



Biometric Identity Management in Large-Scale Enterprises

October 2002

TABLE OF CONTENTS

1. INTRODUCTION.....	4
2. IDENTITY MANAGEMENT.....	5
2.1 What is identity management?	5
2.2 Identity Management and Business IT Systems	5
2.3 Organisational Identity Chaos	6
3. BIOMETRIC IDENTITY MANAGEMENT FUNCTIONS.....	8
3.1 Identity Registration	9
3.1.1. Enrolment	9
3.1.2. Trusting an identity at enrolment	9
3.1.3. Quality capture at enrolment.....	10
3.1.4. Population Coverage	10
3.1.5. Batch Enlistment.....	11
3.1.6. Image Capture	11
3.1.7. Multi-modal	11
3.2 Identity Storage	12
3.2.1. Proven reliability, scalability.....	12
3.2.2. Backup, Archiving & Restoration	12
3.2.3. Industry standard storage architectures	12
3.3 Identity Assurance.....	12
3.3.1. Verification	12
3.3.2. Integration with existing PKI	13
3.3.3. Electronic Signatures.....	13
3.3.4. Identification.....	13
3.3.5. Authorisation.....	13
3.3.6. Enterprise Access Management Integration.....	14
3.3.7. Multi-factor Authentication	14
3.3.8. Policy-based Combinational Biometrics	14
3.3.9. Authentication Policy Management	15
3.3.10. Application Connectivity/Utility.....	15
3.4 Identity Protection	16
3.4.1. End-to-end security.....	16
3.4.2. Securing the biometric	16
3.4.3. Privacy	16
3.4.4. Audit Trail.....	17
3.4.5. System Integrity.....	17
3.5 Identity Issuance	17
3.5.1. Token Issuance	17
3.5.2. Re-issuance.....	18

3.5.3. Biometrics on Smart Cards.....	18
3.6 Identity Life Cycle Management.....	18
3.6.1. Biometric Ageing.....	18
3.6.2. Enrolment Revalidation.....	19
3.6.3. Migration.....	19
3.7 System Management.....	19
3.7.1. Reducing TCO/system administration.....	19
3.7.2. Audit Trail and Reporting.....	19
4. BIOMETRIC IDENTITY MANAGEMENT – IMPORTANT FEATURES.....	21
4.1 Scalability, High Availability.....	21
4.1.1. Scalability.....	21
4.2 Availability.....	21
5. THE MOVE TO STANDARDS.....	23
6. CONCLUSION.....	24
6.1 DaonEngine and large scale identity management.....	24

1. Introduction

With rising security and fraud issues in their day-to-day operations, every organisation is looking to increase the levels of accountability and security among its employees, partners and customers. The most effective way to achieve this is to centralise the identity management functions of the organisation in a single place so that they can be effectively managed and the appropriate level of trust can be maintained in the authentication process.

The most 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 (known as multi-factor authentication). The proper management of this biometric information, including its registration, storage, protection and verification is known as **Biometric Identity Management**.

However, very often, biometric identity management technology is evaluated from a very 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 will not be sufficient where the identity management needs to expand beyond the first implementation. The naive approach can 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 further development.

This paper outlines some of the key functions that should be part of any **enterprise class** biometric security system. It provides a basis on which organisations looking to deploy large scale, long-lived biometric security systems should base their product evaluations. Authentication is a key part of this, but there are many other elements in a biometric security solution that organisations need to consider.

A properly implemented biometric identity management system will allow an organisation to enhance security, streamline processes and significantly reduce its Total Cost of Ownership for IT systems.

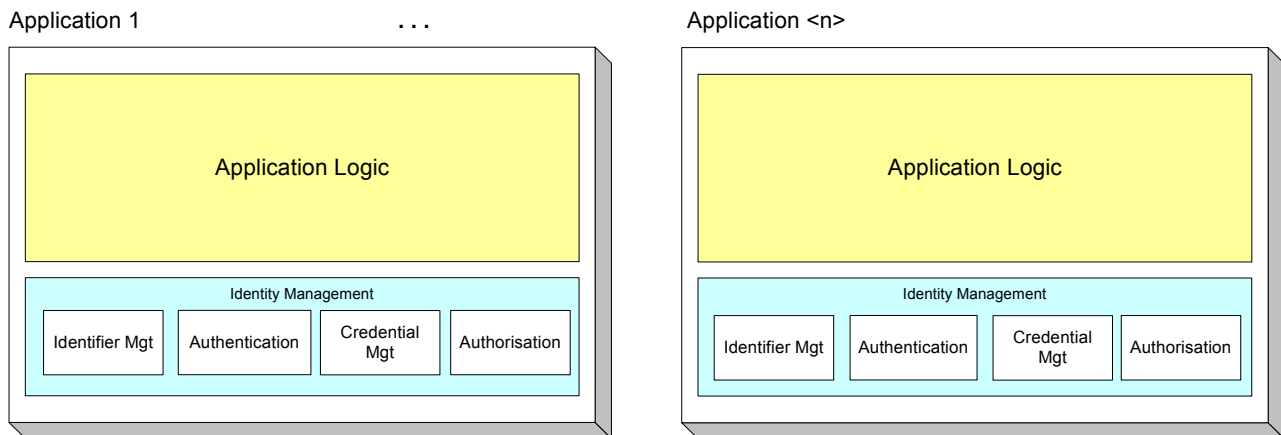
2. Identity Management

2.1 What is identity management?

Identity Management is the registration, storage, protection, issuance and assurance of a user's personal identifier(s) and privilege(s) in an electronic environment in a secure, efficient and cost effective manner.

