CELLMAX
A Voice Biometrics Company

WHITE PAPER

Voice Biometrics as a Natural and Cost-Effective Method of Authentication

Ziv Barzilay
CTO and Founder
CellMax Systems Ltd.

CELLMAX
A Voice Biometrics Company

WHITE PAPER: VOICE BIOMETRICS AS A NATURAL AND COST-EFFECTIVE METHOD OF AUTHENTICATION

TABLE OF CONTENTS

Overview

An influx in post-9/11 venture investment in security technologies has brought about the current quantum leap in voice biometrics. Improved next-generation voice biometrics are a user-friendly method of authentication that provide higher levels of authentication / verification and keep costs low by increasing process automation.

New voice solutions are performing far beyond current market offerings. For example, 2005 tests of a “moderately secured solution” offered by CellMax Systems using to National Institute of Standards and Technology (NIST) standards reached a False Acceptance Rate (FAR) of 170% over other market offerings, and a False Rejection Rate (FRR) of 315%, while FAR for its “highly secured solution” was in the infinite of percentages. Moreover, the newer technologies can adapt to voiceprint changes (e.g., an adolescent boy’s voice cracking or physiological changes due to injury), support input over landline, VoIP, and have even overcome cellular phone distortion.

Physical security has long been the traditional applications space for biometrics. However, data security has become of paramount importance and new regulations are coming into effect all over the world that demand three levels of identification and verification in all transactions done over networks. These higher levels must answer the question, “Is this person who he/she claims to be?” using three factors:

1. Something the person knows
2. Something the person has
3. Something the person is

Voice is the only biometric that literally answers all three. Of all the options, voice biometrics is least invasive, is the one technology that can be applied over phone lines, and is most readily available. Additionally, voice biometrics is the only technology that, aside from a microphone, requires no additional special hardware. Voice is the only biometric output that can be delivered over any type of communication network: landline or mobile phone, wired and/or unwired virtual private network (VPN), voice over IP network (VOIP), radio network and, of course, local microphone.

High rates of accuracy coupled with ease of use will, in the coming years, make voice the biometric technology of choice for identification and authentication in an ever-expanding range of both stand-alone and multi-biometric applications.

Existing Biometric Methods

The leading biometric technologies currently are:

- Fingerprint
- AFIS (Automated Fingerprint Identification System)
- Facial Recognition
- Iris Recognition
- Hand Geometry
- Voice Authentication
- Signature Verification

Voice Biometrics - Definition

Voice biometrics, meaning speaker recognition, identification and verification technologies should never be confused with speech recognition technologies.

Speech recognition technologies have the ability to recognize what a person is saying but do not recognize who the person is. Applications of speech recognition for security purposes or secure transactions are therefore limited.

By contrast, speaker recognition, verification and identification technologies can be used to ascertain if the speaker is the person he or she claims to be.

According to leading voice–based biometrics analyst J. Markowitz, Consultants:

- Speaker identification is “the process of finding and attaching a speaker identity to the voice of an unknown speaker. Automated speaker identification does this by comparing the voice with stored samples in a database of voice models.”

- Speaker verification is “the process of determining whether a person is who she/he claims to be. It entails a one-to-one comparison between a newly input voiceprint (by the claimant) and the voiceprint for the claimed identity that is stored in the system.”

CellMax Systems is both a speaker identification and speaker verification technology.

Voice Biometrics - Technical Outline

Voice biometrics differs from the other forms of biometrics as voice is a complex function created and generated by at least 15 physical parameters (see Fig. I):

1. Nasal cavity
2. Nostril
3. Lip
4. Tongue
5. Tooth
6. Oral cavity
7. Jaw
8. Trachea
9. Lungs
10. Diaphragm
11. Esophagus
12. Larynx
13. Pharyngeal cavity
14. Soft palate
15. Hard palate

