Student ID and Verification System Using New "Software Biometrics" White Paper

Prepared by:

Biometric Signature ID
708 Valley Ridge Circle
Suite 8
Lewisville, TX 75057

Document No.: **0000019**
Revision: **5**
Date: **August 2, 2010**

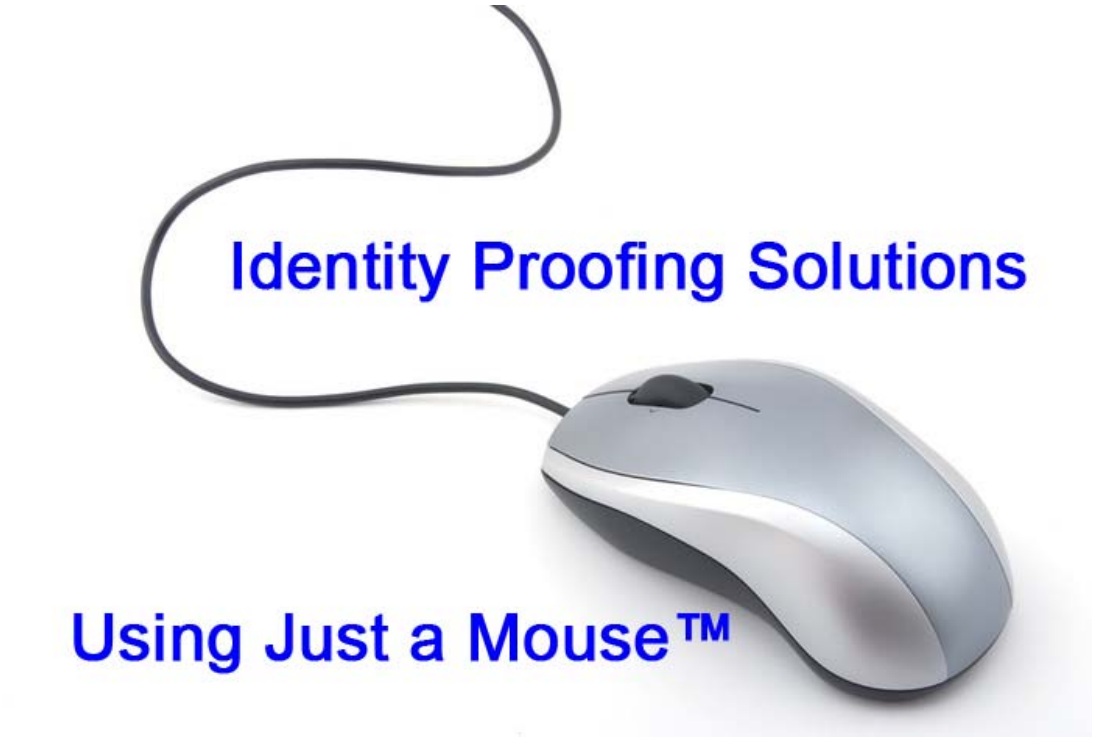

Table of Contents

1 Biometric Signature ID Corporation (BSI)

BSI is an award winning software development company based in Dallas Texas. We specialize in identity and access management solutions the core of which is our patented biometric signature/gesture technology.

We offer the following software solutions:

1. **BioSig-ID Online™** - A patented dynamic biometric signature/gesture authentication solution,
2. **Click-ID Online™** - Human pattern recognition technology for strong identity verification
3. **uSignOnline™** - Electronic signatures that comply with e-sign laws to accept contracts or approve actions online

Summary:
Biometric Signature ID offers a unique signature/gesture biometric and other identity proofing technology that provides the following advantages to current static or other dynamic solutions:

- NO Hardware required – eliminates cost and scalability issues
- Authenticates the physical user
- 93% of students find it “Extremely or Very Convenient” to use
- Little administration required
- Instantly scalable, any PC anytime, anywhere
- 100% enrollment (fingerprint biometrics have a failure to enroll up to 3%)
- Enroll in minutes, validate in seconds
- Age and language independent
- Audit trails tracks event and session records
- Unique closed loop that creates automatic password reset and allows continuity
- Accepted by biometric experts, proven, accurate and reliable
- Allows student ID verification along all points of course delivery and exams

We encourage you to visit our web site at www.biosig-id.com. We have a list of some of our current customers on the site and all three of our technologies are available to view from videos including a student ID verification video. We would also offer to conduct a web demo of our technology at your convenience. If you require any additional information please contact me directly at the numbers below.

Regards,

Jeff Maynard

President and CEO Biometric Signature ID
Direct: 972-436-6862
Mobile: 214-244-7679
Toll Free: 800-871-2817

2 Case Study Results – University Of Maryland University College

Biometric Signature ID specializes in online identity proofing solutions. Our patented dynamic software technology measures the unique biometric characteristics of each student using only a "mouse". Upon initial enrollment, speed, direction, height, length, width, angle of each student's "signature" is stored in a secure database. Only the "real" student can authenticate themselves. This software has opened the door for distance learning to positively establish that the student who registers in a course is the same student who participates and completes the course and receives the academic credit. The software provides the assurance that a student's identity is authenticated.

