National Protective Security Authority

Biometric Authentication in Automatic Access Control Systems

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, NPSA accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at *www.npsa.gov.uk.*

Freedom of Information Act (FOIA)

This document is authorised and issued by NPSA.

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from NPSA. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Contents

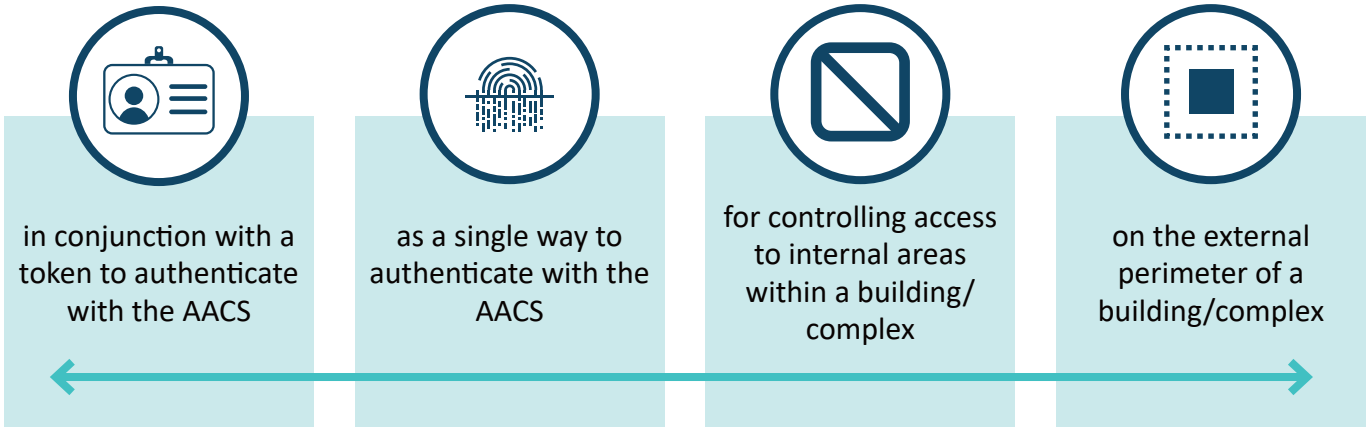
Glossary

Term	Definition
AACS	Automated Access Control System
CNI	Critical National Infrastructure
CSE	Catalogue of Security Equipment
FMNR	False Non-Match rate
FRR	False Rejection Rate
IAPMR	Imposter Attack Presentation Match Rate
NCSC	National Cyber Security Centre
NFC	Near Field Communication
NPSA	National Protective Security Authority
PAD	Presentation Attack Detection
PIN	Personal Identification Number
RFID	Radio Frequency Identification

1 Introduction

1.1 Overview

This guidance document is intended for people designing, building and operating automatic access control systems (AACS) that include biometric authentication. More specifically, it relates to biometric systems that are used:



An AACS is made up of the following components:

Tokens
Physical media (e.g. a smart card) that is presented to a sensor on the AACS; each token is unique and individual

Entrance point
The physical access point to a secured location that is protected by the AACS, usually comprising gates and access control sensors

Database
Contains information about the people that are authorised to use the AACS

Biometric sensor(s) and Processing Application
A system using biometrics to authenticate an individual and to authorise them to pass through a barrier

Communication links
Data links between the building management system, access points and the token and biometric sensors

Power Supplies

1.2 Scope of Document

This document is structured around five main aspects of using a biometric system for automatic access control:

- Selection and Evaluation
- Design and Build
- Choosing a Biometric Modality
- Installation
- Maintenance

2 Selection and Evaluation

The following should be considered when selecting and evaluating the use of a biometric system

2.1 Operational Requirements

2.1.1 Access Control Boundary Location

The function of the access control boundary is to manage access to locations, including internal and external boundaries. The choice of the AACS and biometric design for a particular boundary should reflect the security requirements and the physical situation at the boundary. This includes what it is that the boundary is protecting, the likely threats to the system and the physical location of the boundary.

2.1.2 Performance

The performance of the biometric system is fundamentally important to the security and reliability of the AACS. The biometric system should be able to differentiate between individuals using the AACS and should offer resilience against attacks against the system. The performance requirements will be a function of where and how the AACS is being used.