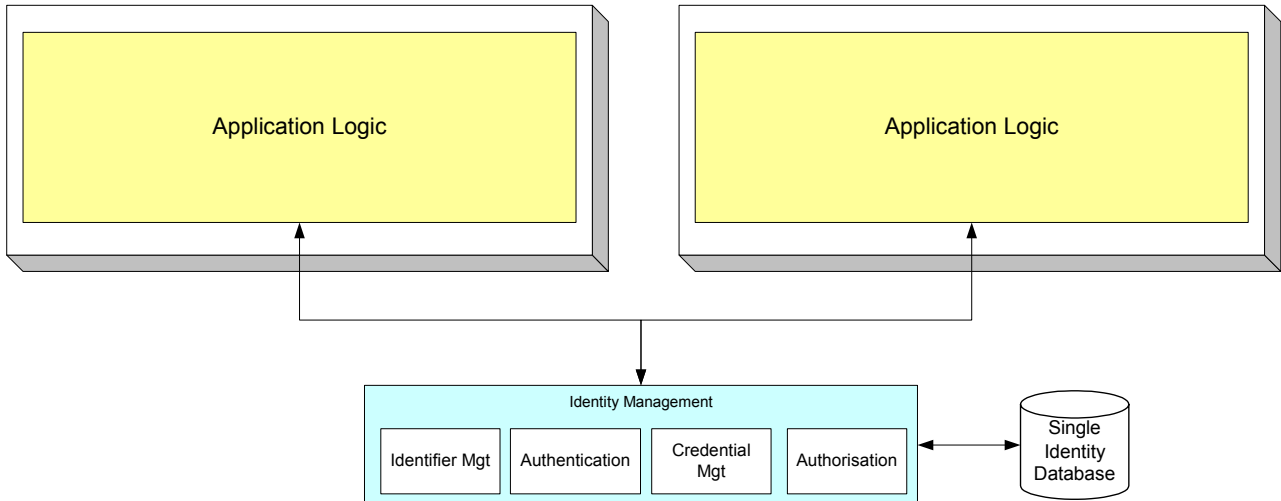
2.2 Identity Management and Business IT Systems

In the past, application providers have had to deal with the problem of identity and credential management. This was due to either insufficient identity management functionality within the operating system infrastructure or a complete lack of standards across the various potential target platforms. This leads most organisations into deploying various “identity stovepipes” as depicted in the following diagram.



In the example above, each application has its identity management functionality built into the core system. This leads to a massive cost of ownership for an organisation – supporting and maintaining the various stovepipe systems.

This is about to change however, as more and more application providers will move to a model where they rely on identity management vendors such as Daon to provide the core application credentialing and authorisation infrastructure they need (see below).



Identity Management is evolving in much the same manner that data management did 10-15 years ago. Today, few companies who are developing highly available, scalable systems would consider building their own database infrastructure – instead they integrate proven technologies such as Oracle, DB2. Identity Management should be no different.

There are many reasons for this.

1. Identity management is not the core business of these application providers. For example, SAP does not want to build authentication systems – they would rather focus on business process management workflows.
2. Having an external, trusted identity management provider allows organisations to provide the greatest flexibility and system security. Business systems should not need to worry whether the authentication of the individual is done through finger, voice, iris or smart card.
3. As complexity in IT infrastructure grows, every organisation has difficulty implementing and managing various disparate identity management systems. This is a key problem for many organisations.

2.3 Organisational Identity Chaos

Daon calls this the “organisational identity chaos” problem. DaonEngine can provide a single authentication infrastructure that helps to solve this problem. By offering a centralised policy-based approach Daon products ensure that:

1. An organisation has a single point of control
2. A reduced Total Cost of Ownership (TCO) is achieved
3. An organisation can react very quickly and effectively as needs arise.

The following diagram depicts the identity chaos problem in a large organisation and how Daon can provide a solution to the problem.



On the left you have the chaotic situation which exists today for many organisations – various, disparate identity types. DaonEngine through its highly robust and scalable infrastructure provides a centralised policy management kernel that can manage elements of these disparate systems. On the right, you have the various mission critical IT systems that an organisation uses. With DaonEngine, instead of a many to many infrastructure between the identity types and the applications, you now have a single point of authority concerning a user's identity. Thus, an organisation can add a new identity type (e.g. voice) and this can be managed by DaonEngine without the organisation having to change the application connectors, policy engine or enterprise IT systems.

