

# Sun<sup>TM</sup> Crypto Accelerator 1000 Board

---

## *Components and Requirements*



Sun Microsystems, Inc.  
901 San Antonio Road  
Palo Alto, CA 94303  
1.800.786.7636  
1.512.434.1551

Copyright 2002 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, iPlanet, Netra, Solaris, Sun Blade, Sun Enterprise, Sun Fire, and Ultra are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

**RESTRICTED RIGHTS:** Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

# Contents

Executive Summary .....	4
Enhanced E-Commerce Security Performance .....	5
Market Value Proposition .....	5
Target Markets .....	6
Technology Overview .....	6
Algorithm Acceleration Support .....	8
Key Features & Benefits .....	9
Components & Requirements .....	10
Components.....	10
Hardware Support .....	10
Configuration .....	10
Scalability .....	11
Software Support .....	12
Warranty .....	12
Licensing & Usage .....	13
Conclusion .....	14

---

## Executive Summary

Enterprises continue to expand their e-business initiatives, resulting in exponential increases in the use of the Secure Sockets Layer (SSL) protocol to protect data confidentiality. Responding to these market demands, Sun is expanding its family of cryptographic accelerators with the addition of the Sun™ Crypto Accelerator 1000 board. Offering a significant performance improvement over the first-generation Sun Crypto Accelerator 1 board, the Sun Crypto Accelerator 1000 board is a dedicated hardware co-processor solution that off-loads SSL functions from a server's CPU, thereby freeing the CPU to perform other tasks and increasing processing speeds for secure transactions.

Businesses use the predominant SSL protocol to secure data transmission over unsecured networks. Supported by the leading Web servers and browsers, SSL increases security by encrypting client-server communications and providing other security functions such as authentication and message integrity. SSL, however, places a high computational demand on Web servers.

SSL benchmarks conducted at Sun show that a two-processor 336-MHz Sun Fire™ 4800 server capable of processing 2500 to 3000 unencrypted Web transactions per second slows to less than 100 transactions per second when SSL is enabled. The most compute-intensive cryptographic operations occur during SSL's *session creation*, in which a cryptographic session is established between a client and a server. The server incurs an additional computational load for *bulk encryption*, since each sensitive message exchanged between the client and the server must be encrypted.

Like the first-generation Sun Crypto Accelerator 1 board, the Sun Crypto Accelerator 1000 board off-loads compute-intensive SSL session creation calculations from a server CPU. Providing additional performance enhancements and product differentiation, the second-generation Sun Crypto Accelerator 1000 board also accelerates SSL bulk data encryption.

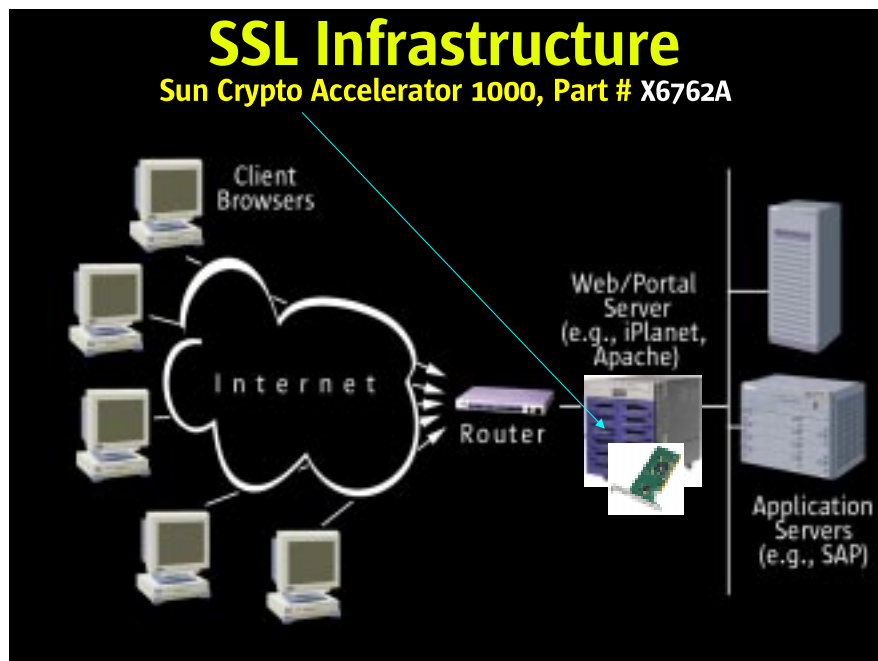
---

# Enhanced E-Commerce Security Performance

## Market Value Proposition

The Sun Crypto Accelerator 1000 board is optimized for Web server applications that use SSL. It provides optimized, scalable SSL operations at speeds much greater than a system CPU can achieve.

