FINEID - S4-2

Implementation Profile 2 for Organizational Usage

v3.0

Population Register Centre (VRK)
Certification Authority Services
P.O. Box 123
FIN-00531 Helsinki
Finland
http://www.fineid.fi

Authors

Name	Initials	Organization
V. Rannou	VR	IDEMIA LTD
Linda Olkkonen	LO	VRK

DOCUMENT HISTORY

Revision Date	Author	Purpose
02/11/2018	V. Rannou	First edition
29/05/2019	L. Olkkonen	Second edition

Table of contents

1 Introduction

1.1 Purpose

This document intends to describe the electrical profile established for VRK cards. The MF, ADF, P15 files, and other Security Data objects will be listed and commented.

The card is the Citiz 2.17i with IDme 1.6i core. This card is compliant with Global Platform 2.1.1 and Javacard API 3.0.1.

Idme is a Javacard implementation of the Identification Authentication Signature for European Citizen Card v1.0.1 (IAS ECC).

1.2 References

Annex II of eIDAS regulation

2 Definitions

APDU	Application Protocol Data Unit
DES	Data Encryption Standard
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
QSCD	Qualified Signature Creation Device
SCA	Signature Creation Application
CGA	Certificate Generation Authority
SCP	Secure Channel Protocol based on GP 2.1
ISK	Initial Secret Key

3 Contact Chip description

3.1 Card

The Card chosen for this project is the Citiz 2.17i with Javacard Idme 1.6i instantiated

3.2 ATR

The ATR of the card will be

Parameter	Value
ATR	3BDD96008031FE450031B8640429ECC1739401808248
Protocol	T=0, T=1
Speed	Fi=512, Di=32, 312500 bits/s for fMax=5 MHz

3.3 Packages

Idme applet is instantiated with following AID: A0 00 00 00 63 50 4B 43 53 2D 31 35

4 IDme Profile

4.1 Files System for personalized cards

MF (3F00)	
Object Properties ADF ROOT	
File Type	DF
File identifier	3F00
AID	A000000063504B43532D3135
Security attributes Contact	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Create file EF	NEVER
Update file	PIN SE#04
Security attributes Contactless	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Create file EF	NEVER
Update file	NEVER

DF.ESIGN (5016)	
Object Properties DF ESIGN	
File Type	DF
File identifier	5016
AID	
Security attributes	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Create file EF	NEVER
Security attributes Contactless	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER

Deactivate file	NEVER
Create file EF	NEVER

EF.ATR (2F01)	
Object Properties EF ATR	
File Type	EF
File Length	6 Bytes
File identifier	2F01
Short File identifier	1D
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.DIR (2F00)	
Object Properties EF DIR	
File Type	EF
File Length	53 Bytes
File identifier	2F00
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER

Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.OD (5031)	
Object Properties EF OD	
File Type	EF
File Length	70 Bytes
File identifier	5031
Short File identifier	11
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.SN (D003)	
Object Properties EF SN	
File Type	EF
File Length	12 Bytes
File identifier	D003
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER

Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.CIAInfo (5032)	
Object Properties EF CIAInfo	
File Type	EF
File Length	129 bytes
File identifier	5032
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#4
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.AOD (4401)	
Object Properties EF AOD	
File Type	EF
File Length	105 bytes
File identifier	4401
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER

Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.PrkD (4402)	
Object Properties EF PrkD	
File Type	EF
File Length	221 Bytes
File identifier	4402
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.CD# 1 (4403)	
Object Properties EF CD#1	
File Type	EF
File Length	198 Bytes
File identifier	4403
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	

Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF.CD# 2 (4404)	
Object Properties EF CD#2	
File Type	EF
File Length	1024 Bytes
File identifier	4404
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#02
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

EF.CD# 3 (4405)	
Object Properties EF CD#3	
File Type	EF
File Length	187 Bytes
File identifier	4405
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	

Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

Data Objects (DCOD) EF (4406)	
Data Objects (DCOD) EF (4406)	
File Type	EF
File Length	1024
File identifier	4406
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

EF.CD# 4 (4407)	
Object Properties EF CD#4	
File Type	EF
File Length	1024 Bytes
File identifier	4407
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#02
Read binary	ALWAYS

Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

EF Object directory file (OD or ODF) (5031)	
EF Object directory file	
File Type	EF
File Length	70 Bytes
File identifier	5031
Short File identifier	11
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF CIAInfo (TokenInfo) (5032)	
EF Object directory file	
File Type	EF
File Length	129 Bytes
File identifier	5032
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#04
Read binary	ALWAYS

Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	SM SE#02

EF Unused Space (5033)	
Object Properties EF Unused Space	
File Type	EF
File Length	1024 Bytes
File identifier	5033
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#02 OR PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

DF.SIGN DF(5016)	
DF.SIGN DF(5016)	
File Type	DF
File Length	
File identifier	5016
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER

Read binary	
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	NEVER
Read binary	

CERTIFICATE#2 EF(50164332)	
CERTIFICATE#2 EF(50164332)	
File Type	EF
File Length	2048 Bytes
File identifier	4332
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#02 OR PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

EF Public EmptyArea (433F)	
Object Properties EF Public EmptyArea	
File Type	EF
File Length	8192 Bytes
File identifier	433F
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER

Update binary	PIN SE#02
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

EF Private EmptyArea (433E)	
Object Properties EF Public EmptyArea	
File Type	EF
File Length	4096 Bytes
File identifier	433E
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#02
Read binary	PIN SE#02
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	PACE PIN AUTH SE#2 + SM

EF CA Certificate #2 (4334)	
Object Properties EF CA Certificate #2 (4334)	
File Type	EF
File Length	1558 Bytes
File identifier	4334
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER

Update binary	PIN SE#02 OR PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

