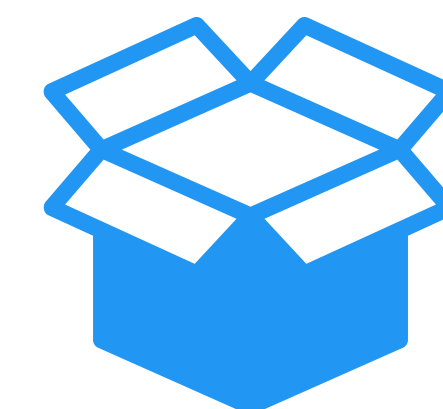
Open-source



Available for different
platforms and languages



Works on IoT
hardware



Works with 3rd
party SDK

SUPPORTED ALGORITHMS

KEY GENERATION

CTR-DRBG [[NIST SP 800-90A](#)]

ELLIPTIC CURVES

Ed25519 [[RFC8032](#)]

X25519 [[RFC7748](#)]

Koblitz [[secp192k1](#), [secp224k1](#), [secp256k1](#)]

Brainpool [[bp256r1](#), [bp384r1](#), [bp512r1](#)]

Nist [[secp256r1](#), [secp192r1](#), [secp224r1](#),
[secp384r1](#), [secp521r1](#)]

KEY EXCHANGE (RSA)

X25519 [[RFC7748](#)]

ECDH [[NIST SP 800-56A](#)]

RSA [[NIST SP 800-56B](#)]

ENTROPY SOURCE

Linux [[/dev/urandom](#)]

Windows [[CryptGenRandom\(\)](#)]

SYMMETRIC

AES GCM [[NIST SP 800-38D](#)]

AES CBC [[RFC3602](#)]

Chacha20-Poly1305 [[RFC7539](#)]

KEY DERIVATION

KDF [[RFC2898](#)]

HKDF [[RFC5869](#)]

SIGNATURE

Ed25519 [[RFC8032](#)]

ECDSA [[FIPS PUB 186-4](#)]

RSASSA-PSS [[RFC4056](#)]

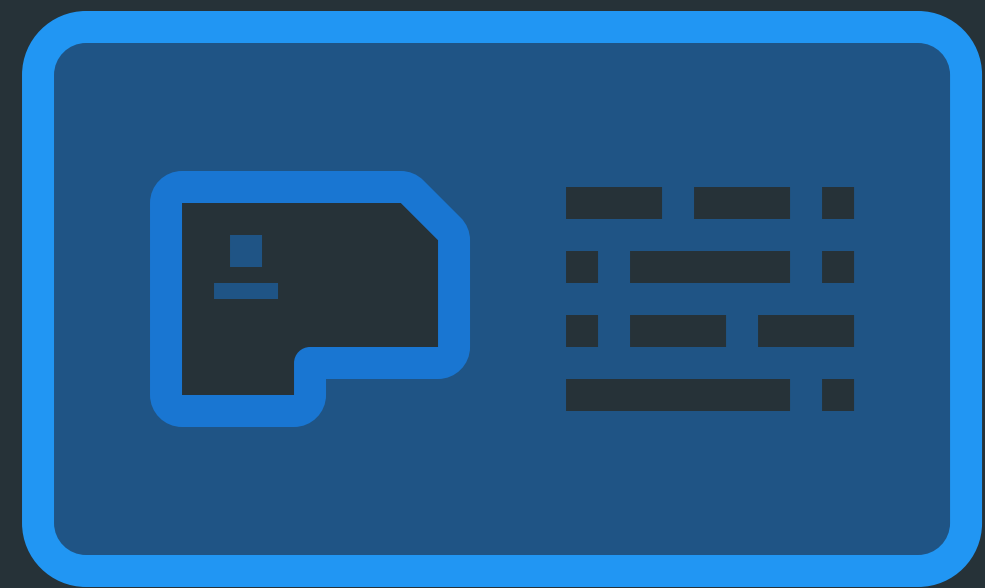
HASHING

SHA-2 (256*/384*/512) [[RFC4634](#)]

Blake2 [[RFC7693](#)]

Virgil Cloud: Services

Global, verifiable and flexible key infrastructure that provides full end-to-end security.



