Oracle PROTECT: Solutions for Homeland Security

Solution Architecture

An Oracle Technical White Paper
June 2005

Oracle PROTECT: Solutions for Homeland Security
Solution Architecture

Oracle PROTECT: Solutions for Homeland Security Solution Architecture

INTRODUCTION

A set of solutions based upon Oracle's core technology, applications, professional services, and partner solutions, Oracle PROTECT: Solutions for Homeland Security assists in preventing, preparing for, and responding to crimes and terrorist attacks on the homeland by providing a flexible and adaptable architecture upon which a decentralized network can be built. Moreover, PROTECT fully integrates disparate systems, leverages resources, and shares data in an efficient, seamless, and interoperable manner.

The goal of the PROTECT program is to provide the capabilities for a fully integrated system in which public and private entities across the United States can share information in a trusted and secure manner to reduce the incidence and fear of crime and terrorism, prepare for a response to critical incidents, and improve the overall safety and security of our homes and communities.

PROTECT fully integrates disparate systems, leverages resources, and shares data in an efficient, seamless, and interoperable manner.

Additionally, Oracle PROTECT: Solutions for Homeland Security exploit trusted information sharing to:

- Promote actionable intelligence sharing;
- Defend our global interests, economy and commerce;
- Safeguard our health, food and water;
- Secure our data, key assets and infrastructures; and
- Maintain continuity of operations of our business enterprises.

The foundation for Oracle PROTECT is Oracle's technology and applications products, which include: Oracle Database 10g, Oracle Fusion Middleware (consisting of the family of products in Oracle Application Server 10g, Oracle Developer Suite, Business Process Management and Activity Monitoring, Oracle Data Hubs and Oracle Collaboration Suite), and Oracle E-Business Suite.

ORACLE PROTECT SOLUTION ARCHITECTURE BENEFITS

Robust Security for Sensitive Information

Oracle's goal is to provide a robust, flexible, secure, and cost effective architecture that addresses the needs of solutions for the defense, intelligence, and homeland security communities. Given that these solutions all deal with sensitive information, the security requirements for this architecture are more stringent than for most commercial systems. A layered security model best addresses these requirements because a layered model has no single point of security failure.

Further, many organizations have the need to not only safeguard sensitive data, but also share this very sensitive data with internal users and partners. Oracle refers to this dual functionality as "Trusted Information Sharing." Trusted Information Sharing is a particular strength of the PROTECT solutions.

Elimination of Information Islands

The flow of this information can be instantly altered and modified as the needs of the systems change because the business rules governing them are maintained as easily accessible metadata, rather than buried inside complex programs.

The PROTECT architecture allows information to be exchanged with any other system within or outside the enterprise, with users within and beyond the enterprise and with sensors and devices of all types. Events can be analyzed and can generate alerts to users (whether they are at their desks or in the field). Or events can initiate complex interactions between a variety of systems, users, or devices. The flow of this information can be instantly altered and modified as the needs of the systems change because the business rules governing them are maintained as easily accessible metadata, rather than buried inside complex programs.

Responsive Software Infrastructure

Oracle's PROTECT architecture provides the ability to:

1. Develop enterprise applications at lower cost;
2. Enable streamlined business processes that can be quickly optimized in response to events; and
3. Make employees more productive by providing them with an efficient workplace to access information and to do work.

Oracle has a strategic commitment to standards adoption across the technology stack. Thus, PROTECT solutions are built according to Service Oriented Architecture (SOA) principles. The PROTECT solutions utilize open standards interfaces throughout the technology stack. This ensures that these solutions can easily integrate with other solutions, existing or future.

Lower Total Cost of Ownership

PROTECT solutions leverage a pre-integrated technology stack, based on Oracle Fusion Middleware and the Oracle Database 10g, that employs low cost GRID computing to provide a lower cost platform with greater scalability, availability and less complexity. By consolidating to a common platform based on modular units of computing power that can be easily reconfigured, updated and repaired, an organization can significantly reduce operational costs and complexity while greatly increasing capacity.

PROTECT SOLUTION ARCHITECTURE LAYERS

The PROTECT solutions have the following architectural layers:

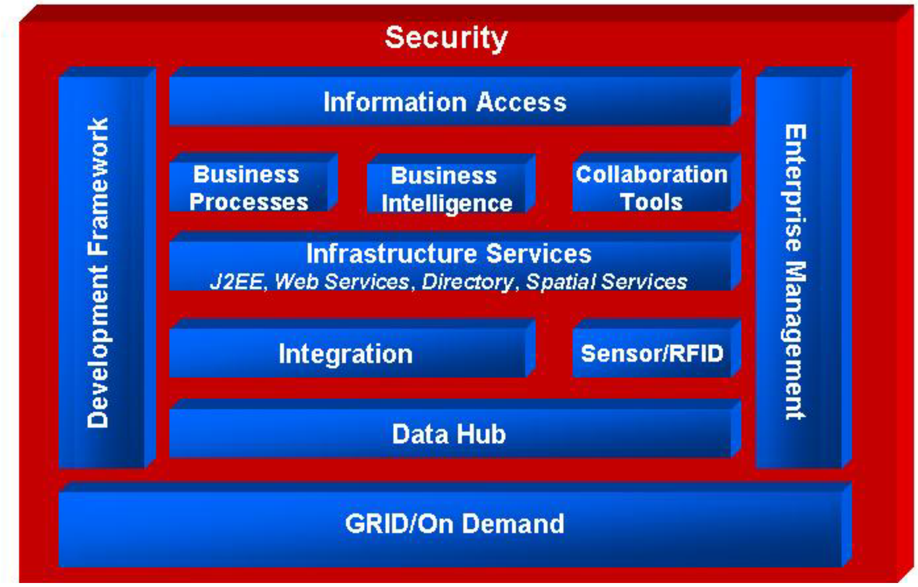


Figure 1: PROTECT Solution Architecture Layers

Security

At the foundation of the PROTECT architecture is the data level security that has become the standard for agencies dealing with the most sensitive data. The Security layer is an integrated set of features that provides defense mechanisms to guard an organization's data. The rest of the architecture builds on this foundation to provide a highly secure technology platform.

Information Access

The next layer of the PROTECT architecture is the Information Access layer, which is a common presentation interface layer for all services and applications that provides all channels with access to the same application. This layer enables access:

- For various types of users (employees, clients, or partners);
- From various devices (personal computers, handhelds, phones, etc.);
- With differing connectivity (wired, wireless, or intermittently connected);
- In support of various user interactions (transactions, queries, alerts, or visualizations); and
- With role-based access control.

Business Processes

The Business Processes layer contains the applications and services that are built upon the rest of the architecture. This layer provides the business specific PROTECT functions, which include:

- Packaged applications from Oracle;
- Packaged applications from the industry leading Oracle Partner Network; and
- Custom developed PROTECT applications.

The functional features of the applications that reside in the Business Process layer are explained in the PROTECT Business White Papers for each PROTECT market area. This technical white paper does not repeat those descriptions.

Business Intelligence

Business Intelligence is also a layer in the PROTECT architecture. This layer contains powerful services and applications that provide summary reports, ad hoc queries, geographic and geospatial queries, visualizations, OLAP, and data mining.

Collaboration Tools

The Collaboration Tools layer provides person-to-person communication tools for the entire organization, including email, web conferencing, instant messaging, and more.

Infrastructure Services

An integral layer of the PROTECT architecture, the Infrastructure Services layer enables a complete SOA framework on which all other solutions are based. This layer provides:

- Complete J2EE and web services framework
- Event-Driven Architecture based on the BPEL standard
- Spatial services: a broad set of built-in functions that provide common spatial features, such as “find the nearest instance of Feature Type Y to Feature Type X.”

Integration

The Integration layer provides the framework for integrating an organization’s disparate systems that are both internal and external to the organization. This layer:

- Provides connections to internal systems, external partners and sensors.
- Supports virtually all data types, communication protocols, transformation, and routing modes.
- Can support complex interactions between systems and instant analysis of trends/thresholds that can, in turn, trigger more messages, such as alerts or automatic recovery scenarios.

- Is key to the Event-Driven Architecture model.

Sensor/RFID

The Sensor/RFID layer provides the edge server that interfaces with and manages the sensor devices. This layer contains device drivers, data filters, event queues, and a management interface. Additionally, the Sensor/RFID layer passes the sensor event data to the other components of the architecture.

Data Hub

The PROTECT architecture includes a Data Hub layer that acts as a unifying platform for data by organizing data into domain specific data models. Because data can be organized into specific data models, organizations can rapidly deploy applications tuned to a specific domain.

Because data can be organized into specific data models, organizations can rapidly deploy applications tuned to a specific domain.

For example, Global Justice Extensible Markup Language (GJXML) is a standard data exchange protocol for law enforcement agencies. The Data Hub layer in the PROTECT architecture can provide a coherent GJXML data model for the exchange of GJXML data and on top of which law enforcement applications can be quickly built and deployed.

The Health Level Seven (HL7) Version 3.0 Reference Integration Model (RIM) provides the same type of unifying platform data model for the healthcare industry, which PROTECT can utilize.

Additionally, the Data Hub layer provides a single source of truth for shared information across the organization and between other agencies.

GRID/On Demand

The GRID/On Demand layer of the PROTECT architecture provides coherent, flexible, centrally managed pools of servers that can replace the often chaotic infrastructure of an organization. Greater flexibility, scalability, and availability, with lower costs of management, are the result of GRID computing.

On Demand is Oracle's suite of hosted operations solutions. For many organizations, hosted solutions make tremendous operational and financial sense. Limited IT resources can be freed up from routine operational support and, instead, be applied to creating unique IT value for the organization.

Development Framework

Rapid, yet robust, development tools are key to creating effective defense, intelligence, and homeland security solutions. The PROTECT architecture includes a Development Framework layer with the following features:

- Oracle's Advanced Development Framework (ADF) is a top rated J2EE/web services development framework that uses modeling and wizard-driven tools to rapidly create secure and standards compliant applications.

- For the non-Java shop, HyperText Markup Language Database (HTML DB) is an alternative rapid development framework that allows users to rapidly become productive web developers for transactional systems.

Enterprise Management

Many recent advances have focused on reducing the complexity of managing multiple systems while increasing availability, reliability and serviceability. The PROTECT architecture provides an Enterprise Management layer that—through the use of Oracle Enterprise Manager—acts as a central management console. This layers also works cooperatively with other central consoles, such as HP OpenView.

