Case Report

1,893 Online Students using BioSig-ID™

For Student ID Verification:

May – December 2011

BIOMETRIC SIGNATURE ID™
* IDENTITY PROOFING SOLUTIONS

Prepared by:

Jeff Maynard BSc.– President
Biometric Signature ID
jeff.maynard@biosig-id.com
708 Valley Ridge Circle-Suite 8
Lewisville, TX 75057

www.biosig-id.com

Office: 972-436-6862
January 15, 2012

Foreword by:

Dr. Mark Sarver PhD - CEO
EduKan Consortia
marks@edukan.org

Document : 000077

Foreword

Dr. Mark Sarver, CEO of eduKan - www.edukan.org
Marks@edukan.org

EduKan manages the online courses for a consortium of six colleges in Kansas - Pratt Community College, Barton Community College, Garden City Community College, Seward County Community College and Area Technical School, Dodge City Community College and Colby Community College.

During the first quarter of 2011, we evaluated multiple student identity verification solutions to remain compliant with the Higher Education Opportunity Act of 2008 mandates and with those required by our accrediting agency, the Higher Learning Commission (North Central Association). We were also searching for a company whose technology would seamlessly integrate with our Pearson eCollege Learning Management System (Learning Studio).

Since our courses feature proctored exams in addition to other assessment opportunities, such as discussion/participation groups and quizzes, we needed a technology that could be used for all gradable events. Additionally, we needed a solution that would allow our students to authenticate their identity randomly and often throughout the duration of course.

We selected Biometric Signature ID Corporation (BSI) because their technology met our needs and aligned with our mission of remaining affordable, accessible, and maintained student privacy. In April 2011, we conducted a pilot test program with 174 students from multiple classes using BioSig-ID™ to authenticate their identity six times before their final exam. The data from the pilot indicated BSI's solution would not only meet the needs of the faculty and administration but also provide the student with a user-friendly means to authenticate. Students who answered our surveys overwhelmingly preferred BioSig-ID (97%) to driving to a facility or finding a proctor for physical proctoring.

EduKan went live in May 2011 with BioSig-ID as the sole student ID authentication system. BioSig-ID replaced physical proctoring, is now used for all other gradable events, ensures compliance and provides random, periodic authentication challenges to the students. An additional feature of the BioSig-ID software that we appreciated immediately was the robustness of the audit trail. Our instructors were able to access this web tool and review certain aspects of the student's re-set, suspicious and re-enrollment activity. Although our instructors still have the ability to conduct physical proctoring on as-needed basis, using BioSig-ID has eliminated the associated costs and inconveniences to both the faculty and the students. Moreover, using BioSig-ID ensures we will remain compliant with HEOA and accrediting agency mandates.

The results reported below are from 1893 students observed from May – December 2011. The outcome has been impressive in achieving our goals of reducing costs, maintaining compliance, and ensuring academic integrity. We also recognize that certain other aspects of using BioSig-ID have additional benefit to eduKan and our colleges. These subjective values are represented under "inputted value" and range from 5%-10% incremental gains for:

- Reduction of help desk calls creating a positive student experience,
- Value to the colleges for gain in reputation,
- Compliance value gains.

As indicated in our results below, for every one dollar we invested in BioSig-ID, we estimate that we received a return in excess of four dollars.

The eduKan results are summarized as follows:

eduKan savings model using BioSig-ID versus physical proctoring		
Actual costs for physical proctoring with 4,000 students (best estimate)	$	152,000.00
Reduction of costs including staff/faculty time when switching to BioSig-ID		80%
Budget gain	$	121,600.00
Regular cost to conduct physical proctoring/student	$	38.00
"Special" limited pricing for BioSig-ID (licenses)/student - 2500 students	$	12.00
Savings est. per student	$	26.00
% savings capital recovery		68%
Additional considerations of inputted value		
*Reduction of help desk calls, enhanced school reputation, compliance	$	9.50
Dollar savings /capital recovery	$	35.50
% savings after using BioSig-ID versus physical proctoring cost per student		93%
Dollar savings combined with inputted savings exceeds the actual costs	$	159,600.00
ROI - Cost of BioSig-ID divided by budget gain (without inputted value)		405%

Case Report

"If it is so easy it can't be wrong"

Background

This quote may very well sum up how students feel about cheating in online courses and maybe their thoughts on academic cheating for all courses. Typically there are few if any deterrents to prevent students from engaging in academic dishonesty. Beyond using a pin or password which is easily circumvented, schools generally do not use any other technology for remote student ID verification. Due to identity theft and mis-representation, Congress is mandating most of the federal agencies to use better security. They are asking the agencies to use strategies that involve at least two "factors" of security. A pin or password combined with either a biometric or a token is becoming the new security standard. This security strategy is called Multi-Factor Authentication or MFA.