Cards Service

Stores and manages user and device cards with public keys and associated information.



KeyKnox Service

Helps users securely store authentication keys, identity keys, chat thread keys, passwords, etc., as well as share and synchronize them between devices.



Brainkey Service

Generates Brainkey – strong cryptographic key based on user passphrase, which can be used for end-to-end encryption, Brainwallet, authentication, etc.

PFS Service

Manages one-time and long-time cards, which are used to solve a Perfect Forward Secrecy scenario.

PasswOrd Service

Implementation of the Password-Hardened Encryption (PHE) protocol. Protects user passwords from offline attacks and makes stolen passwords useless even if database has been compromised.

Identity Service

Validates user identities in messaging, email, applications, etc.

Auth Service

Provides authorization for users and devices. Service is used to deploy high-availability authentication and transaction-signing capabilities at mass scale.

IoT & IIoT Services

Everything you need to identify and manage IoT devices for personal use and industrial IoT devices to enhance manufacturing and industrial processes.

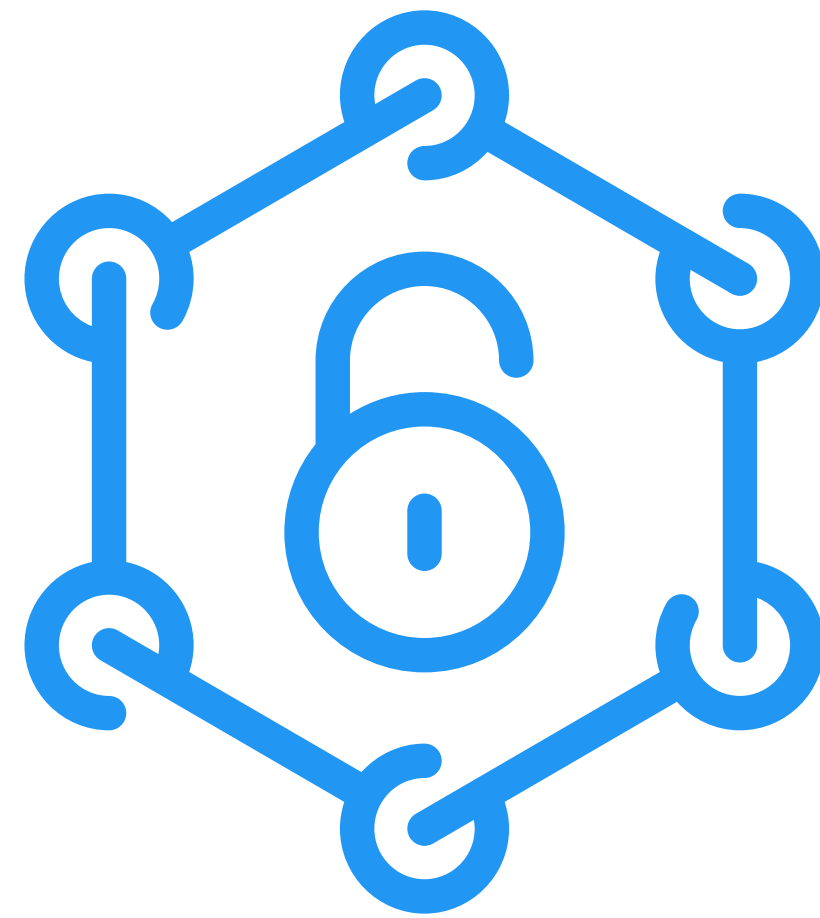
Virgil: NoiseSocket

Perfect for IoT extensible service with simple wire protocol and minimal overhead.

