

Cert. #	Product name	Vendor	Issue date / update date
43	StarSign PIV Applet V1.0 on Giesecke+Devrient Sm@rtCafé Expert 7.0	Giesecke+Devrient Mobile Security	3/13/2018

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)										✓		x
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											2	
On-card key history function tested?											✓	
Off-card key history function tested?											x	
Secure Messaging tested?											Yes	
Crypto Suites tested?											CS2	
Intermediate CVC Tested?											Yes	
Use of Local PIN tested?											✓	
Use of Global PIN tested?											✓	
Local PIN Preferred tested?											✓	
Global PIN Preferred tested?											x	
Use of OCC tested?											✓	
VCI tested with pairing code?											✓	
VCI tested without pairing code?											x	
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											✓	
Cardholder Iris Images											✓	
Biometric Information Templates Group Template											✓	
Secure Messaging Certificate Signer											✓	
Pairing Code Reference Data Container											✓	
Notes												
✓ indicates the feature has been tested.												
x indicates the feature is not supported by the product.												