FINEID - S4-2

Implementation Profile 2 for

Organizational Usage

V4.0

Digital and Population Data Services Agency (DVV)
Certification Authority Services
P.O. Box 123
FIN-00531 Helsinki Finland
http://www.dvv.fi/

Authors

Name	Initials	Organization
A. CHAN	AC	IDEMIA

Document History

Date	Author	Description
12/06/2024	A.CHAN	First edition

Table of contents

1 Introduction

1.1 Purpose

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

The card is IDA applet on Cosmo X. This card is compliant with Global Platform 2.3.1 and Javacard API 3.1.0.

Idme is a Javacard implementation of the Identification Authentication Signature for European Citizen Card v2.0 (IAS ECC).

1.2 References

Annex II of eIDAS regulation

2 Definitions

ADF	Application Dedicated File
AID	Application Identifier
BER	Basic Encoding Rules
CA	Certification Authority
DES	Data Encryption Standard
DF	Dedicated File
ECC	Elliptic curve cryptography
EF	Elementary File
FCP	File Control Parameters
IAS	Identification, Authentication and electronic Signature
MF	Master File
MSE	Manage Security Environment
PACE	Password Authenticated Connection Establishment
PUK	PIN Unblocking Key
PIN	Personal Identification Number
RFU	Reserved for Future Use
Root	The applet instance having the default selection privilege
RSA	Rivest Shamir Adleman
SDO	Security Data Object
SE	Security Environment
SEID	Security Environment Identifier byte
SSE	Static Security Environment
SSESP	Static Security Environment for Security Policy
SK	Secret key – Symmetric key based algorithm
SM	Secure Messaging
SO	Security Officer
TLV	Tag Length Value

3 Chip Description

3.1 Card

The Card chosen for this project is the Cosmo X with Java card ID-A instantiated. There are 3 types of cards described in this document.

- RSA card
  - ➢ 22 – EF files
  - ➢ 3 - PIN/Password
  - ➢ 2 – RSA keys
- ECC card
  - ➢ 22 – EF files
  - ➢ 3 - PIN/Password
  - ➢ 2 – ECC keys
- Temporary card
  - ➢ 4 - PIN/Password

3.2 ATR configuration

Parameter	Value
ATR	3BDD96008031FE450031B8640429ECC1739401808349
Protocol	T=0, T=1
Speed	Fi=512, Di=32, 312500 bits/s for fMax=5 MHz

