*e*Epoch

(*e*Europe Smart Card Charter proof of concept and holistic solution)

Action Research Document:
The ISO 7816 Concept of "Security Environment"

Judith Liu-Jimenez / Raul Sanchez-Reillo

GUTI – University Carlos III of Madrid

Project Funded by
European Commission
Information Society
IST-2001-37936

Version 1.0
Public
10/05/04

eEpoch
WP 1 – Action Research Responsible
Raul Sanchez-Reillo
GUTI – University Carlos III of Madrid
e-mail: rsreillo@ing.uc3m.es

Action Research Document

Document Control Sheet	
Work package 1 Chair	Theo van Sprundel (Axalto, a Schlumberger Company)
Responsible Author(s):	Judith Liu-Jimenez / Raul Sanchez-Reillo (GUTI-UC3M)
Organization:	University Carlos III of Madrid
Subject / Title of Document:	Exploitation and Dissemination plan
Related Task('s):	WP 1, WP 5
Deliverable No.	The ISO 7816 Concept of "Security Environment"
Save Date of File:	14/05/04
Version Number:	1.0
Ref./File Name	SecurityEnvironment.doc
Number of Pages	11
Distribution Category: (P/R/I)*	P
Nature of the Deliverable (T/M/W/R/O)**	T
Target Date	26/05/04

*Type: **P**: Public, **R**: Restricted, **I**: Internal

Nature: **T: Technical, **M:** Management, **W:** working document, **R:** Review, **O:** Other

Document Distribution			
Membertype	Organisation	Name	Distributed
Webpage			
Contractors / Partners	All eEpoch Participants		
European Commission			
Additional			

Change Control Sheet

Date	Issue	Affected Sections	Author / Reference Comments

Review and Approval of the Document

Organisation Responsible for Review	Affected Sections	Approval / Comments	Date

Contents

1. Introduction

This document is intended as an analysis of how close is ISO 7816 standards to the current idea of Security. Security Environments have change deeply during these last years, specially when open networks started to gain importance in sensible data exchange. ISO 7816 is a set of documents created long time ago, with different updates every 5 years. Therefore it could happen that the major ideas shown by ISO 7816 about security, could be far from what today are considered as "best-practices" in security.

This document tries to give an independent view about what it could be understood from reading ISO 7816. Particularly parts 4, 8 and 9 are of great importance in security definitions, being part 8 the one which refers directly to the "Security Environment" concept.

1.1 Context within eEpoch European Project

This document is considered as a report, result of the work being carried on in the Action Research Activity in eEpoch. Action Research is a methodology based in implementing designs by a dynamical study of its viability and performance, being able to make changes as first results comes out from the design.

Action Research is considered inside eEpoch in its Work Package 1, and it is at the service of all partners in eEpoch Consortium as an aid for any potential problem that they consider it can arise. Some issues has been located, being decided to submit two documents based in two different targets. One of those documents is the one presented here. The other one is about how to implement eServices with Interoperable eID.

1.2 Structure of this Document

This document is structured as follows. After this initial introduction, a section devoted to the ISO 7816 standard is presented, including an overview to the security concepts involved in the standard. After that, a section regarding how to understand "Secure Environments" will be placed, followed by another one about the potential inconveniences.

2. The ISO 7816 Standard

The ISO 7816 Standard is prepared by the Joint Technical Committee ISO/IEC JTC1, inside its subcommittee SC17, which is devoted to Cards and Personal Identification. This Standard is divided in 15 parts which describe different aspects about Integrated Circuit Cards with Contacts. In few lines the different specifications can be divided in:

- Physical layer (parts 1 and 2)
- Electronic Signals and Protocols (parts 3, 10 and 12)
- APDUs (parts 4, 7, 8 and 9)
- Data elements and coding (parts 5 and 6)
- Collateral technologies (parts 11 and 15)

From all these parts, 3 of them are related to security issues. Those parts will be describe in the following subsections.