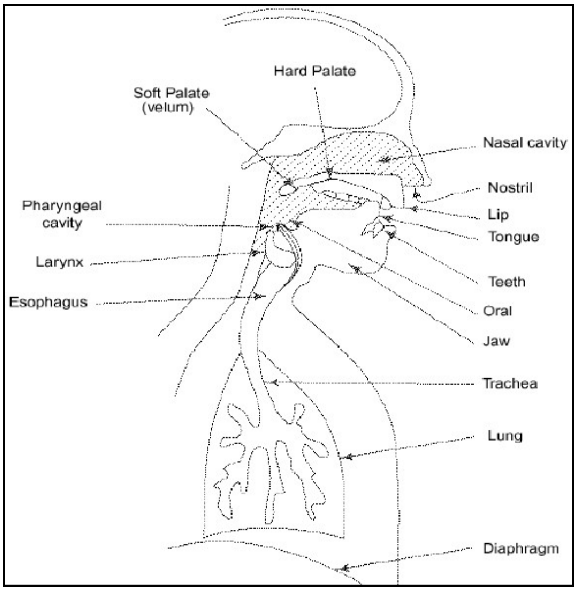


FIG I: VOICE BIOMETRICS - PHYSICAL PARAMETERS

These physical parameters are the basic constant body points that produce the sound waves of the human voice, are calculated as vectors and measured as a voice model or voiceprint.

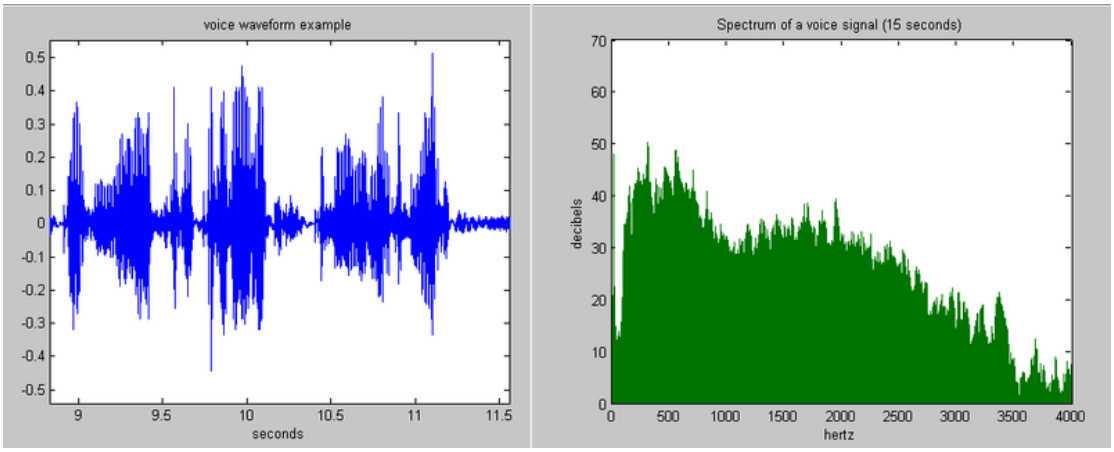


Image courtesy of Wikimedia® a registered trademark of the Wikimedia Foundation, Inc.

FIG II: VOICE BIOMETRICS – VOICE WAVEFORM AND SPECTRUM

Mathematically, sound is represented as a sequence of values, forming a temporal series. There are several techniques to extract features of time series and analyze the original sound waveform, without needing to individually analyze each point of the time series.

Voice Biometrics - Technical Outline (con't)

Like the other biometric markers, the result of a biometric measurement of the voice is totally dependant on 1. input, 2. accurate mathematical algorithms, and 3. computing power.

Input refers to the biometric sample, such as a voiceprint, taken and stored in a database.

Input quality, the most important factor, is greatly affected by the type of input device (professional microphone v. cell phone, for example) and environment (noisy street vs. quiet office). CellMax Systems technology automatically measures voice sample quality, then corrects and cleans, whenever possible, to produce the clearest possible data.

Algorithms are a set of precise steps that describe a limited procedure or task. Algorithms in biometric systems are used to find out whether a sample matches the stored input. The more precise the algorithm, the more accurate the matching process.

Levels of accuracy are measured in terms of False Acceptance Rate (FAR)/ False Rejection Rate (FRR).

- J. Markowitz Consultants defines false acceptance as "when a speaker-verification application allows an impostor to get in." False rejection is "when a verification system rejects a valid user."

- FAR refers to the probability that a biometric system will incorrectly identify a valid user, or will fail to reject an impostor. FRR refers to the probability that a biometric system will fail to identify a true enrollee.

- Real-time algorithms refer to algorithms that process information and return results so rapidly that the interaction appears to be instantaneous.

