ePolymath.com

Trends in Biometrics Security: Heterogeneous Product Offerings and Cost Reduction

By Michelle M. Shen

Manager/Consultant

ePolymath Consulting Firm

Abstract

Demand for higher-level security solution has undoubtedly increased after September 11 Event. The biometric security industry sees a lot of new entrants and participants driven by this demand trend. From buyer side, companies are adopting multiple authentication methods to ensure a higher confidence in an individual's identity. Ease of use, low total cost of ownership, minimum user effort required, flexibility and buyer's desire of self-sufficient technology are key success factors that drive the metamorphosis of the biometric security industry. Limited IT budget, slow recovery of the macro-economic situation, previous heavy investment in IT infrastructure and compatibility with existing architectures are the key inhibitors. Biometric security industry sees its great opportunities in heterogeneous and software/platform-emphasized security and privacy solutions. It is critical for market players (sellers) to understand the value-added feature of biometric solutions and switch the focus from replacing existing authentication methods to reinforcing them. Industry consolidation and strategic partnership will definitely help to bring down the technology R&D costs and accelerate technological innovations.

CONTENTS

The information contained in this document represents the current view of ePolymath Consulting Firm on the issues discussed as of the date of publication. Because ePolymath must respond to changing market conditions, it should not be interpreted to be a commitment on the part of ePolymath, and ePolymath cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. EPOLYMATH CONSULTING FIRM MAKE NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

ePolymath Consulting Firm • 188 Doris Ave • Toronto, ON M2N6Z5• CANADA

1. INTRODUCTION

Biometric security was a $399-million-revenue industry[1] as of the year 2000, and is expected to grow to $1.9 billion by year 2005 thanks to the increasing concern about security since 9/11 and the rapid growth in Internet transaction activities. The use of biometric technology is expanding rapidly, entering an increasing number of physical security (door, buildings) and logical security (PCs, networks) applications. Fingerprint scanning continues to be the leading biometric technology in terms of market share, commanding nearly 50 percent of non-AFIS (automated fingerprint imaging system) biometric revenue.

Demand for higher-level security solution has undoubtedly increased after September 11 Event. The biometric security industry sees a lot of new entrants and participants driven by this demand trend. From buyer side, companies are adopting multiple authentication methods to ensure a higher confidence in an individual's identity. Ease of use, low total cost of ownership, minimum user effort required, flexibility and buyer's desire of self-sufficient technology are key success factors that drive the metamorphosis of the biometric security industry. Limited IT budget, slow recovery of the macro-economic situation, previous heavy investment in IT infrastructure and compatibility with existing architectures are the key inhibitors. Biometric security industry sees its great opportunities in heterogeneous and software/platform-emphasized security and privacy solutions. It is critical for market players (sellers) to understand the value-added feature of biometric solutions and switch the focus from replacing existing authentication methods to reinforcing them. Industry consolidation and strategic partnership will definitely help to bring down the technology R&D costs, technology adoption costs, and accelerate technological innovations.

E-business is still the strongest driving force behind the advanced security needs. Strong interoperability is a key enabler to help biometric vendors expand their product and service lines.

[1] International Biometric Group "Biometric Market Report 2000-2005".

