

Biometric Buyer's Handbook

Product Selection & Implementation Guide

By techBiometric.Com

techBiometric.Com

Facilitating Global Business for Biometric Products

Visit techBiometric.Com - Your Gateway to Global Biometric Business

Table of Contents

Introduction	3
Biometric Identification and Authentication – Important Factors to Evaluate Product Selection.....	3
Chapter I	4
How to Get Prepared	4
Chapter II	6
Designing an Effective Enrolment Process	6
Chapter III	8
Evaluating the Technical Requirements.....	8
Chapter IV.....	10
Considering the Cost and the Output Benefits.....	10
Chapter V.....	12
Consider the Requirements of End Users.....	12
Chapter VI.....	14
What Would Be the Way to Operate	14
Chapter VII.....	16
The Critical System Administration Issues and Concerns.....	16
About tectBiometric.Com	19
Important Links	20

Introduction

Biometric Identification and Authentication – Important Factors to Evaluate Product Selection

Biometrics and its applications have been explored in different walks of life. From fulfilling the security needs at home to creating high-end security environment at offices, airports, banks and hospitals, the technology is enjoying wide acceptance across the globe. However, it is important for an individual or an organization to evaluate the need of biometric products with respect to specific requirements. The product selection must be a careful process so that expected returns on the investment can be achieved. This guide has been designed to help the prospective users of biometrics to investigate various aspects of implementing biometrics.

The guide will help you to take into account various aspects that can form the basis of choosing the most rewarding biometric solution that can fulfill your needs. As you go through different chapters included in this mini guide, you can find yourself as an informed buyer of biometric applications.

Beginning with the tips to help a biometric user plan for the purchase of biometric product, the guide also addresses other important issues like enrolment process design for the biometric product and technical requirements for the flawless installation of the application in the organization.

Not just that, you can also learn about cost issues as well as the considerations from the user's point of view. This will help you to purchase the biometric product available at reasonable rates and appropriate for your end-user. The guide discussed operational issues as well as the system administration concerns associated with biometric implementation in an organization. All these different issues are addressed in the form of chapters to make it an easy way of learning for novice biometric purchasers and users.

Biometrics can be a miraculous security system for your organization, provided that you are able to find the right product after evaluating it on different basis. You can find this guide useful in taking the right decision in this direction.

Visit techBiometric.Com - Your Gateway to Global Biometric Business

Chapter I

How to Get Prepared

Preparation is the key aspect of biometric product selection, so that a satisfying experience is obtained at the end of the installation. Take the help of following points to add value to your preparation of biometric implementation.

Why Biometrics

What are the reasons that have triggered your interest in using biometrics? It is a favorable aspect to evaluate the alternatives to biometrics and learn about the pros and cons of each of one of them. You need to ensure that it will be a right decision to choose biometrics for the specific requirements of your organization.



Learn about Legal and Political Issues

Are there any legal or political hindrances in integration biometric with your organizational setup? Apart from this, it is critical to learn about the legislations that will be affected by implementation of biometrics in your organization. For instance, Human Rights Acts and Data Protection Acts are essential to be considered before planning the biometric implementation.

What are the Security Requirements?

What security measures will be adopted by your organization to store the user data locally or centrally? You need to take a look at all the requirements associated with safe and secure storage of data obtained from the users. Apart from this, it is of great significance to learn about the biometric standards as well as those related to information technology. As a biometric user, you will be required to adhere to these standards compulsorily.

Collect the Evaluation Reports

While opting for a particular biometric system, you can collect the evaluation reports of the same from different organizations. Also, you can research and find the quality tests and evaluations conducted on the biometric program that can help you in preparing for the right purchase. Most importantly, learn about the security evaluation of the biometric product available with an organization already utilizing the services of a similar biometric application.

People to Be Consulted

In order to ensure successful implementation of biometrics in your organizational setup, you will be required to seek assistance and consultation from a number of people.

- First of all, you need to conduct a survey amongst the immediate users of your biometric program and learn about their views regarding biometric implementation.
- Next, it is appropriate to consult the biometric project administrators to obtain their reviews about need of biometrics in the specific environment of your organization.
- Locate the biometric administrators of other organizations, especially those belonging to your own niche. This will certainly guide you about biometric implementation in the right manner.
- Biometric Working Group and many other groups can be consulted to add value to your research about biometrics. You can discuss your biometrics model with the experienced people of these groups and obtain great suggestions in this direction.

