VERIDIUMID

Safeguard your most critical assets by proving identity with single-step multi-factor biometric authentication.

OVERVIEW

The main problem with passwords is that they do not actually authenticate the person using them. The same is true for traditional multi-factor authentication solutions like security codes, PINs, one-time passwords or tokens – none actually identify the user. In addition, these methods are too easily stolen, shared, or cracked, which is one of the reasons why, despite the prevalence of MFAs, nearly two-thirds of all security breaches are due to weak or stolen credentials.

It may finally be time to eliminate these complicated systems altogether. The key is to deploy biometrics as part of a genuine, end-to-end authentication solution, either as a second factor or, even better, as the primary authentication factor, replacing passwords, PINs and tokens with single-step multi-factor biometric authentication.

Biometrics replaces something you know or have, with something you are. All from the convenience of your smartphone.

USE CASES

- Password Replacement
- Token Replacement
- OTP/SMS Replacement
- Single Sign-On
- Remote Access (VPN) Authentication
- Digital Banking
- Identity Verification/KYC
- Electronic Healthcare Record Access
- Healthcare Endpoint Access
- Electronic Prescription Renewal
- Government & Law Enforcement Identity Verification

SINGLE-STEP MULTI-FACTOR BIOMETRIC AUTHENTICATION

VeridiumID works in conjunction with a mobile app to provide single-step multi-factor biometric authentication. Matching can take place on the mobile device or a back-end server hosted in the cloud or on-premises. You can even choose where to store biometric vectors – on the phone, on a server, or split between the two. This puts your company in complete control over user authentication. Built on the IEEE 2410 open standard, it is one of the most flexible biometric authentication solutions on the market today.

THE COMPONENTS

Front-End Mobile SDK

The mobile SDK, available for iOS and Android, is an app development kit that can embed biometric authentication capabilities into any enterprise or consumer app. It includes the systems needed to capture, encrypt, and securely store biometric vectors, as well as a customizable UI and communication module to connect with the back-end server software.

Back-End Server Software

Our server software acts as the authority for authentication matching. It provides the analytics and reporting tools that businesses require to monitor the security and stability of their identity and access management systems. The flexibility of an enterprise-ready software solution allows you to customize the storage and matching of biometrics according to your company's security needs. Data storage and matching can be done on the server, on the mobile device (making it FIDO compliant), or with the biometric data broken up and distributed between the mobile device and the server. This final method, the Distributed Data Model using visual cryptography, provides the most advanced security.

Distributed Data Model

Our Distributed Data Model is a multi-part process that covers encryption and storage of the biometric vector. First, the scanned biometric template is encrypted with Visual Cryptography, a secret sharing scheme. This allows us to encrypt the vector randomly into two separate pieces and avoid creating a key like other encryption methods. This gives you the option to store one piece on the mobile device and send the other to the server.

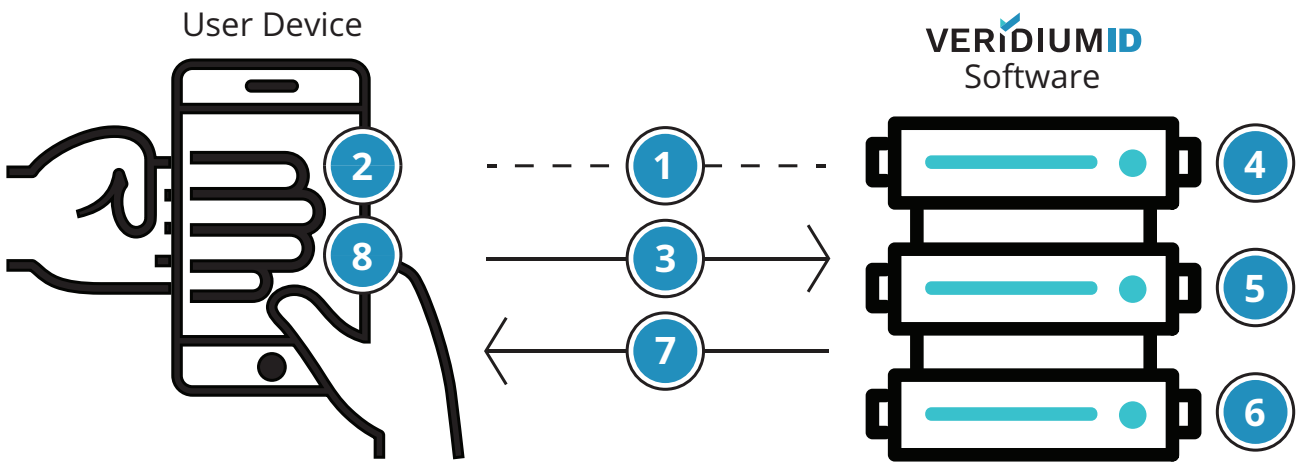
This method protects biometric vectors from being compromised or stolen. The vector cannot be recombined by hackers, or an insider threat, even if they get into one system or the other. Anyone breaching the system would have to pull the vectors for each individual device, and have physical access to the device, as well as the server, in order to recreate the template.

