Yebo Lock and Key System User Manual

Author:	*YeboTech (Pty) Ltd*

INTRODUCTION

OVERVIEW

Yebo locks and keys enable a user to access many different kinds of locks using a single key. These products can be used to replace most conventional mechanical locks, and they offer improved convenience and security.

SCOPE

This manual describes in detail various aspects of the Yebo lock and keys not covered in the product information leaflets.

The information contained herein is intended for those wishing to obtain a deeper understanding of the product than that provided by the information leaflets.

TABLE OF CONTENTS

DOCUMENTATION

PRODUCT INFORMATION LEAFLETS

The information leaflets describe the basic usage of the products in day-to-day use. The information leaflets for different models of key may be found in:

Product	**Reference**
Smart Card AAA Key	YT-KEY_002S-IL-2.0

PRODUCT SPECIFICATIONS

The high-level product specifications are documented in the user requirements document YT-SYS-URS-2.0.

PRODUCT DATA SHEETS

The product data sheets contain summary information about each product. The products applicable to this manual are:

Product	**Reference**
Smart Card AAA Key	YT-KEY_002S-DS-2.0
Plug with Circlip Locking	YT-PLUG_002C-DS-1.1
8k Smart Card	YT-SC8K_001-DS-1.0

PRICE LISTS

Product price lists are available in YT-PRE2008-PL-1.0.

BASIC CONCEPTS

PRODUCT OVERVIEW

The Yebo lock and key system consists of electronic keys and locks.

Technically a lock consists of a *lockset*, which is all the hardware surrounding a lock such as the bolt and the handle; and a *plug*, which is the bit you insert they key into. A Yebo compatible lock is simply a

conventional lockset with a Yebo plug installed. The electronic locks therefore look very much like regular locksets, but you can recognize a Yebo compatible lock by the distinctive shape of the oval key-hole, illustrated below.

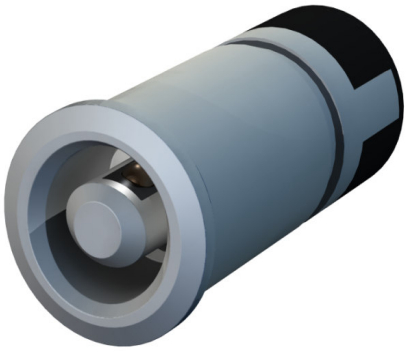

Figure 1: A Yebo electronic plug

The electronic key is about the same size and shape of a car-key, and works just like a regular key. To open a lock, you simply insert the key and turn. If the key is authorized, the lock will open. If the key is *not* authorized, then the key will still turn but the lock won't open. This is the one mechanical difference between a Yebo lock and a conventional lock.

Figure 2: A Yebo electronic key

The other major difference between Yebo locks and conventional locks of course is that they are electronic, which means a great deal of flexibility in managing which keys can access which locks. All keys support basic lock management functions for issuing authorizations, revoking authorizations, and wiping locks. This is what allows you to access a multitude of different locks using just one key, and to easily bar access to your premises without having to change locks or re-cut keys.

AUTHORIZATIONS AND VIRGIN LOCKS

The Yebo system revolves around the concept of *authorizations*. An authorization is a unique, secret electronic code issued to a key by a lock that enables a key to perform an *operation* on a lock. Usually that operation is OPEN (i.e. open a lock), but a lock may support other operations for which authorizations may be individually issued.

A very important kind of authorization is the *master authorization*. A master authorization gives a key the ability to invoke the ISSUE operation on a lock. This means the key is able to issue authorizations to other keys, including master authorizations. A key in possession of a master authorization has complete control of the lock, and such keys are termed *master keys*.

When a lock is brand new, it hasn't issued any authorizations to any key; such a lock is termed a *virgin lock*. A virgin lock will issue a master authorization to any key that asks for it. After issuing this master authorization, the lock is then only accessible to the key to which the master authorization has been issued. Usually one of the first things this master key will do is issue a master authorization to another key, since if that one key becomes damaged or lost then it will no longer be possible to manage the lock.

Authorizations may be *issued* and *revoked*, meaning that keys may be given an authorization to access a lock, and that the authorization may be subsequently taken away. Revocation however means that the authorization issued to a key is invalidated on the lock. The key may still be left in possession of the secret authorization key after the revocation, but it will be useless because the lock will no longer accept it.