Important Parts of Preparation

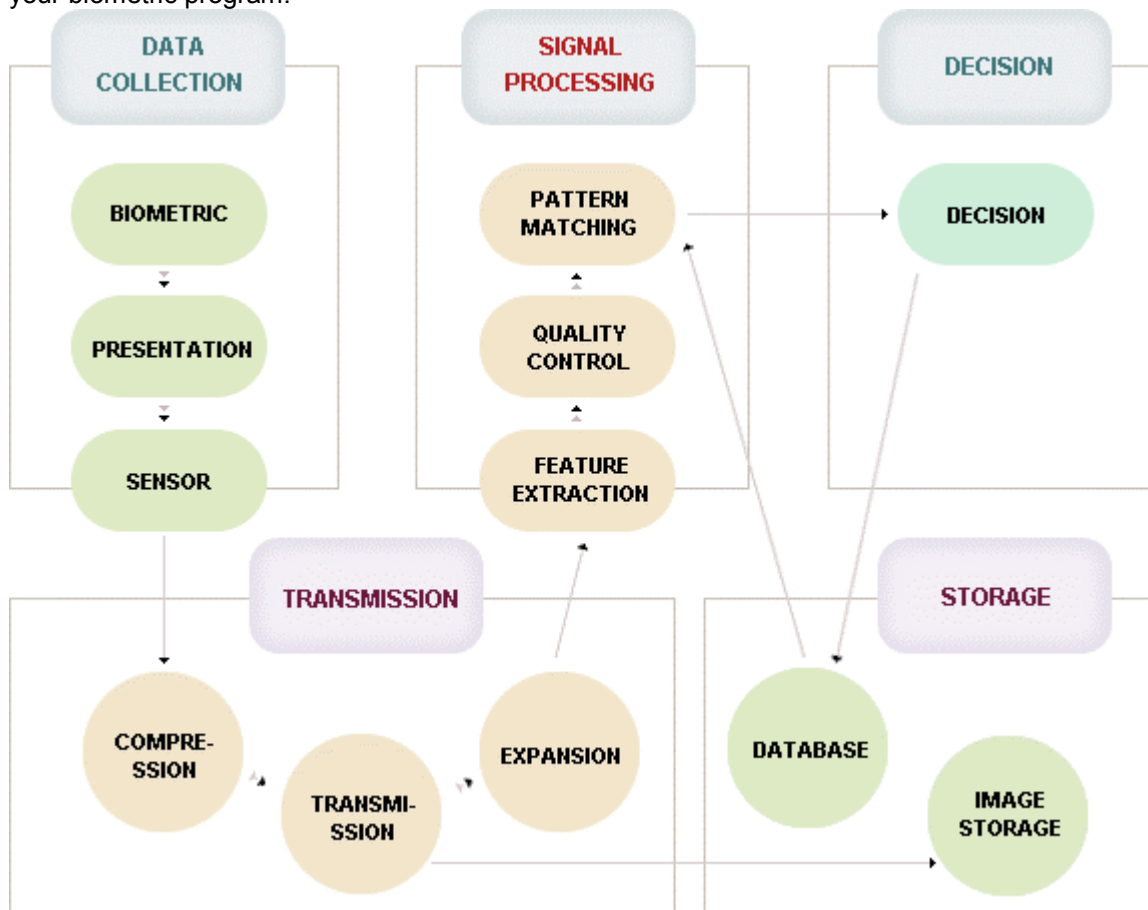
- If you are going to protect government data using biometrics, you need to consult the national policy for ensuring the right move.
- Another important part of your preparation must be the cost and risk analysis to ensure that you are on the right track.
- Most importantly, it is favorable to consider the proposals of more than few vendors, so that you can choose the most appropriate one.
- Finally, don't forget to prepare the evaluation model for the biometrics project and get it reviewed from the administrators as well as other experienced people.

Needless to say, planning is the first step towards installation of a deserving biometric system in your organization. The above-mentioned points can add significant value to your process of planning for biometric implementation. After you go through all these aspects, you need to work upon different issues associated with enrollment process of the biometric product installed in your premises. Refer to the next section to learn about these important issues.

Chapter II

Designing an Effective Enrolment Process

The process of enrolment is critical enough to make proper use of biometrics program installed in the organization. In technical terms, enrolment is defined as the process of registering the users with biometric program and identifying and authenticating them whenever required. So, here are few important aspects that must be taken into account while designing the enrolment process for your biometric program.



Crafting the Enrolment Policy

Needless to say, you need to design an enrolment policy for the users, so that only authorized users are allowed to use the biometric application. For this, you need to take care of following important points.