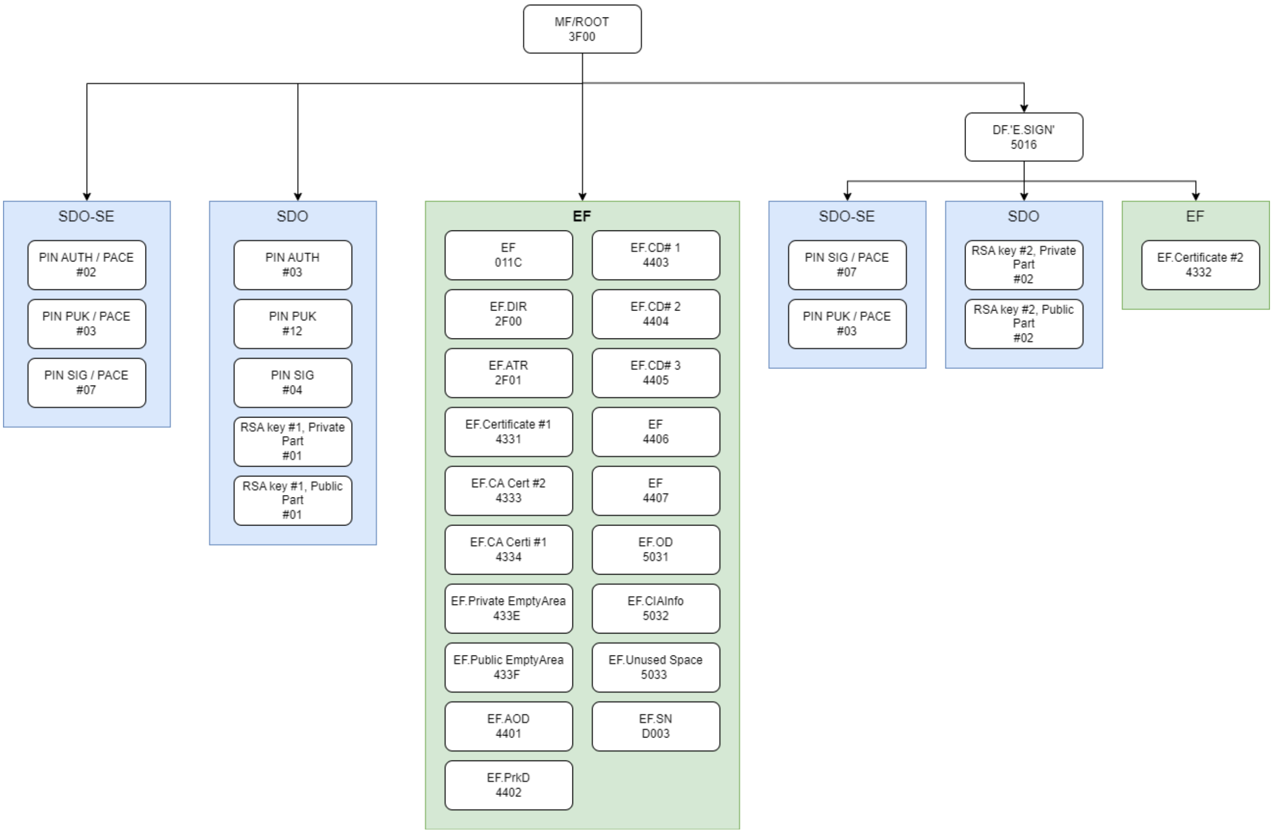
3.2.1 Packages

ID-A applet is instantiated with the following AID: A000000077030C60000000FE00000500

