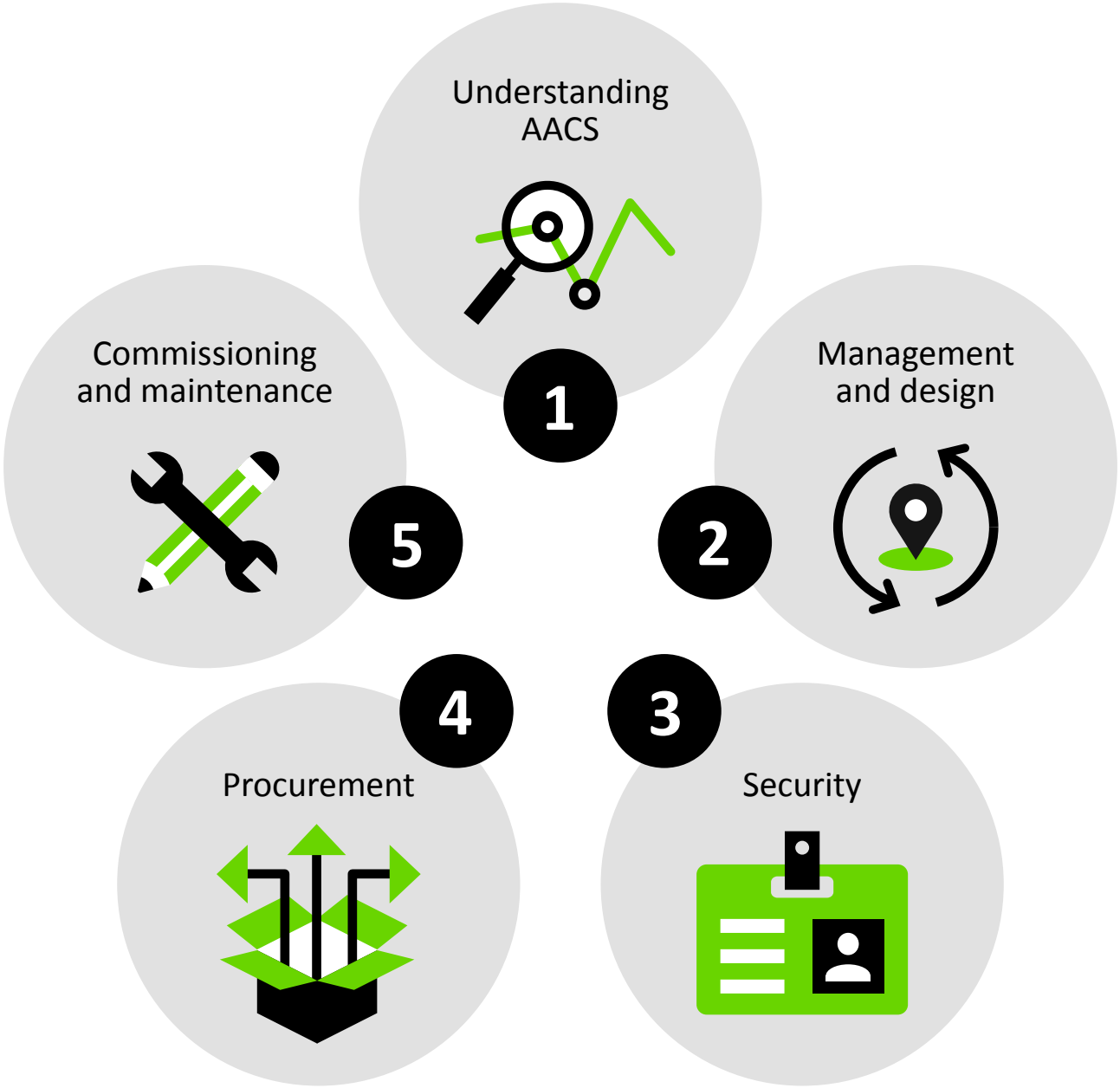
CPNI
Centre for the Protection of National Infrastructure

CPNI Assured Automatic Access Control Systems

For pedestrian systems



Read disclaimer

Disclaimer: This guidance is issued by the UK's Centre for the Protection of National Security (CPNI) with the aim of helping organisations that make up the national infrastructure improve their protective security. It is general guidance only and needs to be adapted for use in specific situations. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any expense, liability, loss or proceedings 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. You should make your own judgement as regards use of the guidance and seek independent advice as appropriate.

1. UNDERSTANDING AACS

INTRODUCTION

Find out about CPNI-graded Automatic Access Control Systems

CPNI GRADING STRUCTURE

Ensure the correct use of the CPNI grading systems

AACS CONCEPTS

Consider the different types of AACS

AACS COMPONENTS

Determine how the system will work and the components needed

ADVANTAGES AND DISADVANTAGES

Weigh up the pros and cons of using AACS

BASIC DESIGN PRINCIPLES

How to select the best AACS

OPERATIONAL REQUIREMENTS

Create a strategic plan of the security needs and define measures required

2. MANAGEMENT AND DESIGN

MANAGEMENT

Understand the users, user interface and alerts of the system

ZONING

Consider assigning areas and times when the system will allow or deny entry

ANTI-TAILGATING

How to prevent a token being used for multiple entries

ANTI-PASSBACK

How to control unauthorised access on a single token

EMERGENCY EXIT

Consider what happens with the AACS in an emergency

SYSTEM DATABASE(S)

Understand how AACS stores their data

UNINTERRUPTIBLE (OR BACK-UP) POWER SUPPLY

Consider a back-up in the event of a mains failure

USER INTERFACES

Ensure that the system is user-friendly

PASSWORDS

Who should have access to the system?

PASSWORD POLICY

How to keep the system secure with passwords

3. SECURITY

NETWORK SECURITY

Ensure that the system is secure against external compromise

TOKENS

Ensure there is a procedure for producing and managing passes

USER ENROLMENT

Establish policies for token issue and use

4. PROCUREMENT

KEY PROCUREMENT STAGES

Consider all of the steps to manage the procurement process

SELECTING A SYSTEM SUPPLIER

What to think about when considering suppliers

DOCUMENTATION

Ensure that the documentation is complete

INSTALLATION

Consider the design requirements when installing a system

5. COMMISSIONING AND MAINTENANCE

COMMISSIONING OVERVIEW

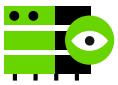
Follow these steps before commissioning

TRAINING

Ensure that there is a system for training users of the system

SYSTEM MAINTENANCE

Ensure the system continues to operate as required



COMMISSIONING OF AACS

Understand the commissioning process

6. FURTHER READING AND GLOSSARY

FURTHER READING

A list of publications and links to help find out more

ABBREVIATIONS AND ACRONYMS

A list of the abbreviations and acronyms used in the document

GLOSSARY

Definitions of words and phrases used in the document

1 UNDERSTANDING AACS

Introduction

A CPNI-graded Automatic Access Control System (AACS) has an intrinsic level of protection that is acquired as a result of the assurance process. An AACS includes restrictions such as limiting user options for PIN setting so that it is not possible to set three repeating digits, i.e. 9996. However, an assured AACS installation can only be created by the use of approved equipment and correctly designed installation, supported by appropriate commissioning and subsequent maintenance regime.

Before considering the installation of an AACS it is necessary to carry out a comprehensive risk assessment to determine the level of security required as an AACS will be only one element of an overall security package. A level 1 and level 2 Operational Requirement must be conducted. The AACS will take into account the operations of the area to be protected, any special features, such as Listed Building status and the need for Heritage Planning or local authority approvals. It is also necessary to consider environmental aspects and the aesthetics of the building or area to be protected.

This guidance document covers physical security, personnel security and information assurance aspects of an AACS. An organisation's information security team should be consulted in the interpretation of the information assurance aspects of the document.

You may also want to read about CPNI grading structure

Go to the start of AACS guidance

Go to the Glossary

CPNI grading structure

CPNI evaluates both systems and components for inclusion in the Catalogue of Security Equipment, (CSE). Two CPNI grading systems, Class Rating and Protection Level, are used depending on the nature of the asset and the threat. Assets can include people, buildings, equipment or information.

> CPNI Class Ratings (Class 1 to Class 4), are focused on the protection of protectively marked material and sensitive information.
>
> CPNI Protection Levels (BASE, ENHANCED and HIGH), are focused on the protection of assets from a forcible attack where the principle attack purpose is asset damage or theft.

The selection of the appropriate CPNI Class rated products or systems will be based on a risk assessment as defined in the Security Policy Framework (SPF) in conjunction with an Operational Requirement based methodology. This risk-based approach takes into account the threat to the site or asset and balances it against the different security measures (guarding, barriers, IDS, AACS etc.) which may be in place.

The selection of the appropriate CPNI Protection Level for products or systems will be made following production of a detailed Operational Requirement (Level 1 and Level 2). CPNI should be consulted to advise on the appropriate Protection Level for the elements to be deployed.

