IP DOOR ENTRY

4G/IP/GSM

SMART DOOR R ENTRY & ACCESS CONTROL

IPGUARD® SYSTEM SPECIFICATION

IPGUARD® 4G/IP/GSM WITH BATICONNECT CLOUD, SMART TECHNOLOGY VISITOR DOOR ENTRY & RESIDENT ACCESS CONTROL

BATI CONNECT CLOUD

TOTAL 24/7/365 REAL-TIME REMOTE MANAGEMENT OF ALL YOUR SITES

IPGUARD
4G/IP/GSM SMART
Visitor Door Entry

Secured by Design
SBD
Police Preferred Specification

1. Development specific communal visitor door entry & resident access control system equipment, operational strategy and drawings to be submitted for approval to both the client and the Design Out Crime Officer (DOCO) representing Secured By Design.
2. Building Control regulations always take priority over all Secured By Design requirements.
3. System and installation must comply fully with the Equality Act 2010 (DDA) to anticipate and prevent disability discrimination and so ensure that disabled persons receive a similar level of service provision as able-bodied persons.
4. System must comply fully with the Data Protection Act 2018, and the UK GDPR, and/or with subsequent legislation.
5. System must comply fully with the latest Secured By Design regulations for visitor door entry & resident access control.
6. No door, irrespective of its location, must open over a visitor door entry or resident access control panel.
7. Visitor Door Entry Panel(s), Proximity Access Control Readers & Keypad Code Pads must be officially certificated by the Loss Prevention Certification Board (LPCB) of the BRE (British Research Establishment Ltd) as having passed the test as a critical component of a door set in compliance with British Standard LPS1175 (SR2) thereby achieving Secured by Design (SBD), Police Preferred Specification.
8. All visitor door entry panels and resident proximity access control panels (readers) to be vandal resistant with security screw fixings.
9. Visitor 4G/IP/GSM smart technology door entry panel(s) to be IPGUARD® range, fully Equality Act 2010 (DDA) compliant. Keypad buttons for calling on panel to be alphanumeric, anti-vandal, tactile, raised and minimum 15mm diameter and with, on the button itself, braille for the blind and large minimum 8mm height illuminated LED digit/characters for the visually impaired.
10. IPGUARD® systems do not require fixed system proprietary equipment installed inside resident dwellings. No cabling is required into each dwelling from the communal areas. Residents utilise their own smart technology IOS/Android smart phones / IPADs / tablets – any mix, to view and answer visitor calls from the IPGUARD visitor door entry panels.
11. Residents / tenants download the free IPGUARD APP (available on both the Apple or Google Play App stores) directly onto their smart phone(s) / IPAD(s) / tablets. If the resident / tenant is using a landline or non-smart mobile calls from the IPGUARD panel will be audio only.
12. Residents / tenants with smart phones / IPADs / tablets automatically have a history of all visitor calls including date, time, status (missed, answered, door opened etc) and a picture of their visitor.
13. Objective is to avoid visitor door entry technologies with finite life spans that operate using system proprietary equipment (fixed or other) inside resident dwellings and so require on-going maintenance and eventual replacement costs.
14. IPGUARD® visitor door entry panel(s) serving communal entrances into a residential building must be equipped with integral anti-vandal colour/mono (day/night) high resolution camera(s) for Equality Act 2010 (DDA) compliance (visually impaired residents must be provided with a close up of the visitor calling), and every integral panel camera must meet the technical specification(s) as stipulated by Secured By Design.
15. IPGUARD® visitor door panel must be installed at 1.4 metres AFFL to its centre.
16. Resident only doors with proximity access control panel (reader) must be installed so that the proximity reader is fitted so that its top is 1.0 metre AFFL.

17. Resident proximity access control panels (readers) must be fully Equality Act 2010 (DDA) compliant; obvious (image of a key), bright, illuminated, and have LED's and buzzer to indicate authorised, declined and door open.

18. IPGUARD® systems must, for security reasons, provide full visitor call logging. The system must identify the visitor calling panel (where the visitor made the call from), the time and date of the call, the duration of the call and whether the resident called opened the door. This is a Secured By Design requirement so that any resident abusing the system can be identified.

19. IPGUARD® visitor door entry panel(s) to include Equality Act 2010 (DDA) information voice output and visual display output messages for visitors.

20. IPGUARD® visitor door entry panel(s) to allow for 3 no telephone numbers per flat so that in the event of an engaged tone or non-answer, the system automatically calls the 2nd and then the 3rd telephone number.

21. Sitewide visitor door entry panels and resident access control systems will all be fully remotely programmable via BATICONNECT CLOUD server. No software will be required.

