



An Oracle White Paper
October, 2011

SHA-256 Support Planning Information for Dept of Defense

Derick Cassidy, CISSP-ISSAP | Master Principal Solution Specialist – Security
Lou Ann Hunt, Oracle Public Sector Security Specialist, Dept of Defense

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Foreword	3
Background	3
Security at Oracle	4
SHA-256 Support across Oracle Technologies.....	6
Infrastructure Tier	6
Oracle Solaris	6
Oracle Enterprise Linux	6
Data Tier:.....	6
Why upgrade to 11g?	7
Best Practices - Oracle Advanced Security Option	7
Best Practices: Enterprise User Security	8
Middleware Tier	9
Oracle Enterprise User Security	9
Oracle Internet Directory.....	9
Oracle Directory Server Enterprise Edition	9
Oracle WebLogic Server.....	10
Oracle Glassfish	10
Oracle iPlanet Web Server	10
Oracle Platform Security Services	11
Available Resources	12
Summary	12
Appendix A: SHA 256 Support Notes for Oracle Products	13
Appendix B: Oracle Lifetime Support Policy	14

Foreword

The purpose of this whitepaper is to provide the Department of Defense with information to assist in evaluation and planning for its announced transition to SHA-256. Although, security is fundamental to all Oracle technologies this paper will focus only on information related to the major Oracle software products, versions and platforms in use across DOD. Further, support of other SHA-2 key hash lengths, which are not part of DOD's current plans, are also considered outside the scope of this paper. Software not included or support across the full SHA-2 standard which are outside of this scope can be provided upon request.

Where a current product supports SHA-256 natively, it is identified. Where there are mitigating controls or configuration options for a current product, these are also identified.

Background

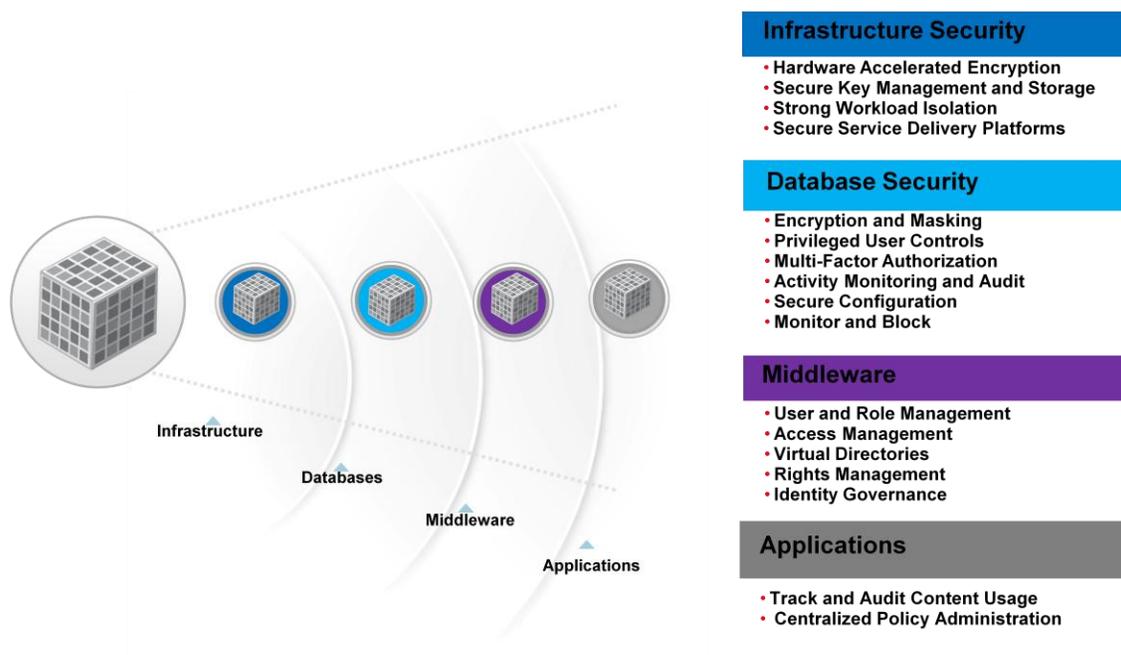
In June 2010, the National Institute of Standards and Technology (NIST) released draft Special Publication (SP) 800-131, "*A Recommendation for Transitioning of Cryptographic Algorithms and Key Sizes*" which provides specific guidance for transitioning to stronger cryptographic keys and more robust algorithms by December 31, 2013. These security algorithms impact software and hardware products that leverage encryption, digital signing, key agreement, key derivation, key wrapping, key transport, hash functions, and message authentication codes.