For the sake of focus, this paper will not address the Business Processes, Collaboration Tools, GRID/On Demand, Development Framework, and Enterprise Management layers of the PROTECT architecture. Please refer to www.oracle.com for multiple resources on these topics.

PROTECT SOLUTION ARCHITECTURE DETAILS

Security

Identity Management

Oracle's identity management framework is consistently rated in the Leader's Quadrant in the Gartner Inc. Extranet Access Management (EAM) Magic Quadrant report.

Many agencies suffer from a fragmented identity management solution. With an enterprise-wide solution, organizations can achieve better security at lower costs and at a lower complexity. An organization cannot replace the security management infrastructure of all of their legacy systems, however, as that idea is not practical. But, an agency can implement a single enterprise-wide solution for managing and authenticating users across the entire organization, including support for groups, roles, provisioning, audits, reports, etc., while protecting sensitive data. This type of solution will help the organization achieve better security while reducing costs and risk. The PROTECT architecture includes an identity management framework that offers this type of single enterprise-wide solution.

The identity management framework is a key component of the PROTECT architecture. It covers all of the significant aspects of a network security framework, including PKI, certificate authority, wallet managers, LDAP, SSO, federated authentication via SAML, and much more. Further, the framework complies with identity management standard interfaces (e.g., LDAP or JAAS), and it can be easily integrated with existing identity management infrastructures. Finally, Oracle's identity management framework is consistently rated in the Leader's Quadrant in the Gartner Inc. Extranet Access Management (EAM) Magic Quadrant report.

Application Level Access Control is Not Enough

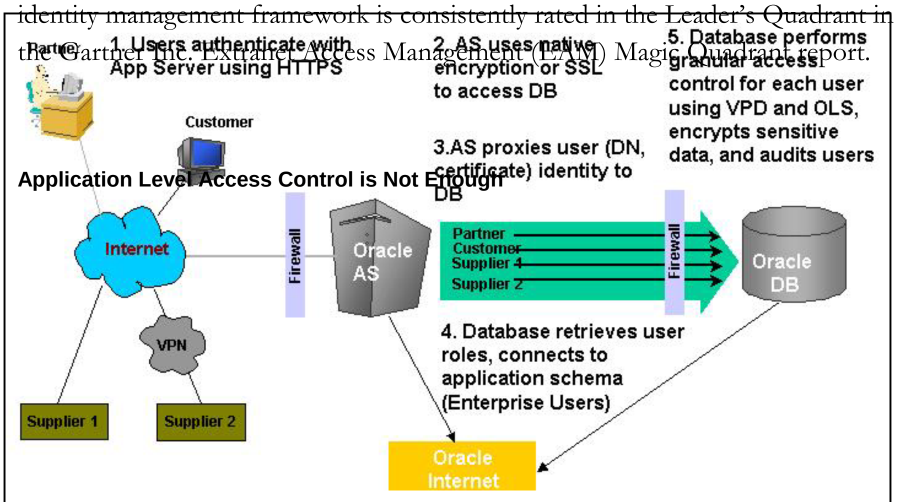

Partner
1. Users authenticate with App Server using HTTPS
2. AS uses native encryption or SSL to access DB
5. Database performs granular access control for each user using VPD and OLS, encrypts sensitive data, and audits users
Customer
3.AS proxies user (DN, certificate) identity to DB
Internet
Firewall
Oracle AS
Partner
Customer
Supplier 1
Supplier 2
Firewall
Oracle DB
VPN
4. Database retrieves user roles, connects to application schema (Enterprise Users)
Supplier 1
Supplier 2
Oracle Internet

Figure 2: Oracle 10g Security: Example

As described above, agencies need to protect sensitive data while, at the same time, allowing personnel to use data effectively. In the intelligence and military communities, sensitive data is often protected by isolating it to networks, but this solution is too cumbersome and often inhibits the mission of the agency. At the other extreme, many organizations protect their sensitive data by relying solely on application layer access controls. Application layer access controls are insufficient, as any breach of the application security exposes all of the data.

Instead of the above solutions, organizations must implement defense in depth, i.e., layers of protection for critical data. A significant portion of the PROTECT Security layer, Oracle's Virtual Private Database (VPD) and Oracle Label Security (OLS)—features of the Oracle Database—allow DBAs to protect specific data effectively and efficiently. In fact, DBAs can control access to data at the granularity of individual rows or columns, and DBAs can define very flexible groups to match the needs of the community. Oracle has been providing this type of "defense in depth" within the Intelligence Community for years.

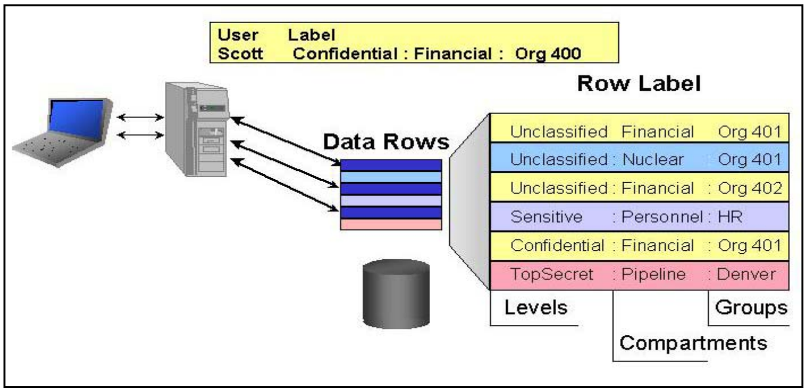

User Label
Scott Confidential : Financial : Org 400
Row Label
Data Rows
Unclassified Financial Org 401
Unclassified : Nuclear Org 401
Unclassified : Financial : Org 402
Sensitive : Personnel : HR
Confidential : Financial : Org 401
TopSecret : Pipeline : Denver
Levels
Groups
Compartments

Figure 3: Oracle Label Security: Fine Grained Access Control

What Type of Auditing is Needed?