EF CA Certificate #1 (4333)	
Object Properties EF CA Certificate #1 (4333)	
File Type	EF
File Length	1919 Bytes
File identifier	4333
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#02 OR PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

User Certificate file #1 (4331)	
Object Properties User Certificate file #1 (4331)	
File Type	EF
File Length	1925 Bytes
File identifier	4331
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER

Update binary	PIN SE#02 OR PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

EF Certificate #2 (4332)	
Object Properties EF Certificate #2 (4332)	
File Type	EF
File Length	2048 Bytes
File identifier	4332
Short File identifier	
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PIN SE#02 OR PIN SE#04
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Update binary	PACE PIN AUTH SE#2 + SM
Read binary	SM SE#02

4.2 Security Data Object (SDO) for personalized cards

2 profiles with different configurations will be described. The PIN objects will be the same on both. The difference will be on the types of asymmetric keys:

- One with 2 RSA 3K certificates: auth & encryption and non-repudiation digital signature
- One with 3 ECC 384 certificates: auth, encryption and non-repudiation digital signature

4.2.1 Security Environment

SE#2 stands for PIN Authent (ID =11)

SE#3 stands for PUK (ID =12)

SE#4 stands for SO PIN (ID =13)

SE#5 stands for AES Mutual Authenticate key (ID =07)

SE#6 stands for DES3 Mutual Authenticate key (ID =08)

SE#7 stands for local Signature PIN (ID =95)

4.2.2 PINs Objects

As PACE is required in contactless, the SDO ID of the PIN have to be formatted like that : 1X. This is a requirement of the applet IDme 1.6.

PIN Auth (11)	
Data object control parameters	
SDO ID	11
Maximum Number Of Tries	05* For test cards Value is set to infinite to allow PACE Tests which could require many tests before success
Remaining Tries Counter	00
Security attributes contact	
Change reference data	ALWAYS
Verify	ALWAYS
Reset retry counter	PUK SE#3
SAC Authentication	ALWAYS
Put data	NEVER
Get data	ALWAYS
Security attributes contactless	
Change reference data	SM SE#03
Verify	SM SE#03
Reset retry counter	PACE PIN AUTH SE#03 + SM
SAC Authentication	ALWAYS
Put data	NEVER
Get data	SM SE#03
Data Object Usage Parameters	

SDO ID	11
PIN Max Size	12 Bytes
PIN Min Size	4 Bytes
Value	

PUK (12)	
Data object control parameters	
SDO ID	12
Maximum Number of Tries	05
Remaining Tries Counter	05
Security attributes contact	
Change reference data	NEVER
Verify	ALWAYS
Reset retry counter	NEVER
SAC Authentication	ALWAYS
Put data	NEVER
Get data	ALWAYS
Security attributes contactless	
Change reference data	NEVER
Verify	SM SE#03
Reset retry counter	NEVER
SAC Authentication	ALWAYS
Put data	NEVER
Get data	SM SE#03
Data Object Usage Parameters	
SDO ID	12
PIN Max Size	12 Bytes
PIN Min Size	8 Bytes
Value	

SO PIN (13) deprecated for perso cards	
Data object control parameters	
SDO ID	13
Maximum Number Of Tries	05
Remaining Tries Counter	00
Security attributes Contact	
Change reference data	SO PIN SE#4
Verify	ALWAYS
Reset retry counter	SO PIN SE#4
Put data	SO PIN SE#4

Get data	ALWAYS
Security attributes Contactless	
Change reference data	SO PIN SE#4
Verify	ALWAYS
Reset retry counter	SO PIN SE#4
Put data	SO PIN SE#4
Get data	ALWAYS
Data Object Usage Parameters	
SDO ID	13
PIN Max Size	8 Bytes
PIN Min Size	8 Bytes
Value	

PIN Signature ID is 15, as this a local PIN and for PACE usage, bits 8 and 5 have to be set

PIN SIGNATURE (15)	
Data object control parameters	
SDO ID	15
Maximum Number of Tries	05
Remaining Tries Counter	05
Security attributes Contact	
Change reference data	ALWAYS
Verify	ALWAYS
Reset retry counter	PUK SE#3
Create	ALWAYS
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
Change reference data	SM SE#2
Verify	SM SE#02
Reset retry counter	PACE PIN AUTH SE#3 + SM
Create	ALWAYS
Put data	NEVER
Get data	SM SE#2
Data Object Usage Parameters	
SDO ID	15
PIN Max Size	8
PIN Min Size	6

2 key Set have been added in the electrical profile to manage the Key Generation

One AES: Kenc : 101112131415161718191A1B1C1D1E1F

Kmac : 404142434445464748494A4B4C4D4E4F

One DES3: Kenc : 101112131415161718191A1B1C1D1E1F

Kmac : 404142434445464748494A4B4C4D4E4F

AES Key Mutual Authenticate (07)	
Data object control parameters	
SDO ID	07
Maximum Number of Tries	0F* For test cards Value is set to infinite to allow Mutual Auth Tests which could require many tests before success
Object Length	128 Bytes
Security attributes contact	
External Authenticate for Role	NEVER
Mutual Authenticate	ALWAYS
Put data	NEVER
Get data	ALWAYS
Security attributes contactless	
External Authenticate for Role	NEVER
Mutual Authenticate	ALWAYS
Put data	NEVER
Get data	ALWAYS

DES3 Key Mutual Authenticate (08)	
Data object control parameters	
SDO ID	08
Maximum Number of Tries	0F* For test cards Value is set to infinite to allow Mutual Auth Tests which could require many tests before success
Object Length	128 Bytes
Security attributes	
External Authenticate for Role	NEVER
Mutual Authenticate	ALWAYS

Put data	NEVER
Get data	ALWAYS
Security attributes contactless	
External Authenticate for Role	NEVER
Mutual Authenticate	PIN SE#02
Put data	NEVER
Get data	SM SE#02