The Federal Department of Education was no exception in complying with new security guidelines and made a new ruling in Section 602.17 of the re-authorized Education Act of 2008, released in late 2009. This act 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.***

Many educational institutions are looking for a student identity verification solution to help manage growth and compliance issues with the Higher Education Opportunity Act of 2008 (HEOA). As more courses are delivered online, institutions are also looking for alternatives to facility limiting on-site proctoring. A solution with the ability to offer student ID authentication for taking exams online and authentication for non-exam courses is desirable. The ideal solution(s) should also respect student privacy, be delivered at random, periodic points throughout the delivery of course content, simple to use, be cost effective and offer the highest deterrent to academic cheating.

Biometric Technologies

Biometrics confirm the identity of an individual through anatomical, physiological, or behavioral characteristics. Some biometric solutions *do not require* any hardware or require users to give up a part of their anatomy (i.e. DNA swabs, fingerprint, iris scans…). These are "dynamic biometrics" that are behavioral in nature and include voice, keystroke and gesture biometrics. Earlier independent third party testing by the Tolly Group suggests that gesture biometrics are 27 times more accurate than keystroke in false positive and false negative parameters [1]. In fact gesture biometrics using BioSig-ID software was found to exceed the national standard set by the national Institute of Standards and Technology (NIST) by a 3 fold factor while keystroke did not meet the standard [2]. Gesture biometrics now offers the same identity authentication attributes as anatomical biometrics (such as fingerprints or iris scans), though software only.

Biometrics are nearly impossible to duplicate or share unlike pins, passwords or tokens. Biometrics authenticate the physical person. Authentication is different compared to verification.

- For example, 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 or access cards.
- These do not authenticate the physical user. They only 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.
- **Importantly, 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 non-repudiation by the user ID owner. There is no way for the system to know who the actual physical user is. Consequently, users can deny it was them and it is near impossible to prove otherwise.**

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.

Because authentication through gesture biometrics can be applied to multiple course elements that are all gradable, assessments are not limited to tests as is the case with physical proctoring or computer based monitoring (digital proctoring). In fact, because gesture biometrics are software only, using existing mouse, stylus, touch pad or touch screens, student identities can be challenged quite frequently when online participating in daily work. Additionally, gesture biometric systems have low implementation costs and staffing needs, unlike physical or digital proctoring. For example many schools demand their students drive to a facility if they are within a 50 mile radius to receive physical proctoring, adding cost and extra effort burdens on students. Alternatively, digital proctoring usually is conducted for only high stakes exams and the technology is not set up to verify student ID other than final event exams. With the high costs of using digital proctoring technology and inability to offer student ID verification continuously throughout the course, schools can only use digital proctoring for a sample of students. A sample of students will usually not satisfy compliance with the HEOA.

