BioPassword
Security • Software • Science

BioPassword Whitepaper

Authentication Solutions Through Keystroke Dynamics

Objective: *The objective of this paper is to provide a basic understanding of the biometric science of keystroke dynamics, and how BioPassword is using keystroke dynamics technology to deliver enterprise security software solutions for multi-factor authentication to monitor and authenticate users, implement cost-effective secure access, and substantially reduce fraud risk.*

BioPassword: Security, Software and Science

Organizations are challenged daily to keep applications and networks secure while maintaining a balance between usability, security and cost. Information must be accessible at all times through diverse computing and networking architectures for an ever-changing population of customers, suppliers, partners, and employees. With these challenges come substantial security requirements for verifying identities, protecting data, ensuring privacy, proving compliance, and shielding the organization from growing internal and external fraud – all without crippling the business or negatively impacting customers.

Based on experience, security professionals know that relying on only userID and password to authenticate users is simply not practical or effective. The success of costly and highly visible attacks (including phishing, pharming, keystroke logging, spyware, and simple brute-force password cracks) on corporations with sensitive and valuable information continues to gain momentum and garner global attention. Responsible corporate management and government legislation are now mandating security strategies incorporating multi-factor authentication—combining something you know (a password or passphrase) with something you are (a biometric) or something you have (i.e. a smart card).

"Phishing attacks, identity theft, and the loss of control of sensitive personal data are driving demand for stronger protection of personal data and stronger controls on access to that information. As organizations increasingly adopt strong authentication solutions, they need to look for the best ratio of cost to security. A software-based behavioral biometric, such as BioPassword, is well positioned to capitalize on this trend by being low cost to deploy and easy-to-use."

Jon Oltsik, Senior Analyst
Enterprise Strategy Group
March 2006

BioPassword is the leader in delivering enterprise security software solutions for multi-factor authentication using the biometric science of keystroke dynamics. BioPassword protects corporate and individual assets with a simple, yet powerful combination of the user's standard login credentials (userID and password) with the behavioral biometric of keystroke dynamics (the user's unique typing rhythm).

Authentication Solutions Through Keystroke Dynamics

BioPassword authentication software is fast, accurate, transparent, scalable to millions of users, and immediately deployable across the organization and the Internet without the need for expensive tokens, cards, or other specialized hardware. Using BioPassword to monitor and authenticate users, organizations can quickly and economically implement secure access, comply with regulatory requirements, and substantially reduce fraud risk.

Keystroke Dynamics: We Know Your Type

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). In this context, biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics, such as fingerprints, irises, voice patterns, typing patterns, facial patterns, and hand measurements, for the purpose of identification and verification.

A behavioral biometric is a measurable behavior trait that is acquired over time (versus a physiological characteristic or physical trait) and is used to recognize or verify a person's identity. Keystroke dynamics is one of several innovative technologies used to automate the process of authenticating or verifying an individual based upon a unique, personal behavior – their typing patterns. Examples of other behavioral based biometrics include Handwriting and Speech Recognition.

The behavioral biometric of keystroke dynamics uses the manner and rhythm in which an individual types characters on a keyboard or keypad.

Origin of Keystroke Dynamics

On May 24, 1844, the message "What hath God wrought" was sent by telegraph from Baltimore, Maryland, to our nation's Capitol in Washington, D.C., starting a new era in long-distance communications. By the 1860's the telegraph revolution was in full swing and telegraph operators were a valuable resource. With experience, each operator developed their unique "signature" and was able to be identified simply by their tapping rhythm.

As late as World War II, the military transmitted messages using Morse Code. Using a methodology called "The Fist of the Sender," Military Intelligence identified that an individual had a unique way of keying in a message's "dots" and "dashes," creating a rhythm that could help distinguish ally from enemy. In fact, military troop movements were able to be tracked by the "signature" of the code operators. In more recent times, the U.S. National Science Foundation, seeing the value of keystroke dynamics, funded a research project on computer security at the RAND Corporation. Based on this extensive research, the testing concluded that the "The Fist of the Sender" concept had strong statistical merit and could be used as a security technology (see http://www.rand.org/pubs/reports/R2526/).

Figure 1 – Telegraph Key

In the early 1980's, the U.S. National Bureau of Standards funded SRI International (formerly Stanford Research Institute) for developing a biometric solution using these same principles as the "Fist of the Sender." SRI International was able to demonstrate the accuracy of their invention, earning a patent. Within their tests, they concluded by typing userID and password keystroke dynamics provided up to 98% accuracy.