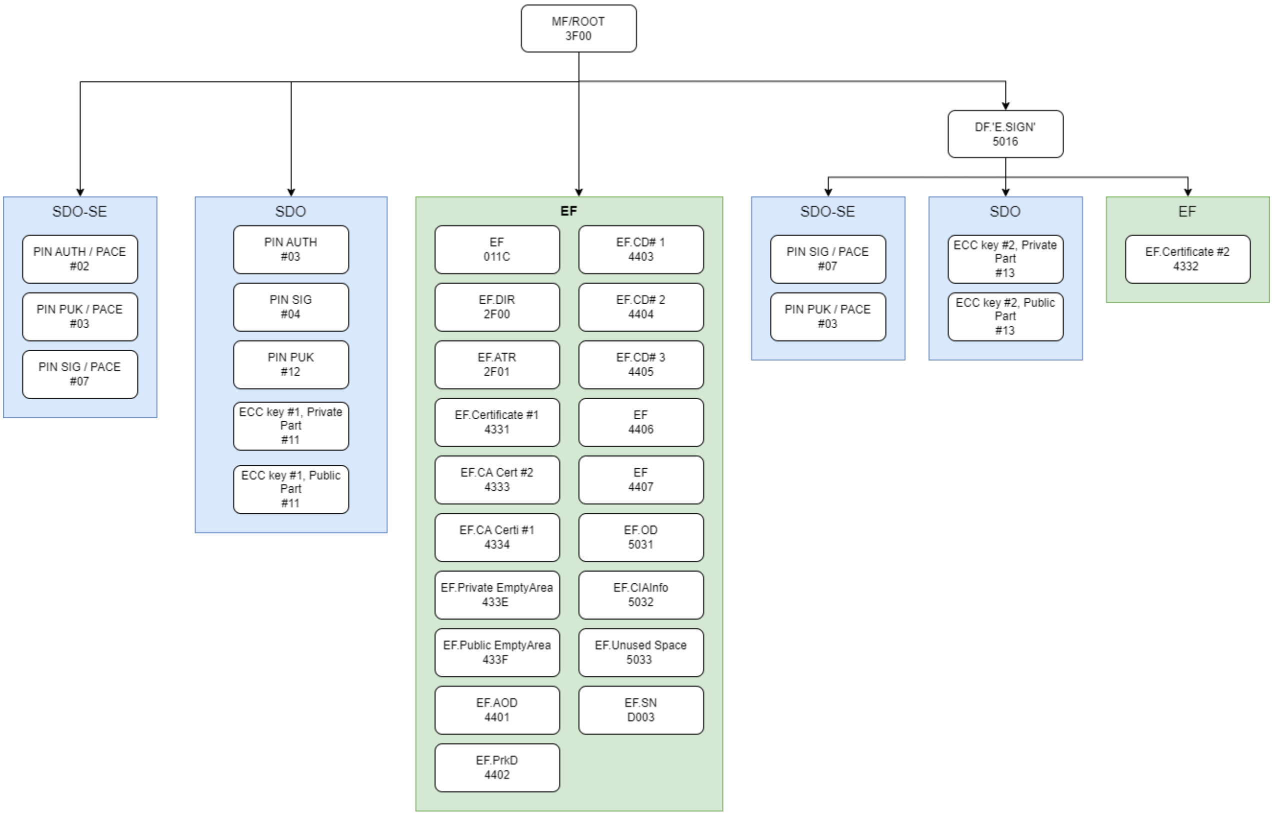
4 Profile description – IAS application

4.1 FILE SYSTEM

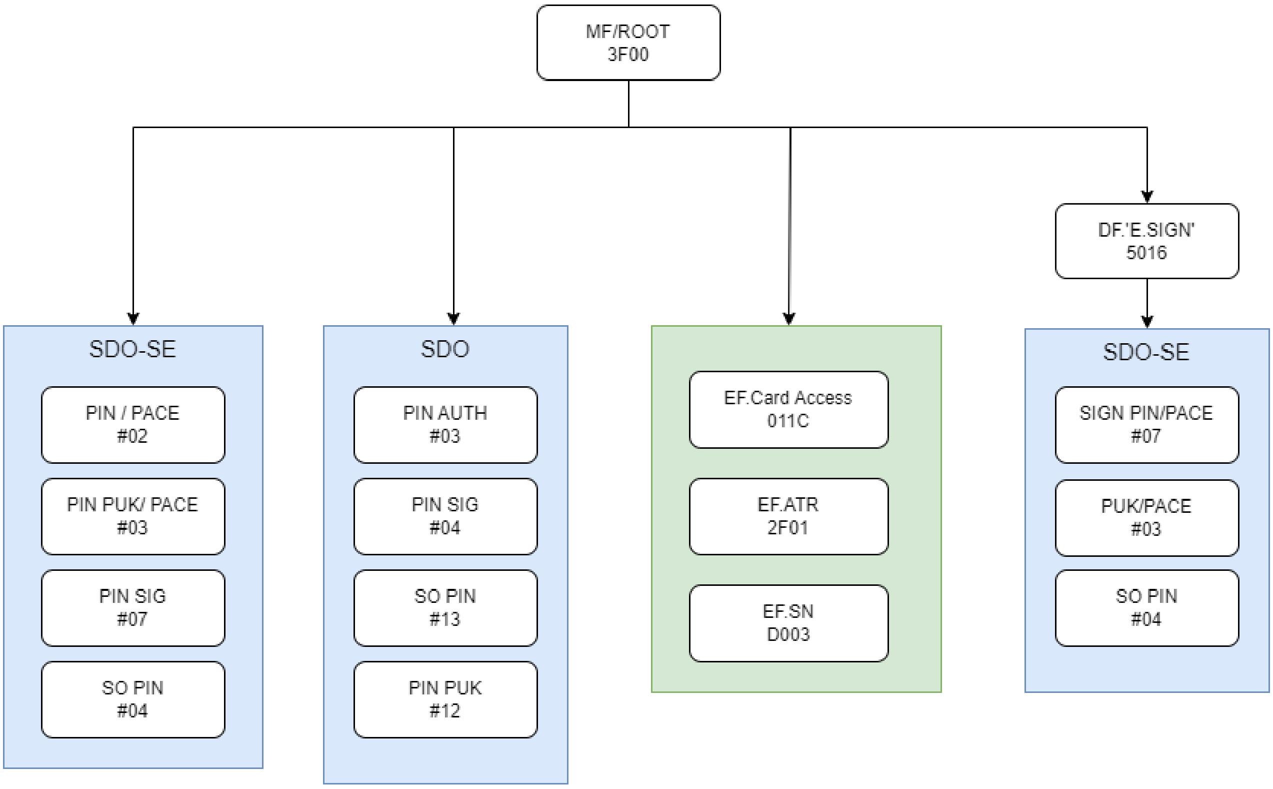
4.1.1 RSA - FILE SYSTEM



4.1.2 ECC - FILE SYSTEM



4.1.3 TEMPORARY - FILE SYSTEM



4.2 SE – Security Environment Lists

SE#2 stands for PIN AUTH (ID =03)
SE#3 stands for PIN PUK (ID =12)
SE#7 stands for local Signature PIN SIG (ID =04)
SE#4 stands for SO PIN (ID =13)

4.2.1 MF (3F00)

	Profile		
Item	**RSA**	**ECC**	**TEMPORARY**
1	SE#2 = PIN Auth #03	SE#2 = PIN Auth #03	SE#2 = PIN Auth #03
2	SE#3 = PIN PUK #12	SE#3 = PIN PUK #12	SE#3 = PIN PUK #12
3	SE#7 = PIN SIG #04	SE#7 = PIN SIG #04	SE#4 = SO PIN #13
4			SE#7 = PIN SIG #04

4.2.2 ADF (E.SIGN)

	Profile		
Item	**RSA**	**ECC**	**TEMPORARY**
1	SE#3 = PIN PUK #12	SE#3 = PIN PUK #12	SE#3 = PIN PUK #12
2	SE#7 = PIN SIG #04	SE#7 = PIN SIG #04	SE#4 = SO PIN #13
3			SE#7 = PIN SIG #04

4.3 RSA - SDO OBJECTS

4.3.1 PIN AUTH – PIN / PASSWORD

SDO ID	‘03’		
Security Attributes		Contact	Contactless
	Change reference data	Always	PACE
	Verify	Always	PACE
	Reset retry counter	SE#03	SE#03 + PACE
	Put Data	Never	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 05 remaining tries		
PIN Length	08 Max; 04 Min		

4.3.2 PIN PUK – PIN / PASSWORD

SDO ID	‘12’		
Security Attributes		Contact	Contactless
	Change reference data	Never	Never
	Verify	Always	PACE