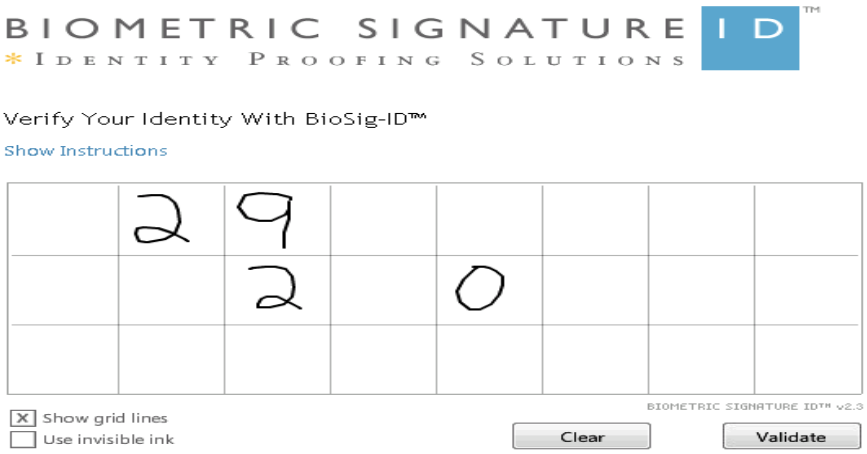
Biometric Signature ID

Biometric Signature ID offers a proven, patented gesture biometric called BioSig-ID for student ID authentication. This software does not require any additional hardware or software downloads, can be used on any PC or device anywhere, anytime and does not collect personal identifying information. In comparison to more traditional verification measures like pins, passwords, tokens and knowledge based questions BioSig-ID cannot be borrowed or shared. BioSig-ID is software only and is activated using flash or HTML 5 and can be used with virtually all devices that accept an input.

BioSig-ID provides physical authentication of the user by measuring unique characteristics of the individual commonly referred as "who you are". The user signs or draws their password in the

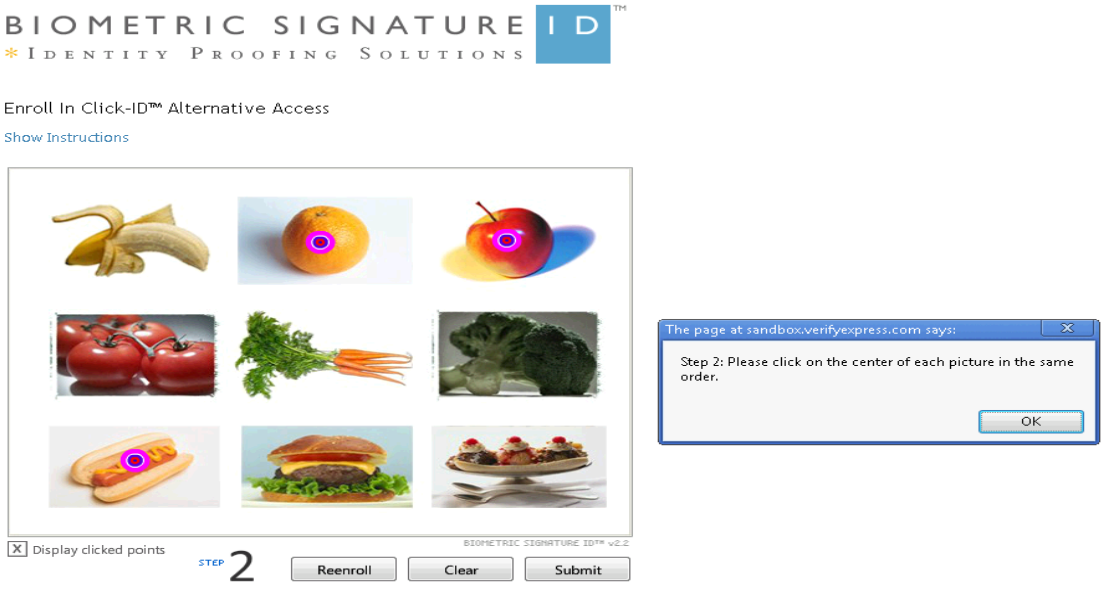
drawing grid supplied using just a mouse, finger, stylus or touchpad. Now that users are un-tethered from keyboards, shapes and objects can be drawn in lieu of or in addition to numbers and letters. See Figure 1.

Figure 1 – The drawing grid and example of a password



Users also are instructed to create a password using a second layer of identity verification called Click-ID™. This is a picture password created when the user selects a picture from a series of pictures and then selects a sequence of objects in the picture by clicking on them. See Figure 2 below.

