

Cert. #	Product name	Vendor	Issue date / update date
51	ZTPass PIV Applet v2.0 on NXP P71D600	ZTPass, Inc.	7/19/2024

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 →
PIV Secure Messaging key (04)												x	x
PIV Authentication key (9A)			✓				✓						
PIV Card Application Administration key (9B)	x			✓	✓	✓							
Digital signature key (9C)			✓				✓	✓					
Key management key (9D)			✓				✓	✓					
Retired Key management keys (80-95)		x	✓				✓	✓					
Card Authentication key (9E)													
Asymmetric			✓				✓						
Symmetric	x			✓	✓	✓							
Maximum number of retired keys tested											20		
Oncard key history function tested?											✓		
Offcard key history function tested?											✓		
Secure Messaging tested?											No		
Crypto Suites tested?											N/A		
Intermediate CVC Tested?											N/A		
Use of Local PIN tested?											✓		
Use of Global PIN tested?											✓		
Local PIN Preferred tested?											✓		
Global PIN Preferred tested?											✓		
Use of OCC tested?											x		
VCI tested with pairing code?											x		
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											x		
Biometric Information Templates Group Template											x		
Secure Messaging Certificate Signer											x		
Pairing Code Reference Data Container											x		
Notes													
✓ indicates the feature has been tested.													
x indicates the feature is not supported by the product.													