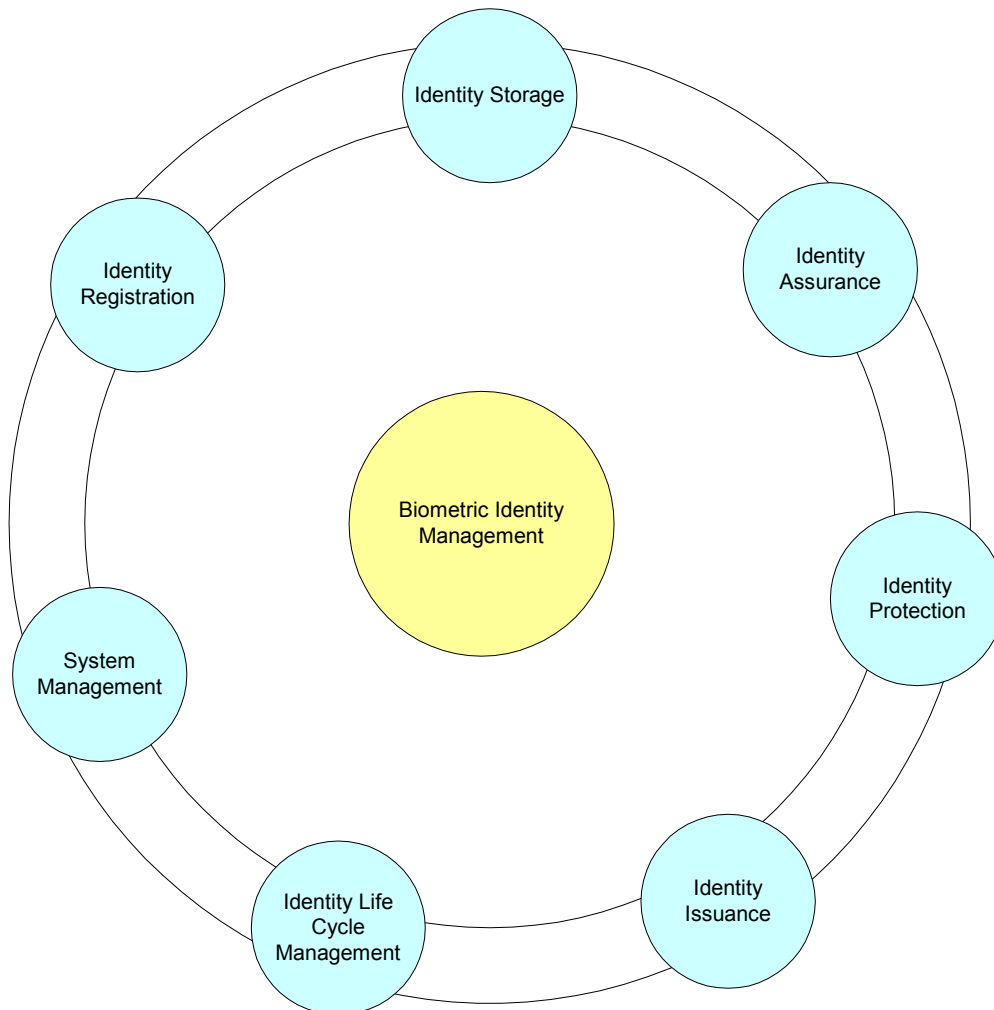
This provides a very significant cost saving to the enterprise, as traditionally the implementation of the connections from the identity types to the business systems has been the prime cost driver for enterprise implementations.

The remainder of this paper concentrates specifically on the features and functions required of a **biometric** identity management system in a large-scale enterprise. Using a biometric identifier to authenticate employees, partners or customers/consumers allows an organisation to have the highest level of assurance in the other participant's authenticity. This document discusses the issues that need to be understood by any organisation deploying this kind of solution.

3. Biometric Identity Management Functions

Biometric Identity Management is concerned with the large-scale, proper management of the biometric identities for an enrolment population. A narrow view of this is traditionally based around enrolment and authentication. In other words, you enrol users into a system and authenticate them.

The following diagram outlines a more rounded view of this by breaking the requirements of a Biometric Identity Management solution into a set of functional groups.



Basic enrolment and authentication are covered under the Identity Registration and Identity Assurance headings. It should be apparent that a proper biometric identity management system must be very much broader in scope.

The key is to have a solution in place that provides functionality to the enterprise in all seven areas:

- Identity Registration
- Identity Storage

- Identity Assurance
- Identity Protection
- Identity Issuance
- Identity Life Cycle Management
- System Management

Each of these areas will now be explored in more detail.

3.1 Identity Registration

Identity Capture is the group of functions a system provides to facilitate the inclusion of users and their biometric data into the system. There are five main functions within the identity capture functional group.

3.1.1. Enrolment

Enrolment is a key feature that every system must provide. The key to successful deployments is a proper enrolment process. Organisations must understand the necessity for a good, managed enrolment process. A weak process will lead to system inaccuracies and an unreliable authentication infrastructure.

Ideally, a good enrolment process is one where the credentials of the user are properly ascertained at the time of enrolment. To drive a quality enrolment, both the enrollee (the person enrolling in the system) and the enroller (the person asserting the validity of the credentials) should biometrically sign the enrolment record. Experience has shown that an enrolment process where neither party can repudiate their participation in the transaction is the best way to drive quality of data and maintain a robust process.