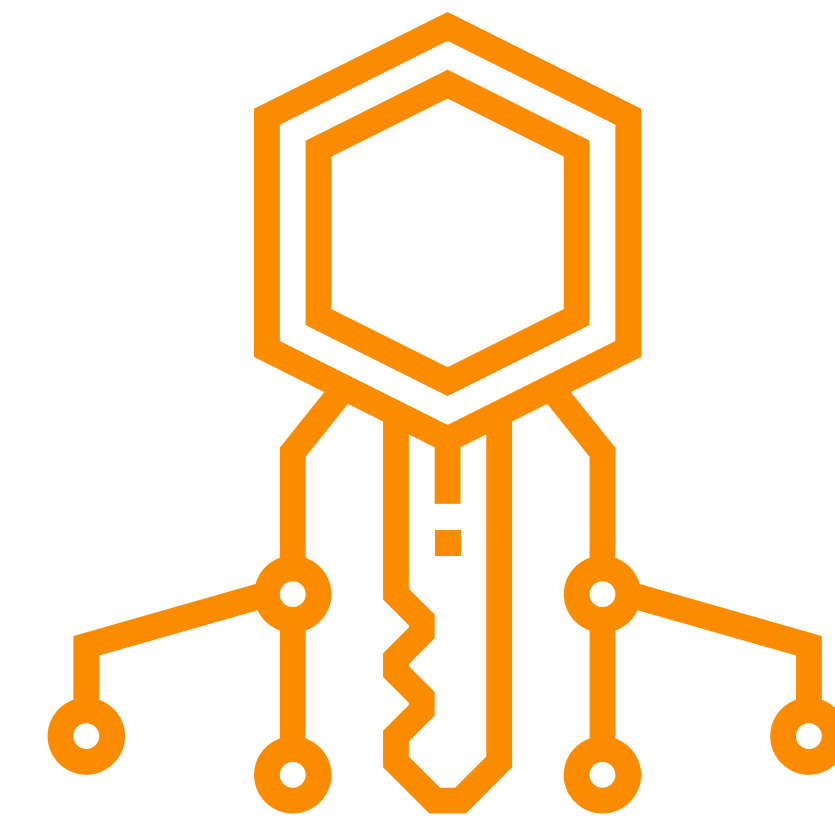
NoiseSocket can encode Noise messages and associated negotiation data into a form suitable for transmission over reliable, stream-based protocols such as TCP. Stores and manages User Cards with Public Keys and associated information. Small and simple codebase, works without certificates, build in padding and fast crypto primitives by default.