NIST SP 800-57, *Recommendation for Key Management – Part 1*, requires the use of SHA-256 in all digital signatures generated, beginning on January 1, 2011. This is reiterated in NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*, which provides the requirements for the digital credentials associated with the PIV card. In compliance with the NIST requirement, the Federal PKI Certificate Policies require that all member Certification Authorities (CA) use SHA-256 when signing new certificates and revocation information issued on or after January 1, 2011.

On October 14, 2010, the DoD CIO released a memo, *DoD's Migration to Use of Stronger Cryptographic Algorithms*, directing all Combatant Command, Service and Agency (CC/S/A) CIOs to begin evaluation of their system portfolios in anticipation of the federal mandate to transition to using the SHA-256 hashing algorithm. The memo directed each organization to identify a point of contact (POC) who will provide liaison, facilitate information sharing and represent their Component to the DoD CIO.

Security at Oracle

Oracle is committed to providing a world-class security model. This includes, but certainly not limited to, ensuring cryptographic advances are incorporated across all of our application and technology products. Oracle's Security strategy looks at security across the four main technology tiers: Infrastructure, Database, Middleware, and Applications. This approach allows Oracle to analyze and review new methods of securing the DoD enterprise. A sampling of the security solutions Oracle provides within this scope can be seen below.



While many of these security topics are outside of the scope of this paper, the adoption and transition to SHA-256 provides a framework for evaluating the DoD's overall security framework. In evaluating the transition to SHA-256, the opportunity to gain security advances in these other related areas should be considered.

Infrastructure Tier: Transitioning to Oracle Solaris 10 to gain SHA-2 compliance would yield multiple security benefits to DoD users. These include the ability to monitor file integrity, the ability to verify user and process rights, and retain a detailed audit trail of all system events. Oracle Solaris 10's networking configuration design and cryptographic capabilities also significantly reduce the system's risk exposure.

Database Tier: Defense-in-depth data security means looking at data security holistically. To do that, one needs to look at the entire life cycle of the data, where the data resides, what applications access the data, who is accessing the data and under what conditions, and ensuring that the systems have been properly configured. In some instances, centralizing key management for future efficiencies could be

as simple as checking a configuration box. The Database Tier has multiple controls for data in motion, data at rest, and for strong authentication (2nd factor) to the database by end users and by middleware tools.

Data protection can be achieved with the use of Transparent Data Encryption (TDE) for symmetric encryption that is native to the database. Data in motion can be protected with the use of certificate based, mutually authenticated, and cryptographically secure sessions – also using native features of the database that are available in the Oracle Advanced Security option.

Middleware Tier: DoD continues to push information silos to expose and share and as such middleware security requirements will continue to grow. Oracle Identity and Access Management solutions address the protection of these enterprise resources and the management of the processes acting on those resources. A sampling of DoD requirements met with these solutions include CAC Authentication (aka CAC enabled access control), Attribute Based Authorization (ABAC), Role Based Authorization (RBAC), Automated Account provisioning and Identity Federation with other Federal Agency partners.

At the core of any Identity discussion, passwords, and crypto associated with password hashing, should reasonably be part of any SHA-256 discussion. Although password hashing is not strictly within scope of the DoD mandates covered in this paper, given the broad use of Oracle directory solutions a brief discussion of SHA-256 in this context will be included.

It is important to note, that while we discuss the use of SHA-256 within the context of the DoD issuing authority, the advertised move of the Federal Bridge to SHA-2 is outside the scope of this document. It is outside the scope, as this document discusses the support for SHA-256 certificates – regardless of issuing authority. Support for SHA-256 certificates within the different stacks means support for all US Government PKI issuers.