2.1.3 Usability and Cost

Ease of use, cost and user compatibility should also be considered. The choice of biometric will need to take account of the intended operating environment. For example, a voice biometric would unlikely be used in a noisy environment.

2.1.4 Security Environment

An AACS will typically use one or more authentication factors to identify users depending on the level of security required. Factors can be knowledge-based (e.g., PIN number), possession-based (e.g., access card) or inherence-based (e.g., fingerprint). This is commonly termed as “something you know, something you have or something you are’’. A biometric system is an example of an inherence-based factor.

Something we know

Something we are

Something we have

For low security environments it could be sufficient to use a biometric on its own (single factor solution). For higher security environments a biometric should be used in conjunction with other authentication factors such as a smart card token (multiple factor solution). The choice of a multiple or single factor solution should be based on a risk assessment and the security requirements of the operating environment

2.1.5 Using Biometrics as part of an AACS

Biometric technologies are used to recognise individuals based on biological or behavioural characteristics. The measurement of the biometric characteristic should be unique to the individual and can be used to authenticate them. They are well-suited for use as part of an AACS, particularly in combination with another factor. However, as with any system that involves human interaction with technology, there are strengths and weaknesses in using biometric technology.

2.2 Strengths and Weaknesses

The use of a biometric to authenticate to an AACS offers significant advantages by providing a means to match the person to an enrolled user in a way other factors cannot.

- It cannot be shared (except via a presentation attack), lost or stolen, in a way a physical token can be
- It cannot be shared, forgotten or guessed in the way a knowledge-based authenticator can be
- It is the only way that you can be certain of the physical presence of the enrolled person
- It is unique to the person

However, different types of biometric modalities offer different advantages and disadvantages. These are further explored under section 3.5 of this document.

One of the main challenges of using a biometric is that it is inherently probabilistic

What does this mean?

Each time the biometric characteristic is captured, it will be slightly different to previous times. For example, two face images from an individual will not be identical; they may be very similar but have slight differences in pose angle, lighting or expression, and this would result in different information being captured. This means that the biometric comparison is not between two things that should be identical (such as authenticating using a password or cryptographic key stored in a smart card), and this introduces an underlying error to the system.

Therefore, when considering the use of a particular biometric technology for access control, it is important to understand how great this error is, what impact it may have on the system, and how it should be minimised. Errors arising from biometric systems can be minimised by:

1. Ensuring good quality data is caputred
2. Ensuring a high-quality enrolment template is created
3. Training the user population in how to present their biometric charateristic to the sensor
4. Understanding the trade-off between security and performance
5. Making sure that an appropriate biometric system is selected for the operating environment

2.3 Threats to a Biometrics System

The main threat relates to presentation attacks against the biometric system. This is where an attacker attempts to trick the biometric system into believing that they are an approved user. To mitigate against this, the biometric system must have liveness and presentation attack detection (PAD) capabilities. The performance of the PAD capability should form part of the performance assessment.

The level of sophistication of any attack will likely be related to the value of the environment being protected by the AACS. An assessment of the security of the biometric system should be made using CPNI's test scheme.

2.4 System Performance

Performance is an assessment of the accuracy of the biometric system.

1. **How good it is at authenticating an individual?**
2. **How long does it take to perform the authentication?**
3. **How secure is the system?**

The main measurements used for the performance of a biometric system are:

False Match Rate (FMR) and False Non-Match Rate (FNMR) - Errors relating to the accuracy of the biometric are measured in two ways: FMR and FNMR. The FMR error measures the likelihood that the system will incorrectly match a person to someone that is enrolled in the system that is them. The FNMR error measures the likelihood that the system will fail to recognise a person who has enrolled in the system.

Alternative measures of performance are *False Acceptance Rate (FAR) and False Reject Rate (FRR)*. These are very similar to FMR and FNMR respectively but consider that an individual may be allowed more than one attempt to authenticate. The FNMR records each time an authentication attempt fails, the FRR records the overall false reject rate, including where multiple attempts to authenticate in a session are allowed.

