ETION CREATE

A REUNERT COMPANY

solid ID

Applications and Use Cases

Multi-Factor Authentication and Secure Remote Access

Most organisations make use of passwords to prevent unauthorised access to their internal corporate networks. The security provided by traditional password authentication can however be easily compromised by weak password selection or malware tools like key loggers. As a single factor of authentication, password authentication is also vulnerable to what is known as "social engineering" attacks, whereby an employee is unwittingly tricked into providing the attacker his/her login credentials.

Recent years have also seen a rapid growth in online services and applications, with clients increasingly expecting service providers to provide them with online access to their accounts. Organisations such as banks, municipalities and other service providers dealing with personal information and data, are increasingly finding themselves being exposed to reputational and even financial loss, as a result of cyber criminals targeting their clients through numerous phishing and similar types of attacks.

As a USB based extension of smart card technology the *SOLID***id**™ provides strong certificate based authentication, enabling organisations to also comply with the General Data Protection Regulation (GDPR) and data privacy. Due to the ever growing number of cyber threats, organisations are increasingly turning to cryptographic solutions such as the *SOLID***id**™ to not only secure their internal corporate networks, but also to limit access to their client facing, online or web-based applications and services. *SOLID***id**™ based authentication requires both the physical token (the first factor, the *SOLID***id**™ itself) as well as the user's PIN to unlock the token (the second factor) in order to complete the authentication. Certificate based authentication also provides web servers the ability to perform mutual authentication of the online transactions. In addition to strong authentication, Virtual Private Network (VPN) solutions further provide both Secure Socket Layer (SSL) or IPsec encryption of the online communications, protecting them from eavesdropping.

The *SOLID***id**™ is designed for use with all Public Key Infrastructure (PKI) environments and as such supports a wide array of cryptographic algorithms and Application Program Interfaces (APIs) which support a wide range of 3rd party web browsers and VPN solutions. **The** *SOLID***id**™ also integrates smoothly with Microsoft Windows Domain Servers for internal use.

Onboard Encrypted Storage

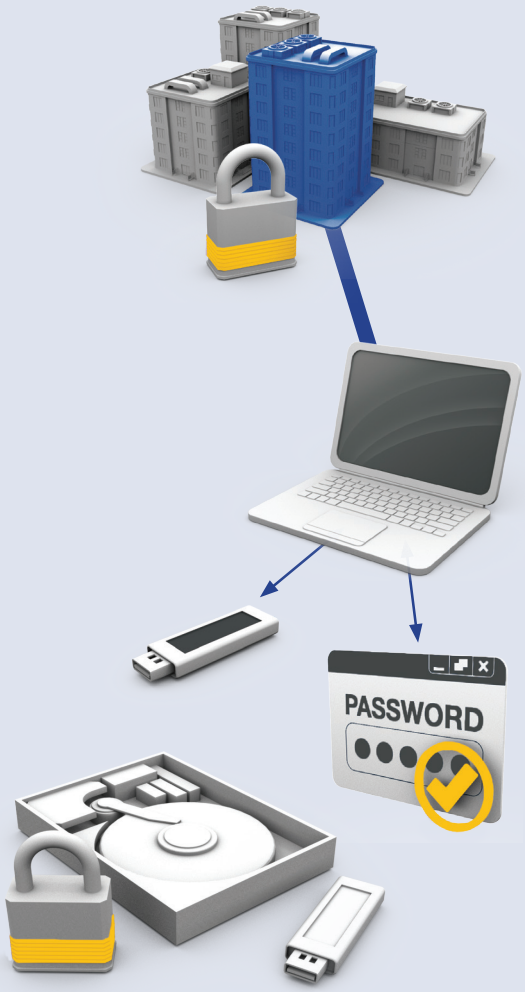
The *SOLID***id**™ provides 1 GB of on-board encrypted storage for files. The on-board encrypted storage is unlocked by means of the portable dashboard application provided on the Read Only Memory (ROM) of the token. Files stored in the encrypted storage are secured using AES 256 bit encryption..

File and Disk Encryption

Organisations are increasingly turning to both file and disk encryption as a means of protecting sensitive data from unauthorised access and theft. In some cases encryption is used as a means of adhering to legislation such as the General Data Protection Regulation (GDPR). The protection offered by encryption is often only as effective as the protection offered to the key(s) used to perform the encryption.

The *SOLID***id**™ makes use of advanced smart card technology to provide hardware security to ensure the secure storage of encryption keys. The *SOLID***id**™ is designed for use with all Public Key Infrastructure (PKI) environments and as such supports a wide array of cryptographic algorithms and APIs, making it suitable for use with most 3rd party encryption applications.

The *SOLID***id**™ forms part of the SOLIDGaurd range of cyber security products. The *SOLID***id**™ is a portable USB based PKI cryptographic token solution. The *SOLID***id**™ provides industry leading features and functionality which cover a wide range of information and cyber security applications. The following paragraphs explain typical applications for which the *SOLID***id**™ may be used in cyber security.



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

76 Regency Drive | Route 21 Corporate Park | Irene x 72 | South Africa
T: +27 12 678 9740 | F: +27 12 345 2561 | E: sales@etioncreate.co.za

ETION CREATE
A REUNERT COMPANY

solid ID

Applications and Use Cases

Email Signing and Encryption

Organisations and individuals alike are increasingly turning to encryption to ensure that sensitive email correspondence does not fall into unwanted hands. This is often as important for internal email correspondence as it is for external correspondence. A related requirement is to digitally sign correspondence so that it cannot be forged.

The *SOLIDid™* provides the required cryptographic tools and security required to easily implement such an email encryption solution. The *SOLIDid™* is compatible with commercial email clients such as Microsoft Outlook, Apple Mail and Thunderbird.

Document Signing

Through the use of properly issued certificates, companies and individuals can digitally sign documents. Properly issued certificates ensure that a digital signature is as binding as if it was signed on traditional paper. This is known as non-repudiation.

Digitally signed documents have the added benefit of being immune to alteration after signing. In today's global village, this is a huge benefit as it may improve collaboration between geographically separated parties and assist in concluding contracts remotely.

Based on advanced smart card technology, the *SOLIDid™* makes use of hardware security to ensure the proper safe keeping of the certificates and keys used with such digital signatures. The *SOLIDid™* makes use of industry standard APIs to ensure compatibility with applications like Microsoft Word and Adobe's Acrobat Reader.

Custom Zero Footprint Applications

The *SOLIDid™* provides "Zero footprint" capabilities for organisations with custom application requirements. Zero footprint functionality implies that the token may be used on any laptop or personal computer, without the need to preinstall software.

The *SOLIDid™* provides a portion of Read Only Memory (ROM) on which portable applications which execute from the token can be stored. The *SOLIDid™* also provides a dashboard application from which these applications can be launched.

The applications present on the *SOLIDid™* can be customised to an organisation's requirements. Examples of applications include a customised secure web browser which securely connects to the organisation's website or portal, providing mutual SSL authentication and a password manager.

Hardware Security Module (HSM)

The advanced cryptographic capabilities of the *SOLIDid™*, combined with its FIPS 140-2 level 3 validation, means that it is suitable for use as a low cost HSM module in applications which require secure key generation, storage and management.

Typical real world applications include the secure storage of certificates used by an organisation's local domain Certification Authority (CA).

The small size of the *SOLIDid™* means that it may easily be securely stored in a safe or vault.