Most e-commerce environments already carry a great deal of encrypted Web traffic, or HTTP traffic. Because SSL is the primary method of encryption used in Web applications, the need for the acceleration of the authentication component has increasingly become more important.



The Sun Crypto Accelerator 1000 board is an ideal solution for customers using the SSL protocol for e-business needs due to the following reasons:

- Supports an increased number of simultaneous secure transactions
- Handles transactions faster than those without hardware acceleration
- Performs up to 4320 new SSL session creation operations per second using the 1024-bit RSA encryption algorithm on Sun servers running Sun™ ONE Web Server (formerly iPlanet™ Web Server) software using the Netscape NSS and the PKCS#11 interface, or Apache Web server software using the OpenSSL\* 0.9.6b driver library set

- Supports 3DES bulk encryption for Apache web servers at a rate of 500 Mbps for a 66-MHz PCI bus and 300 Mbps for a 33-MHz PCI bus
- Reduces the number of time-outs, resulting in fewer dropped connections

These benefits help companies reduce the number of servers needed for processing SSL-based traffic and allow businesses to undertake more cost-effective capacity planning as encrypted network traffic requirements grow.

\* This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit. This product includes cryptographic software written by Eric Young. This product includes software developed by Ralf S. Engelschall for use in the mod\_ssl project.

## Target Markets

Target markets for the Sun Crypto Accelerator 1000 board include both Sun's current installed base and future Web server customers who have a growing need for a high-performance cryptographic solution for SSL-encrypted e-commerce applications. These markets include the following segments:

- E-business
- Internet Service Provider (ISP)/Application Service Provider (ASP)/Managed Service Provider (MSP)
- Banking and finance

Both volume and enterprise computing servers used for secured Web server applications requiring vertical scaling will also benefit significantly from SSL hardware acceleration.

## Technology Overview

SSL is an application layer protocol originally developed by Netscape that completes two functions: authentication and bulk encryption communication between two systems.

SSL authentication is used by many Web applications, including Web servers, portal servers, leading application server platforms, and other Web-based applications. Sun's primary focus has been in the Web server software market. The Sun ONE Web Server and Apache Web server software are used in the majority of the installed base of Sun servers, running on the Solaris™ Operating Environment.

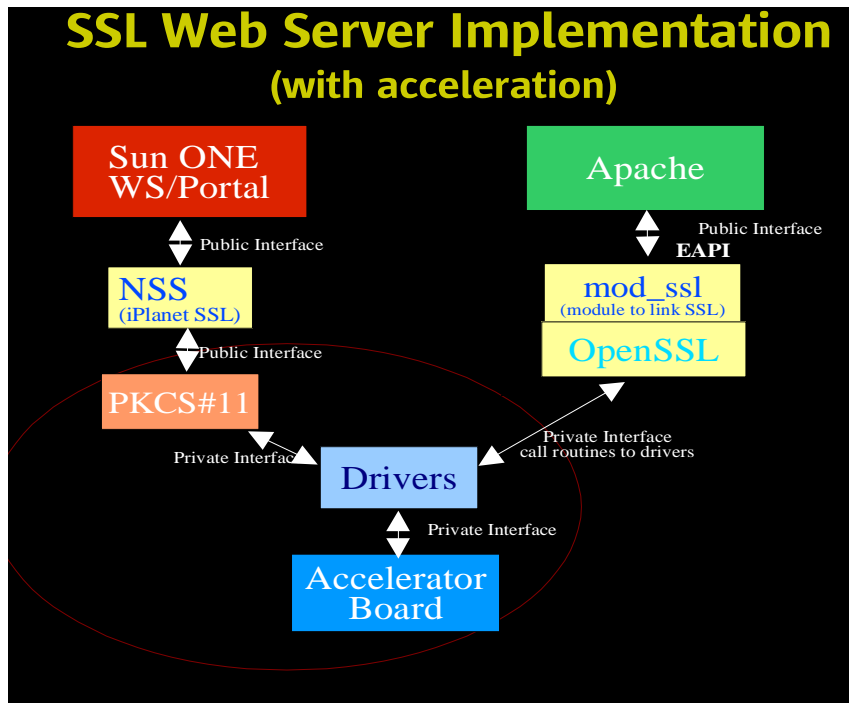
The most common deployment of SSL is between a Web browser client and a Web server, with the implementation following these steps:

1. A client seeks to create a connection with a Web server. It does so by sending a

greeting to the server along with the cryptographic algorithms it supports, also including a string of random bytes that are later used in the handshake.