A 30 day pilot with University of Maryland University College to verify student ID under the direction of Dr. Matt Prineas, Office of the Provost and Dr. Susan Aldridge President was completed. Students from multiple classes were able to authenticate their identity from their own computers using our BioSig-ID, Click-ID and Security Questions software. Students and faculty were asked to authenticate their identity at various times during their course and at the final exam. Focus groups were conducted with faculty and staff to ensure program buy in. The entire program was voluntary, conducted using e-mail and did not require faculty "hands on involvement".

Over 900 signature enrollment and verifications were completed during the trial. The final exam was held at a proctored site and students brought in their "Completion certificate" as proof of completing registration, enrollment and multiple identity authentications throughout the course. Students then validated their identity before taking the exam.

Students were able to enroll in minutes and authenticate their identity in seconds using just their "mouse" or other pointing device. Full audit trails were analyzed of all activity. No personal identifying information was collected ensuring student privacy was not breeched. Survey results were obtained from 83% of students.

Survey Results: Highlights include:

- 93% rated the verification system as "Extremely or Very Convenient"
- 97% would recommend BioSig-ID be used for student identity verification

"BioSig-ID and Click-ID software authentication technology surpassed our expectations in a recent pilot with students and faculty. Biometric Signature ID has created a valuable tool for remote identity proofing to verify student identity that requires little administration and no additional hardware."
Matt Prineas PhD, Office of the Provost-University of Maryland University College

3 Case Study Results – University Of Texas TeleCampus

Abstract; Over a 5 week period (3/23 – 4/30, 2010) approximately 1,400 students from 46 classes from 9 campuses were asked to volunteer to authenticate their identity from their own computers using BioSig-ID and Click-ID software. Test subjects were asked to enroll, create a profile and authenticate their identity 10 times during their course. 172 students registered in the software and 94 completed the required 10 authentications. Full audit trails were analyzed of all activity and an online survey was administered for all students who completed the pilot. A second survey was sent out to the students who did not complete the pilot to compare their responses.

The proof of concept was deemed very successful with 100% of participants able to enroll and validate. A substantial majority of the participants (80%) responded to the survey with 98% of participants rating the verification system as "Somewhat Easy, Very Easy or Extremely Easy" and 99% stated their experience with the pilot was Good, Very Good or Excellent. Combined average time of enrollment in both BioSig-ID and Click-ID was 1:24 minutes, while average authentication only took 21.5 seconds. Combined average time of enrollment in both Click -ID and CSQ was 2:14 minutes, while average authentication took 33.2 seconds.

"The BioSig-ID closed loop software authentication technology was found to be extremely effective in user experience identity testing across 9 campuses using just a mouse. Using a software biometric that requires no hardware and little administration, BSI has become the leader in remote authentication to verify student identity."
Lori McNabb MS, Assistant Director, Student and Faculty Services-University of Texas System TeleCampus

4 Frequently asked Questions and Answers

Revised 2008 Education Act (PART H-PROGRAM INTEGRITY- SEC. 496 Section 602.17. RECOGNITION OF ACCREDITING AGENCY OR ASSOCIATION). Final Ruling published in the Federal Register October 27, 2009.

> (g) Requires institutions that offer distance education or correspondence education to have processes in place through which the institution establishes that the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the course or program and receives the academic credit. The agency meets this requirement if it—(1) Requires institutions to verify the identity of a student who participates in class or coursework by using, at the option of the institution, methods such as:

(i) A secure login and pass code; (ii) Proctored examinations; and (iii) New or other technologies and practices that are effective in verifying student identity; and

(2) Makes clear in writing that institutions must use processes that protect student privacy and notify students of any projected additional student charges associated with the verification of student identity at the time of registration or enrollment.

HOWEVER and in addition in the Final Ruling published in the Federal Register October 27, 2009 the US dept of Education clarified their intent to move beyond Pins and passwords as follows:

"it is clear that Congress anticipated that as new identification technologies are developed and become more mainstream and less expensive, agencies and institutions would consider using them. For this reason, the regulations provide for the use of new technologies and practices that are effective in verifying the identity of students, in addition to methods such as secure logins, pass codes, and proctored examinations".

4.1 How do the BSI solutions compare to random questions developed from databases that offer out of wallet or credit type questions.

a. These databases do not authenticate the physical identity of the student, nor can they confirm that the student is the same person who registered for the course or who takes tests or "participates" throughout the session. They are used for real time assessment of the validity of an asserted identity. If someone knows the answers to the questions they can masquerade as another. This strategy does not authenticate the physical user. The databases are limited for students who have little or no credit history and lack of updates can severely affect their utility.
b. BSI technology on the other hand is the only software dynamic biometric that can establish the identity of the person online using multiple security layers after they have enrolled a profile into the clients' secure database. The BSI solution supports customer registration and subsequent authentication events in seconds.
c. BioSig-ID and Click-ID actually authenticate or verify the students' identity and confirm that the student who enrolled is the same student throughout the course. BSI solutions are not limited by lack of credit history or updates.