It is important to note that every authorization issued is a unique authorization, so when an authorization is revoked, only that authorization (and any copies of it) are rendered invalid. Keys in possession of different authorizations will still be able to access the lock. This is unlike most locks, in which changing the lock renders all keys invalid.

SUPPORTED OPERATIONS

Every lock supports four basic operations:

- OPEN, to open a lock;
- ISSUE, to issue authorizations to other keys;
- REVOKE, to revoke authorizations from other keys; and
- WIPE, to wipe a lock of all authorizations and return it to its virgin state.

When a key is inserted into a lock, it will ask the lock to perform the operation currently selected on the key. Usually the default operation is OPEN, so if you simply insert a key into a lock it will try to open the

lock. You may however select a different operation to perform, and the manner of doing so varies from key to key. Usually you will press a button, and the key will indicate that a different operation, such as ISSUE, is selected. When you then insert the key, the key will ask the lock to perform the ISSUE operation.

LOCK IDENTITIES

Every lock in the world has a unique identity, which it will supply to a key when asked. When a key is inserted, the first thing it usually does is ask for the lock's identity. The key then uses this identity to determine what it is authorized to do on a lock.

SPECULATIVE INVOCATION OF OPERATIONS

Even if a key is *not* in possession of authorization to execute the selected operation, it will try to do so anyway. This is because the lock may either:

- Execute the operation because it does not require authorization; or
- Issue authorization for the operation.

An example of the first case is the QUERY_ID operation, which the key invokes to query the identity of a lock. Usually a lock does not require authorization for this operation.

An example of the second case is a virgin lock. A virgin lock will issue authorization for the ISSUE operation to the first key that tries to invoke that operation on the lock, thus making that key the master key for the lock. Alternatively, the lock may have been instructed by means of an ISSUE operation to issue authorization to the next key that attempts an operation.

ISSUING AUTHORIZATIONS

Authorizations are issued as follows.

Firstly, a key in possession of the master key must perform an ISSUE operation on the lock. Normally, this involves pressing a button on a master key, and then inserting the key into the lock. What this in effect does is tell the lock: "Issue authorization for the next operation requested." This means that the lock will authorize any key to perform any operation on the lock, for the next key inserted into the lock. Such a lock is in an *issue state*, and will remain so until another key is inserted.

If you then take some other key and inserted into the lock, it will usually try to perform the OPEN operation; in which case, it will be authorized to open the lock. If however it attempts to perform for example an ISSUE operation, then it will be given a master key. This explains why, when issuing a master authorization, it is necessary to select the ISSUE function on the key to be authorized before inserting it into the lock.

This means that care must be exercised when issuing authorizations: you must make sure that you do not accidentally leave the lock in an issue state; and secondly, that the next key inserted doesn't ask to perform an unintended operation (for example, ISSUE instead of OPEN). When issuing authorizations, you should always perform the operation yourself and not trust someone else to stick their key.

REVOKING AUTHORIZATIONS

Revocation of authorizations works in a manner very similar to the issuing of authorizations. Firstly the REVOKE operation is selected on a master key, usually by pressing the button twice. The master key is then inserted into the lock, and this puts the lock into a *revoke state*. This means that the next authorization used by a key in the lock will be revoked by the lock.

When the next key is inserted and it attempts to perform an operation, the lock will erase the authorization and tell the key it is no longer authorized.

SPECIAL NOTES ON ISSUE/REVOKE

Note the following:

1. Once locks have been put into an issue or revoke state, they will stay there until another key is inserted. There is no time-out on completion of the issue or revoke authorization process. You should therefore make sure that you don't accidentally leave a lock in an issue or revoke state.
2. If you have put a lock into an issue or revoke state with a master key, and that same key is re-inserted into the lock *without having pressed any buttons on the key*, then this will cause the key to cancel the issue or revoke operation.
3. If you attempt to revoke the only master authorization on the lock, the lock will refuse. The only way to remove all master authorizations from a lock is to wipe the lock. This is to prevent accidental deletion of the only existing master authorization. If however there is more than one issued master key, it is possible for a master key to delete its own master authorization.
4. Note that a key in possession of a master authorization can (and will) used that authorization to perform any operation, but only if it is not in possession of a suitable authorization for that specific type of operation. For example, it is possible to first issue an OPEN authorization to a key, and then an ISSUE authorization. The key is then in possession of two distinct authorizations: one for OPEN, and one for ISSUE.

