

Cert. #	Product name	Vendor	Issue date / update date
49	ActivID Applet 2.7.7 on Thales IDCore 3230 / 230 Platform	HID Global	08/11/2023

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			
	00/03	06	07	08	0A	0C	11	14	27	2E			
Key ↓                                  Algorithm →													
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											5		
On-card key history function tested?												✓	
Off-card key history function tested?												×	
Secure Messaging tested?												✓	
Crypto Suites tested?												CS2	
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?												✓	
<b>Mandatory and conditional data objects tested</b>													
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												✓	
<b>Optional containers tested</b>													
Printed Information												✓	
Discovery Object												✓	
Key History Object												✓	
Retired X.509 Certificates for Key Management												✓	
Cardholder Iris Images												×	
Biometric Information Templates Group Template												×	
Secure Messaging Certificate Signer												✓	
Pairing Code Reference Data Container												✓	
<b>Notes</b>													
✓ indicates the feature has been tested.													
× indicates the feature is not supported by the product.													