Product and system requirements to meet the specific CPNI Grading are contained within CPNI Standards. Products successfully demonstrating compliance against these standards are listed in the CSE. Selection of products from the CSE should be supported by a performance specification appropriate to the specific application/installation.

You may also want to read about AACS concepts

Go to the CPNI Guide to Producing Operational Requirements for Security Measures

Go to the CPNI Catalogue of Security Equipment

Go to the start of the AACS guidance

Go to the Glossary

AACS concepts

Access control is about managing 'Who can go where and when'. Manual access control measures (barriers, structures, portals, locks and guards) are integrated with automatic access control systems to provide functionality such as automated identification/authentication, audit information and zone controlled access.

Access control is based on the presumption that the boundary of the controlled space is secure and that control is provided at every point of entry. The principal component parts of any access control are:

- a perimeter in which all access points are either secured, alarmed, guarded or access controlled
- a portal (barrier, door or gate) to restrict access
- a means of identification/authentication.

While the above can be achieved by having a guard (or just a lock) at a door, a higher level of access control security may be achieved by the appropriate use of technology. Such systems generally contain a specialised token/card reader which will be installed adjacent to a barrier employing an electrical release mechanism.

Authentication may be achieved by any of the following three metrics. For all CPNI gradings other than protection Level BASE two-factor authentication is required:

Something we know – a Personal Identity Number
Something we have – a token or card
Something we are – a biometric measure

Various permutations of the access token/card system may be considered. In simple terms the authorised person receives a Personal Identity Number (PIN) together with a uniquely encoded token/card, which when presented to the keypad/reader head is passed onto the keypad/reader processing unit. On verification of the user's credentials the AACS automatically allows entry, for example, by releasing the lock on the entry door.

Biometrics may be used within the secure perimeter to provide an additional means of verification. CPNI has a Biometrics Standard which is used to evaluate biometrics for use in access control. A guidance document supports the use of products which are listed in the CSE.

AACS can control access at the perimeter envelope of a building and movement within the building. Where this involves a change in security level the use of two-factor authentication should be considered, an alternative authentication method to that used at the perimeter should be considered.

As an AACS is only one aspect of the overall security arrangements of a building or site it should be designed to complement other measures which are in place, for example Intruder Detection Systems and CCTV, as well as assisting security staff in the performance of their duties.

It should be noted that despite the term 'automatic', an AACS still requires a measure of human supervision. CPNI Protection Level BASE systems must ensure guard oversight of perimeter access during working hours and provide portal over-locking outside normal hours. All other CPNI-graded systems require CCTV coverage or guard supervision at portals and readers which control entry to a higher security level.

Installed systems must be managed in a controlled manner with access to the system being restricted to authorised personnel only.

CPNI recommends that AACS entry points and portals are overseen by either monitored CCTV or guards to enable verification of alarms occurring at entry points and portals. Where half or three-quarter height barriers are used at Protection Level BASE there must be provision in place to detect intruders vaulting the barrier, for example visual detection through guard oversight.

You may also want to read about Components

You may also want to read about Advantages and disadvantages

Go to the start of the AACS guidance

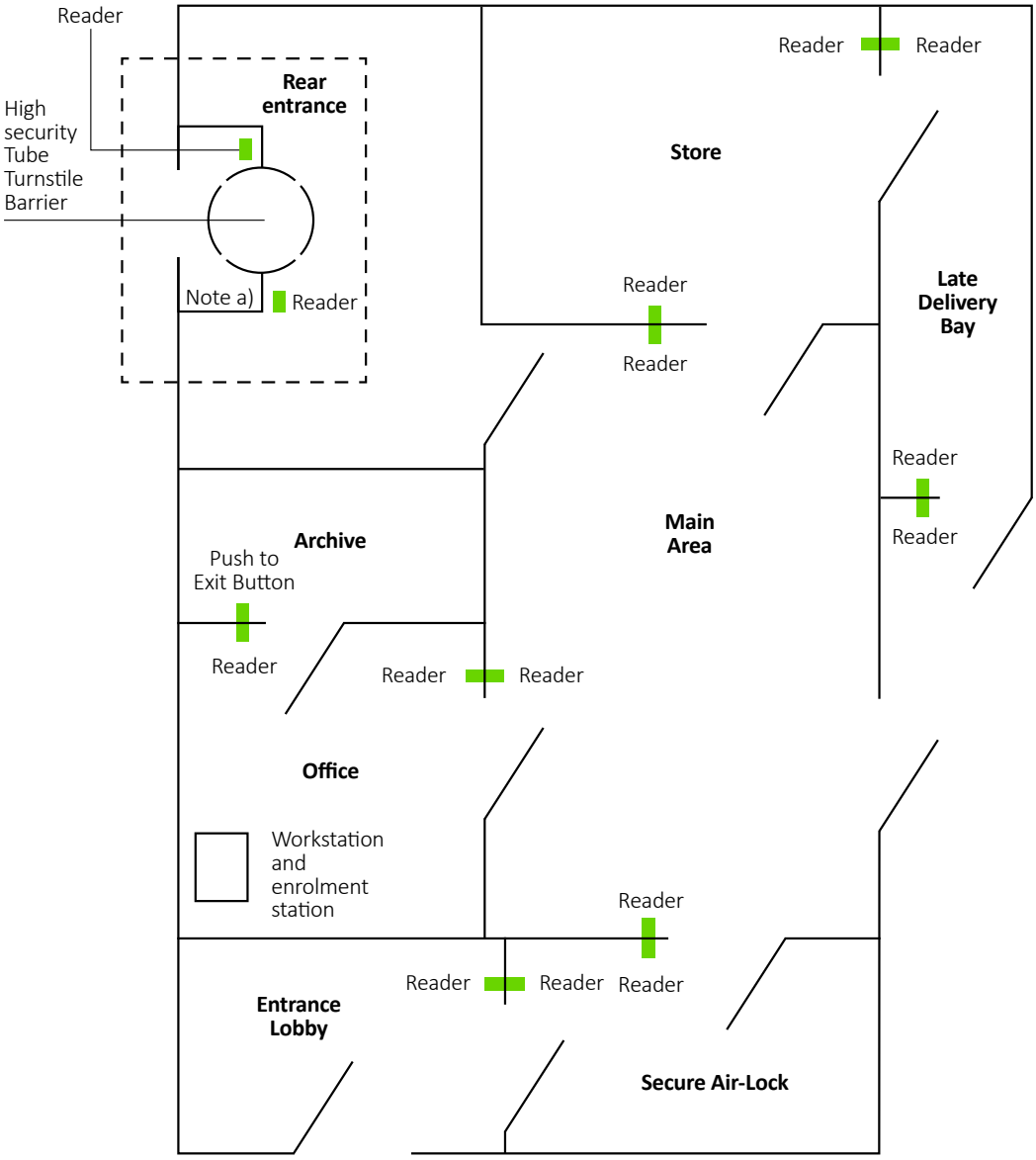
Go to the Glossary

AACS components

An AACS may be considered as comprising a number of separate but integrated components. For an AACS to be effective all the respective components of the system must be of the correct standard and integrate together.

As a simple example, Figure ? shows some of the components which may be used to protect a secure area with two portals providing access.

Components	Consider
Keypads & readers	Means to input user credentials, e.g. PIN, Token or Biometric, for authentication by the controller.
Portal	Controls access to the protected area by receiving release commands from the controller. Anti-tailgate measures, portal type and construction/type of release mechanism to be considered.
Controller	Manages the operation of the AACS to predefined rules, performs authentication, portal release and the processing of AACS alarms. The hierarchy of operation and location of the controller must be considered.
Database	Holds user information and system transactions. May be held locally within a controller, centralised or distributed. Security and resilience of the database to be considered.
Network topology	May be stand-alone or use shared LAN. There are four network topologies defined within this guidance.
Power supplies	May be integral to other components of the AACS or separate. These must have sufficient capacity to supply the load placed upon them and have sufficient reserve capacity to ensure that the system continues to run in the event of a power failure.
Policy	Covers rule-base, time/area definition and database management and should be considered before writing the Operational Requirement.
Procedures & instructions	Must be site specific, i.e. the installer should supply (in addition to the manufacturer's instruction manuals) information regarding the specific use of the system for your site. This should be supplemented with site management procedures written by site management for specific events.



You may also want to read about Advantages and disadvantages

You may also want to read about Basic design principles

Go to the start of the AACS guidance

Go to the Glossary

Advantages and disadvantages

ADVANTAGES OF AN AACS

- AACS are permanent and continue to provide control of entry even in the temporary absence of the guards. However an AACS should not be considered as a total replacement for guards where their use is considered appropriate.
- An AACS is an automatic system; it cannot be distracted, suborned, persuaded or threatened.
- The initial capital expenditure (excluding on-going maintenance costs) is a one-off outlay, as distinct from the recurring costs of guards.
- AACS are programmed to detect the attempted use of passes (tokens/cards) which have been reported as lost or stolen.
- AACS enable an authorised user to indicate that they are being forced to enter under duress.
- An audit trail is provided of the events and actions.
- Zoning of areas is possible allowing higher/selective security.
- Alarms are provided for selected actions/events, for example 'door left open too long'.
- Tokens can be programmed with an automatic expiry date/time.