Auditing is critical as it is the only defense against accidental or malicious abuse of security privileges. To be effective, auditing must be granular enough to catch any breach, yet selective enough not to overwhelm the auditor. Additionally, proper auditing must notify independent authorities when an improper or merely suspicious event occurs.

The PROTECT architecture provides auditing in the Security layer. Oracle Fine Grained Audit and Oracle Selective Audit provide the ability to audit at the data element level as well as create fine grained, flexible, and detailed audit reports.

Some auditing is best designed in the application. For example, if an officer consistently submits crime reports as a lesser offense than is typical for those types of crimes, an alert should go off in case the officer is attempting to "fudge" the crime statistics (because the officer is attempting to suggest a lower crime rate than the actual rate). Other auditing, however, needs to be at the data element level. Auditing at the data element level prevents privileged users from bypassing the application and modifying the data directly. To exemplify, an alert could occur if someone tries to directly modify the crime statistics. Another example is if a privileged user attempts to view the identity of witnesses in an organized crime case.

The PROTECT architecture provides auditing in the Security layer. Oracle Fine Grained Audit and Oracle Selective Audit provide the ability to audit at the data element level as well as create fine grained, flexible, and detailed audit reports. An Audit Manager or IT Security Manager can easily manage both the auditing of data and the creation of audit reports through GUI administrative screens. As a result, the easy to use and very powerful audit system can generate usage exceptions and alerts and feed them to various alerting protocols.

Trusted Information Sharing

As mentioned earlier, many organizations need to protect sensitive data from unwanted exposure, while simultaneously sharing that data with trusted partners. Oracle refers to this dual activity as Trusted Information Sharing. Trusted Information Sharing is a particular strength of the PROTECT solution architecture and the PROTECT business solutions. There are generally two aspects of Trusted Information Sharing:

- Within an organization
- Between organizations.

Within an Organization

PROTECT can extend Oracle's robust security to achieve even higher levels of accreditation, such as DCID 6/3 PL4.

The PROTECT business solution referred to as Cross-Domain Information Sharing extends Oracle security in order to control not only who is accessing the data, but also how, where, and when the data is accessed. For example, Data Vault—an Oracle technology solution within the Cross-Domain Information Sharing solution—can block requests for Secret data from a wireless network without biometric authentication at 3:00 A.M. It can also restrict access to data based upon the user's network. This approach can be used to provide the Director of Intelligence Directive (DCID) 6/3 Protection Level 4 (PL4) accredited solutions for military and intelligence systems. For example, auditing at the data element level will ensure that if a Top Secret cleared user is accessing a PROTECT application from a Secret level network, then that user will have access to, at most, Secret level data. If the same user needs access to the Top Secret data in the same system, the user will have to connect via a Top Secret network to obtain that data.

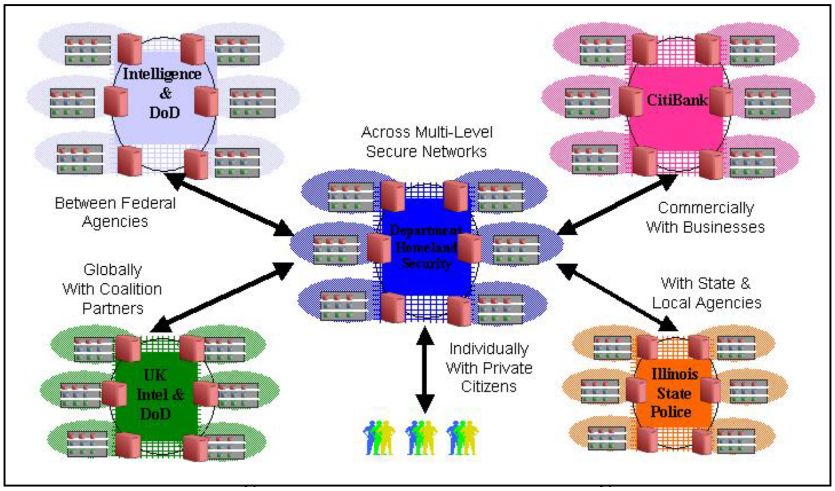
Between Organizations

The PROTECT architecture supports federated SSO via SAML-based identity management. For example, a Federal Bureau of Investigation (FBI) agent could login to System A of the FBI, and then the user could connect to System B of the Central Intelligence Agency (CIA) without the need to re-login. Under the covers, System B will have checked, via a central authentication server, that the FBI agent has already been authenticated.

In the PROTECT model, user names and passwords remain within the agency, but an outside user can still access data.