2.1 ISO 7816/4: Organization, Security and Commands for Interchange

Part 4 is one of the most important ones in smart card specifications. It gives all the basics in the application level, allowing, whenever possible, the guidelines to reach interoperability as well as secure procedures. Its contents can be summarized in:

- APDU structure and coding of the elements of an APDU
- Structures for applications and data
- Security Architecture:
  - Attributes and coding format
  - General Mechanisms
- Definition of Secure Messaging and one of its possible implementations
- An initial pre-specification of "secure environment"
- Commands for Interchange
- Application-independent Card Services

One of the potential problems of this part, is that it leaves many issues open, so that it could be misused and be able to have a card following the standard but without being really interoperable and without the security demanded by users.

2.2 ISO 7816/8: Security related interindustry commands

This part complements Part 4, including many elements regarding security. One of the most important things is the definition of **Security Environment (SE)**, which is defined as *"The SE in a card is the logical container of a coherent set of fully specified security mechanisms which are available for reference in command executed by the card"*.

The different components of a SE could be described by a set of Control Reference Templates (CRT), which are defined for:

- Cryptographic checksum (CCT)
- Digital signature (DST)
- Confidentiality (CT-Asym / CT-Sym)
- Hash (HT)
- Authentication (AT)

Also the time validity of a SE is defined, as well as all commands related to SE and CRTs

2.3 ISO 7816/9: Additional nterindustry commands and security attributes

Written as an extension to parts 4 and 8, this 9^{th} part is devoted to define the new demands of smart card industry. From its definitions the reader can find:

- Coverage of the Smart Card Life Cycle Status
- Description and coding of the security attributes of card related objects
- Definition of an extra set of commands for interindustry interchange
    - Mainly with commands related to control the access to Elementary Files (EFs) and Dedicated Files (DFs)
    - Also specifies data elements associated with these commands
- Establishment of a mechanism for initiating messages originated by the card

3. Understanding "Security Environments"

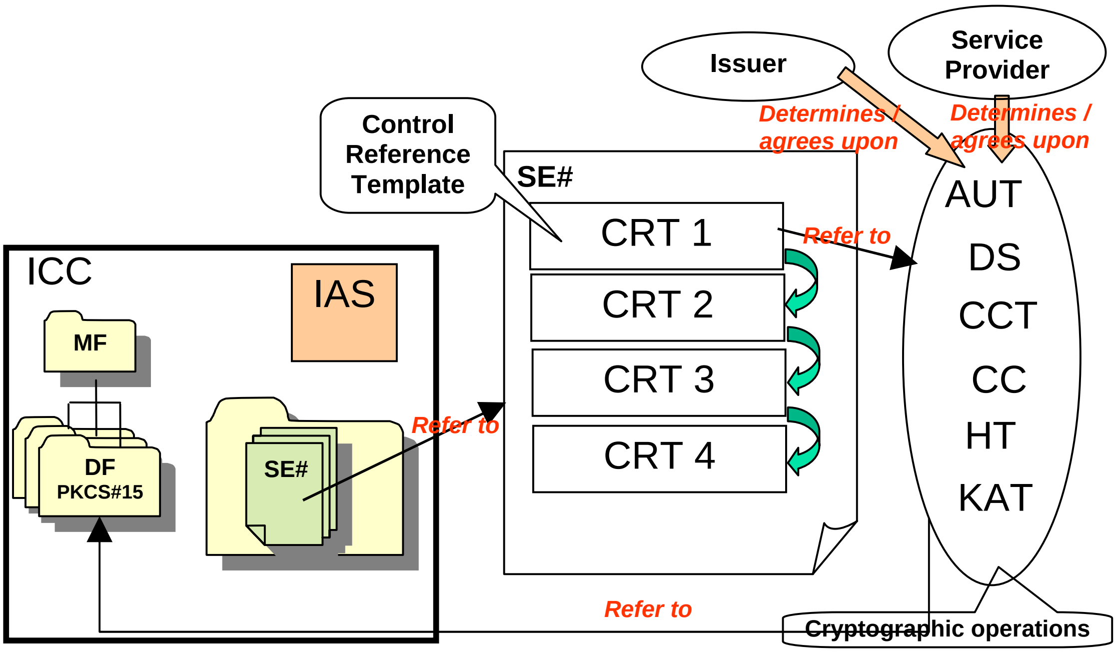
As stated above, the definition of what a security environment is, has been made in Part 8 of the Standard. This definition consists on a set of commands and a full set of data elements. This sets of commands and data elements can be stored in a card under a determined SE number, and several SE can be defined in a single card, so that the application can choose the SE to be applied in the following steps along the usage of the smart card. Regarding the commands, they can be grouped in 4:

- Manage_Security_Environment
  - This is the "central" command, where the definition of the SE active in the card is done. It is used for:
    - Replacing the current SE by another SE stored in the card (RESTORE function)
    - Setting, or replacing on component of the current SE (SET function)
    - Saving the current SE under a determined SE number (STORE function)
    - Initializing cryptographic commands (such as, for example, computing a derived key)
- Perform_Security_Operation
  - This command initiates the computation of security operations. The security operations defined are:
    - Computing Cryptographic Checksum
    - Compute Digital Signature
    - Hash operation
    - Verify Digital Signature
    - Verify Certificate
    - Encipher
    - Decipher
  - This command may be preceded by a Manage_Security_Environment command, where the SE desired could be selected.

- Also, this command can have extra conditions for its proper completion, such as having selected a determined EF or DF, or having performed a previous operation, such as a Verify command.

- Manage_Verification_Process
    - This command can initiate the following operations:
        - Verify data used as a reference. This is needed to initiate the comparison within the card of the verification data sent from the terminal, compared with the reference data stored in the card (such as the Verify command defined in Part 4)
        - Changing reference data
        - Enabling of a verification requirement. This could be used to establish a requirement to compare the verification data with the reference data
        - Disabling of a verification requirement
        - Resetting a retry counter, to its initial value
        - Exchanging reference data, by initiating a comparison of the verification data with the reference data, to after that, conditionally, replace the existing reference data with the new reference data sent to the card in the command
        - The combination of resettin a retry counter and changing reference data
- Mutual_Authenticate
    - This command uses the same functionality as the Internal and External Authenticate commands (as defined in ISO 7816/4), using the same INS code as the one for External Authenticate
    - The Mutual Authenticate is based on a previous Get Challenge command, issued by the terminal, and a key, usually stored secretly in the card.

The following figure (donated by Mr. Mourad Fahrer from Axalto), tries to illustrate the relationship among the different actors in the SE within a card.


Issuer
Service Provider
Determines / agrees upon
Determines / agrees upon
Control Reference Template
SE#
CRT 1
CRT 2
CRT 3
CRT 4
Refer to
AUT
DS
CCT
CC
HT
KAT
ICC
IAS
MF
DF
PKCS#15
SE#
Refer to
Refer to
Cryptographic operations

4. Potential Inconveniences and Conclusions

The major inconveniences about the definitions of SE in ISO 7816/8, comes from the aperture of the standards. In order to allow inter industry compliance, no fixed requirements have been stated. Not even minimal security characteristics for the cryptographic algorithms have been defined. Therefore there could be a card following all points in the standard, but having, for example, a really weak set of cryptographic algorithms, so that security within that card is far below what should be expected. Fortunately, common practice by the industry does not allow this kind of problems, due to the fact that most of the industry is focused on using cryptographic means that assure a more than acceptable level of security.

Also, there could be a potential impossibility of reaching interoperability, due to the opening of the whole ISO 7816 standard, specially referring to Part 4. This is because with a determined group of codes for the CLA element in the APDU, anything outside the standard could be considered as compliant with ISO 7816.

Finally, in some cards and some applications, the definition of SEs, could lead to an extra overhead in command exchange between the application and the card. This should be designed in a way that the security overhead is time and computationally acceptable for the application in use.

4.1 Conclusions

Being aware of the potential inconveniences, and working with the ethic demanded by a security related industry, SE is a great help in the managing of security mechanisms within a smart card. SE definition gives the guidelines to be able to achieve a common way of understanding security in a smart card application.

Although is a potential inconvenience, the opening of the definition allows the integration of any new security technology, such as new cryptographic algorithms. Also, it allows de possibility of having different SEs in a single DF, being able to select one or another depending on the service demanded by the application.

When all partners in a European-wide project are fully compliant with this specifications, then Interoperability is much easier to be achieved.