



...simple, easy, quick, hassle free.

## **ITSO: Customer Media Personalisation and Certification**

Version	Date	Comment
Issue 1	28 July 2009	Initial Publication



...simple, easy, quick, hassle free.

## 1. Introduction

ITSO supports a number of varieties of Customer Media (CM) and ITSO Shells can be loaded onto CM by a Personalisation Bureau at initial creation, by a Retail POSTs owned by an ITSO Licensed Member or at Terminals owned by a third party Card Issuer.

Whilst ITSO does not wish to specify the complete personalisation process of a media on which other applications reside, unless there is a minimum security level applied to the loading of ITSO Shells onto a Licensed Member's CM, there is a risk that the media may remain open to attack. Similar criteria need to apply if the ITSO Shell is loaded on a CM that has been issued by a third party (i.e. a bank or other authority); however the control ITSO has over this process can only be agreed by mutual consent through the Licensed Member.

This paper sets the minimum requirement to ensure that when an ITSO Shell is loaded onto a CM platform:

- The configuration of the CM complies with at least the minimum level of security required by ITSO
- The compliance assessment regime embraces all the available CM configuration options
- The retailing of ITSO Shells complies with at least the minimum level of security required by ITSO
- The compliance assessment regime covers the retailing of ITSO Shells
- Interoperability between third party CM and compatible schemes can be assured.

## 2. Minimum CM configuration requirements

These requirements are set to give assurance that any CM does not have weaknesses that leave the ITSO Shell open to attack.

- Any Personalisation Bureau adding an ITSO Shell to a CM must maintain an appropriate level of overall security and in particular ensure CM and ITSO keys are not vulnerable to misappropriation when loading a CM. The same level of probity shall apply when personalising additional applications on the same CM.
- CM operating systems must have a level of security that mitigates against tampering with their content (particularly for CMD2 Applets on Java card or NFC phones)
- Any transport keys used to load a Shell on a CM must be changed after personalisation and diversified by CM / Shell instance in an acceptable manner
- Any keys used in the above must be securely held by the parties involved and kept available for future use should the ITSO Shell need to be replaced.. (the alternative is to destroy the card and issue a new one).

### 2.1 Additional requirements for use with co-resident applications

These additional requirements must be met where an ITSO CM owner also creates space on their CM for additional third party applications that may be added later.

- Any keys that are needed to allow that application to be further personalised by a third party application owner must also be diversified by CM instance.
- Such keys will be stored securely by the CM owner and only released to the third party application owner when they take over control of the space.



...simple, easy, quick, hassle free.

- It is incumbent on the CM owner to ensure that any additional applications meet good ethical standards before keys are released.
- Where an application is subsequently personalised by the application owner then CM settings will allow them to change any keys used within that application providing they ensure that any replacement keys are diversified per CM instance in an acceptable manner.
- Any keys used by all parties involved are securely held and kept available for future use should the third party application ever need to be deleted (the alternative is to destroy all applications on the card and issue a new one).

### **3. Testing Multiple CM configuration options on CMD2**

For CMD2, the generic operating system may have a SW application loaded onto an underlying operating system that is used to emulate an ITSO CM carrying an ITSO Shell. To ensure that the many combinations of CM platform as supplied by the card manufacturer (i.e. Java Card) + CM application SW (i.e. applet) + ITSO Shell issued by an LM will interoperate within the ITSO environment it is required that the CM Platform Hardware, the Application SW and the ITSO Shell are all tested as part of the overall ITSO approval, certification and verification process:

#### **a. CM Platform Approval**

This shall be given separately to each unique build standard. This shall be verified by an approved ITSO Test House adding and testing the platform using test application SW and a defined range of test Shells (i.e. small, default and large)

#### **b. Application SW Approval**

This will be given separately to any a given version of Application SW. This shall be verified by an approved ITSO Test House adding the Application SW to a defined range of approved platforms and then carrying out the tests as for CM platform Approval

#### **c. ITSO Shell Certification**

This shall be given separately for each unique build standard of the platform hardware having a given version of an operating system with additional application SW as required configured with the configuration(s) of Shell (i.e. small, default and large) that are to be issued by the Shell Owning Licensed Member(s). The resultant fully personalised CM + ITSO Shell shall be verified by an approved ITSO Test House. The Test House shall utilise a selection of test IPEs as part of the process. In the event that a Personalisation Bureau wishes to prove its ability to provide functioning CM / Shell combinations then they may submit an agreed "Test Shell" for Certification but this shall not remove the obligation for a Licensed Member that uses that Bureau to verify their own Shell configurations individually through an approved ITSO Test House.

### **4. Retailing of ITSO Shells**

The ITSO specification does allow Shells being created by a Retail POST either attended or unattended. However in order to maintain the integrity of the ITSO environment it is essential that such a Retail POST comply with the minimum configuration requirements listed in Section 2 above.



...simple, easy, quick, hassle free.

In addition to a normal POST that does **not** retail Shells, a Shell Retailing POST will need to meet additional criteria as follows:

- a) Where the Shell Retailing POST operates off-line, the Licensed Member shall ensure strong requirements for physical security of the POST are met and the POST ISAM shall be configured to shorten the time it may be used when off line from its first-line HOPS
- b) It shall be incumbent upon the Licensed Member responsible for Shell Retailing POSTS to advise ITSO of any misappropriation of Retail POSTS or ISAMs
- c) Where a Shell Retailing POST issues CM that are pre-encoded with Shells and at least one IPE then the CM shall be distributed and held in a secure manner and be pre-encoded in such a way as to be un-usable unless activated by the retailing terminal when sold.
- d) When Loading ITSO Shells onto third party CM the ITSO Licensed Member must agree criteria with the third party Issuer that meet or exceed the above ITSO requirements and those of the ITSO License.

END