BioPassword
Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

SRI International then conducted a feasibility study for the National Bureau of Standards on the use of keystroke dynamics for computer security. The study demonstrated that a familiar passage such as a logon and password sequence was sufficient for virtually error-free authentication of users.

In 1984, International Bioaccess Systems Corporation acquired all the rights to the keystroke dynamics technology that had been developed by SRI International. In 2002, BioPassword, Inc. acquired all rights to the technology, trade secrets, and patents.

Since 2002, BioPassword has filed numerous additional patents to solidify and extend its technology advantage in keystroke dynamics. Furthermore, BioPassword is driving standards for keystroke dynamics as an authentication technology in the INCITS/M1 standards committee (http://www.biopassword.com/BP_Drives_KD_Standards_Dev.php).

For more historical information on example studies on keystroke dynamics, reference:

- Password hardening based on keystroke dynamics, http://www.ece.cmu.edu/~reiter/papers/2002/IJIS.pdf
- Pattern analysis and machine intelligence, http://ieeexplore.ieee.org/servlet/opac?punumber=34

BioPassword delivered the first product based on keystroke dynamics in the PC and Windows workgroup market in 2002. Currently, BioPassword has matured the technology and delivered the world's leading keystroke dynamics solution for authenticating users over the Internet (BioPassword Internet Edition) and as part of an enterprise network/application security framework (BioPassword Enteprise Edition). BioPassword products are used in banking, eCommerce, healthcare, government, education and technology.

For additional validation of keystroke dynamics as a recognized authentication technology, reference:

- Putting an end to Account-Hijacking Identity Theft, http://www.fdic.gov/consumers/consumer/idtheftstudysupp/idtheftsupp.pdf
- Authentication in an Internet Banking Environment, http://www.ffiec.gov/pdf/authentication_guidance.pdf

The Science of Keystroke Dynamics

Keystroke dynamics measures the series of key down and key up event timings while the user types a string. For example, if a user's password is 'password' then key down and key up events are captured for each character.

These raw measurements can be recorded from almost any keyboard and can be recorded to determine Dwell time (the time between key down and key up) and Flight time (the time from "key down" to the next "key down" to the time between one "key up" and the next "key up") as represented in the figure below.

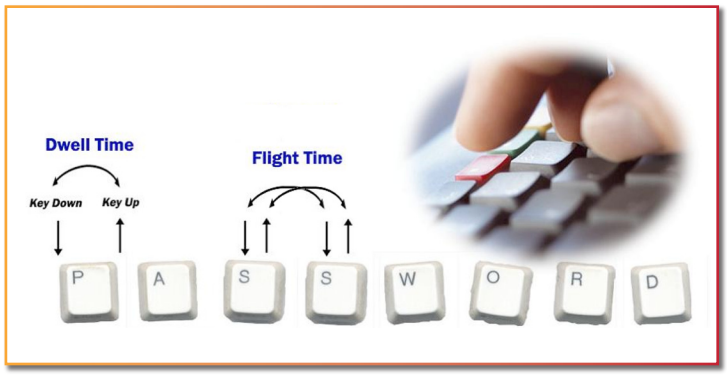

Figure 2 – Keystroke Dwell Time and Flight Time

Once the keystroke timing data is captured, the recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for future comparison.

As with any biometric technology applied to an authentication function, the technology is used for two major functions: enroll and verify user credentials.

BioPassword® Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

Enrollment: Building A Biometric Template

A template that represents the unique biometric signature of the user is derived once nine (9) multiple valid patterns are acquired and processed. For example, the figure below represents the template for a user typing the character string 'biopassword.'

BioPassword can accept a minimum of 8 characters (however, a minimum of 12 is recommended) and can accept from 1-to-6 input fields. Thus, a biometric template could be generated from a single email address, phrase or a combination of userID and password.