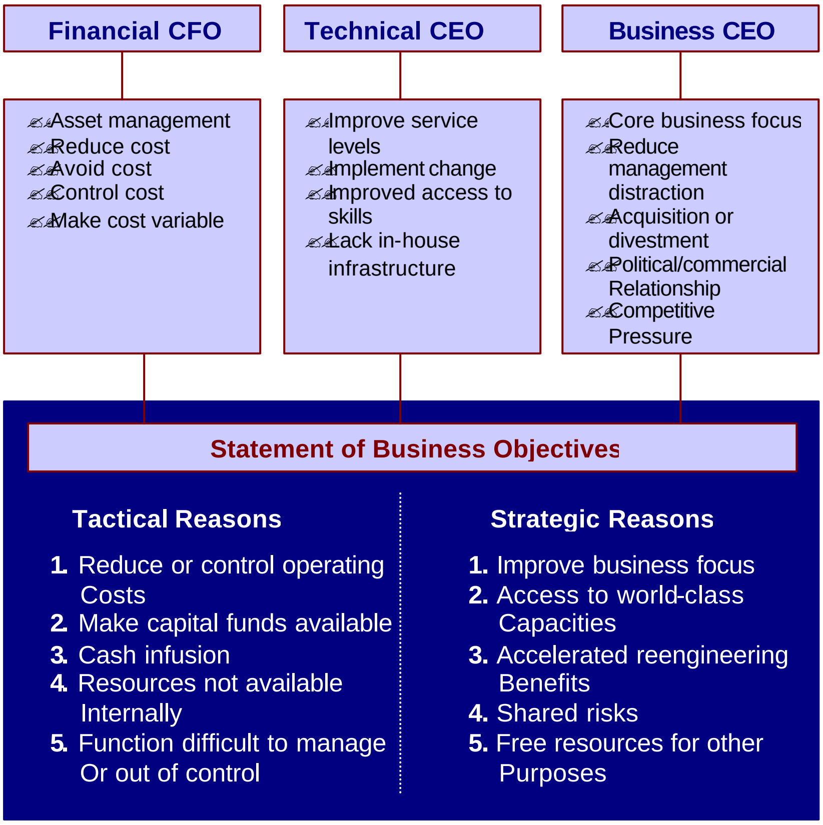
2. BIOMETRIC ASP MODEL

2.1 BACKGROUND

One of the top trends in the biometric industry is the emergence of a Biometric Service Provider model, a biometric-specialized application service provider (ASP) model. Limited IT budgets result in the reduction of total cost of ownership (TCO) from IT projects. BSPs help companies reduce the TCO of biometric security projects, as well as contribute professionalism and employee training. The BSP is the glue between heavy-investment-carrying hardware vendors and software developers as a response to the increasing demand on heterogeneous authentication methods. However, there are also issues related to the BSP model, such as companies' concerns with the loss of identity, confidentiality, and control of the technology.

2.2 REASONS TO USE BSP

CHART 1: REASONS TO USE BSP



Financial CFO

- ✍Asset management
- ✍Reduce cost
- ✍Avoid cost
- ✍Control cost
- ✍Make cost variable

Technical CEO

- ✍Improve service levels
- ✍Implement change
- ✍Improved access to skills
- ✍Lack in-house infrastructure

Business CEO

- ✍Core business focus
- ✍Reduce management distraction
- ✍Acquisition or divestment
- ✍Political/commercial Relationship
- ✍Competitive Pressure

Statement of Business Objectives

Tactical Reasons

1. Reduce or control operating Costs
2. Make capital funds available
3. Cash infusion
4. Resources not available Internally
5. Function difficult to manage Or out of control

Strategic Reasons

1. Improve business focus
2. Access to world-class Capacities
3. Accelerated reengineering Benefits
4. Shared risks
5. Free resources for other Purposes

Reference: Gartner Group, July 1998.

2. BIOMETRIC ASP MODEL

2.3 PROS AND CONS

Pros - End User's Perspectives:

- Access to best-of-breed practices
- Professionalism
- Shorter development cycle
- Cost reduction: less or no investment in infrastructure
- Cheaper solution: subscription services

Pros - Hardware Vendor's Perspectives:

- Bridge between end users and hardware vendors
- Access to larger customer base
- Flexibility and customization
- Cost reduction: BSP takes over some development
- Shorter delivery cycle due to BSP's participation

Cons - End User's Perspectives:

- Privacy and confidentiality concern
- Technology dependence, loss of control
- May need to reengineer the existing system to fit
- Look at architecture - can it be scale? can it be modified?
- Need to manage the vendor relationship
- So goes the BSP, so go you

Cons - Hardware Vendor's Perspectives:

- BSP's access to its customer base
- BSP's flexibility to choose different hardware vendors
- Hardware vendors bear more risks and heavier upfront Costs while BSP has less to lose in case of project failure

2.4 SUMMARY

BSP Model finds its great potential in SME (Small-Medium Enterprises). It's relatively difficult to have much presence in large organization due to its existing heavy infrastructure investment. An example of a successful BSP implementation is the service subscription, which means BSP provides ready-to-go solutions for end users on subscription basis. BSP will build all necessary hardware and software architecture. This way, the financial risks somewhat are transferred from end users to BSP. However, there is a lot concerns raised by end users and should be addressed effectively by BSP.

