Visitor Door Entry & Access Control Requirements, Secured By Design (SBD) Version 2, March 2019.

At a glance:

1. The access control system (proximity readers, radio receivers) must record everything and hold this information for 30 days.
2. The access control system (proximity readers, radio receivers) must be remotely programmable.
3. Every radio transmitter must have its own unique ID (individual) code just like the proximity keyfobs.
4. Proximity keys, radio transmitters must be security protected against copying / cloning.
5. Tradesbutton is never allowed.
6. Audio-visual systems providing live video between the visitor and the resident is required from 4no flats upwards.
7. Visitor panels must be anti-vandal meaning stainless steel, no plastic buttons.
8. **Control equipment inside the building must be housed within steel lockable cabinets.**
9. Electric locking must be part of a certificated doorset. It should not be fitted by 3rd parties.
10. Stainless steel anti-vandal self-resetting emergency exit systems (complying with safety regulations) are required for final exit communal doors. Green breakglass units are not allowed.
11. Compartmentalisation is mandatory for blocks with over 25 flats.
12. Blocks with over 25 flats must also record visitor activity and hold this information for 30 days.
13. The technology by which the visitor door entry system operates is a matter of consumer choice.

Section 28 Telephone and Internet Protocol (IP) based visitor door entry systems with or without remote unlocking.
Parts: 28.1–28.7 on page 47

Secured by Design
SBD
Official Police Security Initiative

Please note as follows with reference to Section 28:

All visitor door entry systems are now Internet Protocol (IP). So complying with Section 28 applies to every installation of visitor door entry on a new-build development today.

Internet Protocol (IP) Hardwired Video Monitor Door Entry Systems.

These systems simultaneously call smart phones, iPads, tablets, wherever they may be, in addition to the wall-mounted flat monitor.

4G/IP/GSM Visitor Door Entry Systems.

These systems call smart phones, iPads, tablets, wherever they may be, but there is NO hardwired wall-mounted flat monitor.

27 Access control and additional security requirements for buildings containing multiple dwellings or bedrooms

Definition

27.1 A building containing multiple dwellings, for the purposes of this document, may include flats, apartments, bedsits or individual bedrooms accessed from a semi-private area and served by a shared or communal entrance doorset including Houses in Multiple Occupation (HMO) and student accommodation.

Visitor door entry system

Definition

27.2 A door entry system is a visitor system that is able to call a dwelling, whether individual or served from a communal entrance. It shall allow a visitor to ring any selected dwelling within the particular system and/or building, and hold a two-way simultaneous conversation between the visitor and occupant of the dwelling. It will allow the occupant to see and identify the visitor and their location, and will enable the occupant of the dwelling to remotely operate the electric locking device from their room terminal, thereby unlocking the communal entrance door(s) associated with the action and allowing the visitor access. This should be repeated at any subsequent communal entrance and landing if compartmentation of the building is required.

27.3 Visitor door entry systems shall be easy to operate and understand and have the ability to display the image of the caller before the call is answered, so the resident can choose whether to answer the call or not.

Access control system

Definition

27.4 A proximity access control system provides electronic access through communal entrance doorsets. This is generally by use of a card or key fob issued to an occupant or person such as staff member, contractor or postal delivery service. It grants access to required areas via locked doors when the valid card or key fob is presented to a proximity reader fitted to the communal entrance doorset. Authorised access can be restricted to certain times of the day for some users.

The access control system will have the facility to record and identify the location, user, type, time and date of every system event. Sufficient memory storage must be available for a period of not less than 30 days. The system will be fully programmable, with access restricted to

the nominated system controller(s) who will be able to manage the system via remote access in order to expeditiously delete lost or stolen proximity cards or key fobs and any enrolled radio transmitters. Radio transmitted must have individual codes, such as those used by access cards or key fobs. Common code radio transmitters shall not be acceptable as they cannot be managed.

27.5 Electronic keys must be security encrypted to protect against unauthorised copying, and be sufficiently robust to avoid constant replacement during everyday use by the residents.

Communal and shared entrance doorset – physical security standards

Definition

27.6 A communal or shared entrance doorset, including integral adjacent panels and side screens, can be defined as an external doorset leading from the street or otherwise public area to an internal semi-private communal area providing access to segregated flats, bedsit or individual bedrooms. They can be further categorized by use as follows:

Physical security requirements for communal entrance doorsets with no electronic visitor door entry system – 4 dwellings or less

27.7 Communal entrance doorsets in blocks serving 4 dwellings or less, over no more than two floors, are not required to be connected to a visitor door entry system and access control system, and can be controlled by non-electronic keys only i.e. requiring residents to meet and greet visitors at the communal door. Doorsets shall comply with the physical security requirements of paragraph 21.1 to 21.17 and 21.19 to 21.22.

