

---

# **Identity Proofing for Student ID Verification Report of Pilot with University of Maryland University College**

---

Prepared by:

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

**Document No.: 0000018  
Revision: 2  
Date: November 5, 2009**



## Case Study

### “Report on the Use of Biometric Signature ID Identity Proofing Technology for Student ID Authentication”

Jeff Maynard BSc, CEO and Founder, Biometric Signature ID.

#### Abstract:

***Section 602.17 of the re-authorized Education Act of 2008 now requires an institution that offers distance education to have processes through which the institution establishes that the student who registers in a distance education course or program is the same student who participates in and completes the program and receives the academic credit.***

***To meet these new requirements and test a solution that would allow more computer based exams at home while maintaining the highest integrity levels UMUC contracted with Biometric Signature ID to run a proof of concept pilot using their dynamic signature/gesture technology to authenticate student identity remotely.***

***Over a 1 month period (July 17-August 15, 2009) 27 students and 3 faculty from multiple classes volunteered 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 at various times during their course and at the final exam. 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. They then authenticated their identity before taking the exam. Full audit trails were analyzed of all activity and an online survey was administered. The proof of concept was deemed very successful with 100% of participants able to enroll and validate. A substantial majority of the participants (83%) responded to the survey with 93% of participants rating the verification system as “Extremely or Very convenient” and almost 100% agreed to recommend BioSig-ID be used for student identity authentication. Combined average time of enrollment in both BioSig-ID and Click-ID was 38 sec, while authentication took up to 23 seconds only. Nearly 900 signature enrollment/authentications were completed by the participants in 28 days for an average of nearly 30 activities per participant. The use of signature/gesture software from Biometric Signature ID proved to be effective in authenticating student ID multiple times during the course and at the final exam. Based on the results of this pilot, there is sufficient evidence that this software is a valuable tool for remote identity proofing to authenticate student identity that requires little administration and no additional hardware.***

## **Introduction**

UMUC has a strong tradition of academic integrity and has invested substantially in providing proctored final exams for undergraduate courses, with over 30,000 individual exams administered each semester. UMUC is the largest public university in the nation with over 189,000 online course enrollments. Their board of regents anticipates that UMUC will grow student enrollment 48% by 2014. Latest statistics point to 12% growth in online course enrollments versus 1% for bricks and mortar. With this explosive growth, enrollment additional strategies that will help manage this growth are being evaluated. One of the strategies that institutions like UMUC can use to “accommodate growth” and better meet the needs of adult working students is to offer significantly more computer based exams (CBE) at home. Since students can take exams at home, a reduction in the number of proctored sites and costs can be achieved. However the education act is also requiring institutions to verify the identity of a student who participates in class or coursework. To do this, solutions that maintain the highest student integrity are being examined.

Many Institutions want to find a solution that could decrease the likelihood that a student could share their “access credentials” thereby affecting the integrity of the system at various points in the delivery of course content and student participation. Biometric Signature ID was selected as a promising identity proofing biometric technology that can provide a solution to compliance and integrity needs. By comparison to more traditional verification measures like pins, passwords, tokens and knowledge based questions, BSI’s patented dynamic biometric technology cannot be borrowed or shared, which addresses the major integrity issues. The software only solution provides a true authentication of the user because it measures unique characteristics of the individual commonly referred as “something that you are” using just a mouse, stylus or touchpad. The software also incorporates “something that you know” making it a true multi-factor authentication system similar to those required for online banking.

There is no perfect system. To do nothing beyond the current status quo does not address the intent of the new requirements for student ID verification aimed at increasing the “Integrity quotient”. “Cheating in academic institutions – A Decade of Research” has been researched by McCabe et al and other researchers like Bowers et al. McCabe found that 67% of students admitted to cheating and 87% admitted cheating on written

assignments. Web sites like the following “teach” strategies of cheating. <http://exam-cheat.uv.ro/cheat.html>. Little research has been done on cheating in Online courses. In research reported by Donna Stuber-McEwen et al (Point, Click, and Cheat: Frequency and Type of Academic Dishonesty in the Virtual Classroom, Online Journal of Distance Learning Administration, Volume XII, Number III, Fall 2009 University of West Georgia, Distance Education Center) their results suggest that cheating in online courses is not as pervasive as some believe, “when there is relative anonymity and a separation between instructor and student, these concerns seem to increase”. They believed however, that as online learning becomes more accepted as a means to an educational end and available to more people, “it is likely that the prevalence of academic dishonesty will increase”.