3.1.2. Trusting an identity at enrolment

Models are available for handling the establishment of identity at enrolment. One of these is the tScheme in the UK (www.tscheme.org). tScheme provides for three levels of risk in the misuse of identity. These are expressed in terms of the financial loss should the enrolment identity prove to be false.

- Level One - inconvenience or minor financial loss only
- Level Two - significant financial loss, inconvenience, obstruction of justice etc
- Level Three - substantial financial loss, risk to personal welfare or safety

This consequentially leads to a set of levels concerning the accuracy of the enrolment.

- Level Zero – no authentication required
- Level One – on the balance of probabilities, the registrant's identity is verified
- Level Two – there is substantial assurance that the registrant's identity is verified
- Level Three – the registrant's identity is verified beyond reasonable doubt.

An organisation can decide on the level(s) of authentication required at enrolment and implement a scheme similar to the tScheme.

3.1.3. Quality capture at enrolment

A further important consideration at enrolment time is the quality capture of the biometric. Every biometric capture activity has differing levels of quality. With finger image for example, quality can vary depending on condition of skin (oily, dry), dirt on finger, dirt on sensor, ambient temperature etc.

Enrolling a poor quality image yields a less accurate system later on. Efforts should be made to ensure that highest quality enrolment images are captured. Generally, well thought out biometric systems will employ a range of techniques to ensure that the best image is captured. This should include the capture of multiple images (of each finger) at enrolment and the enrolment of multiple fingers or iris images. Ideally, for finger-based enrolment, the system should be capable of enrolling all ten fingers.

Good biometric systems will enforce a strict quality process at enrolment. This is usually done through an automated component which returns a quality score based on the image to the enrolment application. If the quality score is not at a sufficient level, then the image is not accepted.

Furthermore, better biometric systems capture more than one image (in many cases, 3) per finger, choosing the best one. In some cases, they even calculate an “averaged” biometric based on a combination of all the images.

3.1.4. Population Coverage

The ability to address all of the relevant population is a key requirement. No single biometric can offer 100% coverage across all populations. The measure of a biometric implementation’s ability to address the intended population is known as the Failure to Enrol (FTE) or Failure to Acquire (FTA).

The key to solving the problem is two fold:

1. Choose an algorithm/vendor with a proven very low FTE/FTA.
2. Always purchase a multi-modal biometric identity solution (multi-modal solutions support the use of different biometric authentication mechanisms – for example, finger, hand, iris).

It should be noted that for most office environments with small to medium implementations, a single form of biometric authentication might suffice. However, consider a low FTE such as 0.05% in a large-scale deployment. The following table shows the number of users in the population who could not be dealt with if an organisation implements a single mode biometric solution.

Population	FTE 0.05%
100	0
1000	1
10000	5
100,000	50
1,000,000	500

A multi-modal or multi-factor approach to Biometric Identity Management (BIM) will reduce this FTE to zero.

3.1.5. Batch Enlistment

Invariably, a BIM solution is deployed into organisations that already have identity systems in place. Such systems include directory servers, HR databases and the like. It is important that biometric identity management systems integrate into or augment existing infrastructures with a minimum of rework.

One function, which should be provided in support of this, is the ability to enlist users in a batch mode. Enlistment is the “data take on” component that allows organisations to feed identity information (name, address, employee id etc) into the system without the need for manual data entry.

Batch enlistment minimises the work required at enrolment time as much of the manual keying of information is complete and the enrolment process simply requires the capturing of the biometric information.

3.1.6. Image Capture

Many systems will require the capture of images at enrolment. There are a number of reasons for this:

1. To provide migration across different algorithms and sensors (see subsequent section in this document).
2. To facilitate background checking (for example with law enforcement agencies) where the situation requires it.

If images are captured, they must be securely stored and managed within the BIM system (see section on privacy later). Furthermore, the facilitation of background checking should only be done where the user consents ahead of time and is aware at enrolment that this will take place.

3.1.7. Multi-modal

The ability to capture more than one mode of identity is important from two perspectives. The first (already discussed) is the ability to address all of the relevant population. The second (discussed in the identity assurance function group below) relates to a technique

termed “Combinational Biometrics” by Daon that allows a flexible, policy based approach to identity establishment.

3.2 Identity Storage

The identity storage function grouping identifies some of the storage characteristics of a large-scale identity management system.

3.2.1. Proven reliability, scalability

Primarily, a large-scale identity system requires a data storage technology that can keep pace with the enrolment population. Organisations looking to deploy a BIM solution with large enrolments should only choose systems whose underlying storage technology has been in mainstream use and clearly has the capacity to handle the requirements.

This implies the use of a terabyte capable relational database such as IBM DB2 or Oracle.

3.2.2. Backup, Archiving & Restoration

Any Biometric Identity Management system must support the backup, archiving and restoration of information. The system should integrate into existing backup management solutions – organisations do not need a “stove pipe” system from a data management perspective.

This requirement is another reason to only deploy a system if it uses an industry standard storage technology.