- Duration of enrolment must be restricted to a specific amount of time, so that it can save the time and make the process highly secure.
- Next, you need to decide upon the number of attempts that must be granted to individual user for accessing the system.
- In case, the user fails in all the permitted attempts, what should be the course of action adopted by your organization?

Handling the Template Database

Biometric templates are created using physical traits like fingerprints, hand geometry, retina features and so on. These templates are stored in the database and the devices like biometric smartcards to help in the authentication and identification process of the enrollees. So, following things must be considered to handle the biometric template database.

- First of all, the appropriate level of security must be applied to keep the template database free from unauthorized access.
- Next, you need to decide the storage capacity of this database to accommodate adequate number of user templates. Also, the future needs for expanding the database must also be taken into account.
- Another important aspect is that whether there will be a centrally located database for the templates or every user will be allowed to carry a portable biometric template in the form of devices like smartcards.
- Apart from this; you need to assess the need of preserving the number of templates per user. For instance, you can create the templates using finger prints only or you can use multiple templates per user that might include templates for left eye, right eye and one finger.
- Also, it is of great significance to decide the number of instances required to create the biometric templates of different users. For instance, some biometric products allow only one reading of the finger print to create the template. On the other hand, there are products that combine multiple readings of the fingerprints to create a single template.

Deciding the Human Intervention

You can decide upon the need of human intervention during the operation of biometric application installed in the premises. For install, you can decide whether you need to employ a supervisor for the process of installment. If yes, then you need to decide upon the level of training that must be offered to the supervisor for handling the process efficiently. Also, the person hired for this task must be trained to maintain the template record on the regular basis. You can discuss with the system administrator about the need of a human operator for the process of enrolment.

Other Important Enrolment Issues

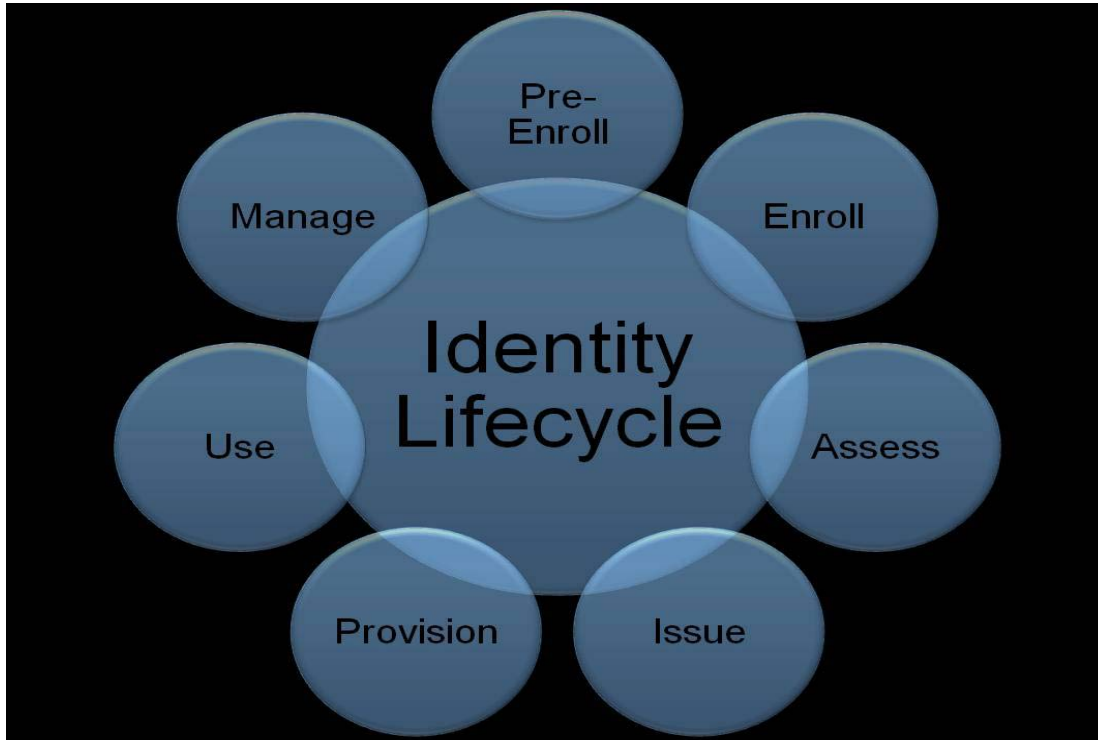
- Another important point is to consider the effect of environmental factors on the process of enrolment. Temperature, light, atmospheric pressure and other important issues must be addressed while designing the enrolment process.
- Also, it is important to consider the validity of a particular template. The physical traits of a user might change with the passage of time and thus, it can hinder the process of biometric authentication and identification. So, decide upon the time period after which, the user will be required to get the biometric template renewed.
- Deciding upon the database backups is another critical aspect of designing the enrolment process. Equally important is to consider the recovery performance of the biometric application to handle the undesirable data loss situations.
- Finally, the role of the vendor must be considered in supporting the process of enrolment. Make sure that the vendor provides you with proper control and quality feedback at regular intervals of time.