Computing refers designing system to process voice biometrics data efficiently so that individuals are quickly identified and verified, or rejected.

The voice biometrics solution developed by CellMax Systems takes as its foundation these 15 parameters that create a personal voiceprint. It then makes calculations using a proven, real-time mathematical algorithm with an unprecedented rate of accuracy: one-to-one verification that can extend beyond 99.8% and one-to-many identification of up to 98%.

Voice Biometrics - Technology

CellMax Systems utilizes a voice verification algorithm to provide an improved method and system for registering and authenticating secure, voice-based, e-commerce transactions over telecommunications networks.

The technology provides a method and system for voice registration involving three major steps:

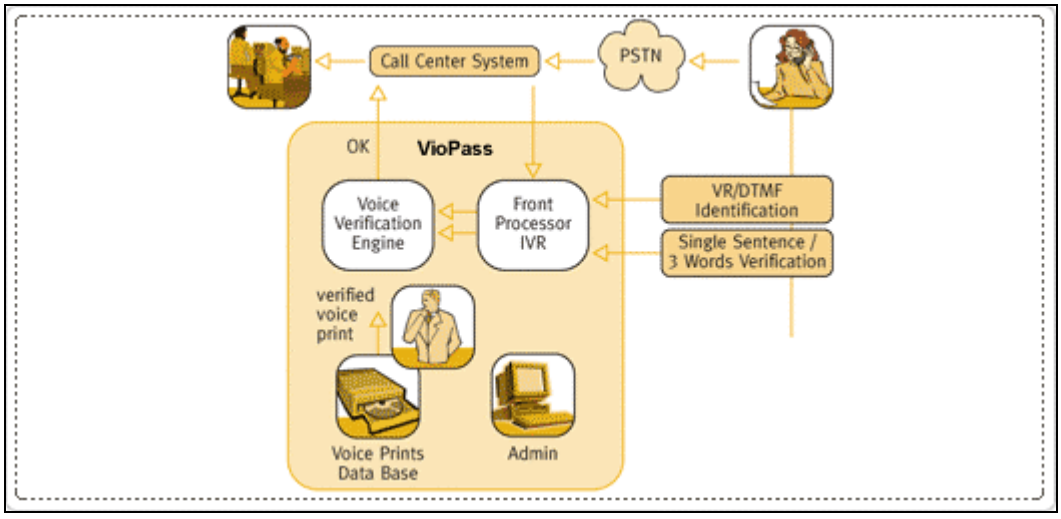
- fractal analysis
- spectrographic analysis
- determination of Lyapunov exponents (see Glossary)

The method performs fractal analysis, where raw data is investigated and each sample gives a set of non-dimensional numbers that characterize a speaker's voice uniquely.

The method also produces a vector consisting of the aforementioned 15 physical voice parameters that form the key index for the verification.

The system performs a spectrographic analysis, investigating the raw data to generate a uniquely identifiable pattern.

The system includes a voice registration unit for providing unique initial identification by finding the speaker/user's voice parameters in a voice registration sample and storing it in a database.



The system also includes a voice-authenticating unit for verifying one of a plurality of users. The voice-authenticating unit includes a recognition unit for providing a voice authentication sample that operates with the database. The voice-authenticating unit also includes a decision unit that operates with the recognition unit and the database, to decide whether the user is the same as the person of the same identity registered with the system. In this way, the user’s identity is verified absolutely.

Voice Biometrics - Applications

Given its ease of use, ability to identify individuals remotely, and high rate of accuracy, the natural target for voice biometrics are companies doing business over communications networks that are interested in preventing identity theft.

This can apply on-site or remote ID verification services such as:

- Voice & card Access Control
- Call Center - Access Control
- Branch to Branch transactions
- Internet login
- Password reset
- Home Arrest
- Secured Conference Bridge
- Forensic Application & Voice lineup
- Call Center Hidden Authentication
- Anti Terror Surveillance
- Anti Drug Surveillance
- Banking - VIP Call center
- Telecom - quality of service
- Conversational Biometrics
- Black List Warning

Voice biometrics meets new regulations designed to protect individuals from identity theft and requiring higher levels of authentication / verification. For example, by the end of 2008, US banks must provide three levels of authentication / verification in all over-network transactions. As mentioned previously, these higher levels must answer the question, “Is this person who he/she claims to be?” using three factors:

1. Something the person knows
2. Something the person has
3. Something the person is

Voice biometrics provides a three-in-one solution. Additionally, voice is the least invasive and most readily available as the only biometric that can be conveyed over phone. CellMax Systems’ open, modular platform can be flexibly applied to any existing analog or digital communications network.