3.2.3. Industry standard storage architectures

Most large organisations have a team of database experts who are responsible for the smooth operation of the enterprise data systems. This team knows their data systems well and ensures that they are optimised for business requirements – performance, business recovery etc.

The use of an industry standard storage technology is key to leveraging off an already highly trained database systems team.

3.3 Identity Assurance

This group outlines the functions a BIM solution should provide in terms of asserting an individual’s identity to other applications within the enterprise.

3.3.1. Verification

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 enrolment and returns the result (either a Boolean value or a score across some predefined range).

It is very important that organisations choose a BIM solution that provides robust verification capabilities.

There is a range of measures in relation to verification.

- False Match Rate – FMR

- False Non-Match Rate – FNMR
- Failure To Acquire – FTA

Rather than devote large sections of this document to verification, a separate white paper is available from Daon dealing with issues in relation to verification algorithm accuracy and suitability within large-scale enterprise deployments.

3.3.2. Integration with existing PKI

Some organisations have invested heavily in the deployment of Public Key Infrastructure (PKI) solutions. This is generally not a cheap investment and organisations should look to make a return on this investment.

A BIM is a natural partner with an existing PKI. A 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 the system is therefore fundamentally flawed. Biometric technologies provide the missing link between the individual and the cryptographic keys assigned to them.

Integration between BIM and PKI systems should be through open standards such as PKCS#7 and PKCS#10.

3.3.3. Electronic Signatures

The key benefit of biometrics is the ability to ensure the involvement of the individual in a transaction. This prevents the individual from repudiating their participation in the 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 the strongest form of digital signature available.

3.3.4. Identification

Identification is the process of identifying an individual from the entire enrolled population without the use of a claim of identity. Identification is primarily a requirement for police/immigration type systems and is rarely used in enterprise deployments.

Where it is used within an enterprise, it is usually for small populations or subsets.

3.3.5. Authorisation

Authentication (validating a claimed identity through the comparison of a presented biometric with a biometric captured at enrolment) is only part of the functionality a BIM solution should provide to the enterprise. Integrating authentication with authorisation provides far more functionality than authentication alone.

This authorisation can be provided internally from the biometric identity management system or through integration with an external system – see Enterprise Access Management Integration.

3.3.6. Enterprise Access Management Integration

Authenticating an individual is only one piece of the puzzle in identity management. The other major component is authorising that same individual to perform a transaction or function. Examples of this include accessing protected resources, signing off financial transactions etc.

Any biometric identity management system must work as part of a bigger solution providing access management to the enterprise. The identity management system may provide this authorisation function itself or may work seamlessly with specialist access management technology such as IBM's Tivoli Access Manager.

There is a symbiotic relationship between authentication and authorisation. Authorisation cannot take place without strong authentication. Authentication is relatively ineffectual in complex business environments without an authorisation function built on top of this.

3.3.7. Multi-factor Authentication

Multi-factor authentication is the combination of a biometric (something you are) with a token of some description (something you have). Two types of tokens are generally used – dumb and smart.

Dumb tokens are tokens (such as magnetic stripe cards) that are only capable 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. Examples of this include 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 (something you are – a biometric – with something you have – a smart token) can increase security under the right conditions.

3.3.8. Policy-based Combinational Biometrics

One reason for multi-modal biometric support has already been discussed – coverage in large populations. A second, very important reason relates to an organisation's ability to implement a very flexible, combinational approach to identity establishment.

For example, an organisation may require 2 fingers in combination to authenticate a user. Alternatively, you can randomise the finger chosen or choose any finger but the last one in each authentication request, or request a "favourite" finger without divulging which one. These simple authentication scenarios guard very effectively against fingerprint spoofing even from insecure devices.

Organisations looking to deploy a secure access solution should look to a technology that allows them to combine various biometric modes with multi-factor (e.g. token) security. This ensures:

- Longevity of investment

The bar is constantly being raised with regard to identity management and security systems and organisations need the ability to move with the market.

- Robust security infrastructure

A flexible, policy based approach is required to allow an organisation to determine the appropriate manner to protect its assets.

3.3.9. Authentication Policy Management

Having a configurable, policy driven approach to identity assurance is important for any enterprise. Not all systems you are trying to protect have the same level requirements from a security perspective and it is important to be able to trade off correctly between security and convenience.

For example, for network access inside the building, it may be sufficient to ask for one finger at authentication – especially if for example the user had to biometrically authenticate to get into the building. Dialling in from a remote location over VPN for example, would require additional security, such as two fingers, randomisation of biometric or the presentation of both a card and a finger.

The key point here is that an enterprise must have the flexibility to carry out its own threat analysis and have a BIM system that is configurable to the enterprise's needs.

Most importantly, a centralised, policy driven identity management function allows an organisation to react quickly to the changing threat landscape. Attackers are changing their methods and constantly finding weaknesses. As each new authentication technology is deployed, its weaknesses will be exposed and it is very foolish of any organisation to “sit still” when protecting their assets. Organisations need to be able to constantly revise their authentication and authorisation policy. Key to doing this effectively is deploying a future-proof extensible technology such as DaonEngine where you can apply different policies and authentication methods while maintaining the same authorisation infrastructure to your business critical IT systems.