DISADVANTAGES OF AN AACS

- AACS require human intervention to deal with visitors, deliveries, breakdown of the system and emergencies.
- AACS alone cannot prevent the entry of an unauthorised person in collusion with an authorised person.
- The concept and layout of an AACS together with the measures to control entry and exit may cause some inconvenience to legitimate users causing increased effort and delay.
- Once commissioned, AACS normally operate without direct operator intervention.

However as these systems may comprise complex technical equipment they can, in themselves, demand attention. Operators need to be fully aware of their role and how to operate the system. Adequate system training should be given to both operating staff and management – an on-going requirement – to ensure that they remain conversant with system, operational and management procedures. While reducing guard numbers, the implementation of an AACS may conversely require higher skill levels for the remaining staff, reflecting the increased complexity of the system.

- AACS need regular and continuing maintenance. Service procedures for a satisfactory system maintenance agreement need clear definition of the actions required on system breakdown or failure.
- Excessive reliance and/or confidence in the system can cause faults or system alerts to be ignored by operators, especially where such alarm events are regular occurrences and operators have become used to ignoring them.

You may also want to read about Basic design principles

Go to the start of the AACS guidance

Go to the Glossary

Basic design principles

Guards, gatekeepers and receptionists have a vital role to play in controlling entry to sites or buildings or secure areas within them. However to be fully effective they need to be supported by suitable access control systems.

The specification and selection of any AACS depends upon a number of factors relating to the Operational Requirement and specific local circumstances:

- the activities undertaken at the site/building
- defined area(s)
- specific assets requiring protection
- defined threat
- personnel on site
- response force arrangements
- alarm reporting method
- integration with other types of equipment or systems
- environmental conditions – while normally installed within environmentally controlled situations this may not always be the case.

> In order to achieve control of access there should be as few points of entry and exit as the site operations and safety considerations allow.

Gates, doors, windows or any other means of entry, together with the means of securing them, should be identified, taking into account the value of the protected assets and the nature of any likely threats.

You may also want to read about Operational requirements

You may also want to read about Advantages and disadvantages

Go to the start of the AACS guidance

Go to the Glossary

Operational Requirements

A specification should be drawn up, based on the outcome of the level 1 and level 2 Operational Requirement. This should include all the critical design elements required but will leave the responsibility for a final working design with the contractor.

Generic guidance on the preparation of operational requirements is given in CPNI's Guide to Producing Operational Requirements for Security Measures. The following items are addressed using the level 2 Operational Requirement which should be completed with reference to the principles in this document:

- Definition of the area into which access is to be controlled - include a sketch or drawing of the area indicating all proposed points of entry and exit.
- Definition of user groups to whom the control of access is to be applied – include numbers and peak flow rates.
- Definition of the control restrictions that may be applied - include zoning and anti-passback boundaries.
- Outline of responses to certain circumstances - include anti-passback reset following network failure, system failure or evacuation.
- outline of any design constraints which may be known should also be identified – include requirements under The Equality Act 2010 and requirements of network design;
- for systems being installed on existing sites it is important to identify what existing measures will remain when the AACS is implemented - include where existing portals, including means of escape, are to be retained.

You may also want to read about Management

Go to the CPNI Physical Security website

Go to the UKPGA website

Go to the start of the AACS guidance

Go to the Glossary

2 MANAGEMENT AND DESIGN

Management

ROLES AND RESPONSIBILITIES

The roles and responsibilities for the secure operation of an AACS are defined in the password tree. Each role will have a defined username and passwords should be chosen in accordance with the policy. Organisations should run the CPNI personnel security tools to determine their personnel security risk profile and particular attention should be paid to the AACS roles defined in the password tree.

USER INTERFACE

User interfaces must be clear, displaying relevant information to the operator. The user interface should assist the operator in their decision-making process, enabling the appropriate response to be deployed.

The use of multiple sensory indicators (audio, visual) should be considered to ensure a timely response to alerts. Actions which operators might be expected to perform may include:

- acknowledge or accept the alert event (silence any audible signal)
- deploy the required response to the alert event
- add any extra details to the alert log (e.g. observed cause of the event)
- reset the alert event when the incident is resolved

ALERTS AND AUDIT LOGS

AACS generate alerts and audit logs. Guards should respond to alerts using standard operating procedures. These must be defined for each of the following events:

- portal forced open
- portal held open (time determined by site)
- revoked or expired token used
- tamper alarms
- anti-tailgating
- unauthorised attempt to access a zone
- duress
- power or network failure

For alert response levels 1 and 2, refer to operational requirements to ensure that the security objective is met.

Consider how multiple alarms are to be processed. Will alarms be stacked or queued by the system and should particular alarms be given higher priority?

Tamper alarms should always be investigated and their cause determined, as they could indicate deliberate sabotage. They should be treated as an attack on the system until investigation of the alarm can determined otherwise.

Audit logs should be reviewed and actioned by the supervisor at the end of each shift to ensure correct operation of the system.

Audit logs can also record details of any changes that are made to the AACS, when and by whom. This will make it possible to identify/audit when changes have been made.

Some systems have tools to monitor behaviours. The use of these tools should only be carried out after reference to CPNI's HoMER guidance document, which outlines the principles of using such tools.

Read more about Passwords

You may also want to read about Zoning

You may also want to read about User interface

You may also want to read about Tokens

Go to the CPNI Personnel Risk Assessment, Pre-Employment Screening, On-going Personnel Security, HoMER and Guard Force Motivation

Go to the the CPNI HoMER guidance

Go to the start of the AACS guidance

Go to the Glossary

Zoning

The system can provide area/time zoning control functions. These are periods when the system will allow or disallow entry/exit. They can be used to simply prevent entry or can generate alarms in the event that a user is within a secured area outside a permitted time. For example time zoning for cleaners between 2000-2400, with access only to non-sensitive areas.

You may also want to read about Anti-tailgating

You may also want to read about Anti-passback

Go to the start of the AACS guidance

Go to the Glossary

Anti-tailgating

For a fully secure system, anti-passback and anti-tailgating should be combined to prevent both multiple uses of token and multiple entries on a single token transaction.

CPNI Protection Level HIGH and Class rating 3 portals provide anti-tailgating features. These portals provide 'one transaction one entry' operation.

Controlled movement of escorted visitors and large items may require an air lock, sometimes referred to as a 'Tiger Trap'. An air lock comprises two portals separated by a secure space where both portals are not permitted to open at the same time. The second portal cannot open until the first is closed. Air locks must be monitored either by guards or CCTV to prevent tailgating.

You may also want to read about Anti-passback

Go to the start of the AACS guidance

Go to the Glossary

Anti-passback

For a fully secure system, anti-passback and anti-tailgating must be combined to prevent both multiple uses of token and multiple entries on a single token transaction.

To prevent 'passback' the system must not let a token be used to gain access more than once without the token then being registered as having left the area. It should go without saying that the individual should have left the area with the token.

Care needs to be taken when defining areas controlled by anti-passback to maximise security and minimise impact on the business.

Anti-passback can be used to stop a single token being used to enable more than one person to enter a facility or to enter multiple facilities. Zoning within a facility can improve the control which passback offers.

Users must swipe in and out of controlled areas; failure to do so may result in them being locked in or out of a particular area. A procedure should be in place to reset a token where this has occurred. Users should be informed that anti-passback is in operation and that they must swipe in and out.

Passback can be enforced at a local level (local anti-passback) and across multiple portals (global anti-passback). A further variation of global anti-passback exists where this is also implemented across multiple sites. Global anti-passback provides greater security but in the event of network failure the system will default to local anti-passback.

CPNI recommends that anti-passback is enabled unless a clear business need can be identified. For anti-passback to be effective the boundary portals for the area which the rules apply must have readers on entry and exit. Within the area push-to-exit buttons can be used.

Following an evacuation, network failure or emergency exit from areas controlled by anti-passback rules, the administrator/supervisor should reset the anti-passback rules. The possible reset conditions are:

- all tokens affected set to OUT
- all tokens affected set to IN
- all tokens affected reset at the next transaction

You may also want to read about Emergency exit

Go to the start of the AACS guidance

Go to the Glossary

Emergency exit

All buildings must comply with Fire regulations and Emergency Exit requirements. Where there is a requirement for means-of-escape it should not rely on the operation of the AACS.

Subject to the specific operational requirements the AACS system can provide for ‘Fail Safe’ or ‘Fail Secure’. In fail safe mode portals will release on system failure; in fail secure mode portals will remain closed.

AACS should not provide the emergency means of escape. Instead, emergency exit should be provided by human operation at portals. When such event occurs portals will signal a door open alert, following which an appropriate response should be defined.

The Equality Act has a number of implications relating to automatic access control systems. In all cases the requirements of the Act must be met.