22. Keypad code final door opening (the door from the public side into the building) is not sufficiently secure, cannot identify the code user and is not permitted by Secured by Design. The system must, however, provide this feature for facilities staff.

23. Tradesperson time-zone programmable door opening buttons on visitor door entry panels are not normally permitted by Secured By Design. However, the IPGUARD® visitor door entry panel(s) must allow for this feature, which must be remotely programmable via the BATICONNECT CLOUD, because it may be specifically instructed because the main entrance door opens into a secure lobby where the post boxes are located.

24. All communal IPGUARD visitor door entry panel(s), all resident access control proximity readers for doors, gates, lifts, all IPKEYSAFE(s), and all radio access control receivers for vehicles on the development to be networked and fully remotely programmable via the BATICONNECT CLOUD server. It must be possible to remotely connect into the sitewide access control system(s) to add or delete proximity key fobs, radio transmitters, keypad codes for facilities staff, and amend individual and/or group access rights to or from one, some or all doors, gates, lifts and change any system parameter.

25. For security compartmentalisation reasons and/or as requested by the Secured by Design DOCO for buildings of over 10no flats sharing a communal entrance, a "Meet & Greet" type access control strategy may be required to achieve Secured by Design certification. Residents would usually "Meet & Greet" their visitor on the ground floor and then escort the visitor to their flat.

    The access control system must, therefore, be capable of providing the following security features:

- Unique proximity key fob per resident programmed to only give access to their floor and any other communal areas relevant to them.
- Every lift must be floor specific proximity reader controlled.
- Every stairwell door onto a floor must be proximity reader controlled.
- Every ground floor stairwell entrance door must be proximity reader controlled.
- Every branch corridor door leading to dwellings must be proximity reader controlled.
- Ground floor stairwell entrance door with a visitor door entry panel with integral resident proximity access control, allowing the visitor to call the resident and request access into the stairwell so that the "Meet & Greet" can take place at the door from the stairwell onto their actual floor.

- Ground floor lifts with a visitor door entry panel with integral resident proximity access control, allowing the visitor to call the resident and request the enabling of the lift call button.
- Lift with floor specific keypad code control (each resident can have unique keypad code for their visitor).
- Lift with a visitor door entry panel allowing the visitor to call the resident and request the enabling of a specific lift floor button.

26. Each lift must be equipped with floor specific proximity access control that is an integral part of the fully and remotely programmable resident access control network. The lift proximity reader system feature means therefore that the proximity key fobs issued to residents are programmed so that they only enable specific lift floor button(s) in order to restrict each resident to their floor only.

27. All doors, vehicle gates, barriers and lifts that provide a means of accessing into the housing development, into any block or core, onto any floor or corridor, into any car park, communal garden or allotment must be proximity reader and/or radio transmitter network access controlled.

28. All visitor ground floor internal lobby doors to be proximity reader networked access controlled. The objective is to create a secure lobby.

29. All bin, recycling and bike stores to be proximity reader networked access controlled.

30. All communal gardens, podiums and terraces must be proximity reader network access controlled.

31. All vehicle gates and barriers to be radio transmitter networked access controlled for cars and proximity reader networked access controlled for cyclists. Both systems are to be on the same site wide access control network and fully remotely programmable.

32. The visitor door entry and resident access control system must have the facility to record and identify the location, user, type, time and date of every system event, and provide this information both in real-time and via remote data-retrieval. Sufficient memory storage must be available for a period of not less than 30 days.

33. Access control to the block(s) and carpark(s) by the residents is to be based on a fully integrated and networked proximity key fob and radio transmitter system. This is a requirement for Secured By Design certification from 2014 onwards. Radio access control for vehicle gates is also a requirement for Equality Act 2010 compliance. The proximity key fob readers and radio transmitter receivers must be remotely programmable and provide a full log of all visitor and resident system events via BATICONNECT CLOUD based server. No software will be required.

34. Proximity key fobs/cards/tags must be security encrypted - minimum MIFARE Classic 13.56 Mhz technology, or MIFARE DESFire 13.56 Mhz. Anti-clone protection is required to prevent access via duplicates meaning copies/clones/forgeries of manufacturer issued original credentials. The same applies for radio transmitters. The system must log and alert the management company of all access attempts using duplicates of original credentials.

35. Older technology proximity key fobs, for example 125Khz and 153Khz, are never acceptable.

36. Radio transmitters for vehicle entrances must also incorporate and utilise the rolling code security feature; transmission and reception.

37. Proximity key fobs and radio transmitters must each have a factory engraved visible unique ID number. This number must identify the scheme and the individual holder. The proximity key fob and radio transmitter ID numbers supplied must be recorded and a hardcopy list supplied by the security specialist.

