

Sun™ Crypto Accelerator I™ Board

*Hardware and Software Components and
Requirements*



Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
1 (800) 786.7638
1.512.434.1511

Copyright 2000 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, CacheFS, Java, Java Studio, Java WorkShop, NFS, Solaris, Solaris Resource Manager, SunOS, SunATM, Sun WorkShop, Sun Visual WorkShop, Trusted Solaris, and Ultra are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

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.

Copyright 2000 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, CacheFS, Java, Java Studio, Java WorkShop, NFS, Solaris, Solaris Resource Manager, SunOS, SunATM, Sun WorkShop, Sun Visual WorkShop, Trusted Solaris, et Ultra sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please
Recycle

Contents

| | |
|---|----|
| Executive Summary | 1 |
| Enhancing E-Commerce Server Security Performance..... | 2 |
| Market Value Proposition | 2 |
| Technology Overview..... | 3 |
| Compatibility | 4 |
| Warranty | 4 |
| SSL Support..... | 5 |
| Sun Crypto Accelerator I Hardware and Software | |
| Components and Requirements | 6 |
| Key Features and Benefits | 6 |
| Scalability | 7 |
| Configurations | 8 |
| Target Users | 8 |
| Supported Application | 9 |
| Licensing and Usage | 9 |
| Conclusion | 10 |

Executive Summary

New market trends from eBusiness and web access demands are redefining performance expectations for security and session transactions over the web. Many financial and commerce organizations who are moving into e-commerce and business-to-business over the web, have a special need for fast and reliable electronic transactional system for their services.

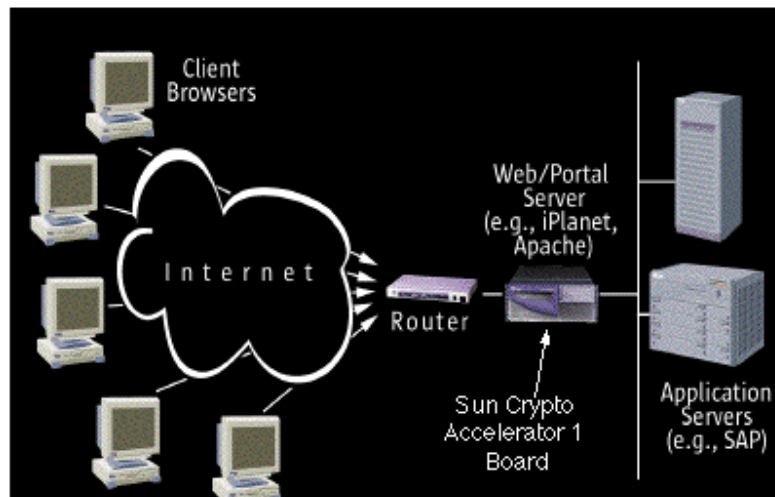
Important things to consider in doing business over the web are that e-commerce requires both security and fast response, since customers can be lost to competitors who are just a click away. With security enabled, Web servers may not keep up with customer demand. Adding additional servers can temporarily help. However, the acquisition and maintenance costs of additional servers are very high.

Sun has developed a solution to deliver a higher performance level for its systems deployed as web servers, the Sun Crypto Accelerator I™ board. This secure sockets layer (SSL) accelerator board is PCI bus based, and supports Sun server platforms using the Solaris Operating Environment. It is a co-processor solution, which off-loads the SSL function from the server's CPU. Used in many web applications, the Sun Crypto Accelerator I board supports iPlanet Web server, iPlanet Portal Server, and Apache Web servers. This accelerator board provides up to five times the performance of a system not using any acceleration, with a speed of 200 operations per sec per board. It is scalable up to 1,400 operations per second. It is suitable for e-commerce applications using SSL encryption via PKCS11 interface.

The Crypto Accelerator I card is the first of a new line of encryption products from Sun. This paper will introduce the co-processor board components and concepts that address the off-loading of the Secure Socket Layer (SSL) processing from the main system board to achieve optimal performance in Web server applications.

Enhancing E-Commerce Server Security Performance

Sun Crypto Accelerator 1 x1133A



Market Value Proposition

The Sun Crypto Accelerator I board is optimized for server usage in web applications using 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 (or HTTP) traffic. Since SSL is the primary method of encryption used in Web applications, such as Web servers, the need for the acceleration of the authentication component has become more and more important. The Crypto Accelerator I board is an ideal solution for such environments:

- It handles more simultaneous transactions
- It handles transactions faster than those without hardware acceleration
- It reduces the number of time-outs, thus resulting in less dropped connections

By adding more Sun Crypto Accelerator I boards to a system, performance can be optimized to the system's SSL authentication load. This results in the use of fewer servers and more cost-effective capacity planning as encrypted network traffic requirements grow.