Application Tier: By relying on the other Tiers cryptographic capabilities, Oracle Applications benefit as the other areas are strengthened. Security within this Tier is often focused on Governance, Risk, and Compliance monitoring and auditing improvements, and as such will not be specifically addressed here.

Additional information across on Oracle Security solutions can be found at <http://oracle.com/security>.

SHA-256 Support across Oracle Technologies

Infrastructure Tier

Oracle Solaris

SHA-256 has been supported since 2005 in Solaris 10 thru the Solaris Cryptographic Framework. To enable SHA-256, DoD users must insure that the Solaris kernel is compiled with the pkcs11_engine.

NOTE: Administrators can verify this engine is correctly compiled by entering the "digest -l" at command line and confirm that the patch levels reflect OpenSolaris's libcrypto.so.0.9.8.

More details can be found in these online technical resources:

- <http://opensolaris.org/jive/thread.jspa?messageID=328450>
- <http://docs.sun.com/app/docs/doc/817-0547/getkw?a=view>

Oracle Enterprise Linux

SHA-256 has been supported in Oracle Enterprise Linux (OEL) since version 4.7 (Released 2008). More details can be found in the release notes: <http://oss.oracle.com/el4/docs/RELEASE-NOTES-U7-en.html>

Data Tier:

Although certificate support is the initial target for the DoD community, it is important to note that cryptographic primitives can be found in many areas of the Oracle Database. Some of these primitives include:

- Certificates for SSL/TLS encryption
- Oracle native network encryption
- Transparent Data Encryption (protection for data-at-rest)
- Database cryptographic toolkit (DBMS_CRYPT package)

Oracle has either current or planned support for SHA-256 across this complete scope. Immediate support for SHA-256 signed certificates used in SSL/TLS connections to the database is included as part of a Oracle Database 11gR2 patch set.

As the DoD community evaluates and plans for moving to SHA-256 based certificates, the key element to consider in the data tier is the database version in use. Oracle Database 11gR2 is required

for SHA-256 support. Earlier versions that are known to be in use across the DoD enterprise will require upgrade.

NOTE: Users can confirm if using certificates at the Data Tier: Check the sqlnet.ora file on the database for
SSL_CLIENT_AUTHENTICATION=TRUE

Alternately, Oracle Net Manager can be used to review Oracle Advanced Security settings.

Why upgrade to 11g?

In addition to being a requirement for SHA-256, all DoD users are strongly encouraged to upgrade from earlier Oracle Database versions to insure ongoing support is available. Of note, Premier support for Oracle 10gR2 ended July 2010. For most DOD, an extended support date applied as documented in the support supplemental statement found at <http://www.oracle.com/us/support/library/057419.pdf>

Extended and Sustaining support will continue to be available per Oracle's Support policy however additional cost and/or support limits could apply. For more details see Appendix B or refer to Oracle's lifetime support policy which can be found at: <http://www.oracle.com/us/support/lifetime-support/index.html>

Of course, upgrading to the latest version of Oracle Database will also provide DoD users with significant functional benefit. Oracle Database 11g Release 2 provides the foundation to successfully deliver more information with higher quality of service, reduce the risk of change within IT, and make more efficient use of IT budgets. By deploying Oracle Database 11g Release 2 as their data management foundation, DoD can utilize the full power of the world's leading database to:

- Reduce server costs by a factor of 5
- Reduce storage requirements by a factor of 12
- Improve mission critical systems performance by a factor of 10
- Increase DBA productivity by a factor of 2
- Eliminate idle redundancy in the data center
- Simplify their overall IT software portfolio

Best Practices - Oracle Advanced Security Option

Oracle Advanced Security is a security option for Oracle Database Enterprise Edition. Oracle Advanced Security provides encryption of sensitive information in database storage, encryption of network connections to/from the database, and strong authentication of database users. These advanced security capabilities provide protection between entities and between machines within the infrastructure to help DoD address privacy and compliance requirements:

- Transparent Data Encryption

- Network encryption
- Strong authentication

Transparent Data Encryption provides easy and effective protection of stored data by transparently encrypting data (using AES with up to 256 bits, or 3DES168) at the tablespace level or at the column level.

