Large-scale Biometric Management:
A Centralized, Policy-based Approach to Reducing Organizational Identity Chaos

By Jim Byrne

With rising security and fraud issues in day-to-day operations, every organization is looking to increase the levels of accountability and security among its employees, partners and customers. This is true not only in the general enterprise, where employees need secure access to their desktops, but also in airports, law enforcement and utilities, where reliable employee credentialing is critical in securing physical and logical access to resources and facilities. The most effective way to achieve this is to centralize an organization’s identity management function in a single place so that it can be effectively managed and the appropriate level of trust can be maintained in the authentication process.

A secure and effective method of authenticating an individual involves the verification of a unique and personal characteristic—a biometric. This is sometimes done in conjunction with a PIN or token, also known as multifactor authentication. Management of this biometric information, including its registration, storage, protection and verification, is known as biometric identity management (BIM).

Often, BIM technology is evaluated from a narrow perspective—quite simply, “does it authenticate a small set of users in a controlled environment?” Although this approach may be sufficient to meet small, narrowly defined requirements, it is not sufficient where identity management needs to expand beyond the first implementation. This approach may lead either to bad implementations that do not move forward or to no implementation at all, where the solution does not address the need for future development. A properly implemented enterprise-class BIM system will allow an organization to enhance security, streamline processes and significantly reduce its total cost of ownership (TCO) for IT systems.

Identity management is the registration, storage, protection, issuance and assurance of a user’s personal identifier(s) and privilege(s) in an electronic environment and in a secure, efficient and cost-effective manner. Previously, application providers have had to deal with the problem of identity and credential management as a result of an insufficient identity management functionality within the operating system infrastructure or a complete lack of standards across various target platforms. This led most organizations to deploy various “identity stovepipes,” where each application had its own identity management function built into the core system. However, supporting and maintaining the various stovepipe systems creates a high cost of ownership for an organization. This is about to change, as more and more application providers move to a model in which they rely on identity management vendors to provide a single core application to credential and authorize users.

Identity management is evolving in the same manner as data management did 10-15 years ago. Today, few companies that are developing highly available, scalable systems are building their own database infrastructure. Identity management should be no different. There are many reasons for this. Identity management is not the core business of application providers. For example, SAP does not want to build authentication systems; it would rather focus on business process management workflows. In addition, having an external, trusted identity management provider allows organizations to provide the greatest flexibility and system security. Business systems should not need to worry whether the authentication of the individual is done through fingerprints, voice patterns, iris scans or smart cards.

As complexity in IT infrastructure grows, every organization has difficulty implementing and managing various disparate identity management systems. This is a key problem for many organizations. To address this “organizational identity chaos” problem, organizations need a single authentication infrastructure that offers a centralized, policy-based approach to solve this problem and ensure that an organization not only has a single point of control, but also gains cost savings. Research analysts, such as Forrester Research, estimate that the annual cost per user for password administration can be anywhere from US $340 to $800. In large companies, employees might need passwords for between five and 15 computer applications, bringing the average annual cost of password administration to US $550 per user.

Features and Functions of a BIM System in a Large-scale Enterprise

Using a biometric identifier to authenticate employees, partners or customers/consumers allows an organization to have the highest level of assurance in the other participant’s authenticity. There are many issues that should be understood by any organization deploying this kind of solution.

BIM is concerned with the large-scale, proper management of the biometric identities for an enrollment population. A narrow view of this is traditionally based on enrollment and authentication. In other words, users are enrolled into a system and are authenticated, which satisfies the identity registration and assurance functions. However, when the requirements of
an enterprise-class BIM solution are broken into a set of functional groups, it becomes apparent that a proper BIM system must be much broader in scope. The key is to deploy a solution that provides functionality to the enterprise in each of seven areas, including identity registration, identity storage, identity assurance, identity protection, identity issuance, identity life cycle management and system management.

Identity Registration

Identity capture is the group of functions that facilitate the inclusion of users and their biometric data into the system. There are a number of main functions within the identity capture functional group:

- **Enrollment**—A proper enrollment process is a key feature that every system must provide to ensure a successful deployment. Organizations must understand the necessity for a good, managed enrollment process. A weak process will lead to system inaccuracies and an unreliable authentication infrastructure. Ideally, a good enrollment process is one in which the credentials of the user are properly ascertained at the time of enrollment. To drive quality enrollment, both the enrollee (the person enrolling in the system) and the enroller (the person asserting the validity of the credentials) should biometrically sign the enrollment record. Experience has shown that an enrollment process in which neither party can repudiate its participation in the transaction is the best way to drive quality of data and maintain a robust process.

- **Quality capture of the biometric**—A further important consideration at enrollment time is the quality capture of the biometric. Every biometric capture activity has differing levels of quality. With fingerprints, for example, quality can vary depending on the condition of skin (oily or dry), dirt on the finger, dirt on the sensor, ambient temperature, etc. Enrolling a poor quality image yields a less accurate system. Efforts should be made to ensure that highest quality enrollment images are captured. Generally, well-thought-out biometric systems employ a range of techniques to ensure that the best image is captured. This includes the enrollment of multiple fingers or iris images and the capture of multiple images (of each finger or iris) at enrollment. Ideally, for finger-based enrollment, the system should be capable of enrolling all 10 fingers.