   When the key is used to open the lock, it will use the OPEN authorization. If you then put the lock into a revoke state and perform the OPEN operation using the key, the OPEN authorization

will be revoked. But the key will still be able to open the lock, because when you re-insert it, it will simply use the master authorization. To bar the key entirely you would have to put the lock into a revoke state again, and then re-insert the key. The lock will then revoke the key's ISSUE authorization, even though this authorization was used to perform an OPEN operation. This is a rather unusual situation, but if in doubt you should always test a key after revoking its authorization.

5. You may wonder what happens if a key is already in possession of an authorization, or even an authorization that is no longer valid (for example, because the lock has been wiped); and you try to authorize it.

   All that happens is that the key is issued with a new authorization, and this new authorization overwrites the old one. When you do this on an already authorized key, the lock also invalidates the existing authorization. The net result is to re-issue the authorization, rendering any copies of the old authorization invalid.

KEY-SPECIFIC BEHAVIOR

The above sections should have provided you with a good general understanding of how the Yebo system works. The interface and indications on specific keys may however vary from key to key. For further information on individual keys, please consult the relevant key's user manual or information leaflet.

MANAGING AUTHORIZATIONS

PROTECTING AUTHORIZATIONS

If you leave your key lying about, your keys could be exploited by an 'attacker'. This section describes some of the possibilities and the measures you can take to ensure your key is not abused.

Obviously, if someone obtains access to your key they can access your locks. In this respect Yebo keys are no different to regular keys.

Unlike most conventional keys however it is not possible for someone with temporary access to your key to make casual copies so that they can access your locks later without your knowledge. While it is theoretically possible to make copies of the electronic tokens on the key, this would require destruction of the key or smart card housing the authorizations. Thus Yebo keys are generally more 'copy-proof' than regular keys.

What is a matter for concern is that someone with temporary access to your *master* authorizations and access to your locks could make use of your key to issue themselves authorizations without your knowledge. Alternatively, a child for example could inadvertently wipe the authorizations on locks. For this reason it is important that keys with master authorizations be protected from misuse by means of some *authentication* mechanism. The authentication mechanism is a means provided by the key that authenticates the person using the key, ensuring that only an authorized user can use the master authorizations on the key.

The simplest authentication mechanism provided is a PIN, or personal identity number. Keys are kept in a 'locked' state, meaning that the key can be used to open locks in a regular manner, but any access to master authorizations for the ISSUE, REVOKE or WIPE operations is barred unless the user first enters the PIN. Once the PIN is entered, the key typically remains unlocked until it has not been used for 2 minutes, at which point it automatically locks itself.

More advanced keys may support alternative authentication methods such as fingerprint scanning, and may also provide optional protection for OPEN authorizations.

PRESERVING AUTHORIZATIONS

If you lose all of the master authorizations to a lock, then you will no longer be able to manage the lock. You may still be able to access the lock using existing OPEN authorizations, but you will no longer be able to wipe the lock, or issue or revoke authorizations. It is therefore important to ensure that you maintain at least two copies of every master authorization.

It is less essential that you maintain copies of OPEN authorizations, as if you are in possession of a master authorization you can always fix the situation.

It is advisable therefore that when you acquire a new lock, and you have acquired the master key from the virgin lock, immediately use your key to issue another master authorization to a second key, for example a spare key or the key of your spouse.

RE-ISSUE OF AUTHORIZATIONS

Keys in possession of a valid authorization, even if only for an OPEN operation, may request a lock to *re-issue* an authorization. What this means is that a new authorization is issued for the same operation, and the old authorization is revoked. The effect is to render any copy of the authorization invalid.

The purpose of this feature is to allow someone who has lost a key, but is in possession of a backup key, to render the lost key useless to anyone who finds it.

Some keys will support a 're-issue' authorization function, which when invoked will cause every authorization on the key to be marked for re-issue. When the key is subsequently used in the locks, the authorizations will be automatically re-issued.

REVOKING AUTHORIZATIONS WITHOUT A KEY

You cannot revoke authorization for a specific key not in your possession as without it, the lock doesn't know which authorization to revoke. The most practical approach is to simply wipe the lock and re-issue authorizations to keys that still need to be able to access the lock. If you ever suspect that someone has access to a lock (for example, they have "borrowed" an unlocked master key and issued themselves access), wiping the lock guarantees that they will no longer be able to access the lock.