While federated SSO is important, other models are also necessary for sharing information. Often organizations do not want to share user identity information with outside agencies. In the PROTECT model, user names and passwords remain within the agency, but an outside user can still access data. This access to data is possible through a Trusted Information Gateway. Trusted Information Gateways communicate with other agencies to share/obtain information. These highly secure gateways manage data sharing agreements between organizations and ensure that such exchanges are approved and tracked. Additionally, Trusted Information Gateways institute very precise controls over whom can see what data. Thus, an outside user obtains information from inside of an agency through their local Trusted Information Gateway.

Such gateways can communicate with numerous organizations and participate in multiple tiers of trusted information networks. Key to the success of this model is the use of industry standard data tagging protocols, such as the International Organization for Standardization (ISO) Rights Expression Language (REL), which designates exactly how sensitive data can be shared and managed. The PROTECT architecture not only uses ISO REL, but it is also designed for Trusted Information Sharing with the eventual goal of creating a Trusted Information Network.


Intelligence & DoD
CitiBank
Across Multi-Level Secure Networks
Between Federal Agencies
Commercially With Businesses
Department Homeland Security
Globally With Coalition Partners
With State & Local Agencies
Individually With Private Citizens
UK Intel & DoD
Illinois State Police

Information Access

Organizations require the ability to deliver information to various types of users (employees, citizens, and partners) with unique needs (languages and disabilities) and over multiple channels (desktop, wireless, or disconnected). Agencies must apply these factors in determining access to sensitive information. Often, they ask the following types of questions to determine information access: Is access to highly sensitive information allowed over wireless connections? Is access allowed over the Internet? Is federated authentication needed? Is federated authentication acceptable? How do we monitor performance over all of these different channels? How do we develop new content and manage it without overburdening our staff?

PROTECT leverages the integrated presentation layers of the Oracle technology stack to provide the appropriate information access for an organization. These presentation layers include three types of major presentation modes, or channels:

- Portal,
- Wireless, and
- Disconnected.

Because the Oracle technology stack integrates these presentation layers, the infrastructure (security, management, availability, etc.) and the application function (the business logic and the data model) remains the same no matter which channel the organization is using for information access. Despite the integration of the layers, the organization can make changes to the presentation layer, if any are necessary, via wizards. Moreover, changes to the presentation layer are isolated to the appropriate channel. For example, changes to a browser's presentation will not affect the cell phone presentation. The following sections of this paper summarize the features of these three modes of presentation.

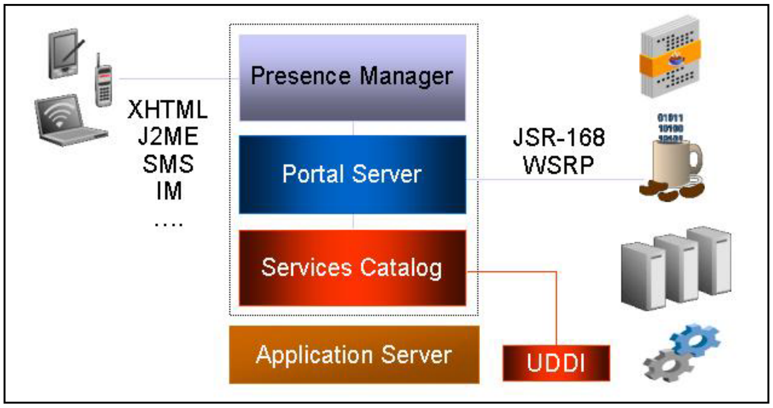


Figure 5: Information Access: Enterprise Portals

Portal Mode

The Portal mode of the PROTECT Information Access layer is based upon the Oracle Portal. Oracle Portal allows administrators to easily create a custom integrated desktop experience for the end user. It is a robust, yet intuitive tool that is the highest rated in the market, according to Network Computing Magazine. In fact, upon evaluating nine leading portal products, Network Computing Magazine in their April 2004 issue concluded: "New portal suites offer an array of linking technologies that require almost no development. At the top, Oracle's code-free environment boasts a nice price and an impressive feature set."

Features of the Oracle Portal include

- Browser-based page design
- "Context Flows"

- Integrated search and publishing
- Community portals
- Crosses geographical boundaries seamlessly
- Out-of-the-box integration with industry-leading collaboration products

Technical details on each of these features are available at www.oracle.com.

Wireless Mode

Another mode of the PROTECT Information Access layer, Wireless is facilitated by the Oracle Application Server (AS) 10g. Oracle AS Wireless enables application development independent of the wireless presentation device or network. In other words, a developer can create an application that outputs XML and then point Oracle AS Wireless to the application using only a URL. At run time, Oracle AS Wireless transforms the XML to the markup language and protocol format appropriate for the specific mobile device.