3. HETEROGENEOUS SECURITY SOLUTIONS

3.1 INTRODUCTION

The need to determine who individuals are and the functions they are permitted to perform has become paramount. The security solution providers should focus on developing biometrics technology that reinforces but not replaces current authentication methods such as passwords.

End users are adopting multiple authentication methods, including both biometric hardware and software solutions, to ensure a higher-level security environment.

Biometrics and other hardware authentication technologies will bridge the current gap between physical and network access. The ability to ensure that only authorized individuals can enter a building, visit restricted departments, and utilize networked resources will be critical to reducing security threats.

3.2 EXAMPLE: FINGERPRINT SMARTCARD SOLUTION

Fingerprint-scan technology adds an additional security layer to a smart card system. Integrating a fingerprint scanner into a smart card reader increases security by adding “something-you-are” to the authentication process, while smart cards provide the “something-you-have” factor. The highest security level, according to the Smart Card Alliance, would be adding “something-you-know,” which is the password factor, in addition to a biometric smart card solution. Integrating a fingerprint-scan sensor with a smart card reader adds to the privacy and security of authentication, and the scanned fingerprint can be directly matched with the stored templates in the smart card. This process is called match on card. The fingerprint-scan biometric smart card solution is a perfect combination of allowing authenticated and authorized information access.

The match on card technology offers higher-level security solution by securing the “source” of the security (fingerprint templates). Advantages also include:

- No external process or data link in order to access the template,
- Device may be networked together directly and share templates

across the network.

A typical heterogeneous security solution is Single Sign-On (SSO) solution, which includes authentication methods like passwords, tokens, smart & proximity cards, and of course, biometrics.

3.3 SUMMARY

The increasing demand on heterogeneous security solutions require biometric vendors's ability to develop interoperatable, compatible and flexible biometric solutions. Fat architectures and diversed vendor supplies result in heavy costs of end users. End users are looking for a sole or few numbers of vendors that can meet all their security, authentication and privacy needs.

Strategic alliance and complementary partnership can lead biometric vendors to more effectively provide heterogeneous security solutions and reach larger customer base. For example, in year 2000, when Identix annouced that its electronic fingerprint-identification technology would be integrated into Microsoft's new Windows 2000 operating system, the small firm's shares doubled in Nasdaq within two weeks.

As from the buyer side, potential is growing in technology outsourcing and third-party consultancy involvement in SMB (Small-Medium Business). These companies are looking for more cost-effective security solutions without investing too much and not at all in infrastructure.

In larger organizations, ongoing merger and acquisition have resulted in companies with many legacy systems to manage. Challenge to biometric vendors is how to integrate biometric functionality into these back-end systems. Again, convenience to use, ease of installation, and user friendly desktop interface are some key enablers. Speaking technical features, interoperability, integrability, reliability and serviceabilty are some key differentiators that will help biometric vendors expand their market presence and increase the market share.

4. BUYER BEHAVIOR ANALYSIS

4.1 EXISTING SECURITY OFFERINGS

Existing authentication and security methods include security software and hardware. The following table will give you a brief idea of the existing security software and hardware offerings and their technical features.

