

Battle of the Biometrics

BY C. MAXINE MOST

For nearly two decades, the Biometrics industry has been comprised of many smaller companies inventing technology and jockeying for position - hoping their technology achieves dominance. In this atmosphere of technological development, competition has been fierce and standard methods difficult to achieve. Now that biometrics are becoming real, and large scale deployment is beginning, the industry is reluctantly adjusting to its new circumstances.

Until very recently, the biometrics industry has been deeply entrenched in a fierce debate over which of the various biometric measurement technologies - face, finger, iris, hand, voice, signature - is "best". Best meaning the most accurate, reliable, secure, least intrusive and easiest to deploy, operate and use. This debate - which had sapped much of the industry's momentum - was quickly cast aside as 9/11 and the subsequent rash of terrorist acts around the world sparked unprecedented interest in biometric authentication. This new focus has forced a mass conversion among biometrics players anxious to seize the moment and it has morphed their rivalry into a somewhat tenuous industry "love fest"

Vendors now - publicly at least - endorse the notion that the choice of technology is environment and application dependent. There is no "best" biometric, just a best fit for a given set of situational constraints. In



fact, the latest push is towards multiple biometrics fused¹ together to increase the accuracy of the authentication process. This represents a radical shift in the evolution of an industry mired in the infighting typical of any early stage emerging technology market. Technology jocks

joust furiously trying to prove that the best technology (theirs) will rise triumphant out of the chaos and become the de facto standard.

Industry focus has now shifted from infighting to tackling the broader issues

¹Fusion is a technique that combines statistical results from two or more biometrics measurements to create a "fused" result that increases the overall accuracy of the authentication process. This is in contrast to a layered biometrics approach that uses the authentication results (positive or negative based on specified thresholds) for each of series of biometrics to determine identity.

What are Biometrics?

associated with large-scale government, law enforcement and commercial deployments – standards, interoperability, enrollment, privacy, centralized versus distributed database management and exception handling. In essence, vendors finding themselves suddenly in the spotlight were forced to quit squabbling and figure out how cooperate to make their technology truly useful. This has accelerated the development of technology and application standards as well as increased the commitment to resolve other outstanding issues. However, persistent barriers remain to achieving the kind of interoperability that will enable biometrics to become ubiquitous.

Many of the key players – vendors, gurus, visionaries, research scientists, bureaucrats – have been involved with biometrics for some twenty years during which time they have become extremely attached to a particular technology. So, while the recent proselytizing of multi-biometrics “coopetition” seems quite genuine and inter-biometric rivalry has subsided, infighting within specific biometric categories persists and in many cases has intensified. Rivalry is particularly strong among fingerscan suppliers where multiple sensor technologies (silicon, optical, ultrasonic), scan sizes (full, partial, sweep), and capture and matching algorithms seem to overwhelm hopes for device interoperability within this single category. This, in turn, forestalls adoption of biometrics especially for large-scale government and commercial applications where single source technology provisioning is not an acceptable option.

One bright light in terms of addressing these interoperability issues is the market entry of a new class of players – BASPs or Biometrics Applications Solutions Providers. These are organizations focused on developing biometrically

Biometrics are measurements of physical, biological or behavioral characteristics of an individual - face, finger, hand, iris, voice, signature - used to create a unique identifier which can be electronically stored, retrieved, and compared for positive identification purposes. Because they can't be lost, stolen or replicated, biometrics are an excellent alternative for replacing passwords, cards, tokens, and other forms of identification. Properly used, biometrics can increase user convenience (as compared to remembering strong passwords or carrying hardware authentication devices) while maintaining a high degree of assurance as to the identity of the person being authenticated.

Biometric technology consists of capture or scanning devices (sensors) combined with template creation and matching algorithms to create and verify the biometric information. Templates are mathematical representations of

enabled solutions, i.e. integrating biometric technology into a useful system designed to solve real world problems. Some of the existing biometric core technology vendors are trying to transform themselves into BASPs. More often, however, these are either new organizations with specific application or vertical market expertise or established solutions providers incorporating biometrics into a family of existing vertically oriented products and services. They fit in the market landscape between the core biometric technology vendors producing sensors, algorithms and devices and the larger system integrators and government contractors (See Industry Market Map). These BASPs will be integral in driving the technology towards its next phase of evolution and bringing biometrics into the mainstream.

Progress towards mainstream ubiquity will occur as convergence takes hold and individual biometric categories disappear. This will be more than just consolidation of the key players, or one technology winning out over another. Rather, an actual merging and morphing of the capture devices and the algorithms behind them will occur. Today biomet-

rics involves the capture, creation, storage and matching of mathematical representations of patterns, two-dimensional or three-dimensional, whether they be the image of a face, finger or iris, the sound of the voice or the rhythm, pressure and speed of a signature. Ultimately, capture devices and algorithms will be mostly indifferent, regardless of scale, to the nature of the type of pattern-data being captured.

Enrollment - The process whereby a user's initial biometric sample or samples are collected, assessed, processed into templates, and stored for ongoing use in a biometric system. If users are experiencing problems with a biometric system, they may need to re-enroll to gather higher quality biometric data.

Submission - The process whereby a user provides biometric samples to a biometric system. A submission may require looking in the direction of a camera, placing a finger on a reader, etc. Depending on the biometric system, a user may have to remove eyeglasses, remain still for a number of seconds, or recite a pass phrase in order to provide a biometric sample.