One of the patterns
(Noise_IK, 0-RTT) has formal
security proof by WireGuard



Transport Secure
Protocol encrypts any
TCP connection



Advanced options like
0-RTT, Perfect Forward
Secrecy and pre-shared keys

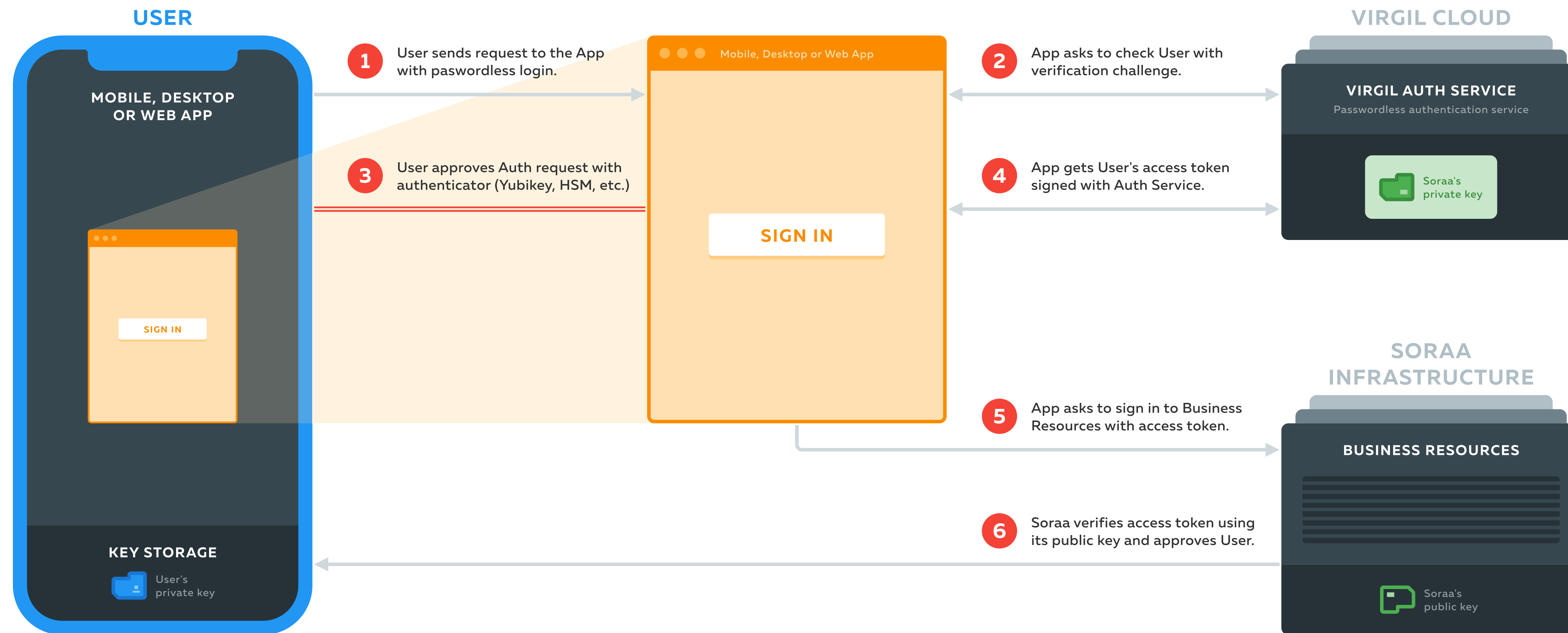
Soraa: Infrastructure Management

Virgil Security helps Soraa to build protected IoT ecosystem from manufacturing to cloud services.



Soraa: Passwordless Authentication

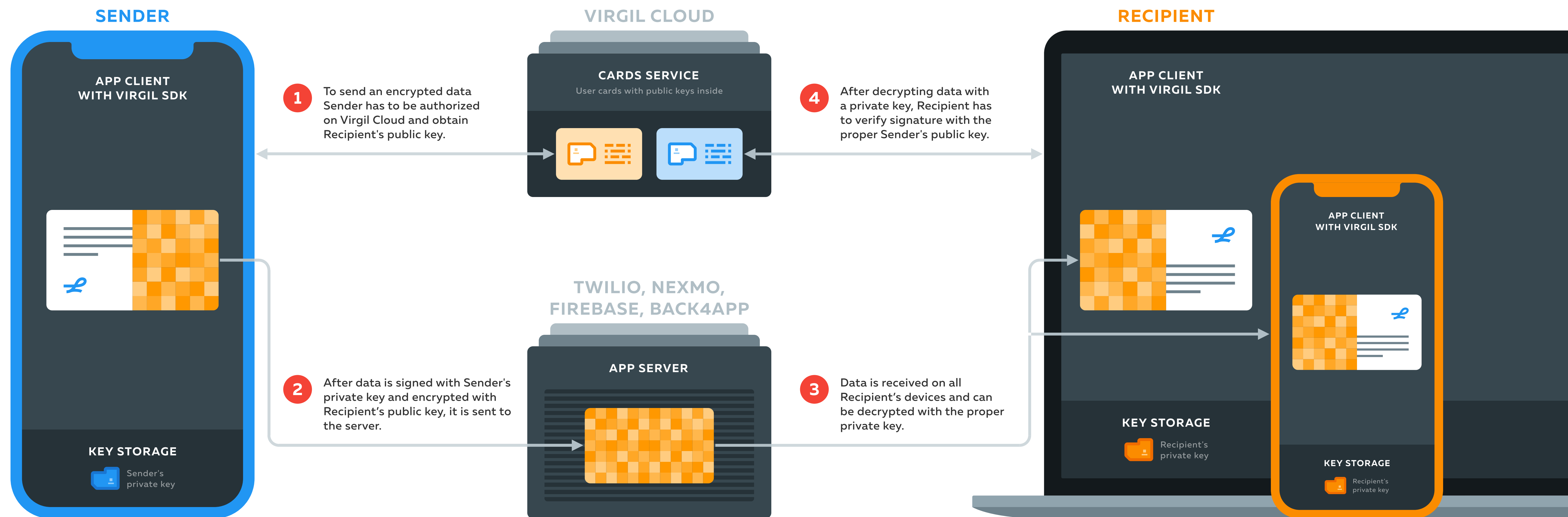
Improve security for your services and your users. Fast and easy-to-use way to authenticate clients on your server.