An example of the level of cheating found by self report from the McCabe and Trevino (1993) research and 1997 update is found in Table 1.

TABLE 1 Self-Admitted Cheating—Summary Statistics						
<i>Variable</i>	<i>1963<sup>a</sup> (%)</i>	<i>1993<sup>b</sup> (%)</i>	<i>1990–1991 (%)</i>		<i>1995–1996 (%)</i>	
			<i>No Code<sup>c</sup></i>	<i>Code<sup>d</sup></i>	<i>No Code<sup>e</sup></i>	<i>Code<sup>f</sup></i>
Serious test cheating <sup>g</sup>	39	64	47	24	45	30
Serious cheating on written work <sup>h</sup>	65	66	56	32	58	42
All serious cheating	75	82	71	44	71	54

<sup>a</sup>*n* = 452. <sup>b</sup>*n* = 1,793. <sup>c</sup>*n* = 3,083. <sup>d</sup>*n* = 3,013. <sup>e</sup>*n* = 1,970. <sup>f</sup>*n* = 2,303. <sup>g</sup>Serious test cheating includes students who have engaged in copying on an exam—with or without another student’s knowledge—using crib notes on an exam, or helping someone else to cheat on a test or exam. <sup>h</sup>Serious cheating on written work includes students who have engaged in plagiarism, fabricated or falsified a bibliography, turned in work done by someone else, or copied a few sentences of material without footnoting them in a paper.

**Table 1: Self-Admitted Cheating Summary Statistics**

The US department of Education is implementing the legislation and has introduced improvements in the integrity of online higher education. The US financial sector has recognized that PINS, passwords or even security questions just don’t go far enough as single credentials for ID verification and instituted multi-factor authentication requirements for all online banking clients in 2008. (Federal Financial Institutions

Examination Council (FFIEC) guidance, “Authentication in an Internet Banking Environment).

Alternative security methods like web cams, and fingerprint readers have been evaluated. While these methods appear to “control the environment” in electronic proctoring, they face opposition and barriers to uptake on several major fronts including:

- privacy issues
- high costs
- deployment and installation issues as many include photo ID and authentication
- costs for real time or after the fact monitoring
- need for policies to deal with infractions
- drain on resources for monitoring by itself are large barriers to uptake
- use and ability to transfer this technology to multiple courses
- limited ability to use for courses that do not have final exams

## “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 need to look at the total cost for the solution. Costs can be pushed down to the student. Can we make revenue on this? Can you reduce help desk calls and save money? Students have choices where they take online courses, don’t make it a burden for them at your institution.
5. **Provide appropriate levels of security.** High accuracy and security levels are necessary. Must provide protection during “normal” usage as well as during loss periods where students forget their credential or pending a replacement of a device or card.
6. **Be easily manageable.** Easily integrate with the organization’s Web site, security architecture and applications, easily scale to support the size of the customer base. Credentials should be easy to distribute, revoke, renew and replace in the event of loss.
7. **Work across different channels of interaction.** Consider leveraging the solution beyond the standard Web browser environment to work 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

# Biometric Signature ID

## Identity Proofing Solutions Using Just a Mouse™

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.

BSI’s BioSig-ID technology offers a new twist to the traditional biometrics like fingerprints or facial scans. These static biometrics rely on physical (anatomical) attributes unique to each individual. However, in distance education it is not always practical or cost effective to use a biometric that requires a reader or other hardware. BSI has created a solution that involves a dynamic biometric using signature/gestures. BSI’s dynamic biometric is behavioral in nature and offers the same identity authentication attributes as anatomical biometrics without any hardware. This removes the largest barriers to uptake – cost and inconvenience. BSI technology also offers multiple layers of identity proofing that provides choices and flexibility. BSI’s closed loop technology provides a self service auto password reset and can provide significant savings to institutions by avoiding the near 50% of calls received for password reset.

BSI’s patented dynamic software technology uses your regular mouse, stylus or touchpad to measure the unique biometric characteristics of each student. These characteristics include the speed, direction, height, length, width, angle of the “signature”, and stores these in a secure database. Only the “real” student can authenticate themselves in subsequent log ins. These unique biometric characteristics cannot be borrowed, duplicated or shared and represent the highest level of identity authentication and security.

