

Biometric Signature ID - BioSig-ID 2.0 User Authentication Solution

Using Signature Gesture Biometrics

Ease of Use, Enrollment, Accuracy and Protection Evaluation

Executive Summary

Single-stage password security mechanisms that act as the front door to user accounts in enterprise networks are susceptible to imposters who successfully steal legitimate user ID and password data.

To strengthen user account security, Biometric Signature ID (BioSig-ID) developed the BioSig-ID solution for Windows client workstations. The solution records a signature profile of a user's mouse gestures while writing a code through an enrollment process, using that to validate the user during account logon. BioSig-ID uses a form of dynamic biometrics known as "signature/gesture dynamics."

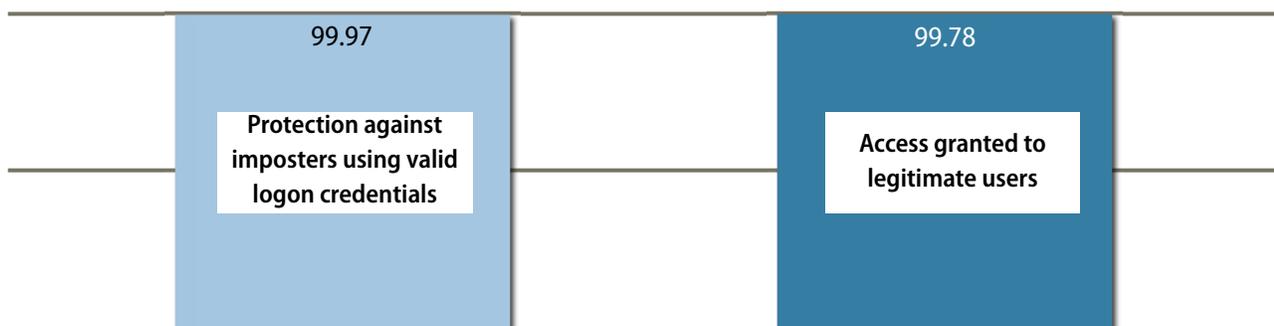
This tokenless approach creates a second layer of account logon verification and guards against the possible use of stolen password and account data to gain entry to the network.

Tolly engineers measured the effectiveness and accuracy of the BioSig-ID solution as tested with 93 test subjects accessing their own accounts and also attempting to access 20 "victim" (other user's accounts) after being supplied with the victims' credentials. Over 15,000 logon attempts were monitored during the evaluation.

The Bottom Line

- 1 Testing demonstrated that BioSig-ID, at a confidence level of 95%, protected users from 99.97% of false match logon attempts from imposters using valid user credentials, while granting access to 99.78% of valid users
- 2 Testing demonstrated that the BioSig-ID solution accuracy rates meet or exceed key industry standards for authentication such as the US electronic code of federal regulations 21 CFR 1311.116
- 3 BioSig-ID signature gesture software demonstrated high user acceptance while adding another dimension of security over a traditional user ID and password security mechanism
- 4 BioSig-ID provides a highly-scalable means of secure access, capable of delivering security and applications within the enterprise, for personal devices, PC access as well as over the Internet

Accuracy of BioSig-ID 2.0 at Detecting and Preventing Access to Imposters while Granting Access to Legitimate Users (%)



Note: Product default accuracy levels used. Imposters were provided with valid user ID and password information for the accounts each was attempting to access. In the test, 100% of the 9,488 imposter logon attempts were blocked. The false acceptance rate (FAR) of 00.03% is extrapolated from the accuracy data collected during those attempts. 100% represents best possible result.

Source: Tolly, December 2010

Figure 1



Background

Biometric Signature ID commissioned Tolly to evaluate the accuracy of its BioSig-ID version 2.0 software-based biometric authentication solution. The solution is implemented on a standard Microsoft Server environment and provides hosted security services to Windows clients. Testing was conducted in a Windows XP Professional environment using 93 test subjects who had no prior exposure to the system.

Tests aimed to show that authentication using biometric dynamics (capturing users' drawing patterns) provides a viable alternative to keystroke biometrics, hardware biometrics, token-based authentication and account credentials (user ID/password) simply and effectively without changing typical user behavior. Test results were analyzed

to determine whether the BioSig-ID dynamic biometric software would meet industry/government standards like those contained in US code of federal regulations 21 CFR 1311.116.