Failure to Acquire/Enrol (FTA/FTE) - The FTA error is where the biometric system fails to capture a biometric characteristic from an individual that is of sufficient quality to be used. An FTE error is where the individual cannot successfully enrol in the system. Where security is not the prime requirement (e.g., in a low security environment) FTA and FTE errors may be a significant factor in selecting a particular biometric system.

Imposter Attack Presentation Match Rate (IAPMR) -This measures the security of the biometric system. It is generally related to the ability of the system to detect deliberate attempts to mimic another's biometric characteristic through a presentation attack. IAPMR error is sometimes known as 'spoofability' and is a measure of how well the biometric system can identify deliberate attempts to spoof the system.

3 Design and Build

This section covers the process of designing a biometric AACS and preparing the system for implementation. It considers the key components required to build a biometric AACS, including:

- Enrolling the biometric characteristics
- Selecting a multifactor solution
- Determining the operating conditions
- Managing enrolments, template storage and data security

3.1 Enrolment

Enrolment of the biometric characteristic into the AACS system should be supervised by an appropriate person to ensure that

- The process is followed correctly
- The system obtains good quality enrolment information
- The person enrolling does not attempt anything mischievous that may compromise the security of the AACS

The user of the AACS will need to enrol in the system by providing one or more measurements of the biometric characteristic to form an enrolment template, which contains features extracted from the biometric characteristic for the individual. This template could be stored in a database within the AACS, an application running on a mobile device or a smart card with a built-in biometric sensor.

When an individual wants to access a place that is protected by the AACS they will authenticate themselves against their template in the system. As the template storage contains sensitive information, both in terms of it being personally identifiable information and security sensitive information, it is very important to make sure it is protected.

3.2 Selecting a Multifactor Solution

It is recommended that a biometric system is used as part of a multifactor AACS. By combining multiple factors in a single AACS, it increases the difficulty to successfully attack the system. It would require the attacker to compromise multiple sources of information, for example, copying or obtaining an individual's smart card token and then reproducing their biometric characteristics sufficiently well to fool the biometric system.

Having conducted a risk assessment and determined the security requirements of the location, an appropriate knowledge-based or possession-based factor can be selected.

- Knowledge-based factors are things like a personal identification number (PIN)
- Possession-based factors are tokens, often in the form of a physical smart card, that contain cryptographically protected information that is unique to the token. A virtual token may be offered as an alternative

3.3 Determining the Operating Conditions

An AACS performs either a

1:1 Comparison (Authentication)

- The user's biometric is compared against a specific biometric characteristic that is enrolled in the system - this is known as authentification
- Comparing a captured biometric to a specific enrolment template is a tightly bound decision

1:n Comparison (Identification)

- Search through a database of enrolled individuals to identify which of them is using the AACS - this is known as identification
- A list of possible matches to enrolled templates is produced, in order of decreasing likelihood of being correct

3.3.1 How to link the multifactor model and the operating mode

Example scenario:

A multifactor solution has been selected for AACS due to one of the following conditions

- The AACS is protecting an external boundary
- It is being used in an unsupervised location
- The AACS is protecting a sensitive or secure location

You implement a multifactor solution with 1:1 comparison

3.3.2 Reasons to use a single factor solution

In some circumstances, for reasons of convenience and speed, a biometric may be used as a single factor

- When the access point is supervised and is not controlling access to a sensitive or high security location
- or as an additional access control measure at the entrance to a higher security area inside a secure location

If a single factor biometric solution is used, it will be a 1: n identification implementation as it will only be using the biometric to authenticate the individual which would result in a check against all the enrolled templates.

3.4 Managing Enrolments, Template Storage and Data Security

3.4.1 Database Storage and Security

Historically, the design of the AACS needs a database of enrolled templates for each person that is authorised to use the AACS. This database must be located securely within the security boundary, and any components of the AACS outside the security boundary must not hold any data. This usually requires a database to hold data for all those enrolled in the system. If multiple locations are served by a single system, either the database must be replicated across different locations, or the systems linked to a central database.

3.4.2 Security for External Components

In addition to the physical location of security-sensitive components of the system, it is important to consider the physical security of any external components, such as the biometric sensor. Anti-tamper security features and protection of cabling are necessary to protect the physical integrity of the sensor.