Users enroll one time in minutes and thereafter authenticate their identity in seconds. An individual enrolls in BioSig-ID using easy to follow instructions. A drawing screen with gridlines appears and an individual is asked to draw their secret code, usually a series of number or letters. By holding the left mouse button down this process is repeated 3x to create a profile. This profile is stored in a secure database. When an individual goes on his computer the next time only a validation screen will appear. The user enters their secret code using their mouse and views this on the monitor. If the “secret code” matches the individual’s enrollment profile, access is granted.

# Biometric Signature ID

## Identity Proofing Solutions Using Just a Mouse™

At enrollment the user enrolls in an alternative access method called Click-ID. The user chooses an image from a list of images and selects 3 specific objects in that image. The user clicks on them with their “mouse” in a certain order. This step is also repeated 3x to create a profile. Identity is verified against a stored profile completed during this enrollment. Thereafter if the image, objects and correct order of the objects is selected, access is granted. Like BioSig-ID the profile is kept in a secure database and is associated with the users’ unique reference ID which can be their e-mail address.

The BioSig-ID Online, Click-ID Online and Complex Security Questions architecture consists of three (3) layers of security. During enrollment, a user enrolls in a minimum of 2 security layers 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.

### **Methods and Procedure**

UMUC elected to use a 2009 summer session for the pilot and identified approximately 160 students who were scheduled to take their final exam in a certain facility as the group from which to draw voluntary participants. These students were from multiple classes. Through an e-mail campaign, these students were canvassed and 27 students (or 17% of potential students) and 3 staff volunteered to participate in the pilot.

Participants were asked to enroll, create a profile and authenticate their identity at various times during their course and at the final exam. 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. They then validated their identity before taking the exam. Full audit trails were analyzed for all activity. No personal identifying information was collected ensuring student privacy was not breached. Online survey results were obtained from 83% of students and faculty who gave the software very high marks for ease of use, simplicity and effectiveness in authenticating student identity.

**Period 1- July 7 to July 19, 2009**

BSI prepared a custom training video for UMUC student participants. An e-mail sent to the student volunteers instructed them to visit the specific website that BSI setup for the pilot. They were instructed to watch the instructional video, enroll their profiles using BioSig-ID and Click-ID and go through the authentication process. A full integration of UMUC's WebTycho online IT system was not done for this pilot.

**Period 2- July 17 to August 13, 2009**

Another e-mail was sent to the student volunteers encouraging them to practice authenticating their identity with BioSig-ID prior to the final exam. The student participants were invited to fill out a short survey on their enrollment and authentication experience. Completion certificates were e-mailed to each student participant with instructions to print out and bring the certificates with them to the proctored test site. A final e-mail was sent to the students instructing them about the validation procedure at the final exam, and reminded the students to practice validation and bring their completion certificates.

**Period 3- August 14 to August 15, 2009**

The final exam was administered over two days and at four different exam start times. Student participants were asked to validate their identity using BioSig-ID prior to taking their exam. Students were directed to a bank of separate computers and asked to validate their identities using UMUC supplied workstations and PC mouse(s). The students also handed over their Completion Certificates and were checked off by the proctor from a list.

**Results:**

- 100% enrollment achieved for all 30 participants.
- Average enrollment time of 48 seconds for BioSig-ID and 28 for Click-ID.
- Survey results were obtained from 83% of participants.
- Participants gave very high marks for ease of use, simplicity and effectiveness in authenticating student identity
- On test day, 100% of eligible students able to validate their identity.
- The students averaged 19 to 23 seconds to validate on test day.

# Biometric Signature ID

## Identity Proofing Solutions Using Just a Mouse™

- Successful communication with students via e-mail campaigns illustrates scalability to a wider audience.
- No personal identifying information was collected ensuring student privacy.
- Closed loop technology (password reset) eliminated all help desk calls.
- Testing time was not impacted due to the very short time required for validation.
- Students seemed “intrigued” with the system and as a consequence spent more of their own time in the system validating their identities 3-7X more than asked.