27.8 Communal entrance doorsets in blocks serving 4 dwellings or less, over more than two floors, are required to have a visitor door entry system and access control system (regardless of the number of flats/apartments, bedsits or bedrooms) and therefore specifiers are again referred to the content of paragraph 21.1 to 21.17 and 21.19 to 21.22. for the requisite physical security standards.

27.9 Tradesperson or timed release mechanisms are not permitted as they have been proven to be the cause of anti-social behaviour and unlawful access to communal developments.

Physical security requirements for communal entrance doorsets with an electronic visitor door entry system – 5 dwellings or more but less than 10

27.10 Communal entrance doorsets serving 5 dwellings or more, but less than 10 falling within this category shall meet the following (in accordance with Section 2A paragraph 21):

- PAS 24:2016;
- STS 201;
- LPS 2081 Security Rating B+.

27.11 Where a communal entrance doorset serves 5 dwellings or more, but less than 10, it is required to have a visitor door entry system and access control system to enable management oversight of the security of the building.

No tradesbutton

27.12 Tradesperson or timed release mechanisms are not permitted as they have been proven to be the cause of anti-social behaviour and unlawful access to communal developments.

27.13 Developments with more than two floors are required to have a visitor door entry system and access control system (regardless of the number of flats/apartments, bedsits or bedrooms) and therefore specifiers are again referred to the content of paragraph 21.1 to 21.17 and 21.19 to 21.22.

Physical security requirements for communal entrance doorsets with an electronic visitor door entry system serving 10 dwellings or more

27.14 Communal entrance doorsets serving 10 dwellings or more, controlled by visitor door entry systems, can enable residents to gain access without the use of a key and grant entry to visitors by means of an electronic door release system. An increased number of dwellings results in doorsets being used more frequently. Likewise the proximity of the development to a high crime area can subject doorsets to more abuse. Therefore specifiers should satisfy the DOCO that the doorset is fit for its intended purpose and environment. Certification to PAS 24:2016 or STS 201 may be acceptable for some developments, but full third party certification to one of the following standards can demonstrate the doorset is of a more robust construction and is able to withstand the day to day use in a communal application:

- STS 202 Issue 6:2015 Burglary Rating 2; or
- LPS 1175 Issue 7.2:2014 Security Rating 2+; or
- LPS 1175 Issue 8:2018 Security Rating A3+; or
- LPS 2081 Issue 1.1:2016 Security Rating B; or
- PAS 24:2016, paragraph 4.4.3 i.e. tested to BS EN 1627 Resistance Class 3 (*Note 27.14*).

Note 27.14: Specifiers are reminded that doorsets utilising non-mechanical magnetic locks fall within the scope of PAS 24:2016 but outside the scope of EN 1627. All testing to this standard utilising a mechanical lock shall be conducted in accordance with the 'UK Police Service (Secured by Design) Interpretation document for BS EN 1627, BS EN 1628, BS EN 1629 & BS EN 1630'. This is a requirement within the UK national forward of BS EN 1627.

27.15 There have been numerous examples of sub-standard doorsets failing, due to poor general performance, leading to insecure properties. In some cases, particularly heavy communal entrance/exit doors have become detached from the frame, which could have resulted in serious injury or worse. Certification to BS 6375 (Parts 1, 2 and 3) provides reassurance that the doorset is fit for purpose and safe in use. Specifiers should be satisfied that the following attributes are addressed:

- Duty level – this is the number of door operations (opening and closing actions) that it has been tested to. In simple terms the more dwellings that are served the higher the duty level should be (BS 6375 Part 2 provides further guidance);
- Weather performance - which may be influenced by the geographical location, temperature and climate (BS 6375 Part 1 provides further guidance);
- Wind resistance – also influenced by the location of the building (BS 6375 Part 1 provides further guidance);
- And relevant sections of BS 6375 Part 3 (applicable to the installation).

Door entry and access control systems

27.16 All communal dwellings (see paragraph 27) with 10 flats, apartments, bedsits or individual bedrooms, or more should have a visitor door entry system and access control system to enable management oversight of the security of the building i.e. to control access to the building via the management of a recognised electronic key system.

27.17 Visitor door entry systems that utilise CCTV must comply with the requirements of paragraph 29.

Small developments (up to 25 flats/apartments, bedsits or bedrooms)

27.18 Visitor door entry systems and access control systems are not normally required for communal developments with 4 or less flats, apartments, bedsits or bedrooms or less spread over no more

than two floors, or where the accommodation is not intended for use by the older or disabled people.

It should be noted however, that regardless of the size of any development where dwellings are inclusively designed to provide accessible housing, consideration should be given to disabled and older residents who may require additional access features such as full automation via remote key fob to enable independent entry through all doors required to gain access e.g. from the building entrance/ exit/car park, through any additional communal or lift doors required to gain access to their dwelling entrance. This may be required due to an inability to operate heavy doors and/or reach and operate controls or wall mounted fobs.