HOW IT WORKS

Once you deploy the back-end software and integrate the SDK with a mobile app, the first step is to register. This involves some method of proving identity. For example, by proving ownership with an email address, employee ID, mobile phone number, government ID, or other verifiable proof of identity.

Once verified, a person scans their biometrics (face, fingers, etc.), which are immediately encrypted and stored. The back-end then sends a signed client certificate to the phone, which stores it in the device's secure storage space to be used during authentication.

To start the authentication process, a user opens the mobile app, which authenticates the session with the back-end using the signed client certificate. This certificate verifies that the user is in the system and owns the mobile device. The user then scans their biometric, producing a new authentication vector. This new vector is matched against the original vector. If the biometric match is successful, the user is authenticated and able to access the application, data, or secure location.



1. The user initiates registration on their smartphone.
2. The VeridiumID SDK captures and breaks up their biometric vector.
3. The SDK sends the encrypted vector piece, user account information and certificate signing request to the VeridiumID server.
4. The VeridiumID server validates the user account on their company database.
5. The company database sends the validation results to the VeridiumID server.
6. The VeridiumID server stores the user's encrypted vector piece and signs the client certificate.
7. The VeridiumID server sends the signed client certificate to the user's phone.
8. The client certificate and other encrypted vector piece are stored in the mobile device's secure storage.

BENEFITS

IDENTITY AUTHENTICATION

At the core of VeridiumID is identity. User identity is authenticated using their biometrics. The pairing of a user's biometric with their device becomes their password. With biometric authentication, you use identity to secure access to your most valuable assets.

SINGLE-STEP MULTI-FACTOR AUTHENTICATION

The solution provides single-step multi-factor biometric authentication to users, combining what the user knows, has, and is. The PIN to unlock the phone is an external factor – what the user knows, the device itself is what the user has, and the biometric represents what the user is.

MULTIMODAL BIOMETRICS

The SDK allows you to use any type of biometric from any vendor, including voice, 4 Fingers, Touch ID, or Face ID. This gives you complete flexibility over what biometrics to use depending on the use case and environment.

IT CONTROL

The back-end server software includes an Administrative Dashboard, which provides real-time risk management monitoring and full customization of features, analytics, and reporting.

OPEN STANDARD

VeridiumID is built on IEEE 2410, the Biometrics Open Protocol Standard. This standard is under constant review by a working committee of security experts to regularly update and improve its security protocols.

SECURING BIOMETRICS

The mobile SDK utilizes visual cryptography and our distributed data model to break up the biometric vectors and store them in multiple locations, minimizing security risks and optimizing user privacy.

REDUCING COSTS

Lost security tokens and passwords are costly for any business. Eliminating these methods with single-step multi-factor biometric authentication from a single vendor saves money and increases security.

PLUG & PLAY

The software can integrate with any existing enterprise applications, including Active Directory, LDAP, Citrix, other VPNs using RADIUS, and single sign-on to third-party services using SAML.

REQUEST A DEMO
www.VeridiumID.com/Demo

VERIDIUM
HANDS ON SECURITY

www.VeridiumID.com
info@VeridiumID.com

United States

100 Hancock Street
10th Floor
Quincy, MA 02171
877.301.0299

United Kingdom

Chalfont Park, Building 1
Gerrards Cross SL9 0BG
United Kingdom
+44 1753 208780