

THALES



WebSentry™

High Security Cryptographic
Devices for e-Business Applications

www.thalesgroup.com/eseurity

>> WEBSENTRY™



The WebSentry™ PCI and Ethernet cryptographic devices bring the highest level of security and performance to application servers for the processing of data encryption, payment transactions and digital signatures.

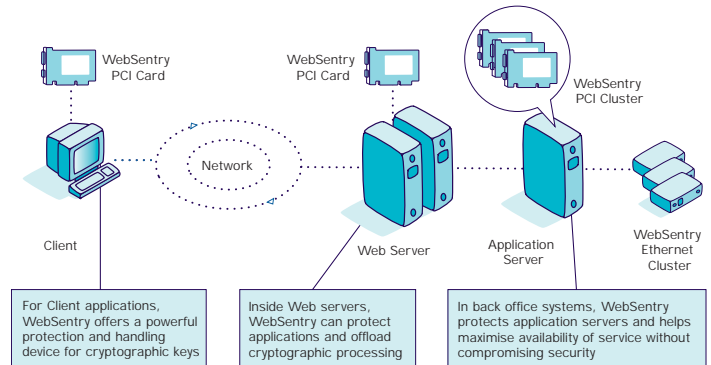
Cryptographic Processors for Secure Applications

The WebSentry platform offers an excellent combination of security, flexibility and performance to deliver cryptographic services to application servers. It supports multiple algorithms, protects cryptographic keys and processes in tamper-resistant hardware and is designed around a scalable architecture which lets WebSentry evolve with your security needs. The WebSentry platform represents the safest investment you can make for the security of your applications.

High Security Tamper-Resistant Devices

WebSentry products offer high levels of physical security. Any drilling, electrical probing or chemical attacks against the device will cause a critical alarm and instant erasure of secret keys and data. The cryptographic core of WebSentry has been certified to the highest security standards by independent certification bodies.

- Tamper-resistant Cryptographic Hardware for Encryption and Digital Signature
- PCI or Ethernet Hardware
- Scalable Platform
- High Availability through Built-in Load Balancing and Redundancy
- Integrated Device Management
- Flexible Upgrade and Enhancement
- Easy Integration with Applications



All cryptographic keys are stored securely within the tamper-resistant area of the device and all the cryptographic processes are executed in the same secure environment, thereby guaranteeing maximum security for the supported applications. Thorough key management implementation guarantees that no plaintext keys can be exposed outside the tamper-resistant circuitry of the device.

Access to the device's cryptographic and management functions can be secured using smart card technology and has multiple levels of access control.

Scalable Cryptographic Platform

By offloading complex cryptographic processes to the WebSentry platform, application hosts free valuable resources for handling business applications.

The built-in 'Resource Manager' automatically provides efficient load balancing and redundancy between WebSentry devices, transparently to the calling application.

The WebSentry platform offers full scalability to applications. Users gain a substantial performance increment with every new WebSentry device added to the system. WebSentry devices can be installed (or removed) independently of the host application, thereby offering extra performance without the need to make application software changes, and limiting disruption of service at the host system.

Flexible Development Options

Multiple Development Interfaces

For application integration, the WebSentry platform is supplied with the industry standard PKCS#11 interface for accessing all the cryptographic functions in the device. Extensions to the interface give developers access to extended cryptographic functions.

Options for integration into Java applications are also available, including interfaces to Java Cryptography Extension (JCE) and Java Secure Socket Extension (JSSE).

For users of the OpenSSL open source toolkit, an optional WebSentry "Engine" can be provided, which gives a higher level of interface to security functions.

Customisable Product

Due to its unique hardware design allowing for programmable cryptography, the WebSentry platform supports the development of custom functions. The loading of custom functions is secured using public key technology and all functions are executed within the tamper resistant hardware of the WebSentry device, thus guaranteeing optimal performance without compromising security.

This unique feature of the WebSentry platform offers application developers the ability to define their own security interface and to support any function or algorithm for their implementation.

Multiple Operating Systems

The WebSentry platform is supported on all the popular Operating Systems used in e-Business implementations. The management application delivers a consistent user experience and the benefits of WebSentry's linear clustered architecture are available to developers regardless of the target system.

This range of options ensures that you can benefit from all the advantages offered by the WebSentry platform to secure your e-Business, whatever your choice of infrastructure.