38. Proximity key fobs and radio transmitters must be physically engraved so that each is individually visually identifiable. A resident must be able to look at their proximity key fob / radio transmitter and read its unique number. Proximity key fobs and radio transmitters (credentials) that force the system administrator to rely on and implement colour coding for differentiation and/or identification purposes because the credentials have no factory imprinted ID number are old technology and totally unacceptable.

    Quantities: 3no proximity key fobs required per plot, 1no radio transmitter required per secure carpark space (if applicable), plus 10% extras of both types. A printed list detailing the incremental sequential ID numbers of every proximity key fob and radio transmitter that have been supplied is required.

39. The access control strategy is based on the principle that a resident only needs to be issued with 1no proximity key and 1no radio transmitter which can be programmed via the BATICONNECT CLOUD to provide the exact door, gate, barrier and lift access authorisation profile for the entire development and, if necessary, for other remote developments. Master and facilities staff proximity key(s) and radio transmitter(s) must also be remotely programmable into all sites, any configuration as instructed.

40. The installation must allow for the provision of floor specific lift access control using 1no proximity reader only installed within each lift car as part of the networked BATICONNECT CLOUD system. A resident would present their proximity keyfob to this reader and it would only enable lift button(s) relevant to their access rights profile.

41. Residents must be able to open IPGUARD doors, gates and access floors via the lift using a “mobile access” feature on their smart phone. This feature must be part of the IPGUARD APP installed on their smart device.

    All usage of the ”Mobile Access” feature must, for security reasons, be logged and this information available to the management company 24/7/365 via baticonnect.com cloud. Management must be able to control who can use this feature.

42. Residents must be able to install the IPGUARD APP onto a tablet or iPad that has WIFI but does not have a SIM or associated phone contract.

43. Residents must be able to purchase an IPGUARD specific Wi-Fi compatible tablet with the IPGUARD APP installed from IP Door Entry Ltd that is dedicated solely for the IPGUARD system.

44. The IPGUARD display “Welcome screen” must be customisable with block name, address, housing association logo and similar if required.

45. The IPGUARD must be able to call up to 3,000 dwellings.

40. All access controlled doors irrespective of location require, on the secure side, a double pole (PTM & PTB) green mushroom type exit button (or similar Equality Act 2010 compliant button) fitted within 1 metre maximum distance of the relevant door pull/push handle at a maximum height of 1 metre AFFL. The door must never open over the exit button. Additional press to exit buttons are to be installed, on the secure side, at distances of over 1 metre from the relevant door to facilitate exit for disabled persons in wheelchairs (as instructed).

41. All internal only fire route access controlled doors must be interfaced with AOV/FIRE alarm systems, as applicable. On alarm activation the 12/24V fail safe electric locking on the door must automatically and immediately fail safe (unlocked).

42. External doors that give access into the building from public areas are not to be interfaced with AOV/FIRE alarm systems unless instructed otherwise.

43. Green plastic emergency exit breakglass units are not permitted by Secured By Design on final exit doors meaning external doors that give access into the building from public areas. Instead, a 2no Double Pole (DP) stainless steel button (each min dia 30mm for Equality Act 2010, Building Regulations Part M Access & Part B Fire Safety compliance) anti-vandal fail-safe emergency exit system with self-resetting latching hold-open of minimum 3 minutes is to be installed and fitted within 1 metre maximum distance of the relevant door pull/push handle at a maximum height of 1 metre AFFL. Resident's must be able to activate the Emergency Exit Device using a closed/clenched fist. The door(s) must never open over the emergency exit systems. Technical submittal required to confirm that the emergency exit device installed is fit for purpose in relation to H&S requirements.

44. Door release exit buttons and other such devices used for exiting via vehicle entrances, pedestrian gates and bike stores must be carefully positioned so that they are not reachable from the public side whether by hand, stick or other object. If visible from the public side, the button itself must be suitably protected from unauthorised activation whilst remaining at all times highly visible and easy to use by persons exiting. The door(s) must never open over door release exit buttons.

45. Full compliance with the building code is required to ensure guaranteed safe egress in the event of an emergency for all persons which includes persons with any disability as defined by the Equality Act 2010 meaning elderly, frail, arthritic, visually impaired, mobility impaired, amputees, persons with arm/leg in plaster and, of course, children and mother's carrying a child etc. Under no circumstances must any emergency egress require the simultaneous use of both hands to unlock and open a door. Fire escape doors and routes must be clearly identified by others. Emergency exit safety devices must be Equality Act 2010 compliant & Building Regulations Part M (Access) & Part B (Fire Safety) compliant.

