

Challenges of Biometric Integration



Application developers, integrators and software solution providers are challenged with growing demand for biometric security features and functions.

With a wide variety of integration options available, software providers need a clear picture of the implications and impact biometric solutions have on their products, services, and customers.

Summary:

- Business Value
- Biometric Business Challenges
- Solution Descriptions
- Development Implications
- Integration Differentiators
- Technical Specifications

Overview

Biometric authentication components are emerging as an essential part of comprehensive business software applications and will play a central role in existing and future applications, networks, and information storage facilities. These biometric components utilize physical traits or behavioral characteristics for reliable identity authentication. Application developers, integrators and software solution providers are challenged with growing demand for biometric security features and functions. With a wide variety of biometric component integration options available, software providers need a clear picture of the business implications and development impact biometric solutions have on their products, services, and end-users.

Of the different types of biometric authentication (fingerprint verification, hand geometry, voice recognition, retinal scanning, iris scanning, signature verification, facial recognition), fingerprint recognition is the most mature biometric technology. It is suitable for a large number of recognition applications, and has been adopted by numerous government agencies, corporate enterprises and private institutions.

“Frost & Sullivan research indicates biometric authentication removes security loopholes in network software applications, facilitate faster, simplified, accurate, and non-intrusive authentication procedures, increases productivity, and provides an audit trail that cannot be repudiated.”

Biometric Value

Software developers, application integrators, solution vendors, and end-users recognize biometric authentication as an important aspect of their business and operational strategy, and are quickly forming a clearer understanding of the economic value biometrics provide. The key to identifying the value of biometric integration begins with identifying your business and the value to you and your clients.

Developer : Integrator : Vendor

- » Provide value to clients with security sensitivity
- » Competitive market differentiator
- » Enhance application solutions portfolio
- » Develop new marketing opportunities
- » Create new revenue stream

Enterprise : Client : End-User

- » Speed and optimize business processes
- » Reduce IT support and increase productivity
- » Safeguard company/personal assets
- » Insurance against liability
- » Compliance with Federal data regulations
- » Tighten internal controls and accountability
- » Protection of intellectual property and knowledge assets
- » Improve profitability and productivity
- » Reliable audit capabilities

Business Challenges

The value of biometric authentication may differ from developer and integrator to enterprise and end-user, but the business challenges are generally very similar. The return on investment (ROI), adoption process, and ease (and cost) of development (or integration) are at the core of these business challenges. Biometric software vendors and integrators are challenged to quantify benefits, ROI, and cost savings internally and to their clients.

Return on Investment

For a VAR or integrator, selling biometrics is no different than selling any other product - focus on the technology's ROI. For example, biometrics are ideal for increasing security when using technology that accesses confidential records (i.e., patient records, financial records) from a network. In another example, in time and attendance applications, eliminating "buddy punching" (payroll savings) is the obvious ROI. Biometric authentication typically presents definable ROI across a wide variety of applications.

At the enterprise/end-user level, data accuracy, elimination of manual entries and printed cards, and the added integrity of biometric records dramatically increase the confidence that the correct employees are on site. ROI can be realized in reduced supervisory and monitoring time and improve the employee-supervisor relationship. It's estimated that 1% to 5% of payroll can be cut with the use of biometric time and attendance readers.

Adoption Process

The direct and indirect integration and implementation costs for vendors and end-users are critical to the adoption process. While internal development of biometric components with the help of SDK's may seem logical, vendors and integrators should be apprehensive of this approach. Knowledge acquisition, testing, compatibility and maintenance of biometric components are unique, and costs can meet or exceed those of the application biometric authentication is being integrated into.

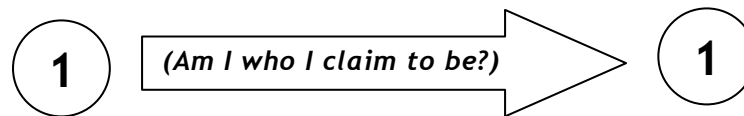
Ease and Cost of Development (or Integration)

While cost savings, ROI, and enhanced security are immediate benefits of biometric authentication for end-users, software developers and application providers in most cases continue to struggle with integration and implementation. Substantial amounts of time, capital investment and development resources are required to make integration of biometrics work with most applications - the technology is changing quickly enough that there's a good chance improvements will be available by the time the initial integration is complete if developed internally.

