

ORACLE CROSS-DOMAIN SECURITY EXPRESS



KEY FEATURES AND BENEFITS

"THE INDUSTRY'S FIRST DCID 6/3 PROTECTION LEVEL 4 CERTIFIED AND ACCREDITED SOLUTION OF ITS KIND."

FEATURES

- Web-based Mandatory Access Controls (MAC) Configuration Manager
- Web-based MAC Reporting
- Published Procedural Language/Structured Query Language (PL/SQL) Application Programming Interfaces (APIs) for use by applications
- Auditing and Alerting
- Configuration support for security domains and factors
- Rules engine for managing database access
- Realms for protecting database schemas and roles and implementing fine-grain system privilege management
- Separation of Duties

BENEFITS

- Enabling technology used for US Government system Accredited DCID 6/3 for Protection Level 4 (PL4) Confidentiality
- Extensible to meet DIACAP and SABI cross-domain
- Accelerates implementation of a secure Information Sharing database
- Supports highly configurable systems for broad application use case implementation
- Offers implementation support from skilled Oracle security architects and system implementers

The Oracle Cross-Domain Security Solution (CDSS), with Cross-Domain Security Express (CDSE) as its implementing framework enables customers to achieve DCID 6/3 PL4 certified and accredited systems in a highly extensible, scalable, and cost effective fashion. CDSE is highly configurable, supports and integrates with a broad range of applications where there is a need to efficiently and precisely restrict data access across domains, and is supported by Oracle's top security engineers and architects.

The Cross-Domain Problem

The Intelligence Reform and Terrorism Prevention Act, passed by Congress in 2004, established the expectation that the "vast intelligence enterprise" of the United States would become more unified, coordinated, and effective. This law charged the intelligence community and government agencies to integrate foreign intelligence and domestic US intelligence components to reduce gaps in understanding threats to our national security and to improve our reaction. This intelligence strategy — designed to provide more comprehensive and accurate intelligence analysis— substantially increases requirements for secure data sharing capabilities.

An information system must be Certified & Accredited (C&A) by the appropriate Accreditation Authority in accordance with each Authority's prescribed compliance requirements and governance. Cross-Domain Solutions (CDSs) can provide the ability to share data between multiple operating domains (e.g. among users on Top Secret and Secret networks). However, sharing sensitive data across security domains and networks has been impeded by both technical and cultural challenges. A viable CDS requires a tremendous investment for initial C&A and many solutions are limited with respect to the integration of an organization's applications. As a result, most of today's highly secured systems have been designed to restrict access to entire user populations rather than implement data sharing on the basis of mandatory access controls and an individual's need-to-know. Most CDSs today are based on one-way replication through data transfer guards that copy data from one network to another. This model inherently builds in additional and extensive Operations and Maintenance (O&M) costs. These solutions have a number of operational limitations, including:

- An inability to integrate with or scale to the broader Enterprise
- Transient data sets that reduce the ability to find data relationships that lead to actionable intelligence
- Latency and synchronization issues that decrease the integrity of the data available, thus decreasing its value to decision makers

- Duplicative hosting of applications and databases

It is no longer necessary to allow modern information systems to be isolated on distinct networks or “air-gapped” such that they are not available to users who need access. We can and should build systems using the innovative technologies available today to support the collaborative intelligence needed to succeed against our enemies.

Cross-Domain Security Express –The Cross-Domain Solution

Oracle’s National Security Group challenged its top engineers and security architects to engineer the first Cross-Domain Oracle database providing a practical and robust solution to the Cross-Domain security problem. The result is the Oracle Cross-Domain Security Solution (CDSS), with Cross-Domain Security Express (CDSE) as its implementing framework. CDSE is an Oracle Cross-Domain implementation support package, consisting of software that extends key Oracle products that enable the patented CDSS architecture and a comprehensive implementation methodology including Installation and Configuration, Concept of Operation’s (CONOPS), Design, Privileged User’s Guide, and Test Plan documentation. CDSE is designed to assist information systems developers achieve DCID 6/3 Protection Level 4 (PL4) or DoD SABI C&A for SECRET-to-UNCLASSIFIED systems as well. CDSE’s architecture and methodology leverages the capabilities of Oracle Database Vault, Label Security, Advanced Security options and other key Oracle technologies to structure a multi-factored and multi-layered approach to database security.