2. The server responds to the greeting, sending back a message containing the server certificate (which include the server's public key), a session identifier, and another string of random bytes different from those sent by the browser.
3. The client verifies the signature on the server's certificate using the public key that is contained in a publicly available database built into the browser. This database is used by a large number of certificate authorities (CAs), one of which provided the original digital certificate and keys used by the server.
4. The client generates another string of random bytes, along with more information about its SSL capabilities. This is called a key exchange message. This message is now encrypted by the client using the public key of the server and is sent back to the server.
5. The server decrypts the key exchange message using its private key. This operation takes a long time to complete in software and thus is handed off to the Sun Crypto Accelerator 1000 board.
6. The client and server independently generate the session key for use in the rest of the SSL transaction. The session key is generated using the random bytes from both the initial greeting messages plus the bytes from the key exchange message. The authentication is complete, and the SSL session is established.
7. The client sends a message to the server requesting a change from public key encryption to using bulk encryption algorithms. This message also includes the session key.
8. The bulk encrypted transmission takes place.

The Sun Crypto Accelerator 1000 board is able to off-load the SSL functionality normally done by the system processor, taking on the various operations to speed up the authentication steps described above and the bulk encryption using 3DES (Apache servers only). By optimizing the complex mathematical operations involved in SSL procedures, the board can further speed SSL processing.



The Sun Crypto Accelerator 1000 interfaces with specific drivers based on the Web server software deployed. For Sun ONE Web Server software, it uses Network Secure Server (NSS) via the PKCS 11 public interface. For Apache Web server software, it uses OpenSSL via mod\_ssl libraries.

### Algorithm Acceleration Support

Algorithm	Sun ONE Web Server		Apache Web Server	
	Hardware	Software	Hardware	Software
RSA	Yes	Yes	Yes	Yes
DSA	Yes	Yes	Yes	Yes
D-H	No	No	Yes	Yes
DES	Yes	Yes	Yes	Yes
3DES	No	Yes	Yes	Yes
ARCFOUR	No	Yes	No	No

### Key Features & Benefits

<b>Feature</b>	<b>Benefit</b>
<p>Off-loads and optimizes the authentication portion of the SSL functionality for up to 4320 operations per second per card. Scalable to handle large SSL authentication loads.</p>	<p>The board optimizes server usage by handling more simultaneous transactions, speeding transactions, and helping reduce time-outs, resulting in fewer dropped connections. These benefits contribute to cost-effective server capacity and security systems planning to handle the transaction load increases of e-business.</p>
<p>1024-bit and 2048-bit RSA key sizes for strong encryption support. 3DES bulk encryption at 500 Mbps for Apache web servers.</p>	<p>The Sun Crypto Accelerator 1000 board supports existing public key encryption and thus existing applications with the support of RSA. The key size determines the strength of the encryption. The 1024-bit and 2048-bit keys are considered the strongest size for public key encryption by today's market. In addition, the RSA algorithm is one of the most widely used public key encryption algorithms in the market.</p>
<p>Investment protection by supporting common hardware and software installations.</p>	<p>Sun has the largest installed base of Web servers in the market today. These implementations are generally Sun ONE Web Server and Apache Web server software solutions. By supporting these applications and a majority of Sun servers and workstations, the Sun Crypto Accelerator 1000 board works with existing solutions, protecting technology investments for both Sun's installed base and new Web server implementations.</p>

---

# Components & Requirements

## Components

The Sun Crypto Accelerator 1000 board includes the following components:

- Sun Crypto Accelerator 1000 PCI add-on co-processor board
- Sun Crypto Accelerator 1000 Drivers v1.0
- Sun Crypto Accelerator 1000 installation guide and documentation
- Sun Crypto Accelerator 1000 Support Software v1.0

## Hardware Support

The Sun Crypto Accelerator 1000 board is compatible with most entry-level Sun servers, Sun Fire™ servers, and Sun workstations. Phase 2 of the Sun Crypto Accelerator 1000 release will include support for the Sun Fire 15000 server and Solaris 9 Operating Environment.

The Sun Crypto Accelerator 1000 board sits on a 32/64-bit, 33/66-MHz PCI bus. It can be used in racked configurations of multiple servers, with each server using a board and running Sun ONE Web Server or Apache Web server software.

## Configuration

Configuration recommendations are one board for a one-processor server, up to two boards for an eight-processor server, and up to four boards for a server with 12 processors or more. Multiple boards are supported for large SMP machines, allowing customers to deploy as many as four cards to address high-availability and Dynamic System Domains computing needs.

For Web server needs, the current generation of Sun Fire servers with support for as many as 16 CPUs can support a second Sun Crypto Accelerator 1000 board to enhance SSL processing performance. One card can perform up to 4320 secure connections per second in a server with 16 CPUs, while two cards can provide more than 6200 secure connections per second in a server with 24 CPUs.