Technology Overview

The Sun Crypto Accelerator I board is able to off-load the SSL functionality normally done by the system processor (CPU). The board is able to leverage its key feature, the ability to complete complex mathematical operations and provide optimized performance for Web server implementations of SSL. SSL is an application layer protocol that was originally developed by Netscape.

The SSL software is able to complete two functions: to provide a method of authentication, and to complete bulk encryption communication between two systems. The standard reference implementation is between a client and server — typically a browser and a Web server. The scenario can be described as follows:

1. A client seeks to create a connection with a Web server. It does so by sending a greeting along with the cryptographic algorithms it supports to the server along with a string of random bytes (which 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 certificate authority (CA) database built into the browser. This database contains a number of CA's, which are trusted by the browser.
4. The client generates another string of random bytes called pre-master secret, 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 sent back to the server. (It is encrypted because the pre-master secret must be kept secret.) The server decrypts the key exchange message using its private key. This operation, which takes significant CPU processing time when executed in software, is instead handed off to the Sun Hardware Crypto Accelerator I board.
5. Now the client and server know the pre-master secret. Using that shared piece of secret information and the random bits exchanged, the client and the server independently generate the session keys for use in the rest of the SSL transaction. The SSL session is established.
6. The bulk-encrypted transmission then takes place.

Compatibility

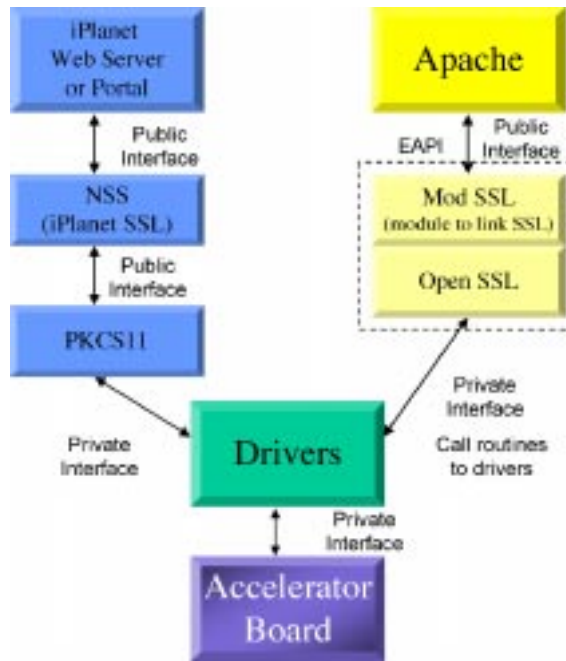
Sun Crypto Accelerator board is compatible with most Sun enterprise and mid-range Sun servers. It sits on a 32bit, 33 MHz PCI bus. Compatibility with the Sun Enterprise™ 10000 server, as well as the Netra servers, is targeted for availability in the first half of 2001. For a list of supported Sun servers and switches, see the Requirements and Configuration section of this document.

Sun Crypto Accelerator board is compatible with PKCS11 supported SSL on Web server applications such as iPlanet Web server 3.6, 4.0, & 4.1 and iPlanet Portal Server 3.0 sp1 (open mode implementation); it is also supports Apache (running Open SSL 0.9.4). The SSL accelerator board works in the Solaris™ Operating Environment, versions 2.6, 7, and 8.

Warranty

The Sun Crypto Accelerator I 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 time of the initial service request, during business hours. Reasonable efforts will be made to respond to and acknowledge requests within eight (8) business hours.

SSL Support



SSL is an encryption protocol developed by Netscape for encrypting entire sessions between computers, including both authentication and bulk encryption. This protocol has been incorporated into a large number of Web-based applications including Web servers (iPlanet, Apache), portal servers, leading application server platforms, and other Web-based applications.

SSL Provides basic security services to higher layer protocols such as HTTP. The SSL protocol provides authentication and private, encrypted communication between the two systems. The most common deployment is between a web browser client and a web server.

Sun Crypto Accelerator I Hardware and Software Components, Benefits and Requirements

Hardware and software components include:

- Sun Crypto Accelerator I PCI add-on co-processor board
- Sun Crypto Accelerator I Drivers v1.0
- Sun Crypto Accelerator I installation guide

Sun Crypto Accelerator I board has a minimum requirement of a 200MHz UltraSPARC™ system with 64 MB RAM. The hardware scalability is dependent on the size of the machine and the number of available PCI slots. The solution scales well and can be used in a scenario where multiple accelerator boards per system are required.

Software requirements include the Solaris™ 2.6, 7, or 8 Operating Environment. The CD packaged with the product provides driver configurations for iPlanet Web Servers using PKCS11. Source patches are available for Open SSL.