CDSE Enables DCID 6/3 PL4 Certified and Accredited Systems

The US Government performed extensive C&A testing to certify and accredit a CDSE-enabled US Government system in compliance with the Director of Central Intelligence Directive (DCID) 6/3 PL4. Indeed Oracle engineers combined CDSE and requisite Oracle Database security products to create a Cross-Domain Database instance which serves as the first data management platform of its kind that is accredited by the Defense Intelligence Agency. CDSE extends the capabilities of Oracle products and other implementation techniques to provide the following key functions within Oracle’s Cross-Domain Security Architecture:

- **Mandatory and Discretionary Access Controls** – CDSE extends Oracle’s Database Vault to add significant capabilities for managing user accesses to data including: network-level access controls integrated with trusted operating systems for cross-domain security, and separation of duties for security and maintenance operations. Authorized network users are only allowed to access data labeled appropriately for the network (at its level or below), with further restrictions on the user’s clearance.
- **Data-Specific Labeling** – CDSE provides unique services for the isolation and labeling of specific data for release to the enterprise. This service can be integrated with mission applications and human-review processes to ensure accurate data labels for broader dissemination. Oracle Label Security enforces label-based access control to limit access to data by a disparately cleared user base.

- **Identity Management Integration** – The Cross-Domain Database is capable of mediating data requests from multiple domains simultaneously. Public Key Infrastructure (PKI) and enterprise directory stores can be leveraged to minimize the O&M requirements for user management.
- **Auditing** – CDSE provides holistic system audit capability that captures events from the devices and applications running within the system enclaves. These records can be stored locally or shipped to an enterprise audit repository as needed.

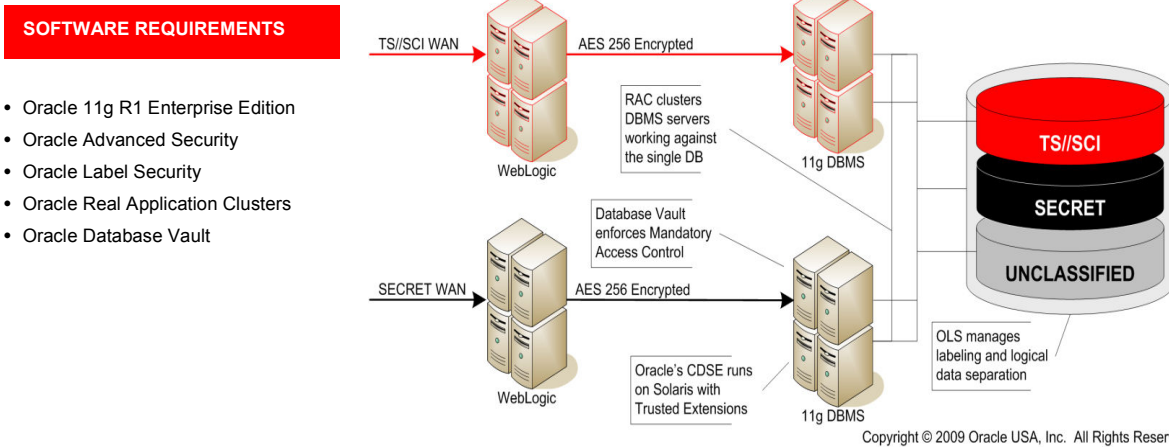


Figure 1. Conceptual Architecture for Cross-Domain Security

Oracle CDSE supports development of systems that meet both data security and data sharing requirements for even the most sensitive data. The data is written once and shared among users across networks as dictated by stringent, but sophisticated, security rules. Users on the highest domain can access data across all domains, without having to log into multiple networks.

Oracle CDSE is an Oracle National Security Group (NSG) offering. CDSE is International Traffic in Arms (ITAR) controlled. Oracle offers this capability to the U.S. Government (or under State Department license to identified countries).

Contact Us

For more information about Oracle Cross-Domain Security Express please contact NSG at 703.364.2213 or e-mail NSG_SOLUTIONS_US@oracle.com.

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

Copyright © 2009, 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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. 1009