4.2 Some systems try to control the environment using web cams, how does BSI manage for this?

a. Web cams have some inherent issues – they are hardware, costly, they may have compatibility issues with certain operating systems, require training and or maintenance and require mailing costs. Faculty members in some cases must monitor the web cam or "rule" on issues of potential fraud, costing time and resources. Then there are huge privacy issues. What happens in shared dorm rooms, do we want to be taking recordings of the children running around while Dad is taking the exam in his dining room? All of these factors limit their practical use.

b. If a student wishes to “cheat” they can represent themselves as another individual, they can position the web cam in a manner that allows others to press the keys, they can set up another PC linked to the one that is viewed and other methods can thwart the intended use of controlling the environment.
c. BSI’s position is that the environment cannot be controlled without great expense and that the costs may outweigh any possible gain. BSI offers a no hardware solution that significantly reduces costs and the associated “Pain and inconvenience” that limits uptake with any hardware system is avoided. The Education Act says the student identity must be verified and BSI’s solutions do that- we validate that the student who started the course/test is the same person who authenticates their identity throughout. By having the student verify identity in a random fashion multiple times it becomes nearly impossible to circumvent the system.
d. If the institution requires a web cam solution for higher risk tests for example, BSI has integrated a “netbook” web cam with our technology that can provide this level of environment control.

4.3 How does BSI’s solution compare with other biometric systems?

a. Static biometric like fingerprints, facial scans etc. require the use of costly hardware. This hardware requires mailing, training and maintenance adding costs and reducing scalability. Fingerprint readers have been known to range in effectiveness from only 30% to 99.9%, which is why they have not been adopted in airports – you need to pull people out of line to process manually. In addition there is a failure to enroll with fingerprint readers up to 3%. This means up to 3% of people will not be able to enroll in the system and a back up plan is required.
b. Dynamic biometrics like voice and keystroke while offering certain advantages over static biometrics do not measure up to signature gestures because voice is not advanced enough in technology so it has limited application to authenticate identity. Keystroke captures only one biometric index-time between strokes which limits its authentication reliability and requires users to enroll up to 20 times.
c. Most other companies offer a biometric solution. In contrast BSI offers a solution that contains biometrics. Our closed loop technology provides for multiple security layers, which is more flexible and scalable with other systems.
d. BSI requires no additional hardware and reduces costs while increasing scalability. BSI uses a “training enrollment” that offers a 100% enrollment. Since the user is in control of what they draw/write or select they have little of no issue in producing 100% effectiveness. BSI’s BioSig-ID requires the user to enroll only 3 times and collects up to 6 biometric indexes for maximum reliability and effectiveness.
e. BSI technology works as an integrated system and provides for Identification, Authentication and Authorization, a first for a biometric.

4.4 Can you explain the issues surrounding situations where the student fails to validate their identity during a test or course?

a. One of the policies NY State DMV uses is the 3rd time and out policy. If a student is unable to verify their identity after the third time the test stops and they must call the administrator. This is an option for administrators.
b. We already know that fingerprint readers with up to 3% failure to enroll rates will cause failure to verify identity. The use of security questions are also going to create failures for the reasons stated. It should be remembered that the student is in “combat” conditions and is highly stressed, pressed for time in an environment that will add to a higher degree of failure to verify identity.
c. The overall objective is to allow the student to complete the test or course, to verify they are the same student throughout, avoid help desk calls and reduce resource management costs seamlessly.
d. BSI is the only solution provider who has developed an ideal solution for this combat environment using our “Unique closed loop” technology. This technology allows the student to validate their identity after a failure to validate and re-enroll a new signature profile. This avoids a help desk call or a stoppage of the exam/course. This technology is automatic and requires no manual intervention. This achieves the objective of allowing the student to complete the test or course and to verify they are the same student throughout.
e. The BioSig-ID Online and Click-ID Online architecture consists of three (3) layers of security. During enrollment, a user enrolls in a minimum of 2 security methods consisting of a primary and alternative access method. If a user is unable to enroll in the primary access method for any reason, the alternative access method defaults to become the primary and the third alternative access method becomes secondary. This provides maximum security and flexibility for users. The alternative access is also a profile re-set technology, helping avoid help desk calls in the event they "forget" their primary access method or otherwise fail to verify their ID. This technology is unique to our solutions and is patent pending. Example architecture is as follows:

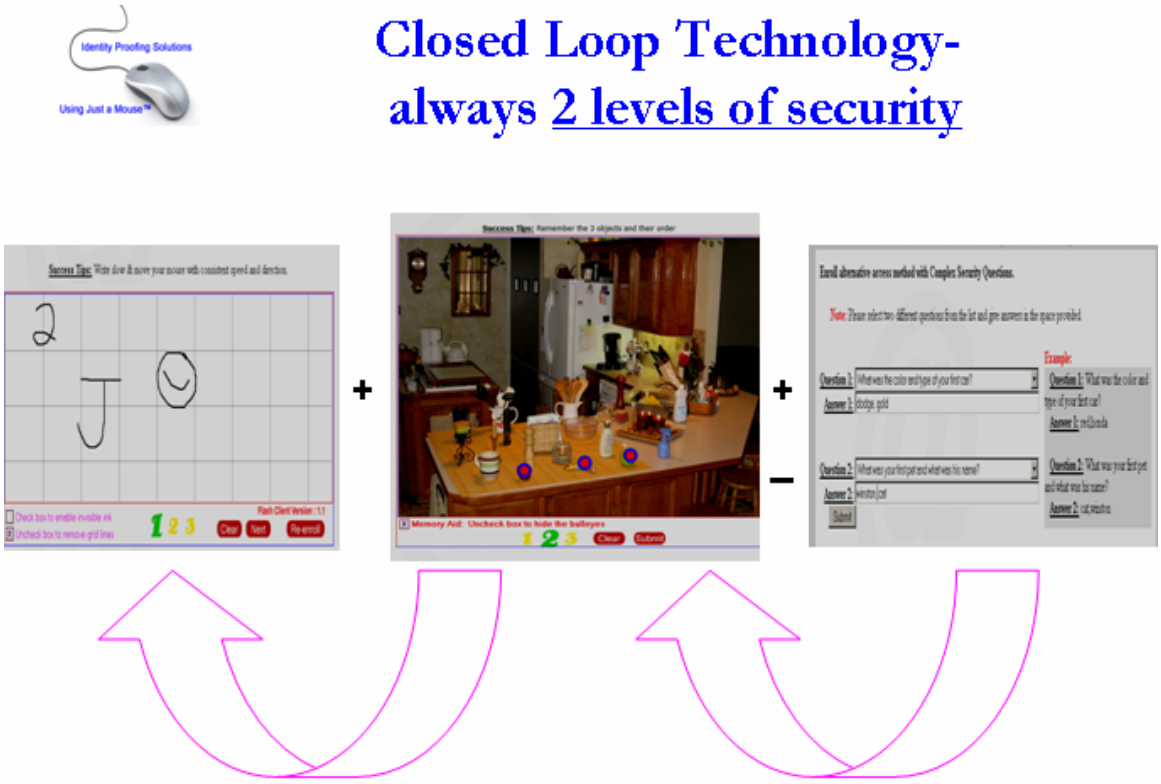

Figure 1 Modular Relationship between BioSig-ID, Click-ID, and Complex Security Questions

4.5 Please comment on BSI's technology pertaining to privacy, and security versus PINS and passwords.

a. BSI biometric solutions are unique to each individual and cannot be lost, stolen, or borrowed compared to Pins, passwords, tokens, cards and other security solutions. If I know your PIN for example it is a 100% security failure and is unacceptable as the single point of identity validation in today's environment. This failure is why the federal government mandates multi-factor authentication for online banking and more.

b. One key element of collecting biometric data is privacy. If your fingerprint is hacked from a database it is gone forever. With dynamic biometrics we have advantages called Revoke and Replace. This means that the dynamic signatures you make can be instantly revoked and you can always create a new one in any event where the database might be compromised. This is only true for dynamic biometrics.

4.6 Do you have different levels of security solutions?

c. YES, institutions can choose to use our BioSig-ID, Click-ID and Complex Security Questions solution (BCC solution). This is the most popular approach for schools and accreditation bodies.

d. The next level up provides for knowledge based questions to be asked to the students one time and this is during initial enrollment. This additional aspect adds an extra security dimension to the BCC solution and helps to add to the confidence levels that the student who is about to enroll is the right student.
e. The last option for schools is to add a web cam combined with our technology. BSI offers an "integrated web cam and netbook" solution. This approach provides a locked down browser environment best suited to replace proctored high risk exams. Unlike other solutions in the marketplace that have a "single product" the addition of an in-expensive netbook provides the student with a significant value added tool. Students can lease to buy this netbook or lease by the semester and depending on the school's policy can use this in one of three locked down environments.

4.7 What is the value of using your uSignOnline electronic signature?

a. As was addressed above, controlling the environment is very difficult, expensive and can be circumvented. One of the solutions that helps to "commit" the student is for them to sign a contract stating only they were completing the exam and complying to the school code of conduct. This is a psychological "Deterrent" to students and goes along way to keeping them honest. Use of uSignOnline forms a
binding contract that is the same as signing a contract using pen and paper. Sig-ID signed just with their mouse or stylus creates both a 'moral" and legal agreement with the student and helps prevent fraud.

4.8 Is the BSI technology capable of providing random periodic challenges to check identity during the course as well as exams?

a. The revised Education Act is calling for student ID to be verified using a process that ensures the student who signed up for the course is the same student who does the course work and writes the exams. BSI's technology is ideal for this purpose for the following reasons:
    I. No hardware beyond a mouse is required.
    II. Access is from any PC, anywhere anytime.
    III. An audit trail is created each time a student validates their identity and is used as an ongoing record the same student is signing in and validating their Identity.
    IV. The BSI system sits behind the institutions firewall and can be effectively secured and managed.
    V. Students have the ability to use the closed loop automatic password reset. This allows the student to gain access to their personal data, discussion groups etc.. at all times with no help desk calls.

b. A key point to make here is ease of use. Any system used in random periodic challenges should be simple to use, fast and efficient. Web cams or fingerprint readers certainly are not ideally suited for this application.

