A guide to **Token and Reader Technology** in Access Control Systems

british security industry association

Introduction

It is recognised in the industry that there are various levels of security offered by the different credential types available in the market. Credentials can include tokens, fobs, badges, biometric images or memorised information. This guide is about tokens that store electronic credential information such as a numeric identifier or biometric data. The aim of this leaflet is to help you make an informed choice when selecting the credential for your security system.

Where electronic credentials are data stored in the memory of a card or token it is theoretically possible to create a process to clone any of them. However, manufacturers can incorporate processes and systems to ensure that these details remain confidential and not accessible to those who would want to duplicate them.

It is very difficult for manufacturers to prevent the cloning of credentials as the technologies they are designed around are usually open standard hardware (e.g. the majority of 125 KHz credentials).

Various types of cards and tokens are available. Like mechanical keys, some types offer greater protection against copying. However, the protection given may decrease over time as copying techniques improve. It is recommended that the type of credential used be agreed between the installer (or system supplier) and the client based on a risk assessment of the site.

Why do people clone cards and tokens?

There are several reasons why people will clone cards and tokens. This is not always done with criminal intent. Possible reasons are:

- To avoid paying official fees for replacement devices.
- To obtain duplicates in case of loss.
- To gain unauthorised entry to properties.
- To duplicate access privileges.
- Fraudulent use with time-and-attendance.
- Fraudulent monetary transactions (e.g. cashless catering or transport fares).
- To gain access to privileged systems or facilities (e.g. photocopiers).

Selecting an appropriate level of security

Different levels of security are required for different types of access control application, which is not to say that all different credential types do not have their place in the market.

When selecting a credential for your site you should consider what is most important for your application. A few considerations are listed below:

- Is it a system requirement to ensure that all credentials are unique? Or should, for example, the system administrator be allowed to generate a duplicate credential?
- How readily can the credential be copied by a person without access to the administration software?
- Do you require a higher level of security for your credential information and other data on the card/token? e.g. Encryption.

Other advised security measures for credentials

There are other steps that can be taken to mitigate any risk from a security breach or misuse:

- Ensure the fast removal of stolen credential authority from the system.
- Discourage the sharing of credentials between users.
- Do not leave credentials where they can be accessed when not in use.
- Encourage reporting of suspicious activity at the facility.
- Discourage "tailgating" where one employee uses a card to gain access and others follow without using their own cards.
- Utilization of relevant security reports to monitor for excessive use of a single credential.

- Use of time schedules so that access is only granted at expected times.
- Where possible, systems may identify use of multiple identical credentials.
- Where extra security is required, two-factor authentication (see BSIA Form 132) can be used. For example, PIN & token or Biometric & token.
- Alternatively extra security can be provided by the simultaneous use of two or more credentials ("dual key", "dual custody").

Be aware that in some cases a card or token can be copied without a criminal taking possession of it by using radio techniques to extract data. The criminal will need to be very close to the credential, typically within a few centimetres. This applies to 125kHz proximity cards which can be scanned, copied and / or replayed and to early, low security 13.56MHz memory cards.

Credential types

There are many different types of credential on the market and to help you to query your supplier/manufacturer we have graded, for the purposes of this document, the technology types into low, medium and high grades.

Within these grades different levels of security will still be offered but the following information should help you make a judgement.

1. Low Security – High cloning risk

Some IDs can be generated on site by the end user; this represents a very practical solution for some customers, but can allow duplicate credentials to be created. If this is not an issue then these IDs tend to be cost effective and are probably a good solution for your site.

Examples of this level are Magstripe and Barcode credentials, but you may want to question your supplier over any credential that can be written on site (e.g. Smart Cards). Some may offer a higher level of security, others may be readily duplicated.

2. Medium Security – Cloning possible with the right knowledge and tools

Within this category are manufacturer generated credentials, generally with an ID written to a chip with no encryption in place between the reader and the credential. That is not to say there isn't any security in the system to protect from duplication, but generally duplicates will need to be sourced through a manufacturer, a locksmith or somebody with specialist chip programming capabilities.

Examples of this level are 125KHz LF Credentials and 13.56MHz CSN Credentials.

3. High Security – Cloning unlikely as long as the manufacturing processes are robust

Within this category manufacturers should put in place a level of encryption on the credential in order to provide security. This can come in various guises and if this is required for your site it is advised that you do some basic research. Common schemes employed in the industry are DES (Data Encryption Standard) and AES (Advanced Encryption Standard). These are used to provide security and ensure two things:

- That the credential data remains protected.
- That readers used in the system can validate the credential before processing the data and passing it to the rest of the system.

Under these schemes the production of cards and tokens tend to be heavily controlled by the manufacturer and the ability to duplicate these credentials depends more on the level of protection of the processes and security scheme.

The BSIA accepts no responsibility for any loss or liability that may arise from reliance on information or expressions of opinion that are contained in this guide. References to other sources of information are for information only and the BSIA takes no responsibility for any material found in them.

Worcester
Kirkham House
John Comyn Drive
Worcester
Worcestershire
WR3 7NS

London
Market House
85 Cowcross Street
Farringdon, Islington
London
EC1M 6PF

tel +44 (0)845 389 3889
fax + 44 (0)845 389 0761
info@bsia.co.uk
www.bsia.co.uk

@thebsia