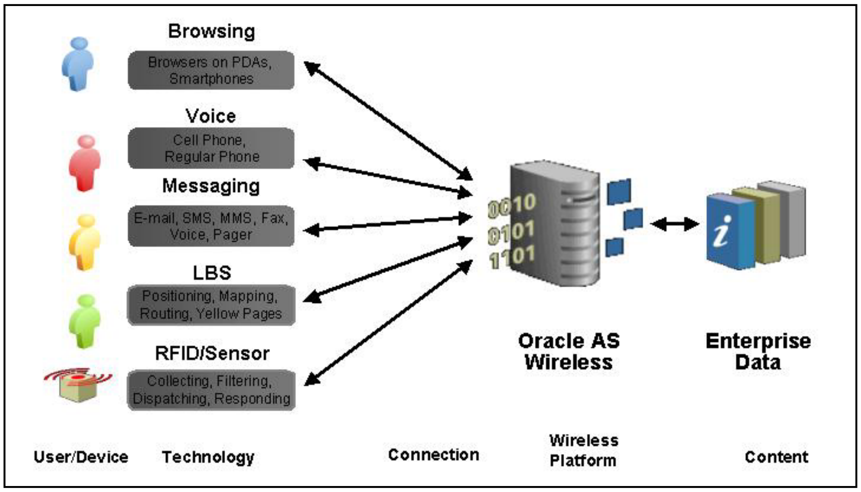

Browsing
Browsers on PDAs, Smartphones
Voice
Cell Phone, Regular Phone
Messaging
E-mail, SMS, MMS, Fax, Voice, Pager
LBS
Positioning, Mapping, Routing, Yellow Pages
RFID/Sensor
Collecting, Filtering, Dispatching, Responding
0010
0101
1101
Oracle AS Wireless
Enterprise Data
User/Device
Technology
Connection
Wireless Platform
Content

Figure 6: Multi-Channel Wireless Support

Several benefits to the Oracle AS Wireless model include:

- **Wireless Infrastructure Independence:** First, and most importantly, is that Oracle AS Wireless allows users to develop applications with a single unified programming model based on J2EE, HTTP and XML standards without rewriting or customizing the application each time a new device or new network needs to access the application.
- **Scalability:** Oracle AS Wireless keeps a single representation of the data content in an XML format in memory. As a result, Oracle AS scales very efficiently as requests for the same content increase from multiple users from many different devices.

- **MultiChannel Unification:** Using a unified programming model, Oracle AS makes any application that is deployed on the infrastructure easily and simultaneously accessible from multiple channels—email, browser, push, voice, and any device's micro-browser—with consistent state across all these different access channels.

Disconnected Mode

Oracle Database Lite is an addition to the Oracle Database 10g used for rapid development and deployment of mission-critical applications for mobile and small footprint devices.

In many scenarios, users need to access applications even while they are not connected to the network. Police in patrol cars or warfighters in the field, for example, often must operate with intermittent connectivity. In the PROTECT architecture, this Disconnected Mode is enabled via Oracle Database 10g Lite Edition. Oracle Database Lite is an addition to the Oracle Database 10g used for rapid development and deployment of mission-critical applications for mobile and small footprint devices. Oracle Database Lite uses data synchronization to reliably and securely exchange data between an Oracle Database and a remote environment. Personnel can utilize corporate information and perform functions while disconnected from the enterprise database.

Figure 7 displays the components of the Oracle Database Lite solution. The two main components of Oracle Database Lite are:

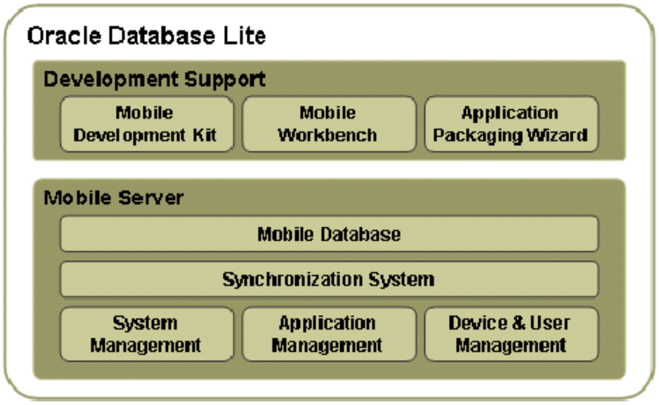


Figure 7: Oracle Database 10g Lite Edition

1. Developer tools to quickly and efficiently deploy applications into production; and
2. A mobile server for scalable deployment and management of applications, users, and devices.

Oracle Database Lite is a Java-enabled, secure, relational database management system that is self-administering and self-tuning, requiring no DBA involvement. It provides JDBC, ODBC, ADOCE, and ADO.Net programming interfaces and an object-oriented interface called SODA. This flexibility allows developers to build database applications from a variety of programming languages such as Java, C/C++, and Visual Basic.

Additionally, Oracle Database Lite includes a Packaging Wizard to bundle all application components (executables, DLLs, images, etc.) into a unique selfexecutable file for simple deployment to mobile or lightweight enterprise environments.

Finally, Oracle Database Lite includes a reliable, bi-directional synchronization server with a publication and subscription-based model allowing data and services to be synchronized between thousands of mobile users and the Oracle Database in the enterprise. The synchronization server easily integrates with existing systems and does not require additional middleware.

Business Intelligence

Oracle Business Intelligence

Homeland security depends upon the effective analysis of data obtained from a variety of sources. Effective analysis requires several key capabilities:

1. Acquiring the appropriate data;
2. Transforming, cleansing and organizing the data; and
3. Analyzing the data

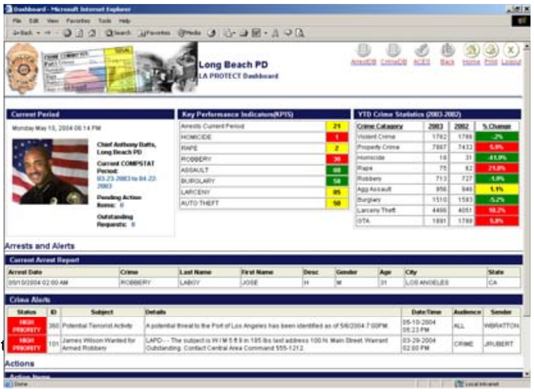
An organization’s attention is often unduly focused on the features of the end user analytical tools while overlooking the other aspects of data analysis. This may result from the fact that the first two steps can be difficult. However, those steps are also the most critical in achieving effective analysis.