4.9 Use with Learning Management Systems

Two integration methods exist;

a. Our system sits in front of the learning management system and after the student signs in we are a URL re-direct. When the student has authenticated their identity they are re-directed back to the location they would normally be at.
b. BSI can provide a full integration with your learning management system.

4.10 "Ideal" Attributes for Online Student ID Verification

1. **Multiple purpose**. Fits easily into both a final exam situation or in courses that offer participation grades and submission of academic work and is adaptable to periodic, random challenges for student ID verification.

2. **Enroll once**. Ideally, students should be able to enroll at the beginning of their first course and keep their "secret profile" for use in multiple courses and for multiple years (policy based).

3. **Be easy for students to use**. Solutions must be simple and intuitive to use and must not scare students away with confusing or cumbersome technology impediments. They will flood the help desk with questions and complaints.

4. **Be cost-effective**. Institutions can't afford to pay for rolling out strong student ID verification for every student if it costs too much. Institutions need to look at the total cost for the solution even if costs are pushed down to the student. Students have choices where they take online courses, don't make it a burden for them at your institution. They may go elsewhere.

5. **Provide appropriate levels of security**. Naturally, high accuracy and security levels are necessary. The solution must provide protection during "normal" usage as well as during loss periods where students forget their credential or pending replacement of a device or card.

6. **Be easily manageable**. Solutions should easily integrate with the organization's Web site, security architecture and applications and should easily scale to support the size of the customer base. Credentials should be easy to distribute, renew, replace in the event of loss, and revoke.

7. **Work across different channels of interaction**. Given the efforts to implement and roll out student ID verification for Internet activity, it is reasonable to consider leveraging the solution beyond the standard Web browser environment that works with Web-enabled smart phones.

8. **Psychologically acceptable**. Make this security solution a "fun" thing to do versus a threatening one. More pressure may add to less enrollment. Many people have a stigma attached to leaving their fingerprint on a device that could be used/compared/stored by a third party. This may be especially true from those in the military. Some students may also react strongly to being "monitored" from web cams at their homes and or being "talked to" during an exam. Privacy issues could

become a huge barrier to uptake even after getting consent, especially if the exam does not go well.

5 Product Review

5.1 BioSig-ID™ - Dynamic Biometrics

BioSig-ID is a patented product using unique Dynamic biometric handwriting & gesture technologies. Activation is from any mouse, stylus or touchpad on any PC anywhere, anytime. BioSig-ID captures HOW you write/draw including your speed, direction, width, angle and length which is unique to each individual. The software allows access to only registered users who authenticate themselves against a stored profile. Users enroll one time and thereafter validate their identity in seconds.

5.2 Two Factor Authentication in One

BioSig-ID is a proven two factor solution to user authentication and with unique biometric data it cannot be lost, stolen or forgotten like PINS, tokens, cards and passwords. In an increasingly regulated market BioSig-ID provides a low cost, instantly scalable identity management solution for both the desktop and browser based account access.

Unlike finger, retinal or face scans only Dynamic biometrics allows the enrollee to introduce a secret code into the biometric process. The users can enroll with “a code or drawing” of their own choice which is their secret code (Figure 4).

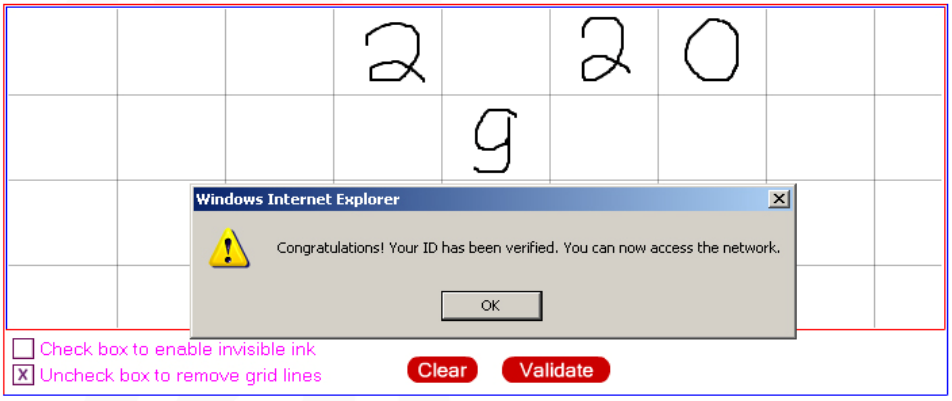

Figure 2 Drawing area and secret code used with BioSig-ID

Dynamic biometrics combines secrets with biometric samples (your unique way of drawing for example) to provide two-factor authentication in one process. BioSig-ID goes further than other static or dynamic biometrics because BioSig-ID is a unique 4 layer authentication that requires no special hardware:

1. Use of a reference ID = something you know
2. Choose your secret code = something you know
3. Draw or sign your secret code = something you are
4. Choose objects using Click-ID = something you know

5.3 Revoke and Replace

Only Dynamic biometrics allow an infinite number of different secret biometric samples (codes, images, and numbers) generated by the same individual. Revocation is instant and replacement is only a re-enrollment. If your fingerprint gets hacked it is gone forever. With BioSig-ID you can always change your drawing behavior.