27.19 Developments containing up to and including 9 flats, apartments, bedsits or bedrooms spread over more than two floors (three floors or more including basement level accommodation) shall comply with the requirements of paragraph 27.8.

27.20 Smaller developments containing up to and including 25 flats, apartments, bedsits or bedrooms shall have a visitor door entry system and access control system. The technology by which the visitor door entry system operates is a matter of consumer choice, however it should provide the following attributes:

- Access to the building via the use of a security encrypted electronic key (e.g. fob, card, mobile device, key, etc.);
- Vandal resistant external door entry panel with a linked camera;
- Ability to release the primary entrance doorset from the dwelling or bedroom (in the case of student accommodation or House in Multiple Occupation);
- Live audio and visual communication between the occupant and the visitor;
- Ability to recover from power failure instantaneously;
- Unrestricted egress from the building in the event of an emergency or power failure;
- Control equipment to be located in a secure area within the premises covered by the CCTV system and contained in a lockable steel cabinet to LPS 1175 Security Rating 1 or STS 202 Burglary Rating 1.

27.21 Developers and installers of visitor door entry systems and access control systems should be aware that UL 293 provides reassurance that a system has been assessed against a prescribed security test regime.

27.22 Tradesperson release mechanisms are not permitted as they have been proven to be the cause of anti-social behaviour and unlawful access to communal developments.

27.23 Specifiers are reminded that the installed electronic release hardware must form part of the certificated doorset range.

Developments with more than 25 flats, apartments, bedsits or bedrooms

27.24 Larger developments containing more than 25 flats, apartments, bedsits or bedrooms shall have a visitor door entry system and access control system. The technology by which the access control system operates is outlined within UL 293, however it must provide the following attributes:

- Access to the building via the use of a security encrypted electronic key (e.g. fob, card, mobile device, key etc.);
- Vandal resistant external door entry panel with a linked camera;
- Ability to release the primary entrance doorset from the dwelling or bedroom (in the case of student accommodation or House in Multiple Occupation);
- Live audio/visual communication between the occupant and the visitor;
- Ability to recover from power failure instantaneously;

No plastic buttons etc

No battery backup. Doors to fail unlocked.

System control equipment must be in steel lockable cabinets

- Unrestricted egress from the building in the event of an emergency or power failure;
- Capture (record) images in colour of people using the door entry panel and store for those for at least 30 days. If the visitor door entry system is not capable of capturing images, then it should be linked to a CCTV system or a dedicated CCTV camera should be installed for this purpose. This information should be made available to police within 3 days upon request;
- All visitor and resident activity on the visitor door entry system should be recorded and stored for at least 30 days. This information should be made available to police within 3 days upon request.
- Systems must comply with General Data Protection Regulations (GDPR).

27.25 SBD recommends the use of colour monitors to enable the occupier of the dwelling or bedroom with the identification of visitors or to assist the occupier to accurately describe the colour of clothing to the police of the perpetrators of antisocial behaviour or those otherwise misusing the system.

27.26 Specifiers are reminded that the installed electronic release hardware must form part of the certificated doorset range.

27.27 In the event of a power failure door locks shall revert to a safe (unlocked) mode unless there is a fire evacuation policy in place that requires doors to remain locked, such as that operated within some care homes.

27.28 Tradesperson release mechanisms are not permitted as they have been proven to be the cause of anti-social behaviour and unlawful access to communal developments.

Security compartmentation of developments incorporating 25 or more flats, apartments, bedsits or bedrooms

27.29 Developments of over 25 flats, apartments, bedsits or bedrooms can suffer adversely from anti-social behaviour due to unrestricted access to all areas and floors of the building. SBD therefore seeks to prevent unlawful free movement throughout the building through the use of an access control system. How this is achieved is a matter for the specifier, the following two methods are acceptable:

1. Lift and stairwell access controlled separately:

- To prevent the lift and stairwell providing unrestricted access onto a residential landing, each resident should be assigned access to their

floor only via the use of a security encrypted electronic key (e.g. fob, card, mobile device, key etc.) both on the stairwell/landing door and lift;

On ground floor

- Access to stairwells from the communal lobby should be restricted to residents to reduce the risk of anti-social behaviour or criminal activities;
- Unrestricted egress from a landing into the stairwell and from the stairwell to the communal lobby/emergency fire exit should be provided at all times.

2. Lift and stairwell access jointly controlled via an additional secure doorset:

- An additional secure doorset prevents access to each landing from both the lift and stairwell. Each resident should be assigned access to their floor only via the use of a security encrypted electronic key (e.g. fob, card, mobile device, key etc.) for this doorset;
- Access to stairwells from the communal lobby should be restricted to residents to reduce the risk of anti-social behaviour or criminal activities;
- Unrestricted egress from a landing into the stairwell and from the stairwell to the communal lobby/emergency fire exit should be provided at all times.