- **Population coverage**—The ability to address all of the relevant population is also a key requirement. No single biometric can offer 100 percent coverage across all populations. The measure of a biometric implementation’s ability to address the intended population is known as the failure to enroll (FTE) or failure to acquire (FTA).

Identity Storage

The identity storage function identifies some of the storage characteristics of a large-scale identity management system. Primarily, a large-scale identity system requires a data storage technology that can keep pace with the size of the enrollment population. This implies the use of a terabyte-capable relational database, such as IBM DB2 or Oracle.

Any BIM system must also support the backup, archiving and restoration of information. The system should integrate into existing backup management solutions. This requirement is another reason to deploy a system only if it uses an industry standard storage technology. The use of an industry standard storage technology also lets an organization leverage the knowledge of its existing, highly trained database systems team.

Identity Assurance

This group of functions asserts an individual’s identity to other applications within the enterprise.

Verification is the process of determining an individual’s identity based on the presentation of a claim and a biometric in support of that claim. For a given claim, the system matches the presented biometric against the one stored at enrollment and returns the result (either a Boolean value or a score across some predefined range). It is very important that organizations choose a BIM solution that provides robust verification capabilities.

Some organizations have invested heavily in the deployment of public key infrastructure (PKI) solutions. As this is not a cheap investment, organizations should look to make a return on this investment. A BIM is a natural partner with an existing PKI system, as one key weakness of PKI solutions is that they do not authenticate the individual; they simply prove that an individual’s private key was used in a decryption or signing process. PKI implementations generally rely on passwords to form the link between the private key and the individual. The vulnerability of password systems is well known and documented and, therefore, is fundamentally flawed.

According to Ernst & Young, employees commit 84 percent of fraud detected in commercial organizations. This includes the sharing or violation of the use of passwords in organizations. Biometric technologies provide the missing link between individuals and the cryptographic keys assigned to them.

The key benefit of biometrics is the ability to ensure the involvement of the individual in a transaction. This prevents individuals from repudiating their participation in a transaction later on. The most useful BIM deployments should provide adequate levels of security across the entire infrastructure and provide integration with PKI in such a way that it is capable of generating standards-compliant digital signatures. The use of a biometric to ascertain the identity of the individual is a strong form of a digital signature.

Authentication (validating a claimed identity through the comparison of a presented biometric with a biometric captured at enrollment) is only part of the functionality that a BIM solution should provide to the enterprise. Integrating authentication with authorization provides far more functionality than authentication alone. This authorization can be provided internally from the biometric identity management system or through integration with an external system.

Multifactor authentication is the combination of a biometric (something you are) with some sort of token (something you have). Two types of tokens are generally used—dumb and smart. Dumb tokens (such as magnetic stripe cards) are capable only of carrying a claim of identity or an encrypted biometric. There is no capability in a dumb token to carry out any processing. Furthermore, dumb tokens can be easily copied or duplicated. Smart tokens, on the other hand, are
devices that have the ability to carry out independent processing within the token (e.g., smart cards). Smart tokens are secure computers in their own right. Most have the ability to securely store and process information such as biometric templates and cryptographic keys. Implementing a two-factor policy can increase security under the right conditions.

Identity Protection
This function group deals with the protection of an individual’s identity and the integrity of the scheme, as encryption of biometric data at the earliest possible time during both enrollment and verification is critical. Furthermore, all participants in the transaction—the client, the authentication server and the requesting application—should digitally sign their transmissions to ensure component integrity and nonrepudiation. Man-in-the-middle attacks should be guarded against using challenge-response protocols and digital signatures.

It is important that biometric templates and images be protected in any identity management system. Organizations wishing to deploy a solution must ensure that data are encrypted securely. Consider the damage that would be done to any organization should the biometrics of its enrollment database be published on the Internet. There are ways to guard against this happening. Best-in-class deployments use a tamper-resistant hardware security module (HSM) to perform all cryptography. Keys are generated on board the HSM itself to ensure effective key generation and management protocols. These keys should never be exported in the clear outside the HSM. The US federal government has a published standard regarding HSMs—Federal Information Processing Standard (FIPS) 140. Organizations should look for systems that use FIPS 140-accredited HSMs to obtain a level of assurance regarding the security of stored biometrics. Be aware, however, that using an HSM does not necessarily make a system secure (no more than using a biometric reader does). It is how the identity management system is designed and put together that ensures the security of the system.

Privacy is obviously a concern of every individual, and organizations must act appropriately to protect personal privacy if they expect to obtain acceptance from employees, partners and customers. Measures that should be implemented include giving participants a written guarantee that the organization will not share or divulge their biometric, will implement best-in-class security and management procedures for the system, and will immediately remove any personal information upon the request of the owner.

A secure and complete audit trail must also be maintained for every operation the system performs. No matter how trivial, operations should be logged in a tamper-proof manner for later interrogation, if required. This secure audit trail guards against system administrators being able to tamper with or amend records. For example, the use of secure FIPS-certified HSMs to generate symmetric message authentication codes (MACs) on each transaction is desirable, as the keys required for MAC generation are available only within the HSM.