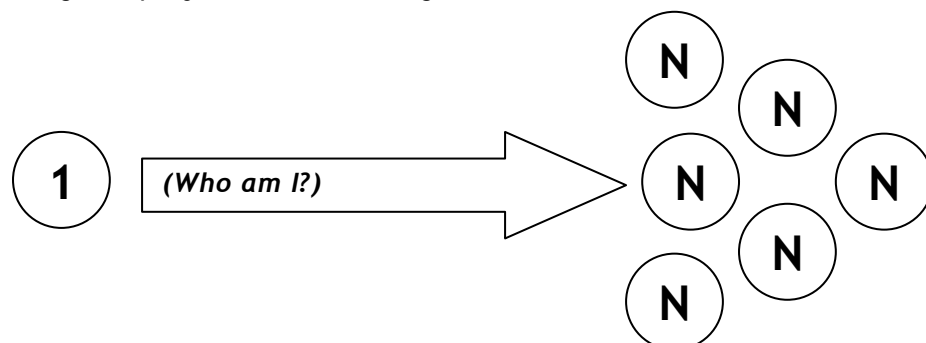
The more logical solution for application developers and integrators is to build long-term relationships with biometric technology development companies that manage the biometric component entirely - which ensures your resources are focused on their core competencies and your core business. Depending on the application context, a biometric system may be called either a verification system or an identification system.

Solution Descriptions

A **verification system** authenticates a person's identity by comparing a captured biometric characteristic (fingerprint) with a biometric template pre-stored in a system database. It conducts a one-to-one (1:1) comparison to determine whether the identity claimed by the individual is true. A verification system simply rejects or accepts the submitted claim of identity based on this comparison. (Deployment Examples: verifying a financial transaction, receiving prescription medication, accessing an online secure data source, employee entry/exit tracking)



An **identification system** recognizes an individual by searching the entire biometric template database for a match. This sophisticated system conducts a one-to-many (1:N) comparison to establish the identity of the individual. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity as the verification system requires. (Deployment Examples: front counter check-in, HIPAA patient ID regulation compliance, detention center inmate booking, employee time tracking)



Integration Differentiators

The methodology of implementing a biometric solution is most directly related to, and most often determines, the amount of capital resources required for integration, impact on long-term revenue, and ultimate end-value for the client. Application developers and integrators have **two choices** when implementing and integrating a biometric system:

Software Development Kit (SDK)

System dependencies between the host application and the SDK complicate integration and require deep knowledge of biometric system processes. Additionally, developers should be prepared to face the complexities of continually recompiling (or completely changing and adjusting) code as updates are made to system libraries. Ongoing maintenance, testing and support resources will also be required with an SDK implementation.

M2SYS Bio-Plugin™ Biometric System

The ideal biometric development and integration candidate is a complete system integrated into your application with 1:N **and** 1:1 matching capability and no system dependencies between host and fingerprint software. **Bio-Plugin™ is a patented multi-user, high-performance 1:N fingerprint matching server and complimentary client software system** with seamless database management and compatibility with distributed users over WAN (or through CITRIX MetaFrame) and compatibility with a variety of development environments including: C++, VB, .NET, Delphi, PowerBuilder, Java, Clarion, and web applications.

Development Considerations

Consider the following challenges any fingerprint recognition SDK presents which can significantly hamper development resources and prolong time to market.