	Reset retry counter	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 05 remaining tries		
PIN Length	08 Max; 04 Min		

4.3.3 PIN SIG – PIN / PASSWORD

SDO ID	‘04’		
Security Attributes		Contact	Contactless
	Change reference data	Always	PACE
	Verify	Always	PACE
	Reset retry counter	SE#03	SE#03 + PACE
	Put Data	Never	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 00 remaining tries		
PIN Length	08 Max; 04 Min		

4.3.4 RSA Private 01

SDO ID	‘01’		
Length	0180h (3072 bits)		
Non-Repudiation Flag	00h		
Security Attributes		Contact	Contactless
	PSO CDS	SE#02	SE#02 + PACE
	Internal Authenticate	SE#02	SE#02+ PACE
	PSO Decipher	SE#02	SE#02+ PACE
	Gen Asymmetric Key Pair	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.3.5 RSA Public 01

SDO ID	**‘01’**		
Length	0180h (3072 bits)		
Algo ID	‘00’ – No Limitation		
Security Attributes		**Contact**	**Contactless**
	PSO Verify Certificate	Never	Never
	External Authenticate	Never	Never
	PSO Encipher	Never	Never
	Gen Key Pair	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.3.6 RSA Private 02

SDO ID	**‘02’**		
Length	0180h (3072 bits)		
Non-Repudiation Flag	01h		
Security Attributes		**Contact**	**Contactless**
	PSO DS	SE#07	SE#07 + PACE
	Internal Authenticate	Never	Never
	Internal Authenticate	Never	Never
	PSO Decipher	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.3.7 RSA Public 02