46. Fireman switches are not permitted by Secured by Design outside the main entrance door (the final exit door) meaning the main external door that gives access into the building from the public side. Instead, a Gerda ACB (Access Control Box) manufactured by Gerda Security Products Ltd, enquiries@gerdasecurity.co.uk, must be installed outside the main entrance door into the building for the fire brigade. A separate supply only price per Gerda ACB box must be provided by the electrical contractor / security specialist. The Fire Installation Company is responsible for connection of the Gerda ACB, supplying & installing an override switch inside the ACB and the associated FP cabling back to the Access Control Equipment cabinet location. The security specialist is responsible for the interface connection at the Access Control equipment cabinet.

47. All electric locking supplied must have Secured By Design certification as part of a complete doorset (by the door supplier). Electric locking circuits must only use 4-core, 1mm² /core lock circuit cable ref 4 x 1 YY/LSZH per lock, or Fire Protected equivalent.

48. All cabling to visitor door entry panels, resident access control proximity readers, radio access control receivers, exiting devices, every locking device to be run on the secure side of the installation and concealed. Where cabling cannot be concealed it must be contained within metal conduit to prevent tampering.

49. Control equipment for the visitor door entry and resident access control systems must be housed in locked cabinets sited within secure internal locations.

50. If the 4G/GSM signal on site does not meet the thresholds laid out in the 'IPDE IPGUARD Signal Test' document, then the visitor door entry and resident access control system shall be supplied complete with 4G/IP/GSM router with aerial(s) by the security specialist.

51. The visitor door entry and resident access control system shall be supplied complete with its own data & communications package (4G/IP/GSM or other as appropriate) by the security specialist and will include unlimited communications and programming access for 12no months from handover.

52. Secured by Design requires that the data & communications package (remote connectivity) for the visitor door entry & resident access control must be live at handover and demonstrated as operational.

53. The security specialist is to liaise with the relevant Secured By Design DOCO and ensure compliance with the requirements of the latest edition of the Access Control section of Secured By Design, New Homes. Every scheme must comply with the latest Secured By Design guidelines.

54. The security specialist is to include for unlimited remote programming of resident visitor door entry and access control requirements for a minimum of 12 months for each building from handover date.

54. The security specialist is required to maintain, record and process all system and resident proximity and radio access control data as demanded by National Security Inspectorate (NSI) document NCP109.

55. Residents must be issued with a User Information Manual. This manual must advise residents how to register telephone numbers and purchase proximity keys and radio transmitters online. This process must be logged as required by National Security Inspectorate (NSI) document NCP109.

56. Site specific “As Installed” visitor door entry and resident access control system drawings and strategy, together with operating manuals must be provided.

57. The security specialist must attend concierge locations & management company offices (as instructed) to demonstrate full remote access and programming control for every block on every site. All programming control to be available via the BATICONNECT.COM CLOUD based server. No software is required.

58. Objective of this Performance Specification is to make best use of modern technology to maximise performance and cost benefits, and to achieve consistency of visitor door entry and resident access control systems, equipment, strategy, operation and programming on all housing developments. This specification must be strictly adhered to. The visitor door entry and resident access control will be the IPGUARD® 4G/IP/GSM Smart Visitor Entry System with BATICONNECT® CLOUD.

59. The security specialist, will issue a certificate to confirm that the visitor door entry and resident access control system installations and strategy comply fully with the requirements of this document.

60. The security specialist will issue a National Security Inspectorate (NSI) certificate to confirm full compliance with NSI document NCP 109.

61. Full ownership, with full access rights to the system, belongs solely to the Client reference the entirety of the systems, installations and programming.

62. The door entry and access control equipment can be commissioned by IP Door Entry Ltd.

    A current IP Door Entry Approved Installer shall be able to commission the entire system, themselves. Approved Installers are installers that have been trained to install and commission IP Door Entry Ltd systems. Non-current Approved Installers shall employ IP Door Entry or IP Door Entry’s agent to commission the systems. The installer must prove that they are a current Approved Installer, and this shall be confirmed with IP Door Entry Ltd.

63. Contact IP Door Entry Ltd for supply, training and technical support for IPGUARD & BATICONNECT CLOUD.

    Support contact email:
    support@ipdoorentry.co.uk

    Sales contact email:
    sales@ipdoorentry.co.uk

    Web: www.ipdoorentry.co.uk

    Tel: 08000-156496

IP DOOR ENTRY

08000 156496
sales@ipdoorentry.co.uk
www.ipdoorentry.co.uk
ipdoorentry

IP Door Entry Limited
Unit DC4 Prologis Park
Eastman Way
Hemel Hempstead
HP2 7DU

BATI CONNECT CLOUD
24/7/365
www.baticonnect.com