SDK	M2SYS Bio-Plugin™
Understanding the parameters involved with fingerprint comparison, how they work, why they are significant, and how data needs to be extracted from an image	No knowledge required
Data type mapping, database management, data synchronization, exception handling	No knowledge required
System optimization to perform 1:N comparison for large databases. Opening a recordset from the database and matching one-by-one will not produce fast results	High performance fingerprint server performs multi-threaded, memory-based search for every request
Handling poor image quality, bad image acquisition, and unpredictable user input	System already designed to address these issues
Releasing a new version of your core software as you fix bugs in your fingerprint module will lead to a serious version management problem and excessive regression testing burden	Although appearing to your end users as having a seamlessly integrated fingerprint module, your core software is completely separate. You can independently release new versions of Bio-Plugin and your application
Investing time and resources in constantly resolving software defects and optimizing system performance to stabilize the fingerprint module	System has been continually optimized. M2SYS has learned from many different installations in various industry verticals how to optimize and stabilize Bio-Plugin to handle any unpredictable situation

Development Implications

M2SYS' Bio-Plugin™ for fingerprint recognition is a complete biometric system that also includes high-end server software capable of processing tens of thousands of fingerprint records within seconds. As opposed to using a low level SDK, developers can use Bio-Plugin™ to integrate a seamless, robust fingerprint recognition system nearly instantly. In addition, it prevents wasting the time, money, and resources needed to architect an optimized solution, and eliminates the headache associated with developing and maintaining a complete, reliable system (data transfer implementation, mapping data-types, linking libraries, understanding the result of making a call, storage management, fast data retrieval, etc.).

Bio-Plugin™ Biometric System Features/Benefits:

- » Rapid integration of complete fingerprint recognition system;
- » Minimal (if any) internal development resource requirements;
- » Includes verification (1:1) and identification (1:N) server software;
- » Compatible with WAN and CITRIX environments;
- » Rely on biometrics partner for ongoing best-of-breed development;
- » Compression algorithm reduces data size and improves speed;
- » Enroll fingerprints at 0.2 - 0.4 seconds;
- » Match against 30,000 records per second;
- » Multi-threaded, multi-processing, scalable system performance;
- » Adaptive image filtration eliminates scan "noise";
- » Allows minutiae extraction from even poor quality prints;
- » Does not require presence of fingerprint core or delta points;
- » Fully tolerant to fingerprint translation and rotation.

Technical Specifications

M2SYS Bio-Plugin™ Biometric Operating System enables developers to immediately add a complete, seamless fingerprint recognition system to applications without investing significant time, money, and resources required by an SDK to develop a comparable system from scratch. The following table summarizes M2SYS Bio-Plugin™ advantages when compared to low-level SDK's:

Category	SDK	M2SYS Bio-Plugin™
Product Structure	DLLs; building blocks to develop a system	Complete system already developed, including high-performance recognition engine
Development Time	8-12 months	1-2 days
System Dependencies	Host software always dependent on DLLs, need to constantly recompile code	No system dependencies
Documentation	May not include needed information for some development environments	Integrates with a variety of development environments and can provide sample code. Examples include: C++, VB, .NET, Delphi, PowerBuilder, Java, Clarion, and web applications
Support	Minimal vendor support, you are responsible for developing and supporting the system	Dedicated M2SYS engineer involvement to ensure successful completion of integration
Development Focus	Commitment required to developing, maintaining, and supporting the fingerprint system distracts from concentration on your core product	Remain focused on your core business and development competencies

Contact Us

M2SYS Technology
1050 Crown Pointe Parkway Suite 470
Atlanta, GA 30338 USA
info@m2sys.com

Web: www.m2sys.com
Tel: (770) 393-0986
Fax: (678) 559-0219

More Information

For the latest information about our product and services,
please see the following resources: <http://www.m2sys.com>

Articles & Resources

*"U.S. Biometric Network Authentication Markets Report,"
Frost & Sullivan 2004/03*

*"Biometrics: corporations have begun to see the value of
biometrics." CFO, 2002*

*"Handbook of Fingerprint Recognition,"
D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, 2003*

Copyright ©2008 M2SYS Technology. All Rights Reserved. M2SYS Technology logos, and trademarks or registered trademarks of M2SYS Technology or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others. Information regarding third party products is provided solely for educational purposes. M2SYS Technology is not responsible for the performance or support of third party products and does not make any representations or warranties whatsoever regarding quality, reliability, functionality, or compatibility of these devices or products.