TABLE 1: SOFTWARE AND HARDWARE SECURITY

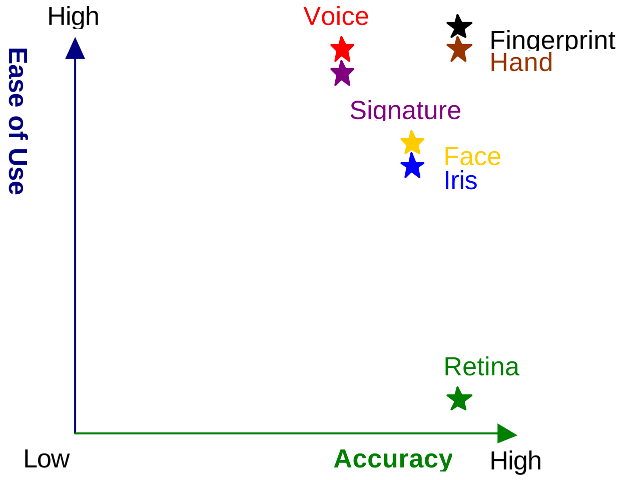
Security Software	Features
Security 3As	-Authorization software: Determine the resource access in conjunction with business policy. -Authentication software: Is used for verifying users' identities and avoiding repudiation. -Administration software: Security management solutions that focus on increasing end-user productivity, reducing administrator errors, providing management of various security technologies from a single point of control.
Firewalls	Software that identifies and blocks access to certain applications and data. These products may also include VPN encryption as an option.
Antivirus software	Identifies or eliminates harmful software And macros.
Encryption	Uses cryptographical mathematical algorithms to protect the confidentiality of data, applications, and users' identities.
Security Hardware	**Features**
Biometrics **Token and smart card**	Please refer to Table 3. Token yields a one-time password or uses a challenge-and-reply method.
Firewall/VPN appliances	A single-board computer with a hardened operating system (OS) and a limited applications set.
Cryptographic acceleration	Includes cryptographic chips, acceleration boards for SSL, acceleration boards for VPN, devices for acceleration and security of public-key operations, and standalone SSL appliances.
Standalone VPN appliances	Usually an IP VPN.
IDS appliances	A combination of hardware, software, and networking technologies. Their primary function is intrusion detection.

Reference: IDC Report – IT Security Software, Hardware and Services Forecast and Analysis, 2001-2005.

4. BUYER BEHAVIOR ANALYSIS

Among all the security hardware, biometrics security counted for 5.5% market share as of year 2001, and slightly improved to 5.8% in year 2002. Companies will adopt biometrics hardware and software solutions as one of multiple authentication methods used. The following diagram shows the performance (ease-of-use versus accuracy) matrix by biometric technologies.

DIAGRAM 1: PERFORMANCE MATRIX
BY BIOMETRIC TECHNOLOGIES



Biometric technologies will continue to improve, becoming even more accurate and reliable as technology evolves. The growing interest in the combined usage of biometrics and smart cards as well as heterogeneous security solutions should also cause an increased growth path for both technologies in the futures. Hopefully in the near future, standards will be available which allow multiple reader technologies from various manufacturers to be utilized within the same system.

4.2 BUYER'S NEEDS ANALYSIS

✍ **Convenience to use**

Based on a security technology adoption survey conducted by IDC, only 0.6% of the North American companies claim that they are currently using biometrics as one of their Internet and network secuirty technologies. One of the main inhibitors is the inconvenience of use. As a rule of thumb, security is usually the inverse of convenience. Companies need easy to use, intuitively designed biometric solutions to reinforce their security systems.

- **Minimum user knowledge and effort**

  User training and education contributes to over 30% of an advanced security technology rollout. A biometric solution with minimum user knowledge and effort would be very welcomed by purchase decision makers. All that end users care about is the desktop functionality and friendly desktop interface.

- **Fast delivery and installation**

  Companies want technology that delivers. Biometric solutions might intimidate some companies as they are not familiar with the technologies. A lot of companies do not carry the expertise to implement a biometric system. They need biometric solutions that can be fast delivered and easily installed.

- **Compatibility with existing infrastructure or network systems**

  Incompatibility with companies' existing network systems means additional deployment costs. Previous infrastructure investment has more or less killed most companies' IT budget. Companies need biometric solutions that are ready to be deployed with minimum in-house development work.

- **Interoperability with other IT security solutions**

  More and more companies tend to adopt multiple/complementary security solutions. Whether or not the biometric solutions are interoperable with other security/authentication solutions is one of the key successor factors that lead to companies' purchase decisions.

- **Technology that can turn "Cost Center" into a "Profit Center"**

  IT department is long known as a cost center to the company. Not quite. Consider an advanced technology adoption that can lead to cost savings from human resources and process engineering, and therefore results in a remarkable technology contribution to profits. Companies' IT decision makers need this type of biometric technologies to justify their decision, to show a tangible return on investment from the biometric solutions.

4. BUYER BEHAVIOR ANALYSIS

4.3 BENEFITS AND RISKS ANALYSIS

Before implementing a biometric solution, a lot of companies want to know what benefits will the solution bring to their organizations, and what potential risks will be. Here are some perceived benefits and risks from potential buyers.