SDO ID	**‘02’**		
Length	0180h (3072 bits)		
Algo ID	‘00’ – No Limitation		
Security Attributes		**Contact**	**Contactless**
	PSO Verify Certificate	Never	Never
	External Authenticate	Never	Never
	PSO Encipher	Never	Never
	Gen Key Pair	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.4 ECC – SDO OBJECTS

4.4.1 PIN AUTH – PIN / PASSWORD

SDO ID	**‘03’**		
Security Attributes		**Contact**	**Contactless**
	Change reference data	Always	PACE
	Verify	Always	PACE
	Reset retry counter	SE#03	SE#03 + PACE
	Put Data	Never	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 05 remaining tries		
PIN Length	08 Max; 04 Min		

4.4.2 PIN PUK – PIN / PASSWORD

SDO ID	**‘12’**

Security Attributes		**Contact**	**Contactless**
	Change reference data	Never	Never
	Verify	Always	PACE
	Reset retry counter	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 05 remaining tries		
PIN Length	08 Max; 04 Min		

4.4.3 PIN SIG – PIN / PASSWORD

SDO ID	**‘04’**		
Security Attributes		**Contact**	**Contactless**
	Change reference data	Always	PACE
	Verify	Always	PACE
	Reset retry counter	SE#03	SE#03 + PACE
	Put Data	Never	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 00 remaining tries		
PIN Length	08 Max; 04 Min		

4.4.4 ECC Private 01

SDO ID	**‘11’**		
Length	0180h (384 bits)		
Non-Repudiation Flag	00h		
Security Attributes		**Contact**	**Contactless**
	PSO CDS	SE#02	SE#02 + PACE

	Internal Authenticate	SE#02	SE#02 + PACE
	PSO Decipher	SE#02	SE#02 + PACE
	Gen Asymmetric Key Pair	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.4.5 ECC Public 01

SDO ID	**‘11’**		
Length	0180h (384 bits)		
Algo ID	‘00’ – No Limitation		
Security Attributes		**Contact**	**Contactless**
	PSO Verify	Never	Never
	Gen Key Pair	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.4.6 ECC Private 02

SDO ID	**‘13’**		
Length	0180h (384 bits)		
Non-Repudiation Flag	01h		
Security Attributes		**Contact**	**Contactless**
	PSO CDS	SE#07	SE#07 + PACE
	Internal Authenticate	Never	Never
	PSO Decipher	Never	Never
	Gen Key Pair	Never	Never

	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.4.7 ECC Public 02

SDO ID	**‘13’**		
Length	0180h (384 bits)		
Algo ID	‘00’ – No Limitation		
		Contact	**Contactless**
	PSO Verify	Never	Never
	Gen Key Pair	Never	Never
	Put Data	Never	Never
	Get Data	Always	PACE
Content			

4.5 TEMPORARY – SDO OBJECTS

4.5.1 PIN AUTH – PIN / PASSWORD

SDO ID	**‘03’**		
Security Attributes		**Contact**	**Contactless**
	Change reference data	Always	PACE
	Verify	Always	PACE
	Reset retry counter	SE#03	SE#03 + PACE
	Put Data	SE#04	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 05 remaining tries		
PIN Length	08 Max; 04 Min		

4.5.2 PIN PUK – PIN / PASSWORD

SDO ID	**‘12’**		
Security Attributes		**Contact**	**Contactless**
	Change reference data	Never	Never
	Verify	Always	PACE
	Reset retry counter	SE#04	Never
	Put Data	SE#04	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 05 remaining tries		
PIN Length	08 Max; 04 Min		

4.5.3 PIN SIG – PIN / PASSWORD

SDO ID	**‘04’**		
Security Attributes		**Contact**	**Contactless**
	Change reference data	Always	PACE
	Verify	Always	PACE
	Reset retry counter	SE#03	SE#03 & PACE
	Put Data	SE#04	Never
	Get Data	Always	PACE
Retry Counter	05 tries; 00 remaining tries		
Usage Counter	No usage counter		
PIN Length	08 Max; 04 Min		

4.5.4 SO PIN – PIN / PASSWORD

SDO ID	**‘13’**		
Security Attributes		**Contact**	**Contactless**

	Change reference data	SE#04	SE#04+PACE
	Verify	Always	PACE
	Reset retry counter	SE#04	SE#04 + PACE
	Put Data	SE#04	SE#04 + PACE
	Get Data	Always	PACE
Retry Counter	05 tries; 05 remaining tries		
PIN Length	08 Max; 08 Min		