### **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

### **Discussion:**

The revised education act raises the bar for student verification, with the intent to ensure the integrity of distance learning. Current methods using Pins and passwords, or security questions fall short of authenticating the “real physical user” and provide little assurance that the students who complete the course or take a computer based exam are who they say they are. If we allow simple pins and passwords to continue to be the acceptable criteria to meet the requirement we have not advanced on the “integrity quotient” and the intent of the revisions. While Pins and passwords are still acceptable for the short term accrediting bodies may look for more than the bare minimum and will likely want to see institutions adopting stronger authentication methods. The real question for institutions is where they want to set the threshold of academic integrity: this internal decision, rather than the force of external requirements, should determine their needs for new technology.

This pilot study reported that the participants were able to authenticate their identity in seconds using a mouse from any PC, anywhere to establish proof they are who they say they are. The use of signature/gesture software from Biometric Signature ID proved to be effective in authenticating student ID multiple times during the course and at the final exam. Based on the results of this pilot, there is sufficient evidence that this software is a valuable tool for remote identity proofing to authenticate student identity that requires little administration and no additional hardware.

# Biometric Signature ID

## Identity Proofing Solutions Using Just a Mouse™

***Special thanks to Matthew Prineas PhD, Office of the Provost and his team at the University of Maryland University College for his significant contributions in the development and implementation of the pilot.***

***Dr Prineas can be reached at 301-985-7931 or at [mprineas@umuc.edu](mailto:mprineas@umuc.edu)***

For more information or to arrange for a no obligation trial of BSI's technology, contact:

Jeff Maynard CEO  
Biometric Signature ID  
972-436-6862  
[Jeff.maynard@biosig-id.com](mailto:Jeff.maynard@biosig-id.com)  
[www.biosig-id.com](http://www.biosig-id.com)

### **Glossary of Important Terms:**

The distinction between “Verification and Authentication”

Verification of an identity is when you have reason to believe at some confidence level (a prediction) that the individual is who they say they are. Typical measures include; pins, passwords, tokens, knowledge based questions, cards etc. These measures do not authenticate the physical user. Rather they verify the physical item in the users' possession or that the user knows the answer to a question. They all fall short of authenticating the “real physical user”. It could be anybody masquerading as you with your stolen or borrowed passwords. In addition, there is no way to positively link the usage of the system or service to the actual user; that is, there is no protection against repudiation by the user ID owner. For example, when a user ID and password is shared with a colleague, there is no way for the system to know who the actual physical user is.


Authentication on the other hand is when you can positively identify the user based on who they ARE from anatomical, physiological or behavioral characteristics unique to that individual. This requires a biometric. Biometric solutions that do not require any hardware do exist. These are dynamic biometrics that are behavioral in nature and offer the same identity authentication attributes as anatomical biometrics like fingerprints and are equally difficult to duplicate and nearly impossible to share.

# Biometric Signature ID

Identity Proofing Solutions Using Just a Mouse™

## Enrollment drawing area.

Users “draw their secret code” three times to create a profile



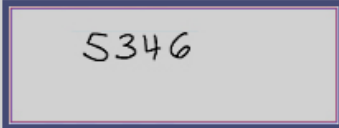
University of Maryland University College

Home    FAQ    Sign Out

### Enroll BioSig-ID Profile

**Directions:**

- Select 3 or more different characters/initials/shapes to use as your personal ID (see example)
- Using your mouse, hold the left mouse button down
- Draw these different characters/initials/shapes in the space provided
- Use the lines as the reference
- Select "Next" after completed

**Example:** 

**Success Tips:** Write slow & move your mouse with consistent speed and direction.

	2		9					
		2		0				

Check box to enable invisible ink  
 Uncheck box to remove grid lines

**1 2 3**

Flash Client Version : 1.1

**Clear**    **Next**    **Re-enroll**

# Biometric Signature ID

Identity Proofing Solutions Using Just a Mouse™

**Click-ID Human Pattern Recognition - serves as the second layer of security**



University of Maryland University College

[Home](#)

[FAQ](#)

[Sign Out](#)

**NEXT STEP:** BioSig-ID Technology allows you to create an alternative access for your personal protection and flexibility.

**Direction:** Please click on an image below to begin.



[The Animals](#)



[The Kitchen](#)



[The Shoes](#)



[The Numbers](#)

**Completion Certificate (optional) – presented at exam**