Benefits:

✍ **Increased Security**

1. Biometric information cannot be lost, stolen, or forgotten; it cannot be written down or discovered by social engineering; it cannot be shared with other users, so reducing abuse; and it cannot, without duress, be used by anyone other than the individual.
2. By installing biometrics, companies can positively verify users' identities, improving personal accountability (positive identification of users in audit trails) and allowing high-value transactions to be offered at remote terminals and over the Internet.
3. In conjunction with smart cards, biometrics can provide strong security for PKI credentials held on the cards, thus providing greater trust in PKI services, especially digital signatures for non-repudiation.

✍ **Increased Convenience**

1. A user is not required to present a card or remember a password or PIN. Since biometric information cannot be lost, stolen or forgotten, it is always available to the individual.
2. Organizations can implement recognition systems rather than simple authentication systems, so users no longer have to manually log on to information systems.

✍ **Reduced Costs**

1. Organizations can eliminate the overheads of password management, including up to 40 percent of help desk calls for password resets, and so improve customer service. (Details please refer to Michelle Shen's publication "A Financial Snapshot of Biometric Smart Card Solution".

Risks:

✍ **Privacy Concerns**

1. If an organization holds a central repository of templates, users

4. BUYER BEHAVIOR ANALYSIS

have no control control over the distribution of this data and are wary of:

1) Misuse of the data
2) Use for purposes other than the purpose for which it was originally collected

2. Other privacy concerns include fears about the ability to search records about a person and monitor in the real time.

✍ **Personal and Religious Concerns**

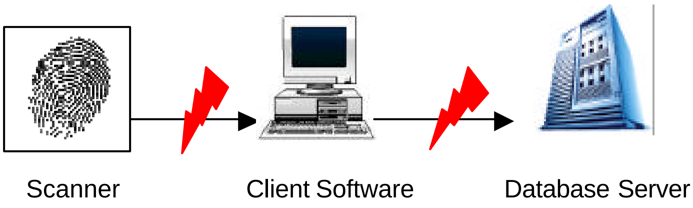
1. Concerns over hygiene and the possibility of actual harm (e.g., with retina systems where light is shone into the eye)
2. Some cultural and religious taboos can inhibit the use of biometrics systems.

✍ **Suitability for All Users**

1. Between 1% to 3% of the general public does not have the body part required for mapping any one biometric.
2. Biometrics can therefore be perceived as “Socially Regressive” in that it excludes the disabled and the old.

✍ **If Compromised, a Biometric Cannot be Reissued**

1. Biometrics is vulnerable to some kinds of capture and reply attacks. The following chart illustrates the possible holes.



2. A biometric trait is “issued” for life, the data must be protected \ against attacks for the next 30 years or more, which requires longer-key and more dynamic encryption credentials to protect the biometric templates.

✍ **Biometric Systems Are Still Not Foolproof**

1. Submission of a facsimile or recording of an enrollee’s biometric.
2. Submission of a latent image on a fingerprint sensor.
3. Electronic attacks, such as the transmission of a reference template, replay of a captured trial template, or replay of a captured sample to recreate a new trial template.

Reference: Gartner Research “Biometric Authentication: Technology Overview”, July 19, 2002.

4.4 SUMMARY AND RECOMMENDATIONS TO BIOMETRIC VENDORS

Whether or not biometric vendors can foster the buyers' perceived benefits, address their concerns and overcome the risks is the key success factor to a sustained growth of the market share.

One common problem with biometric market new entrants is that they do not study the market before they enter. Biometrics is such a glorified industry that it attracts professionals from various industries to start up their own business, hoping to grab some market share before the overall market gets mature. They do not have a targeted market segment where they can sell their products and services to on a sustainable basis. It is true that these biometric vendors have great products and services on the way. They are able to get some venture capital funding to start up, or even worse, to get money out of their own pocket to support their new product prototyping and design. A typical new biometric product development cycle takes at least 6 months. Yet there are many market new entrants every day as the market is still growing and fresh. By the time their final products are ready to market, they have already lost the market share or a better chance of market expansion.