Over time biometric capture devices for most routine applications will become ubiquitous, cheap, reliable commodities compressed into a tiny form factor that will be embedded in everything from PDAs and PCs to POS terminals, ATMs and airport kiosks. As with most technology, these devices will blend into the landscape of modern life and become essentially invisible. Do you know who makes the hard drive in your PC? How the bank processes your pin number at an ATM? What the kiosk at the airport does with the credit card you insert to identify yourself when you check in for a flight? Convenience will rule and except for high security applications or high value transactions, where more specialized equipment may be required, biomet-

identification & authentication

rics will become utterly mundane, and the technology to process them will become virtually interchangeable. What does this mean for the battle of biometrics? In many ways, the battle will simply become irrelevant; the vast majority of the 200+ vendors in the industry will not survive the shakeout.

How do we get from the current state of this highly fragmented, chaotic marketplace to a more integrated environment? The evolution towards ubiquity will certainly not be smooth, but the needs of customers will eventually win out. Which categories will prevail? Which will fade and which may persist in spite of the move towards convergence? Which players will seize the opportunity to dominate which applications in which markets? Who are today's technology and application innovators and do they have what it takes to continue to ride the wave? And how will this market progress contribute to facilitating the evolution of digital identity management?

These questions will drive Digital ID World Magazine's on-going exploration of the biometrics market on its circuitous path from fledging technology-driven market towards full throttle enablement of the digital ID revolution. ■

C. Maxine Most is the Principal of Acuity Market Intelligence (www.acuity-mi.com), an emerging technology market research and analysis firm and the Editor of Biometrics Market Intelligence (BMI) (www.biometricsmi.com), a quarterly report providing market insight and analysis for the biometrics industry. For more information Ms. Most may be reached at cmaxmost@acuity-mi.com

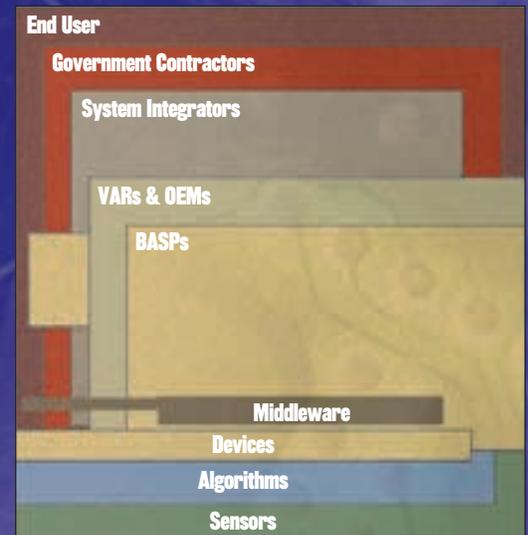
Biometrics Industry Market Map

The biometrics Industry Market Map categorizes industry players and indicates the types of relationships that will most likely develop as the marketplace matures. The relative size of each player category is an indication of the overall percentage of the total market opportunity that category represents.

The first three levels include the hardware sensors and the highly specialized hardware dependent algorithms that provide the basis for any biometric solution. As hardware price/performance curves drop and demand for algorithmic sophistication increases, the hardware portions of biometrics solutions - sensors and devices - will become commodities whereas the algorithms will be increasingly valued as a means of solution differentiation.

While middleware will become increasingly important in creating standards based interoperable solutions, ultimately this is free-ware fodder. The lion's share of industry revenues will be claimed by the organizations that focus on

solving specific end user problems - Biometrics Application Solutions Providers (BASPs), some VARs, OEMs and ultimately the organizations that will swallow the BASPs and any other promising emerging biometrics innovators: Systems Integrators and Government Contractors.



Source: Acuity Market Intelligence

Consultants though not specifically represented on the Map, they will provide specialized services to Vendors, Integrators and End-Users as the market develops.

End Users will ultimately decide the fate of biometrics. End-user acceptance will depend on the reliability and ease-of-use of biometrics systems, not just the technologies.

Government Contractors will also likely the acquisition game as proven biometrics market leaders emerge. In addition to the broad-based Integrators mentioned above, the Boeings and Lockheed's of the world ultimately fully integrate biometrics-based security into a wide range of government systems and services.

System Integrators both security focused (TYCO, RSA, CSA) and more broad-based (EDS, IBM, Raytheon) - will form strategic (and not so strategic) alliances as they integrate biometrics into larger security solutions and engage in a wait and see posture before aggressive acquisitions of biometrics companies begin. As the dominant Application Solutions Providers clearly emerge, the integrators will make their move and biometrics will become an integrated enabling technology.

VARs (Value Added Resellers) & **OEMs** (Original Equipment Manufacturers) that bring a vertical market focus to biometrics solutions will also capture market share and revenue as the industry evolves. Though may eventually be almost completely superseded as the larger players engulf the industry.

BASPs (Biometrics Application Solutions Providers) become the dominant force in the industry in the near-term creating the vertical market focus that will accelerate mainstream adoption. Solutions and support drive the lion's share of industry revenues as proven market-specific deployments then encourage buyouts by the physical and logical security behemoths and other broad based systems integrators and government contractors.

Middleware is destined to become freeware as market growth will depend on widespread adoption of standard application interfaces. As Sun Microsystems' giveaway of the Network File System (NFS) transformed the networking industry, so too must the interoperability layers of biometrics applications become standardized and interoperable.

Devices within specific categories (i.e. finger scan) become increasingly undifferentiated as the technology stabilizes. Patent protection runs out on protected technologies (i.g. iris scan) and competition works towards further leveling of the playing field

Algorithms will ultimately become the most important key differentiator of biometrics technologies. As Sensors and Devices reach technology plateaus, innovations in algorithms will enable continued overall performance improvements.

Sensors become increasingly more accurate and less expensive. In some cases, specialized sensors will be developed for high-end security applications. The bulk of sensors will be mass produced for what will become mainstream applications of biometric technology.