For installing the biometric application, you certainly need to consider the technical issues and aspects related to this process. For this, you can refer to the next chapter of this guide and learn some important issues in this direction.

Chapter III

Evaluating the Technical Requirements

Biometrics is purely based upon the revolutionary technology and hence, the biometric selection process remains incomplete without considering the technical issues associated with it. However, most of the biometric users belong to non-technical backgrounds and hence, these users often overlook the importance of evaluating the technical side of biometrics applications. The following discussion will help you to have the sound technical knowledge regarding value-added biometric installation.



Computer Resources Required

How much computer support would be required to allow the overall biometric system to perform well for your organization? It is an important aspect that must be previewed before opting for the biometric application for your organization. You can discuss the issue with other organizations having biometric solutions installed in their premises. Also, take an idea from the product vendors to decide upon the type of computer resources to support your biometric application.

Upgrading and Replacing

Another important aspect that must be taken into consideration is the future needs for expanding the technical resources installed at your premises. For this, you need to have conversation with the product vendors to make sure that it would be easy to upgrade the existing technical resources in the future. Equally important is to learn about the replacement of the technical resources, if required in the future. Thus, the choice of the vendor should play an important role in deciding the existing as well as future requirements for the technical resources.

Evaluating Different Features and Facilities

The technical features like data transmission, data translation, data capture and others must be learnt to evaluate the worth of the biometric system being offered by the vendor. Apart from this, you need to have an idea about other features like storage facilities, authentication policy as well as user management. All these things play important role for the biometric application to work wonderfully for the organization.

Cost Analysis

Of course, you need to evaluate the overall cost required to setup the hardware as well as software components associated with biometrics. Apart from this, you also need to take into account the cost required for training your staff. To reduce the cost, you can prepare the list of hardware you already have to contribute towards biometric installation.

Compatibility between Biometric Systems

Another important issue is to consider the interoperability of the new biometric system with the existing applications of the organization. Also, consider the amount of flexibility offered by the biometric system, along with backward compatibility. The exchange of data between two biometric systems in the same organization is another technical issue that must be addressed.

It is very important to consider the above-mentioned technical issues as the base for selecting the most appropriate vendor. Don't hesitate to discuss all these issues with the vendors and compare the information provided by each one of them.

With all these technical issues addressed, you can move towards an important issue of overall cost analysis. While opting for the biometric program, it is of great importance to consider the overall cost required to be spent, along with the desirable returns on the cost incurred. The next chapter will help you to have the cost analysis for biometric installation in your organization.

Visit techBiometric.Com - Your Gateway to Global Biometric Business

Chapter IV

Considering the Cost and the Output Benefits

The cost analysis of installing biometric application at your organization is an important task, as it will help you to decide the worth of the security system you want to install at the organization. Apart from the investment cost, you can also evaluate the biometric system on the basis of benefits offered by it in various terms. The following discussion will help you to have a cost and output analysis of a biometric product while choosing one for your organization.



Factors Contributing to the Cost

First of all, you need to evaluate the factors that contribute towards the cost of installing the biometric application in an organization. From hardware to software costs to investment made on training and maintenance must be learnt from different vendors and the most reasonable proposal must be chosen, without compromising with the quality.

Also, the future upgrading and replacement costs of hardware and software for biometric system must be taken into account. All these factors will help you to decide the right product as well as the vendor for your organization. The cost of providing adequate security to the biometric systems and hiring human operators must not be ignored. A good idea would be to sum up all the costs for different products and then, evaluate the cost differences between these products.

Excepted Benefits from Biometric System

While choosing a biometric product, you are required to ensure that the money spent by you will be returned in the form of deserving benefits. So, what should be the benefits you must expect after installing biometric application in your organization?