4.2.3 Asymmetric keys

2 RSA 3K certificates Profile

RSA key #1, Private Part (01)	
Data object control parameters	
SDO ID	01
Non-Repudiation Flag	00
Object Length	384
Security attributes	
PSO Compute Digital Signature	PIN SE#2
Internal Authenticate	PIN SE#2
PSO Decipher	PIN SE#2
Generate Asymmetric Key Pair	SM SE#5 or SM SE#6
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
PSO Compute Digital Signature	PACE PIN AUTH SE#2 + SM
Internal Authenticate	PACE PIN AUTH SE#2 + SM
PSO Decipher	PACE PIN AUTH SE#2 + SM
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	NEVER
Get data	SM SE#02

RSA key #1, Public Part (01)	
Data object control parameters	
SDO ID	01
Object Length	384
Security attributes Contact	
PSO VERIFY CERTIFICATE	NEVER
Internal authenticate	NEVER

PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	ALWAYS
Security attributes Contactless	
PSO VERIFY CERTIFICATE	NEVER
Internal authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	SM SE#02

RSA key #2, Private Part (02) Signature Key	
Data object control parameters	
SDO ID	02
Non-Repudiation Flag	01
Object Length	384
Security attributes	
PSO Compute Digital Signature	PIN Signature SE#7
Internal Authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	ALWAYS
Security attributes Contactless	
PSO Compute Digital Signature	PACE PIN Auth SE#7 + SM
Internal Authenticate	Never
PSO Decipher	Never
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	SM SE#02

RSA key #2, Public Part (02)	
Data object control parameters	
SDO ID	02
Object Length	384
Security attributes	
PSO VERIFY CERTIFICATE	NEVER
Internal + external auth	NEVER

PSO Decrypt	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SE#6
Put data	Never
Get data	ALWAYS
Security attributes Contactless	
PSO VERIFY CERTIFICATE	NEVER
EXTERNAL AUTHENTICATE	NEVER
PSO Decrypt	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	SM SE#02

ECC 384 certificates Profile

Asymmetric ECC keys for Authentication

ECC key #1, Private Part (01) id-PACE-Nist-P384	
Data object control parameters	
SDO ID	01
Non-Repudiation Flag	00
Object Length	384
Security attributes	
PSO Compute Digital Signature	PIN SE#2
Internal Authenticate	PIN SE#2
PSO Decipher	PIN SE#2
Generate Asymmetric Key Pair	SM SE#5 or SM SE#6
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
PSO Compute Digital Signature	PACE PIN AUTH SE#2 + SM
Internal Authenticate	PACE PIN AUTH SE#2 + SM
PSO Decipher	PACE PIN AUTH SE#2 + SM
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	NEVER
Get data	SM SE#02

ECC key #1, Public Part (01) id-PACE-Nist-P384

Data object control parameters	
SDO ID	01
Object Length	384
Security attributes Contact	
PSO VERIFY CERTIFICATE	NEVER
Internal authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	ALWAYS
Security attributes Contactless	
PSO VERIFY CERTIFICATE	NEVER
Internal authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	SM SE#02

Asymmetric ECC keys for encryption

ECC key #2, Private Part (02) **id-PACE-Nist-P384**	
Data object control parameters	
SDO ID	01
Non-Repudiation Flag	00
Object Length	384
Security attributes	
PSO Compute Digital Signature	PIN SE#2
Internal Authenticate	PIN SE#2
PSO Decipher	PIN SE#2
Generate Asymmetric Key Pair	SM SE#5 or SM SE#6
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
PSO Compute Digital Signature	PACE PIN AUTH SE#2 + SM
Internal Authenticate	PACE PIN AUTH SE#2 + SM
PSO Decipher	PACE PIN AUTH SE#2 + SM
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	NEVER
Get data	SM SE#02

ECC key #2, Public Part (02) id-PACE-Nist-P384	
Data object control parameters	
SDO ID	01
Object Length	384
Security attributes Contact	
PSO VERIFY CERTIFICATE	NEVER
Internal authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	ALWAYS
Security attributes Contactless	
PSO VERIFY CERTIFICATE	NEVER
Internal authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	SM SE#02

Asymmetric ECC keys for non-rep digital signature

In the current profile, instead of setting the Access Condition for Generate Asymmetric Key Pair to SO PIN SE#4, the Mutual Authentication using SE#5 (AES Key) or SE#6 (DES3 Key) is set. This can be discussed after either to keep the SO PIN which will be blocked after perso or using these Mutual Auth Keys.

ECC key #3, Private Part (03) id-PACE-Nist-P384	
Data object control parameters	
SDO ID	02
Non-Repudiation Flag	01
Object Length	384
Security attributes	
PSO Compute Digital Signature	PIN Signature SE#7
Internal Authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never

Get data	ALWAYS
Security attributes Contactless	
PSO Compute Digital Signature	PACE PIN Auth SE#7 + SM
Internal Authenticate	Never
PSO Decipher	Never
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	SM SE#02

ECC key #3, Public Part (03) **id-PACE-Nist-P384**	
Data object control parameters	
SDO ID	02
Object Length	384
Security attributes	
PSO VERIFY CERTIFICATE	NEVER
Internal + external auth	NEVER
PSO Decrypt	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SE#6
Put data	Never
Get data	ALWAYS
Security attributes Contactless	
PSO VERIFY CERTIFICATE	NEVER
EXTERNAL AUTHENTICATE	NEVER
PSO Decrypt	NEVER
Generate Asymmetric Key Pair	SM SE#5 OR SM SE#6
Put data	Never
Get data	SM SE#02

4.3 Temporary Card

Temporary card file structure is quite similar to the RSA card ones, except on the presence of the SO PIN which is used to enable the personalization of the card: update files, generate keys and also erase the card and redo a person.