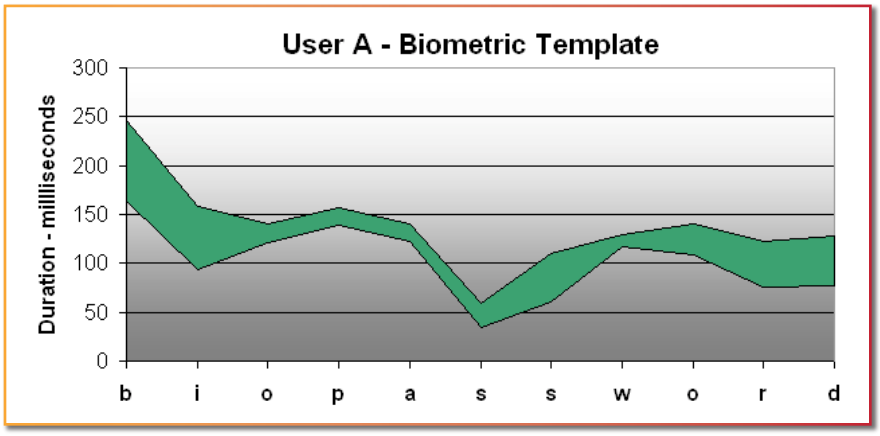

Figure 3 – User A Biometric Template for Word: 'biopassword'

Authentication: Validating Biometric Timings

As part of the authentication process, the user types an authentication attempt and this sample is compared against the biometric template created during the enrollment process. Based on keystroke timings (and their fit to the stored template) a 'biometric score' is returned as the result of the comparison process. The score may then be used for making monitoring and/or access control decisions.

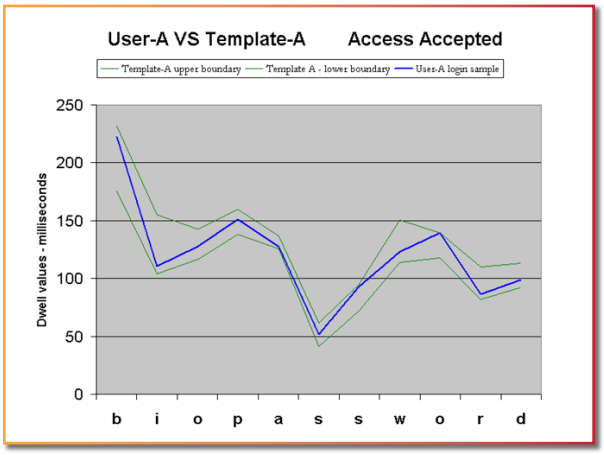

Figure 5 – User A Typing Template

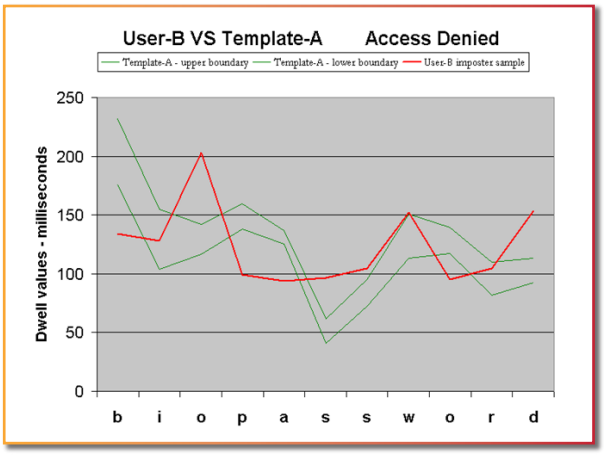

Figure 4 – User B Typing Template Credential(s)

As an example, in Figure 4, User A enters "biopassword" against their stored template. Based on the keystroke timings and the pattern that was generated against the template, User A is verified. In Figure 5, User B attempts to authenticate with User A's password and fails against the template. As you can see, the User B pattern is well outside the template stored for User A.

By adding the ability to score a pattern against a template, BioPassword gives the customer the ability to associate business rules (such as requiring a challenge question or monitoring a specific transaction) with each authentication attempt rather than requiring a simple access/no access decision.

BioPassword
Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

Adaptive Learning for Biometric Templates

As described above, User A has a template that was stored at enrollment. However, this template might need to evolve over time (for example, User A might become more familiar with typing 'biopassword' and require the solution to learn (adapt) to the new pattern). Based on neural network technology, BioPassword incorporates adaptive learning to ensure the users' biometric templates evolve with their changing typing patterns. BioPassword's adaptive learning capability captures and refines the user biometric template each time the user successfully verifies their biometric credential(s). Therefore, the longer a user has the template, the better it will become.

By being readily available (using any keyboard), uniquely identifying users (biometric template) and learning over time (using the neural network properties), BioPassword has developed the industry leading authentication technology using the science of keystroke dynamics.