Identity Issuance
Security can be increased further through the combination of multiple authentication factors in a single authentication transaction. This group of functions deals with issuing a credential (and possibly biometric identifiers) on tokens, such as smart cards.

A solution should support the issuance of various token types. Older tokens (such as magnetic stripe cards) are being phased out by organizations in favor of smart cards (both contact and contactless varieties). A token issuance function should support open standards, such as PKCS#11, for management of the token information. The system should also support a range of smart cards to ensure that an organization is not limited to a single card supplier. The issuance of the token should be recorded in the database and a secure audit entry generated. When the smart card contains cryptographic keys, the generation of these keys should be done in a secure manner, such as on the smart card itself or in a secure HSM. Tokens are very often lost, broken or stolen. When this happens, the identity management solution must be able to securely reissue the token and deliver it to the person requiring it. Audit trail and reporting functions must be available to allow an organization to track token reissuance statistics.

There is also a growing interest in authenticating an individual to a biometric stored on the smart card (as opposed to the central server). This model works in certain situations, such as when it is not feasible to connect a biometric reader to a central server. However, the performance and accuracy of authentication on a smart card is not equivalent to that which can be achieved on a server. Neither is the flexibility of a server-centric, policy-based approach available. Furthermore, the match-at-server model supports easy upgrades to authentication algorithms or the introduction of new modes as required. Management of card hot lists also becomes an issue in offline environments. The authentication terminal/reader is generally not powerful enough to maintain a complete list of all blocked or hot-listed cards. As stated earlier, smart cards have a finite life span and are often broken, lost or stolen. In these situations, they need to be reissued to individuals immediately. Unlike traditional PIN-protected smart cards in which a new PIN is simply generated, the issuance of biometrically protected smart cards is more complex. People have only 10 fingers, one voice, one face and two eyes. To reissue a PIN-protected card does not require any knowledge of the individual’s biometric characteristics, nor does it require the user to provide any personal information to the issuance system. With biometric cards, however, the situation changes. The issuance of the card involves the secure storage of an individual’s personal biometric data on the card. This requires the proper capturing of this data (enrollment) and the subsequent secure storage (management).

Identity Life Cycle Management
A biometric is unique to an individual. However, that does not mean it is static. As people grow older, a biometric element (such as an individual’s fingerprints) changes. For example, a person accumulates damage to fingers (e.g., from cuts and scratches) and the brittleness of their skin increases.
Some algorithms support the automatic aging of biometric templates. For example, through a process known as progressive enrollment, each verification operation slightly modifies the enrollment template to allow for aging or cracked/damaged fingers. BIM engines must support this function in situations where the organization has chosen an algorithm that does include progressive enrollment. In situations where progressive enrollment is not supported, an organization must be able to determine which enrollees are in danger of not being accepted by the system (generating a false reject) because the enrollment record is out of date compared to the current state of the individual’s biometric. To do this, a biometric identity management system must support the generation of reports based on time of enrollment, time of last verification, verification frequency, etc. Armed with this information, the enterprise can ensure that steps are taken to contact the individual and revalidate the enrollment prior to the effective period for the first enrollment expiring.

System Management

As organizations deploy a single identity management solution in an attempt to move away from “identity stovepipes,” it is important that they look to deploy a solution that integrates with existing system management technologies. This leads to a reduced cost of administration and allows the effectiveness of the system to be constantly managed within the existing critical systems infrastructure. Integration with systems such as IBM’s Tivoli Enterprise Console is a requirement, as is support for open standards, such as SNMP. In addition, organizations must be able to report against the activity of their identity management systems to ensure effectiveness of the system, analyze activity and spot trends, as well as provide data for conflict resolution, employee disputes, etc. Organizations deploying a large-scale identity management system must ensure that the data in the audit trail are complete and that a method exists to query this information in an efficient manner. For example, audit trail logs should be stored securely and should be accessible through an SQL interface to a relational database. In a large-scale system, searching audit logs in text files is not sustainable.

Conclusion

Identity management is now entering mainstream utility within the enterprise. Biometric algorithms have reached the levels of accuracy required, and the cost per user has declined significantly in recent years, yielding a form of authentication that is most cost-effective and secure. This is clear from the explicit requirements in recent legislation requiring the deployment of biometric technologies, such as the US VISIT Program or Schengen System II, as well as recent biometric standards adopted by the International Civil Aviation Organization (ICAO). Organizations looking to deploy a BIM solution need to look at the bigger, long-term picture and deploy a centralized, policy management solution that enables multifactor, multimodal and flexible authentication and authorization policies, while maintaining individual privacy. It is clear that this can be done effectively only through a scalable, highly available and secure infrastructure.

Jim Byrne

is senior vice president, government business, at Daon Ltd. He is responsible for defining strategy, managing operational activity, and achieving revenue and profitability goals via Daon’s sales, partnership and field delivery teams across the global government business area. Byrne has more than 15 years’ experience across both government system integrators and enterprise software product vendors.