



WebSentry™



High Security Cryptographic Devices
for e-Business Applications

- **Tamper-resistant Cryptographic Hardware for Encryption and Digital Signature Applications**
- **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 Using PKCS#11 or Customised Interface**



The WebSentry™ PCI and Ethernet cryptographic devices bring the highest level of security and speed 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.

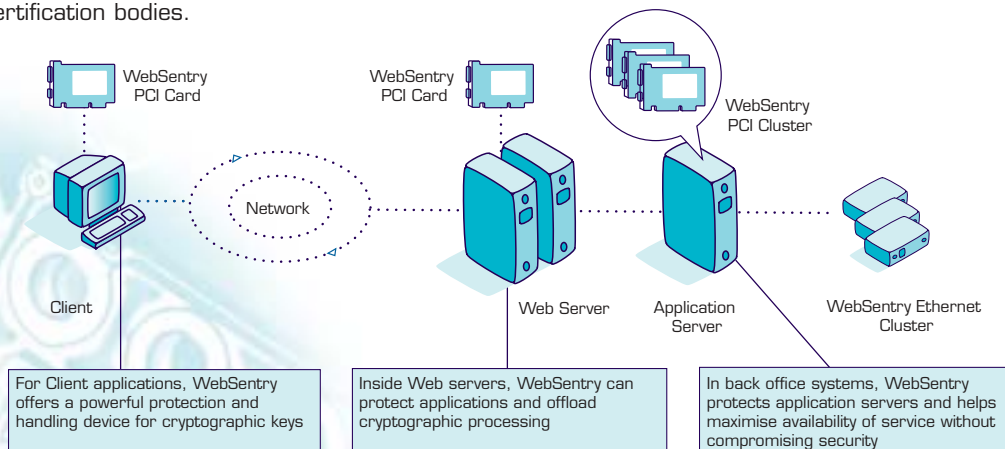
All cryptographic keys are stored securely within the tamper-resistant area of the device and all the cryptographic processes are executed in the same secure environment, thereby guaranteeing maximum security for the supported applications. Any drilling, electrical probing or chemical attacks against the device will cause a critical alarm and instant erasure of secret keys and data. Moreover, the WebSentry architecture and key management implementation guarantee that no plaintext keys are exposed outside the tamper-resistant circuitry of the device.

High Security Tamper-Resistant Devices

WebSentry products offer high levels of physical security. The cryptographic core of WebSentry has been certified to the highest security standards by independent certification bodies.

Scalable Cryptographic Platform

By offloading complex cryptographic processes such as key generation, digital signature and encryption 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. There is no limit to the number of devices you can put in a single system, and 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

PKCS#11 Interface

The standard library supplied with the WebSentry platform conforms to the PKCS#11 standard. The WebSentry PKCS#11 library gives access to all the cryptographic functions in the WebSentry device, in total conformity with the standards used in the security industry.

Because of the high security of the device, additional functions based on the PKCS#11 protocol give developers access to extended key management functions.

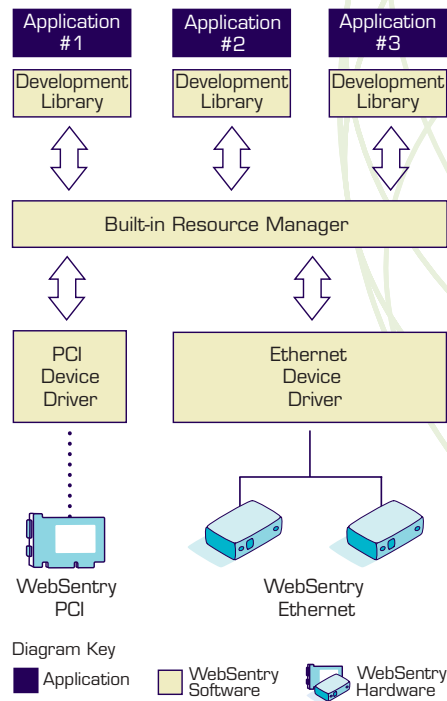
Static and dynamic versions of the library are available, which offers maximum flexibility for integration of the WebSentry platform into applications.

Custom Interface

Due to its unique hardware design, 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.

WebSentry Architecture



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. Access to the management application can be secured using smart card technology and has multiple levels of access control: "Crypto Officers" for the configuration tasks and "Users" for the operational tasks.

Upgrades and enhancements to the WebSentry platform are done seamlessly and in total security through the WebSentry management application. In the longer term, you can upgrade the security and functionality of the WebSentry devices without the cost of new hardware, thus maximising the return on your overall security investment.



Technical Specifications

Programming Interfaces Specifications

Interface Type	Industry Standard PKCS#11 v2.01 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 bit) HMAC signature and validation (160 bits) SET™ OAEP key wrapping Secure Socket Layer (SSL) v3 key generation and derivation mechanisms MD5 and SHA-1 message digest Hardware-based random number generator
Operating Systems	Windows NT 4.0 Workstation or Server Windows 2000 Professional or Server Linux Solaris

Device Security

Physical Security	Tamper evident chassis (Ethernet module) Tamper detection envelope surrounds cryptographic module Motion detection and temperature sensitive device Protection against voltage, chemical and penetration attacks
--------------------------	---

Security Certification

Security sub-system validated FIPS 140-1 level 4
WebSentry devices under validation to FIPS 140-2 level 3*
Security sub-system under validation to FIPS 140-2 level 4*

Device Specifications

PCI Card

Communications Interfaces	PCI bus rev 2.1 (32 bit, 33MHz) Smart card reader with integral PIN Pad, RS232 auxiliary port 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

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.

THALES

EUROPE, MIDDLE EAST, AFRICA

THALES e-SECURITY LTD.

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

AMERICAS

THALES e-SECURITY, INC.

2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
e-mail: [americas.sales@thales-
esecurity.com](mailto:americas.sales@thales-
esecurity.com)

ASIA PACIFIC

THALES e-SECURITY (ASIA) LTD.

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-
esecurity.com](mailto:asia.sales@thales-
esecurity.com)