KEYS

ABOUT KEYS

The Yebo key is used to securely store the authorizations you received from locks.

Keys are typically the size of a regular key, and they house a battery and some electronics. You only ever need to carry one key to access all Yebo-compatible locks; that is the whole point of the Yebo system. There may however be a wide variety of keys to appeal to different tastes, and different keys will have different features depending on the anticipated user.

This section describes some of the important features of keys and what to look out for.

MEMORY AND SMART CARD KEYS

The biggest differentiator between is how authorizations are stored on keys.

- "Memory" keys are keys that store the authorizations in an internal memory in the key itself.
- "Smart Card" keys are keys that store the authorization on a replaceable smart card.

Typically, memory keys are cheap entry-level keys, and are intended for people who do not have their own key but need to have access to Yebo locks. Such users may include children, domestic help, or staff. The limitation of memory keys is that if the key gets damaged, the authorizations will be lost. It is therefore not a good idea to use memory keys to store lock master keys, unless additional master authorizations are maintained on other keys as well.

Smart card keys enable a user to easily swap the authorizations to another key simply by moving the smart card. The smart card is a small, very robust device that will survive many domestic accidents capable of destroying a key. The advantage of the smart card is that if the key gets damaged, or if you simply see a nicer key, you can easily swap the card over to the new key. Users who own Yebo locks and maintain master authorizations on their key should invest in a smart card key.

BATTERIES

The key battery is used to power both the key and the locks the key is inserted into. Typically a battery will last between two to five years in 'typical use' scenarios. "Typical use" is usually defined as accessing 20 locks per day.

If the battery goes flat, you will not be able to access locks. Every key supports a highly visible indication of when a battery is going flat, usually with at least a 3 month notice period. This indication consists of a brief flash of the indicator light every 10 seconds. When this indicator starts to flash, the battery should either be replaced, or you should ensure that you have a spare battery close at hand.

If the battery goes flat this does not mean that you lose any authorizations stored on the key. A key or smart card without a battery will retain its authorizations for many decades.

Battery life, battery replacement and the type of battery the key uses depends on the specific key model. Please consult the relevant information leaflet.

DOUBLE-ENTRY LOCKS

INTRODUCTION

Double-entry locks are locks that contain two cylinders on each side of the door. These locks are typically fitted with a 'profile' cylinder that contains keyways on opposite sides of the lock.

MATCHED AND UNMATCHED CYLINDERS

There are two kinds of profile cylinders:

- *Matched* cylinders, which make each side of the lock behave like a single lock;
- *Unmatched* cylinders, which make each side of the lock behave like separate locks.

When using matched cylinders, the two keyways in a double-entry lock operate much like a single lock, in that issuing authorization on one side of the lock will allow the holder to access the lock from the other side as well. It is not therefore necessary to issue authorizations from both sides of the lock when using matched cylinders. The same applies to acquiring the master authorization from a virgin lock; acquiring the master authorization from one side of the lock will make the key a master key for the other side of the lock as well.

When using unmatched cylinders, the two keyways behave like independent locks. When acquiring the master keys from a virgin lock, it is necessary to acquire the master key for each one as if they were independent locks. When you issue an authorization to access the lock from the one side, it does not mean that the holder can access the lock from the other side as well. So for example you could authorize a

key to open a door from the inside, perhaps as a means of egress in the case of fire, but not from the outside.

The choice of matched or unmatched cylinders depends on your application. Generally speaking, unmatched cylinders are more secure and flexible but there is a slight inconvenience in having to manage authorizations on both sides o the lock. Matched cylinders are more convenient but slightly less secure; see 'special precautions' in the following section.

SPECIAL PRECAUTIONS WHEN USING MATCHED CYLINDERS

There are special precautions that should be observed when issuing and revoking authorizations on matched cylinders:

- If you issue authorizations to multiple keys, ensure that you either always issue the authorizations from only one side of the lock; or alternatively, after issuing an authorization to a key you always test it immediately on the other side of the lock before issuing another authorization.
- When you revoke an authorization, make sure you revoke the authorization from both sides of the lock.
- When you wipe a lock, make sure you wipe both sides of the lock.
- Do not issue more than 1,008 authorizations from just one side of the cylinder before inserting the authorized keys into the opposite side of the cylinder.

