



OMNI IDENTITY

BioPassword Internet Edition

BioPassword Internet Edition

Omni Identity, Inc.

BioPassword Internet Edition is a multifactor authentication software solution that monitors and enforces Web-based application authentication to prevent fraudulent logins and transactions.

BioPassword Enterprise Edition software can be deployed across the Internet without significant integration and hardware costs. BioPassword is an ideal multifactor authentication solution for online banking, eCommerce, digital rights management or any Internet portal. BioPassword solutions make the risk of easily guessed passwords irrelevant and stolen credentials worthless!

An online security solution that monitors and enforces multifactor authentication, beyond the standard userID and password, is no longer a “nice to have” and is being mandated by responsible corporate management and federal legislation.

Social engineering attacks, such as phishing, cost U.S. banks and credit card issuers about \$929M in 2005 (Gartner Research).

BioPassword secures Web-applications from social engineering attacks, such as phishing and pharming, keystroke logging, brute force attacks, and simple password vulnerabilities.

It is the only multifactor authentication software that combines user's login credentials (userID and password) with the behavioral biometric science of keystroke dynamics (their unique typing rhythm) to provide a low-cost, accurate security solution that is specific to the user.

BioPassword requires no change in user behavior, monitors and authenticates users and is immediately deployable across the Internet without the need to deploy or manage expensive hardware tokens, cards, or other security devices.

In January 2005, the Anti-Phishing Working Group (APWG) reported 2560 unique Phishing attacks. That is 47.4 attacks per day on average. And the attack volume has grown over 28% per month from June 2004 to January 2005.

Fraud Monitoring

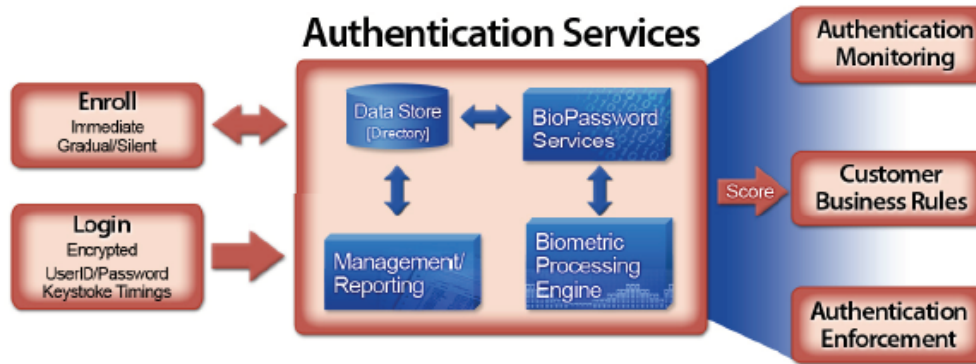
Use BioPassword to monitor the authentication pattern of groups or individuals for fraud or connect BioPassword to internal business rules which allow activation of challenge questions, limited access to applications and data, or simply the recording and reporting of failed login attempts.

Authentication Enforcement

BioPassword combines the userID and a password with a user's biometric template. Organizations can reliably deny access to users who are attempting to use someone else's credentials.

BioPassword Internet Edition at Work

BioPassword is integrated into the current authentication environment. Web authentication services are installed on an authentication server and a Flash-based browser plug-in is loaded when users authenticate to a Web-based application. The plug-in collects user keystroke timings and the Web Service builds a mathematical template that uniquely identifies the user. Subsequent login attempts by the user are compared to their stored template to authenticate login credentials.



- Web Service – Exposes biometric APIs, a standard compliant SOAP interface.
- Flash-based Client Control – Displays login screen to user, collects keystroke timings, and sends data to Web Agent.
- Sample application – A .NET application that publishes a browser Flash plug-in, facilitates enrollment and authentication, and provides a Web-based Management Console.
- Comprehensive implementation documentation.

BioPassword Internet Edition

BioPassword has clear advantages over other authentication solutions including:

Usability

- User-friendly - No change in user behavior
- Non-invasive - No capture of physical information
- Available anywhere there's a keyboard - No special equipment
- Flexible enrollment [immediate, gradual, silent]

Security

- "Rhythm" cannot be shared, lost or forgotten
- ONLY "resettable" biometric – Simply generate a new template
- Authenticates the User - Not the browser settings, geo- coordinates, or pictures!

Integration

- Seamlessly integrates with existing technology environments and processes
- Scalable across the Enterprise *and* the Internet
- Can use "template scoring" with other profiling characteristics to enhance other security solutions

Cost

- Reduced password changes results in far fewer help desk calls and dramatically lower support costs
- Does not require distribution, management or replacement of a special sensor, tokens, cards or keyboards

By using BioPassword, you make the risk of easily guessed or weak passwords irrelevant and stolen credentials completely worthless!

Features

Biometric Authentication Based on Keystrokes

Custom Security Levels

Multiple Enrollment Options

Adaptive Biometric Learning

Software-Only Authentication

Clientless Software

Web Services Architecture

Benefits

Accurately verifies user identities using multifactor authentication based on biometric science.

Customize the biometric authorization threshold to your employee or customer requirements.

A variety of enrollment options provides immediate, gradual, and silent enrollment for building user templates.

Adapts template to user's changing typing rhythm over time.

Easy-to-use authentication software without any special hardware to install or maintain.

Supports all Flash-enabled browsers.

Integrates easily with Web applications across existing infrastructure.

Technical Specifications

Platform Requirements for Web Service

- Windows Server 2003 SP1 or later

Supported Browsers for Flash Control

- Microsoft Internet Explorer 6.0 or later
- Mozilla Firefox 1.5 or later
- OS X Safari

Development Environment for Flash

- Macromedia Flash Professional 8

Omni Identity, Inc.

499 North Canon Drive, 4th Floor
Beverly Hills, CA 90210 USA

310-540-1115 | main

866-639-9840 | fax

www.omniidentity.com

info@omniidentity.com