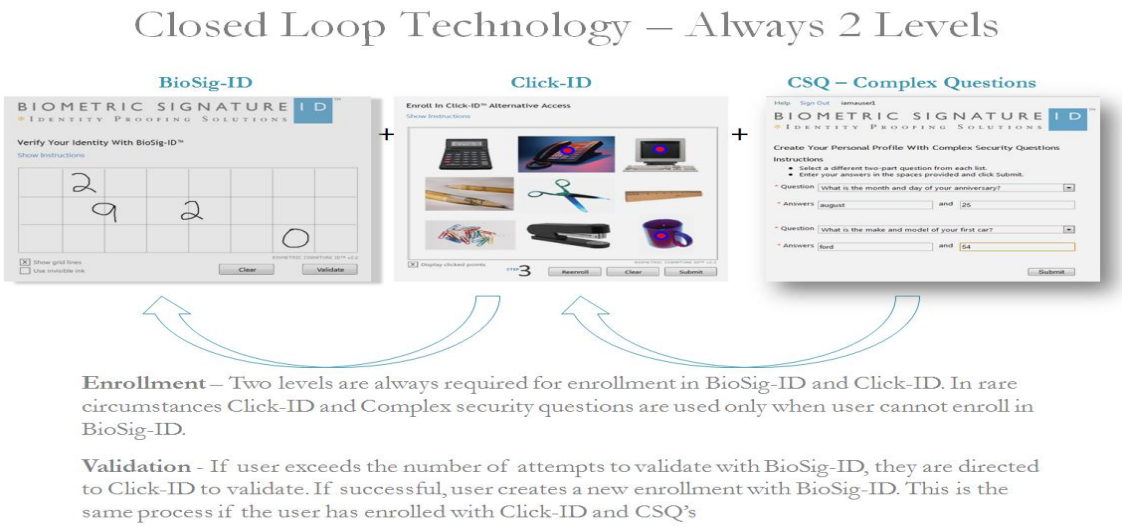
Figure 2 – Click-ID the second layer of security



This second layer of identity verification creates a "closed loop technology" that permits the user to complete a self service password reset and re-enrollment, thus avoiding help desk calls. If the user has physical limitations and cannot complete an enrollment with a pointing device they can bypass this stage. In this case Click-ID becomes the primary authentication with complex security questions

as the second layer. Some physically impaired students can become exempt from using the software all together. An example of this closed loop is illustrated in Figure 3.

Figure 3 – Closed Loop



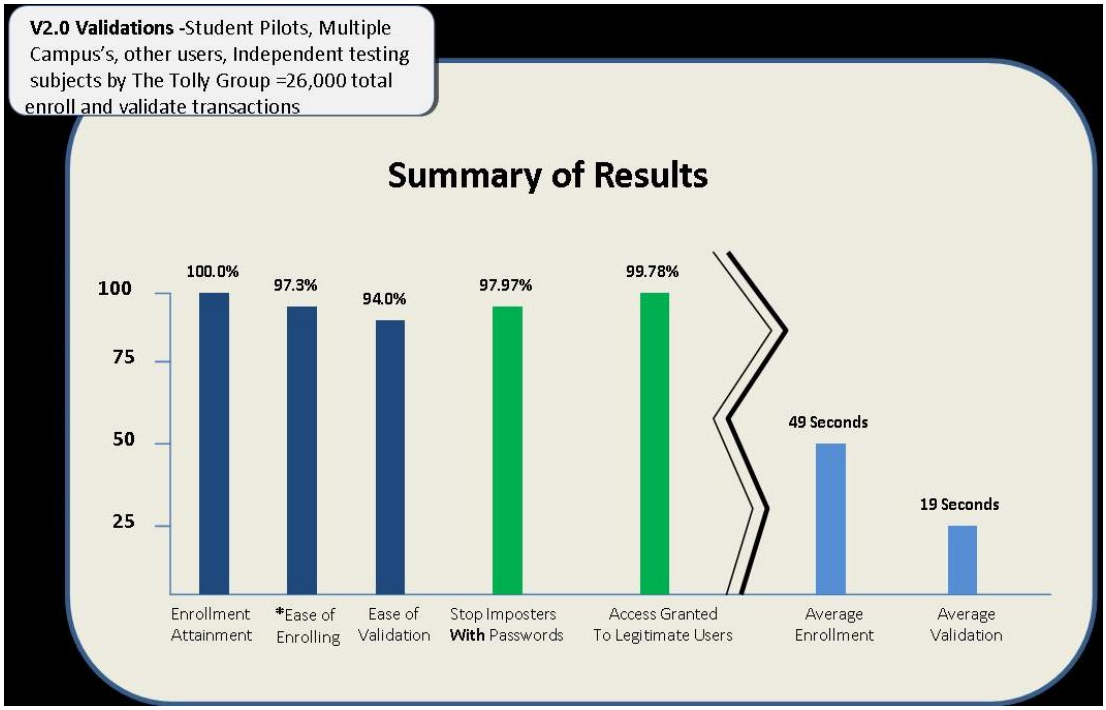
In a recent published report by the Tolly Group [2], the BioSig-ID software was found to be 99.97% effective in identifying imposters and stopping them from having a successful log in. This in spite of the fact the imposters had the correct log in credentials (e-mail and password) of the original user. This level of accuracy exceeds the National Institute of Standards and Technology (NIST) requirements cited in CFR 21, 1311.116 standard by a 3 -fold factor. This achievement has been well received by federal agencies looking to implement a biometric system to conform to the new standard of Multi-Factor Authentication (MFA). This standard requires that security needs to consist of any two of the following:

- Something you have (i.e. a card or token)
- Who you are (i.e. always a biometric)
- Something you know (i.e. Pins, passwords, security questions)

Biometric Signature ID is also currently working with global leaders in support of the National Standards for Trusted Identity in Cyberspace (NSTIC)- a White House initiative to create an authentication credential that will allow users to navigate the Internet without fear of identity theft.

The BioSig-ID software has been assessed by 22 colleges and universities, user groups and in production users. A summary of the results from over 26,000 enrollments and validations from multiple schools and populations is described in Figure 4.

Figure 4 – Experience data from 26,000 actions



The BioSig-ID software was initially evaluated in 22 Universities and colleges in the US with students of various ages, gender, in graduate and undergraduate levels. Using online surveys (Survey Monkey) 98% of the 407 students responded that they had a positive experience in using the software. In some schools, it was also reported by nearly 45% of students that they found the software entertaining. (Data on file).

Results

The following is a detailed report of activity from a cohort of nearly 2,000 students from three different institutions using two different learning management systems. The activity results were analyzed using the robust audit trail technology resident in the BioSig-ID software. An example of the reporting tool (Custom Detail Report) and the data that is collected is found in Table 1 below. The data that is collected is all public domain information rather than private information including the IP trace route. (Note for security reasons, the signature data shown below is not typically provided and is shown here for illustration purposes only.

Table 1- Custom Detail Report

Custom Detail Report

From: 12/22/2011 **To:** 12/29/2011

UserID: <Unspecified>

Name	Time Stamp	Signature Data	Server IP	Client IP	IPTrace Route	Device	Context	Action	Success	Accuracy	App
l.com	12/23/2011 9:49:05 PM		2002:4834:fe19::4834:fe19	64.134.60.140	64.134.60.140: [...	None	Enroll	CreateUser	True	0	Biosig-ID
le@aol.com	12/25/2011 11:38:22 PM		2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	None	Enroll	CreateUser	True	0	Biosig-ID
le@aol.com	12/25/2011 11:38:48 PM	292 0	2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	Mouse	Enroll	CreateProfile	True	100	Biosig-ID
le@aol.com	12/25/2011 11:39:00 PM	2920	2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	Mouse	Enroll	CreateProfile	True	87	Biosig-ID
le@aol.com	12/25/2011 11:39:10 PM	2920	2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	Mouse	Enroll	CreateProfile	True	69	Biosig-ID
le@aol.com	12/25/2011 11:39:28 PM		2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	None	Enroll	CreateProfile	True	100	Click-ID
le@aol.com	12/25/2011 11:39:38 PM		2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	None	Enroll	CreateProfile	True	92	Click-ID
le@aol.com	12/25/2011 11:40:30 PM		2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	None	Enroll	CreateProfile	True	75	Click-ID
le@aol.com	12/25/2011 11:41:06 PM	292 0	2002:4834:fe19::4834:fe19	71.123.154.58	71.123.154.58: [...	Mouse	Validate	ValidateProfile	True	76	Biosig-ID

Over a 7 month period (May 2011-December 2011) 1893 students from three higher education schools and multiple classes authenticated their identity from their own computers using BioSig-ID and Click-ID software. In two schools, the students authenticated through Pearson eCollege Learning Studio and one school used the Black Board building block module. Both LMS systems were integrated with the BioSig-ID software. Test subjects were asked to enroll, create a profile and authenticate their identity at various times during their course (usually before a gradable event). The audit trails were analyzed for all activity.

In addition, data was gathered from the BioSig-ID knowledge based help desk. This help desk was available 24 x 7 for students. One school, did not have access to this help desk until October and student help desk calls before this time were received by trained BSI operators.