3.4.3 Physical/Virtual Token Storage and Security

An alternative approach to managing enrolments and templates is to store the biometric on a smart card or to have the biometric sensor on the card itself and communicate the result of the biometric comparison to the controlling sensor. The card may be either:

- A physical token
- A virtual smart card application running on a mobile device

The choice of approach requires careful assessment of both the risks and threats to the system and to the location the AACS is protecting.

3.4.3 Physical vs Virtual Tokens: Advantages and Disadvantages

Physical Tokens

There are two possible approaches to using a physical smart card with an AACS that uses biometrics:

- A physical card used in conjunction with a locally enrolled biometric template
- A physical card that contains a biometric template (often referred to as “on-card biometric”)

The advantages and disadvantages of this approach are

Card used with locally enrolled biometric template

Advantages

- Two factor authentication is used which is considered best practice for authentication security, particularly for locations where security is particularly important
- A compromised biometric will not be automatically accepted at all sites using the credentials. To exploit a compromised biometric characteristic, it would be necessary to target multiple sites which would be very costly and difficult to implement
- Not depending on an on-card solution avoids issues around power supply and processor limitations. This means that there will be no limitations to biometric functionality. In addition, it is possible to update biometric templates and biometric functionality without needing to recall or reissue the token
- There is an easily seen physical sign that the individual has authority to be at the site

Disadvantages

- Users will have to enrol and provide their biometric characteristics at each location they visit, leading to replication of effort and resources, and a degree of inconvenience to the individual

On-card biometric solutions

Advantages

- It is convenient. Biometric authentication will be concurrent with the token authentication and users do not need to perform multiple actions and throughput at the AACS barrier is therefore higher
- A single card can be used easily at multiple locations as the biometric template is stored within the card and is therefore mobile
- Some cards can also include the biometric sensor removing the need for the barriers to have additional hardware

Disadvantages

- Power supply and processor limitations. The card will depend on the contact or RFID interface for power, meaning there will only be limited processing capability, which could affect the level of sophistication of the biometric authentication
- Additional costs for more complex cards compared to standard RFID tokens especially if it includes the additional complexity of having a sensor embedded in the card
- Compromise of the card affects all sites it is used at, and a lost card would require re-enrolling the biometric characteristics
- Attackers can target in-depth attacks on biometric template security within the card either through a presentation attack or by breaking the chip security
- Cards with integrated sensors are limited to fingerprints

Virtual Tokens

There is an increasing trend for virtual tokens to be used, typically based on mobile devices, where the mobile device serves as the user's credential and communicates with the sensor via RFID, NFC or Bluetooth.

Virtual Tokens

Advantages

- It is less likely to be lost, mislaid or stolen
- The virtual token can benefit from security features found on mobile devices
- The token is presented in a convenient form that people are familiar with

Disadvantages

- Not having a visible physical pass when within the security boundary. It is not immediately clear whether the individual has the authority to be there
- The binding of the virtual token to the device, which could lead to practical issues in the event the mobile device is lost, stolen or replaced
- Possible cyber security weaknesses against the virtual token app or the wider mobile device

4 Choosing a Biometric Modality

There are several modalities that can be used as part of an AACS. This section covers the following technologies and considerations

- Facial Recognition
- Fingerprint Recognition
- Iris Recognition
- Palm and Finger Vein Recognition
- Privacy and Data Protection
- Exception Handling

The biometric performance requirements are related to various factors:

- **Is it easy to use the biometric capture device?**
- **Is everyone able to provide the biometric characteristic?**
- **How accurate does the biometric modality need to be?**

  The accuracy of a particular biometric modality will affect both the security of the system and its useability. If there is a relatively high False Non-Match Rate, it will require multiple attempts to authenticate by legitimate users which will slow down the throughput of the AACS.

  Security will be affected if the False Match Rate is relatively high as it will make it more likely that an imposter may successfully authenticate to an enrolled template. This is also relevant to deliberate attempts to fool the system via a presentation attack, with different biometric modalities having different levels of resilience.

- **What are the environmental conditions where the AACS will be used?**
  The environment in which the AACS is located is also important and may have a significant influence on what is possible or practical. This could include influencing the system's ability to capture biometric characteristics accurately or safely (e.g., it would not be desirable to have a contact-based sensor in an infectious disease laboratory)
- **How long does it take to process the biometric characteristic?**
- **How acceptable is it to the user population?**

  There is a relatively small number of biometric modalities that are usually considered for an AACS. Those that are generally available are explored in the next subsections.