You may also want to read about System databases

Go to UKPGA website

Go to the start of the AACS guidance

Go to the Glossary

System database(s)

AACS can store their data in a number of locations within the secure area. The databases have been tested to ensure that they are secure and up to date. Any components which have contained or processed the database should be destroyed to CPNI Standards.

Any back-up copies should be afforded protection commensurate with the information contained within them. This applies to their storage and their movement.

The control of the data records must meet the requirements of the Data Protection Act.

You may also want to read about Uninterruptable back-up power supply

You may also want to read about Components

Go to the CPNI Disposal of sensitive information

Go to the start of the AACS guidance

Go to the Glossary

Uninterruptible (or back-up) power supply

Any AACS will require that provision be made to allow operation to continue in the event of a mains failure. This will normally be in the form of a rechargeable standby battery system and which may be further supplemented by other measures. The system should continue in operation until support can be deployed to the site; the minimum time should be determined by the system operational requirement.

You may also want to read about User interface

You may also want to read about Operational requirements

Go to the start of the AACS guidance

Go to the Glossary

User interfaces

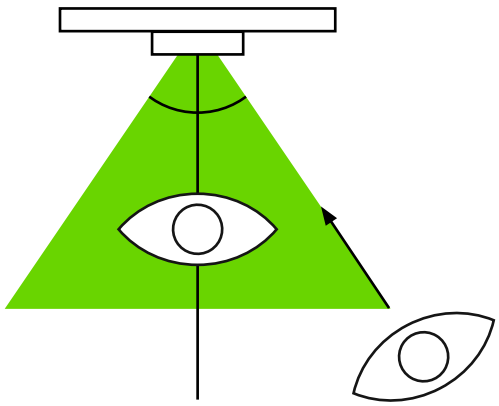
Audible and visible cues should be used at the reader head to enable users to interact with the system.

The Equality Act has a number of implications relating to Automatic Access Control Systems (AACS).

In all cases the requirements of the Act must be met.

Duress PINS can be used in conjunction with a clear procedure and defined response. It is recommended that switching the order of the first pair or last pair of digits is used to minimise detection. In all cases staff must be fully aware of the duress procedure. Where threat from duress has been identified additional measures other than AACS controls should be implemented.

Keypads and readers should be positioned to avoid oversight by any unauthorised persons. Some manufacturers provide options for reducing the risk of oversight; where these form part of a system in the CSE they have been tested to ensure that it is impossible to observe code entry at angles of 30° or greater.



Keypad oversight

You may also want to read about Basic design principles

You may also want to read about Network security

Go to the UKPGA website

Go to the start of the AACS guidance

Go to the Glossary

Passwords

The authority granted to particular users and administrators responsible for an AACS should reflect their specific needs. CPNI has produced the following tree intended to define where specific responsibilities may lie. In practice it is recognised that an individual may have multiple responsibilities but under no circumstances should a 'Super-user' be created who has full unrestricted access to the system.

User	Functionality
Administrator	Data base, configuration files, creation of configuration device/programming terminal, back up, log in engineers, view all logs, connection of external devices/ media
Supervisor	Log in engineers, operational configuration files, alarm suppression, zone de-activation, temporary revocation rights, issue temporary passes, view guard logs, view/print roll call of areas, system status
Guard	Accept & re-set alarms, view alarm logs, incident logs, system status
Enrolment officer	Enrol/revoke users, assignment of user profiles, pin control, production of passes
Engineer*	Error logs , network configuration **Should not access:** Database nor any enrolment officer capabilities, configuration files
Remote engineer*	View error logs/fault data

* Engineer log requires administrator or supervisor authentication

You may also want to read about Password policy

You may also want to read about Management

Go to the start of the AACS guidance

Go to the Glossary

Password Policy

The following password requirements are to be met for systems applying for CPNI Protection Levels BASE and ENHANCED and CPNI Classes 1, 2 and 3.

AACS ISOLATED OR WITH REMOTE ACCESS

- use of a Basic password scheme
- 9 characters in length
- it is recommended that if possible machine-generated passwords are used
- if manual password selection is required, a mixture of upper, lower case characters, numbers and symbols covering all options of a standard keyboard should be used. The passwords should be set by the administrator and not the user to ensure passwords confirm to the Department's password policy
- passwords must be changed at least every 3 months
- account lock out should be set at 3 or 5 attempts

AACS CONNECTED TO INTERNAL ICT NETWORK

- The password system used by the AACS must be at least the same strength/complexity as that used on the internal ICT system. This is to say that both the AACS side and the internal ICT network side must be protected to the same level of that of the highest domain side. This may require an additional CESG approved password product being deployed on Host PCs, and/or use of two-factor authentication.
- For ENHANCED protection level systems CESG-approved password-machine-generated schemes must be used, with two-factor authentication.
- Departments should consult with their IA professionals or CESG consultants if required.

AACS COVERING MULTIPLE SITES

- For systems networked to multiple sites or systems applying for CPNI Protection Level HIGH or CPNI Class 4 the following requirements must be met:
- CESG-approved robust password systems must be used
- CESG advice must be sought prior to deployment of a given system

You may also want to read about Management

You may also want to read about Tokens

Go to the start of the AACS guidance

Go to the Glossary

3 SECURITY

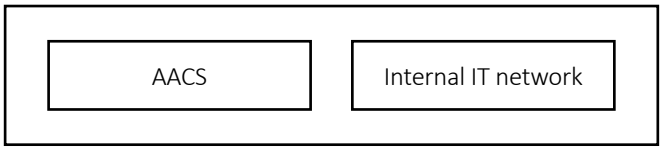
Network security for CPNI-assured AACS

INTRODUCTION

Of particular concern is the threat from external compromise where networked electronic security systems are deployed. The threat can be both to the security system directly or from an attacker using the security system to penetrate other IT networks. In addition to its Top 20 Critical Security Controls and the CPNI Trusted Software Initiative, CPNI has defined four network topologies to assist in the choice of security measures. Further guidance can be found in CPNI's Running Physical Security over IP Networks.

NETWORK TOPOLOGY SCENARIO 1: ISOLATED SYSTEM

The security network is constructed independently from any other network or system and has no external connections outside the protected area.



Security requirements

The AACS forms part of a layered, physical, defence-in-depth approach to security which is designed to slow down an attacker whilst an incident response takes place.

The external facing components of the system are minimised, for example with AACS this would be the token Reader/PIN Pad. All other components, i.e. the wiring, controllers, host computers and network infrastructure are housed within the secure boundary.

Most importantly, the network controlling and monitoring the system is isolated from any main internal network.

No remote access facility is required as part of the system.

Subject to correct physical installation and subject to the equipment being contained within the protected area, no additional encryption for information transmission is required.

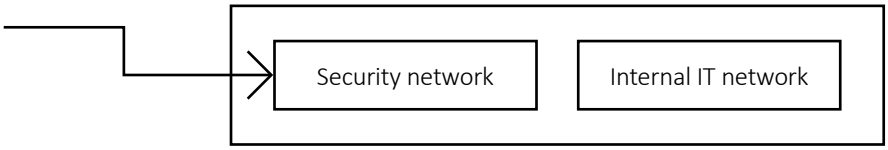
All computer equipment and network switches should be locked down in line with CESG policy.

Where data are held this should be protected to meet DPA requirements.

Encryption of data-at-rest (e.g. the status of data held on a hard drive or other media that is not being accessed by the server) should be deployed as required in line with the Information at Risk Management Lifecycle.

NETWORK TOPOLOGY SCENARIO 2: ISOLATED SYSTEM WITH REMOTE ACCESS

The security network is constructed independently from any other network or system but has external connections outside the protected area. This may be to remote equipment or to allow external access, for example for remote maintenance.



Security requirements

The system forms part of a layered physical, defence-in-depth approach to security which is designed to slow an attacker down whilst an incident response takes place.

The external facing components of the system are minimised, for example with AACS this would be the token Reader/PIN Pad. All other components, i.e. the wiring, controllers, host computers and network infrastructure are housed within the secure boundary.

Subject to correct physical installation and subject to the equipment being contained within the protected area, no additional encryption for information transmission is required to the internal network.

The network controlling and monitoring the system is isolated from any internal network.

A variation of this scenario is the use of the VPN to connect multiple sites together, where control of the system is local but the main site hosts the master database which regularly updates the local databases.

The remote access facilities should be protected with a CESG Commercial Product Assurance (CPA) approved VPN product suitable for the CPNI grade of AACS and the data held within the system. For Protection Level BASE this should be a minimum of impact level 2; for all other CPNI gradings this should be a minimum of impact level 3. In all cases a risk assessment must be carried out to ensure the minimum impact level required for the data on the network is selected. Refer to the CESG website for a list of approved devices.