Security and Usability

There are industry-defined measures for describing the security associated with biometric technologies. The terms are described as:

- FAR – False Accept Error Rate: Rate that system accepts imposters falsely accepted to the system. For example, an FAR of 3% indicates that 3 out of every 100 imposters are falsely accepted as valid users.
- FRR – False Reject Error Rate: Rate that system rejects legitimate users are falsely rejected and denied access to the system. For example, FRR of 3% indicates that 3out of every 100 legitimate users are rejected as invalid users.
- CER – Cross-over Error Rate (Equal Error Rate): Rate at which FAR equals FRR. In the above examples the CER is 3%.

Keystroke dynamics and the BioPassword solution compare favorably with other biometric security solutions and are far superior to other non-biometric implementations such as profiling technologies and complex passwords.

Figure 6 below shows False Accept Rates (FAR) vs. False Reject Rates (FRR) for BioPassword and other biometric authentication technologies. BioPassword has a 3% cross-over error rate which is better than vein biometrics and similar to voice and fingerprint recognition.

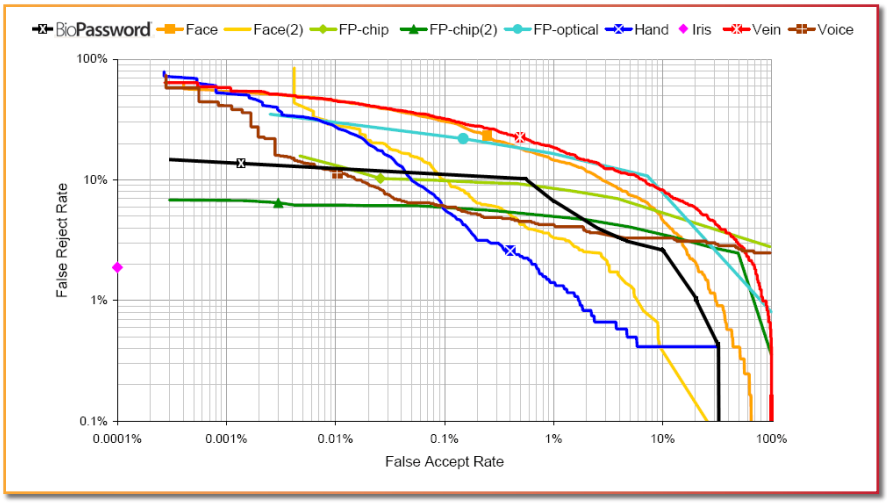

Figure 6 – False Accept Rates vs. Reject Rates for Biometric Security Technologies.

As many companies have found, security, usability and cost are critical components to understand as part of any security technology implementation. There are tradeoffs to be made for each type of technology. Unlike other biometric security technologies, keystroke dynamics is the only security technology that offers the opportunity to tailor security and usability to offer a "best fit" solution for each application environment. BioPassword template scores can be customized for different business applications.

BioPassword
Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

High value transactions should require higher template scores for authentication. Consumer Internet portals could require lower template scores to minimize the number of false rejects.

As examples, BioPassword can be tailored (adjustable FRR or FAR thresholds) to the appropriate application need whether users are:

Consumers on the Internet

- Lower FRR to assure easy website access

Employees on the Corporate Network

- Raise FRR to assure secure access to corporate assets

High-value transactions

- Lower FAR to assure verification of individual user

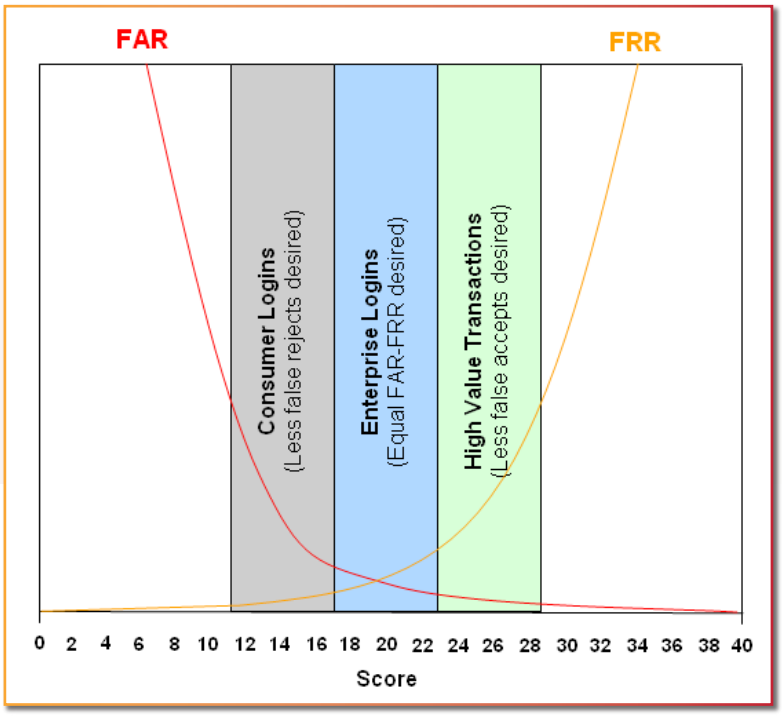

Figure 7 – BioPassword Business Application Confidence Levels

Advantages of Keystroke Dynamics

Using keystroke dynamics in authentication software delivers a solution that is fast, accurate, scalable to millions of users, requires no change in user behavior and is immediately deployable across the organization and the Internet without the need for expensive tokens, cards or other specialized hardware.

For the moment, the only ubiquitous "sensor" is a PC keyboard, which makes typing rhythm – based on measurement of the distinctive timing of and between keystrokes – the only viable biometric technology for "in band" consumer authentication.

State of the Art of Online Consumer Authentication
Gartner Group
May 2006

A users "rhythm" cannot be shared, lost or forgotten. Furthermore, a password with a biometric template can easily be reset. If a fingerprint/handprint template is stolen, it is stolen for life.

By using BioPassword to monitor and authenticate users, organizations can quickly and cost effectively implement secure access, comply with regulatory requirements, and substantially reduce the risks of fraud.

BioPassword
Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

Authentication Solutions Through Keystroke Dynamics

Security professionals are faced with identifying and evaluating a myriad of authentication technologies. By plotting alternative authentication technologies as cost of ownership versus level of security, we have created an 'Authentication Curve' to help position technology options. The diagram is divided into 4 major components:

- Low Cost/Low Security (standard passwords, profiling technologies)
- High Cost/Low Security
- Low Cost/High Security (BioPassword Authentication Monitoring and Enforcement
- High Cost/High Security (Smart Cards /Tokens/Other physical biometrics)

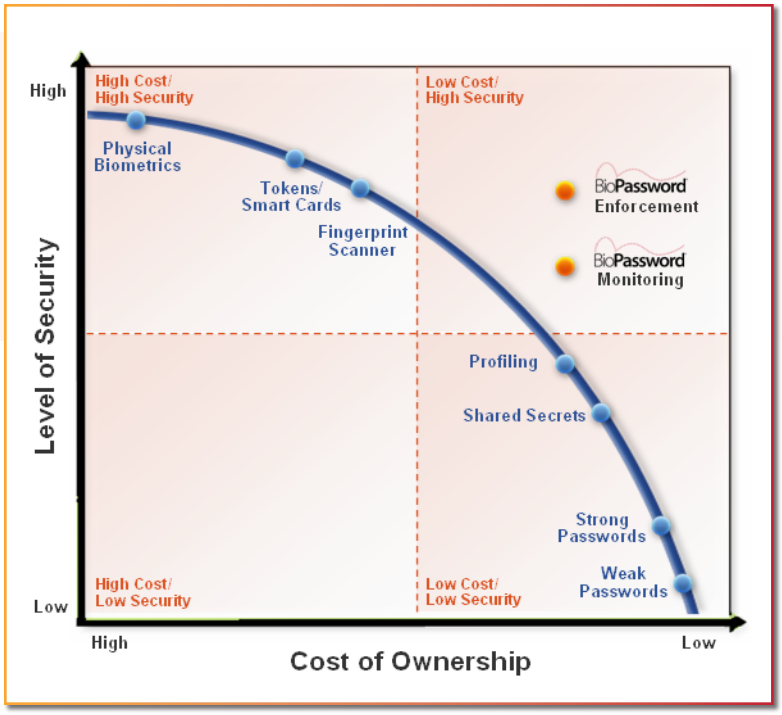

Figure 8 – Authentication Technology Curve

As organizations look to evaluate technology, it is clear that solutions at the top of the curve are practical for only a small fraction of the community that needs the high cost/high security options. The vast majority of the user population remains unaccounted for with these expensive alternatives. BioPassword delivers a software-only solution that is quickly, easily and cost-effectively deployed across the enterprise network or over the Internet.

