

## Knowledge Base

### Frequently Asked Questions

We've tried to anticipate some of your questions. If you would like more information, or have questions, comments or suggestions about this section, please <<http://www.acsysbiometrics.com/contact.html>> contact us.

#### **How can biometrics be applied to security?**

Biometric security can be implemented in any situation in which there is a need to protect resources (people, money, information, facilities) from unauthorized access. Biometric security provides the ultimate in identity protection: while your ID card, personal identification number (PIN), and password can be stolen or mimicked, your face, fingerprint, retina, iris, or voice cannot. Biometric technology is being applied to airport check-in and boarding procedures, automatic banking machines (ABMs), access control, time & attendance, data co-location, PC and server security, and unobtrusive surveillance.

#### **Has the E-signature Act in the U.S. changed or accelerated the trend toward biometric security applications?**

The U.S. Electronic Signatures in Global and National Commerce Act (also known as E-Sign) will give electronic signatures (facsimiles of handwritten signatures, or recorded verbal agreements) the same standing as handwritten originals. However, the act does not specify how to secure such e-signatures. Biometric security is a natural fit.

#### **What is the size of the biometric security market currently, and what are the projections for the future?**

The Gartner Group cites biometrics as one of the top ten technologies to watch for in the next five years. The Wall Street Journal stated that the biometric market would grow to over \$1.1 billion in 2001. Biometric applications in the Internet & smart card sectors are forecast to account for over 70% of the growth.

We foresee large growth as the technology and market mature. Both Microsoft and Dell have endorsed biometric authentication. Forrester Research stated early in 2001 that it believed it would be another two to three years before biometrics came into general use. However, the events of 9/11 have accelerated the adoption rate significantly.

#### **What factors/trends do you see impacting the biometrics space in the near future?**

Public safety will continue to be a major concern and will speed the introduction of biometrics in the public and private sectors, but privacy concerns will resurface and will need to be addressed by the biometrics industry, as well as by business and government.

#### **What are the biggest barriers/drivers in the biometric market?**

Because the biometric industry is relatively young, there is a shortage of end-to-end solution



providers able to provide complete, turnkey solutions on a large scale. The technology is ready, but the solution providers are faced with a need to grow quickly to meet demand. The lack of interoperability standards may also hinder the implementation of comprehensive solutions, but the need for improved security and intelligence will drive the development of standards.

**What are some of the challenges to increasing customer acceptance of biometrics?**

Biometric vendors must establish and follow privacy guidelines, including third-party auditing where appropriate, to alleviate public concerns over the misuse of personal information.

**Where is your greatest potential market?**

Access control, data security, airport check-in and boarding security, online transaction security, IT security, time & attendance.

**What industries have the most potential for your technology?**

Any industry that has assets, data, and people to protect: in short, every industry.

**What type of potential do you see for biometrics in the financial services industry?**

Biometrics will be the "next thing" in online transaction security, and will help e-commerce develop beyond niche markets.

**Does your company have an international presence? Where are your solutions available?**

Our development facility is in the heart of Toronto, and we have sales offices in the U.S.. We have undertaken projects in the U.S. and Canada, and have numerous channel partners to assist us in deploying our solutions to large enterprises around the world.

**How does aging affect the system accuracy?**

Periodic retraining allows the system to adapt to gradual changes due to aging.

**How is AcSys FRS different from other face recognition solutions?**

AcSys FRS takes a 3-D approach to the problem of face recognition. Rather than building a template from a small number of frontal images, AcSys FRS uses a live video feed to capture facial images from numerous angles. The engram (template) that it creates from these captured images can be used to recognize the user's face from the same variety of angles. Each time the system recognizes the user, it captures additional images and updates the engram with new memories without increasing the size of the engram. As a result, the system continues to learn the user's face over time and improves its ability to recognize the user while maintaining a consistent template size – making the system scalable to enterprise requirements.

**What is HNeT?**

HNeT is an acronym for Holographic/Quantum Neural Technology. HNeT gives AcSys FRS its biomimetic capabilities. It allows AcSys FRS to emulate the brain's cognitive processes at the cellular level and learn human faces in much the same way as humans do. HNeT was developed by AND Corporation. AcSys Biometrics holds the worldwide rights to HNeT for face and voice recognition applications.