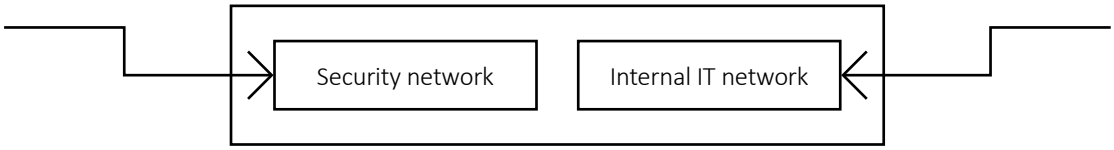
Access for remote users should be granted on a least privilege concept. CESG policy, guidance and consultants should be used to ensure the correct configuration and operation of the VPN connection for organisations covered by the SPF. For organisations not covered by the SPF the usual Information Risk Management process should be followed. Risk treatment could be via CESG engagement or via other means; however it should be treated as part of the overall Information Risk Management Lifecycle.

Encryption of data-at-rest should be deployed as required in line with the Information at Risk Management Lifecycle.

All computer equipment and network switches should be locked down in line with CESG policy. Where data are held this should be protected to meet DPA requirements.

NETWORK TOPOLOGY SCENARIO 3: CONNECTED SYSTEM WITH REMOTE ACCESS

The security network is connected to or shared with other networks. External connections exist outside the protected area. This may be to remote equipment or to allow external access, for example for remote maintenance or be via other networks. The threat comes from compromise of the security network from the shared network and vice versa.



Security requirements

The system forms part of a layered physical, defence-in-depth approach to security which is designed to slow down an attacker whilst an incident response takes place.

The external facing components of the system are minimised, for example with AACS this would be the token reader/ keypad. All other components, i.e. the wiring, controllers, host computers and network infrastructure are housed within the secure boundary.

The network controlling and monitoring the system is connected to the main internal network (LAN) infrastructure by logical separation.

CESG-approved encryption devices for the internal network (LAN) and AACS will be required in order to prevent a pass through attack from either domain and enforce data separation between domains. The attack could be from either:

- the internal network to the AACS controller
- the AACS to the internal network

At Protection Level BASE the encryption devices should meet CESG impact level 2 as a minimum; for all other CPNI gradings the encryption devices should meet CESG impact level 3 as a minimum. In all cases a risk assessment must be carried out to ensure the minimum impact level required for the data on both of the networks is selected.

Data separation between the internal LAN and AACS must be ensured, including the separation of encrypted packets.

The AACS should not be dependent on any components of the internal LAN. Sharing of network resources (such as Domain Controllers) between the AACS network and any non-AACS network is not acceptable.

Remote access facilities should be protected with a CESG Commercial Product Assurance (CPA) approved VPN product suitable for the CPNI grade of AACS and the data held within the system. For Protection Level BASE this is impact level 2; for all other CPNI gradings this is impact level 3. Refer to the CESG website for a list of approved devices.

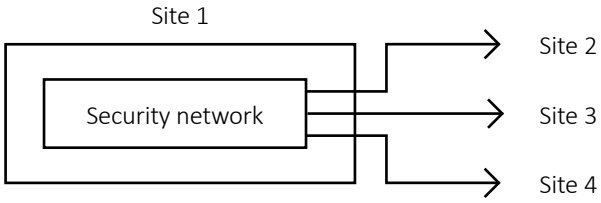
Access for remote users should be granted on a ‘least privilege’ concept. CESG policy, guidance and consultants should be used to ensure the correct configuration and operation of the VPN connection for organisations covered by the Cabinet Office’s Security Policy Framework (SPF). For organisations not covered by the SPF the usual Information Risk Management process should be followed. Risk treatment could be via CESG engagement or via other means; however it should be treated as part of the overall Information Risk Management Lifecycle.

All computer equipment and network switches should be locked down in line with CESG policy. Where data are held this should be protected in line with the SPF to meet Data Protection Act requirements.

Encryption of data-at-rest should be deployed as required in line with the Information at Risk Management Lifecycle.

NETWORK TOPOLOGY SCENARIO 4: CONTROL OF MULTIPLE-SITES

The security network is connected to external locations outside the protected area. These may consist of other networks or systems and will be exchanging information for operational purposes.



Security requirements

There may well be cases where customers wish to connect or control multiple sites on a single Electronic Security System via a WAN or the internet.

The Electronic Security System hosts a master database at the main site. The link between sites may well be over existing Bearer links already used to pass traffic between sites. Data separation between ICT traffic and AACS data must be ensured, including separation of encrypted packets.

If organisations have a requirement for this scenario, advice from IA professionals must be sought and their guidance adequately documented for audit purposes. This scenario would not be evaluated against CPNI Standards and would require bespoke testing.

Where a number of organisations have the same requirement, CESG should be engaged to review the overall architecture pattern used.

You may also want to read about Tokens

You may also want to read about Operational requirements

Go to the CPNI Cyber webpage

Go to the NCSC website

Go to the start of AACS guidance

Go to the Glossary

Tokens for CPNI-assured AACS

DESIGN AND SELECTION

Tokens and readers should be approved by CESG's Commercial Product Assurance process: Foundation grade for protection levels BASE and ENHANCED and Class ratings 1 and 2; and Augmented grade for Protection Level HIGH and class rating 3.

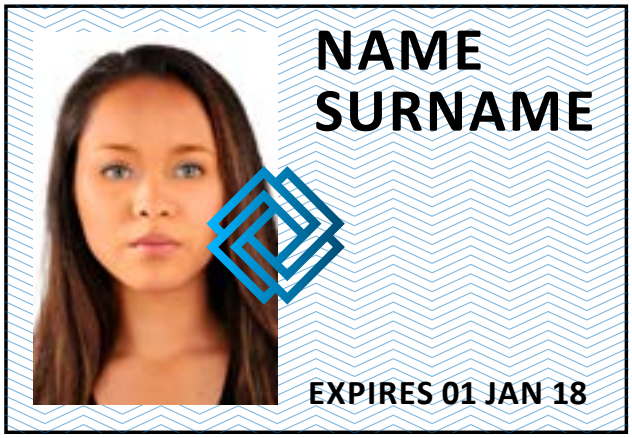
Front of pass

Recommended security features for official photographic building designs are:-

- a validation logo which overlaps the face
- a background design which will deter substitution of the photograph
- a photograph taken in maximum close-up (only head not shoulders) and occupying about one third of the pass area
- a bold design to aid recognition
- an intricate background design and text information written onto the background, to deter forgery
- secure lamination to prevent tampering

Colour coding can be used to distinguish between categories of pass.

The pass design and text should contain no indication of the identity of the issuing department or of the building or site.



Example photographic pass design

Reverse of pass

The reverse of the card should have a unique reference number.

Ref No. _ _ _ _ This is an official document. The unauthorised possession, use, retention, alteration, destruction or transfer to another person is an offence. The loss of this pass must be reported to the Issuing Authority immediately. If found this pass should be handed in to the nearest police station.	Ref No. _ _ _ _ This is an official document. The unauthorised possession, use, retention, alteration, destruction or transfer to another person is an offence. The loss of this pass must be reported to the Issuing Authority immediately. If found this pass should be placed in the nearest post box for return to: Freepost, PO Box . . . . .

Examples of details on reverse of pass

LOST PASS RETURNS

Organisations may operate their own PO Box number for the return of passes. The PO Box should be registered in such a way that the organisation's identity and location is not identified by an enquiry on the Box number. All tokens returned in this manner should be securely destroyed.

You may also want to read about User enrolment

You may also want to read about Network security

Go to the CPNI Disposal of sensitive information website

Go to the start of AACS guidance

Go to the Glossary

User enrolment

ENROLMENT STATION

A separate work station and reader for enrolment should be setup giving the security required. This should be located within the secure perimeter and be protected physically with controlled access.

A clear policy should be defined covering the distribution and control (regular audit) of tokens.

For Protection Level BASE token-only operation is permitted; should PINS be required these can be user generated. At Protection Level ENHANCED, HIGH and Class ratings 1 and 2, two-factor authentication is required and PINS must be machine generated. At Class rating 3 and 4 two-factor authentication is required and secure machine-generated and printed PINS must be issued.

Token blanks should be kept secure at the appropriate CPNI-graded container/lock and only keyed at issue.

TOKEN ISSUE

Prior to enrolment the applicant's identity must be verified using CPNI's pre-employment screening process. A further identity check should be made at the point of card issue.

Permanent staff and permanent contractors

Tokens should be set to expire on security clearance expiry date or contract expiry date. Where neither exists a suitable token expiry date should be determined.

Tokens and PINS should only be issued to the owner. Third party collection should not be permitted.

Escorted visitors

The following should apply to escorted visitors:

- must have a nominated host and prior appointment;
- must be required to produce ID in accordance with CPN's Personnel Security Pre-Employment Screening;
- must not be issued with an AACS token; and
- must be issued with a pass clearly identifying them or an escorted visitor pass should display photo, expiry date and any other information found on permanent staff passes.

A culture of challenging escorted visitors without an escort should be encouraged.

