DATASHEET

An end-to-end, biometrics-based authentication solution

VERIDIUMID

Safeguard your data by proving Identity with a flexible, secure, and enterprise-ready solution.

VeridiumID is based on the IEEE 2410 Biometrics Open Protocol Standard – the first global standard for the biometric authentication of digital transactions, physical access, Active Directory, and any other instances where true authentication is needed.

The main problem with passwords is that they do not actually authenticate the person using them. The same is true for traditional multifactor authentication solutions like security codes, PINs, and one-time passwords – 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.

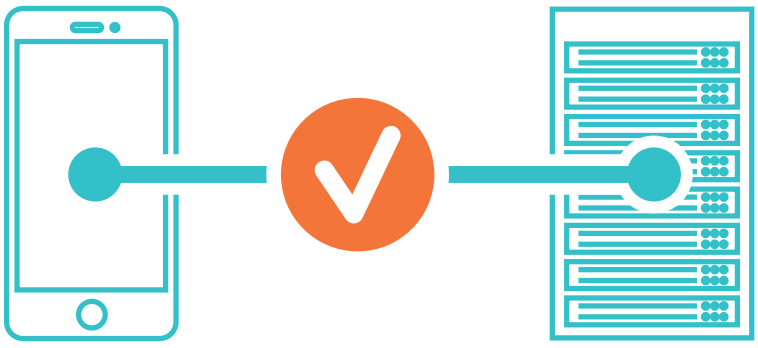
It may be time to eliminate these antiquated systems altogether. The key is to deploy biometrics as part of a genuine, end-to-end authentication solution, either as a second factor or, even better, as the primary authentication factor, replacing passwords with biometrics.

With an end-to-end biometric authentication solution, you are the password. Biometrics replace something you know with something you are.

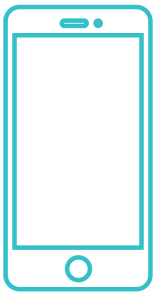
INTRODUCING

VeridiumID works in conjunction with an enterprise's mobile app to provide a protocol for biometric authentication, with matching taking place on the client or back-end server. It is highly customizable and can be hosted in the cloud or on-premise. This puts your company in complete control of user authentication. Built on an open standard, it is one of the most flexible biometric authentication solutions on the market today.

END-TO-END BIOMETRIC AUTHENTICATION SOFTWARE

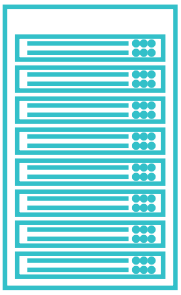


The components



FRONT-END MOBILE SDK

The mobile SDK, available for iOS and Android, is an easily pluggable and highly extendable mobile 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.



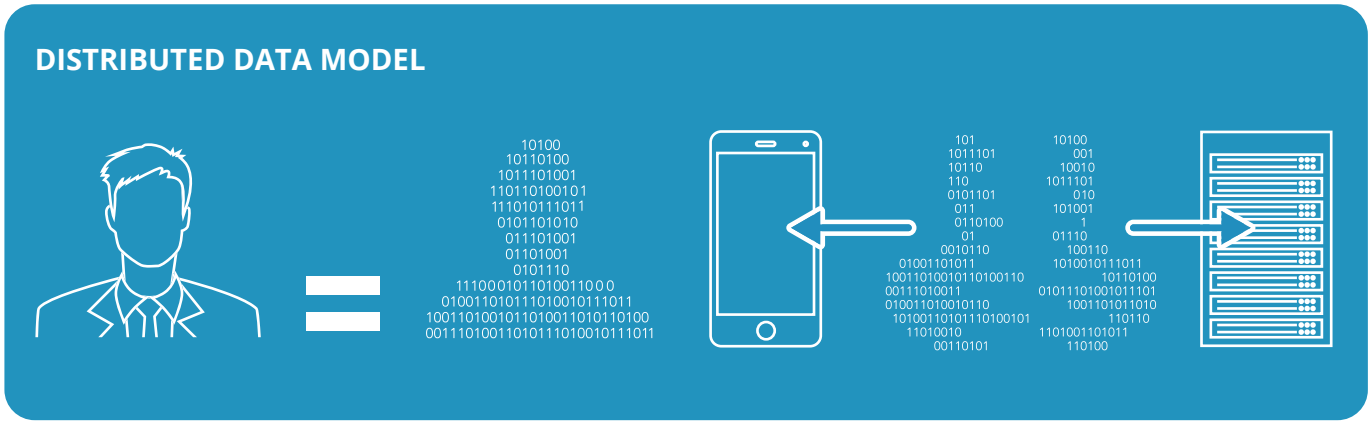
BACK-END SERVER SOFTWARE

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 compatible), or with the biometric data broken up and distributed between the mobile device and the server. This final method provides the most advanced security, as described below.