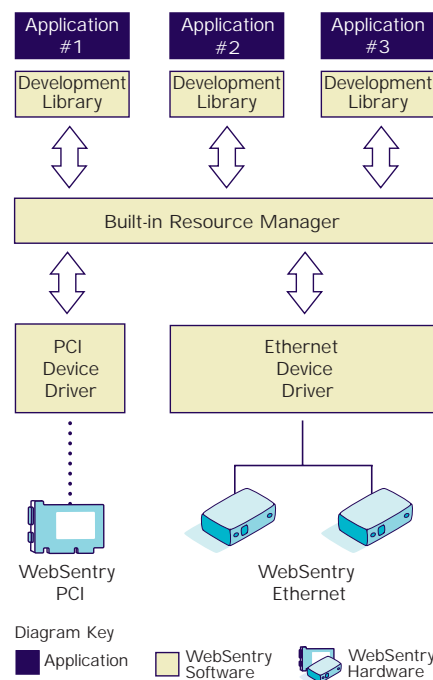
Integrated and Simple Device Management

A single management application can be used for installation and configuration of all WebSentry devices, simplifying the overall management of the security platform.

WebSentry devices support a highly secure and very flexible key management scheme that makes the WebSentry device adaptable to the most complicated security policies. All top level key components are held on smart cards under PIN control. The smart card reader used with the WebSentry device has an integral PIN pad for secure PIN entry.

Upgrades and enhancements to the WebSentry platform are done seamlessly and in total security through the WebSentry management application. In the longer term, upgrades to the security and functionality of the WebSentry devices can be performed, avoiding the cost of new hardware, maximising return on security investment.

WebSentry Architecture



Technical Specifications

PROGRAMMING INTERFACES SPECIFICATIONS

Development Interfaces	PKCS#11 v2.01 Java JCA / JCE / JSSE and J-P11 wrapper OpenSSL 0.9.6 and 0.9.7 Soft-loadable custom interface
Cryptographic Functions	DES and triple-DES key generation, encryption and decryption DES and triple-DES MAC generation and verification RSA key pair generation, signature and verification (512 to 2048 bits) DSA key pair generation, signature and verification (512 and 1024 bits) HMAC signature and validation (160 bits) Secure Socket Layer (SSL) v3 key generation and derivation mechanisms MD5 and SHA-1 message digest Certificate storage within tamper-resistant memory Hardware-based random number generator
Operating Systems	Microsoft Windows NT, 2000, XP and 2003 Linux SUN Solaris Other Operating Systems available on request

DEVICE SECURITY

Physical Security	Tamper evident chassis (Ethernet module) Tamper detection envelope surrounds cryptographic module Active zeroisation of sensitive data in case of attack Protection against voltage, chemical, temperature and penetration attacks
Security Certification	Security sub-system validated FIPS 140-1 level 4 Security sub-system under validation to FIPS 140-2 level 3* Random Number Generator validated to FIPS 186-2

PCI CARD SPECIFICATIONS

Communications Interfaces	PCI bus rev 2.2 (32 bit, 33MHz) Smart card reader with integral PIN Pad RS232 auxiliary port
Environmental	Operating Temperature: 23°F to 104°F (-5°C to 40°C) Storage Temperature: 15°F to 110°F (-10°C to 60°C)
Power	Approx. 5W from PC +5V supply
Physical Dimensions	Short Format – L6.9" (17.5cm) x W3.9" (9.8cm) x H0.7" (1.9cm)

ETHERNET DEVICE SPECIFICATIONS

Communications Interfaces	10BaseT Ethernet Smart card reader with integral PIN Pad RS232 auxiliary port
Environmental	Operating Temperature: 23°F to 104°F (-5°C to 40°C) Storage Temperature: 15°F to 110°F (-10°C to 60°C)
Power	External power supply, less than 7W, +/-12V and +5V supply
Physical Dimensions	L9.0" (23.0cm) x W8.7" (22.0cm) x H1.4" (3.5cm)

*Check on the NIST website for status of these validations.

EUROPE, MIDDLE EAST, AFRICA

Meadow View House, Crendon Industrial Estate
Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ, UK
Tel: +44 (0)1844 201800, Fax: +44 (0)1844 208550
e-mail: emea.sales@thales-esecurity.com

AMERICAS

2200 N. Commerce Parkway, Suite 200, Weston, Florida 33326, USA
Tel: +1 888 744 4976, +1 954 888 6200, Fax: +1 954 888 6211
e-mail: sales@thalesesec.com

ASIA PACIFIC

Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road, Central, Hong Kong, PRC
Tel: +852 2815 8633, Fax: +852 2815 8141, e-mail: asia.sales@thales-security.com



Certificate no. EMS 73638



Certificate no. FSA9836

The Thales policy is one of continuous development and consequently the equipment may vary in detail from the description and specification in this publication. All rights reserved.