IDesia Ltd.
7 Halamish Street
Caesarea Industrial Park
P.O.B. 3080, Israel 38900

t. +972.4.6371938
f. +972.4.6376088

www.idesiabiometrics.com

IDesia
the heart of biometrics

Technical Report - Phase II, 2004

This non confidential technical report of Idesia Ltd. presents its Bio-Dynamic Signature (**BDS™**) platform, a novel biometric identification technology which promises to revolutionize the field of biometrics. In order to understand the fundamental importance of this development, a short review of the basic science of biometrics is presented, followed by an experimental result analysis based on phase II of lab testing 2004.

Biometric identification

Biometric identification is a relatively new field of science, dealing with the determination or verification of individual identity using physiological characteristics. Biometric identification characteristics, unlike identification codes or passwords, cannot be lost or transferred and are always in possession of the individual. Ideally, it should provide the ultimate level of security. Physiological identification can be based on simple characteristics such as scars or birthmarks, height, weight, or the more complex fingerprint, facial and eye scans, or DNA analysis, or on behaviorally-mediated performance criteria such as handwriting or speech signatures.

The more unique such a characteristic is to an individual, the more effective it can be in providing certain identification. However, there are usually a number of tradeoffs in relation to certainty. DNA analysis, for example, can, except in the case of some identical twins, provide absolute identification certainty, but the necessary enrollment and identification testing procedures are somewhat invasive, technologically complex, relatively expensive, and time consuming. Furthermore, fingerprint, iris, or retinal patterns, while somewhat easier to process, are considered unfriendly, and can be vulnerable to "spoofing" attacks, which are deliberate attempts to fool the identification system; spoofing can often be done with relatively simple tools, such as a photographic image or a solid model of the static identification pattern.

The ideal biometric identification technology would be accurate and certain, because it is based on unique characteristics, non-invasive, simple to implement, rapid to run, and resistant to spoofing. IDesia's BDS™ technology meets these criteria.

IDesia Ltd.
7 Halamish Street
Caesarea Industrial Park
P.O.B. 3080, Israel 38900

t. +972.4.6371938
f. +972.4.6376088

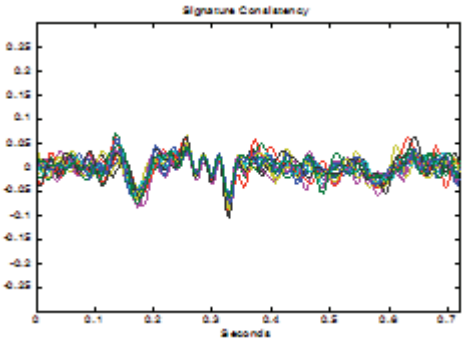
www.idesiabiometrics.com

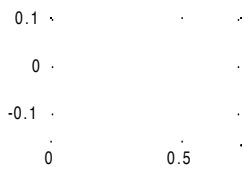
IDesia
the heart of biometrics

BDS™ Technology

The BDS technology is based on dynamic electrophysiological characteristics of the living body, primarily of the beating heart. All functioning human hearts, even those which are pathological, share numerous common characteristic features. However, IDesia's scientists determined that these gross common features obscure minute individual differences. Genetic and environmental influences in early life interact to shape fine details of the human electro signals, which are unique and consistent to every individual. Academic publications have already presented the potential of personal identification by analyzing the differences between human electro cardio signals. IDesia is the first one that invented a breakthrough method and developed the IP and algorithms to do so. The presented statistic results in this document present a superior potential over existing technologies, for better and cost effective biometrics mass market applications. On going R&D program, together with external professional labs, will soon present a commercial BDS system.

Applying its novel concept of identification and elimination of population-common features, IDesia developed a unique, inexpensive chipset sensor together with rigorous mathematical algorithms to define and identify these features, and to utilize them in biometric identification. Signature consistency is demonstrated in the graph on the right, where sixteen signatures of one individual taken at different times are presented. Signature diversity is presented below, where signatures of nine individuals are shown.