Tolly engineers evaluated the accuracy and effectiveness of the BioSig-ID solution in allowing legitimate users to log into their accounts while simultaneously detecting and blocking account access attempted by imposters who possessed another user's valid user ID and password.

Additionally, test subjects were surveyed for their opinions on the ease-of-use and effectiveness of the BioSig-ID solution. Testing was conducted in December 2010.

Test Results

Engineers determined that BioSig-ID was 99.97% effective at detecting and

Biometric Signature ID

BioSig-ID 2.0

Ease-of-Use, Vulnerability, and Accuracy Evaluation



Tested December 2010

guarding against unauthorized users who have used the proper logon data, attempting to gain access to network resources. Test results showed that the system granted 99.78% of legitimate users access to the system. See Figure 1.

BioSig-ID 2.0: Example of Accuracy Detection Report

User Name	Time Stamp	Signature Data	Server IP	Client IP	IPTrace Route	Context	Action	Success	Accuracy
group1user76@test.com	12/11/2010 6:42:37 PM		172.20.20.10	172.20.20.103	172.20.20.103; [...]	Enroll	CreateUser	True	0
group1user76@test.com	12/11/2010 6:44:07 PM	Mom	172.20.20.10	172.20.20.103	172.20.20.103; [...]	Enroll	CreateProfile	True	100
group1user76@test.com	12/11/2010 6:44:24 PM	Mom	172.20.20.10	172.20.20.103	172.20.20.103; [...]	Enroll	CreateProfile	False	0
group1user76@test.com	12/11/2010 6:44:42 PM	Mom	172.20.20.10	172.20.20.103	172.20.20.103; [...]	Enroll	CreateProfile	False	0

Source: Tolly, December 2010

Figure 2



False Acceptance Rate

Engineers assessed BioSig-ID's False Acceptance Rate (FAR), or the rate that a system grants access to the system to imposters. With 9,488 attempts to break in using another user's credentials created in the BioSig-ID system, there were no successful logins. In fact, the highest recorded accuracy of any attempt was 31% - much lower than the threshold accuracy required to validate successfully.

Given the existence of no False Accepts, accepted statistical usage allows the estimation of the FAR to be based on the rule of 3. As a result, with 95% statistical confidence levels, BioSig-ID's FAR was 0.0003 (0.03%), meaning it would allow fewer than 3 in 10,000 attempts of imposters possessing another user's credentials to log into the system.

Like many security tools, BioSig-ID has a number of security level settings that can be used to customized the system to

provide more, or less, rigid adherence to the biometric screening parameters. The system default mode was used for this test.

In the BioSig-ID system, each character may be written using variables of direction, order, speed, length, height, slant, number of strokes or angle.

For example, the password MOM in figure 2 appears to the human eye to be identical in all three examples. The accuracy levels of the 2nd and 3rd samples are zero because the user likely altered the order or number of strokes and the BioSig-ID software detected these subtle differences.

With traditional authentication schemes an imposter possessing valid user ID and password information can use that to access another's PC or to log in to personal or corporate accounts. With BioSig-ID, even though the imposter may know your password (i.e. MOM) the imposter would have no way of knowing

Survey Results:

As part of the evaluation subjects were asked to complete online surveys describing their experiences.

- 100% of subjects were able to enroll in the BioSig-ID software
- 98% found it easy to extremely easy to enroll in BioSig-ID
- 94% found it easy to extremely easy to validate their passwords created with BioSig-ID
- 98% found BioSig-ID easy to use
- 42% found the process entertaining
- 96% believed it was impossible to break into another's password
- 71% stated BioSig-ID gives higher protection versus passwords
- 100% reported they had a positive experience with BioSig-ID

Subjects were also asked to enroll and validate their biometrics using a portable fingerprint reader. Highlights included:

- 5% stated they were not able to enroll using the reader
- 35% said they had failure to validate
- 44% of subjects rated BioSig-ID as more convenient to use than the fingerprint reader