7

Twilio, Nexmo, Firebase, Back4App: Encrypted Communication

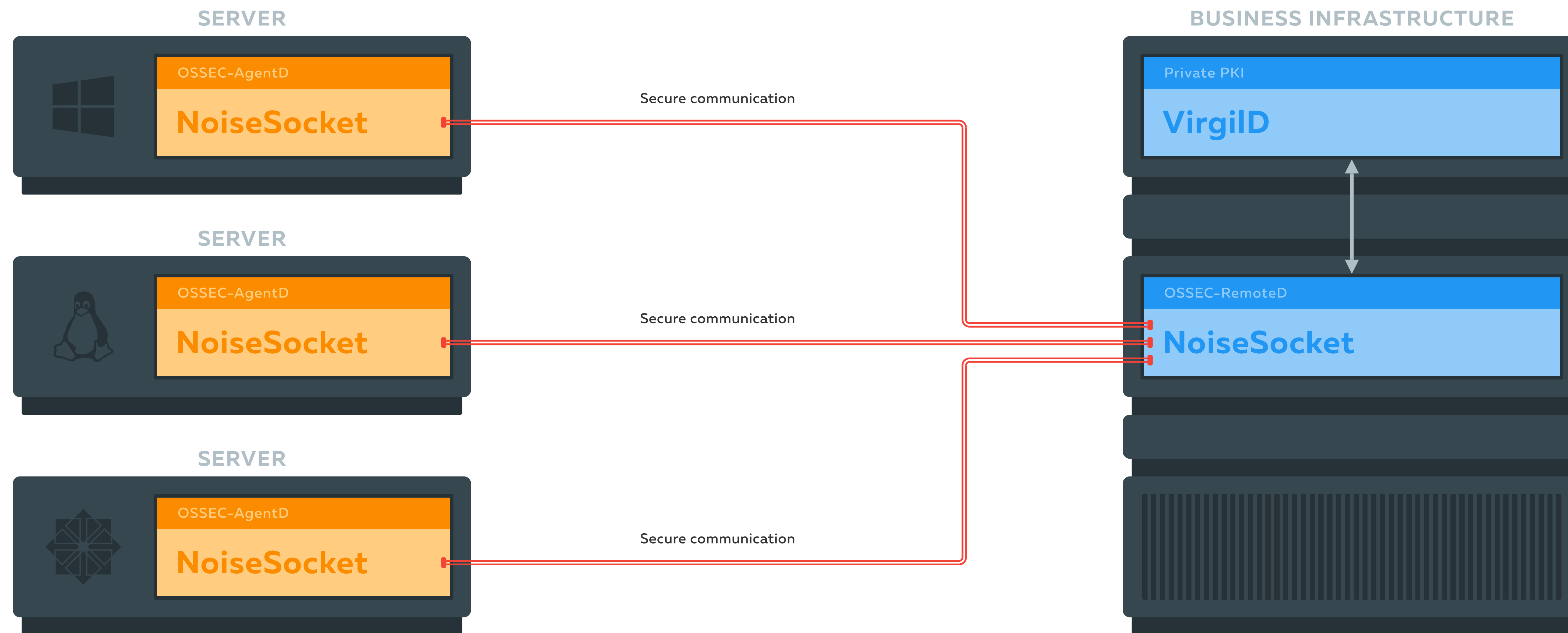
Build end-to-end encrypted applications on any platform with multi-device support, 1.9¢ per public key.



8

Omnicom-OSSEC: NoiseSocket

Identify, verify and protect all connections in your host-based intrusion detection systems.



lotelic: Crypto Chip

Use free crypto library inside your chips for adding secure boot to IoT device design.

