

Cert. #	Product name	Vendor	Issue date / update date
50	ID-One PIV 243	IDEMIA	1/2/2024

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			
												Mandatory and conditional data objects tested		
PIV Secure Messaging key (04)												Card Capability Container		
PIV Authentication key (9A)												Card Holder Unique Identifier		
PIV Card Application Administration key (9B)												X.509 Certificate for PIV Authentication		
Digital signature key (9C)												X.509 Certificate for Card Authentication		
Key management key (9D)												X.509 Certificate for Digital Signature		
Retired Key management keys (80-95)												X.509 Certificate for Key Management		
Card Authentication key (9E)												Cardholder Fingerprints		
Asymmetric												Cardholder Facial Image		
Symmetric												Security Object		
												Optional containers tested		
Maximum number of retired keys tested										20	Printed Information			
On-card key history function tested?										✓	Discovery Object			
Off-card key history function tested?										✓	Key History Object			
										Retired X.509 Certificates for Key Management				
Secure Messaging tested?										✓	Cardholder Iris Images			
Crypto Suites tested?										CS2 CS7	Biometric Information Templates Group Template			
Intermediate CVC Tested?										✓	Secure Messaging Certificate Signer			
										Pairing Code Reference Data Container				
												Notes		
Use of Local PIN tested?												✓	✓ indicates the feature has been tested.	
Use of Global PIN tested?												✓	✗ indicates the feature is not supported by the product.	
Local PIN Preferred tested?												✓		
Global PIN Preferred tested?												✓		
Use of OCC tested?												✓		
VCI tested with pairing code?												✓		
VCI tested without pairing code?												✓		