The situation might remind us of the "Dot-Com Era". The biometric technologies can never be hotter and fancier after the tragic 911 event. Biometric vendors can avoid the "bubble" by properly addressing the potential risks of implementing a biometric solution. For example, a biometric smart card solution addresses the privacy concern by protecting the "source" of the security, as well as controls and authenticates access to certain system resources. Biometric tycoon SecuGen's fingerprint-scan systems overcome the threat of "gummy finger" by adding more characteristics such as temperature, pulse and transparency to its hardware and software design. These are good examples that how biometric vendors should properly response to users' concerns. There are also some failed cases such as unnecessary value-added security solution like a portable fingerprint pill case (what about you lose the case at all?). These biometric vendors are pushed out of the market right away, or are killed before they even enter the market.

5. VENDOR MARKET ANALYSIS

5.1 SERVICE AND PRODUCT OFFERINGS

The following table illustrates the current horizontal and vertical markets of the biometric technologies, and the biometric technology applications in each vertical market.

TABLE 2: BIOMETRIC VERTICAL AND HORIZONTAL MARKETS OVERVIEW AND TECHNOLOGY APPLICATIONS

Vertical Horizon tal	Law Enforcement	Government	Financial	Health care	Travel and Immigration
Physical Biometrics					
Iris	Corrections	N/A	Same as fingerprint	Kiosk-based authentication	Airport (allow hands-free)
Fingerprint	Corrections	Desktop, card-based ID solutions, Info system access (e-gov)	Account access, ATMs, Service kiosks, Online banking, Access to PCs and networks, Physical access	Access to data on PCs and networks, Desktop applications, Secure remote access	1:N functionality for immigration, Airport security, Physical access
Face	Surveillance Police, Mug shots	Image-based ID systems	Same as fingerprint	Kiosk-based	Airport security, Physical access
Hand	Kiosk-based probationary offenders' identification	N/A	Same as fingerprint	Kiosk-based	Same as fingerprint
Retina	N/A	N/A	Same as fingerprint	N/A	N/A
Behavioral Biometrics					
Signature	Tablet-based system	Tablet-based system	Same as fingerprint	N/A	N/A
Voice	Probation, Home Arrest	Physical access	Same as fingerprint	N/A	N/A
Emerging Biometrics					
Keystroke Analysis	N/A	N/A	N/A	N/A	N/A
Smart Cards	N/A	Combined with fingerprint as card-based ID solution	Combined with fingerprint as card-based ID solution	Combined with fingerprint as card-based ID solution	Combined with fingerprint as card-based ID solution

5. VENDOR MARKET ANALYSIS

5.2 TRENDS ANALYSIS

Whether or not biometric vendors can foster the buyers’ perceived benefits, address their concerns and overcome the risks is the key success factor to a sustained growth of the market share.

One common problem with biometric market new entrants is that they do not study the market before they enter. Biometrics is such a glorified industry that it attracts professionals from various industries to start up their own business, hoping to grab some market share before the overall market gets mature. They do not have a targeted market segment where they can sell their products and services to on a sustainable basis. It is true that these biometric vendors have great products and services on the way. They are able to get some venture capital funding to start up, or even worse, to get money out of their own pocket to support their new product prototyping and design. A typical new biometric product development cycle takes at least 6 months. Yet there are many market new entrants every day as the market is still growing and fresh. By the time their final products are ready to market, they have already lost the market share or a better chance of market expansion.

The situation might remind us of the “Dot-Com Era”. The biometric technologies can never be hotter and fancier after the tragic 911 event. Biometric vendors can avoid the “bubble” by properly addressing the potential risks of implementing a biometric solution. For example, a biometric smart card solution addresses the privacy concern by protecting the “source” of the security, as well as controls and authenticates access to certain system resources. Biometric tycoon SecuGen’s fingerprint-scan systems overcome the threat of “gummy finger” by adding more characteristics such as temperature, pulse and transparency to its hardware and software design. These are good examples that how biometric vendors should properly response to users’ concerns. There are also some failed cases such as unnecessary value-added security solution like a portable fingerprint pill case (what about you lose the case at all?). These biometric vendors are pushed out of the market right away, or are killed before they even enter the market.