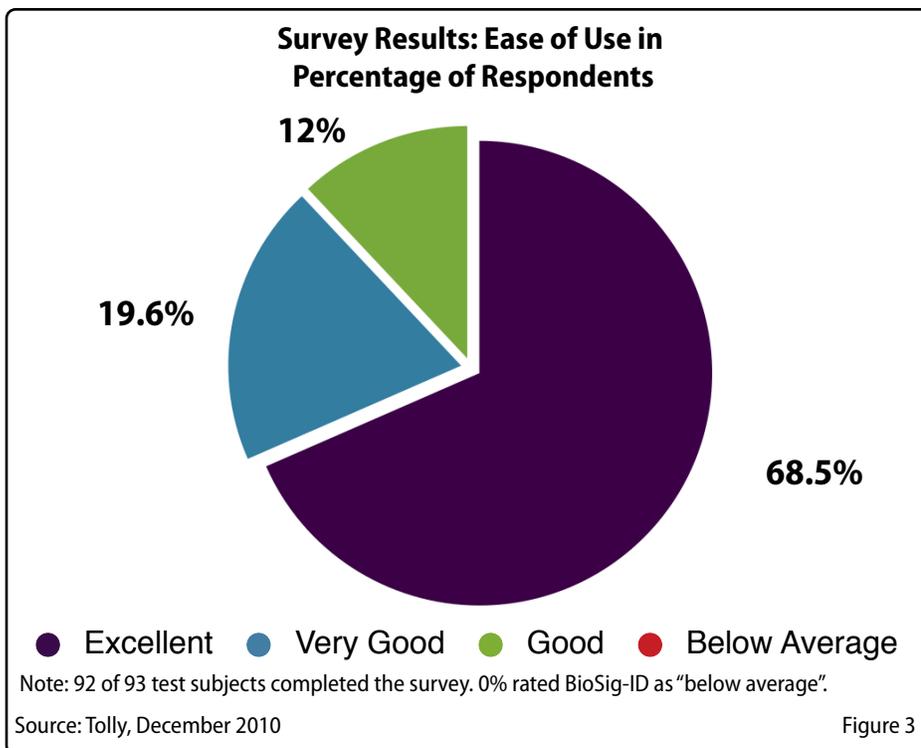
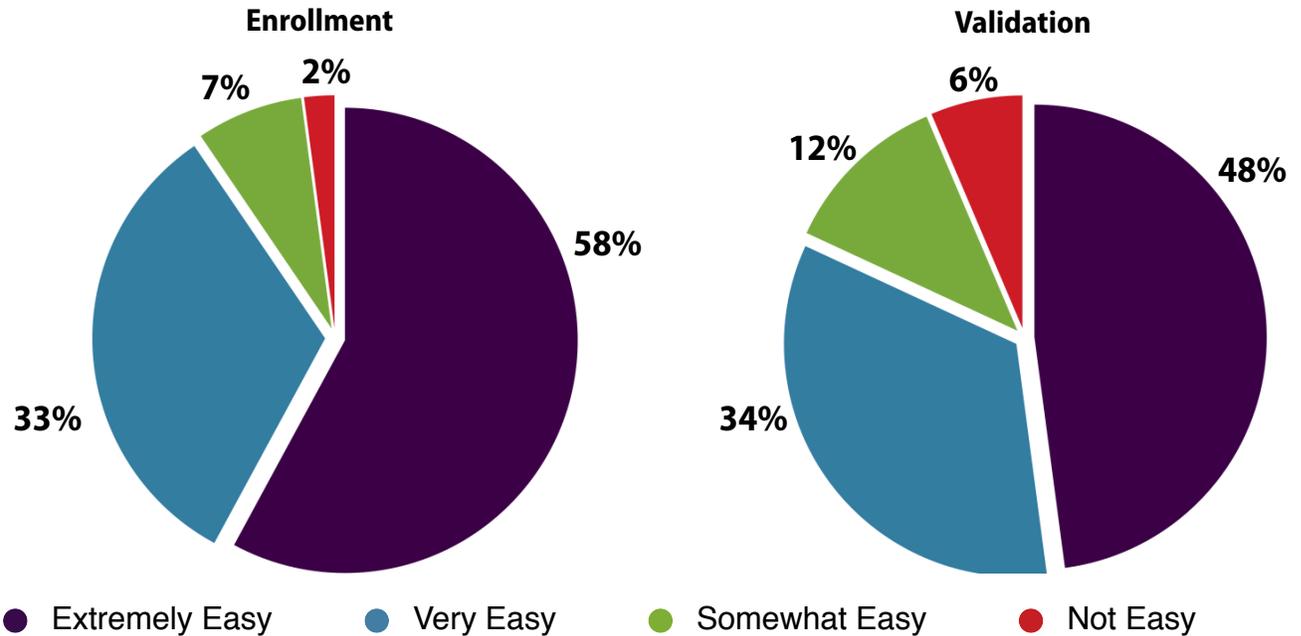


Figure 3
Source: Tolly, December 2010

Survey Results: Ease of Enrollment and Validation in Percentage of Respondents



Note: 92 of 93 test subjects completed the survey.

