

Cert. #	Product name	Vendor	Issue date / update date
45	HID Global ActivID Applet Suite v2.7.6 on Giesecke & Devrient Sm@rtCafé Expert 7.0	HID Global, Inc.	5/9/2019

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)										✓	x	Card Capability Container	✓
PIV Authentication key (9A)			✓				x					Card Holder Unique Identifier	✓
PIV Card Application Administration key (9B)	x			x	x	x						X.509 Certificate for PIV Authentication	✓
Digital signature key (9C)			✓				x	x				X.509 Certificate for Card Authentication	✓
Key management key (9D)			✓				x	x				X.509 Certificate for Digital Signature	✓
Retired Key management keys (80-95)		x	✓				x	x				X.509 Certificate for Key Management	✓
Card Authentication key (9E)												Cardholder Fingerprints	✓
Asymmetric			✓				x					Cardholder Facial Image	✓
Symmetric	x			x	x	x						Security Object	✓
Optional containers tested													
Maximum number of retired keys tested											5	Printed Information	✓
On-card key history function tested?											✓	Discovery Object	✓
Off-card key history function tested?											x	Key History Object	✓
Secure Messaging tested?											Yes	Retired X.509 Certificates for Key Management	✓
Crypto Suites tested?											CS2	Cardholder Iris Images	x
Intermediate CVC Tested?											Yes	Biometric Information Templates Group Template	x
Use of Local PIN tested?											✓	Secure Messaging Certificate Signer	✓
Use of Global PIN tested?											x	Pairing Code Reference Data Container	✓
Local PIN Preferred tested?											x	Notes	
Global PIN Preferred tested?											x	✓ indicates the feature has been tested.	
Use of OCC tested?											x	x indicates the feature is not supported by the product.	
VCI tested with pairing code?											✓		
VCI tested without pairing code?											✓		