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 methodology. This allows us to encrypt the vector randomly into two separate pieces and avoid creating a key like other encryption methods. This gives us the option to store one piece on the mobile device, and send the other to the server.

This way user privacy is fully ensured. 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.



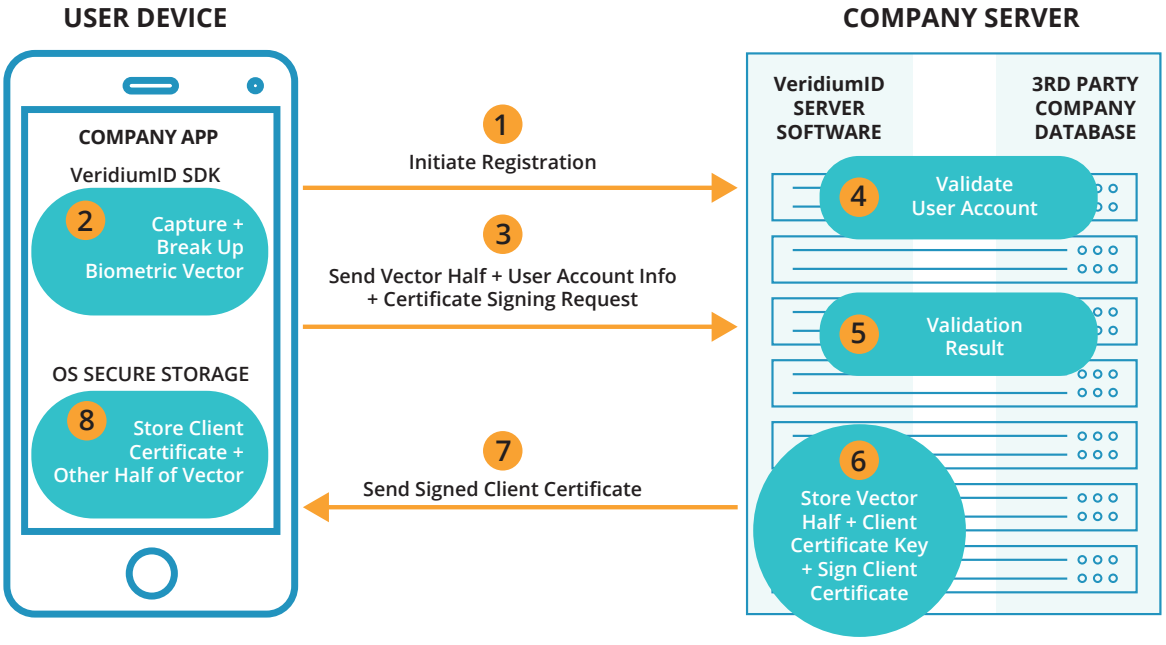
How it works

FRONT-END MOBILE SDK

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 of an email address, an existing account or a mobile phone number.

Once verified, a person scans their biometrics (face, fingers, etc.), which are immediately encrypted. VeridiumID gives your company the option to store encrypted vectors on the mobile device, on the back-end server, or split between the mobile device and the server, using visual cryptography. The back-end then sends a signed client certificate to the phone, which stores it in the device's operating system's secure storage space – protected by the phone's PIN – to be used during authentication.

To start the authentication process, users open the mobile app, which authenticates the session with the back-end using the signed client certificate. This certificate establishes that the users are already verified and own the device. Users then scan their biometric again, producing a new authentication vector. This new vector is matched against the original vector. If the biometric match is successful, the users are verified and able to perform whatever task the authentication is required for.



Benefits

Proving Identity	At the core of VeridiumID is identity. User identity is assured during a customizable registration process. The pairing of a user's biometric with their device becomes their password. With biometric authentication you know users are exactly who they say they are.
Multifactor Authentication	The solution provides multifactor authentication to businesses, 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. This also allows you to include multiple biometrics (face, voice, 4 Fingers, or Touch ID), giving you complete control over what biometric 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 Vectors	The mobile SDK utilizes visual cryptography to break up the biometric vectors for optional storage in multiple locations, minimizing security risks and optimizing user privacy.
Reducing Costs	Lost security tokens and password resets are costly for any business. Replacing these methods with an end-to-end solution from a single vendor saves money and increases security.
Plug & Play	The software can be easily integrated into any existing enterprise environments, including support for Active Directory, LDAP, and Radius.