Enrollment

The results confirm that 100% of participants were able to enroll and validate. No student was exempted totally from authenticating their identity. Four (4) participants only requested an accessibility option allowing them to bypass the first part of the BioSig-ID authentication that required use of a device to activate (See Table 2). Two of these students had physical limitations and two students had poor touchpad responsiveness. In all four cases students were able to enroll and validate using Click-ID as the primary authentication method and also enrolled in complex security questions. IP addresses were captured for each user. Many more IP addresses were reported than

were students. If the user had a dynamic IP address protocol, each time they logged in they could be using a different IP address. In our future version we will be able to drill down more on these addresses to determine if it is the same student. For this reason, the IP trace addresses that determine if the same student uses a suspicious IP address especially during a final exam was not reported on.

Table 2

	School 1	School 2	School 3
Exemptions from using software	**0**	**0**	**0**
IP Addresses	**6306**	**211**	**133**
Accessibility option	**3**	**0**	**1**

Validations

As indicated in Table 3 over 28,178 validation attempts were made by the 1893 students. School 2 and 3 had less attempts since they were only involved in one academic session (Fall) while school one participated in both the Summer and Fall sessions. This accounts for the higher number of validations of 12.4 versus 4.6 and 4.5 respectively. Some students validated up to 40 times to test the limits of the system and we believe it was due to the intrigue/entertainment factor previously reported.

Table 3

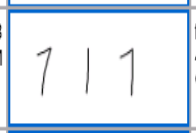
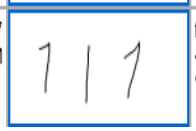
	School 1	School 2	School 3	Total	Average
Number of Students	1709	109	75	1893	
True Validations	19513	396	266	20175	
Validations per Student	11.4	3.6	3.6		
Validation Attempts (total)	26957	717	504	28178	
Validations (true)	21222	505	341	22068	
Validations per student	12.4	4.6	4.5	7.2	7.2

Testing of the software

As described in Table 4, many students spent more time in our system that was required. Previous reports suggest that nearly 45% of users found the BioSig-ID software entertaining. As described in Figure 4, this student was challenging the system.

Table 4

The user switched the order to challenge the system

ame	Time Stamp	Signature Data	Server IP	Client IP	IPTrace Route	Device	Context	Action	Success	Accuracy	App
r@gmail.com	11/3/2011 6:15:16 AM		fe80::dc1c:8b43:f1a8:3755%13	76.7.194.4	76.7.194.4:[72. ...	Mouse	Reenroll	CreateProfile	True	68	Biosig-ID
r@gmail.com	11/3/2011 6:15:25 AM		fe80::dc1c:8b43:f1a8:3755%13	76.7.194.4	76.7.194.4:[72. ...	Mouse	Reenroll	CreateProfile	True	58	Biosig-ID
r@gmail.com	11/3/2011 6:15:40 AM		fe80::dc1c:8b43:f1a8:3755%13	76.7.194.4	76.7.194.4:[72. ...	Mouse	Validate	ValidateProfile	True	90	Biosig-ID
r@gmail.com	11/8/2011 1:36:57 AM		fe80::dc1c:8b43:f1a8:3755%13	76.7.194.4	76.7.194.4:[72. ...	Mouse	Validate	ValidateProfile	False	0	Biosig-ID
r@gmail.com	11/8/2011 1:37:08 AM		fe80::dc1c:8b43:f1a8:3755%13	76.7.194.4	76.7.194.4:[72. ...	Mouse	Validate	ValidateProfile	False	0	Biosig-ID
r@gmail.com	11/8/2011 1:37:17 AM		fe80::dc1c:8b43:f1a8:3755%13	76.7.194.4	76.7.194.4:[72. ...	Mouse	Validate	ValidateProfile	False	31	Biosig-ID

In Table 5, we list the number of successful validations. These numbers represent a better consensus of reality. For example, the first attempt to validate is very consistent across all schools at 89%. This means that when the students were trying to authenticate 89% were successful on their first attempt, with another 9% successful on their second attempt. Consistent with previous data we find that approximately 2% of students require a third attempt before they are successful in validating. We cannot rule out the "gaming" of the system on purpose and it is our belief that more students will validate on their first attempt that what is indicated.