Because BioPassword has the capability to offer the security of considerably more expensive hardware-based authentication options and the lower cost of less secure profiling technologies in a single product, BioPassword is the best alternative when using a cost versus security model for selecting/evaluating authentication options.

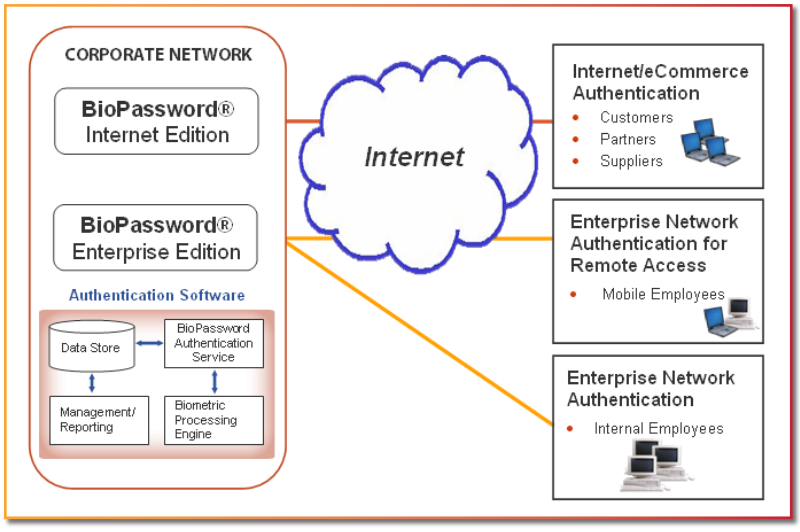

Figure 9 – BioPassword Products: Internet Edition and Enterprise Edition

BioPassword Technology Solutions Overview

BioPassword multi-factor authentication software solutions are ideal for protecting enterprise network applications, online banking sites, eCommerce users, digital content, Internet portals, or individual laptops and PCs. BioPassword technology can be quickly and easily integrated into an existing application or corporate network infrastructure.

BioPassword
Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

A BioPassword deployment installs our biometric authentication services on an existing authentication server, and a small client control (or flash-based browser plug-in for Web-based applications) for collecting keystroke timing data, and then encrypting the information. This data is sent to the Biometric Processing Engine (BPE) which builds a mathematical template uniquely identifying the user. Subsequent login attempts by the user are compared to their stored template in order to authenticate login credentials. BioPassword technology is packaged as BioPassword Internet Edition for use in online applications and BioPassword Enterprise Edition for internal corporate networks and remote access users (including Citrix environments).

BioPassword Internet Edition

BioPassword Internet Edition is a software integration package which is available to organizations for implementing multi-factor authentication monitoring and enforcement solutions for Web-based applications.

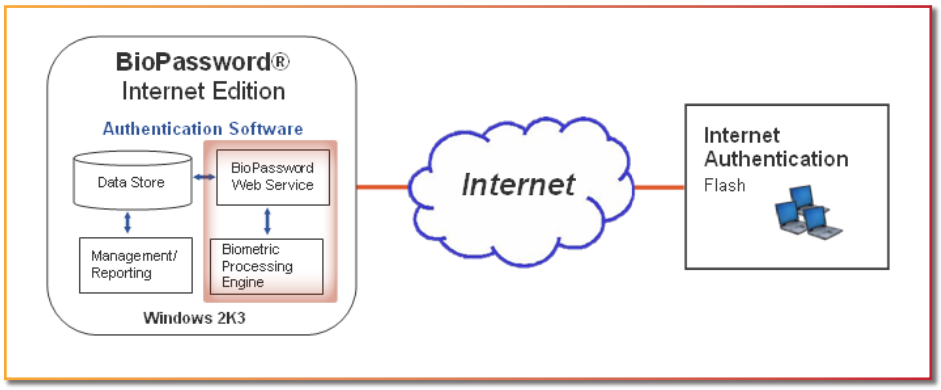

Figure 10 – BioPassword Internet Edition

This product comes with a Biometric Processing Engine (BPE), Web Service (defines biometric APIs, a standard SOAP-compliant interface as Windows .NET Web Service), sample application (.NET application that publishes a Flash plug-in to browsers, facilitates enrollment and authentication, and provides a Web-based reporting and management console (See Figure 10). In addition, BioPassword Internet Edition comes with comprehensive integration and implementation documentation for rapid deployment.