4.1 Facial Recognition

Facial recognition systems may be 3D or 2D, and commonly uses digital photographs or video to capture images. Visible light and infrared may both be used during this process.

Consistency of pose, lighting and facial expression is critical to performance and reliability.
The photograph used to enrol into the system must also be recent. These requirement can make this system difficult to manage in an access control application.

About the technology:

Approaches to facial recognition have changed rapidly in recent years. Newer systems, based on artificial intelligence or machine learning techniques, are trained on large numbers of face images (typically hundreds of thousands of images).

These systems can work quite accurately with high resolution (more than 100 pixels between the eye centres), full frontal images in good lighting. However, performance degrades as resolution reduces, pose angle increases or lighting varies.

Face biometric system performance is also very sensitive to the data used to model the face characteristics and care needs to be taken to avoid introducing a performance bias as a result of poor quality or non-representative training data. This could be because the training data is not representative of the target user population, meaning the system would be prone to higher errors for part of the population due to not being properly trained to recognise the range of people using it. Demographic bias is usually one of age, gender or ethnicity; it is very important that any system does not demonstrate any bias as it will lead to higher errors and will be inherently unfair against part of the user population.

Advantages

- No specialist equipment required, just camera
- Everyone can provide face biometric characteristics
- Easy to capture images of face

Disadvantages

- Presentation attacks are relatively easy to perform, especially on unmonitored AACS
- Accuracy is not as good as other modalities e.g. iris
- Care needs to be taken to avoid introducing a performance bias e.g, demographic base

4.2 Fingerprint Recognition

In access control applications, users place their finger onto a fingerprint sensor. The sensor may be:

Optical
a photographic image of the fingerprint is captured

Capacitive
the conductivity of the skin is used to capture where the fingerprint friction ridges are in contact with the sensor

Ultrasonic
high frequency sound is used to capture the fingerprint pattern using measuring reflections of the sound wave from the finger

About the technology:

Fingerprint systems analyse the locations of "minutiae" – the endings and branching or splitting of the friction ridges on the pad of the finger. Often, additional information, such as the number of ridges between minutiae points, is also used.

Advantages

- Relatively accurate modality
- Capture technology is cheaper and faster in comparison with other modalities
- Easy to capture fingerprint characteristics

Disadvantages

- A proportion of the population will not be able to provide good quality fingerprint characteristics
- The limited size of many fingerprint scanners means only a part of the fingerprint pattern for an individual may be captured

4.3 Iris Recognition

About the technology:

Iris recognition devices take a greyscale photograph of the iris pattern using an invisible and harmless infrared light source. Iris melanin is transparent under infrared illumination. The use of infrared illumination is a very important factor in considering the use of an iris biometric system as it makes it equally easy to see all irises irrespective of eye colour, which is not the case with the visible spectrum.

Iris recognition algorithms locate the boundaries of the iris and then process the iris portion of the image to provide a distinct and concise representation of an individual's iris pattern. This representation offers a very high level of discrimination between individuals within a population.

Advantages

- The most accurate of all modalities
- Can differentiate between individuals in a large population

Disadvantages

- Relatively complex compared to other biometric modalities because specialist equipment is required to capture images
- Difficult to accurately locate the iris within the periocular region and then extract the iris image
- The image can be obscured by cosmetic contact lenses

4.4 Palm and Finger Vein Recognition

About the technology:

These modalities are based on the images of veins in the hand or finger. The system exploits the fact that veins absorb more infrared light than other types of tissue, which makes it possible to capture the vein pattern beneath the skin. The hand or finger is illuminated with low intensity infrared light. The light absorbing veins return a dark pattern against the more translucent skin and other tissue.

The blood vessels just under the skin form a distinctive pattern for each person. Vein patterns can be captured by illuminating a body region with infrared light and photographing the reflected light.

In some systems, photographs are taken of the infrared light transmitted through the body tissue being imaged. Blood vessels absorb infrared light more than the surrounding tissue and appear darker in the acquired image.