Failure to observe the above precautions could result in a key that has been issued an authorization not being able to access the opposite side of the lock; or a key with a revoked authorization being able to access the lock from one of the sides.

Should for any reason you find that an authorization issued from one side of the lock does not work on the other, you can attempt the following remedies:

- Issue the authorization from the *other* side of the lock, and then try it in the opposite side;
- Wipe both cylinders using your master key and re-issue the required authorizations.

GENERAL RECOMMENDATIONS

Since it is not always obvious whether the lock you are using has matched or unmatched cylinders, it is recommended that you always test a key on both sides of the lock when issuing authorizations so as to avoid any surprises.

AUTHORIZATION CAPACITIES

OVERVIEW

Individual data sheets may provide cryptic specifications about authorization capacities. This section contains further information about what these parameters mean.

KEY AUTHORIZATION CAPACITIES

A key has to store the identity code of every lock it accesses in order to recognize the lock when it is inserted. In addition, the key needs to store every authorization it receives from a lock. The number of locks a key can access is therefore related to the size of its memory.

There are two kinds of key:

- Memory keys, which contain a fixed memory capacity (usually about 8k (bytes) memory);
- Smart card keys, which can accept smart cards of different sized memory starting at 8k[1].

Typically, 64 bytes are required to store both the identity of a lock and an authorization to perform an operation on that lock, so an 8k memory provides capacity for 128 authorizations to different locks.

What happens if for example a lock is wiped and a key is still in possession of an authorization (now no longer valid) to that lock?

One of a number of three things:

- If the key is never subsequently inserted into that lock, then the authorization will remain on the key forever, occupying memory space. The only way to remove this authorization would be to make use of a key management utility.
- If the key is subsequently inserted into the lock, the lock will tell the key that the authorization is no longer valid. Some locks will provide *strong evidence* of this, meaning that the key can be certain that the advisory really is from the original lock and that it can safely delete the authorization.
- Otherwise, a key will usually require three or more notifications that the authorization is invalid before deleting it. This is to prevent accidental erasure in the event of a glitch or error. Some keys may never erase the authorization unless strong evidence is provided so as to prevent a malicious attack called the *key erasure attack*.

Under normal circumstances, a consumer's key may accumulate a few 'dead' authorizations over a period

[1] At the time of writing, only 8k smart cards are available.

of years, but this is nothing to be worried about as most keys have more memory than the typical user will require in a lifetime.

PLUG AUTHORIZATION CAPACITIES

The standard consumer plug may be specified as having a capacity of '227 simultaneous authorizations with 7,264 unique authorizations between wipes, and a limit of 65,536 wipes'. What this means is that:

- You can issue only 227 authorizations simultaneously, so that up to 227 keys can have simultaneous access to the lock;
- Between lock wipes, there are only 7,264 *unique* authorizations. If you issue more than 7,264 authorizations between lock wipes, then some of the secret authorization codes issued will start to be re-used. This may occur if for example you have a high turnover of keys, and authorizations are being frequently issued and erased.
- You can wipe a lock up to 65,536 times.

If you exceeded the 227 simultaneous authorization limit, you will have to revoke some authorizations before you can issue any more.

If you have exceeded the 8064 authorization issue limit, then it is still possible to issue more authorizations. However, the implication is that it is conceivable that an old key still in possession of a previously revoked authorization will be able to access the lock as a result of that authorization being re-used.

When a lock is wiped, a completely new set of authorizations is created, so wiping a lock is an absolute guarantee that no previously issued authorization will ever be valid. However, even this has a limit: if you wipe a lock more than 65,536 times, then it will indeed start to re-use old authorizations.

Most consumer applications will never approach anywhere near these capacity limits, and when assets such as homes or automobiles change hands the lock is typically wiped anyway. If however you are employing a lock in a small business environment, you should take particular note that if you do approach the 8064 issue limit, which could conceivably occur over a period of years if you have a large staff turnover. It might then be possible for an old key with a previously revoked authorization to access the lock. In this situation you may wish to wipe the lock and re-issue all authorizations.

Different cylinders may support different limits depending on their memory capacity. Please consult the relevant data sheet.