3.3.10. Application Connectivity/Utility

For a biometric identity deployment to be successful, it must provide large-scale integration with legacy systems within the enterprise. Organisations should be able to quickly and easily leverage off their investment in a BIM solution to enable it to be the single point of authentication to all their systems.

This inter-system connectivity should be provided through a robust API (Application Programming Interface). Ideally, this API must be callable from various technologies (C, C++, Java) and should support the secure provision of its services over a distributed infrastructure.

The key to a successful connectivity within the enterprise is ensuring that the identity management solution has an easy to use (yet fully featured) programming model.

It is important when assessing biometric identity management technologies that it integrates with enterprise COTS (Commercial Off The Shelf) products. Examples of this include:

- Windows NT/2000/XP
- Web Services/Systems
- Physical Access Management Systems
- Siebel

- External Authorisation Systems

3.4 Identity Protection

This function group deals with the protection of an individual's identity and the integrity of the scheme.

3.4.1. End-to-end security

It is not sufficient to simply attach a biometric reader to each PC in the organisation and expect to have a secure infrastructure. In fact, this can be a very dangerous practice as organisations may feel secure and become complacent when in fact their security is as weak as ever.

A total end-to-end approach must be taken. This involves encrypting the biometric data at the earliest possible time during both enrolment and verification. 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 non-repudiation.

Man in the middle attacks should be guarded against using challenge-response protocols and digital signatures and nonces should be used to prevent replay attacks.

A more detailed discussion on the security requirements for large-scale BIM deployments is available by contacting the author.

3.4.2. Securing the biometric

It is very important that biometric templates and images be protected in any identity management product. Organisations wishing to deploy a solution must ensure that this data is encrypted in a secure manner. Consider the damage that would be done to any organisation should the biometrics of its enrolment database be published on the Internet.

There are ways to guard against this happening.

Best-in-class deployments will use a tamper-resistant hardware security module (HSM) to perform all cryptography. Keys should be generated on board the HSM itself to ensure effective key generation and management protocols. The keys should never be exported in the clear outside the HSM.

The US Government has a published standard regarding HSMs – it is known as FIPS 140 (FIPS is short for Federal Information Processing Standard). Organisations 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 a HSM does not necessarily make a system secure (no more than using a biometric reader does). It is how the identity management product is designed and put together that ensures the security of the system.

3.4.3. Privacy

Privacy is obviously a concern of every individual and organisations 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 organisation will:

- Not share or divulge their biometric.
- Implement best-in-class security and management procedures for the system.
- Maintain the integrity of the system.
- Remove any personal information immediately at the request of the owner.
- Only deploy a solution that meets the requirements stated in the identity protection section of this document.

3.4.4. Audit Trail

A secure and complete audit trail must be maintained for every operation the system performs. No matter how trivial, it should be logged in a tamper-proof manner that can be interrogated later if required.

A secure audit trail should guard against system administrators being able to tamper with or amend records.

For example, the use of secure FIPS-rated HSMs to generate symmetric MACs (Message Authentication Codes) on each transaction is desirable. The keys required for the MAC generation should only be available within the HSM.

3.4.5. System Integrity

Maintaining the internal integrity of the system is a key feature. A well-designed identity management system will include autonomic functions such as the ability to detect integrity errors internally and to raise alerts on the enterprise systems management console.

Integrity checks should be applied to binaries/executables, biometric data, audit trail, identity registration records and more.

3.5 Identity Issuance

It is well recognised that security can be increased through the combination of multiple authentication factors (for example, something you have – a token; something you are – a biometric) in a single authentication transaction. This group of functions deals with issuing a credential (and possibly biometric identifiers) on tokens such as smart cards.

3.5.1. Token Issuance

A solution should support the issuance of various token types, in particular smart cards. Older tokens (such as magnetic stripe cards) are being phased out by organisations in favour of smart cards (both contact and contact-less 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 – thus ensuring that an organisation is not tied to a single card supplier. The issuance of the token should be recorded in the database and a secure audit entry generated.

Where 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.

3.5.2. Re-issuance

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 organisation to track token re-issuance statistics.

3.5.3. Biometrics on Smart Cards

There is a growing interest in authenticating an individual to a biometric stored on a smart card (as opposed to a central server). This model works in certain situations (for example, where 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 upgrade to authentication algorithms and even the introduction of new modes as required (if there is no biometric stored on the card – just a claim of identity).

Management of card hot-lists becomes an issue in offline environments. The authentication terminal/reader is generally not powerful 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 and stolen. In these situations, they need to be re-issued to individuals. Unlike traditional PIN protected smart cards where you simply generate a new PIN, the issuance of biometrically protected smart cards is more complex.

People only have ten 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 have provided 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 (enrolment) and the subsequent secure storage (management).

3.6 Identity Life Cycle Management

A biometric is unique to an individual, however that does not mean that it is static. In many cases, a biometric element (such as an individual's fingerprints) will change over time, as they grow older. Even if the fingerprint itself stays static, a person will accumulate damage to their fingers as they grow older (e.g. from cuts, scratches) and the brittleness of their skin will increase.