When information travels to and from the Database, Oracle Advanced Security provides a high level of security by offering support for the following encryption standards:

- AES (256, 192, and 128 bits)
- 3DES (112 and 168 bits, 2 and 3 keys)
- RC4 (256 and 128 bits)

Oracle Advanced Security supports both industry standard Secure Sockets Layer (SSL) encryption for DoD users who want to leverage their X509 Public Key Infrastructure (PKI) certificates and a light-weight Oracle native network encryption capability. Support for SHA-256 signed certificates that are used to protect database connections with SSL/TLS is included as part of a generally available patch set that is installed on Oracle Database 11gR2 (11.2.0.3).

Oracle Advanced Security also optionally protects the integrity of information, making sure the message has not been modified since it left the source by adding an encrypted digest to the message.

Two-factor (or "strong") authentication is based on something the user has (a smart card (CAC card), token, etc.) and something the user knows (a PIN or passcode). Oracle Advanced Security supports the following industry-standard authentication methods:

- Kerberos
- RADIUS (Remote Authentication Dial-In User Service)
- PKI certificate based authentication (including the use of SHA-2 digital certificates).

Best Practices: Enterprise User Security

To meet SHA-256 requirements, users may also want to consider simplifying user management and externalizing authentication thru use of Enterprise User Security (EUS), a feature of Oracle Database Enterprise Edition. Additional information on this configuration can be found in the Middleware Tier section of this paper.

Middleware Tier

Oracle Enterprise User Security

Enterprise User Security, a critical component of Oracle Identity Management, lets you create and administer large numbers of users in a secure, LDAP-compliant directory service. Although technically a feature of the Oracle Database (Enterprise Edition) Enterprise User Security (EUS) is included here, as the password for the account is stored in a the Middleware Tier – ie: Oracle Internet Directory or Oracle Directory Server Enterprise Edition.

EUS is compatible with a SHA-256 password stored within a supported LDAP directory.

Oracle Internet Directory

Oracle Internet Directory (OID) is an LDAP v3 compliant directory with meta-directory capabilities. It is built on the Oracle database and is fully integrated into Oracle Fusion Middleware and Oracle Applications.

Oracle Internet Directory fully supports SHA-256 (salted and unsalted) to support hashing of the user password attribute for comparison within OID. Details can be found at this link:

http://download.oracle.com/docs/cd/E17904_01/oid.1111/e10029/pwdstore.htm#g1049881

With the user password attribute being hashed using SHA-256, although not specifically covered under the DoD Memo to move to SHA-256 for certificates, we felt that it is important to point out Oracle's support of SHA-256. Using OID as a user repository and centralizing user management features – such as using Enterprise User Security – we feel that the *intent* of the Memo is addressed, and these features can be used as a mitigating factor when determining if a product that does not support SHA-256 cannot be immediately upgraded.

Oracle Directory Server Enterprise Edition

As part of Oracle Directory Services Plus, Oracle Directory Server Enterprise Edition (formerly Sun Directory Server Enterprise Edition) is the a high-performance directory server that provides a core LDAPv3 directory service with embedded database, directory proxy, synchronization with Microsoft Active Directory, and a Web console to manage your software all in one package.

Starting with 11gR1 PS2 (ODSEE 11.1.1.5), Oracle Directory Services Enterprise Edition support SHA-256 for LDAP SSL based authentication, as well as password hashing.

Oracle WebLogic Server

Starting from 11gR1 PS2(WLS 10.3.3), the Oracle WebLogic Server supports SHA-256 certificate for SSL sessions when JSSE-based SSL provider is configured for WebLogic Server. Please, note that JSSE-based SSL is not enabled by default.

Details on how to configure JSSE-based SSL can be found at http://download.oracle.com/docs/cd/E21764_01/web.1111/e13707/ssl.htm#BABEFCA.

Prior to 11gR1 PS2(WLS 10.3.3), although Oracle WebLogic Server itself does not support SHA-256, Oracle HTTP Server can be used to terminate SSL sessions and validate SHA-256-based certificates. In this scenario, validated certificates are subsequently passed to WebLogic Server, which uses them, via the X.509 Identity Asserter, to establish the user's identity..

