Oracle Advanced Security Option

The Oracle Advanced Security option provides a comprehensive suite of security features to protect an enterprise's networks and to securely extend corporate networks to the Internet. The Oracle Advanced Security option (formerly Advanced Networking Option™) provides a single source of integration with network encryption and authentication solutions, single sign-on services, and security protocols. By integrating industry standards, it delivers unparalleled security to the Oracle network and beyond. Oracle Advanced Security option contributes to overall security frameworks, establishing Oracle8i as the solution for secure transactions in network and Internet environments.

The Oracle Advanced Security option provides a comprehensive suite of security features to protect an enterprise.

SOLUTIONS TO SECURITY CHALLENGES

The Oracle Advanced Security option delivers security solutions and integrates industry standards to provide unparalleled security to the Oracle network and beyond. Oracle Advanced Security option provides a single source of integration with network encryption, single sign-on services, smartcard, token and biometric user authentication. The Oracle Advanced Security option resolves major challenges to network and Internet security in the following ways:

- Ensuring the privacy of your data and communications (by integrating encryption and integrity checking)
- Authenticating users, databases and web servers (by integrating authentication support)
- Allowing remote access and extending networks to the Internet (by integrating secure remote access into the network)

ENSURING THE PRIVACY OF YOUR DATA AND YOUR COMMUNICATIONS: ENCRYPTION

Encryption techniques ensure data privacy by changing messages into an encrypted form during transmission and using data integrity measures to ensure that they have not been viewed or modified. Oracle Advanced Security option delivers proven, standard techniques to secure your data as it travels across client/server networks, three-tier computing models and the Internet.

Encrypting Data in Your Network

Oracle Advanced Security option protects data from unauthorized viewing using RSA Data Security's RC4 or the Data Encryption Standard (DES) encryption. A secret, randomly generated key for each Net8™ session safeguards all network traffic.

Tamper-Proof Data

Oracle Advanced Security option makes it virtually impossible for an intruder to modify, make additions to, or delete data without being detected. Using the MD5 message digest algorithm, Upon arrival, Net8 immediately checks packets for tampering.

Connecting Databases to Web Application Servers

For businesses to fully embrace the Internet, companies must feel secure about exposing their internal networks and databases. While web application servers support Secure Sockets Layer (SSL) to protect data privacy between the browser and the web server, Oracle Advanced Security option ensures data privacy and integrity between web servers and corporate databases with your choice of SSL or other data encryption and integrity methods. This provides an end-to-end solution for the privacy and integrity of data flowing through networks and across the Internet.

AUTHENTICATING USERS, DATABASES AND WEB SERVERS: AUTHENTICATION

Authentication — verifying the identity of a user or machine — is considered a cornerstone of computer security. Moreover, when an organization relies on the infrastructure of the Internet for communications, it is paramount to verify who is retrieving data.

Authentication Methods

Organizations achieve authentication using one of two main methods. Passwords are the most common means of proving user identities and organizations often use stronger means of authentication including tokens, smartcards, even fingerprints. Certificate-based authentication gives users and machines unique digital certificates. Certificate-based authentication uses Public Key Infrastructure (PKI) to achieve security by implementing certificates and a certificate authority and SSL to identify who is at the other end of the connection. Oracle Advanced Security option integrates both of these methods so that you achieve strong security in client/server and Internet environments.

ALLOWING REMOTE ACCESS AND EXTENDING NETWORKS TO THE INTERNET

The Internet opens doors for a business or organization to utilize its infrastructure, to do business with partners and other companies, and to communicate with those inside and outside of the organization. By the same token, however, the Internet opens doors for those inside and outside of an organization to access its valuable data. Therefore, networks must be protected from intentional and unintentional security threats.

Firewall Support

To strengthen remote access capabilities and the extension of networks to the Internet, all leading firewall vendors build in support for secure Net8 connections through firewalls. This ensures high levels of data security as information flows into and out of corporate networks via the Internet. Firewalls can provide Oracle environments with the security necessary to deploy truly distributed Internet and intranet applications.

Internet Standards for Authenticating Users and Machines

Oracle Advanced Security option provides the Oracle environment with both SSL support and RADIUS (Remote Authentication Dial-In User Service) support. This uniquely positions Oracle Advanced Security option as a critical piece of the security infrastructure. Oracle Advanced Security option offers a variety of solutions to provide data

privacy, data integrity and verification of users. The outcome is truly secure systems both within your network and expanding to an Internet environment (see Figure 1).