3.6.1. Biometric Ageing

Some algorithms support the automatic aging of biometric templates – for example, through a process known as progressive enrolment where each verification operation can modify the enrolment template slightly to allow for aging or cracked/damaged fingers.

Biometric identity management engines should support this function in situations where the organisation has chosen an algorithm that supports it.

3.6.2. Enrolment Revalidation

In a situation where progressive enrolment is not supported, an organisation must be able to determine which enrollees are in danger of not being accepted by the system (generating a false reject) because the enrolment record is out of date compared to the current state of the individual's biometric.

In order to do this, a biometric identity management system must support the generation of reports based on time of enrolment, 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 enrolment prior to the effective period for the first enrolment expiring.

3.6.3. Migration

Using multiple algorithms and sensors within an organisation can lead to interoperability issues. Today, the template formats for most algorithm vendors are considered a trade secret and are not disclosed. This can lead to issues with migration of enrolments across algorithms and sensors.

More importantly, as the next generation of spoof resistant fingerprint sensors is deployed, the templates will contain more than just minutiae or pattern elements of interest but also elements such as temperature.

This makes the migration of enrolment records even more difficult as the lowest common denominator (the image) is no longer the sole source of information in the template.

Daon has specific methods for dealing with this. The interested reader is invited to contact us for more information.

3.7 System Management

As organisations deploy a single identity management solution in an attempt to move away from identity stovepipes, the last thing they need to do is create a system management stove pipe as a result.

3.7.1. Reducing TCO/system administration

It is important that an organisation looks 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 thus a requirement as is support for open standards such as SNMP.

3.7.2. Audit Trail and Reporting

It is a requirement for any organisation to be able to report against the activity of its identity management system. This is required to:

- a) Ensure effectiveness of the system
- b) Analyse activity, spot trends
- c) Provide data for conflict resolution, employee disputes etc

As an organisation deploying a large-scale identity management system, you must ensure that the data in the audit trail is complete and that you have a method of querying this information in an efficient manner.

For example, audit trail logs should be stored securely and accessible through an SQL interface to a relational database. In a large-scale system, searching audit logs in text files is not sustainable.

4. Biometric Identity Management – Important Features

4.1 Scalability, High Availability

4.1.1. Scalability

For any identity management system to be worth the investment, it must scale to meet the organisation's projected requirements. An organisation's requirements should be specified in a number of ways

- Number of users enrolled
- Number of concurrent authentication sessions supported
- Average response time
- Longest response time
- Availability criteria – for example, mean time between failures

Having stated projected levels of service, an organisation should ensure that there is room for growth should they need it. An organisation considering an identity management system should subject it to availability and scalability testing as part of the purchase evaluation.

Scalability is generally expressed in two ways – Vertical and Horizontal. Vertical scalability is scalability offered through platform ranges. For example, a system might be available on a range of platforms from Windows 2000 up to high-end Unix variants. Horizontal scalability on the other hand, is that scalability offered through the introduction of new servers into a cluster. With horizontal scalability, you should be able to easily add new servers to take on any further load. In this scenario, the system should be capable of using the extra server automatically should it need to.

Horizontal scalability also adds to a fault tolerant architecture if implemented correctly.

Of course, scalability is a function of all the components in the system. Scalable systems are generally designed to be resource and computationally efficient. As a result, most are multi-threaded and built on proven technology (for example, a robust, efficient database). In choosing a scalable solution, organisations must take into consideration both the benchmarked performance of the system and the underlying technology platform.

4.2 Availability

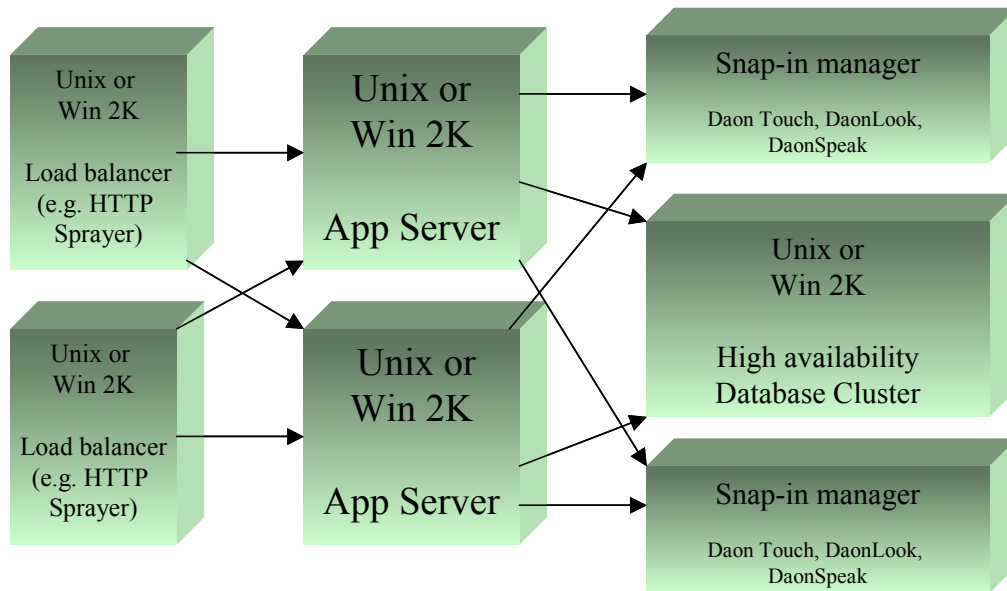
In a mission-critical enterprise scenario, availability is a key requirement. While no single technology component can ever be guaranteed to be 100% available, a high availability system will be built in such a way as to a) minimise average time between failures of any component and b) minimise average failure time for any component.