Advantages

- Vein patterns have a particular resilience to presentation attacks
- Accuracy is relatively good, being largely comparable to face biometrics but not as accurate as fingerprint or iris modalities

Considerations

- Products are designed to work with body parts that can easily be presented to the sensor, including palms, fingers, wrists and the back of the hand

4.5 Other Modalities

Several other biometric modalities are used in non-AACS applications:

- **Voice biometrics** are widely used in telephone banking applications but are not suitable for physical access control applications as they are very sensitive to interference from background noise
- **Hand geometry** has been used in physical access control applications in the past, but it does not provide the level of uniqueness across a population and there are few, if any, implementations in use at this time
- **Palms** (the surface features as distinct from palm vein patterns) have become an area of interest in recently but this technology is largely experimental and is unproven as a large-scale biometric

While some of these are likely to always be impractical, some technologies may mature to the extent that they are viable options. A flexible approach to currently unproven modalities is encouraged.

4.6 Privacy and Data Protection

Biometric characteristics are sensitive personal information and there are several legislative and statutory requirements for the protection of this data.

You should take expert advice on the implications of these for your specific context.

4.7 Exception Handling

There will always be some people who struggle to use a biometric system. It might be because their biometric characteristic is damaged or is of poor quality. For example

- A bricklayer or baker could have damaged fingerprints due to the nature of their work
- The individual may be missing fingers
- The individual may have a medical condition that makes it difficult to use the sensor (arthritis can make it very difficult to get a finger in the correct position to capture a print).

In some cases, it is simply that the individual does not have good quality biometric characteristics and the biometric system will struggle to authenticate them.

The proportion of a user population that cannot use the biometric system will vary depending on the modality. In this case, the system should have a suitable exception handling system. The overall solution and individual components should not discriminate against any individual. Sites will need to make reasonable adjustments to 'assist' those that cannot use the biometric system and are instead utilising the exception handling process. This is likely to put an additional burden on the access control staff/ security officer. It is for this reason that a well specified and designed biometrics system should be deployed.

An exception handling system should not be less secure than the biometric system, although it can be accepted that it may be a less convenient authenticator, for example taking longer to process than for the biometric system. If this is not the case, it will introduce a significant vulnerability to the AACS as attackers will avoid the biometric authentication method and use the weaker exception handling route.

5 Installation

This section covers the practical considerations and necessary steps for installing and maintaining an AACS that includes biometrics, including:

Ensuring accuracy and security in the operational environment

Installation of the biometric system

5.1 Ensuring Accuracy and Security

The main purpose of the biometric component of an AACS is to provide the means to authenticate an individual against an enrolment template. This will allow the AACS to verify if the person presenting the biometric characteristic at the access point is authorised to enter the location. The overall security of the AACS is completely dependent on the biometric component working as expected. Therefore, it is essential that the biometric system is evaluated to ensure that it meets the operational requirements.

As described above, performance is characterised in terms of accuracy (FMR error and FNMR error) and security (usually measured in terms of IAPMR i.e., how successful the biometric system is at detecting presentation attacks).

A biometric system should only be used if it is available in the NPSA Catalogue of Security Equipment (CSE), which will ensure it has been independently tested and proved capable of meeting the requirements for a biometric-enabled AACS for a Critical National Infrastructure (CNI) operational environment. Using a biometric system from the catalogue, provides the certainty that it will work as expected and will meet the performance requirements set out.

5.1.1 Assessing Suitability

NPSA has a test scheme to provide a framework for assessing the suitability of a biometric system for a particular operating environment. The assessment considers the likely level of security required, possible threats to the system and possible threat actors. Inclusion in the CSE is dependent on successful assessment of the biometric system against the requirements specified in the NPSA test scheme. Testing of the biometric functionality should focus on accuracy and security. There are other aspects of performance that could be considered such as speed of operation or ease of use, but they are generally not a significant factor in assessing suitability.

5.1.2 Understanding and Managing Risk

Presentati on att acks, parti cularly at CNI locati ons, are a signifi cant risk to a biometric AACS. It is therefore criti cal to understand the level of risk posed by an att acker, based on their capability, resources and the ti me required to implement an att ack. Performing a risk assessment on the system, including likely threat actors, identi fi cati on and miti gation of risks, and any residual risks that must be controlled will ensure the security of the system is managed eff ecti vely.