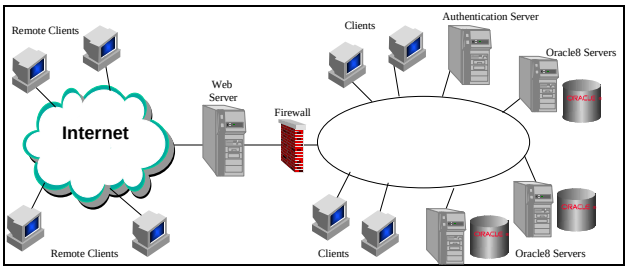

Figure 1: Today's Network Environment

SUPPORTING INDUSTRY STANDARDS

Oracle extends the network by interoperating with the protocols that many organizations have standardized upon. The Oracle Advanced Security option — like many Oracle products — supports industry standards to provide the convenience required by Oracle's customers and to protect the investments of organizations using Oracle products.

SSL SUPPORT IN ADVANCED NETWORKING OPTION

Secure Sockets Layer (SSL) is the leading security protocol for the Internet, preventing eavesdropping, message tampering or forging. SSL support in Oracle Advanced Security option expands your encryption choices and provides public key authentication based on the SSL standard. By using SSL, Oracle servers can authenticate users by utilizing standard X.509 version 3 certificates. SSL provides authentication, encryption and data integrity. Among the encryption provided by SSL is Triple DES (3DES), which increasingly is being used by organizations requiring strong security. Oracle Advanced Security option support for SSL allows you to protect systems with proven, reliable security techniques.

The complete package includes an Oracle Wallet, Oracle Wallet Manager and a certificate server. The wallet stores the X.509 certificates and authentication data. The Wallet Manager is the interface to manage the wallet. A certificate server provides the certificate; a directory server stores this information. Together they provide PKI-based security to Oracle.

Benefits of SSL Support

The benefits of SSL support in Oracle Advanced Security option are many, including:

- Industry-standard support integrated into the Oracle environment, including single sign-on with PKI
- Secure end-to-end communications
- Support for Enterprise JavaBeans™ and for thin clients

Support for SSL in Oracle Advanced Security option closes the loop for secure end-to-end communications between any client, a web server or application server, and an Oracle data server. SSL secures not only Net8 but also other protocols such as IIOP (Internet Inter-ORB Protocol). By capitalizing on Java™ support, Oracle Advanced Security option secures IIOP connections, giving Oracle the ability to work with thin clients and Enterprise JavaBeans (EJB).

The Oracle8*i* Single Enterprise User addresses the requirement that each user have only one account—rather than separate accounts for each application, database, or network service. This single enterprise user is created once for the entire enterprise, along with his/her roles, privileges and access rights. Fewer user accounts make for stronger security and reduced cost of ownership.

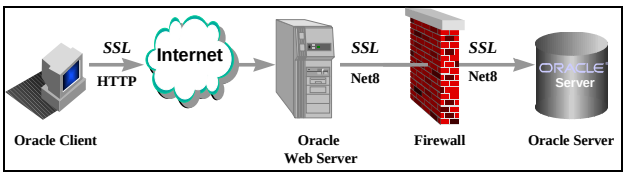

Figure 2: SSL Secures Oracle and Internet Communications

RADIUS SUPPORT IN ORACLE ADVANCED SECURITY OPTION

The RADIUS (Remote Authentication Dial-In User Service) protocol is an industry standard implemented by almost all organizations allowing users to access the network remotely. RADIUS provides user authentication, authorization and accounting between a client and an authentication server. Many enterprises have standardized on RADIUS because of its widespread acceptance in the industry, its flexibility, and its ability to centralize all user information in order to ease and reduce the cost of user administration.

Benefits of RADIUS Support

RADIUS support provides two major benefits for Oracle customers. First, it enables support for new authentication technologies including token cards, smartcards and challenge-response. Second, it readily integrates into existing systems by making the Oracle8*i* data server a RADIUS client, thus capitalizing on the infrastructure and investment that organizations have already made.

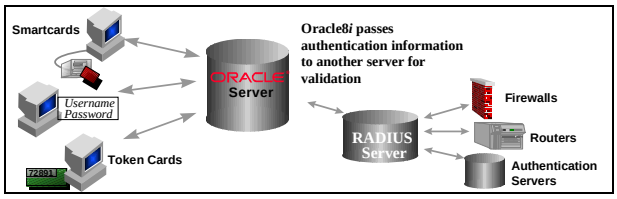

Figure 3: RADIUS Integration in a Network with Oracle, Remote Access and Strong Authentication

Opening Authentication Support

Now you can choose virtually any mechanism available to authenticate network users. Many token and smartcard manufacturers support RADIUS today; therefore any RADIUS-compliant device can authenticate Oracle users with little modification required by the authentication provider. Since many organizations have implemented RADIUS for remote access to their networks, Oracle easily integrates into existing systems and takes advantage of the investments that an organization has already made.

