Document Sealing Engine 200

Digital Signing & Time Stamping Appliance

PRODUCT | DATA SHEET

nCipher's Document Sealing Engine (DSE 200) is a networked appliance that cryptographically seals documents by applying a digital signature and independently, auditable time stamp. The Document Sealing Engine is a cost effective solution for organizations that require non-repudiation for document tracking, storage and submission.

Cryptographically Sealing a Document

While it is easy to determine when a hand written document has been tampered with, this is not so with electronic documents; leaving them vulnerable to undetectable manipulation and of dubious validity in the eyes of the law. Driven by the need to protect intellectual property, maintain legally valid business records, demonstrate compliance with industry standards best practices and, in many cases, comply with local and national laws, organizations are seeking document/content preservation solutions that meet both security and regulatory requirements without breaking the IT budget.

Organizational Solution

nCipher's Document Sealing Engine is a networked appliance that cryptographically signs, seals and time stamps a document, affixing a digital signature that binds an identity to the signed data. The DSE 200 can digitally signs documents or audit information on behalf of a person, a department, an organizational unit or even an entire company. Because most regulatory agencies do not require the submission of digital signatures from individual employees, but will accept a digital signature that represents the organization as a whole, the DSE 200 represents an easily implemented compliance solution.

With the DSE 200 integration toolkit, your organization can easily integrate the Document Sealing Engine into new or existing critical business applications, to sign, seal and time stamp documents enterprise wide.

Digital Signature

The DSE 200's digital signatures are produced using a digital certificate and are cryptographically bound to a document through standard public key signing methods. These digital signatures not only identify a group or organization signing the document, but also time stamp the signature and cryptographically seal the document making it tamper evident. The use of digital signatures in combination with a time stamp yields a trustworthy digital original that maintains its evidentiary value over time, even beyond the expiration of the original signing certificate.

Tamper Evident

With paper documents it is immediately evident when one word has been crossed out or written over. On an electronic document however, it might be impossible to tell even if whole paragraphs have been rewritten; so if the document and signature are to have credence, freezing the content of an electronic document is fundamental. The DSE 200 creates a cryptographic hash, a digital "fingerprint", which uniquely represents the content of the document at the time of signing, effectively freezing it. If even a comma is changed, the digital signature will fail and display a warning to the user.

Secure Time Stamping

The Document Sealing Engine is designed to operate with independently provided calibration and audit services. These service providers offer traceable and secure links to official Coordinated Universal Time (UTC) time sources. Once calibrated via an authenticated secure network connection, the DSE 200 is ready to provide time stamps to any PKIX compliant time stamp request.

FIPS 140-2 Security

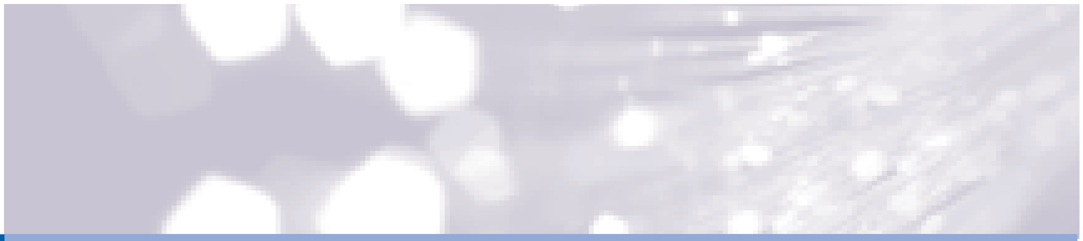
Cryptographic keys are the backbone of all cryptographic operations, but if left unprotected in a software environment, they become vulnerable to attack. To combat a wide range of potential attacks, including physical tampering, the DSC 200 utilizes an internal hardware security module (HSM). This HSM protects the internal time source and as stores and manages the cryptographic keys used in the signing and sealing process. By conducting all signing and cryptographic operations within the security boundary of the HSM, organizations can be confident in the level of protection provided.

The Document Sealing Engine's HSM, has been independently validated to the Federal Information Processing Standard (FIPS) 140-2 Level 3, a widely accepted security benchmark for securing cryptographic keys.

Integration Toolkit

The DSE API/SDK developers tool kit that contains a set of functions and sample code that enables simple and therefore rapid integration of document sealing functionality into new or existing applications. The toolkit supports Solaris, Linux and Windows platforms and is available in Java language classes and in C language libraries.

NCIPHER™
redefining cryptographic security



System Highlights

- Digital signing and time stamping appliance
- Automated time calibration
- Implements time stamping as specified by the IETF PKIX Time Stamp draft
- Up to 125 time stamps per second, 1024-bit RSA signatures
- 1U, Rack-mounted network appliance
- VeriSign time stamp certificate compatible
- Secure web-based management
- Tool kit support for ANSI C, MS VC++, Java
- Automatic error notification

Front Panel

- Connectors:
  Dual Ethernet port
  Serial Port for communications
  VGA connector for VDU
  Dual USB ports
- LED Indicators:
  Power
  HDD Activity
  Ethernet Activity

Rear Panel

- Power: On/Off

Technical Specifications

- Form Factor: 1U (1.75") x 17" W x 18" D (4.5cm x 43.2cm x 45.7cm)
- Network: Dual 10/100 Base-Tx Ethernet
- Serial Port: DB-9
- Video Port: 15 pin VGA
- 2 USB 1.1 ports
- Input Voltage: 100-240 volts AC auto switching, 50-60Hz (nominal)

  Maximum Power Consumption: 240 watts (2.1 amps at 110 volts AC)
- Mounting Systems: 19" rack mount
- Temperature/Humidity (Operational): +10 to +35^{O}C, 10 to 85% relative humidity, non condensing
- Acoustic Noise: <50dB at 1m in front of the system at full load
- Standards Certifications:

  FCC: CFR47, Part 15, Subpart B, Class A

  UL: 1950

  CE: EN55022, Class A; EN55024-1; EN60950

  FIPS 140-2 Level 3 certification

Every effort has been made to ensure the information included in this data sheet is true and correct at the time of going to press. However, the products described herein are subject to continuous development and improvement, and the right is reserved to change their specifications at any time. ©2003 nCipher Inc., CodeSafe, Document Sealing Engine and nCipher are trademarks or registered trademarks of nCipher Corporation Ltd. All other trademarks contained herein are the property of their respective holders.

NCD220 US ISSUE AUGUST 2003

nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801 USA
Tel: +1 781 994 4000
Fax: +1 781 994 4001

nCipher Corporation Ltd.
Jupiter House, Station Rd.
Cambridge, CBI 2JD UK
Tel: +44 (0) 1223 723600
Fax: +44 (0) 1223 723601

nCipher Corporation Ltd.
15th Floor, Cerulean Tower, 26-1
Sakuragaoka-cho, Shibuya-ku
Tokyo 150 8512
Tel: +81 3 5456 5484
Fax: +81 3 5456 5737