NATIONAL SECURITY INSPECTORATE (NSI)
Code of Practice for Design, Installation and Maintenance of Access Control Systems NCP 109 (Issue 1) July 2012.

NCP 109 (ISSUE 1) JULY 2012

The successful operation of an access control system… **The usefulness of the whole system and its security** and social acceptability **can be jeopardised by lack of care**.

This care has to extend to the **security of credentials such as tokens** and of information regarding the system, its design, installation and method of operation and to ensuring adequate maintenance, to preserve the security of access.

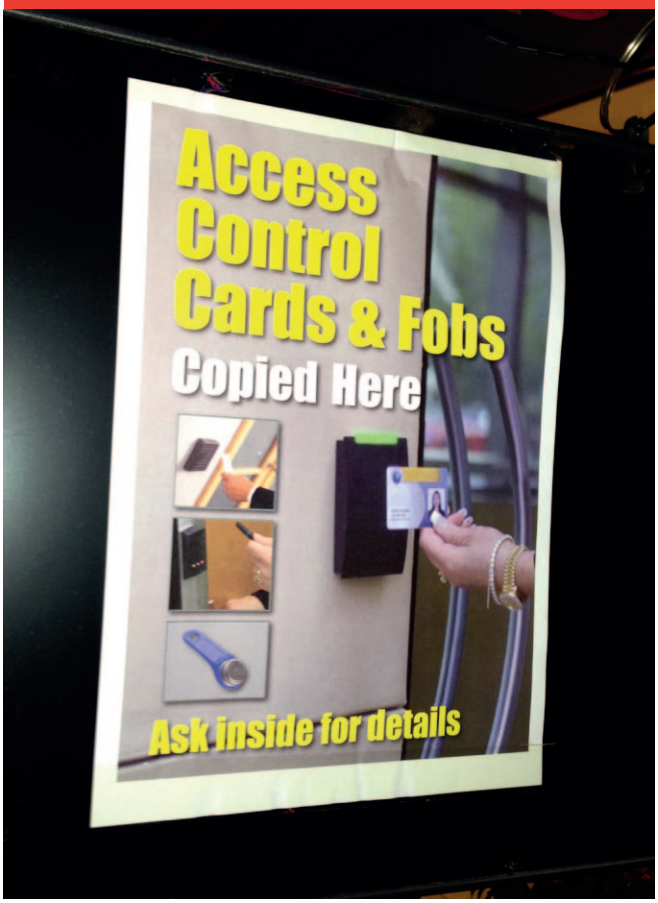
2.11 Credential. Any token or memorised information or biometric used to identify an individual to an access control system in order to verify user access.

NACD ADVISES:

Your client / development must be supplied with **security-encrypted**, visibly ID numbered, completely traceable proximity keys and radio transmitters.

Unscrupulous locksmiths and newsagents do not care about the security of your building and **are making unauthorised copies** of proximity keys and radio transmitters. Make sure your building and residents are protected against forgeries by using **security-encrypted** proximity keys and radio transmitters.

THIS MUST BE PREVENTED!



SECURED BY DESIGN 2014 (SBD 2014) Electronic Access Control Systems

Compliance requirements (1).

PROXIMITY KEYFOBS

KCP4000

Proximity keyfobs must be security encrypted to prevent unauthorised copying. Confirmation of security encryption is required.

SBD 2014
A1.1 **Proximity keys must be security encrypted to protect against unauthorised copying…**
(obviously same applies for radio transmitters)

RADIO TRANSMITTERS

TEL433

Radio transmitters must be security encrypted to prevent unauthorised copying. Confirmation of security encryption is required.

SBD 2014
38.1.1 **An access control system must be applied to all vehicular and pedestrian entrances to prevent unauthorised access in to the car park.**

38.1.2 Inward opening **automatic gates or roller grilles** must be located at the building line or at the top of ramps to avoid the creation of a recess. **They must be capable of being operated remotely by the driver whilst sitting in the vehicle**, the operation speed of the gates or shutters shall be as quick as possible to avoid tailgating by other vehicles. **This will allow easy access by a disabled driver**, and should satisfy the requirements…

RADIO ACCESS CONTROL FOR VEHICLE GATES IS ALSO REQUIRED FOR EQUALITY ACT 2010 COMPLIANCE.

Proximity keyfob and radio transmitter system must be fully networked = DUCTS REQD!

SBD 2014
A1.3 **Every proximity access controlled door and radio access controlled vehicle entrance will be included on the network.**
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 key fobs and radio transmitters.**

Proximity keyfobs and radio transmitters must be remotely programmable = COMMS REQD!

SBD 2014
A3.3 **The communications package required for full remote connectivity of the visitor door entry, resident access control and CCTV systems must be live at handover** and demonstrated to the DOCO.