Source: Tolly, December 2010

Figure 4

Limitations of Password and PIN Security

PINs (personal identification numbers), security questions, tokens and traditional passwords can be compromised and used by imposters to access systems guarded by traditional security gateways.

BioSig-ID software captures the speed, # of strokes, direction, length, height, width and angle of the user’s mouse, stylus, finger or touchpad movements as you log in with a password created with BioSig-ID. These are unique and BioSig-ID can distinguish one user from all others. The user is authenticated against this previously created profile and when identity is confirmed, access to the device, files or accounts is granted. Unlike pins, passwords, tokens or security questions that only verify a person has knowledge or possesses hardware, with BioSig-ID the physical person is identified and authenticated.

BioSig-ID created passwords may appear the same to an imposter by visual inspection. But since the signature can be written out of order, on a slant, with a different number of strokes etc., the imposter has no way of determining these variables, could not duplicate the password and would not gain access. The software detects differences in the way that the password is input and can successfully differentiate between valid users and imposters.

BioSig-ID offers a tiered biometric authentication approach to provide unprecedented levels of security across a variety of hardware and software environments, requiring nothing more than a mouse and a browser.

Since signatures/characters both on paper and written with pointing devices like a mouse can change from one day to the next, the BioSig-ID software adds a learning effect. This program allows the software to adjust over time to the changes (i.e. speed, length, height, speed, etc.) the user makes without having to re-enroll.

Source: Biometric Signature-ID, January 2011

how it was written and would be denied access.

False Deny Rate

Tolly engineers measured the False Deny Rate (FDR). A "false deny" occurs when the system rejects legitimate users after six consecutive attempts to access their accounts. The FDR for the test was 00.22%, meaning BioSig-ID successfully allowed 99.78% of legitimate user attempts to gain access to their accounts. In total 14 attempts were denied out of 6,237. The software can also be configured to offer a range of security levels which can be configured to make the software more or less flexible during "signature profile" comparison.

Test Methodology

Enrollment

Over the course of a four-hour session, test subjects were introduced to the theory behind BioSig-ID with a short video presentation.

Users were then asked to enroll in BioSig-ID 2.0 and practice for 20 minutes using various combinations of characters/shapes/letters to create their personal log in password. During the practice the users could view the "accuracy" scores of each attempt and be better able to determine which combination of 3 or 4 characters they wished to use. Subjects were provided feedback on their performance by means of an accuracy score (% closeness to enrolled

profile), the majority of users demonstrated acceptable proficiency in as little as 2 minutes.

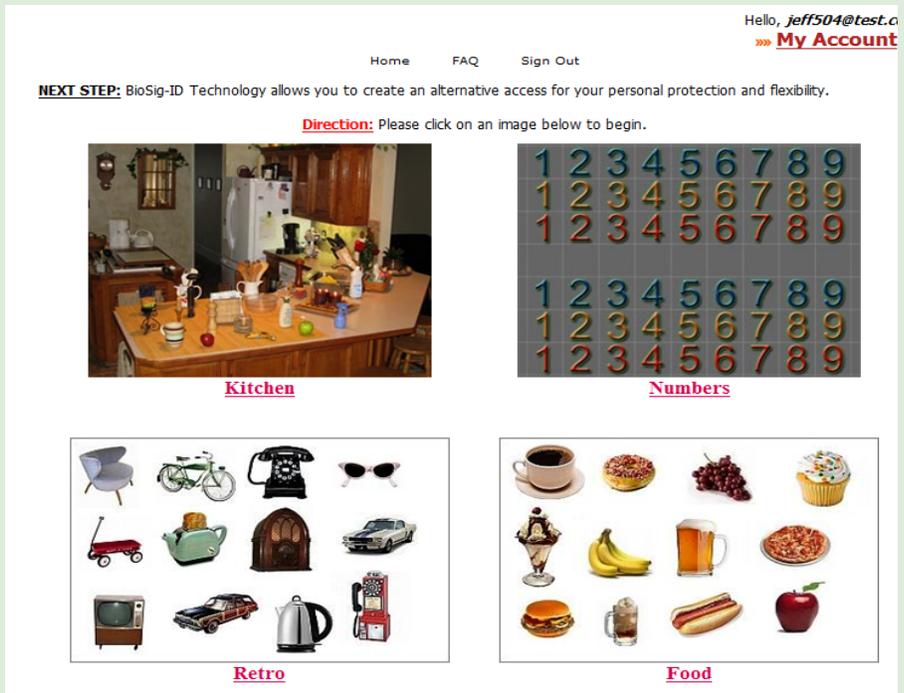
After the practice session tests subjects were asked to create their password and validate this 60 times in a row. Breaks were permitted as needed.