- Monetary benefits to make your investment sensible for your organization. The biometric system should help you to achieve the target of high-level security for your organization, so that you don't experience any type of monetary losses.
- Non-monetary benefits like improvement in the image of the organization for taking care of the safety and security of the user enrolled with it. An organization with biometric security installation automatically gets noticed for its concern regarding the security of user data. But for this, it is important to choose the right product that can achieve the good image for the organization.

- The speed and accuracy with which the biometric system performs is another aspect that must be considered while carrying out the cost analysis. The installation of biometric application must not hamper the regular working of your organization.
- Compatibility and ease of use are other benefits you should look for while purchasing the biometric program for the organization. Your staff members must find it easy to use the program and already existing applications should bear compatibility with this newly installed biometric system.
- Most importantly, the biometric system installed at your organization must be capable of providing desired level of security, which is certainly the ultimate target of your organization to achieve.

In order to confirm all these benefits from the biometric system purchased by you, it is suggested to consult the organizations already using a similar biometric system. You can also compare the biometric products and the vendors providing these products, so that a good decision can be taken in this direction. However, it is not a good thing to compromise on the quality of these security systems with the associated costs.

After considering the cost issues, another important set of considerations is related to the end-users of the biometric products. For this, you can refer to the next chapter and learn about the user-related issues that must be addressed while purchasing a biometric system for your organization.

Chapter V

Consider the Requirements of End Users

Ultimately, it is the end user that must be privileged by the implementation of biometrics in your organization. Hence, it is of great significance to cater to the needs of your end users and choose the biometric system according to their needs and requirements. Switching over to biometric security can act as a considerable change for your customers as well as employees and hence, you need to make it as smooth as possible. Here are few tips to assist you in evaluating the exact needs and desires of the end users of the biometric system.



Conduct the Survey

Before you actually make a purchase of biometric product, it is suggested to learn about the product and explain about the same to your regular customers as well as the employees, whosoever would be using the new installation. Make them familiar with the aim of installing a biometric system and also the level of changes that would be induced in the setup. The next step is to obtain the reviews and reactions of the end users. If you find more of the negative response, you need to replace your choice with a better choice. The end user suggestions will help you in taking a better decision.

Educate the Users about Biometrics

Not every person is familiar with biometrics technology, its working and the associated advantages in terms of accurate identification and secure authentication. Thus, before actually introducing the end users to the biometric system, it is better to educate them about the biometrics and its popularity in the real world. This will help the end users to have better understanding of the system as well as your aim for installing it in the organization.

Recognize the End Users

Your employees could be the end users of the biometric product installed by you. At the same time, it could be your business customers, who would be required to use the biometric system. In

any case, it is a critical aspect to evaluate the needs of the end users to make it a value-added decision for the organization.

Evaluate the Acceptance of Biometric Products

Take a look around you and evaluate the acceptance of biometric products amongst the employees as well as the customers of organizations belonging to your own niche. If possible, have a good conversation with these users to have many small reviews about different biometric products. There are higher chances of acceptance of the biometric system, which already enjoys a higher level of acceptance amongst the end users of other organizations.

Probability of Fraudulence

What is the probability of fraudulence behavior of the end users associated with your organization? Take a look at the past records and this will help you decide the level of security you expect from the biometric installation. Also, decide upon the appropriate way of dealing with the end users found guilty of showing such behavior.

Type of Training Required

Will you be required to arrange for extensive training for the end users to use the biometric system properly? The cost of providing training to the end users and also the level of efforts required in this procedure are the factors that must be analyzed before choosing the biometric program with specific level of sophistication.

Physical Traits Used

Which physical traits of the end users will be utilized by the biometric system for preparing the biometric templates? It is important to choose the biometric product that is applicable to majority of end users associated with your organization.

The habituated and non-habituated nature of the end users must also be considered while choosing the biometric products. As obvious, there will be a mix of familiar and unfamiliar users that would be using the system. So, it is important to inform your vendor about the same and ask him to prepare the proposal for biometric installation, after considering the requirements of different types of end users.

As you finish with this, the next step is to evaluate the operational issues you forecast after the successful installation of biometric products in your organizational setup. You can learn about the biometric products operational issues in the next chapter.

Visit techBiometric.Com - Your Gateway to Global Biometric Business

Chapter VI

What Would Be the Way to Operate

The different biometric systems operate in different manners to meet the specific requirements of different situations and users. Thus, it is very important to consider the operational issues of the biometric product you want to purchase to ensure that it performs exactly the way it suits your organizational needs. Here are few aspects to help you evaluate the operational procedures of the biometric system purchased by you.