BioPassword Enterprise Edition

BioPassword Enterprise Edition is a complete client/server solution designed for Windows 2000/2003 enterprise networks that may also be running Citrix Presentation Server or Web Interface software that protects user accounts and network resources by strengthening Active Directory password-based authentication. BioPassword Enterprise Edition can be quickly and easily integrated into corporate network environments for local or remote access (See Figure 11).

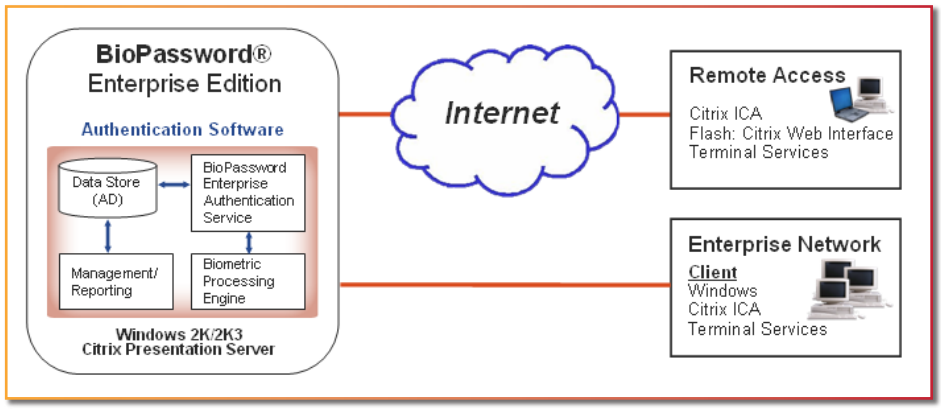

Figure 11 – BioPassword Enterprise Edition

BioPassword Enterprise Edition stores biometric settings and timings with user credentials in Active Directory. BioPassword relies on the BioPassword Enterprise Authentication Service that runs on each Domain Controller in a BioPassword-enabled environment to serve as a distributed biometric authentication and data access point.

BioPassword
Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

Each client communicates with the Authentication Service to submit BioPassword timing samples for authentication (biometric scoring) and also to retrieve configuration information for users and client devices.BioPassword Enterprise Edition is unique as it provides a complete solution to monitor all possible login processes for Windows clients including: Windows login GINA, Windows Change Password dialog, "Connect As" dialogs, Command line (cmd.exe) windows that are executing "net.exe use /user:", Command line (cmd.exe) windows that are executing "runas", Windows RunAs dialogs, and Windows Join Domain dialogs.

In addition to Windows environments, BioPassword Enterprise Edition works seamlessly with Citrix ICA clients and Citrix Presentation Server to protect applications published over the network and over the Internet (using Citrix Web Interface).

Authentication Process

For all BioPassword products, the authentication process has two components. The first, enrollment, is used to register users with the software system. The second part includes authentication monitoring and/or authentication enforcement to protect Internet/ Enterprise applications and networks.

Enrollment Options

As discussed earlier, BioPassword requires an enrollment process. One of the strengths of keystroke dynamics and thus, BioPassword is that the input device for the enrollment process is nearly ubiquitous – the keyboard. In addition, after enrollment the user requires no specific changes in their well understood authentication process.

The user experience associated with enrollment must be flexible, fast, and painless. Another advantage of BioPassword is the flexible set of enrollment options. The user experience associated with enrollment must be flexible, fast and painless. Users can be enrolled immediately, gradually, or silently (See Figure 12 – Enrollment Process).

- **Immediate Enrollment** offers the ability to enroll a user at any time, enabling immediate authentication monitoring and enforcement. Most users enroll within one to three minutes.
- **Gradual Enrollment** offers the ability to enroll users over time—a template is created after several logins. This is very valuable when used as part of a phased deployment strategy.
- **Silent Enrollment** offers the ability to enroll users over time without any user notification. This feature is valuable to administrators who want to implement two-factor authentication without notifying users to establish and understand authentication patterns of their user base before setting security thresholds.

