

eEpoch

(eEurope Smart Card Charter proof of concept and
holistic solution)

**Annex (informative) to the document
LOAD of APPLETS protocol
Schlumberger**

GUIDELINES FOR PERSONALIZATION

Document Control Sheet	
Responsible Author(s):	Mourad Faher
Organization:	Schlumberger
Subject / Title of Document:	Personalization Guidelines for Load of Applet protocolOP cards Issuers
Related Task('s):	
Deliverable No.	D3.2
Save Date of File:	16.03.2003
Version Number:	1.0
Ref./File Name	Annex to [LoadApplet_for_IASenabledCard.pdf]
Number of Pages	5

Document Distribution			
Membertype	Organization	Name	Distributed
Web page	[Project Web Site]	Internet	DD/MM/YY
Contractors / Partners			
European Commission			
Additional			

Contents

1.	Introduction	4
1.1	Revision log	4
1.2	References	4
1.3	Abbreviation	4
1.4	Personalization guidelines.....	4

1. Introduction

1.1 Revision log

Version / Date	Brief Description of Changes, Name
Draft 1.0 / 01-09-03	Initial document : Mourad Faher
V1.0 / 20.10.03	Revision: Mourad Faher

Table 1: Revision log

1.2 References

[LoadApplet] LOAD of APPLETS Protocol, Version 1.0, 14.05.2003, Schlumberger

[E-SIGN K, Part 1] Application Interface for smart cards used as Secure Signature Creation Devices, Version 1.06, 10.07.2003, CEN/ISSS WS/E-Sign Draft CWA Group K; Part 1 – Basic requirements

[E-Sign K, Part 2] Application Interface for SmartCards used as Secure Signature Creation Devices, Version 0 Release 11, 26.06.2003, CEN/ISSS WS/E-Sign Draft CWA Group K; Part 2 – Optional features

[CIA] Cryptographic Information Application, Version 0.2, 22.08.2003, Giesecke & Devrient

[IAS IOP Interface] IAS IOP Interface, Version 1.1, 20.10.2003

1.3 Abbreviation

1.4 Personalization guidelines

Main aspects of personalization process for eEpoch Open Platform IAS-enabled cards:

The Open Platform Secure Messaging protocol being adopted for the load of Applets during both the pre and post-issuance phases, the Personalization Bureau may use it accordingly in its secure environment to load the application embodying the eServices offered by the card.

The IAS Application itself may be loaded as such in EEPROM, or embedded in ROM.

Each Applet loaded onto the card consists of its bytecode and its cryptographic objects. Those cryptographic objects are to be stored in an ISO 7816-15 (PKCS#15) compliant file system, and they consist of the actual data representing the objects and the references (or pointers) to those data.

The Applet's bytecode is loaded according to the Open Platform specification while the cryptographic objects are to be loaded depending on the card architecture. Either the PKCS#15 File System is hard implemented or logically represented. In the former case, the cryptographic objects' references are stored in the PKCS#15 files while in the latter case they are stored along with the related cryptographic object's data within Java containers.

To summarize, the Load of Applets process is divided into at least two steps:

- The pre-personalization represented by the load and installation of the applications' bytecode,
- The personalization corresponding to the load of the cryptographic objects (PIN(s), Biometrics, Private Keys, Public Keys, Certificates...) associated with the application.

The personalization process is performed transparently and may be handled by the Card Manager through a Secure Channel. The Card Manager may request the IAS application to store cryptographic objects.

From the eService Applet standpoint, the methods involving cryptographic objects / operations may be accessed through the Shareable Interface implemented by the IAS application [§ IAS IOP Interface]

At issuance, the OP cards may be still enabled for subsequent load operations, provided the Issuer allows the OP IAS-enabled cards to update or upgrade or even add new applications with new eServices following a controlled protocol. But the cards may also have their load application capability disabled before they are issued to cardholders. In effect, it remains up to the Issuer to lock the Load feature through its on-card Security Domain for example.

Guidelines will be provided to the Issuer for personalization purposes.