



Is your authentication causing headaches?



Strong biometric authentication for web and mobile service providers

Authentication has traditionally been described as a trade-off between security and convenience. But in reality, conventional methods don't really offer a high level of either. Passwords are especially painful; since most users have dozens of different user names and passwords to remember, they cope with unsafe password practices that put them at risk. Tokens can be easier but are rarely used for primary authentication and may require additional hardware. And neither one is able to verify the physical presence of the user.

As a result, organizations and individuals have become the victims of increasingly frequent and sophisticated cyber attacks and are facing growing problems of identity theft and data theft, which cost our global society over USD 388 billion last year. Providers of web and mobile services need to give their users a better way to be recognized.

Recognize your users with cloud-based biometrics!

Only biometrics can prove the user's presence, since it is based on unique user traits that cannot be lost, stolen, guessed or shared. BioID Connect allows your web, cloud or mobile services to quickly and easily add strong and convenient biometric authentication that recognizes users naturally, by the way they look (face). Users can log in easily: they simply look at the camera.

With BioID's unique authentication as a service model, you can quickly integrate strong authentication that verifies the user's physical presence with standard webcams or smart phone cameras. No special client hardware or software is required, and the integration with your application can be running in a few days.

Applications

- Login without passwords
- Combine with passwords or tokens for strong multi-factor authentication
- Secure app launch and session control for single sign-on
- Transaction authorization: payments, configuration changes, approvals
- Content personalization
- Account sharing prevention

Benefits

For your users

- Better user experience: just look at the camera
- No password hassles
- Reduced risk of identity theft

For you

- Reduced fraud risk: verifies user's physical presence
- Increased security: biometric traits can't be lost, shared or stolen
- Quick and easy integration



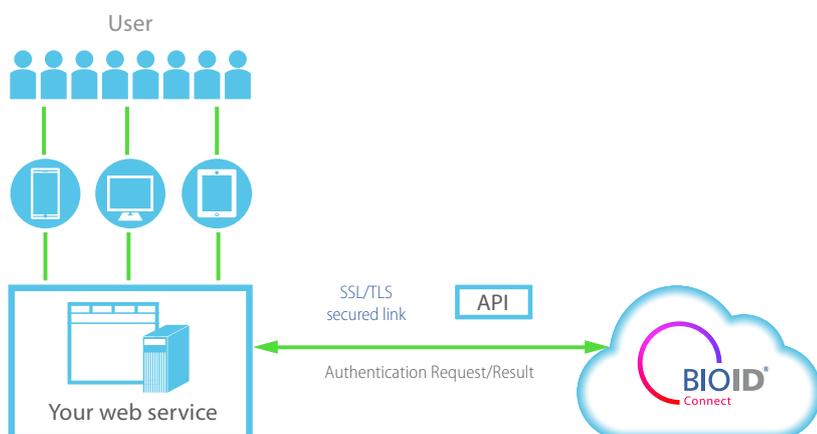
How it works

Integration of BioID Connect is done with a simple API. A typical integration is possible within days.

Once you've integrated BioID Connect with your service, your users will be guided to provide snapshots of their face that teach BioID Connect how to recognize them.

After that, whenever the user logs in or any time you want the user's presence verified, you send them to BioID Connect with their unique, anonymous identifier. We take another sample, make sure it's from a live person and not a photo, compare it to the initial snapshots, and return the user to you along with the verification result.

Your organization and your end users can count on BioID Connect: whenever you need it, it just works. It recognizes your users, and it recognizes when someone else is pretending to be one of them.



BioID Connect enables biometric authentication as a service for any web, cloud or mobile service.

→ learn more: www.bioid.com/products/bioidconnect

Biometric recognition

- Highly accurate face recognition
- Easy to use, just look at the camera

Liveness detection

- Ensures physical presence of the user
- Prevents fraud using photos of the user

Simple integration

- Authentication as a service: very little to install or maintain
- Integration via simple API

Built for security

- Data transfer protected with strong TLS/SSL encryption
- Access control with API key

Privacy inclusive

- No need to share users' personally identifiable information
- Biometric data is kept anonymous



Contact

Phone (Germany) +49 911 9999 898 300
Phone (USA) +1 775 525 5859

Web www.bioid.com
E-mail sales@bioid.com

© BioID AG 2012

BioID Connect Product Brief 2012-10