This allows WebLogic to leverage SHA-256 certificates, without itself being specifically certified with SHA-256. This allows DoD to meet the mandate of the memo, using other Oracle technology to mitigate the WebLogic limitation.

Details can be found at: http://download.oracle.com/docs/cd/E13222_01/wls/docs81/ConsoleHelp/security_ldapx509identityasserter_general.html

It should be noted that the support for SHA-256 within the Middleware platform is a function of the base JDK. Any software running on WebLogic that leverages the native cryptographic functions of the base JDK will inherit support for SHA-256 natively.

Oracle Glassfish

Built using the GlassFish Server Open Source Edition, Oracle GlassFish Server delivers a flexible, lightweight and extensible Java EE 6 platform. It provides a small footprint, fully featured Java EE application. It is considered to be the reference implemented for the Java EE platform.

Oracle Glassfish leverages the Network Security Services (NSS) libraries to support cross-platform development of security-enabled client and server applications.

NSS 3.11 and later have support for SHA-256. Therefore, Oracle Glassfish is fully certified and supported with SHA-256 certificates.

Details: <http://www.mozilla.org/projects/security/pki/nss/nss-3.11/nss-3.11-algorithms.html>

Oracle iPlanet Web Server

The former Sun Java System Web Server is the leading Web server in the world's largest companies, delivering a single, secure infrastructure for all Web technologies and applications.

Oracle iPlanet Web Server leverages the Network Security Services (NSS) libraries to support cross-platform development of security-enabled client and server applications.

NSS 3.11 and later have support for SHA-256. Therefore, Oracle iPlanet Web Server is fully certified and supported with SHA-256 certificates.

Details: <http://www.mozilla.org/projects/security/pki/nss/nss-3.11/nss-3.11-algorithms.html>

Oracle Platform Security Services

Oracle Platform Security Services (OPSS) provides enterprise product development teams, systems integrators (SIs), and independent software vendors (ISVs) with a standards-based, portable, integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications..

OPSS is the underlying security platform that provides security to Oracle Fusion Middleware including products like WebLogic Server, SOA, WebCenter, ADF, OES to name a few. OPSS is designed from the ground up to be portable to third-party application servers. As a result, developers can use OPSS as the single security framework for both Oracle and third-party environments, thus decreasing application development, administration, and maintenance costs.

OPSS and the associated Oracle Security Developer Toolkit (OSDT) both support SHA-256.

Available Resources

Oracle has a number of training and consulting resources available to help DoD with this SHA-256 transition.

Informational Sessions, Hands-On Workshops, and on-demand webcasts are available across a large variety of topics. For a listing of the currently available sessions please refer to <http://oracle.com/events>.

Alternately, Oracle's Public Sector Account Managers can provide additional assistance and site specific guidance. Oracle Point of Contact information has been provided to the DISA PKI office to help connect DOD users to resources as needed.

Summary

This whitepaper was a direct result of the DoD CIO's Oct 14, 2010 memo *DoD's Migration to Use of Stronger Cryptographic Algorithms*, directing all Combatant Command, Service and Agency (CC/S/A) CIOs to begin evaluation of their system portfolios in anticipation of the federal mandate to transition to using the SHA-256 hashing algorithm.

Oracle is committed to supporting both the US Federal government as a whole, and DoD specifically with respect to SHA-256. The purpose of this whitepaper was to provide related information across the major Oracle software versions and platforms in use by DoD to assist in evaluation and planning for this SHA-256 transition. The body of this paper and the associated appendix outline various Infrastructure, Data, and Middleware software packages, their support for the SHA-256 standard, and our continued commitment to make world-class, standards based software and systems.

Given the complexity of this DoD's task, direct discussion with Oracle's Account Teams is encouraged to both insure mission continuity during the CAC Crypto upgrade and determining if concurrent improvements in the overall security architecture are possible.

