Buyer's Guide – Hotel Access Control Systems

Sub Headings = Noto Sans Font, 16 Size & Bold

Hotel access control systems are not just about guest room entry; they affect security, operations, emergency planning, insurance compliance, and data protection. A modern system should integrate with your PMS, support mobile keys, enable staff permissions, provide audit trails, and protect sensitive guest data.

Key Buying Considerations & Best Advice

1. Identify the hotel's operational needs

Different hotels need different levels of sophistication:

- Budget hotels: simple keycard or PIN-based locks
- Mid-scale: online locks, PMS connectivity, room automation
- Luxury: smartphone credentials, NFC/BLE mobile keys, queue-less check-in

2. Select the right technology

Common hotel credential technologies:

- RFID (most common) – secure, inexpensive
- Magstripe – legacy, less secure
- BLE Mobile keys – guest convenience, app-based
- NFC – increasingly used with modern smartphones
- PIN codes – useful for staff areas

3. Decide between Offline, Semi-Online, or Fully Online

- Offline: Cheaper, programmed at front desk
- Online: Live updates, central management, better audit trail
- Cloud-managed: Remote access, updates, PMS integration

4. Integrate with your PMS

Essential for:

- Automated check-in/out
- Auto-expiring keys
- Guest journey apps
- Housekeeping & maintenance workflows

5. Prioritise cybersecurity

Access control = personal data. Choose systems offering:

- Encrypted card technology
- Encrypted BLE/NFC communication
- Secure APIs
- Firmware update support

6. Plan for lifecycle cost

Ask about:

- Lock battery life
- Replacement cards
- Software licences
- Cloud service fees
- Support contracts

Questions to Ask an Access-Control Supplier

System & Technical

1. What lock technologies are supported (RFID / BLE / NFC)?
2. Is the system fully online, or do locks require physical reprogramming?
3. What cyber-security protections are used (encryption, secure keys, firmware)?

4. Does the system comply with relevant British Standards? (see below)
5. What integrations exist with my PMS (Opera, RoomMaster, Guestline, etc.)?
6. Can staff access profiles be customised by role?
7. What is the typical battery life and maintenance cycle?

Installation & Operational

8. Can locks fit my existing door structure, fire doors, and architecture?
9. What is the warranty and support SLA?
10. What are the costs for software licences and yearly maintenance?
11. How is onboarding/training for staff handled?

Data Protection & Legal

12. How does your system support compliance with UK-GDPR / DPA 2018?
13. Where is data stored (UK/EU servers)?
14. How long are access logs retained? Can retention periods be controlled?
15. Do you provide audit logs for security incident investigations?

Top 5 Hotel Access Control Systems (2025)

These are well-established, hospitality-grade systems used internationally.

1. ASSA ABLOY VingCard

Industry leader; widely adopted by hotels.

- BLE mobile keys
- High security RFID
- Robust PMS integrations

- Excellent support & lifecycle
  Best for: Mid–Luxury hotels, chains

2. SALTO Systems (SALTO KS & SALTO Space)

Flexible, cloud-based, strong in boutique hotels.

- Mobile keys
- Wireless online network
- Granular staff control
  Best for: Boutique / design-led hotels

3. Onity (HT Series / Trillium Series)

Long-standing hospitality provider.

- RFID & mobile keys
- Cost-effective for larger estates
  Best for: Midscale hotels, budget-to-premium chains

4. dormakaba Saflok & Ilco

Trusted global hotel lock brand.

- Mobile keys, RFID
- Advanced audit & reporting
  Best for: Hotels needing strong compliance & reporting

5. TTLock / TThotel (for small hotels & guesthouses)

Budget-friendly cloud-based system.

- Mobile app keys
- PIN/IC cards
- Remote room access
  Best for: Small hotels, AirBnBs, independent operators

Challenges & Pitfalls to Consider

1. Wireless signal problems

Metal-framed fire doors, thick walls, and old buildings can disrupt online lock connectivity.

2. Mobile key adoption

Not all guests download apps; ensure you keep a fallback option (RFID cards).

3. Battery management

Locks failing due to depleted batteries = guest lockouts.
Plan a routine maintenance schedule.

4. Door condition

Old or warped doors may prevent proper lock installation.

5. Fire door compliance

Only use locks approved for fire doors—critical for life-safety.

6. Staff misuse or poor audit practices

Without proper role-based permissions, staff may have broader access than needed.

7. Data-protection breaches

Access logs contain sensitive personal data (room numbers, dates, usage).

Location & Installation Considerations

Placement

- Ensure guestroom locks are positioned to withstand frequent use.
- Staff and back-of-house areas should use higher-durability locks.
- Locks on external doors must be weatherproof and rated for outdoor use.

Environmental factors

- Avoid BLE-only locks where mobile signal/guest WiFi is poor.
- Ensure emergency exits meet BS EN 179 / EN 1125 for panic hardware.

Power & Cabling

- For wired online systems, pathing cable through old buildings may be invasive.
- For wireless systems, ensure network spans all floors, corridors, and basements.

UK DPA 2018 / UK-GDPR Responsibilities for Hotels

Hotel access control systems handle personal data including:

- Guest room number
- Check-in/check-out times
- Access logs (who entered which door and when)
- Staff access logs

Under the Data Protection Act 2018 and UK-GDPR, hotels must:

✓ Have a *lawful basis* for processing access-data
Usually legitimate interest (security), but document it.
✓ Complete a Data Protection Impact Assessment (DPIA)
Especially for cloud-based or large-scale monitoring systems.
✓ Display privacy information
Guests should know how their access data is used.
✓ Implement strict access controls
Only authorised staff view access logs.
✓ Secure data appropriately
Encryption, strong passwords, MFA, secure APIs.
✓ Set retention policies
Most hotels store logs 30–90 days, longer only for security incidents.
✓ Maintain supplier due diligence
Ensure suppliers meet GDPR and follow secure development.

Relevant British Standards & Legislation

- BS EN 14846 – Electromechanical locks
- BS EN 1906 – Hardware & durability of lock components
- BS EN 179 – Emergency exit devices for non-public areas
- BS EN 1125 – Panic exit devices for public areas
- BS EN 60839-11-1 – Electronic access control systems (EACS)
- BS EN 50133 – System requirements for access control
- BS EN 60529 (IP Ratings) – For outdoor/weatherproof locks
- BS EN 1634-1 – Fire resistance of door sets & hardware

Relevant UK Legislation

- Data Protection Act 2018 (UK-GDPR)
- Health and Safety at Work Act 1974
- Regulatory Reform (Fire Safety) Order 2005
- Building Regulations Part B (Fire Safety)