Furthermore, high availability systems tend to use redundant components (e.g. a bank of servers) to ensure that should any one of these fail individually, the others can automatically take the load until the component can be brought back into service.

It can immediately be seen that the horizontally scalable architecture outlined in the previous section is applicable to high availability situations. However, it should be noted that simply running a bank of servers alone is not sufficient.

A proper load balanced, highly available configuration must support multiple redundant systems and distribution of processing across all components.

In the example shown below (supported by DaonEngine's technology), an organisation can run multiple application servers and authentication subcomponents (shown as snap-ins) in a highly fault tolerant fashion. Please see Daon's product fact sheets for more information on snap-ins.



The diagram above (although at a high level) shows that there is no single point of failure.

Finally, a well-designed system will ensure that the user interactions are as stateless as possible. By stateless, we mean that should a server fail during an authentication (which may involve many requests back and forth to the user or partner application), the information required for another server to continue to handle the request is not stored on the component(s) that failed.

Of course, the previous examples are at a very high level and in reality, there are many further considerations in the design of solutions like this. Interested readers are invited to contact Daon should they wish to discuss further.

In choosing a solution, organisations should ensure that it provides the functions and features required of a high availability implementation. This includes

- Fault tolerance (redundancy) on all components
- An underlying database with proven availability
- Stateless interaction
- Built on platforms (e.g. operating systems) proven to run in high availability deployments

5. The move to standards

The use of biometric authentication within the enterprise is showing the classic technology “emergence” profile. Symptoms of this include the hardware cost per device dropping significantly while IT spend is increasing exponentially.

As a result, certain standards are beginning to emerge as de-facto, while new ones are being created. Many standards relate to biometrics and identity management. The following are some of the more relevant ones.

BioAPI

www.bioapi.org

BioAPI has become the de-facto industry standard addressing the operating system independent integration of various biometric types.

Common Criteria

www.commoncriteria.org

Common Criteria “*represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community*” according to its website. It is the amalgamation of a range of standards relating to the security of IT systems and is now moving to address security of biometric authentication schemes.

tScheme

www.tscheme.org

tScheme addresses standards around establishing a person’s identity primarily at enrolment. tScheme is a UK based organisation. Whilst tScheme is not specifically a technology standard, it is an important one as it sets minimum criteria for a properly managed enrolment process.

Bioprivacy

www.bioprivacy.org

The International Biometric Group’s (IBG) bioprivacy initiative is an important one when it comes to establishing a solution that protects the individual’s privacy. Although, primarily not a technical standard, it does address the needs of a privacy enhancing biometric authentication system through its 25 “Best Practices for Privacy-Sympathetic Biometric Deployment”.

Liberty Alliance

www.projectliberty.org

The liberty alliance is a cross-industry body developing standards for federated identity management.

A prospective implementer of a biometric identity management system should ensure that a vendor supports or intends to support the technical standards outlined above and provides technology that allows the operational support for the non-technical standards.

6. 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.

Organisations looking to deploy a biometric identity management solution need to look at the bigger, long term picture and deploy a centralised, policy management solution that enables multi-factor, multi-modal, flexible authentication and authorisation policies whilst maintaining individual privacy. This needs to be provided on a scalable, highly available and secure infrastructure.

6.1 DaonEngine and large scale identity management

Daon's biometric identity management system (DaonEngine) is designed to be the engine on which the organisation manages identities for its various IT systems. DaonEngine provides the required features outlined in this paper. It has been independently assessed as best in class from many perspectives including performance, scalability, robustness and security.

It is a multi-modal identity management system allowing an organisation to authenticate and authorise users in various different ways (e.g. finger, smart card) and supports easy integration with external applications within the enterprise.

Ten key points on DaonEngine:

1. DaonEngine has proven scalability and high performance for 1 million+ users.
2. DaonEngine supports many forms of biometric authentication including finger, voice iris.
3. DaonEngine supports the personalisation and use of smart cards.
4. DaonEngine has undergone rigorous high-availability and scalability testing which far exceeds any of its competitors.
5. DaonEngine uses FIPS 140 level 4 HSMs to manage the cryptographic keys used to protect biometric information.
6. DaonEngine uses extensive internal integrity checks to ensure the correct functioning of the system.
7. DaonEngine provides an organisation with the ability to implement a totally flexible and configurable policy driven approach to authentication of the individual.
8. DaonEngine integrates with best-in-class authorisation systems.
9. DaonEngine can support any biometric sensor and algorithm through its snap-in architecture.
10. DaonEngine provides a detailed low-level XML based API and a high-level Java and C++ API.