Multi-biometric Applications

A new CellMax Systems invention combines the techniques of voice verification and fingerprint matching. A voice registration unit that finds voice parameters in a registration sample and stores it in a sample database, and an RF-based fingerprint registration unit finds fingerprint parameters in a registration sample and stores it in a sample database.

By combining two biometric techniques, the advantages of one overcome the shortcomings of the other, and vice-versa, as well as allow operators to control the level of security.

The result is an almost foolproof system that uses the tried and true biometric technique of fingerprint-based identification together with voice biometrics to improve verification by using both parameters, thus enabling users to obtain access to a wide range of activities and services.

Voice Biometrics - The Case For Standardization

The day is coming when voice biometrics will be part of everyday life, be it in on-site or remote situations. We will be able to call over a landline or mobile phone, laptop or PC, simply say a few words, be automatically, instantaneously processed, and our secure transaction will begin. Voice biometrics has the potential to replace the swipe ID cards, cash or tokens that get lost or stolen, personal identification (PIN) numbers that are forgotten or used by others, and fingerprint and iris scans that require special equipment.

However, industry standardization is needed to bring this vision into reality. The biometrics industry overall currently includes hundreds of separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. The voice biometrics segment alone includes dozens of hardware/software vendors.

Standards are now being formulated to provide a common software interface, allow sharing of biometric templates, and permit effective comparison and evaluation of different biometric technologies.

Actively involved standards organizations include:

- American National Standards Institute (ANSI)
- European Telecommunications Standards Institute (ETSI)
- International Standards Organization (ISO)
- International Telecommunication Union (ITU-T)
- Internet Engineering Task Force (IETF)
- World Wide Web Consortium (W3C)
- Institute of Electrical and Electronics Engineers (IEEE)

Biometric standards currently under development for voice interface include:

- Biometric Application Program Interface (BioAPI)
- Media Resource Control Protocol (MRCP)
- Voice Extensible Markup Language (VoiceXML)
- Voice Browser (W3C)

Of these, BioAPI has been cited as the one truly organic standard stemming from the BioAPI Consortium, founded by over 120 companies and organizations with a common interest in promoting the growth of the biometrics market.

In January 2007, ISO approved a new work group for standard for Voice Data File Format. Ziv Barzilay, founder and CTO of CellMax Systems and member of the Standards Institution of Israel, was chosen by the ISO / International Electrotechnical Commission (IEC) Joint Technical Committee (ISO/IEC JTC) Special Committee (SC) 37 as the editor of the "Speech Data Interchange Format for Speaker Recognition" project.

The project's goal is to create an international standard that will enable universal installation, communication and interface between all voice biometric formats.

Conclusion

In the past, voice biometrics took a back seat to other physical biometric methods of identification and verification, such as fingerprints, facial recognition and iris scans, but new algorithms and more robust computer processing power have increased accuracy rates exponentially, making voice biometrics a competitive threat to the more invasive, traditional methods of identification and verification.

In addition, new legislation for higher levels of security in commerce make voice biometrics an attractive low-cost option for enterprises now required to ask for three levels of ID to prevent identity theft and fraud in commerce and homeland security. These deadlines are imminent and non-compliance is not an option.

Moreover, the voice biometric technology developed by CellMax Systems is paving the way for voice's inclusion by international standards organizations as a physical biometric parameter.

Of the many types of highly accurate biometric technologies available today, voice biometrics is the most user-friendly and cost-effective, and next generation technologies will make voice biometrics solutions commonplace. PIN numbers can be forgotten, magnetic swipe cards may be lost or stolen and scanners require an investment in devices. By contrast, voice is the only biometric technology that enables immediate authentication any where at any time – simply by using a landline phone, mobile phone or microphone. Voice is the verifier and the person is the password.

