

# SUN ENTERPRISE AUTHENTICATION MECHANISM™

While firewalls can fend off intruders from the outside, they cannot address security incidents that originate from within. Growing evidence indicates that most security breaches start with people inside—or known to—the enterprise. For true network security, an agile company must protect valuable data resources from unauthorized access from both inside and outside the enterprise.

## THE SOLARIS™ OPERATING ENVIRONMENT

The Solaris™ 8 Operating Environment is the established OS leader for availability, scalability, and security in the Internet age. In Solaris 8 software, Sun delivers a trustworthy, universal platform to meet the needs of .com businesses — from small startups to large Fortune 1000 enterprises.

It's no surprise that the Solaris Operating Environment is the leading UNIX® environment today. Solaris software was originally designed with the Internet in mind. TCP/IP, the central Internet protocol, has been at the core of Solaris networking for more than 15 years. Through its time-tested design — a small, stable kernel, modular and extensible components, and well-defined interfaces — Solaris software delivers rock-solid stability and predictability for business-critical applications. And the Solaris 8 Operating Environment provides complete compatibility with prior versions, so you can be confident that your current applications will continue to run.

## SUN ENTERPRISE AUTHENTICATION MECHANISM™

Sun Enterprise Authentication Mechanism™ software delivers an extra layer of security inside your firewall to protect your enterprise from unauthorized access. Powerful authentication and single sign-on capabilities enable Sun Enterprise Authentication Mechanism to provide a more secure login process, enabling you to better protect your data privacy and integrity.

Through compliance with Internet Requests for Comment (RFC) 1510 and 1964 (which define the Kerberos v5 protocols, the de facto industry standard), Sun Enterprise Authentication Mechanism software allows enterprises to seamlessly integrate secure solutions with other vendors' compliant security products.

## CENTRALIZED AUTHENTICATION AND MANAGEMENT

Sun Enterprise Authentication Mechanism software offers a single repository for enterprise authentication information — the Key Distribution Center (KDC). The KDC maintains a database of user, server, and password information through which Sun Enterprise Authentication Mechanism software can authenticate users, servers, and applications. Anyone attempting to access information may be checked against the KDC database before being ticketed as an authenticated user. Because security information is centralized, Sun Enterprise Authentication Mechanism enables you to manage and control all of your enterprise-wide logins from a single console, reducing the costs of administering and managing security.

## SECURE KEY MANAGEMENT

Sun Enterprise Authentication Mechanism software provides support for robust encryption. During the authentication process and when transmitting KDC entries over the network, all the information exchanged between the user and the KDC is encrypted for an extra level of security.

## EASE OF USE

Sun Enterprise Authentication Mechanism software provides a Java™ technology-based administrative tool for easy access and configuration. Users can load authentication information in batch mode, which is particularly useful for enterprises that lose or gain large numbers of users each year.

- Centralized authentication with robust encryption, for a more secure login process and secure key management
- A single repository for enterprise authentication information simplifies management
- A Java technology-based administrative tool delivers easy access and configuration
- Single sign-on capabilities save time and simplify access to multiple applications
- Hot standby capability speeds access to information
- Reduced contention for security verification improves performance
- Multiple realms enhance cross-organizational and cross-system operation
- Programmable security APIs permit quick adoption of new security technologies
- Built-in support for secure FTP, NFS™, telnet, and r\* commands
- Compliant with Internet RFC 1510 and RFC 1964

With its single sign-on capabilities, Sun Enterprise Authentication Mechanism can authenticate user access to multiple applications by ticketing<sup>1</sup> a user only once, at first log in. Users need not memorize multiple passwords, or enter passwords more than once during a session.

### **HOT STANDBY CAPABILITY**

Sun Enterprise Authentication Mechanism software's distributed architecture delivers data center-class predictability and availability of enterprise system resources. You can replicate your security information for faster access to information as well as duplicate copies in the event of an emergency.

Should the master KDC fail, the read-only replicated slave KDC still holds the necessary information for the authentication process to take place without interruption. And, if the master becomes unrecoverable, you can easily convert the replicated slave into a new master.

### **FASTER PERFORMANCE**

Sun Enterprise Authentication Mechanism software is faster and more reliable because its replicated KDCs reduce contention for security verification from across the enterprise. For example, replicas may be created for use by different business units or field offices. Instead of competing for a single copy, each division or office has its own copy. Access to secured applications is faster and more predictable, a must in an agile organization.

### **MULTIPLE REALMS**

A realm is the set of users or servers registered with a specific KDC—the scope of authentication for a given KDC. Separating an enterprise into multiple realms enables Sun Enterprise Authentication Mechanism to operate across organizational boundaries and among different systems. A client in one realm can be authenticated to a server in another.

Sun Enterprise Authentication Mechanism software allows enterprises to isolate individual departments from each other, decentralizing user-level control to local network administrators. In a large organization, realms enable Sun Enterprise Authentication Mechanism to be configured to allow administration at the local level.

### **ENHANCED SECURITY**

Currently, Sun Enterprise Authentication Mechanism software supports secure FTP, NFS, telnet, and r\* commands. These secure network services, combined with robust encryption support, enable your enterprise to preserve data privacy and data integrity by eliminating “snooping” around the network and tampering with data. Users can access files, resources, or services securely over the network.

### **COST-EFFECTIVE**

Sun Enterprise Authentication Mechanism software offers unlimited usage and feature-rich security mechanisms at a significantly lower cost than many third-party solutions. Central management requires fewer administrators, enabling you to lower the overall cost of securing your enterprise.

### **PROGRAMMABLE SECURITY APIS**

Sun Enterprise Authentication Mechanism software allows Independent Software Vendors to secure applications using the Remote Procedure Call API (RPCSEC\_GSS). This API is an implementation of the RPCSEC\_GSS security protocol defined in Internet RFC 2203. Future security products from Sun or third parties can be easily plugged into the interface without requiring modifications to the application, enabling you to adopt evolving security technologies quickly and easily. For example, if Sun decided to provide a new security mechanism based on a different encryption protocol, this mechanism would be easily accessible by any application using the RPCSEC\_GSS interface.

### **REQUIREMENTS**

- Solaris 8, Solaris 7, or Solaris 2.6 Operating Environment on SPARC™ or Intel Architecture platforms
- Sun Enterprise Authentication Mechanism 1.0
  - KDC: 2 Gbytes of disk space; 64 Mbytes of memory
  - Client: 32 Mbytes of memory

### **FOR MORE INFORMATION**

To learn more about Sun Enterprise Authentication Mechanism and the Solaris Operating Environment, please visit our Web site at [www.sun.com/solaris/](http://www.sun.com/solaris/).

---

1. Applications need to be modified to take advantage of single sign-on. By default, Sun Enterprise Authentication Mechanism supports single sign-on to NFS, telnet, FTP, and r\* commands.