Features and Benefits

Sun Crypto Accelerator board provides the following features and benefits:

| Features | Benefits |
|---|---|
| A coprocessor solution that off-loads the authentication portion of the SSL functionality at a rate of 200 operations/second per card, it is also scalable to handle large system SSL authentication loads. | Optimizes server usage. Allows a more cost-effective implementation to handle transaction load increases in e-commerce situations. It can handle more simultaneous transactions, faster transactions, with fewer time-outs and less dropped connections. The Crypto Accelerator I is optimized performance for system SSL authentication load. These benefits result in more cost-effective server utilization. |

| Features | Benefits |
|---|--|
| 1024-bit RSA encryption | The Sun Crypto Accelerator I supports existing public key encryption, such as those based on RSA. The key size determines the strength of the encryption — a 1024-bit key is considered a strong size for public key encryption in today's market. In addition, the RSA algorithm is one of the most widely used public key encryption algorithms in the market. |
| Supports iPlanet and Apache Web servers using PKCS11 and OpenSSL version 0.9.4 interfaces | The Sun Crypto Accelerator I works with existing applications. Sun has the largest installed base of Web servers in the market today. These implementations generally use either the iPlanet and Apache Web server solutions. By supporting both the installed base and new Web server implementations, customers can obtain the performance benefit of the Crypto Accelerator I board across a wide variety of solutions. |

Scalability

The board provides an almost linear scalability. With Crypto boards, a Sun Enterprise 6000 server, with 18 CPUs, can process up to 1,400 SSL operations per second. This is due to application limitations rather than hardware. Future implementations of Web server and portal software will allow for a full linear 1,600 operations per second scalability using 8 cards. However, a more common solution would be having two Web servers with four Crypto cards each, sharing the load. This would bring the numbers closer to the expected 1,600 SSL operations per second, and the solution would also address high availability needs.

Configuration

Sun Crypto Accelerator I supports the following platforms (X-Options only):

Sun Crypto Accelerator I Board Maximum Configuration

| Servers | Maximum number boards per system |
|---------------------------|---|
| Sun Ultra™ 60 | 1 |
| Sun Ultra™ 80 | 1 |
| Sun Enterprise™ 220 | 1 |
| Sun Enterprise™ 250 | 1 |
| Sun Enterprise™ 420 | 2 |
| Sun Enterprise™ 450 | 2 |
| Sun Enterprise™ 3000/3500 | 3 |
| Sun Enterprise™ 4000/4500 | 4 |
| Sun Enterprise™ 5000/5500 | 4 |
| Sun Enterprise™ 6000/6500 | 8 |
| Sun Enterprise™ 10000 | 8 - First Half 2001 |
| Netra™ 11xx | 1 - First Half 2001 |
| Netra™ 14xx | 1 to 2 - First Half 2001 |
| Netra™ Tx | 1 - First Half 2001 |

Target Users

The target markets are both Sun's current installed base and future Web server customers who have a growing need for a high-performance cryptographic solution for the SSL encrypted e-commerce applications, such as for the following applications:

- Web servers
- ISP/ASP/MSP — Internet service providers, application service providers, managed service providers
- Banking and finance

| Industry/Customer | Key Features |
|--|---|
| Banking/Financial Services | Much of the banking industry has been using SSL as a method of encryption for a number of years. The Sun Crypto Accelerator I board improves the number of simultaneous transactions that can be performed per server, with good scalability. This is important as many financial services organizations have large server web implementations. |
| ISP, ASP, MSP | Since this market has a tendency to install large distributed server farms with lots of machines, the benefit is the reduced need for additional server capacity in order to accommodate the web session load. The accelerator board completely off-loads and speeds up the process of authentication as well as doing five times the number of simultaneous connections. |
| Internet/intranet web implementation by a brick and mortar or e-business company | Most of these companies are in need of intranet or Internet Web access for employees, as well as customers. The result is a high demand for SSL, as part of a secure connection architecture. The benefit of this card is that it increases the speed and the number of connections per server, resulting in reduced costs and better server resource utilization. |

Supported Applications

The Accelerator Card supports SSL implementations on the following applications:

- iPlanet Web Server versions 3.6, 4.0, 4.1.
- iPlanet Portal Server SP1 (Open Mode Configuration)
- Apache (using Open SSL 0.9.4)

Licensing and Usage

One or more Sun Crypto Accelerator I boards can be used per server/system. The maximum number of accelerator boards that can be configured is noted in that table above. There are no licensing issues with this product.

Conclusion

The Sun Crypto Accelerator I card offers e-commerce organizations an opportunity to add Web servers to their services for the sole purpose of creating more systems availability, rather than enhancing performance speed. Since the Sun Crypto Accelerator I card handles large systems SSL authentication loads, Web servers can take full advantage of their CPU resources to run at their optimal system performance and throughput.

The Sun Crypto Accelerator I card is a cost-effective solution that increases your e-commerce server's throughput and lowers customer wait times, as well as the number of customers your server can manage simultaneously.



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

1 (800) 786.7638
1.512.434.1511

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