



ETION  
CREATE

A REUNERT COMPANY



SOLID

ID

Cryptographic token



## BENEFITS OF THE SOLIDid™

### Onboard Encrypted Storage

- ▶ Offers 1 GB of on-board encrypted storage for files and other data

### Upgradeable and Extensible

- ▶ Offer the ability to upgrade and extend the supported feature sets as required
- ▶ Ensure that tokens can be upgraded to address any future security vulnerabilities or attacks
- ▶ Provide the ability to add new algorithms and features as they become available

### Onboard Key Generation

- ▶ Offers the ability to perform on-board key generation, encryption and other cryptographic processing
- ▶ Ensures that cryptographic keys and functions cannot be compromised or altered by malware or other attacks

### Ease of Deployment

- ▶ USB based solution offering the security of a smart card without the need for costly smart card readers or other biometric devices
- ▶ No maintenance required, as tokens have no batteries which need replacing

### Compact

- ▶ Small and rugged, with a tamper-resistant construction for extra security

### Customisable

- ▶ Customised branding – The SOLIDid™ is fully customisable to fit client branding
- ▶ Additional / Custom algorithm support available on request
- ▶ Portable / Custom applications available on request

The SOLIDid™ forms part of the SOLIDGaurd range of cyber security products. The SOLIDid™ is a portable USB based PKI cryptographic token solution. The SOLIDid™ provides industry leading features and functionality which cover a wide range of information and cyber security applications.

As a USB based extension of smart card technology, the SOLIDid™ makes use of advanced cryptography to provide security for certificate based authentication, verification, signing and encryption. No other token solution currently on the market provides the wide range of cryptographic algorithms, curves and key sizes provided by the SOLIDid™.

Typical uses of the SOLIDid™ includes secure remote access for VPN and Web clients; multi-factor authentication; encryption and digital signing of emails and documents; digital certificate, key and password storage; and on-board key generation. As a FIPS 140-2 Level 3 validated solution, the SOLIDid™ provides additional cryptographic security by means of a hardware based true random number generator for improved security of on-board key generation.

Unlike other cryptographic tokens the SOLIDid™ is fully upgradeable, giving users the flexibility to change in step with the ever changing demands of the modern information security world. The SOLIDid™ provides the most flexible and extensible token solution in the market.

The SOLIDid™ is designed for use with all Public Key Infrastructure (PKI) environments and as such supports a wide array of cryptographic algorithms and APIs along with a host of different operating systems.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.





ETION  
CREATE



**Solid**  
ID

Cryptographic token



## TECHNICAL SPECIFICATIONS (SID5000)

<b>Symmetric</b>	AES	128, 192, 256 ECB, CBC, CFB, OFB, CTR, CCM, GCM, XTS
	TDES-EKE (Triple DES)	ECB, CBC, CFB, OFB
<b>Asymmetric</b>	RSA*	1024, 2048, 3072, 4096
	DSA	2048/224, 2048/256, 3072/256
	Diffie-Hellman	2048, 3072, 4096
	ECC, ECDSA, ECDH (Elliptic Curve Cryptography)	Primary: 224, 256, 384, 521 Kolbitz: 233, 283, 409, 571 Binary: 233, 283, 409, 571 Brainpool curves available as add-on
<b>Hash Digest</b>	SHA1*	Yes
	SHA2	256, 384, 512
	MD5*	Yes
<b>Digital Signing</b>	RSA (PKCS#1)	Yes, on-board
	DSS (FIPS-186)	Yes, on-board
<b>Certificate and Key Storage</b>	250	
<b>Onboard Encrypted Storage</b>	1 GB	
<b>Random Number Generation (RNG)</b>	Hardware True Random Number Generation (TRNG) On-board RNG based on RBGs specified in SP 800-90 (HASH, HMAC, CTR) and ANS X9.62-2005 (HMAC)	
<b>Upgrades and Extensions</b>	Additional curves for the above	

## OTHER FEATURES

### Supported Cryptographic APIs

- PKCS#11
- PKCS#15
- Microsoft CSP (CAPIv1) & KSP (CAPIv2)
- Microsoft PC/SC
- Apple Native PC/SC

### Supported Operating Systems

- Microsoft Windows 7 & 10
- Microsoft Windows Server 2008 & 2012
- macOS High Sierra (10.13) & Mojave (10.14)
- Linux (future)

### Cryptographic Functions

- Encrypt/decrypt
- Sign/verify
- Digest
- Key generation
- Wrap/unwrap
- Derive

### Certifications

- FIPS 140-2 Level 3 (HSID5000A)
- RoHS
- IPX7
- CE

\* Some algorithms not available in FIPS mode.

### Supported Applications (Tested)

- Windows Smart Card Logon
- Microsoft Office: Word, Outlook, PPT and Excel
- Microsoft Office and Outlook for Mac
- Adobe Acrobat Reader
- Mozilla Thunderbird, Firefox
- Apple Mail
- TrueCrypt / VeraCrypt

# Should support any application which supports the above listed Cryptographic APIs.