Type of Identification

Some biometric products are used for positive identification to grant access to the authorized users. At the same time, there are other systems that are used for negative identification to spot the people with criminal backgrounds. Thus, you should choose the biometric system that performs according to the type of identification your organization want to introduce in its security setup.

If you need to have both positive as well as negative identification, there is another important issue to be addressed. You will be required to decide, whether there will be a single template for both positive and negative identification, or different templates for both the processes.

Type of Environment

What would be the type of environment in which the biometric system will be installed? For instance, your organization might follow a standard or a non-standard environment, which can directly influence the operation of the biometric system installed in the premises. Moreover, you need to decide, whether you want an open or a closed biometric system. In any case, you need to evaluate all the existing aspects in your organization.

Openness of the System

Would you like your biometric system installation to be disclosed to all the employees or you want its operation to be known to reliable users only? For this, you need to select the most trustable

employees of the company, which maintains the efficiency of the system's operations and don't pose any security threat to it.

Also, you need to evaluate the need of human operators for operating the biometric system. While most of the biometric systems can work on their own, you can consider the need of employing human hands to perform different tasks like supervision of enrolment process and maintenance of records. It should be remembered that appropriate training is required to make the human operators eligible enough to handle the operations of a biometric system.

Acceptance of Poor Quality Data

Another evaluation of biometric system's operations is based upon the quality of data accepted by it. You should learn about the system's capability to reject the poor quality data from entering the database. The system should flag the data which doesn't adhere to the standards. Also, it is important to evaluate that how many times the system will flag the attempt of inputting the poor quality data. Purchasing a biometric system on the basis of these aspects will assist in maintaining the efficiency of various operations performed by it.

Different Operational Procedures

Apart from the above-mentioned points, you need to have knowledge about some important operational terms associated with biometric systems to make a good decision in this regard. Here are the most important of these terms and aspects.

- Throughput rate of the biometric system is an important factor which must be evaluated while making a purchase. The throughput rate should be checked for both, the enrolment process as well as during the operational usage of the system.
- False match errors rate defines the number of times a biometric system falsely matches the erroneous data with that stored in the template database. Needless to say, it is an important factor to evaluate the operational performance of a biometric system. For more information on this factor, it is important to discuss the issue with the owners of other organizations that have installed a similar biometric application.
- False non-match defines the number of times a biometric system falsely reject the correct data, even if it matches with the template database. This means that even the authorized users are sometimes denied the access to the system due to erroneous behavior of the system. Again, you can evaluate a biometric system already installed in some other organization on the basis of this factor.
- It is also important to decide the number of times you want the system to tolerate false match errors as well as false non-match errors. This number can help you decide the performance capability of the system in achieving the targets set by the organization.
- Finally, you need to decide how many attempts you want the biometric system should allow an individual to access the system using the biometric data. And what should be the course of action, if a particular user fails in every attempt to access the system. All these factors directly influence the operational behavior of a biometric system.

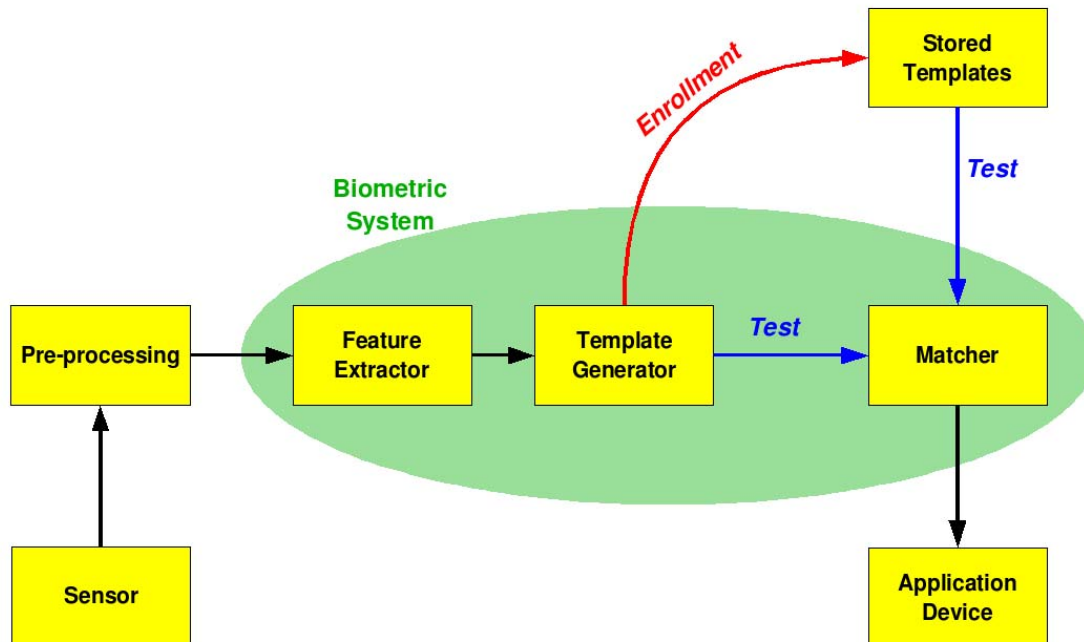
It is true that you won't be able to completely assess the operational behavior of a biometric system, without actually installing and using it for a definite period of time. Still, by learning about these factors and discussing those with the experienced users and the product vendors can help you to bring down the probable disadvantages associated with the operational behavior of the system finally selected by you.