The BioSig-ID software requires users to enter their signature a minimum of three times to create a profile, averaging the results to account for the natural variability in our writing. Engineers observed that all users completed enrollment with 99% successfully enrolling in three of three attempts. The average enrollment time was 1.6 minutes and authentication averaged 17 seconds. (See Figure 5.)

Optional Verification Factors: Click-ID

BioSig-ID software offers optional verification factors (not tested for this report) such as human pattern recognition (Click-ID) or knowledge-based validation. The addition of these factors create a closed loop that offers a self service password reset function. This function allows the user and companies to avoid costly help desk calls and creates alternatives for users with disabilities.

Since the BioSig-ID identity authentication requires no hardware and is flash activated, its applications to create secure log ins are many including: device log ins, cloud computing, online banking, healthcare, government agencies, social networks, distance education or financial services.

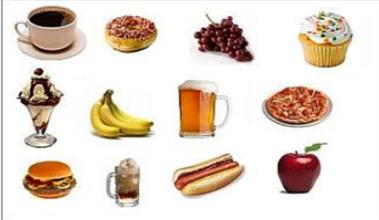


[Home](#) [FAQ](#) [Sign Out](#) Hello, [jeff504@test.c](#)
[» My Account](#)

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.

 **Kitchen**
  **Numbers**

 **Retro**
  **Food**

Source: Biometric Signature-ID, January 2011

All data was compiled using the BioSig-ID reporting tool that compiles all activity, including failure and success, time, etc.

False Deny Rate Testing

Engineers analyzed the data collected from the 93 test subjects, generating a total of 6,237 validation attempts. The test was deemed to have failed if a valid user could not gain access to the system in 6 or fewer attempts.

It should be pointed out that one test subject was responsible for 10 of the 14 failures. Upon review of her activity it became clear she did not understand the instructions.

False Acceptance Rate Testing

Subjects were given a typed sheet containing 20 user ID's and associated passwords. They were informed both verbally by staff and on the bottom of each page was a special note telling them that the passwords may not have been written as they appear (i.e. may be slanted, out of order, etc.). Users were then asked to sign in using each of 20 user ID's and attempt to gain access by validating these 20 different user profiles.