IDesia Ltd.
7 Halamish Street
Caesarea Industrial Park
P.O.B. 3080, Israel 38900

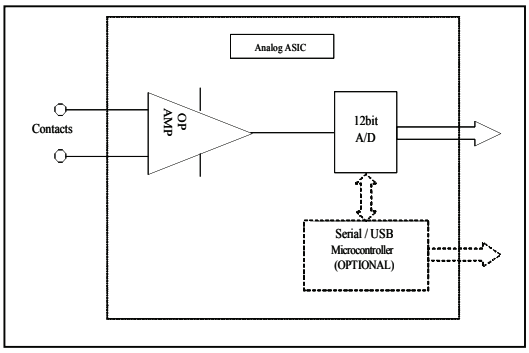
t. +972.4.6371938
f. +972.4.6376088

www.idesiabiometrics.com

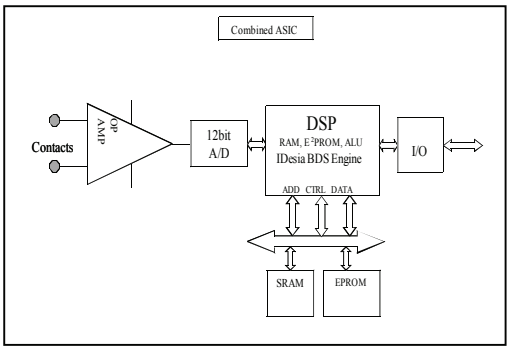
IDesia
the heart of biometrics

BDS™ Chip-Set

Based on a simple conductive sensor, the basic acquisition Sensor Chip is based on a miniaturized Analog ASIC comprised of a low gain and low frequency bio-amplifier and a signal digitizer, providing a low cost front-end solution. A Combined ASIC including both acquisition and processing hardware (ProSensor Chip) provides a complete cost-effective solution. Both models are based on proprietary know-how and are being developed in collaboration with leading IC manufacturers knowledgeable in the relevant field. A schematic representation of the two chip configurations and a basic specification for the Analog ASIC chip are shown below.



Sensor Chip (Analog ASIC)



ProSensor Chip (Combined ASIC)

Parameter	Value	Notes
Inst. Amp	*1 channel*	*Low-noise*
Supply Voltage	*±3-5V*	*USB Power*
Input Range	*2mV PTP*	*Full Scale*
Input Impedance	*1GOhm*	
BPF	*2.0 - 80 Hz*	*HP: 1st order, LP: 5th order*
Notch	*50/60Hz, -20dB*	*EUROPE/USA*
CMRR	*100dB*	
Noise	*<1uV*	*Ref. to Input*
ADC Resolution	*12bit*	
Sampling Freq	*250Hz*	
USB uC	*-*	*Optional*
Power Consumption	*<2 mW* *<0.02 mW*	*Operation* *Standby*

Analog ASIC: Technical Specification

IDesia Ltd.
7 Halamish Street
Caesarea Industrial Park
P.O.B. 3080, Israel 38900

t. +972.4.6371938
f. +972.4.6376088

www.idesiabiometrics.com

IDesia
the heart of biometrics

Proof of the BDS™ Concept

Industry Figures

There are a number of complex statistical parameters which describe the efficacy of any biometric identification system. Fortunately, the most useful are also the most intuitive.

First, a biometric system should not accept an impostor who tries to fool the system. Thus, the *False Acceptance Rate* (**FAR**) must be as small as possible. Second, a biometric system should not reject a genuine individual. Thus, the *False Rejection Rate* (**FRR**) must also be as small as possible. The intersection point of the FAR and FRR curves, is called the *Equal Error Rate* (**EER**). Ideally, both FAR and FRR should be as close to zero as possible, thus minimizing also the EER. However, current commercially available biometric identification systems usually fall significantly short of this. The accuracies of a number of different biometric technologies are given in the table below (Source: Court *Technology Library - Biometrics and the Courts*: http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html). It can be seen that iris scan leads the list, its accuracy considered the best available today with vendor reported error rates of over 1:100,000. Fingerprint, second on the accuracy list, is reported to present error rates of 1:500+. These figures represent vendor data, while real-life error rates are considered to be more conservative, in the order of 5% for commercial fingerprint systems and 1% for iris scans.

BIOMETRICS COMPARISON CHART

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors	False Pos.	False Neg.
Fingerprint	✓	✓	◎◎◎◎	▶▶▶	1 in 500+	dryness, dirt, age	Ext. Diff.	Ext. Diff.
Facial Recognition	✓	✗	◎◎◎	▶▶	No data	lighting, age, glasses, hair	Difficult	Easy
Hand Geometry	✓	✗	◎◎◎	▶▶	1 in 500	hand injury, age	Very Diff.	Medium
Speaker Recognition	✓	✗	◎◎	▶	1 in 50	noise, weather, colds	Medium	Easy
Iris Scan	✓	✓	◎◎◎◎	▶▶▶	1 in 131,000	poor lighting	Very Diff.	Very Diff.

