VIRGIL SECURITY

A distributed trust system. Apps, devices, users.

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

VirgilSecurity.com GitHub.com/VirgilSecurity

---

by Dmytro Matviiv
dmytro.matviiv@virgilsecurity.com

VIRGIL SECURITY .COM

Introducing Virgil Security

We make every developer a security expert. Public key management as a service and easy-to-use cryptographic software building blocks.

HEADQUARTERS

Manassas

VA

ESTABLISHED

2014

NO. OF EMPLOYEES

38

Primarily Kyiv

KEY EXECUTIVES

CEO Michael W. Wellman

CTO Dmitry Dain

TOTAL INVESTED

$4.9 M

MOST RECENT FINANCING

$4 M Series A

Oct 2016

NEXT FINANCING

Q2 2019

VIRGIL SECURITY .COM

Virgil Cryptographic and SDK Libraries

High-level open-source cryptographic libraries that allow you to perform all the necessary operations for securely storing and transferring data for HIPAA and GDPR compliance.

Open-source

Available for different platforms

Works on IoT hardware

Supports 3rd party SDKs

SUPPORTED PLATFORMS

Cryptographic Library is suitable for:

- **Linux, MacOS and Windows** on desktop;
- **Android, iOS, tvOS and watchOS** on mobile;
- **Various browsers** for web.

SUPPORTED LANGUAGES

Cryptographic Library is written in C++ and supports bindings for the following programming languages: **C, C++, C#, Go, Java, JavaScript, PHP, Python, Ruby**.

Languages that can use the Virgil Cryptographic Library directly, without any bindings: **Objective-C and Swift**.

SUPPORTED ALGORITHMS

Hashing: **SHA-2 (256/384/512) and Blake2**.

Digital signature: **Ed25519, ECDSA and RSASSA-PSS**.

Key generation: **CTR-DRBG**.

Key derivation: **KDF2 and HKDF**.

Key exchange: **X25519, ECDH and RSA**.

Symmetric algorithms: **AES GCM and AES CBC**.

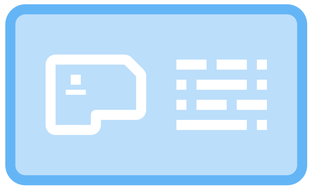
Elliptic curves: **Ed25519, X25519, Koblitz** (secp192k1, secp224k1, secp256k1), **Brainpool** (bp256r1, bp384r1, bp512r1), **NIST** (secp256r1, secp192r1, secp224r1, secp384r1, secp521r1).

Full specification: github.com/virgilsecurity/virgil-crypto

VIRGIL SECURITY .COM

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's 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.

PHE Service

Implementation of the Password-Hardened Encryption (PHE) protocol. Protects users' passwords from offline attacks and makes stolen passwords useless even if the 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 a mass scale.

IoT & IIoT Services

Contain everything you need to identify and manage IoT devices for personal use and industrial IoT devices in order to enhance manufacturing and industrial processes.

VIRGIL SECURITY .COM

Introducing PURE

Virgil Security presents a free toolkit that protects users' passwords from data breaches and both online and offline attacks.

Virgil's PURE is an implementation of the Password-Hardened Encryption (PHE) protocol that provides developers with a **technology to protect users passwords from offline/online attacks** and makes stolen passwords useless even if your database has been compromised.

PHE is a new, more secure mechanism that protects user passwords and **lessens the security risks associated with weak passwords**. Neither Virgil nor attackers know anything about user passwords.

Authors of the PHE protocol: **Russell W. F. Lai, Christoph Egger, Manuel Reinert, Sherman S. M. Chow, Matteo Maffei and Dominique Schroder.**