Oracle provides the industry’s finest partitioning, clustering and high performance data analysis services as part of the Oracle Database and its various features.

PROTECT solutions can obtain data from a wide variety of sources both inside the enterprise and beyond. While bulk transfer is important, the need for near real time updates is also critical. The Integration section below describes how data can be obtained in near real time from any source within and beyond the organization. And, with the upcoming Trusted Information Gateway feature, organizations will also have very precise control on how and for whom sensitive data is obtained.

Besides acquiring the appropriate data, PROTECT solutions can handle the second key capability of effective analysis: Data of all types (numeric, structured and unstructured text, spatial, and image) can be transformed, cleansed, and organized into various data models using Oracle’s robust Data Warehouse Builder. Handling large data stores is challenging, especially when ensuring effective latency and throughput needs. This is an area in which Oracle excels—Oracle provides the industry’s finest partitioning, clustering and high performance data analysis services as part of the Oracle Database and its various features. An additional critical aspect is access control. In the PROTECT solutions, users can only access the data that they are allowed to see. Access control can be provided down to the granularity of an individual data element.

Data needs to analyzed and presented in a number of ways. In the past, this required purchasing, learning


Dashboard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
ArrestDB CrimeDB ACES Back Home Print Logout

Long Beach PD
LA PROTECT Dashboard

Current Period

Monday May 10, 2004 06:14 PM

Chief Anthony Batts, Long Beach PD

Current COMPSTAT Period: 03-23-2003 to 04-22-2003

Pending Action Items: 0

Outstanding Requests: 0

Key Performance Indicators(KPIS)

Arrests Current Period	21
HOMICIDE	1
RAPE	2
ROBBERY	30
ASSAULT	60
BURGLARY	58
LARCENY	85
AUTO THEFT	50

YTD Crime Statistics (2003-2002)

Crime Category	2003	2002	% Change
Violent Crime	1762	1788	-2%
Property Crime	7867	7433	5.8%
Homicide	18	31	-41.9%
Rape	75	62	21.0%
Robbery	713	727	-1.9%
Agg Assault	958	948	1.1%
Burglary	1510	1593	-5.2%
Larceny Theft	4488	4051	10.2%
GTA	1891	1788	5.8%

Arrests and Alerts

Current Arrest Report

Arrest Date	Crime	Last Name	First Name	Desc	Gender	Age	City	State
05/10/2004 02:00 AM	ROBBERY	LABOY	JOSE	H	M	31	LOS ANGELES	CA

Crime Alerts

Status	ID	Subject	Details	Date/Time	Audience	Sender
HIGH PRIORITY	360	Potential Terrorist Activity	A potential threat to the Port of Los Angeles has been identified as of 5/6/2004 7:00PM	05-10-2004 05:23 PM	ALL	WBRATTON
HIGH PRIORITY	101	James Wilson Wanted for Armed Robbery	LAPD - - The subject is W / M 5 ft 9 in 185 lbs last address 100 N. Main Street. Warrant Outstanding. Contact Central Area Command 555-1212	03-29-2004 02:00 PM	CRIME	JRUBERT

Actions

Action Items

Figure 8: Consolidated Business Intelligence

and maintaining multiple analytical tools. In the newest version of Oracle Discoverer, knowledge workers can perform ad hoc queries, OLAP analysis and report generation from a single tool. Moreover, by combining Discoverer's pure HTML interface with Oracle Portal, any user can have access to any analytical tool.

Search

Searching through data is a key feature of the PROTECT business solution offerings, as organizations need their knowledge workers to quickly and effectively perform ad hoc searches for data stored across their organizational intranet. At the same time, the data these knowledge workers can access must be restricted by the person's role, classification, and other privileges.

Oracle Enterprise Search extends the definition of enterprise search by including automatic classification, visualization, and other advanced features to provide enterprise users with a more direct and accurate response to their searches.

Oracle currently offers two out-of-the-box search solutions based on Oracle Text technology: Ultra Search and Enterprise Search. Ultra Search is included with the Oracle Database, the Oracle Application Server, and Oracle Collaboration Suite. Oracle Enterprise Search, on the other hand, is a standalone enterprise search server with its own install and administration tool.

Oracle Enterprise Search performs all the major functions of Oracle Ultra Search. Moreover, Oracle Enterprise Search adds the following key features:

- Better quality search results;
- More advanced "Secure Search;"
- Simple "one-touch" install – no database setup required;
- Simple administration, monitoring and tuning; and
- A short-term roadmap that includes more advanced search features, such as visualization and automatic classification.

Additionally, Oracle Enterprise Search extends the definition of enterprise search by including automatic classification, visualization, and other advanced features to provide enterprise users with a more direct and accurate response to their searches.