Unescorted visitors

The following should apply to unescorted visitors:

- must have a nominated host and prior appointment
- must be required to produce ID in accordance with CPNI's Personnel Security Pre-Employment Screening
- must be issued with a token reflecting the host organisation's pass design but distinguishing them as an unescorted visitor
- tokens not in use should be given the same level of protection as active staff tokens
- tokens should only be issued to visitors who have the same level of trust as members of staff
- tokens should be set to expire at the end of the working day and be handed in when they leave the site

Unescorted visitors must be informed of the policy on lost tokens and PINS.

Regular visitors

Organisations often have regular visitors who require unescorted access. These visitors should be provided with unescorted tokens and PINs valid for a fixed period of time (3, 6, 12 months). Further limitations such as minimum number of visits within a time frame may also be used, i.e. 3 visits per month to ensure continued validity of token.

The issuing procedure for these tokens should be the same as for staff and permanent contractors. This should include:

- personnel security measures and ID verification
- full background verification of business need and parent organisation affiliation should be conducted
- the parent organisation must agree to inform host organisation of changes to vetting or employment status

A threshold should be set whereby regular unescorted/escorted visitors are transferred to regular visitor status. Regular unescorted/escorted visitor access does not provide the same level of assurance and is therefore a vulnerability.

Contractors (non-permanent)

These users should be treated as either escorted or unescorted visitors dependent upon the level of assurance/trust achieved during their selection.

CONTROL OF TOKENS AND PINS

Staff should treat their AACS tokens as they would their bank cards, keeping them secure when not in use and reporting their loss immediately.

Tokens should be displayed at all times within the building but made secure immediately on leaving the premises. A culture of challenging anyone without a token should be encouraged.

Users should memorise their PIN and securely destroy any paper upon which it is printed. Users should not use the same PIN for any other use.

> Lost or stolen tokens must be reported and removed from the system immediately. If tokens have been misplaced and there is a possibility of compromise, these tokens should be destroyed and new ones (and PINs where applicable) issued.

The identities of staff arriving at site without their tokens should be verified by a member of staff within the building and a record of the verification should be kept; where possible the member of staff verifying the identity should be more senior. The staff member providing the verification should escort the other member of staff immediately to the pass office for issue of a token: a new token if irretrievably lost or stolen and the member of staff has the relevant identification and sponsor as detailed under 'enrolment of permanent members of staff and contractors'; or an unescorted visitor.

The identities of staff who have forgotten their PINs should be verified by a member of staff within the building and a record of the verification should be kept; where possible the member of staff verifying the identity should be more senior. The staff member providing the verification should escort the other member of staff immediately to the pass office for a PIN reset.

Effective procedures should be in place for ensuring that those leaving the organisation are not permitted to retain their tokens. Tokens which are retained should be destroyed and deleted from the system. Tokens which are not retained should be deleted from the system.

AACS will alarm if a revoked/deleted token is used, a clear response procedure should be in place for these events.

You may also want to read about Network security

You may also want to read about Management

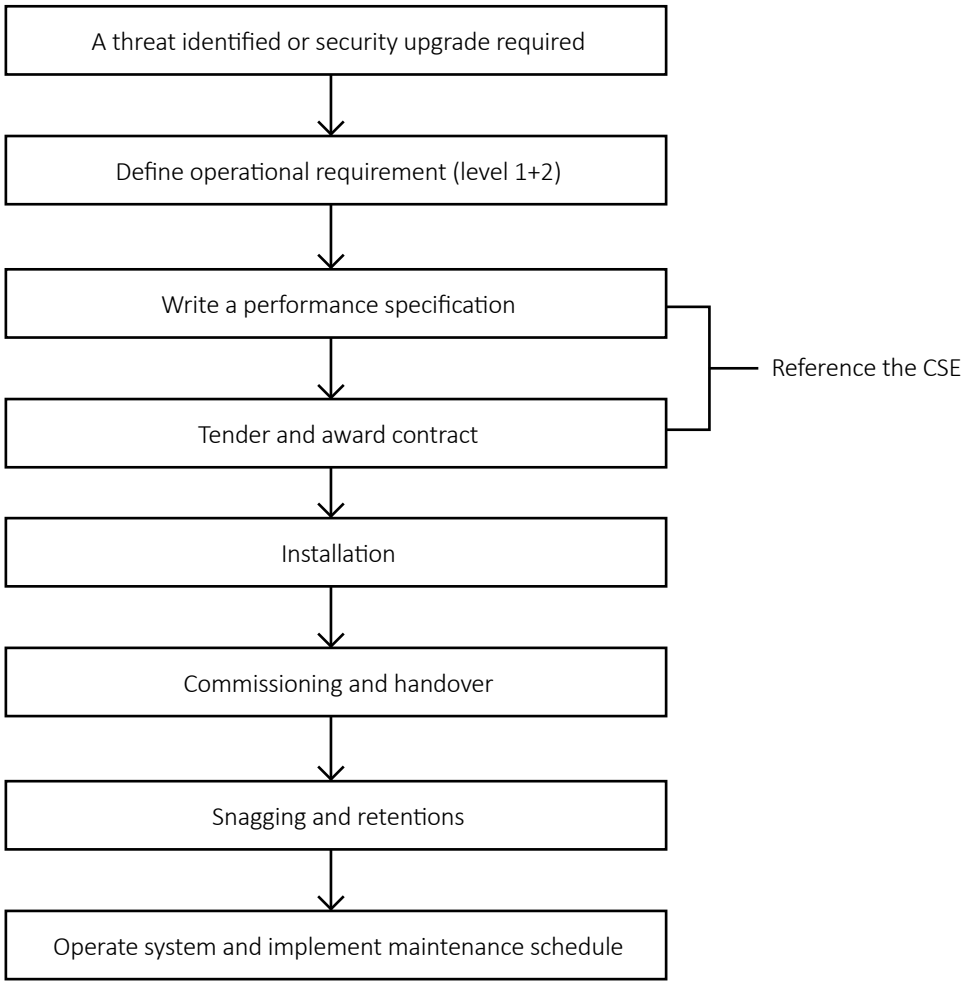
Go to the start of AACS guidance

Go to the Glossary

4 PROCUREMENT

Key procurement stages

When considering the procurement of an automated access control system, the flowchart at **Figure ?** shows the recommended stages for selection and installation. Many organisations may have their own procurement policies in place which will take precedence over this simplified approach.



Recommended stages for procuring an AACS

To ensure success it is essential to involve all the relevant stakeholders: not just the system owner and operators but also those staff who will find themselves, to whatever degree, interacting with the imposed security measures. For many systems, early involvement of trade union/staff associations – and where the public is involved, 'action groups' – will ease the final implementation process.

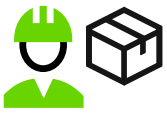
Before attempting to write a performance specification for a new AACS, it is important to ensure that a detailed operational requirement has been produced to provide the necessary details about the requirement.

You may also want to read about Selecting a supplier

You may also want to read about Installation

Go to the start of AACS guidance

Go to the Glossary



Selecting a system supplier

To control the quality of their installed product, some manufacturers operate a franchise system whereby they only supply the product to selected installers who have undergone the appropriate training and have specific product knowledge. This can have the effect of limiting the user's choice of installer/maintainer, but does improve the likelihood of a good installation!

THE CURRENT BEST PRACTICE GUIDANCE IS:

Following the production of an Operational Requirement, the performance Specification should include the requirement for the installed equipment to be chosen from the Catalogue of Security Equipment. Installers invited to compete for the work should be able to demonstrate that the manufacturer of the equipment they are intending to use certifies them as competent to undertake the installation.

Consideration should be given to using an installation and maintenance company which is accredited by a suitable security auditor, such as NSI (NACOSS) or SSAIB.

Once a performance specification has been published and tenders received from competing system installers, the user should assess the bids for technical compliance with the specification before deciding which to procure. It may be prudent to use an appropriately qualified consultant to assist with the preparation of the tender documentation and assessing the competing quotes.

You may also want to read about Documentation

You may also want to read about Installation

You may also want to read about Operational requirement

Go to the start of AACS guidance

Go to the Glossary

Documentation

Manufacturers of the proposed AACS should provide the documentation listed below to ensure that informed decisions can be made regarding the system's suitability and the accuracy of the information provided in the tender documentation.

- details of any certification or formal testing from approved bodies (including CE Certification) or declaration of conformity
- a list of approved suppliers, installers and maintainers
- procedures, manuals and drawings for installation, commissioning and maintenance
- a parts list – availability, cost, ease of replacement
- a price list
- Details of health and safety issues associated with the installation, running or maintenance of the system, including information on toxic or dangerous materials in the product or which may be released in a fault condition, during an attack or over the lifetime of the product.
- Maintenance burden including reliability (request that the contractor provides a figure for the mean time between failure for their system in their tender), maintainability (how easy is the system to maintain) and service life (AACS are likely to be the subject of modifications or overhaul within 10 years. It is important to consider the length of service life expected and this should be included in the specification).

You may also want to read about Installation

You may also want to read about Operational requirements

Go to the start of AACS guidance

Go to the Glossary

Installation

The contractor should be instructed to install the AACS according to the manufacturer's installation instructions. If these are not followed then problems of responsibility could arise if the AACS fail to perform as expected.

