IMAGEWARE® SYSTEMS

GoVerifyID®

Accelerate your Authentication Journey with our 2FA, Biometric, and MFA Solutions

Enhance CA Single Sign-On with mobile 2FA and biometrics.

CA Single Sign-On is an authentication solution that permits a user to enter one username and password in order to access multiple applications.

ImageWare's GoVerifyID, integrated with CA Single Sign-On, allows users to simply respond to a secure push notification, enter a PIN, use a fingerprint, take a selfie, show their palm, or speak a phrase on their mobile devices to authenticate for SSO managed applications.

Biometric-enabled Single Sign-On is viewed as the next generation authentication solution due to its high level of identification accuracy, security, and usability.

GoVerifyID is a complete, end-to-end, enterprise-ready security solution that can be seamlessly integrated into your existing CA SSO authentication process. It includes a mobile app your customers or employees can download and install on their tablets and smartphones.

GoVerifyID, integrated with CA Single Sign-On, is the best choice for advanced, two-factor and biometric-enabled, mobile authentication.

Benefits

- Data protection
- High identity assurance
- Streamlined login
- Software as a Service
- Quick and easy set-up

Features

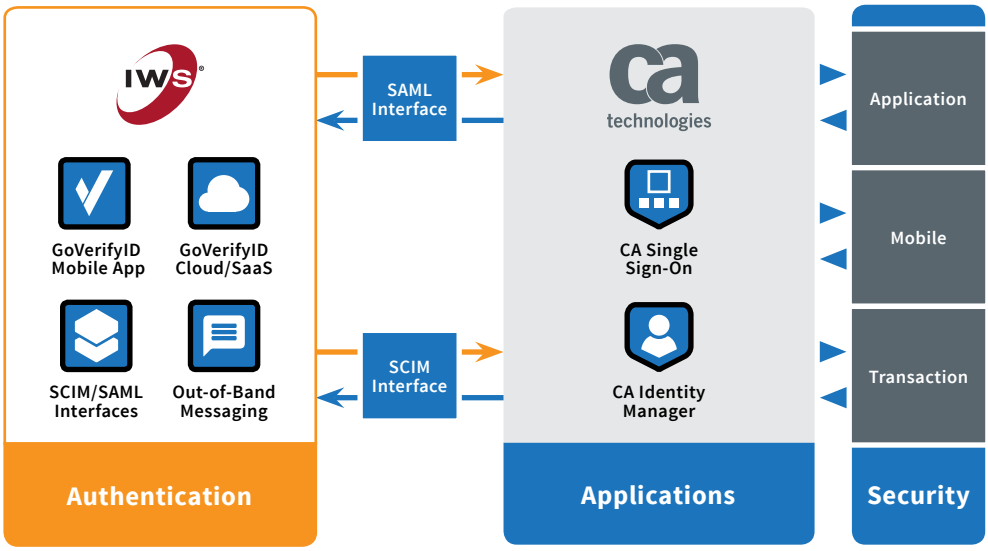
- Seamless integration
- Anonymous storage
- 2FA and biometrics
- Cloud matching
- Mobile access

ca technologies ADVANCED TechPartner

VALIDATED BY ca technologies

CA Single Sign-On and GoVerifyID. Better Together.

Together, CA SSO and GoVerifyID provide multi-modal two-factor and biometric user authentication and single sign-on for all your applications. Flexible, mobile authentication, combined with secure web application access, provides the ultimate in security and user experience. Seamless integration and cloud deployment allows your users to instantly access all their apps by simply responding to a secure push notification, taking a selfie, using a fingerprint, showing their palm, or speaking a phrase.



Biometric user authentication with CA Single Sign-On

User Provisioning:

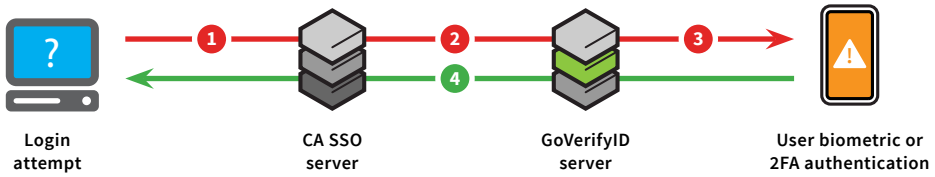
- The CA Identity Manager is configured to point to the ImageWare SCIM interface.
- Users are automatically loaded from CA Identity Manger to the ImageWare system.

System Configuration:

- The CA SSO system is configured to point to the ImageWare SAML interface.
- CA SSO user authentication requests are redirected to the ImageWare system.

Mobile 2FA and biometric user authentication: How it works

1. The user attempts to log into an application managed by CA SSO.
2. The CA SSO server pings the GoVerifyID server for an authentication request.
3. The user is asked to submit their biometrics or 2FA factor for authentication.
4. Based on the results from the servers, the user login request is approved or denied.



For more information, contact us at (858) 673-8600 or sales@iwsinc.com

IWS IMAGEWARE SYSTEMS, INC.
Authentication Assured™

V180901