4.6 RSA - EF and DF Files

4.6.1 File - MF (3F00)

ID	‘3F00’		
AID	‘A000000063504B43532D3135’		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate File	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Create File DF	Never	Never
	Create File EF	Never	Never
	Put Data	Never	Never
Content			

4.6.2 File - EF.Card access (011C)

ID	‘011C’		
Length	0052h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never

	Read Binary	Always	PACE
Content			

4.6.3 File - EF.DIR (2F00)

ID	‘2F00’		
Length	001Ch bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.4 File - EF.ATR (2F01)

ID	‘2F01’		
Length	003Eh bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never

	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.5 File - EF.Certificate #1 (4331)

ID	‘4331’		
Length	05A1h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.6 File - EF.CA Certificate #2 (4333)

ID	‘4333’		
Length	055Ah bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never

	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.7 File - EF.CA Certificate #1 (4334)

ID	‘4334’		
Length	0ACEh bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.8 File - EF.Private EmptyArea (433E)

ID	‘433E’		
Length	1000h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never

	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	SE#02	SE#02 + PACE
Content			

4.6.9 File - EF.Public EmptyArea (433F)

ID	'433F'		
Length	2000h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.6.10 File - EF.AOD (4401)

ID	'4401'		
Length	0087h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**

	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.11 File - EF.PrkD (4402)

ID	‘4402’		
Length	00B6h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.12 File - EF.CD# 1 (4403)

ID	‘4403’
Length	0084h bytes

Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.13 File - EF.CD# 2 (4404)

ID	'4404'		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.6.14 File - EF.CD# 3 (4405)

ID	'4405'

Length	0086h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.15 File - (DCOD) (4406)

ID	‘4406’		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.6.16 File - (DoDF) (4407)

ID	‘4407’		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.6.17 File - EF.OD (5031)

ID	‘5031’		
Length	0046h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.18 File - EF.CIAInfo (5032)

ID	‘5032’		
Length	001Dh bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.19 File - EF.Unused Space (5033)

ID	‘5033’		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.6.20 File - EF.SN (D003)

ID	‘D003’		
Length	000Ch bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.6.21 File - DF.ESIGN (5016)

ID	‘5016’		
DF (AID)	‘452E5349474E’ (E.SIGN)		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate File	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Create File DF	Never	Never
	Create File EF	Never	Never

	Put Data	Never	Never
Content			

4.6.22 File - EF.Certificate #2 (4332)

ID	‘4332’		
Length	0800h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7 ECC – EF and DF

4.7.1 File - MF (3F00)

ID	‘3F00’		
AID	‘A000000063504B43532D3135’		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate File	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Create File DF	Never	Never
	Create File EF	Never	Never
	Put Data	Never	Never
Content			

4.7.2 File - EF.Card access (011C)

ID	‘011C’		
Length	0052h bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never

	Read Binary	Always	PACE
Content			

4.7.3 File - EF.DIR (2F00)

ID	‘2F00’		
Length	001Ch bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.4 File - EF.ATR (2F01)

ID	‘2F01’		
Length	003Eh bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never

	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.5 File - EF.Certificate #1 (4331)

ID	‘4331’		
Length	05B4h bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.6 File - EF.CA Certificate #2 (4333)

ID	‘4333’		
Length	063Ah bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never

	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.7 File - EF.CA Certificate #1 (4334)

ID	‘4334’		
Length	063Ah bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.8 File - EF.Private EmptyArea (433E)

ID	‘433E’		
Length	1000h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**

	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	SE#02	SE#02 + PACE
Content			

4.7.9 File - EF.Public EmptyArea (433F)

ID	'433F'		
Length	2000h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.7.10 File - EF.AOD (4401)

ID	'4401'	
Length	0087h bytes	
Status	05	Operational

Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.11 File - EF.PrkD (4402)

ID	‘4402’		
Length	00C0h bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.12 File - EF.CD# 1 (4403)

ID	‘4403’