About the Author

Ziv Barzilay is the Chief Technology Officer and Founder of voice biometrics company CellMax Systems Ltd., as well as the developer and patent-filer of CellMax Systems' innovative technology. Ziv Barzilay is a member of the Biometric Committee at the Standards Institution of Israel (SII) and the editor of the "Speech Data Interchange Format for Speaker Recognition project" of the Biometric Committee of the International Standards Organization (ISO).

About CellMax Systems

CellMax Systems is a pioneering Voice Biometrics company that specializes in highly accurate identification and verification of the human voice for access control. The company's VioMetrics product suite includes a range of ID management and security applications for the telecommunications industry and financial markets, as well as surveillance solutions for intelligence agencies. More than a password replacement tool, CellMax Systems' technology, which is patented in the US, enables cost-effective fraud prevention and thwarts identity theft, while offering smooth system integration and low-cost implementation. CellMax Systems has a growing client base of global system integrators, telecoms, commercial enterprises, banks, call centers and government agencies. Founded in 2003, CellMax Systems' headquarters and R&D facilities are located in Tel Aviv, Israel.

Glossary of Terms Used in This Article

AFIS (Automated Fingerprint Identification System) - A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications (e.g. background checks for soccer coaches, etc).

Authentication - The process of establishing confidence in the truth of some claim. The claim could be any declarative statement for example: “This individual’s name is ‘Joseph K.’ ” or “This child is more than 5 feet tall.” 2. In biometrics, “authentication” is sometimes used as a generic synonym for verification.

Authentication factor - In authentication, a factor is a piece of information used to verify a person's identity for security purposes. The three most commonly recognized factors are: 'Something you know', such as a password or PIN; 'Something you have', such as a credit card or hardware token; 'Something you are', such as a fingerprint, a retinal pattern, or other biometric. (Source: Wikipedia)

Biometric Application Program Interface (BioAPI) - The BioAPI Consortium was founded to develop a biometric Application Programming Interface (API) that brings platform and device independence to application programmers and biometric service providers. The BioAPI Consortium is a group of over 120 companies and organizations that have a common interest in promoting the growth of the biometrics market. The BioAPI Consortium developed a specification and reference implementation for a standardized API that is compatible with a wide range of biometric application programs and a broad spectrum of biometric technologies. (Source: BioAPI Consortium)

Facial Recognition - A biometric modality that uses an image of the visible physical structure of an individual’s face for recognition purposes.

False Acceptance (also: False Match) - Occurs when an individual is incorrectly matched to another individual’s existing biometric. Example: Frank claims to be John and the system verifies the claim.

False Acceptance Rate (FAR) - A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept.

False Rejection (also: False Non-Match) - Occurs when an individual is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim.

False Rejection Rate (FRR) - A statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false reject.

Fingerprint Recognition - A biometric modality that uses the physical structure of an individual’s fingerprint for recognition purposes. Important features used in most fingerprint recognition systems.

Hand Geometry Recognition - A biometric modality that uses the physical structure of an individual's hand for recognition purposes.

Identification - A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity.

International Organization for Standardization (ISO) - ISO is a network of the national standards institutes of 146 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. Although ISO standards are voluntary, the fact that they are developed in response to market demand, and are based on consensus among the interested parties, ensures widespread applicability of the standards. Consensus, like technology, evolves and ISO takes account both of evolving technology and of evolving interests by requiring a review of its standards at least every five years to decide whether they should be maintained, updated or withdrawn. In this way, ISO standards retain their position as the state of the art, as agreed by an international cross-section of experts in the field.

Iris Recognition - A biometric modality that uses an image of the physical structure of an individual's iris for recognition purposes, as illustrated below. The iris muscle is the colored portion of the eye surrounding the pupil.