While it is important not to compromise the system performance by including too many physical constraints, there are some significant design requirements that should be considered and may need to be included. These include:

- The mounting location of controllers, power supplies and where applicable network equipment: these must be located within the protected area minimising the possibility of accidental damage or deliberate attack. Careful consideration must be given to cables and junction boxes connected to the portal release mechanism and/or activation equipment when fitted to or in close proximity to the portal. Further information can be found in CPNI's CNI Electronic Security Systems: Implementation Guidance.
- Future site expansion: provision should be made for potential expansion plans at the site. The security of additional components must meet that of the installed AACS.
- Environment: while this will be critical for components installed outside buildings, internal conditions may also need to be considered including, humidity, temperature and atmospheric contamination. The installer/specifier should be informed of any specific environmental issues, for example if the equipment is to be located within noisy or high vibration areas.

Key to achieving a successful result will be the definition of unambiguous success criteria and metrics set out in a measurable commissioning schedule. This may be presented as part of the specification or may be a requirement placed on the installer, in any event once drawn-up it must be agreed by all parties.

The system should be installed to meet the guidance given in CPNI's Implementation of Electronic Security Systems Guide8 and BS EN 50133-79.

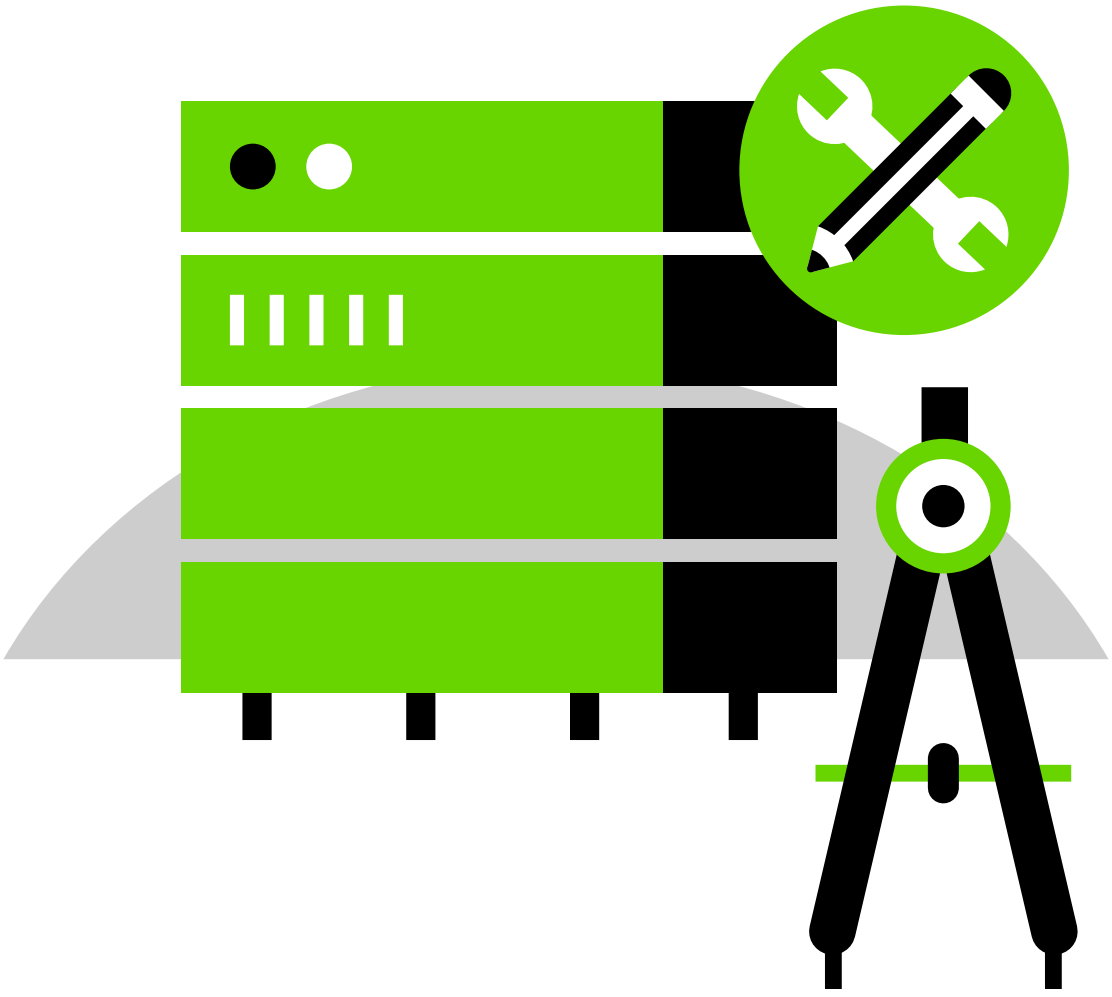
You may also want to read about Commissioning

You may also want to read about Components

Go to the start of AACS guidance

Go to the Glossary

5 COMMISSIONING AND MAINTENANCE



Commissioning introduction

AACS have cryptographic components within them. It is important that the cryptographic keys are kept secure and are only available to the site. AACS have been designed with a one-click keying process to be conducted on site. This ensures that the keys are only available to the site.

Immediately prior to commissioning the system must be keyed. A limited number of tokens should be produced to enable commissioning to take place.

Following installation and prior to acceptance of the AACS, the system should be subjected to a range of commissioning tests. This gives the user confidence that the AACS is working at the level determined by the performance specification/ operational requirement. It gives the user the chance to reject the installation if it does not fulfil the stated requirements. The contract must state that commissioning tests will be performed prior to acceptance of the system.

Tests should be identified and implemented during the commissioning of the system to ensure that the AACS is functioning correctly.

Following successful commissioning the roll out of user tokens can be undertaken.

Read more about AACS Commissioning

You may also want to read about Training

Go to the start of AACS guidance

Go to the Glossary

Training

A range of training appropriate to user access level and position and responsibilities will be required. Training should be undertaken by both the system installer and the site management and should cover the duties and responsibilities for:

- system administration, operators, supervisors and managers
- system users – including as a minimum the use and security of tokens, policy regarding PINS, wearing of badges, the policy in the event of a lost token, procedures to follow in the event of a system failure, rules for visitors, emergency evacuation procedures and any specific local requirements.

There will also be a need to establish the scale of the training required, including:

- a short list of the persons to received training
- how many people would be involved
- where and when training is to be provided, e.g. on-site training with initial course during commissioning and a refresher course later

You may also want to read about System maintenance

You may also want to read about User enrolment

Go to the start of AACS guidance

Go to the Glossary

System maintenance

To ensure that the installed AACS continues to operate as required it is important that a comprehensive maintenance programme is followed. The maintenance schedule should also have tasks to check that the OR is still applicable, whether the installation still fulfils the OR and determine whether there has been any change in site layout etc.

During the life of an AACS the initial operating parameters may change and components may degrade. Maintenance should be designed to ensure that the system still meets the security requirements detailed in the levels 1 and 2 operational requirements. Only regular maintenance and testing of the system will ensure the integrity of the system.

Maintenance must be undertaken using suitably approved and security cleared staff. It is dictated that access by engineers must require that they first be granted access by an administrator or supervisor before being able to use their own engineering codes. Any device used to maintain the system (programming terminals, laptops) should remain on site and be appropriately protected.

Remote engineer access is limited to ‘read only’ viewing rights of the logs. This will allow fault diagnosis.

Following any maintenance, repairs, upgrades or adjustments, the AACS should be retested to ensure that it continues to operate as required in the specification.

When placing a maintenance and support contract it is essential to state what response times are required to fix problems or resolve issues. If a maintenance contract exists the operators should be told who has the authority to call out the maintenance team if a problem arises and what response time to expect.

The contract should stipulate an expected level of reliability from the system, defining the acceptable level of availability expressed as a percentage. A system with 99% reliability could be expected to be non-operational for 4 days per year.

It is imperative that the supplier approves the maintenance regime and any maintenance contractors. This will ensure that where applicable the supplier can be held accountable for any failure of the AACS to maintain the required performance measures during the warranty period.

The maintenance log book must be kept up to date. It should include details of maintenance tasks carried out along with the corresponding test results. The maintenance log should also contain a copy of the commissioning test results which can be used for comparison with any subsequent tests.

Details of all breakdowns, repairs, replacements and system changes should also be recorded in the maintenance log book so that it is a complete history of the AACS.

Maintenance log books should be appropriately marked and protected. The information contained in the log book is sensitive by its nature and in the wrong hands it could be used to take advantage of any vulnerability identified during maintenance tasks. Log books should not be removed from the site for which they are applicable. Any copying should be strictly controlled.

Physical security and information assurance requirements for maintenance intervals and patching regimes are contained within CPNI’s Implementation Guide and Physical Security over Information Technology Guide.