Table 5

Successful Validations	School 1	School 2	School 3
1st Attempt	18933	442	305
% 1st attempt	89%	88%	89%
2nd Attempt	1897	50	31
% 2nd attempt	9%	10%	9%
3rd Attempt	392	13	5
% 3rd Attempt	2%	3%	1%

Re-Enrolls

An important aspect of the BioSig-ID software is the ability to allow continuity. Typically, password security systems do not offer a secure continuous technology. For example, after three times of failing your password usually one of these events occurs:

- you are frozen or locked out
- you are required to call the help desk or be contacted by phone
- you agree to be sent an e-mail for a re-set

In contrast, BioSig-ID allows a self-service password re-set. The user is allowed to continue if they are able to validate using the second layer of security (Click-ID). This creates two large benefits to the institution and the user.

1. Unlike an auto e-mail and reset that does not require any validation, BioSig-ID forces the user to validate their identity before they can continue. This is a huge security improvement.
2. The seamless continuity with BioSig-ID's second layer of security allows a better user experience. This helps to explain in part why 98% of users have a positive experience with BioSig-ID.

During the period studied, 3567 net reenrolls were completed. See Table 6. School 1 and 2 were very similar at 1.8/1.9 average per student while school 3 was 3.12. School 3 however, had an entire class that did not watch the mandatory "How to use video" and this caused an abnormally high level of reenrolls. An important aspect of these numbers is the good use of the reenroll function, continuity and avoidance of help desk calls for password resets. This is very apparent when we consider the reset rates.

Resets

A reset is when the student requests a new password (see Table 6).

Table 6

School	1	2	3	
Reenrolls	3219	217	234	Totals 3670
Resets	80	0	*23	Totals *82
Net Reenrolls	3139- 1.8%	217- 1.9%	211- 2%	Totals 3567

The most common reason reported by the help desk ticket system for a re-set was forgetting what password they created with BioSig-ID or Click-ID. School one and two were using the same learning management system that during this period was not gated. Gating means that they could not advance to the next stage unless they validated their identity. This was a feature that was only changed and incorporated in mid December. The students were asked by their instructors to validate their identity at least 6 times before a gradable exam was to take place.

The students would not receive their access exam password until they successfully authenticated themselves. Some students would validate all six times within a short period (say a week) and then not again for months. At the exam, they would not remember their passwords as they had not used it in some cases for months. They would understandably ask to be reset.

School two employed a slightly different protocol and used less of the final event exams requiring their students to validate on a more consistent basis. If you do not use a password frequently it becomes very difficult to remember. The learning management system has since completed this gating and the school will also be increasing the frequency required for validations for all gradable events. School three who used a different learning management system used the gating system. If we subtracted the one class of students who all had to be reset as the instructor did not have the students watch the mandatory video the level of resets falls to 2% (similar to other schools). It is difficult to draw conclusions about this activity by itself. However, when we compare this activity combined with help desk calls to other schools we can see some major differences.

Help desk calls comparison

This is a report of the total number of help desk calls during the period May 2011 to December 22, 2011 involving the 1893 students who used BioSig-ID versus another large university who did not use BioSig-ID. There may be differences between groups, but since the BioSig-ID students were from multiple colleges and universities, of different ages, gender and backgrounds the groups may be closely representative of each other.

The following statistics are from school 4 that supports 9 full time, 4 FTE's for technical support, several managers and other support staff to total over 20 FTE's/PT's and a budget in excess of $1.5M annually, running 24x7. This university is a large 35,000 student university in Texas that logged 5747 help desk calls (3103 of these were for password resets) in an average month of a new session (data on file). We chose the 1st month of a new session to compare data. We believed it more closely resembled the introduction of new stresses to students that might create similar conditions as the students who had to register, enroll and create a new password using BioSig-ID. The students using BioSig-ID used the BioSig-ID help desk for problems. The other university used a dedicated help desk that collected very comprehensive statistics on each call. They used the Black Board Learning Management System.

When we review School 4 stats we found there was a 16.4% calls to student ratio for password resets

In contrast, BSI's overall rates were less than 3% or 607% superior. See Table 7.