SO PIN ID is 13 with the Security Environment SE#4

4.3.1 Files System

MF (3F00)	
Object Properties ADF ROOT	
File Type	DF

File identifier	3F00
AID	A000000063504B43532D3135
Security attributes Contact	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Create file EF	SO PIN SE#4
Security attributes Contactless	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Create file EF	SO PIN SE#4

DF.ESIGN (5016)	
Object Properties DF ESIGN	
File Type	DF
File identifier	5016
AID	452E5349474E
Security attributes	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Create file EF	SO PIN SE#4
Security attributes Contactless	
Delete file (DF itself)	NEVER
Terminate file	NEVER
Activate file	NEVER
Deactivate file	NEVER
Create file EF	SO PIN SE#4

EF.ATR (2F01)	
Object Properties EF ATR	
File Type	EF
File Length	6 Bytes
File identifier	2F01
Short File identifier	E8
Security attributes	
Delete file	NEVER

Terminate file	NEVER
Activate file	NEVER
Update binary	NEVER
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Update binary	NEVER
Read binary	PACE PIN AUTH SE#2 + SM

EF.SN (D003)	
Object Properties EF SN	
File Type	EF
File Length	12 Bytes
File identifier	D003
Short File identifier	E0
Security attributes	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Update binary	NEVER
Read binary	ALWAYS
Security attributes Contactless	
Delete file	NEVER
Terminate file	NEVER
Activate file	NEVER
Update binary	NEVER
Read binary	PACE PIN AUTH SE#2 + SM

4.3.2 Security Data Object (SDO)

Profile for temporary card is similar to the RSA one, except that no key is generated.

4.3.3 Security Environment

SE#2 stands for PIN Authent (ID =11)

SE#3 stands for PUK (ID =12)

SE#4 stands for SO PIN (ID =13)

SE#5 stands for AES Mutual Authenticate key (ID =07)

SE#6 stands for DES3 Mutual Authenticate key (ID =08)

SE#7 stands for local Signature PIN (ID =95)

4.3.4 PINs Objects

As PACE is required in contactless, the SDO ID of the PIN have to be formatted like that: 1X. This is a requirement of the applet IDme 1.6.

PIN Auth (11)	
Data object control parameters	
SDO ID	11
Maximum Number of Tries	05* For test cards Value is set to infinite to allow PACE Tests which could require many tests before success
Remaining Tries Counter	05
Security attributes	
Change reference data	ALWAYS
Verify	ALWAYS
Reset retry counter	PIN SE#3
Put data	NEVER
Get data	ALWAYS
Data Object Usage Parameters	
SDO ID	12
PIN Max Size	12
PIN Min Size	04

PUK (12)	
Data object control parameters	
SDO ID	12
Maximum Number of Tries	05
Remaining Tries Counter	05
Security attributes Contact	
Change reference data	NEVER
Verify	ALWAYS
Reset retry counter	NEVER
Put data	NEVER

Get data	ALWAYS
Security attributes Contactless	
Change reference data	NEVER
Verify	SM SE#3
Reset retry counter	NEVER
Put data	NEVER
Get data	SM SE#3
Data Object Usage Parameters	
SDO ID	12
PIN Max Size	12
PIN Min Size	08

SO PIN (13)	
Data object control parameters	
SDO ID	13
Maximum Number of Tries	05
Remaining Tries Counter	05
Security attributes Contact	
Change reference data	SO PIN SE#4
Verify	ALWAYS
Reset retry counter	SO PIN SE#4
Put data	SO PIN SE#4
Get data	ALWAYS
Security attributes Contactless	
Change reference data	SO PIN SE#4
Verify	ALWAYS
Reset retry counter	SO PIN SE#4
Put data	SO PIN SE#4
Get data	ALWAYS
Data Object Usage Parameters	
SDO ID	03
PIN Max Size	08
PIN Min Size	08

PIN Signature ID is 15, as this a local PIN and for PACE usage, bits 8 and 5 have to be set

PIN SIGNATURE (15)	
Data object control parameters	
SDO ID	15

Maximum Number of Tries	05
Remaining Tries Counter	05
Security attributes Contact	
Change reference data	ALWAYS
Verify	ALWAYS
Reset retry counter	PUK SE#3
Create	ALWAYS
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
Change reference data	SM SE#2
Verify	SM SE#2
Reset retry counter	PACE Auth PIN SE#3 + SM
Create	ALWAYS
Put data	NEVER
Get data	SM SE#2
Data Object Usage Parameters	
SDO ID	95
PIN Max Size	8
PIN Min Size	6

2 key Set have been added in the electrical profile to manage the Key Generation

One AES : Kenc : 101112131415161718191A1B1C1D1E1F

Kmac : 404142434445464748494A4B4C4D4E4F

One DES3 : Kenc : 101112131415161718191A1B1C1D1E1F

Kmac : 404142434445464748494A4B4C4D4E4F

This can be discussed either to keep or to keep the SO PIN as on previous profile.

AES Key Mutual Authenticate (07)	
Data object control parameters	
SDO ID	07
Maximum Number of Tries	0F* For test cards Value is set to infinite to allow Mutual Auth Tests which could require many tests before success
Object Length	16
Security attributes Contact	

External Authenticate for Role	NEVER
Mutual Authenticate	ALWAYS
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
External Authenticate for Role	NEVER
Mutual Authenticate	SM SE#2
Put data	NEVER
Get data	SM SE#2

DES3 Key Mutual Authenticate (08)	
Data object control parameters	
SDO ID	08
Maximum Number Of Tries	0F* For test cards Value is set to infinite to allow Mutual Auth Tests which could require many tests before success
Object Length	16
Security attributes Contact	
External Authenticate for Role	NEVER
Mutual Authenticate	ALWAYS
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
External Authenticate for Role	NEVER
Mutual Authenticate	SM SE#2
Put data	NEVER
Get data	SM SE#2