You may also want to read about Operational requirements

Go to the start of AACS guidance

Go to the Glossary

Commissioning of AACS

INTRODUCTION

Following installation and prior to acceptance of any AACS, the system should be subjected to a range of commissioning tests. This gives the user confidence that the AACS is working at the level determined by the performance specification/ operational requirement. It gives the user the chance to reject the installation if it does not fulfil the stated requirements. Contracts placed for AACS must state that commissioning tests will be performed prior to acceptance of the system.

COMMISSIONING TESTS

Commissioning tests assess the functionality and performance of an AACS to ensure that the system is installed and performs to the required specification. All those concerned with commissioning will need access to, and be conversant with, the contents of the specification.

Documented commissioning tests also provide performance data from which any future deterioration can be measured and remedial action justified.

The installation contractor may provide a site acceptance test (SAT) following system installation. This comprises a structured demonstration of (all) the system functions to show that it is performing to specification. Although helpful, this should not preclude the owner/end user from conducting independent testing of the new system to satisfy themselves regarding its performance.

The performance of the AACS over an extended period cannot be determined during the commissioning period. The installation contractor should remain liable for any inability of the installation to meet the specified performance criteria over an extended period, which may be revealed during the warranty period. Provision should be made for additional tests to be carried out at the appropriate time(s). If deemed appropriate a retention of 15% of the contract price may be applied for a twelve month period of satisfactory performance.

Where the AACS is installed as part of a security system (for example with an existing alarm management system or CCTV) the system should be tested as a whole. This will ensure that the AACS operates effectively as part of the integrated system.

Commissioning tests should not only test AACS performance, but should also test any other required functionality. This could include a test to remove mains power to the system to ensure that the uninterruptible power supply (UPS) works as required; or that the AACS fails safe, depending on the requirement given in the specification. The tests should be non-destructive.

When commissioning or performing any other form of test, it is essential to have good communication (for example radios) with the control room. This ensures that the control room is able to confirm if an alarm or other event is received. It will also allow them to check whether the tests have generated any unexpected/spurious alarms.

The results of these commissioning tests should be used to determine whether the AACS meets the specification and whether the system should therefore be accepted. The results should be documented along with the AACS settings for each portal. These should be retained and used to make comparisons with results of subsequent tests to check on the

AACS continued performance. It is important that the settings are read directly from the system rather than any figures recorded in the documentation.

COMMISSIONING TEST PLAN

A commissioning test plan should be devised to evaluate the performance of the system in relation to the defined operation. The amount of time required for commissioning will vary depending on the size and complexity of the system and can range from a few hours to several days. It should not be assumed that a successful outcome on one portal is indicative that all other portals will respond correctly. The complex nature of AACS means that many of these systems will need to be programmed individually for each device or portal connected to it and the chance or error is proportionate to the size of the system. Therefore all tests should be applied to every portal and device as appropriate.

Examples of commissioning tests

Test description: Check operation of portal xxx	Comment
Test operation of portal using a valid token/PIN	The portal should open to allow entry. The event should be recorded in the system log
Test operation of portal using valid token and invalid PIN (three times)	The portal should not open. An alarm should be generated and recorded in the system log. The token should be invalidated
Test operation of portal using invalidated token but valid PIN	The portal should not open. An alarm should be generated and recorded in the system log
Open portal using valid token and PIN. Prevent the portal from closing for xxx seconds	Portal 'held open' alert should be generated and recorded in the system log
In conjunction with the installer, cause the portal to be opened without first using a token at the reader	Portal 'forced' alert should be created and recorded in the system log
Create a tamper event by removing the cover from a reader or reader from the mounting surface	A tamper alert should be generated and recorded in the system log
If anti-passback is in operation attempt access with a valid PIN/Token which has already been used for the portal	Alarm sounded, portal should not open, anti- passback alert recorded

COMMISSIONING DOCUMENTATION

On acceptance and handover of an AACS, drawings and manuals covering the installation, operation and maintenance must be provided to the person responsible for maintenance and operation of the system on the site. It is of particular importance that manuals covering system operation are written so that they can be read and understood by a non-technical user. The commissioning documentation should include the following information:

- a description of the manner/limitations of operation, including duration of backup power systems
- copies of any certificates of compliance with relevant standards or schemes
- set up parameters of the installed AACS
- comprehensive instructions for the switching on/operation/switching off/isolation of the system
- comprehensive instructions for dealing with emergency conditions and any precautionary measures necessary
- instructions for maintenance of the system to keep it in an effective and safe condition, including frequency of activities and the materials to be used
- names, addresses and telephone numbers of all equipment suppliers, together with type and model references, serial numbers, duty rating, capacity and the order number and date

SYSTEM DRAWINGS

To assist with future system maintenance and to help prevent inadvertent damage to components due to other non-associated works on the site it is useful to have detailed drawings of all parts of the system.

Drawings should include diagrams and schedules to show all the information necessary so that the system can be safely operated, maintained, inspected and tested, as far as is reasonably practicable. The drawings should be fully cross-referenced and co-ordinated with the operation and maintenance manual.

The drawings should also include wiring diagrams for the various components and for the system as a whole. In addition to schematic diagrams, drawings should be included showing the physical arrangements (panel & rack layouts, cabling layouts etc.) to assist the location and identification of the components which make up the system. A schematic layout of the overall system and interconnection diagrams should also be provided. In all installations cable run drawings must be provided showing the exact location of cable runs, where they penetrate walls and floors and in what containment they are enclosed.

You may also want to read about AACS Commissioning

You may also want to read about Training

Go to the start of AACS guidance

Go to the Glossary

6 FURTHER READING AND GLOSSARY

Further reading

- CPNI Guide to Producing Operational Requirements for Security Measures CPNI Catalogue of Security Equipment CPNI Systems Integration Guide
- CPNI Implementation of Electronic Security Systems Guidance Document CPNI Guidance on Running Physical Security over IP Networks
- BS EN 50133-7 Alarm Systems. Access Control Systems for use in Security. Applications Guidelines.
- BS 7671 Requirements for electrical installations. IET Wiring Regulations.
- Equality Act 2010
- Data Protection Act

Abbreviations and acronyms

AACS	Automatic Access Control System
CCTV	Closed Circuit Television
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
CSE	Catalogue of Security Equipment
DDA	Disability Discrimination Act
DPA	Data Protection Act
EMC	Electro-Magnetic Compatibility
GUI	Graphical User Interface
HoMER	Hollistic Management of Employee Risk
HVM	Hostile Vehicle Mitigation
IP	Internet Protocol
LAN	Local Area Network
NSI	National Security Inspectorate
OR	Operational Requirement
PIN	Personal Identification Number
PSU	Power Supply Unit
SAT	Site Acceptance Test
SSAIB	Security Systems and Alarms Inspection Board
SSG	Security Services Group
UPS	Uninterruptable Power Supply

Glossary

For the purposes of this publication, the following terms and definitions apply. Other terms, not included in the document, are included here for reference purposes.

ACCS Automatic Access Control System	
Access Control System	Equipment used to control the passage of people and vehicles into and out of protected areas and premises.
Alert	An indication that an event has occurred which requires a response.
Area zoning	Allows a token holder access only at defined access points.
Audit	Listing in real time of selected cardholders' transactions to monitor progress through protected areas.
Catalogue of Security Equipment	The CSE provides a list of products and systems which are suitable, within the use of a clear OR and Specification, for use on the CNI estate.
Duress	If an unauthorised person should force an authorised user to present his/her token to operate a portal, then the use of a special code entered into the key pad will provide warning to the control guards.
Emergency release	A portal release that will operate in an emergency.
Event	Occurrences which are reported by Access Control and Monitoring Systems.
Fail safe also known as 'fail released'	A locking device that unlocks the portal if power fails and requires the continuous application of power to stay locked.
Fail secure also known as 'fail locked'	A locking device that locks the portal if power fails and requires the application of power to unlock the door.
Installer	The person or company responsible for the supply of, installation, commissioning and decommissioning of the product or equipment.
Log	An electronic or paper-based report which lists the AACS events and alarms that have occurred.
Network topology	The design of the AACS network and its connections with other networks.
OR Operational Requirement	CPNI produce a guide to the production of Operational Requirements which form the basis for procurement of security systems on the CNI estate.
PIN Personal Identity Number	The use of the Personal Identity Number raises the level of security of the system. In addition to presenting a valid token, it is necessary for the user to enter a PIN.
Portal release	An electrical or mechanical device used to lock or unlock a door, e.g. electric-strike.

Portal	The physical means of controlling access through an access point, e.g. doors, gates, turnstiles.
Protected area	An area monitored and controlled by a manned or electronic security system, or enclosed by portals, e.g. secure rooms.
Tamper alert	An alert raised by the system to indicate its integrity has been compromised. Typically this is a result of someone gaining access to the control circuitry or causing damage to the system.
Time zone	A period of time during which a token can be legitimately used.
UPS Uninterruptable Power Supply	A backup system that continues to supply power in the event of a mains power failure for a defined period of time.
VPN Virtual private network	