Finally, you need to take a look at the system administration concerns of the biometric system to complete the evaluation process of a biometric system. Continue to read the last chapter of this guide to get familiar to the important issues and concerns in this category.

Chapter VII

The Critical System Administration Issues and Concerns

Biometric system administration is another important part of the overall process of installing such a system in an organization. There are a number of significant points which better be evaluated in advance to avoid any type of distress in the future. Here are some of the most important system administration issues one must address while choosing a biometric system for any type of organization.



Backup Arrangements

Do you need to make backup arrangements for the database prepared by the biometric system? What would happen in the situations like equipment failure? It is important to answer these questions while implementing a biometric system in your organization. Along with it, you need to evaluate the additional costs required to provide the backup support to the biometric system. Also, the need of hiring expert system administrators for this task must be taken into account to have an immediate action during undesirable situations. Backup is also required in case the user data is temporarily unavailable in the original database due to some type of repair or maintenance procedure.

Disaster Recovery Procedures

Needless to say, a biometric system needs to have disaster recovery policy in case the whole of the user data is lost due to a number of reasons. You would definitely not like the idea of obtaining the user templates every time you lose them. So, it is important to ensure that the biometric system has the capability to recover the data after any type of disaster.

Repairs and Replacements

What should be the duration of repairing or replacing one or the other part of the biometric system chosen by you? It is critical to evaluate this factor, so that the working of your biometric system is not interrupted for long period of time. For this, you need to avail the repair and replacement guarantee from the vendor at the time of purchase. Also, you need to have a conversation with the system administrator regarding this issue and use his knowledge to choose a good product.

Assigning Some Important Roles

While choosing a biometric system, it is important to think of different individuals, who will be playing a significant role in using or administrating the system in your organization. Here are the most important role-players in this regard:

- The security officer is required to ensure the physical security of the biometric system installed in the premises.
- Auditors and inspection officers are required to regularly assess the proper working of the biometric system and handle any issue arising out of it.
- System administrator is of course the most important individual, who will be taking care of the overall functioning of the biometric system to ensure security to the user data.

Apart from hiring people for these roles, it is also important to maintain their substitutes to handle the emergency situations. This will help you ensure that the working of the biometric system is not interrupted in any case and your organization extracts maximum benefits out of the investment.

Training the Administrator

The system administrator is required to be trained to handle the working of hardware and software components of the biometric system. This training procedure is also applicable for other members of the staff, who will be using the system for one or the other reason. It should be an ongoing process to train every new employee of your organization, who is inexperienced to use a biometric system.

Automatic Behavior of System

Up to what limit the biometric system should perform automatically? And, what should be the role of system administrator to help the system to perform according to the requirements. Make sure that you go through this aspect while purchasing a biometric product. It depends upon your wish, whether you want the system to perform automatically or you want the intervention of human administrator to a larger extent.

Handling of Invalid Access

Another important concern that must be addressed is that how capable the biometric system is to handle the invalid access attempted by a user. It is favorable to choose the system that automatically locks itself after a particular user fails in all permitted number of attempts to access the system. The role of the system administrator in this situation must also be defined well in advance.

Maintaining the Records

Needless to say, it is of great significance to maintain the records on a biometric system to help the owner of the organization evaluate the system at regular intervals of time. So, it is an important system administration issue that must be addressed using following points:

- How many new biometric templates have been created in a day, a week, a month and so on?
- How many times the biometric templates have been used to verify the attempts made by the user to access the system.
- How many enrolment attempts were rejected by the system in a day or a week and what are the reasons behind this?
- What is the average enrolment processing time utilized by the biometric system? Also, what is the average time utilized by the system to verify the access attempted by a user?
- What types of errors are expected to be shown by the biometric system? For this, you need to learn about different categories of errors from the vendor.
- For what duration of time did the system remain down due to some fault or error experienced by it?
- What is the quality of the biometric template captured and prepared by the system? Do these templates adhere to the quality standards set by the manufacturer?