The following table shows the maximum number of Sun Crypto Accelerator 1000 boards that are supported for use in compatible Sun workstations and servers.

Servers	Maximum number boards per system (PCI)	Number of CPUs suggested
Sun Ultra™ 10	1	1
Sun Ultra™ 60	1	2
Sun Ultra™ 80	1	2
Sun Enterprise™ 220	1	2
Sun Enterprise™ 250	1	2
Sun Enterprise™ 420	1	4
Sun Enterprise™ 450	1	4
Sun Enterprise™ 3500	NS	NS
Sun Enterprise™ 4500	NS	NS
Sun Enterprise™ 5500	NS	NS
Sun Enterprise™ 6500	NS	NS
SunBlade™ 1000/2000	1	2
SunBlade™ 1500/2500	1	2
Sun Fire V120	1	1
Sun Fire 280R	1	2
Sun Fire V480	1	4
Sun Fire V880	2	8
Sun Fire V1280	2	8
Sun Fire 3800	NS	NS
Sun Fire 4800	4	12
Sun Fire 4810	4	12
Sun Fire 6800	4	24
Sun Fire 12K/15K	NS	64
Netra™ T4	1	2
Netra™ T1120/25	1	2
Netra™ 14xx	1	4
Netra™ T1 AC200	1	1
Netra™ 100/105	NS	1

## Scalability

Scalability of the Sun Crypto Accelerator 1000 board is based on a combination of additional CPUs and on a number of processes supported within an individual Web server or within multiple virtual Web servers residing on one machine. The following table provides some examples for scaling encryption performance numbers using the Sun Crypto Accelerator 1000 board. Internal tests included use of 1-GHz and 750-MHz processors. As shown in the following table, different server platforms were deployed for the benchmark estimates.

<b>Web Server</b>	<b>Sun Server Platform</b>	<b># of CPUs</b>	<b>RSA Operations per Second</b>
Sun ONE & Apache	Sun Fire 280R	2	550 to 668
Sun ONE & Apache	Sun Fire V880	8	1500 to 2000
Sun ONE & Apache	Sun Fire 4800	12	Up to 3000
Sun ONE	Sun Fire 6800	16	4320
Sun ONE	Sun Fire 6800 with 2 accelerator boards	24	6200

## Software Support

The Sun Crypto Accelerator 1000 board supports SSL implementations on the following applications:

- Sun ONE Web Server, v4.1 SP 9 and v6.0 SP 1
- Apache 1.3.12 Web server software

The Sun ONE Web Server software uses NSS via the PKCS#11 interface to communicate with the accelerator board. Apache 1.3.12 Web server software, which is bundled with the Solaris 8 Operating Environment, uses the OpenSSL 0.9.6b driver library set to interface with the board. The OpenSSL 0.9.6b driver library set has been tuned to work with the board and is bundled with the product.

The SSL accelerator board supports the Solaris 8 Operating Environment, revision 5 (7/01) and subsequent revisions within Solaris 8. The Solaris 9 Operating Environment, Sun ONE Directory Server (formerly iPlanet Directory Server), and Sun ONE Portal Server (formerly iPlanet Portal Server) products will be supported in the future.

## Warranty

The Sun Crypto Accelerator 1000 board is covered under the same warranty terms of the machine in which it is installed. If the host machine is no longer under the original

manufacturer's warranty, this product will be covered under standard warranty terms and conditions, which includes a one-year warranty. Warranty service response begins at the time of the initial service request during business hours. Reasonable efforts will be made to acknowledge and respond to requests within eight business hours.

## Licensing & Usage

One or more Sun Crypto Accelerator 1000 boards can be used per server. There are no licensing issues with this product.

## Conclusion

The Sun Crypto Accelerator 1000 board offers e-business organizations significant performance gains and supports more cost-effective capacity planning as encrypted network traffic requirements grow. Because the board handles SSL authentication loads, Web servers are able to take full advantage of their processor resources to perform at their highest possible capacity performance and throughput levels. As a result, companies can scale their systems in support of operational growth and system availability instead of adding processors simply to handle SSL processing needs.

In addition, the Sun Crypto Accelerator 1000 board handles transactions faster than those without hardware acceleration and helps reduce the number of time-outs, resulting in fewer dropped connections. These benefits help companies handle a larger number of customers simultaneously while aiding in increasing customer satisfaction through faster response times.



Sun Microsystems, Inc.  
901 San Antonio Road  
Palo Alto, CA 94303

1.800.786.7638  
1.512.434.1511

<http://www.sun.com/security/>