4.3.5 Asymmetric keys

2 RSA 3K certificates Profile

RSA key #1, Private Part (01)	
Data object control parameters	

SDO ID	01
Non-Repudiation Flag	01
Object Length	384
Security attributes	
PSO Compute Digital Signature	PIN Auth SE#2
Internal Authenticate	PIN Auth SE#2
PSO Decipher	PIN Auth SE#2
Generate Asymmetric Key Pair	SM SE6 or SM SE5
Put data	NEVER
Get data	AWAYS
Security attributes Contactless	
PSO Compute Digital Signature	PACE PIN AUTH SE#2 + SM
Internal Authenticate	PACE PIN AUTH SE#2 + SM
PSO Decipher	PACE PIN AUTH SE#2 + SM
Generate Asymmetric Key Pair	SM SE#6 or SM SE#5
Put data	NEVER
Get data	SM SE#2

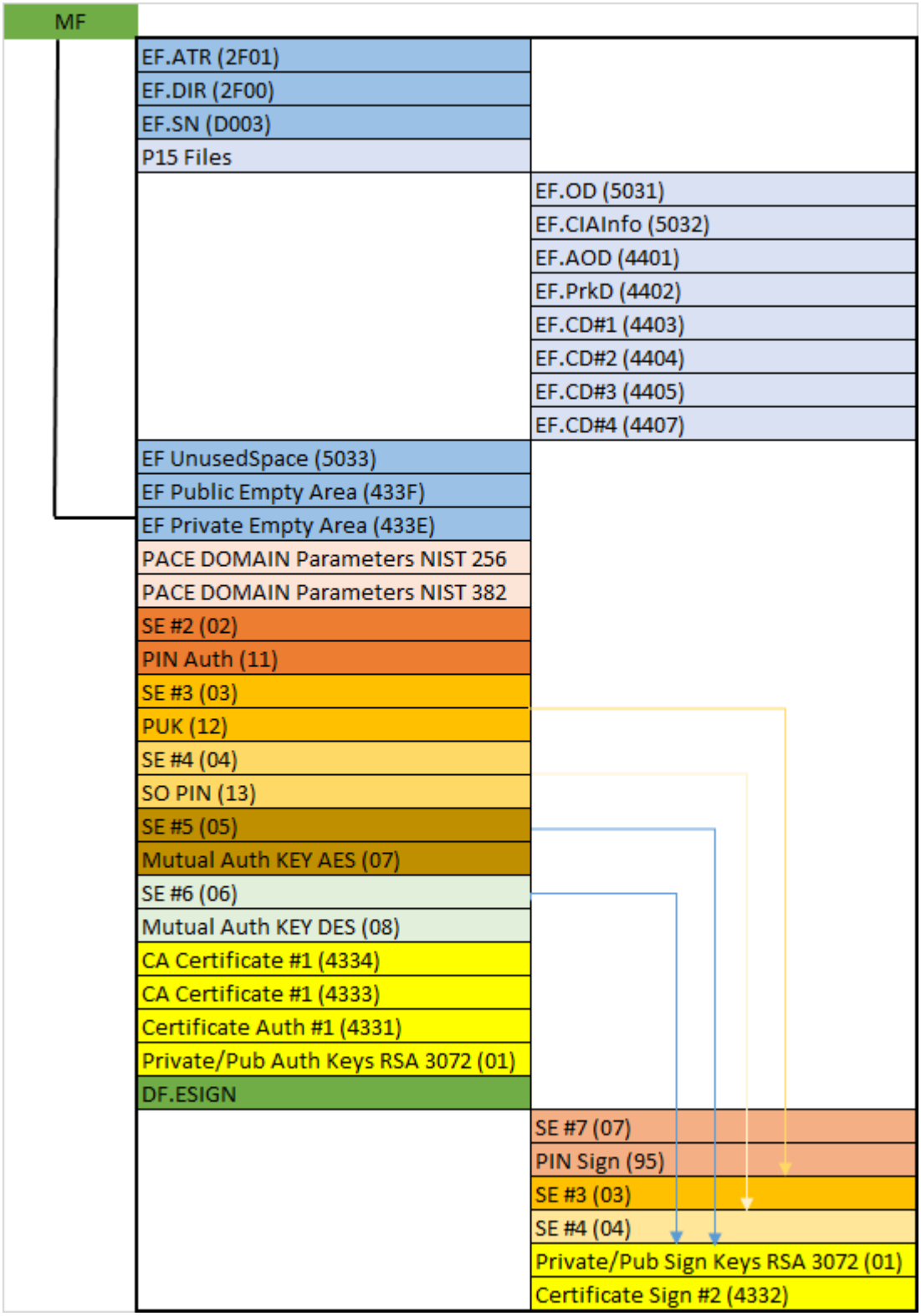
RSA key #1, Public Part (01)	
Data object control parameters	
SDO ID	01
Object Length	384
Security attributes Contact	
PSO Verify Certificate	NEVER
External authenticate	NEVER
Generate Asymmetric Key Pair	SM SE#6 or SM SE#5
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
PSO Verify Certificate	PACE SE#2
External authenticate	PACE SE#2
Generate Asymmetric Key Pair	NEVER
Put data	NEVER
Get data	ALWAYS

In the current profile mainly for Temporary cards, instead of setting the Access Condition for Generate Asymmetric Key Pair to SO PIN SE#4, the Mutual Authentication using SE#5 (AES Key) or SE#6 (DES3 Key) is also set. This can be discussed after either to keep the SO PIN which will be blocked after perso or using these Mutual Auth Keys. For test purposes, we keep these 3 possibilities.