Length	0084h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.13 File - EF.CD# 2 (4404)

ID	'4404'		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.7.14 File - EF.CD# 3 (4405)

ID	‘4405’		
Length	0086h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.15 File - (DCOD) (4406)

ID	‘4406’		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE

Content	

4.7.16 File - (DoDF) (4407)

ID	‘4407’		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.7.17 File - EF.OD (5031)

ID	‘5031’		
Length	0046h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never

	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.18 File - EF.CIAInfo (5032)

ID	‘5032’		
Length	001Dh bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.19 File - EF.Unused Space (5033)

ID	‘5033’		
Length	0400h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never

	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	SE#02	SE#02 + PACE
	Read Binary	Always	PACE
Content			

4.7.20 File - EF.SN (D003)

ID	‘D003’		
Length	000Ch bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.7.21 File - DF.ESIGN (5016)

ID	‘5016’		
DF (AID)	‘452E5349474E’ (E.SIGN)		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**

	Delete File	Never	Never
	Terminate File	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Create File DF	Never	Never
	Create File EF	Never	Never
	Put Data	Never	Never
Content			

4.7.22 File - EF.Certificate #2 (4332)

ID	‘4332’		
Length	0800h bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.8 TEMPORARY – EF and DF

4.8.1 File - MF (3F00)

ID	‘3F00’		
AID	‘A000000063504B43532D3135’		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate File	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Create File DF	SE#04	Never
	Create File EF	SE#04	Never
	Put Data	SE#04	Never
Content			

4.8.2 File - EF.Card access (011C)

ID	‘011C’		
Length	0052h bytes		
Status	05	Operational	
Security Attributes		Contact	Contactless
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never

	Read Binary	Always	PACE
Content			

4.8.3 File - EF.ATR (2F01)

ID	‘2F01’		
Length	003Eh bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Update Binary	Never	Never
	Read Binary	Always	PACE
Content			

4.8.4 File - EF.SN (D003)

ID	‘D003’		
Length	000Ch bytes		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate EF	Never	Never
	Activate File	Never	Never

	Deactivate File	Never	Never
	Update Binary	SE#04	Never
	Read Binary	Always	PACE
Content			

4.8.5 File - DF.ESIGN (5016)

ID	‘5016’		
DF (AID)	‘452E5349474E’ (E.SIGN)		
Status	05	Operational	
Security Attributes		**Contact**	**Contactless**
	Delete File	Never	Never
	Terminate File	Never	Never
	Activate File	Never	Never
	Deactivate File	Never	Never
	Create File DF	Never	Never
	Create File EF	SE#04	Never
	Put Data	SE#04	Never
Content			

5 ISO 7816-15 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
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFF0000000000000000FFFFFFFF
ec_Param_A
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFF0000000000000000FFFFFFFC
ec_Param_B
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
ec_Order_P
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC7634D81F4372DDF581A0DB248B0A77AECEC196ACCC52973
ec_Coord_P_x
AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB7
ec_Coord_P_y
3617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
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 #03 has to be used for Internal Authentication and Decipher operations
For using the Private key of RSA Key 2 in contactless, PIN Sign #04 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)	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12
RSA 3072 (s)	30.78	105.75	14.79	19.75	11.44	12.06	19.2	27.07	9.22	28.72
On Board generation	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
ECC 384 (s)	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12
RSA 3072 (s)	13.31	30.96	37.77	17.42	11.51	59.26	13.1	24.09	37.27	39.69
On Board generation	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
ECC 384 (s)	0.13	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12	0.12
RSA 3072 (s)	43.61	9.57	36.9	35.71	31.56	18.82	10.66	12.59	116.07	19.88
On Board generation	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
ECC 384 (s)	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.11
RSA 3072 (s)	45.75	37.45	59.41	37.19	28.81	25.21	38.88	43.78	58.68	18.39
On Board generation	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**
ECC 384 (s)	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
RSA 3072 (s)	61.44	10.82	21.71	26.33	20.17	28.34	8.28	22.96	54.8	35.92

On Board generation	Mean Time (s)
ECC 384 (s)	**0.12**
RSA 3072 (s)	**27.71**