Handling the Tampering Attempts

The biometric system database can be tampered by an unfaithful employee or an unauthorized user. So, what are the procedures to handle the tampering attempts made on your system? First of all, you need to learn about the tampering prevention technologies that can be integrated with the biometric system to avoid the occurrence of these situations. Another way to avoid tampering is to modify the captured data using codes and encryption keys to restrict the possibility of the data to get tampered.

Above all, the biometric system should come with the guarantee of maintaining the integrity of user data stored in its database. The choice of the vendor certainly plays an important role in addressing all types of system administration issues and concerns.

The process of choosing and purchasing a biometric product requires an organization to put good quantity of efforts. The evaluation tips and factors discussed in all the chapters of this guide can definitely help you in making right selection of the vendor as well as the type of biometric product you want your organization to have. At the same time, you have learnt the role of other individuals and organizations that can significantly contribute towards a good final decision. From end users, employees, biometric experts to the organizations already using similar applications, there are many people and places you need to visit and make the right investment decision.

Remember the fact that buying the best biometric system available in the market doesn't essentially provide the peace of mind. The implementation and installation issues, along with constant support from the vendor and evaluation feedback from the end user and employees are other factors that can decide the effectiveness of a biometric system. Biometrics is certainly one of the most publicized security alternatives an organization can use to avoid any type of security threat. So, making investment in the right type of product can guarantee the success of a biometric system for any type of organization.

Visit techBiometric.Com - Your Gateway to Global Biometric Business

About tectBiometric.Com

techBiometric.Com is the largest single point source catering to - biometric systems manufacturers, suppliers, system integrators & custom developers, companies dealing in access control devices, consultants, biometrics research institutes and trade show/event organizers.

We intend to help biometrics manufacturers, suppliers, designers, buyers and researchers in their different needs and requirements for effectively managing all their operations, marketing their products and services profitably and sharing experiences and ideas with biometrics experts from across the world. The portal makes it easier than ever for -

- The biometric sellers to advertise themselves and get exposure to a larger audience around the world.
- The biometric buyers to locate and purchase various devices & systems from reliable sources.
- The biometrics experts/researchers to publish their profiles and get noticed in front of a wide audience and to make potential customers.
- The biometrics trade show/event organizers to list their events and get noticed by potential visitors & exhibitors.

With late-breaking biometrics industry news and issues, insightful commentary on the new technology developments and innovations, and expert takes on the hottest industry updates, we aspire to be your first stop for what's new and what's next.

We have created this platform for biometrics businesses to search for one another by specifying their needs, while offering credible, efficient and reliable services. Our objective is to dissolve physical boundaries and make process of business simple, easily accessible and free to every individual across the globe.

Contacts

For Advertisements in This Guide Write to Us at info@techbiometric.com

General Information: info@techbiometric.com

Press Releases: pr@techbiometric.com

Event Promotions: events@techbiometric.com

Disclaimer: This is a general information guide for biometric products & systems. The author of this guide assumes no responsibility for the accuracy of the information. Information on the guide book may contain errors or inaccuracies; the sites' proprietors do not make any warranty as to the correctness or reliability of the content of this guide book.

Visit techBiometric.Com - Your Gateway to Global Biometric Business

Important Links

- **Biometric Company Directory:** <http://techbiometric.com/business/companies>
- **Biometric products Information:** <http://techbiometric.com/biometric-products/>
- **Biometric market Reports:** <http://techbiometric.com/biometric-market/>
- **Biometric Press Releases:** <http://techbiometric.com/business/press-releases>
- **Biometric Trade Events:** <http://techbiometric.com/business/trade-events>
- **Biometric Applications:** <http://techbiometric.com/biometric-applications/>
- **Biometric Video Gallery:** <http://techbiometric.com/business/video-gallery>
- **Biometric Associations:** <http://techbiometric.com/biometrics-associations-organizations/>
- **Biometric Expert Panel:** <http://techbiometric.com/business/ask-an-expert>
- **Biometric Articles:** <http://techbiometric.com/category/articles/>

A techBiometric.Com Release June 2009 | Copyright © All Rights Reserved