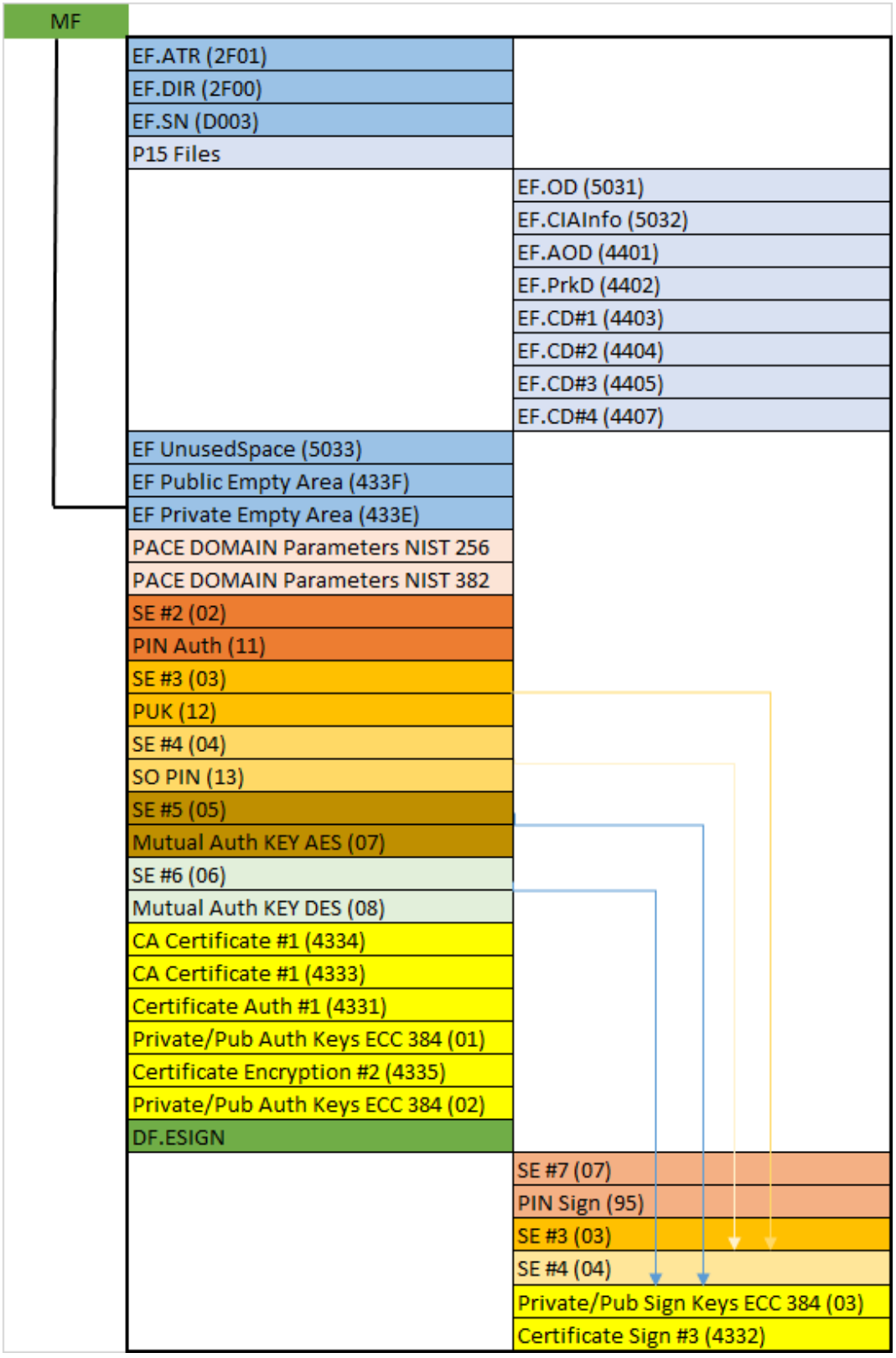
RSA key #2, Private Part (02) Signature Key	
Data object control parameters	
SDO ID	02
Non-Repudiation Flag	01
Object Length	384
Security attributes	
PSO Compute Digital Signature	PIN Signature SE#7
Internal Authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 or SM SE#6
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
PSO Compute Digital Signature	PACE PIN Sign SE#7
Internal Authenticate	Never
PSO Decipher	Never
Generate Asymmetric Key Pair	SM SE#6 or SM SE#5
Put data	Never
Get data	SM SE#2

RSA key #2, Public Part (02)	
Data object control parameters	
SDO ID	02
Object Length	384
Security attributes Contact	
PSO Compute Digital Signature	NEVER
Internal Authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#5 or SM SE#6
Put data	NEVER
Get data	ALWAYS
Security attributes Contactless	
PSO Compute Digital Signature	NEVER
Internal Authenticate	NEVER
PSO Decipher	NEVER
Generate Asymmetric Key Pair	SM SE#6 or SM SE#5
Put data	NEVER
Get data	SM SE#2

4.4 Global Electrical Profile for two 3K RSA Certificates



4.5 Global Electrical Profile for three ECC 384 Certificates



5 ISO7816-15 Files

5.1 EF.OD Value

```
CONTEXT_SPECIFIC [ 8 ] {
       SEQUENCE { OCTET_STRING { #3F004401 } } -- authentication objects
}
CONTEXT_SPECIFIC [ 0 ] {
       SEQUENCE { OCTET_STRING { #3F004402 } } -- private keys
}
CONTEXT_SPECIFIC [ 4 ] {
       SEQUENCE { OCTET_STRING { #3F004403 } } -- Certificates
}
CONTEXT_SPECIFIC [ 4 ] {
       SEQUENCE { OCTET_STRING { #3F004404 } } -- (Additional) certificates
}
CONTEXT_SPECIFIC [ 5 ] {
       SEQUENCE { OCTET_STRING { #3F004405 } } -- Trusted certificates
}
CONTEXT_SPECIFIC [ 6 ] { -- Useful certificates
       SEQUENCE { OCTET_STRING { #3F004406 } }
}
CONTEXT_SPECIFIC [ 7 ] { -- Data objects
    SEQUENCE { OCTET_STRING { #3F004407 } }
    }
```

