

# **ESTONIA eID-eRP cards on CosmoX**

Differences with  
CosmoV8

## Table of contents

<b>Introduction.....</b>	<b>3</b>
Purpose of the document .....	3
<b>Discrepancies CosmoX vs. CosmoV8.....</b>	<b>3</b>
ATR.....	3
Platform level .....	3
IAS applet .....	3
SELECT command .....	3
PKCS#15 files.....	4

## Introduction

### Reference documents

#### Purpose of the document

This document sets out the usage differences between a Estonia eID/eRP card personalized on a CosmoV8 (with *LDS* and *IAS-ECC V2* applets) and on a CosmoX (with *TnD* and *ID-A* applets).

Except this, Estonia eID/eRP card personalized on a CosmoX behaves the same way than on CosmoV8, following [EST\_CosmoV8].

## Discrepancies CosmoX vs. CosmoV8

### ATR

ATR value has changed:

- CosmoV8, cf. [EST\_CosmoV8], : 3B **DB** 96 00 80 B1 FE 45 1F 83 00 12 23 3F **53** 65 49 44 0F 9000 **F1**
- CosmoX, cf. [EST\_CosmoX], : 3B **DC** 96 00 80 B1 FE 45 1F 83 00 12 23 3F **54** 65 49 44 **32** 0F 9000 **C3**

### Platform level

Manufacturing data (got through a GetData 'DF50' on *Issuer Security Domain*) are no longer available on CosmoX after perso, due to different traceability management on CosmoX.

### IAS applet

SELECT command

*IAS-ECC V2* applet on CosmoV8 was not checking proper setting of SELECT command P1 parameter, as per IAS ECC standards:

B8	B7	B6	B5	B4	B3	B2	B1	MEANING	COMMAND DATA FIELD
0	0	0	0	0	0	X	x	<b>Selection by file identifier</b>	
						0	0	- Select Root	Root identifier (0x3F00)
						0	1	- Select child DF	DF identifier
						1	0	- Select EF under the current DF	EF identifier
						1	1	- Select parent DF of the current DF. Upper limit = ADF or Root	None

For instance, putting '01' for P1 parameter for the selection of a EF actually selects the targeted EF, with *IAS-ECC V2* applet on *CosmoV8*.

On the other hand, this example fails with *ID-A* applet on *CosmoX*, as *ID-A* applet *does* check proper setting of SELECT command P1 parameter.

#### PKCS#15 files

Some differences exist within Middleware/PKCS#15 files:

- Deletion of "EF Container AWP", FID='F001', no more useful on *CosmoX* with IDplug middleware
- Certificate Definition files – 'CD' of ADF PKI & ADF QSCD: no 'update' access mode defined in 'accessControlRules' block, as update would require a device authentication with a symmetric key – [EST\_CosmoX]
- Data Container Object Definition files – 'DCOD':
  - DCOD of ADF QSCD is empty – [EST\_CosmoX]
  - DCOD of ADF PKI refers to minidriver files EF.CardId (FID='FD00') and EF.CardCf (FID='FD02') – [EST\_CosmoX], instead of EF.Container.AWP (FID='F001')