Aside from the output of a risk assessment, other factors, such as whether an access system is unsupervised, will aff ect the overall risk, what form presentati on att ack detecti on needs to take, and defi ne the relati ve prioriti es in assessing the security of the system.

The FMR and FNMR errors should refl ect the risk assessment for the operati ng environment, which will be a functi on of the building being protected, the physical locati on of the site, and the sensiti vity of acti viti es taking place inside it.

5.1.3 User Behaviour

It is important to consider how users interact with the biometric system over a prolonged period. Users will usually become accustomed and will learn how to present their biometric so that authenti cati on takes places successfully and swift ly.

To gain the benefi t from a biometric system, the AACS needs to miti gate double entry. The access control point should not allow people to tailgate thereby bypassing the biometric sensor.

5.1.4 Security

The biometric sensor must have anti-tamper devices fitted to detect the opening or removal of them from their mountings. Further guidance can be found in the NPSA AACS guidance document and standard.

Alarm signals for the biometric system will include spoof alarms (which will alert a security offi cer in the event the presentati on att ack detecti on identi fi es a possible att ack) and tamper alarms of the biometric device.

5.2 Installation

The biometric system should be installed in accordance with the manufacturer's recommendations. If these are not followed, problems of responsibility could arise if the system fails to perform as expected and functionality would very likely be impacted.

The biometric sensor, wider AACS networks and token parts of the system must be physically separate, although they may be contained within a single housing.

The overall design of the system will be a function of the security requirements of the environment being protected. In higher security environments the storage of biometric enrolment references, system settings and data network must be stored on the secure side of the perimeter being protected by the biometric system. In some circumstances, the biometric template may be stored on an AACS token but only if the risk assessment does not preclude this, as this could be a less secure option.

IP connections between the sensor and the rest of the system should be protected in accordance with NPSA guidance for running security systems over IP networks.

5.2.1 Configuration

Biometric systems should, wherever possible, be set to perform authentication (a 1:1 comparison against the biometric template of a single individual) rather than identification (a 1: n comparison against the biometric references of everyone that is enrolled), unless the physical access control system is protecting a low security location where a single factor biometric solution has been approved to be used.

When a multifactor is being used the AACS must ensure the biometric template is linked to the other factors so that authorised personnel cannot swap factors and still gain entrance. The specific biometric enrolment template for an individual should be linked to a specific token that was given to the same individual and subsequently linked together.

The number of attempts the biometric system should allow is an important security consideration and should form part of the risk assessment preceding design and implementation of the system. If only one or two attempts are allowed, there is a risk that the user would be locked out of the system and unable to gain access if the biometric system makes an error in capturing their information (FNMR are typically of the order of 1-5% so a person could be locked out 1 in every 20 attempts). Allowing too many attempts would weaken the security of the system and an attacker could keep trying to gain access with the possibility that a random attempt is successful.

Where passwords are used to control administrator or security officer access, they must be changed from the default supplier password, and should follow NCSC (National Cyber Security Centre) password guidance to ensure they are appropriate for use.

5.2.2 Commissioning

Commissioning tests shall be carried out to confirm the functionality, security and usability of the system prior to being accepted.

However, some performance aspects will only be confirmed once the system becomes operational. For example, measuring FRR for regular users requires that users have had a period of operational use to become familiar with it. Therefore, performance in operational use should be monitored when the system is live to confirm that performance requirements are being met.

Commissioning tests can also provide performance data which can be used to monitor deterioration in performance and used to justify and plan remedial action.

5.2.3 Enrolment

All enrolments onto the system should be overseen by a trusted person who is trained on how to capture a high-quality biometric reference using the system.

Systems should have the facility to enrol at least two biometric references for each person where applicable. Fingerprint and iris systems should capture multiple biometric characteristics (e.g., left and right eyes or fingers). This is not applicable for face or voice biometrics.

Enrolments shall be logged, including

Supervisor's details

Date and time of enrolment

Test authentications to show the enrolment was successful

Issues or limitations encountered

5.2.4 Response to a Failure to Authenticate

Any failed attempts shall be logged, including

If a user suffers consistent rejection at the point of entry, re-enrolling the individual may result in better quality biometric data and a better AACS performance.