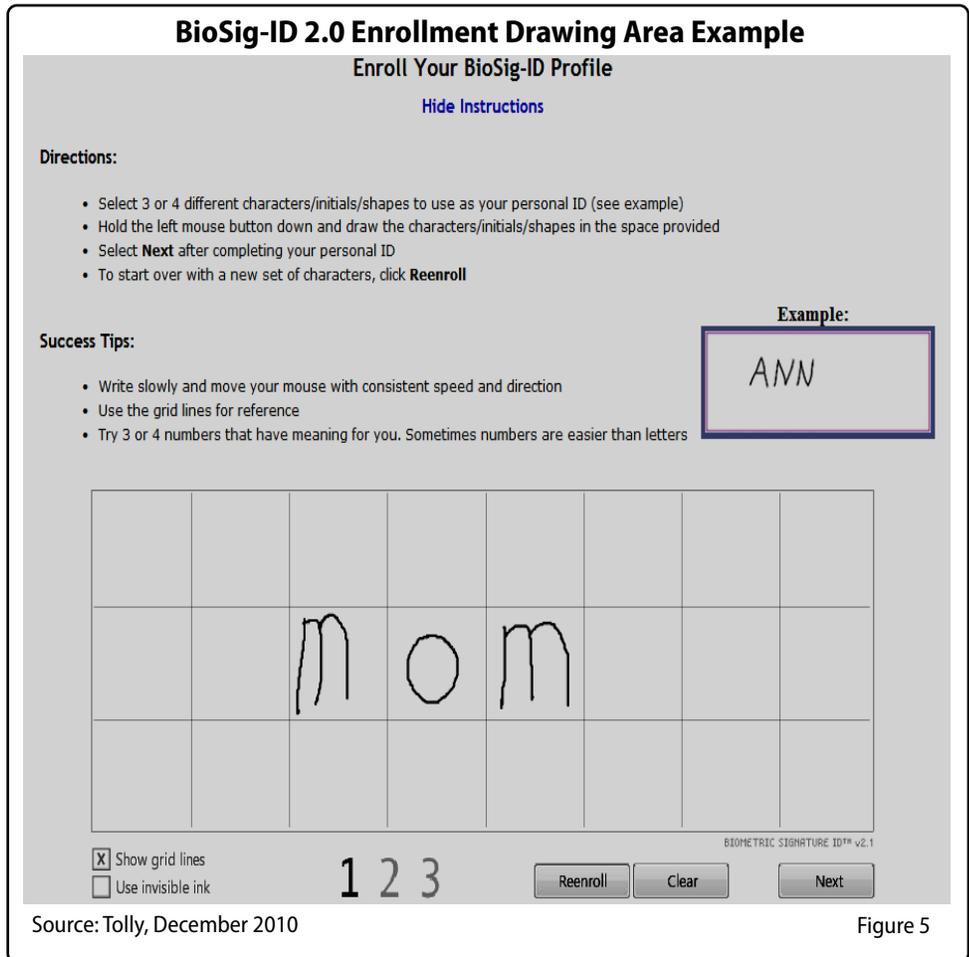
Subjects were given six attempts to falsely validate each set. If the imposter was able to validate using the supplied credentials the test was deemed to have failed.

Engineers analyzed the data collected from the 93 test subjects, generating a total of 9,488 "spoofing" attempts

Survey & Fingerprinting Experience

A prepared survey was then completed by each subject, providing insights on each subject's user experience and perceived security benefits.

Four subjects at a time were then taken to the fingerprinting lab, where they would enroll and validate with an Eikon



Upek model #E322311 "Biometric Fingerprint Identity Verification System." Test subjects were given a user ID and were then asked to enroll three fingers using a fingerprint reader, and to validate their identity 60 times. This process mimics the same process used with the BioSig-ID software.

At the end of the process, test subjects completed a survey focused on their user experience.

Test Setup

24 Windows XP stations were deployed to simulate a real-world client/server environment. BSI deployed 30 identical Microsoft Intellipoint Optical, 3-button mice to standardize testing. Twenty-six

laptops – (Toshiba Tecra M2, running at 1.6GHz, 1GB RAM, 40GB Hard drive, DVD/CD, wireless, 14" TFT screen, with Microsoft Windows XP Professional Service Pack 3) were used.

No BioSig-ID software was installed on any client as the system runs using a standard Adobe Flash browser plugin.

Clients were connected via a Fast Ethernet network to a Windows Server 2003 machine, which hosted the web page clients used to authenticate, as well as the backend processing and reporting tools required for data collection and analysis.



About Tolly...

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by e-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
<http://www.tolly.com>

About Biometric Signature ID...

BioSig-ID (BSI) has perfected a way to identify persons by the movements they make with their mouse when logging in. With increasing amounts of data being stored and accessed over the internet, making sure only the right people gain access to this data is very important. Unlike other biometrics like fingerprinting, vein or iris, BioSig-ID does not require any additional hardware or installation, giving it large cost and accessibility benefits.

BSI was awarded the "2010 New product innovation of the year award in North America for signature biometrics" and has been recognized by the State of Texas Emerging Technology Fund as breakthrough technology.

Visit us at: www.biosig-id.com or telephone at +1 972.436.6862.

Source: Biometric Signature-ID, January 2011

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.