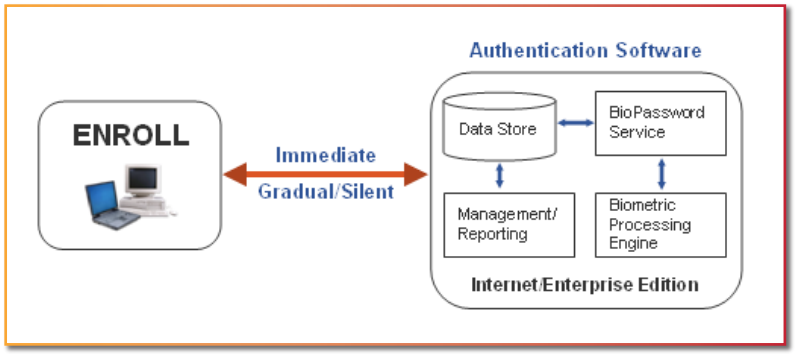

Figure 12 – Enrollment Process

BioPassword Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

To develop a valid biometric template a user must proviate a minimum of nine (9) samples. Although many customers simply use a combination of logon userID and password, BioPassword can accept a minimum of 8 characters (however, a minimum of 12 is recommended) and can accept from 1-to-6 input fields. Thus, a biometric template could be generated from a single email address, phrase or a combination of userID, password, and domain.

Authentication Monitoring and Enforcement

BioPassword technology can be used to monitor the authentication pattern of groups or individuals. As part of the Login process (See Figure 13 – Authentication Monitoring and Enforcement), BioPassword combines a userID and password with a user's biometric score to work with an organization's business rules to monitor or enforce secure access. Additionally, it can be connected with profiling software to activate business rules that trigger challenge questions, restrict access to applications and data, or simply record and report failed logon attempts.

BioPassword may also be used to enforce a second factor of authentication. Organizations using BioPassword can reliably deny access to users who are fraudulently attempting to use another person's credentials.

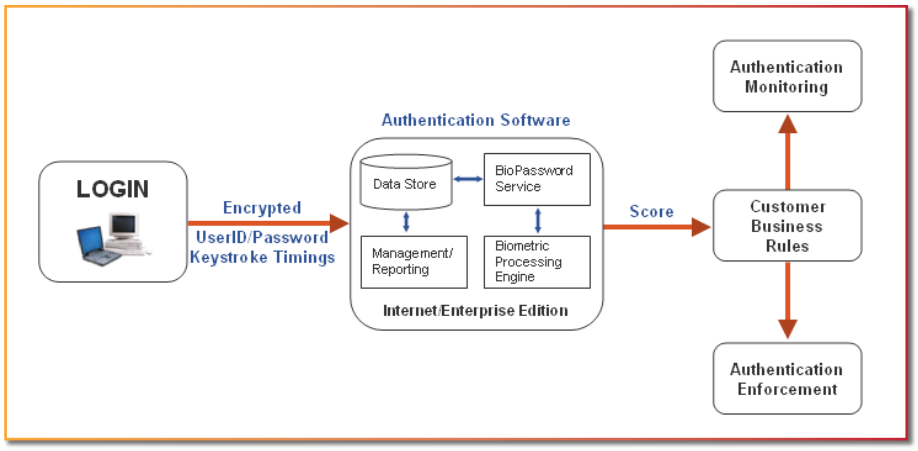

Figure 13 – Authentication Monitoring and Enforcement

BioPassword
Security • Software • Science

Authentication Solutions Through Keystroke Dynamics

BioPassword Advantages

BioPassword has clear advantages over other authentication solutions including:

Usability

- Available anywhere there's a keyboard – No special equipment required.
- User-friendly – No change in user behavior
- Non-invasive – No fingerprints, blood vessels or eyeballs
- Flexible enrollment (immediate, gradual, or silent)

Security

- A person's typing "rhythm" cannot be lost or forgotten.
- The only "resettable" biometric – Simply generate a new template.
- Authenticates the user – Not the browser settings, cookies, geo-coordinates, or pictures
- Most extensive software protection for Windows environments including ConnectAs, RunAs, command line and Join Domain dialogs

Integration

- Seamlessly integrates with existing technology environments and processes – Complete Windows integration
- Scalable across enterprises and the Internet
- Can use template scoring with other profiling characteristics to enhance other security solutions

Cost

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

BioPassword: Security · Software · Science

BioPassword is the leader in delivering enterprise security software solutions for multi-factor authentication using the biometric science of keystroke dynamics. BioPassword authentication software is fast, accurate, transparent, scalable to millions of users, and immediately deployable across the organization and the Internet without the need for expensive tokens, cards, or other specialized hardware. By using BioPassword, you make the risk of easily guessed or weak passwords irrelevant and stolen credentials completely worthless.

BioPassword, Inc.
1605 NW Sammamish Road, Suite 105
Issaquah, WA 98027
www.biopassword.com
Tel: 425.649.1100
Fax: 425.649.1110
sales@biopassword.com

BioPassword
Security • Software • Science