Any alarms from the biometric system, for example tamper, spoof, loss of power, loss of data connection, etc, must be logged and displayed to an operator in a security control room (ideally) or an access control office. These alerts should be monitored 24/7 and/or supported by security guard guidelines and processes.

6 Maintenance

6.1 Updating Enrolled Templates

To maintain the AACS the system must allow the

- Change of biographical information
- Re-Enrolment of an individual's biometric information
- Deletion of a record

Some biometric systems allow for the updating of the enrolled template with each successful authentication. This has the advantage of increasing the number of samples used to define the individual's biometric characteristic and to allow for changes to the biometric characteristic itself over time, e.g., to reflect the ageing of a person's face.

However, there are some disadvantages to this too. The template may be updated with poor quality data that would degrade the representativeness of the template as an accurate reflection of the individual's biometric characteristic. There is also an attack type against the template whereby carefully formed presentation attacks are used to change the template to be a combination of biometric information from different people or even to embody a completely different person.

6.2 Software and Component Upgrades

Software updates and upgrades need to be undertaken to ensure the system continues to function securely. Manufacturer upgrades to software, firmware and components, must be properly authorised before being installed.

Details of any upgrades must be logged, and all biometric data must be securely removed/destroyed from any device being uninstalled.

Engineer access to the system for maintenance may allow access to error logs, and network configuration, but shall not permit access to the stored biometric references or configuration files. This may require that biometric references are deleted from components prior to maintenance and reinstated before the component is put back into use.

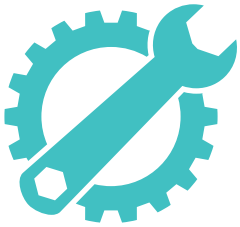
6.3 System Administration

Administration of enrolment and deletion of biometric references, as well as the adjustment of operational parameters of the biometric system should be protected with an authenticator with suitable strength and security. The method of protection must not rely on the same biometric approach that is used for access in the AACS.

It is important that there is a segregation of duties between the administration of the AACS, the person supervising the enrolment, and staff supervising the access point where the biometric is used to reduce the risk from insider misuse of their privileges

6.4 Routine Maintenance

Routine maintenance should be performed to ensure the system continues to operate reliably and securely.



- Follow the manufacturer's recommendations on cleaning the sensor
- Check that audible and visual indicators to users are functioning properly
- Check that tamper resistant fittings have not been breached
- Check that screws, hinges, seals and so on are in good condition
- Check that the system parameters are set to the correct values

6.5 Monitoring Performance

The performance of the biometric system should be monitored to ensure it is operating correctly and within the expected tolerances. Attention should be paid to differences in performance levels and FRR between terminals and over time. Any significant deterioration should be investigated as it could indicate a problem in a particular area, or with a particular terminal.

7 Summary

This guidance document has covered the use of Biometric Authentication in Automatic Access Control Systems. The content can be summarised as follows

Key Points

1. Operational requirements should guide the selection and specification of a Biometric System for AACS
2. Biometric modalities have associated strengths and weaknesses
3. The choice of a multiple or single factor solution should be based on a risk assessment and the security requirements of the operating environment
4. The performance requirements of the biometric system should reflect the risk assessment for the operating environment
5. AACS should be installed following the manufacturer's installation procedures
6. Commissioning tests should be conducted upon installation and prior to acceptance
7. Regular maintenance and testing is paramount to ensure the integrity of the AACS

Further Information

Specialist advice and supporting guidance documents are available from the NPSA website *www.npsa.gov.uk.*

- NPSA Evaluation Standard for Access Control
- NPSA Guide to Producing Operational Requirements for Security Measures
- NPSA Catalogue of Security Equipment
- CAPSS Guidance
- Equality Act 2010
- Data Protection Act
- The National Cyber Security Centre has more information about biometrics recognition and authentication systems and provides a good introduction to the use of biometrics, understanding biometric recognition technologies and how to build secure authentication systems: https://www.ncsc.gov.uk/collection/biometrics
- NCSC guidance to ensure passwords are appropriate for use can be found here: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
- There is a useful guide to the use of biometrics as an authenticator in the GDS digital identity guidance portfolio, which gives useful information about the relative strengths and weaknesses of biometrics and other factors, how to judge the strength of a particular biometric modality or technology and how they should be used to authenticate an individual: https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services