5.2 EF.AOD Value (read and parse EF)

```
SEQUENCE {
       SEQUENCE {
              UTF8String { "grund PIN" },
              BIT_STRING { #06, #C0 }                 -- flags = 1100 0000
},
SEQUENCE { OCTET_STRING { #01 } },                     -- authID
CONTEXT_SPECIFIC [ 1 ] {
       SEQUENCE {
              BIT_STRING { #03, #08 },                 -- password attributes: 0000
       1000
                                                       -- = initialized

              ENUMERATED = #01;                        -- Password type
              INTEGER = 4;                             -- length min
              INTEGER = 12;                            -- stored length
              CONTEXT_SPECIFIC[0,"IMPLICIT"]=#11;      -- pwd reference,
              SEQUENCE { OCTET_STRING = #3F00 }        -- path
              }
       }
}
SEQUENCE {
       SEQUENCE {
              UTF8String { "signatur PIN" },
              BIT_STRING { #06, #C0 }
},
       SEQUENCE { OCTET_STRING { #02 } },
       CONTEXT_SPECIFIC [ 1 ] {
              SEQUENCE {
                     BIT_STRING { #03, #48 },          -- bits: 0010 1000
                                                       -- flags; local + initialized
                     ENUMERATED = #01;
                     INTEGER = 6;
                     INTEGER = 12;
```

```
                    CONTEXT_SPECIFIC[0,"IMPLICIT"]= #0095;
             }
       }
}
```

5.3 EF.CD #1 (4403)

```
SEQUENCE {
       SEQUENCE {
             UTF8String { "aut. och kryptering certifikat" },
             BIT_STRING { #06, #40 },                -- Flags: Modifiable
             BIT_STRING { #07, #80 },
             SEQUENCE {
                    SEQUENCE {
                          BIT_STRING { #07, #80 },   -- Read
                          NULL -- Always
                    },
                    SEQUENCE {
                          BIT_STRING { #06, #40 },   -- Update
                          OCTET_STRING { #01 }       -- authID = 1
                    }
             }
       },
SEQUENCE {
       OCTET_STRING { #45 },
       SEQUENCE {
             INTEGER = 3;                            -- issuer and serial number
       hash
             OCTET_STRING { #40D6EF520F5F7655F07245B0586091D2AF45ABF6 }
       }
},
CONTEXT_SPECIFIC [ 1 ] {
       SEQUENCE {
             SEQUENCE { OCTET_STRING { #3F004331 } }
             }
       }
}
SEQUENCE {
       SEQUENCE {
             UTF8String { "signatur certifikat" },
             BIT_STRING { #06, #40 },
             SEQUENCE {
                    SEQUENCE {
                          BIT_STRING { #07, #80 },
                          NULL = "NULL";
                    },
                    SEQUENCE {
                          BIT_STRING { #06, #40 },
                          OCTET_STRING { #01 }
                    }
             }
       },
       SEQUENCE {
             OCTET_STRING { #46 },
             SEQUENCE {
                    INTEGER = 3;
                    OCTET_STRING { #897A431C21AB0ECED1FB09F76DDE74510993AE32 }
       }
},
CONTEXT_SPECIFIC [ 1 ] {
       SEQUENCE {
             SEQUENCE { OCTET_STRING { #3F0050164332 } }
             }
```

```
      }
}
```

5.4 EF.CD #3 (4405)

```
SEQUENCE {
      SEQUENCE {
            UTF8String { "VRK TEST Root CA - G2" },
            BIT_STRING { #00, null },                    -- flags = NULL
            SEQUENCE {
                  SEQUENCE {
                  BIT_STRING { #07, #80 },               -- Read
                  NULL                                   -- always
                  }
            }
      },
      SEQUENCE {
            OCTET_STRING { #48 },
            BOOLEAN = #FF;                               -- CA certtificate
            SEQUENCE {
                  INTEGER = 2;                           -- subjectKeyIdentifier
                  OCTET_STRING { #853DA0E1FCB10927E4DABD1F868B400672420A81} -- ok
            // from certificate: 853DA0E1FCB10927E4DABD1F868B400672420A81
            }
      },
      CONTEXT_SPECIFIC [ 1 ] {
      SEQUENCE {
            SEQUENCE { OCTET_STRING { #3F004334 } }
            }
      }
}
SEQUENCE {
      SEQUENCE {
      UTF8String { "VRK TEST CA for Test Purposes - G4" },
      BIT_STRING { #00, "NULL" },
      SEQUENCE {
            SEQUENCE {
            BIT_STRING { #07, #80 },
            NULL = "NULL";
            }
     }
},

SEQUENCE {
      OCTET_STRING { #47 },
      BOOLEAN = #FF;
      SEQUENCE {
            INTEGER = 2;
            OCTET_STRING { #3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 } -- ok
            // from certificate: 3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1
      }
},
CONTEXT_SPECIFIC [ 1 ] {
      SEQUENCE {
            SEQUENCE { OCTET_STRING { #3F004333 } }
            }
     }
}
```

5.5 EF.PrkD (4402)

FINEID specifies key usage and access flags as follows:
usage {decipher, sign, keyDecipher},
accessFlags {sensitive, alwaysSensitive, neverExtractable,cardGenerated},

From PKCS#15 v1.5, usage and access flags are defined as follows:

KeyUsageFlags ::= BIT STRING {
encrypt (0),
decrypt (1),
sign (2),
signRecover (3),
wrap (4),
unwrap (5),
verify (6),
verifyRecover (7),
derive (8),
nonRepudiation (9)
}
KeyAccessFlags ::= BIT STRING {
sensitive (0),
extractable (1),
alwaysSensitive (2),
neverExtractable (3),
local (4)
}

```
SEQUENCE {
      SEQUENCE {                                    -- Common object attributes
            UTF8String = "aut. och kryptering nyckel", -- label
            BIT_STRING { #07, #80 },                -- flags => private
            OCTET_STRING = #01,                     -- authid
            SEQUENCE {
                  SEQUENCE {
                  BIT_STRING { #05, #20 },          -- execute
                  OCTET_STRING = #01                -- AuthID
                  }
            }
      },
      SEQUENCE {
            OCTET_STRING = #45,                     -- id
            BIT_STRING { #02, #64 },                -- keyUsage => decrypt, sign,
      unwrap
            BIT_STRING { #04, #B8 },                -- accessFlags => OK
            INTEGER = 1                             -- keyReference
      },

      CONTEXT_SPECIFIC [ 0 ] {                      -- subclass attributes
            SEQUENCE {
                  CONTEXT_SPECIFIC [ 0 ] {
                  SEQUENCE {                        -- credentialIdentifier
                        INTEGER = 4,                -- subjectKeyHash
```

```
                        OCTET_STRING = #9C1C8A7660902998E839949900B8AA0AA3155856
                                                        -- SHA1 of modulus
                    }
                }
        }
},
CONTEXT_SPECIFIC [ 1 ] {                                -- typeAttributes
        SEQUENCE {
                SEQUENCE { OCTET_STRING = #3F00 },
                INTEGER = 3072
                }
        }
};
SEQUENCE {
        SEQUENCE {
                UTF8String = "signatur nyckel",
                BIT_STRING { #07, #80 },
                OCTET_STRING = #02,
                INTEGER = 1,
                SEQUENCE {
                        SEQUENCE {
                                BIT_STRING { #05, #20 },
                                OCTET_STRING = #02
                        }
                }
        },
        SEQUENCE {
                OCTET_STRING = #46,
                BIT_STRING { #06, #0040 },              -- keyUsage, nonRepudiation
                BIT_STRING { #03, #B8 },                -- Access flags: 1011 1000
                                                        -- * Sensitive
                                                        -- * alwaysSensitive
                                                        -- * neverExtrable
                                                        -- * cardGenerated (=Local)
        INTEGER = 2
        },

      CONTEXT_SPECIFIC [ 0 ] {
                SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
                        SEQUENCE {
                                INTEGER = 4,
                                OCTET_STRING = #8B8EB8CFE08AFC37C6F4CA9F6228A52F8BB169E3
                        }
                }
        }
},
CONTEXT_SPECIFIC [ 1 ] {
        SEQUENCE {
                SEQUENCE { OCTET_STRING = #3F005016 },
                        INTEGER = 3072
                }
        }
}
```

6 PACE Configuration

For contactless usage, the PACE protocol has to be used. The following parameters are set:

id-PACE-Nist-P256

ec_P	FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
ec_Param_A	FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC
ec_Param_B	5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
ec_Order_P	FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
ec_Coord_P_x	6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296
ec_Coord_P_y	4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
ec_G	04 %ec_Coord_P_x %ec_Coord_P_y
ec_H	00000001

Id-PACE-Nist-P384

ec_P
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFF00000000 00000000FFFFFFFF
ec_Param_A
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFF00000000 00000000FFFFFFFC
ec_Param_B
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2 A85C8EDD3EC2AEF
ec_Order_P
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC7634D81F4372DDF581A0DB248B0A77 AECEC196ACCC52973
ec_Coord_P_x
AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296 C3A545E3872760AB7
ec_Coord_P_y
3617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E81 9D7A431D7C90EA0E5F
ec_G
04 %ec_Coord_P_x %ec_Coord_P_y
ec_H
00000001

As previously said, the PIN are used to identify and enabling the PACE protocol.

For using the Private key of RSA Key 1 in contactless, PIN Auth 11 has to be used for Internal Authentication and Decipher operations

For using the Private key of RSA Key 2 in contactless, PIN Sign 95 has to be used for Compute Digital Signature operation.

The OID supported will be the following for NIST 384 and 256 bits:

id-PACE-ECDH-GM-AES-CBC-CMAC-256 = 04007f00070202040204

id-PACE-ECDH-IM-AES-CBC-CMAC-256 = 04007f00070202040404

7 Key generation Performance

7.1 RSA 3K vs ECC 384 (Nist P384) on board Keys generation

On Board generation	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ECC 384 (s)	1,33	1,33	1,33	1,33	1,34	1,33	1,33	1,33	1,33	1,33
RSA 3072 (s)	95,47	37,30	62,73	107,21	79,27	47,60	30,21	94,46	58,40	65,46
On Board generation	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
ECC 384 (s)	1,33	1,34	1,33	1,33	1,34	1,33	1,34	1,33	1,34	1,33
RSA 3072 (s)	80,68	17,08	102,20	138,99	184,96	31,30	73,84	120,38	51,78	30,30
On Board generation	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
ECC 384 (s)	1,33	1,33	1,33	1,34	1,33	1,33	1,33	1,33	1,33	1,33
RSA 3072 (s)	56,22	64,11	28,42	21,12	182,78	107,02	40,95	36,47	231,76	141,59
On Board generation	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
ECC 384 (s)	1,34	1,33	1,33	1,34	1,33	1,34	1,33	1,34	1,33	1,33
RSA 3072 (s)	29,05	56,68	56,77	102,59	88,31	191,96	187,55	129,25	58,22	100,75
On Board generation	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**
ECC 384 (s)	1,34	1,33	1,33	1,34	1,33	1,33	1,34	1,33	1,33	1,34
RSA 3072 (s)	84,09	45,22	115,62	84,64	52,35	76,32	253,57	117,38	73,96	66,99

On Board generation	**Mean Time (s)**
ECC 384 (s)	**1,33**
RSA 3072 (s)	**87,83**