Protection from online and offline attacks

User data encryption with a personal key

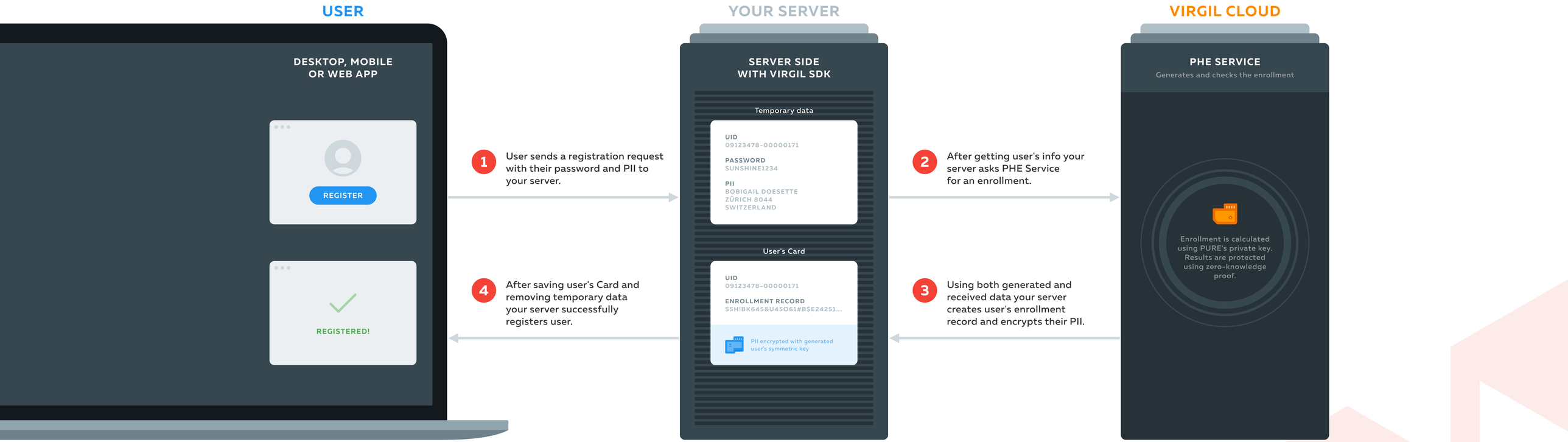
No trust, no cost, no downtime

Instant invalidation of stolen databases

VIRGIL SECURITY .COM

PURE: Create a Record

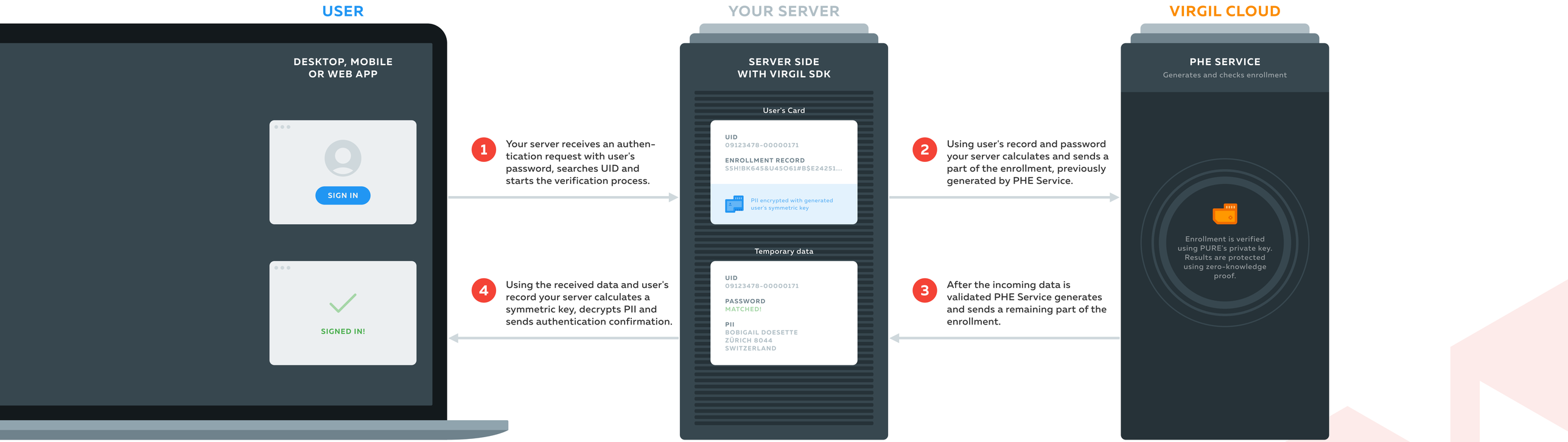
Create a protected user password and generate a user symmetric key to encrypt personally identifiable information (PII).



VIRGIL SECURITY .COM

PURE: Retrieve a Record

Verify a user password with the record from your database every time when the user signs in.



Want to work with Virgil Security?

Contact me anytime via dmytro.matviiv@virgilsecurity.com

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

VirgilSecurity.com GitHub.com/VirgilSecurity