Table 7

Number of calls	Accounts	# calls by school	# of students during period	Percentage of calls and LMS
	School 1	1	75	1.3% - Black Board
	School 2	4	109	3.6% - eCollege Learning Studio
	School 3	47	1709	2.7% - eCollege Learning Studio
Total		**52**	**1893**	Totals
				2.7% calls to student ratio
5747 total	**School 4 did not use BioSig-ID™**	**5747**	**35,000**	**16.4% calls to student ratio – BlackBoard user**

*Note Approx 12 calls were due to Windows IE 9 issues with new code created by Pearson eCollege requiring BSI to be a third party, so students had to allow cookies. This has subsequently been fixed. Without these calls the percentage of calls is reduced down to 2%.

Costs of help desk calls

In the commercial world the average cost per help desk call ranges from $13-$21(fully loaded) depending on the switch used and the level and location of personnel. If we use the example of a help desk call costing $15 (low commercial domestic US level) and assume that Biometric Signature ID's closed loop reduces a percentage of all calls, the total savings can be modeled as follows:

- Focusing on just their password resets (54% of their 5747 calls or 3103 calls) we could have reduced the help desk calls at School 4 by 80% (2482 calls reduction).
- Using $15/cost per call, the savings would be:
  - $37,236.00 per month or
  - $446,832.00 per year or
  - $11.28/student.

Notes: Schools may determine costs differently and savings will come from reduction in staff versus reduction in calls or reduction of fixed overhead. Regardless, reducing the number of help desk calls will be a financial benefit to the school. BSI technology can be an instrument of cost reduction to the school.

Summary

During the time period studied, the 1893 students were all able to enroll and create a password with BioSig-ID. Regardless of the learning management system used, or the school they attended, we noted no significant difference between validations, re-enrollments or resets in the student population. We also continue to notice that a significant number of students find BioSig-ID offers an entertainment or intrigue factor as many more validations were performed than required.

We reported a reset rate of less than 3% versus in school 1 versus 0% in school 2. School 3 had a revised reset rate less than 2%. The code change for schools one and two is expected to further reduce these levels as students will perform more validations with less time between authentication attempts.

To put the number of resets in perspective, we compared a large Texas -based university and their number of password calls including resets. They reported a call to student ratio of 16.4%. In our cohort of students the same ratio was less than 3%. The difference in help desk call volume would associate with a significantly better user experience in favor of BioSig-ID. This difference is also associated with a large savings in help desk costs estimated at over $11 per year per student. In some cases depending on volume pricing this savings pays for most of the cost of using BioSig-ID software or more than pays for the cost with additional net savings.

As described in Dr. Mark Sarver's foreword, the regular cost of physical proctoring at eduKan was $38/student/exam. By replacing physical proctoring with BioSig-ID the cost per students savings was $35.50 or a 93% REDUCTION. Overall, 97% of the EduKan students preferred BioSig-ID to physical proctoring and by using the BioSig-ID software to authenticate student Identity, eduKan experienced an estimated ROI greater than 400% with an 80% reduction in staff and faculty time required to administer physical proctoring. The software easily paid for itself and eduKan realized a budget gain of $159,000.

We have discussed some of the positive behavioral findings from a significant cohort of students that establish why an increasing number of schools are beginning to use the BioSig-ID technology for student ID validation to replace physical proctoring and use it to authenticate students before other gradable events or randomly. These user behavioral based findings should serve as extra or bonus reasons to use the gesture biometrics software.

BioSig-ID adds a valuable tool for student ID verification and can be used with confidence for the following reasons:

1. Compliance with the Revised Higher Education Act and regional accreditation bodies
2. Significant reduction of physical proctoring costs and a budget gain
3. To enhance a school's reputation by ensuring academic integrity
4. BioSig-ID can be used to challenge students at random, periodic times and is instructor placed
5. No extra per use charges – flat rate license fee/student/year
6. Reduction of help desk calls creates potential $ savings AND a better user experience

BioSig-ID™
The Missing Piece of Password Security
For Student ID Verification

For additional information please contact:
Jeff Maynard BSc
jeff.maynard@biosig-id.com

References

1. The Tolly Test Report, January 2011, Report # 201114, Biometric Signature ID 2.0 User Authentication Solution
2. The Tolly Test Report, August 2007, Report # 207233, BioPassword Enterprise Edition 3.2, Accuracy Evaluation of Keystroke Dynamics