5.4 How Does BioSig-ID™ Work?

Enroll (one time only) in the drawing area three times. Your enrollment “profile” is kept in a secure database and when you validate, your signature is compared to your “stored profile”. If it falls within a certain threshold, access is granted. Click-ID Image Technology creates an alternative access method and is strong authentication by itself. There is always a two layer approach using a primary and alternative access method for maximum flexibility and security. The alternative access is a profile re-set technology, that helps avoid help desk calls and is unique compared to all other biometrics.

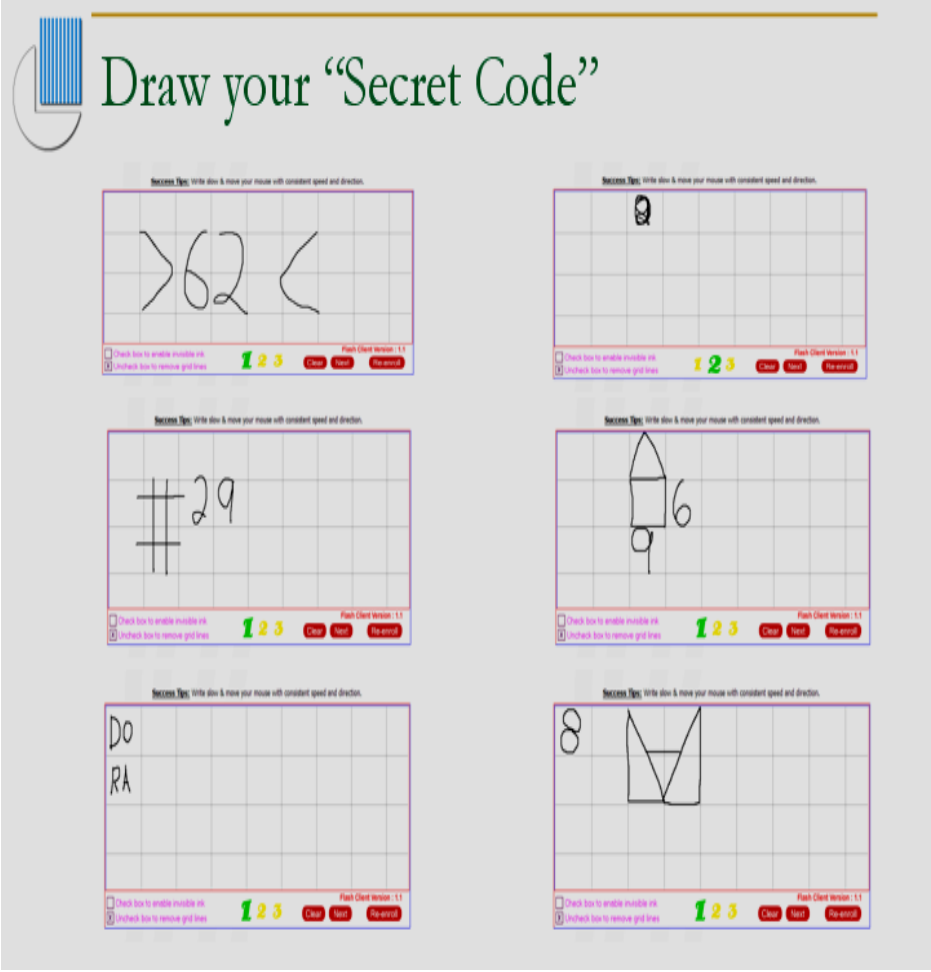

Figure 3 BioSig-ID secret code examples

Figure 4 After student verifies they can access records or exams

5.5 Click-ID™ Technologies for Identity Verification

Provides patent pending identity verification using images that are chosen from a list. After you choose an image the user must select specific objects in the image and in a sequence they must remember. Their identity is verified against a stored profile completed during enrollment. Enrollment profiles are kept in a database as binary code and used to compare to a new selected image and objects. If the selections are correct, identity is positive and access is granted. Every image that is presented after enrollment is changed so the user must remember what objects they selected and in the correct order. Each identity validation is randomly changed and acts as a one time password, a strong defense against duplication and hackers.

No need for any special equipment or hardware, just a mouse, stylus or touchpad. Audit trail log creates compliance document for multi-purposes. Application is for any browser based systems. Replaces tokens, smart cards, images, IP addresses, device reputation or other biometrics that require hardware. Augments PINS and passwords.

Click-ID by itself is stronger than a “hard” password or complex questions and infinitely easier to use as it requires only clicking on specific objects to verify the user’s identity. BioSig-ID combines with patent pending Click-ID™ Image technology that creates an alternative access and our unique “Closed loop technology”.