IDesia Ltd.
7 Halamish Street
Caesarea Industrial Park
P.O.B. 3080, Israel 38900

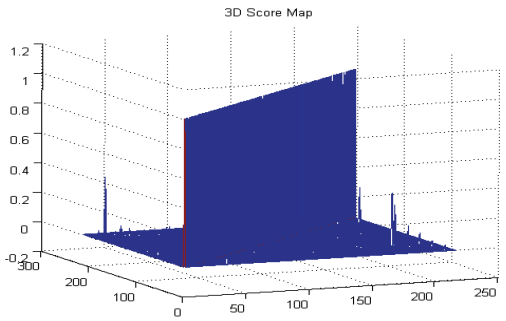
t. +972.4.6371938
f. +972.4.6376088

www.idesiabiometrics.com

IDesia
the heart of biometrics

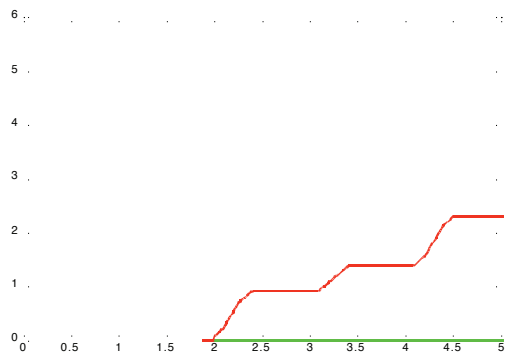
BDS™ Performance

Controlled Study



As part of its ongoing test plan, IDesia has tested over 200 subjects in its biometric laboratory. This testing provided for over 40,000 possible false matches (pairs), and some 200 possible true matches. In a controlled setting, FAR, FRR, and the resulting EER, were all found to equal zero; *that is, the BDS™ technology demonstrated perfect performance, with no false acceptances and no false rejections.* The 3D Score Map presents the match and non-match scores, where the diagonal values represent true matches and off-diagonal values present non-match scores; the true match scores present significantly higher values than the non-match scores.

False Acceptance Rate (FAR) / False Rejection Rate (FRR) Curves



FAR/FRR curves can be used to graphically illustrate system performance. With this method, tuning the decision threshold (x-axis) provides a way of describing performance by comparing False Acceptance Rates and False Rejection Rates. Performance is indicated by characteristic decline of the FAR/FRR curves as a function of the decision threshold. One objective performance descriptor is the Equal Error Rate (EER) value, obtained from the point where the two curves meet. The FAR/FRR curves of the BDS™ system, calculated from a pool of 216 subjects, present perfect performance in a controlled laboratory setting. Moreover, rather than a point intersection, the EER is obtained as a plateau between the intersections of the FAR/FRR curves with the x-axis, indicating a robust zero-error threshold region.

IDesia Ltd.
7 Halamish Street
Caesarea Industrial Park
P.O.B. 3080, Israel 38900

t. +972.4.6371938
f. +972.4.6376088

www.idesiabiometrics.com

IDesia
the heart of biometrics

The IDesia BDS™ system is unique in employing a dynamic biological signal, resistant to spoofing, as it specifies a changing signal from a living subject. Further, the system employs a comparison metric, that is, a scale of "goodness of identification", rather than a simple binary identification decision ("correct identification" vs. "imposter"), allowing tuning the sensitivity of the system as required.

BDS™: Friendly and Easy to Integrate

Once an individual is enrolled in the system, any two fingers (one of each hand) and a few seconds are all it takes to verify or determine his identity. The system itself requires only two small conductive plates, wired to miniaturized signal acquisition and processing hardware, and can easily be implemented in a compact package, or as a security add-on for popular electronic devices such as cellular phones, laptops, and memory dongles. IDesia's first product, intended for personal computer security, is illustrated here.

BDS™ Advantages

The following is a partial list of the main advantages:

- High performance – lab tests indicate FAR, FRR, EER = 0.
- Easy enrollment – simply touch the sensor plates until the system indicates enroll completion, and you are in!
- Fast database search – based on a distance metric, the signatures can be clustered to facilitate efficient data binning.
- Verification accomplished in just 2-3 seconds. Enhanced performance is time dependent.
- Spoof proof – the dynamic features of the bio-signal are much harder to simulate than any static biometric like fingerprint or iris.
- Low cost durable sensor – superior over fingerprint solutions.
- Low power – suitable for portable, battery-operated devices.
- User Friendliness – simple to use, easy to integrate, non-intrusive.

IDesia Ltd.
7 Halamish Street
Caesarea Industrial Park
P.O.B. 3080, Israel 38900

t. +972.4.6371938
f. +972.4.6376088

www.idesiabiometrics.com

BDS™ Advanced Features

The unique physiological features utilized by the BDS™ technology provide additional capabilities beyond those of conventional biometric identification systems, some of which are:

- **Multi-level security** – BDS™ unique metric provides means for presetting an application-specific security level, facilitating a multi-level security platform.

- **Spoof-proof** – Special active sensors can provide further protection against spoofing, using a proprietary biological challenge-response mechanism.

- **Enrollment Fraud** – biological features measured by the BDS™ system can prevent enrollment fraud on government/national database.

- **Additional features** of the BDS technology are confidential and can't be described in this document.