Appendix A

SHA 256 Support Notes for Oracle Products				
Oracle Product	Version	SHA-256 Support	Mitigating Configuration	Notes
Solaris	10	Yes		Kernel must be compiled with pkcs11_engine enabled
Oracle Linux	5.x	Yes		
Oracle Database	11gR2	Yes	Leverage Advanced Security Option or possible use of Enterprise User Security Configuration	Oracle Database 10g and below will not support SHA-256. Customers must upgrade to 11gR2 or higher to achieve support for SHA-256 Patch Requirements: 11.2.0.3 patch set
Oracle Internet Directory (OID)	11g	Yes		SHA-256 for storing password hashes.
Oracle/Sun Directory Server EE	11g	Yes		Patch Requirement: 11.1.1.5 Patch set
WebLogic Server	11g (10.3.4, 10.3.5)	*Yes		Web Services are supported by leveraging the Sun JSSE provider. With regards to SSL, there is a distinction between the use of SHA-2 in certificate signing algorithms and the use of SHA-2-based cipher suites. The former is enabled through the use of the Sun JSSE provider. The latter may be possible through the use of the RSA SSLJ JSSE provider - testing and qualification of that provider is in process. Use of SHA-2 in web services is supported. * For certificate signing algorithms the Sun JSSE provider can be leveraged. For SHA-2 cipher suites, the RSA SSLJ JSSE provider is in testing and qualification.
Glassfish	2.1.1 3.2	Yes		
iPlanet Web Server	7	Yes		
Oracle HTTP Server		Yes	Can leverage iPlanet Web Server where supported	Oracle HTTP Server has the ability to terminate an SSL session with a certificate that contains a SHA-256 certificate.

Appendix B: Oracle Lifetime Support Policy

With Oracle Support, you know up front and with certainty how long your Oracle products are supported. The Lifetime Support Policy provides access to technical experts for as long as you license your Oracle products and consists of three support stages: Premier Support, Extended Support, and Sustaining Support. It delivers maximum value by providing you with rights to major product releases so you can take full advantage of technology and product enhancements. Your technology and your business keep moving forward together.

Premier Support provides a standard five-year support policy for Oracle Fusion Middleware products. You can extend support for an additional three years with Extended Support for specific releases or receive indefinite technical support with Sustaining Support.

Please reference all lifetime support information and product specific timelines at <http://www.oracle.com/us/support/lifetime-support/index.html>

Premier Support

As an Oracle customer, you can expect the best with Premier Support, our award-winning, next-generation support program. Premier Support provides you with maintenance and support for Oracle Fusion Middleware products for five years from their general availability date. You benefit from

- Major product and technology releases
- Technical support
- Access to My Oracle Support
- Updates, fixes, security alerts, data fixes, and critical patch updates
- Tax, legal, and regulatory updates
- Upgrade scripts
- Certification with most new third-party products/versions
- Certification with most new Oracle products

Extended Support

Your technology future is assured with Oracle's Extended Support. Extended Support lets you stay competitive, with the freedom to upgrade on your timetable. If you take advantage of Extended Support, it provides you with an extra three years of support for specific Oracle releases for an additional fee. You benefit from

- Major product and technology releases

- Technical support • Access to My Oracle Support
- Updates, fixes, security alerts, data fixes, and critical patch updates
- Tax, legal, and regulatory updates
- Upgrade scripts
- Certification with most existing third-party products/versions
- Certification with most existing Oracle products Extended Support may not include certification with some new third-party products/versions.

Sustaining Support

Sustaining Support puts you in control of your upgrade strategy. When Premier Support expires, if you choose not to purchase Extended Support, or when Extended Support expires, Sustaining Support will be available for as long as you license your Oracle products. With Sustaining Support, you receive technical support, including access to our online support tools, knowledgebases, and technical support experts. You benefit from

- Major product and technology releases
- Technical support
- Access to My Oracle Support
- Fixes, updates, and critical patch updates created during the Premier Support stage
- Upgrade scripts created during the Premier Support stage

Sustaining Support does not include

- New updates, fixes, security alerts, data fixes, and critical patch updates
- New tax, legal, and regulatory updates
- New upgrade scripts
- Certification with new third-party products/versions
- Certification with new Oracle products



SHA-256, Planning Information for
Dept of Defense
August 2011

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

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2011, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0611

Hardware and Software, Engineered to Work Together