Cert. #	Product name	Vendor	Issue date / update date
54	IDPrime PIV 4.1 FIDO2.1 on IDcore3230	Thales	6/22/26

Tested Features

Algorithm Description → / Tested combinations of key and algorithm	3 Key Triple DES - ECB	RSA 1024 bit modulus	RSA 2048 bit modulus	AES-128 - ECB	AES-192 - ECB	AES-256 - ECB	ECC: Curve P-256	ECC: Curve P-384	Cipher Suite 2	Cipher Suite 7
Key ↓ Algorithm →	00/03	06	07	08	0A	0C	11	14	27	2E
PIV Secure Messaging key (04)									✓	✓
PIV Authentication key (9A)			✓				✓			
PIV Card Application Administration key (9B)				✓	✓	✓				
Digital signature key (9C)			✓				✓	✓		
Key management key (9D)			✓				✓	✓		
Retired Key management keys (80-95)			✓				✓	✓		
Card Authentication key (9E)										
Asymmetric			✓				✓	✓		
Symmetric				✓	✓	✓				

Maximum number of retired keys tested	20
Oncard key history function tested?	✓
Offcard key history function tested?	✓
Secure Messaging tested?	✓
Crypto Suites tested?	CS2, CS7
Intermediate CVC Tested?	✓
Use of Local PIN tested?	✓
Use of Global PIN tested?	✓
Local PIN Preferred tested?	✓
Global PIN Preferred tested?	✓
Use of OCC tested?	✓
VCI tested with pairing code?	✓
VCI tested without pairing code?	✓

Mandatory and conditional data objects tested	
Card Capability Container	✓
Card Holder Unique Identifier	✓
X.509 Certificate for PIV Authentication	✓
X.509 Certificate for Card Authentication	✓
X.509 Certificate for Digital Signature	✓
X.509 Certificate for Key Management	✓
Cardholder Fingerprints	✓
Cardholder Facial Image	✓
Security Object	✓
Optional containers tested	
Printed Information	✓
Discovery Object	✓
Key History Object	✓
Retired X.509 Certificates for Key Management	20
Cardholder Iris Images	✓
Biometric Information Templates Group Template	✓
Secure Messaging Certificate Signer	✓
Pairing Code Reference Data Container	✓

Notes

✓ indicates the feature has been tested.

× indicates the feature is not supported by the product.

Color	Card	Config	Key History	Opacity	PIN usage policy
	1	2.0	20 on card	CS2	7810
	2	2.1	20 off card	CS7	7810
	3	2.2	0	CS2	7810
	4	2.3	0	CS2	7810
	5	2.4	0	CS2	7C10

Card Profile 2.0

Key ID	Alg ID
04	27
9A	7
9B	08
9C	14
9D	14
Retired KMKs	20
82	7
83	7
84	7
85	7
86	7
87	7
88	7
89	7
8A	7
8B	7
8C	11
8D	11
8E	11
8F	11
90	11
91	14
92	14
93	14
94	14
95	14
9E	
Asymmetric	11
Symmetric	0C

Optional Features	Yes/No
Printed information buffer	Yes
Cardholder iris images	Yes
Discovery Object	Yes
PIN Usage Policy (tag 0x5F2F)	7810
Uses Local PIN	
Uses Global PIN	
Local PIN Preferred	
Uses OCC	
VCI implemented	
Requires pairing code	
Secure Messaging	Yes
Crypto Suite	CS2
Intermediate CVC	Yes
Key History	Yes
Key history keys with oncard certs	20
Key history keys with offcard certs	0

Notes:

Valid PIN Usage Policy byte 1

Secure messaging
OCC support

Card Profile 2.1

Key ID	Alg ID
04	2E
9A	7
9B	0A
9C	07
9D	07
Retired KMKs	20
82	7
83	7
84	7
85	7
86	7
87	7
88	7
89	7
8A	7
8B	7
8C	11
8D	11
8E	11
8F	11
90	11
91	14
92	14
93	14
94	14
95	14
9E	
Asymmetric	14
Symmetric	0A

Optional Features	Yes/No
Printed information buffer	Yes
Cardholder iris images	Yes
Discovery Object	Yes
PIN Usage Policy (tag 0x5F2F)	7810
Uses Local PIN	
Uses Global PIN	
Local PIN Preferred	
Uses OCC	
VCI implemented	
Requires pairing code	
Secure Messaging	Yes
Crypto Suite	CS7
Intermediate CVC	Yes
Key History	Yes
Key history keys with oncard certs	0
Key history keys with offcard certs	20

Notes:

Valid PIN Usage Policy byte 1

Secure messaging
OCC support

Card Profile 2.2

Key ID	Alg ID
04	27
9A	11
9B	0A
9C	11
9D	11
Retired KMKs	0
82	
83	
84	
85	
86	
87	
88	
89	
8A	
8B	
8C	
8D	
8E	
8F	
90	
91	
92	
93	
94	
95	
9E	
Asymmetric	07
Symmetric	0A

Optional Features	Yes/No
Printed information buffer	Yes
Cardholder iris images	Yes
Discovery Object	Yes
PIN Usage Policy (tag 0x5F2F)	7810
Uses Local PIN	
Uses Global PIN	
Local PIN Preferred	
Uses OCC	
VCI implemented	
Requires pairing code	
Secure Messaging	Yes
Crypto Suite	CS2
Intermediate CVC	Yes
Key History	No
Key history keys with oncard certs	0
Key history keys with offcard certs	0

Notes:

Valid PIN Usage Policy byte 1

Secure messaging
OCC support

Card Profile 2.3

Key ID	Alg ID
04	27
9A	07
9B	0C
9C	14
9D	14
Retired KMKs	0
82	
83	
84	
85	
86	
87	
88	
89	
8A	
8B	
8C	
8D	
8E	
8F	
90	
91	
92	
93	
94	
95	
9E	
Asymmetric	11
Symmetric	08

Optional Features	Yes/No
Printed information buffer	Yes
Cardholder iris images	Yes
Discovery Object	Yes
PIN Usage Policy (tag 0x5F2F)	7810
Uses Local PIN	
Uses Global PIN	
Local PIN Preferred	
Uses OCC	
VCI implemented	
Requires pairing code	
Secure Messaging	Yes
Crypto Suite	CS2
Intermediate CVC	Yes
Key History	No
Key history keys with oncard certs	0
Key history keys with offcard certs	0

Notes:

Valid PIN Usage Policy byte 1

Secure messaging
OCC support

Card Profile 2.4

Key ID	Alg ID
04	27
9A	07
9B	08
9C	14
9D	14
Retired KMKs	0
82	
83	
84	
85	
86	
87	
88	
89	
8A	
8B	
8C	
8D	
8E	
8F	
90	
91	
92	
93	
94	
95	
9E	
Asymmetric	11
Symmetric	0C

Optional Features	Yes/No
Printed information buffer	Yes
Cardholder iris images	Yes
Discovery Object	Yes
PIN Usage Policy (tag 0x5F2F)	7C10
Uses Local PIN	
Uses Global PIN	
Local PIN Preferred	
Uses OCC	
VCI implemented	
Secure Messaging	Yes
Crypto Suite	CS2
Intermediate CVC	Yes
Key History	No
Key history keys with oncard certs	0
Key history keys with offcard certs	0

Notes:

Valid PIN Usage Policy byte 1

Secure messaging
OCC support
without pairing