AUTHENTICATION SUPPORT

For maximum flexibility, the Oracle Advanced Security option supports a number of different authentication and single sign-on services.

SINGLE SIGN-ON SUPPORT

Oracle Advanced Security option minimizes maintenance of multiple passwords by supporting secure, single sign-on capabilities in a distributed environment. A user only needs to log on once a day, and can automatically connect to any other Kerberos- or SESAME-based service without having to give a user name and password again. This eliminates both the need for the user to remember and administer multiple passwords, and the time spent logging into multiple services.

Kerberos-Based Authentication

Oracle Advanced Security option supports the Kerberos network authentication protocol, which provides strong authentication and single sign-on. Use of the Kerberos protocol ensures passwords are never transmitted across the network — making password theft from the network impossible. This technology ensures that clients and servers communicate safely over an insecure network.

SMARTCARD, TOKEN AND BIOMETRIC AUTHENTICATION SERVICES

Token card, smartcard and biometric authentication offer security far stronger than conventional passwords, providing higher assurance of valid user identity.

Token Authentication

Token card technologies enhance user authentication. Oracle Advanced Security option supports Security Dynamics tokens, which strengthens security through two-factor authentication: the user must *know* the PIN and *have* the SecurID electronic token card. In addition RADIUS support in Oracle Advanced Security option allows integration with a variety of token cards. Organizations can choose which token(s) they would like to use to protect networks from unauthorized use.

Smartcard Authentication

Oracle Advanced Security option now integrates with RADIUS-compliant smartcards, which allows these smartcards to authenticate Oracle users. Smartcards are becoming popular as strong security devices. Having a processor means they can generate dynamic passwords; because they have memory, they are useful for storing data such as username, a certificate or a medical record. Smartcards are being widely deployed and organizations relying on smartcards for proof of user identities can do so when users connect to Oracle.

Biometric Authentication

Considered the ultimate technology for verifying a user's identity, biometric authentication is based on a physical characteristic (e.g., a fingerprint) of an individual. Oracle Advanced Security option supports Identix TouchNet biometric devices, which allow users to log on with a username and a fingerprint rather than a password. This technology eliminates password stealing or "borrowing." And because biometric authentication is based on the user's fingerprint, traditional problems of forgotten passwords and lost tokens are eliminated.

SEAMLESS INTEGRATION WITH DCE

Oracle Advanced Security option integrates Oracle with security, directory and transport services provided by Open Software's Foundation DCE. Oracle Advanced Security option allows complete application portability between traditional Net8 configuration and DCE. It also allows the development of new DCE applications, or the migration of existing applications to or from DCE, now or in the future. The DCE Integration facilities use the DCE Remote Procedure Call (RPC) service for secure communication and the DCE Cell Directory Services (CDS) for Oracle service naming and location transparency. DCE Integration facilities work with the DCE Security Service to provide single sign-on and centralized privilege management. For customers who implement this standards-based advanced security service, the DCE Security Service can be used with traditional network protocols.

Likewise, the DCE Directory Service can be used with any Net8 configuration.

SUMMARY: INTEROPERABILITY

Organizations are increasingly facing security challenges as they extend networks to the Internet. The Oracle Advanced Security option provides a comprehensive range of network security features that increase security and user reliability in distributed networks. Through support of industry standards such as SSL for public key infrastructure and RADIUS for integration with existing infrastructures and enhanced authentication choices, the Oracle Advanced Security option protects your investment in hardware and software. Through support of single sign-on services such as Kerberos, and enhanced user authentication devices including smartcards and biometric devices, the Oracle Advanced Security option ensures user reliability and simplifies account management. Encryption technology provided by Oracle Advanced Security option provides strong protection for all data in your network.

The Oracle Advanced Security option is a sound technology investment, as it remains on the forefront of security trends by adapting to prevailing technology standards and protocols. This allows Oracle to deliver a complete, timely secure network solution, representing a sound technology investment. By integrating with proven security solutions on the market and by providing complete security solutions, the Oracle Advanced Security option is the definitive solution for securing your network, your data, and your users.

ORACLE ADVANCED SECURITY OPTION KEY FEATURES AND ENHANCEMENTS

Network Encryption Services

Highly optimized industry-standard data encryption algorithms.