Have you been supplied with the correct proximity keys and radio transmitters?

MAKE SURE YOU RECEIVE MODERN, SECURE AND EASILY MANAGEABLE PROXIMITY & RADIO ACCESS PASSES

	Proximity Keyfob Type	Security Encryption	SBD 2014 Compliant	Action
BEST PRACTICE	Visible unique ID number on each proximity keyfob and radio transmitter. All are site and sequentially numbered. +2 ✓✓	MIFARE (2ND Gen), DESFIRE. **SAME NUMBERING ID PRINCIPLES AS THE HIGHEST SECURITY MECHANICAL KEYS**	YES	Most advanced manufacturing process and obviously the best. The visible unique ID number on each proximity keyfob and radio transmitter identifies the site (scheme) and the user. Example key numbers: 9184500001, 9184500002, 9184500003 etc. Only this numbering system technology enables batch loading and deleting, total accuracy and control, and full audit traceability from manufacturer to end-user.  etc. *Logical and sequential numbering*
MINIMUM LEVEL	Visible unique ID number on each proximity keyfob and radio transmitter. +1 ✓	MIFARE (2ND Gen), DESFIRE.	YES	The system owner and user can accurately identify the proximity keyfob and radio transmitter simply by looking at it. Example key numbers: 2398165095, 9278276028, 1067939890 etc.  *Random numbering*
DO NOT USE: SUB-STANDARD TECHNOLOGIES	NO visible ID number on the proximity keyfob and radio transmitters. Manufacturer states "use colour tags to differentiate & administer" -1 ✗	MIFARE (2ND Gen), DESFIRE.	YES	**DO NOT USE.** Old technology manufacturing process cannot factory imprint unique ID number onto each proximity keyfob and radio transmitter. Administrator is forced to either buy a mix of coloured proximity keys, attach colour stickers / tags, or physically mark each key with a coloured pen. It is labour intensive, complicated and inherently inaccurate "people will make errors". It is fundamentally flawed, make sure that you are not supplied with old technology. 
	125 or 153Khz technology -2 ✗✗	None	NO	**TOTALLY UNACCEPTABLE** for all new developments / systems. Existing and growing unauthorised copying of proximity keys and radio transmitters voids security for residents. Start planning switch-over upgrade strategy for existing buildings (talk to manufacturer / supplier).

Check that you have been supplied with the correct proximity keys and radio transmitters.

PROXIMITY KEYS & RADIO TRANSMITTERS MUST EACH HAVE A VISIBLE UNIQUE ID NUMBER

EXISTING SECURITY PRINCIPLES FOR HIGH SECURITY MECHANICAL KEYS:

KABA
Master Key System

- The system owner is the "responsible person" and must use a registration card which carries the "responsible persons" signature and **unique system number** in order to purchase keys.
- A tailor-made key plan including **a logical key and cylinder numbering** system that is flexible enough to last.

ASSA ABLOY
Master Key Solutions Planned Systems with complete support

Multi level — Level 3
This is the **highest level of security** and offers the **most rigid key control.**

- Each key will be **stamped with a unique system number and key reference**.
- The keys can be **sequentially numbered to assist the end user in recording who has been given which individual key**.

YALE
PRO-KEY [Master Key System] BSEN1303 Grade 5 [or CEN5]

- The Yale Key **ID number is stamped on the key** and the cylinder, **it identifies the dealer, suite number and key reference**.

THE SAME SECURITY PRINCIPLES APPLY TO ELECTRONIC KEYS & TRANSMITTERS.

Proximity key fobs and radio transmitters are the electronic equivalent of mechanical keys.

Identification, numbering, monitoring, controlling and recording (traceability) of proximity key fobs and radio transmitters must follow the same successful procedures already existing for high security mechanical keys.

Proximity key fobs and radio transmitters must each have a factory engraved or **stamped visible unique ID number** to facilitate control of the system by the system owner and residents. Proximity key fob and radio transmitter numbers supplied for a residential building must be recorded by both the manufacturer and the security installer, and a list of these numbers together with the **unique identifying scheme or site number** provided to the system owner. Each resident must be able to **look at** a proximity key fob and radio transmitter and read **its number**.

The **unique visible ID number** on a proximity key fob and radio transmitter must enable the manufacturer to advise the authorised parties; when the access pass was supplied, the purchaser and the system owner.

KCP4000 Proximity Keyfob

- KCP4000 proximity keys are each **engraved with a unique 10 digit ID number.**
- The first 5no digits **identify the scheme/site**, the last 5no digits **identify the user**.
- They are also **sequentially numbered** for ease of administration control and security.

