Buyer's Guide to SSAIB Approved & Compliant Access Control Systems

A comprehensive Buyer's Guide for customers considering a SSAIB-Approved and Compliant Access Control System. This guide covers system types, components, integration, British Standards, installation, and practical advice, including a customer checklist and summary.

Overview

A SSAIB-approved access control system ensures secure, regulated entry to buildings, rooms, or zones—protecting people, property, and information. These systems also provide audit trails, restrict unauthorised access, and can be integrated with fire, intruder, CCTV, lifts, and barriers for a complete security solution.

This guide will help you understand your options, evaluate key components, ask the right questions, and plan for a compliant, efficient installation.

What is SSAIB Approval?

The Security Systems and Alarms Inspection Board (SSAIB) certifies that:

- The system meets UK and international standards
- Installers are vetted, competent, insured, and quality-assured
- Work is insurance and police-recognised
- Maintenance, documentation, and service procedures are in place

Key System Components

1. Types of Readers

Reader Type	Description	Usage
Proximity Readers	Use fobs/cards to unlock doors	Most common, cost-effective
Biometric Readers	Fingerprint, iris, or facial recognition	High-security or hygiene-conscious areas
Keypads (PIN)	Require numeric code entry	Basic or backup access
Mobile/App-based Readers	Use smartphones via BLE/NFC	Modern, convenient for staff
Multifactor Readers	Combine PIN + fob/biometric	High-security facilities

2. Types of Locks

Lock Type	Description	Suitable For
Maglocks (Electromagnetic)	Fail-safe; unlocks on power failure	Emergency escape routes
Electric Strikes	Controlled by reader; can be fail-safe or fail-secure	Internal/external doors
Solenoid Bolts	High-security locking	Data centres, labs
Shear Locks	Flush-mount magnetic locks	Doors requiring aesthetics

Lock Type	Description	Suitable For
Electric Latches	Replaces traditional mechanical locks	Residential or light commercial

3. Access Credentials

Credential	Pros	Considerations
Key Fobs	Convenient, low cost	Can be lost or cloned
Cards (RFID, Smart Cards)	Scalable, printable for ID	Risk of duplication
Mobile Credentials (Apps)	No physical token	Depends on smartphone availability
Biometrics	Non-transferable	Hygiene, data protection (GDPR)

Wired vs Wireless Access Control

Feature	Wired	Wireless
Reliability	High	Moderate to high
Installation	More disruptive (cabling)	Minimal disruption
Maintenance	Low (no batteries)	Requires battery management
Security	Less susceptible to signal interference	Encrypted protocols reduce risk
Best For	New builds, high security	Retrofits, heritage sites

Hybrid systems combine both for flexibility.

Integration with Other Systems

CCTV

- Link access events to video footage
- Real-time verification of entry attempts
- Useful for investigations

Intruder Alarms

- Automatically arm/disarm based on access events
- Shared fobs/cards across systems
- Event linking for threat detection

Fire Alarms

- Auto-unlock doors on fire alarm trigger
- Required for emergency egress routes (BS 7273-4)

Other Equipment

- Lifts: Floor access control based on permissions
- Barriers: Vehicle entry controlled by same access token
- Electronic Gates: Secure perimeter entry
- Turnstiles: Pedestrian control at entry points

Installation Considerations

Installation Time

- Varies by system size:
  - Small (1–3 doors): 1– 3 days
  - Medium (4–10 doors): 4 – 10 days
  - Large (multi-site): Phased over weeks

Cable Routes

- Run through walls, ceilings, under floors
- May require surface trunking in finished buildings

Possible Disruption

- Access to all controlled areas needed during install
- Temporary disablement of doors/gates during wiring
- Business hours vs after-hours installation considerations
- 240V 3amp unswitched fuse spur adjacent each access control unit

Challenges & Pitfalls

Challenge	Solution
Lost credentials	Enable quick remote deactivation
Cloned cards/fobs	Use encrypted smart cards or mobile credentials
Inadequate cabling paths	Use wireless readers or plan with IT/construction team
Compatibility with existing systems	Use open-platform, standards-based systems
Power loss	Use UPS and fail-safe lock strategies
GDPR compliance	Ensure biometric or access logs are protected and justified

Relevant British Standards

Standard	Description
BS EN 60839-11-1	Electronic access control systems – system requirements
BS 7273-4	Fire protection – interface between fire detection and access systems
BS 7858	Screening of individuals working in secure environments
BS 9263	Code of practice for the design and installation of electronic access control systems
BS EN 50133	Functional requirements and system design (legacy standard)
BS EN 61000	Electromagnetic compatibility (EMC) for electronic equipment

Key Questions to Ask Your Installer

1. Are you SSAIB certified for access control?
2. What reader and lock types do you recommend for each area?
3. Does the type of door matter? i.e. wood, UPVC, Glass, metal
4. Does it matter if the doors are single leaf, double leaf, rotating?
5. Will the system integrate with existing CCTV, fire, intruder systems or time and attendance?
6. Can we allocate different access levels?
7. Do we need a PC to manage the software?
8. What are the features of the system?
9. Is the system scalable for future expansion?
10. Is this system open-platform or proprietary?
11. What data protection measures are in place
12. Can you provide a fire and emergency interface?
13. What are the ongoing maintenance requirements and service costs?
14. Can I control/access the system remotely via an app or browser?
15. What support/warranty is included?

Access Control System Buyer's Checklist

Task / Item	Completed?
Site access risk assessment completed	YES / NO
SSAIB-certified installer selected	YES / NO
System scope agreed (number of doors/zones)	YES / NO
Reader types and lock functions specified	YES / NO
Integration with other systems planned	YES / NO
GDPR and data protection reviewed	YES / NO
Wired vs wireless decision made	YES / NO
Fire alarm interface (BS 7273-4) included	YES / NO
Installation disruption assessed	YES / NO
Training and handover scheduled	YES / NO
Maintenance plan agreed	YES / NO

Summary of Key Points

- SSAIB certification ensures compliance, quality, and insurance acceptance
- Understand the differences in readers, credentials, and lock types
- Choose wired, wireless, or hybrid based on your building and security needs
- Integrate access control with fire, CCTV, intruder, and automation systems
- Follow British Standards such as BS EN 60839-11-1 and BS 7273-4
- Plan installation carefully to minimise disruption
- Ensure ongoing support, updates, and user training