Native Encryption	SSL Encryption *
RC4_40	RC4_40
RC4_56	RC4_56
RC4_128	RC4_128
DES_40	DES_40
DES_56	DES_56
	3DES *

Minimum acceptable encryption level can be specified by both client and server. Allows higher levels of security for sensitive data servers or exposed data links. US export restrictions permit only 40-bit and limited 56-bit algorithms for general export. Longer key lengths require special permissions for use outside of the US/Canada.

Allows encrypted sessions to start in one network protocol and end in another. No decryption and re-encryption during protocol conversion.

Data Integrity Checking

Cryptographically secure data integrity of every Net8 packet to protect against data modification, transaction replay and transaction removal. Uses industry-standard algorithms:

Native Integrity	SSL Integrity *
MD5	MD5
	SHA *

Immediate, automatic termination of operations where violations are detected. Records all violations in log files.

Enhanced Authentication Integration

Support for third-party devices to replace passwords and provide strong authentication:

Biometrics—Identix TouchNet fingerprint readers

Token cards—Security Dynamics SecurID tokens

RADIUS-compliant token cards *

RADIUS-compliant smartcards *

Support for third-party authentication services:

Kerberos

CyberSafe Challenger (Kerberos-based)

Public key authentication with SSL *

SESAME

Banyan Systems' Enterprise Network Services

DCE Security Services

Public Key Infrastructure (PKI) support.

X.509 v3 Digital Certificates *

Single Sign-On

Integration with products and protocols that allow users to access selected databases in the environment without having to provide a username and password multiple times. Integrates with single sign-on services:

PKI with X.509v3 Certificates *

Kerberos

CyberSafe Challenger

SESAME

Bull ISM

DCE Security Service

DCE Integration

Transparent use of DCE RPC, directory and security services. Integrates existing applications into DCE without modification. Connects heterogeneous platforms. Flexible integration options:

Full integration

Directory service integration only

Security service integration only

Provides Oracle® Call Interface and ODBC interface

Secure Communication Over DCE RPC.

Supports two-tier, client/server architectures. All DCE packet protection options supported, from no protection to full encryption with DES.

Third Party Support

Interoperable with any third party tool that uses Net8. Works with all major protocols supported by Net8. Fully supported by Oracle Transparent Gateway® and Oracle Procedural Gateway®, allowing fully encrypted, client/server sessions to non-Oracle data sources.

Hardware and Software Requirements

The Oracle Advanced Security option runs on most major hardware and operating system platforms supported by Oracle worldwide. Not every service is implemented on every platform. Check with your Oracle representative for detailed availability information.

The Oracle Advanced Security option is available worldwide. Network encryption features are subject to import and export regulations. A special domestic version is available for use in U.S./Canada.

*** = New in Oracle8*i***

ORACLE ADVANCED SECURITY OPTION PARTNERS

ENCRYPTION SERVICES

RSA Data Security, Inc.

Network encryption services use the RC4 and MD5 algorithms developed by RSA Data Security.

TOKEN, SMARTCARD AND BIOMETRIC AUTHENTICATION

Security Dynamics Technologies, Inc.
ACE/Server and SecurID Token Cards

SecurID credit card-size tokens generate random numbers at set intervals that replace passwords. The one-time use passcode generated by the SecurID card and the user's PIN are compared with information in the ACE/Server to provide strong two-factor user authentication.

Identix, Inc.
TouchNet

The Identix TouchNet is a serial-based fingerprint verification device which uses fingerprints to replace passwords. User identities are assured by the touch of a finger at a desktop terminal.

SINGLE SIGN-ON INTEGRATION

CyberSafe Corporation
TrustBroker Security Suite

CyberSafe's TrustBroker Security Suite provides secure authentication to Oracle Advanced Security option. This combination delivers a single sign-on solution to heterogeneous Oracle environments.

Bull Worldwide Information Systems OpenMaster

AccessMaster, as part of Bull's OpenMaster software suite, provides enhanced security services to Net8. Includes centralized user management, authentication and identification when connecting to distributed databases and no change in application code.

Banyan Systems, Inc.
Enterprise Network Services

Banyan Systems' Enterprise Network Services authenticates all users on a network.

DCE INTEGRATION

Gradient Technologies, Inc.
PC-DCE

Gradient's PC-DCE brings the Distributed Computing Environment (DCE) to desktop platforms including Microsoft Windows. It provides single sign-on, centralized privilege management and interoperability across heterogeneous systems.

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
+1.650.506.7000
Fax +1.650.506.7200
http://www.oracle.com/