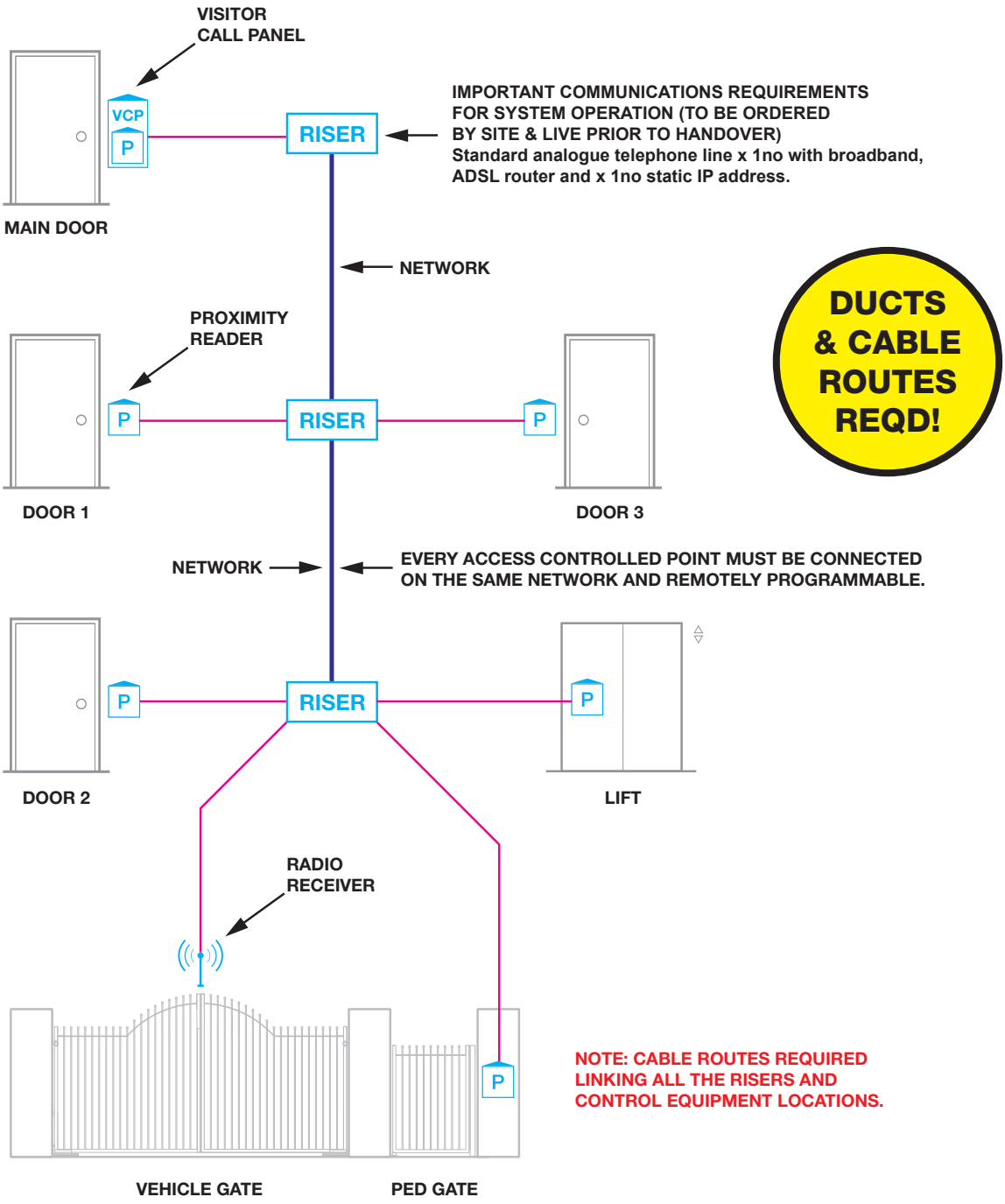
TEL433 Coded Radio Transmitter

- TEL433 radio transmitters are each **engraved with a unique 10 digit ID number**.
- The first 5no digits **identify the scheme/site**, the last 5no digits **identify the user**.
- They are also **sequentially numbered** for ease of administration control and security.