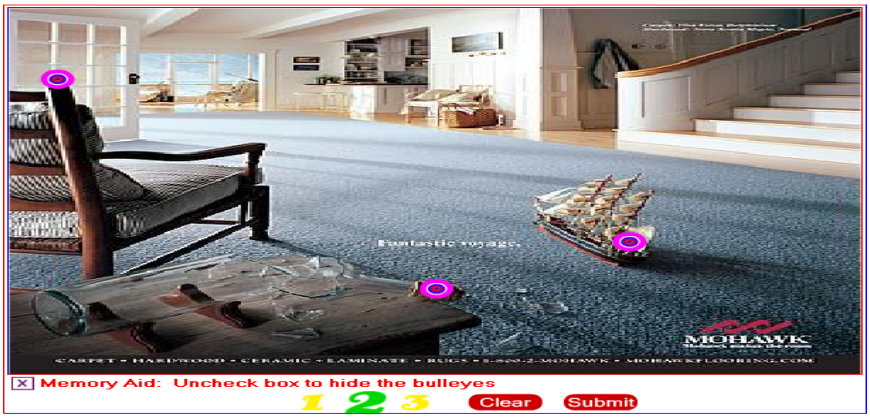

Figure 5 Click-ID picture example

5.6 uSignOnline™ Electronic Signature

uSignOnline provides a representation of the signature made by a client using a pointing device such as a mouse. uSignOnline demonstrates “intent” by a user for verification and evidence of ownership with online contracts, agreements, chargebacks, credit card purchases or other electronic purchases especially when used with other personal identifiers. Use of uSignOnline to sign provides a contract between two parties that is as binding as when signed with pen and paper. Eliminate the hassle and time spent getting documents signed.

Figure 6 uSignOnline signature example

uSignOnline™ Online Audit Trail Log

==========

The following is the record of when an individual user(s) completed a document or agreement using signatures created with uSignOnline™ Online. These records form an electronic signature and record compliant to the Electronic Signatures in the Global and National Commerce Act, Section 101, indicating the users' acceptance of the terms and conditions.

On November 19, 2008, 1:45:14 PM, the BSR Server stored the signatures for the user with Unique ID: EveAdams at IP Address: 127.0.0.1 from the webserver: 127.0.0.1 with SessionID: 81e6d3c598358a6b6f0d9eef655d0c9b.

Figure 7 uSignOnline audit trail log

6 Appendix A - Federal Government Validation

We have attached a brief summary of the validity of dynamic signature/gestures from the following:

1. NIST SP 800-32 Section 2.2.4 in its entirety
… "Biometric authentication relies on a unique physical characteristic to verify the identity of system users. Common biometric identifiers include fingerprints, written signatures, voice patterns, retinal scans, and hand geometry. The unique pattern that identifies a user is formed during an enrollment process, producing a template for that user. When a user wishes to authenticate to the system, a physical measurement is made to obtain a current biometric pattern for the user. This pattern can then be compared against the enrollment template in order to verify the user's identity…. ***Biometrics provide a very high level of security because the authentication is directly related to a unique physical characteristic of the user which is more difficult to counterfeit.***

2. National Institute of Standards and Technology, US Department of Commerce, Annual Report 2006, Computer Security Division – page 25
"Automated recognition of individuals based on their behavioral and biological characteristics"
..."Biometrics currently are increasingly being used to authenticate a person's identity, secure borders, restrict access to secure sites…
They provide higher degrees of security than other technologies like tokens, encryption and can be used to overcome their weaknesses.
Biometrics can use behavioral characteristics that are learned or acquired such as signature verification"
ISO/IEC JTC1 SC37 Standing document - NIST

3. Study Report on Biometrics in E-Authentication 8/21/2006 Ver. 0.5- Conducted with NIST, the Office of Management and Budget (OMB) and the International Committee for Information Technology Standards (INCITS). (Mr. Maynard of BSI participated in the creation of this document as a committee member and is listed on page 132)

<u>Excerpts:</u>
"Biometrics is a rapidly advancing field that is concerned with electronically identifying a person based on his or her physiological or behavioral characteristics. Because a biometric property is an intrinsic feature of an individual, it is difficult to duplicate and nearly impossible to share".

Two Factor Authentication in One
One of the properties which the use of Dynamic biometrics introduces compared to static biometrics is the ability of the enrollee to introduce a secret, which is under the control of the user, into the biometric process. For instance, the users of signature/gesture biometrics can enroll with "signs" of their own choice which may or may not be their

signatures. The biometric process therefore combines both a secret (sign) and the associated biometric sample into one operation giving it two-factor authentication status.

Dynamic biometrics therefore combines **secrets** with **biometric samples** to provide two-factor authentication in one process. Where the Dynamic biometric process involves a secret it is possible to build that knowledge into the threshold setting and to make the biometric FRR threshold more user-friendly without sacrificing the security of the overall biometric test. Further security can be added, as with all biometric systems, by requiring, for example, the use of a PIN with the biometric sample. In the case of the Dynamic biometric technology, the authentication process would then involve two secrets and a biometric sample. The PIN would have a multiplicative effect upon the inherent entropy of the biometric data, which contain both a secret and a biometric sample.

Revocation of the Dynamic Biometric Template
Because there are an infinite number of different secret samples that one individual can generate using Dynamic biometrics, the revocation of the template for whatever reason requires no more than a re-enrollment. The re-enrollment of different secret samples can be undertaken at any time and in the same way that passwords and PINs can be changed.