JTC 1/SC 37 - Established in June 2002, ISO/IEC Joint Technical Committee 1 (JTC 1/SC 37) is the international technical committee within ISO responsible for creating and maintaining standards in biometrics. SC 37 is comprised of 26 participating countries with numerous others observing. SC 37 works in conjunction with SC 17, which is the international technical committee for cards and personal identification, and SC27 that is responsible for IT security for ISO. (Source: BioAPI Consortium)

Lyapunov exponents - One of a number of coefficients that describe the rates at which nearby trajectories in phase space converge or diverge, and that provide estimates of how long the behavior of a mechanical system is predictable before chaotic behavior sets in. (Source: McGraw-Hill Dictionary of Scientific and Technical Terms)

Media Resource Control Protocol (MRCP) – MRCP specifies a common interface to media processing resources that provide capabilities such as automatic speech recognition, speech synthesis (text-to-speech), as well as speaker verification and identification. MRCP allows client devices, such as VoiceXML browsers, to interact with these resources in a standards-based, vendor-independent manner. There are two versions of the protocol; the original MRCP (now commonly referred to as MRCP v1) draft has been superseded by the newer MRCP v2 specification, which is under active development by the Internet Engineering Task Force (IETF). (Source: The VoiceXML Forum)

Recognition - A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term "recognition" does not inherently imply the verification, closed-set identification or open-set identification (watchlist).

Retinal Recognition (also: Retinal Scan) - A biometric technique that uses the unique patterns on a person's retina to identify them. (Source: Wikipedia)

Signature Verification (also Dynamic Signature Verification or Signature Dynamics) - A behavioral biometric modality that analyzes dynamic characteristics of an individual's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.

Verification - A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

Voice Browser – A web browser that presents an interactive voice user interface to the user. In addition, it typically provides an interface to the PSTN or a PBX. Just as a visual web browser works with HTML pages, a voice browser operates on pages that specify voice dialogues. Typically these pages are written in VoiceXML, the W3C's standard voice dialog markup language, but other proprietary voice dialogue languages remain in use. (Source: Wikipedia)

Voice Recognition (also Speaker Recognition) - A biometric modality that uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes. Sometimes referred to as "voice recognition." "Speech recognition" recognizes the words being said and is not a biometric technology.

Voice Extensible Markup Language (VoiceXML) - VoiceXML is a markup language for creating voice user interfaces that use automatic speech recognition (ASR) and text-to-speech synthesis (TTS). (Source: W3C)

VXML Forum - An industry organization founded by AT&T, IBM, Lucent and Motorola to establish and promote the Voice eXtensible Markup Language (VXML). The goal of VXML is to make Internet content and information accessible via voice and phone. (Source: VoiceXML Forum)

Source: National Science & Technology Council's (NSTC) *Biometrics Glossary* unless otherwise noted.

Bibliography

Bolle, Ruud, Pankanti, Sharath, *Biometrics, Personal Identification in Networked Society*. Ed. Jain, Anil K.. Norwell, MA, Kluwer Academic Publishers, 1998.

Kohonen, Teuvo, *Self-Organizing Maps* (second ed.). Springer Verlag, Berlin, Germany, 1997.

Koolwaaij, Johan W. and Boves, Lou. *A New Procedure for Classifying Speakers in Speaker Verification Systems.* Proc. Eurospeech '97. Rhodes, Greece, 1997.

Markowitz Ph.D, Judith, *Glossary for Speaker Verification; Glossary for Speech Recognition; Glossary for Speech Analytics*. Markowitz Consultants website, 2006. <www.jmarkowitz.com>.

National Science & Technology Council's (NSTC) Subcommittee on Biometrics, *Biometrics Glossary*, 2005. <http://www.biometricscatalog.org/biometrics/GlossaryDec2005.pdf>

"Authentication factor." Wikipedia, The Free Encyclopedia. 11 December 2006, 04:47 UTC. Wikimedia Foundation, Inc. <http://en.wikipedia.org/wiki/Authentication_factor>. Information retrieved February 20, 2007.

"Retinal Scan." Wikipedia, The Free Encyclopedia 26 January 2007, 11:47 UTC. Wikimedia Foundation, Inc. <http://en.wikipedia.org/wiki/Retinal_scan>. Information retrieved February 20, 2007.

"Voice Browser." Wikipedia, The Free Encyclopedia. 3 October 2006. 03:23 UTC. Wikimedia Foundation, Inc. <http://en.wikipedia.org/wiki/Voice_browser>. Information retrieved February 20, 2007.

For further information contact:

Eran Singer
VP Sales
CellMax-Systems Ltd.
P.O. Box 58201
Building 7, Kiryat Atidim.
Tel-Aviv.
61580
Israel

Tel: 972.3.648.4223, Ext. 106
Mobile: 972.52.587.0758
E-mail: eran@cellmax-systems.com

Website: www.cellmax-systems.com.