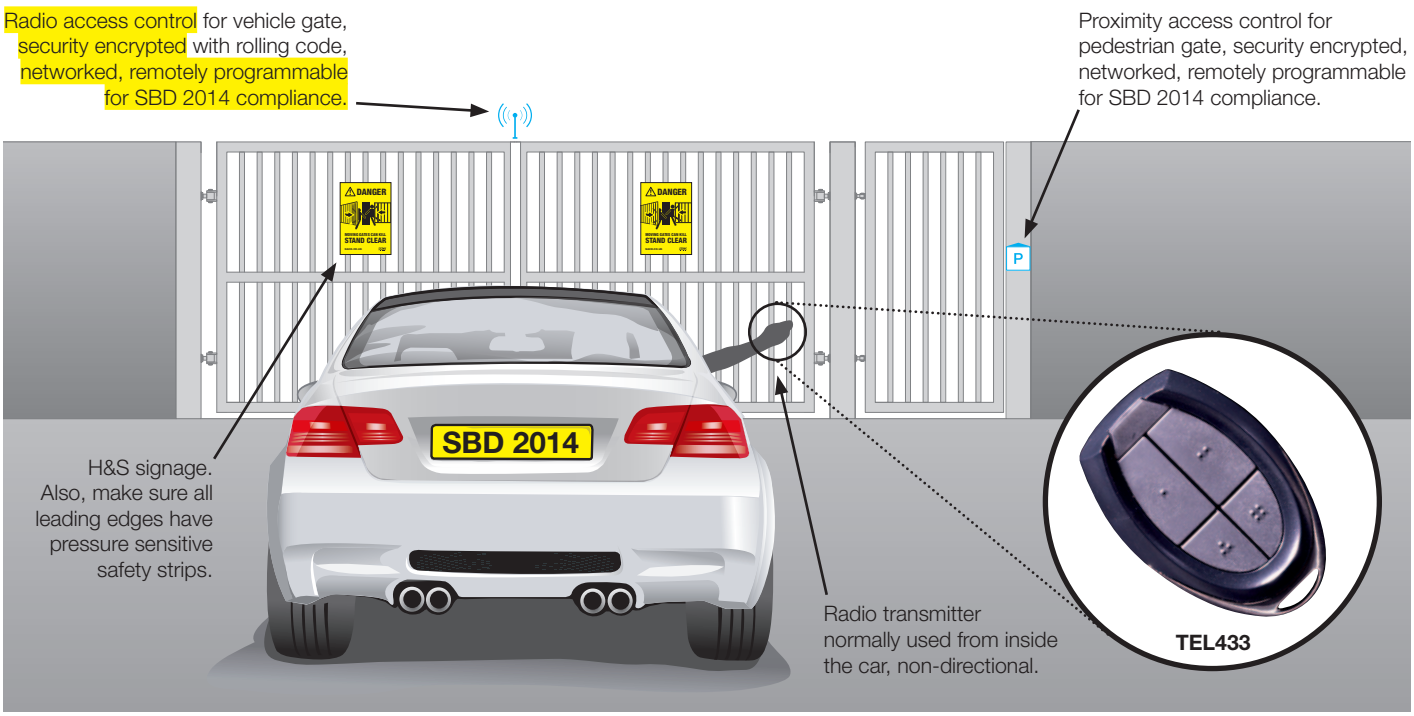
SECURED BY DESIGN 2014 (SBD 2014) Electronic Access Control Systems

Compliance requirements (2).

ALL ACCESS CONTROLS MUST BE NETWORKED AND REMOTELY PROGRAMMABLE



Vehicle Entrances must be part of an integrated access control strategy



The security encryption / identification / standards of the radio access control transmitters and the associated networked programming administration (on-site and remote) must be the same as for the proximity access control system. Both the radio and the proximity access control should be on the same network and share the same access control platform and programming. Whatever you are able to program to, or information you are able to obtain from, the proximity access control readers and keyfobs – the same must be available to/from the radio access control receivers and transmitters.

Radio transmitters must be security encrypted to prevent unauthorised copying. Confirmation of security encryption is required.

TICK ☐

SBD 2014

38.1.1 **An access control system must be applied to all vehicular and pedestrian entrances to prevent unauthorised access in to the car park.**

38.1.2 Inward opening **automatic gates or roller grilles** must be located at the building line or at the top of ramps to avoid the creation of a recess. **They must be capable of being operated remotely by the driver whilst sitting in the vehicle**, the operation speed of the gates or shutters shall be as quick as possible to avoid tailgating by other vehicles. **This will allow easy access by a disabled driver**, and should satisfy the requirements…

RADIO ACCESS CONTROL FOR VEHICLE GATES IS ALSO REQUIRED FOR EQUALITY ACT 2010 COMPLIANCE.

Proximity keyfob and radio transmitter system must be fully networked = DUCTS REQD!

TICK ☐

SBD 2014

A1.3 **Every proximity access controlled door and radio access controlled vehicle entrance will be included on the network.** 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 key fobs and radio transmitters.**

Proximity keyfobs and radio transmitters must be remotely programmable = COMMS REQD!

TICK ☐

SBD 2014

A3.3 **The communications package required for full remote connectivity of the visitor door entry, resident access control and CCTV systems must be live at handover** and demonstrated to the DOCO.