27.30 In the event that a lift opens directly into an apartment a security protocol must be agreed between the occupiers and the lift maintenance company to ensure access cannot be gained without the proper authority.

27.31 Alternative methods of creating compartmentation within the building may be discussed with the DOCO.

27.32 Whether access at these locations is provided to legitimate visitors as well as residents via additional call points, is a matter for the overall access control strategy. It is not the intention of Secured by Design to restrict legitimate free flow of residents through the building, this will be at the discretion of the management company concerned.

27.33 It is imperative that the fire service should have unrestricted access to all floors in the event of an emergency so the internal access control system utilised should incorporate the following features:

27.33.1 Where unlawful free internal movement is restricted via the lift then the fire service must be afforded access via a 'firefighter's mode' or an evacuation lift in 'evacuation mode'.

27.33.2 If unlawful free internal movement has been restricted via an access control system acting on dedicated external doorsets and any additional doorsets providing access to individual floors/ landings then an electronic release must be incorporated within the system to allow the fire service free access to all of the communal areas of the building. The electronic release system must be weatherproof, easily identifiable and located close to the entrance that Fire and Rescue Teams would use in the event of an emergency. It has been agreed between the police and fire and rescue services that the most practical means of achieving this aim is to install a switch within an Access Control Box (ACB). The key system for the ACB should be of a restricted type acceptable to the local fire and rescue service. An ACB must be secure for obvious reasons and therefore shall be tested and certificated to one of the following standards:

- LPS 1175 Issue 7.2:2014 Security Rating 2; or
- LPS 1175 Issue 8:2018 Security Rating A3+; or
- STS 205 Issue 1:2011 Burglary Rating 2.

27.33.3 The use of an ACB is in addition to the installation of a Premises Information Box (PIB), which are recommended by the fire and rescue service and are referenced within clauses of BS 9991:2015. The ACB should be clearly marked with a photo-luminescent identification sign in the same way as the PIB. The exact location of an ACB should be specified following

consultation with the local Fire and Rescue Service.

Emergency door release devices

27.34 Break glass emergency door exit release devices (often green in colour) on communal external doors that provide an important aid to egress in the event of an emergency have proven to be abused rendering some buildings insecure for long periods of time. SBD recommends vandal resistant stainless steel self-resetting emergency exit systems are installed as an alternative. The installation and system type must be in full compliance with the Building Regulations and achieve final 'sign-off' by local Building Control or Approved Inspector.

27.35 If the break glass emergency door release device provides access to residential areas as part of the emergency egress route, additional security must be provided to restrict access to the fire egress route only to maintain the security of the building line. This is also a requirement of Part Q of the Building Regulations (England and Wales).

28 Telephone and Internet Protocol (IP) based visitor door entry systems with or without remote unlocking

28.1 To ensure that the viewed image is of appropriate quality, systems of this kind shall be demonstrated to the DOCO on equipment similar to that used by residents (e.g. TV smart phone or tablet), prior to receiving Secured by Design accreditation.

28.2 All systems shall comply with UL293 and the Internet Protocol security shall be tested and certificated to British Standard's Institute Kitemark for the Internet of Things (IoT) Devices, by 1st October 2019.

28.3 The system must be capable of catering for a minimum of 2 and a maximum of 6 devices being activated as controllers per dwelling.

28.4 Only the management body shall be permitted to add a device to the system, however the principal resident(s) shall be permitted to remove a device from the system.

28.3 Remote unlocking (e.g. when operated from outside the boundary of the residence utilising mobile equipment such as smart phones and tablets) should only be permitted when there is both a live audio and visual feed. Systems should not permit users to remotely release the door lock where there is audio only communication, e.g. poor signal area, loss of signal, etc.

28.4 If the facility of remote unlocking is abused by a resident, the system shall be capable of restricting their ability to unlock a door by way of a land-line in the residence linked to a visual monitor only.

28.5 If residents do not possess the required equipment to use the system, a dedicated device should be installed inside the dwelling to give audio and visual communication.

28.6 Specifiers are reminded that if telephone and/or IP based visitor door entry systems are utilised there should be no usage charge incurred by the resident as a result of a system activation.

28.7 Specifiers are reminded that if telephone and/or IP based visitor door entry systems are utilised, they shall also comply with the requirements of paragraph 27.

29 CCTV and Recording

29.1 CCTV is not a universal solution to security problems, it forms part of an overall security plan. It can help deter crime and criminal behaviour, assist with the identification of offenders, promote personal safety and provide reassurance for residents and visitors. Even the smallest development will benefit from the installation of a good quality CCTV system, which does not need to be expensive.

All the latest ranges of Video Door Entry are IP protocol systems calling wall-fixed video monitor and also simultaneously connect to remote smart devices.