Dealing with the Sample Variability in Dynamic Biometrics
It is reasonable to believe that the sample-to-sample variations associated with Dynamic biometrics are greater than those associated with Image-Based biometrics, after eliminating the effects of rotational variations (in image based samples). However, these authors are not aware of any studies which try to validate this belief. It is not clear, for instance, how the inherent variations associated with placing one's finger, eye, face, hand or palm on or in front of an imaging device or swiping the finger across a sensor, compare to the variations inherent in submitting different samples of the same sign/gesture, phrase or keyboard sequence. What is clear is that Dynamic biometrics add a new dimension to the biometric sample – that of time. This itself, introduces its own variability but it also adds a further powerful set of discriminating data.

One way of dealing with sample variability is to measure and store it as part of the template. Most Dynamic enrollment processes (and some Image-Based ones) capture a number of samples from which to form the template. It makes complete sense to use these enrollment samples not only to measure feature means but also to measure the feature deviations. Typically, in this case, the template would be adaptive so that the estimated means and deviations continue to change and be reflective of the individual as biology changes over time. Some Dynamic biometric technologies measure sample variations and provide for an adaptive template. One of the ensuing benefits of measuring the sample variability and storing it in an adaptive template is that it is then much easier to determine individual sample distributions. Individual FRR thresholds can then be determined in an efficient manner, on an a priori basis, using sound statistical theory, as opposed to setting them based upon empirical data after the event. When the sample variations are measured during enrollment, it is possible to test the samples for consistency before forming the template. This prevents two or more people colluding.

Multi-factor authentication can take two primary forms: the use of multiple biometrics or the use of biometrics in conjunction with smart cards and PINs. Both methods reduce the likelihood of an imposter being authenticated. Spoofing also becomes more time consuming and challenging when multiple body physiological or behavioral characteristics need to be copied and imitated. Impostors for whom a biometric matches an enrolled user are unlikely also to match with respect to a secondary biometric.

Adding randomization to the equation also adds security. Verification data, for example, could be randomized, such as asking for three fingerprints one day and a different combination of two fingerprints the next day. Additionally, where time provides, designers of biometric technologies and systems should explore random or cued challenges. That is, even if a person correctly authenticates once, the system might still challenge the user to re-authenticate to help increase its confidence that the biometric data submitted is genuine. Cued challenges could also be paired with certain behaviors causing alarm – such as an uncommon stillness, lack of movement, or change during the acquisition of biometric data.

4. Financial Institution Letter
FIL-103-2005

FFIEC GUIDANCE
Summary: The Federal Financial Institutions Examination Council (FFIEC) has issued the attached guidance, "Authentication in an Internet Banking Environment." For banks offering Internet-based financial services, the guidance describes enhanced authentication methods that regulators expect banks to use when authenticating the identity of customers using the on-line products and services. Examiners will review this area to determine a financial institution's progress in complying with this guidance during upcoming examinations. Financial Institutions will be expected to achieve compliance with the guidance no later than year-end 2006.

Excerpt from page 8 of the FFIEC guideline on use of acceptable biometrics for online bank customers:

Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (*something a person know*s) or a token (*something a person has*).
Various biometric techniques and identifiers are being developed and tested, these include:

- fingerprint recognition; face recognition; voice recognition; keystroke recognition; handwriting recognition; finger and hand geometry; retinal scan

5. Gartner Research (Research Report on all known vendors in the identity access and management and authentication markets).
Publication Date: 26 September 2008 ID Number: G00159589

Market Overview: Authentication
Ant Allan PhD

Highlights include:
Vendors Offering Knowledge-Based Authentication Methods- page 15, we are featured as being one of 5 vendors offering Image and Image Recognition Technology (e.g. Click-ID)

Vendors Offering Biometric Authentication Methods- page 29, we are featured as being the only vendor offering signature/gestures. (eg. BioSig-ID)

7 About the Founder

Mr. Maynard is the CEO and founder of Biometric Signature ID. He is the creator of several patented and patent pending inventions using handwriting biometrics and image pattern technologies to verify identity. He is a former CEO running 2 divisions using biometrics in healthcare for a public traded company. Previously Mr. Maynard was a partner in a software firm that created predictive modeling software for large healthcare clients like United Healthcare. The company was sold to a public company. Mr. Maynard received his undergraduate degree from York University, Toronto and completed executive training from Harvard/MIT, and Kellogg School of Business. He is a committee member for the INCITS/NIST "Study Report on Biometrics in e-authentication 2007, member of Center for Ethical Identity Assurance (www.ceiaglobal.org), volunteer for the Biometric Technology Working Group for the National Biometric Security Project. Mr. Maynard has been a guest lecturer at University of Texas, Dallas Business School, a judge for the UTD Business School Idea Competition, a keynote speaker at 3 conferences, has been an invited speaker at the Texas Technology Executives Network, the Technology Executive Network Group and is a co-star presenter at UNT division of MIS graduate studies. He has published selected works on biometrics including in the trade journal - Smart Card and Identity News entitled "Click Click Who's There?" white papers "Student ID Identity Proofing Solutions" "Internet Based Identity Proofing", and is a sought out speaker on the application of Dynamic biometrics.