Architecturally, Oracle Enterprise Search consists of the following distinct components:

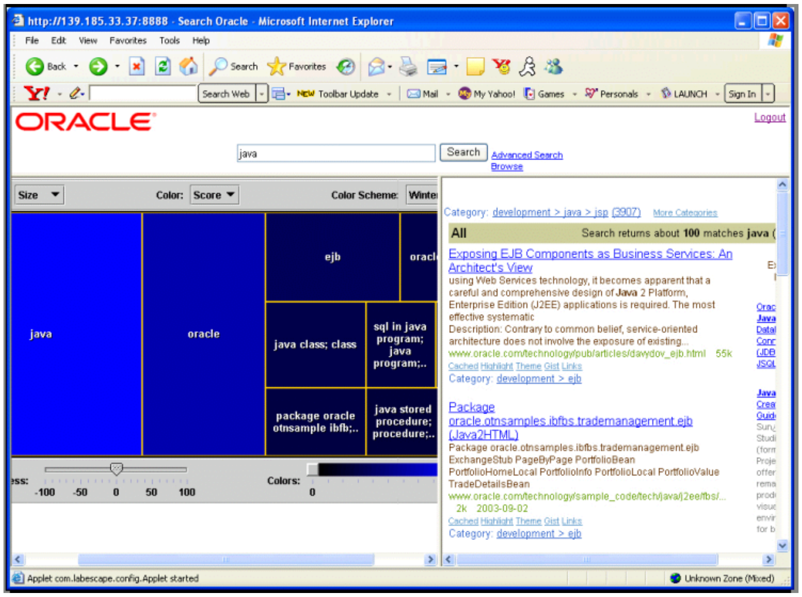
- **Crawler**: The Crawler is a Java process activated by the Oracle Enterprise Search server according to a set schedule. When activated, the Crawler spawns a configurable number of processor threads that fetch documents from various data sources and indexes them using Oracle Text. This index can then be used for querying. The Crawler's crawling abilities extend to the following data sources:
  - Website (HTTP Protocol)
  - Database tables
  - Oracle and any ODBC compliant database

  - A local database or a remote database
  - Fulltext and 'fielded' columns
  - Files (file:// Protocol)
  - Emails (IMAP Protocol)
  - Mailing lists through IMAP
  - Custom sources

- **Enterprise Search Server:** The Enterprise Search Server consists of a data repository and Oracle Text. Oracle Text provides the text indexing and search capabilities required to index and query data retrieved from the organization's data sources. It operates as a "black box" that indexes information from the Crawler and serves up the query results.

- **Query UI and API:** An out-of-the-box UI is the major interface to the Enterprise Search Server. Oracle also provides an API for querying indexed data. The API also contains interfaces for Basic Search, Advanced Search, Query Result Display, Customization and Embedding, Help, Feedback, URL registration, and other features.

- **Federator**: Federator provides the ability to federate queries to other heterogeneous data sources including Oracle Files and email. These results can be combined and displayed together.


http://139.185.33.37:8888 - Search Oracle - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Search Web Toolbar Update Mail My Yahoo! Games Personals LAUNCH Sign In
ORACLE
Logout
java
Search
Advanced Search
Browse
Size
Color: Score
Color Scheme: Winte
java
oracle
ejb
oracl
java class; class
sql in java program; java program;..
package oracle otnsample ibfb;..
java stored procedure; procedure;..
-100 -50 0 50 100
Colors: 0
Applet com.labescape.config.Applet started
Unknown Zone (Mixed)

Category: development > java > jsp (3907) More Categories

All Search returns about **100** matches **java** (

Exposing EJB Components as Business Services: An Architect's View
using Web Services technology, it becomes apparent that a careful and comprehensive design of **Java** 2 Platform, Enterprise Edition (J2EE) applications is required. The most effective systematic
Description: Contrary to common belief, service-oriented architecture does not involve the exposure of existing...
www.oracle.com/technology/pub/articles/davydov_ejb.html 55k
Cached Highlight Theme Gist Links
Category: development > ejb

Package oracle.otnsamples.ibfbs.trademanagement.ejb (Java2HTML)
Package oracle.otnsamples.ibfbs.trademanagement.ejb ExchangeStub PageByPage PortfolioBean PortfolioHomeLocal PortfolioInfo PortfolioLocal PortfolioValue TradeDetailsBean
www.oracle.com/technology/sample_code/tech/java/j2ee/ibfbs/... 2k 2003-09-02
Cached Highlight Theme Gist Links
Category: development > ejb

Figure 9: Oracle Enterprise Search

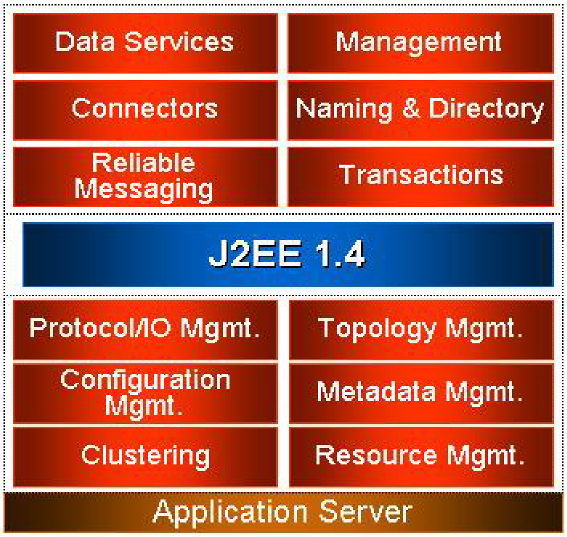
Infrastructure Services

Increase Agility with Service Oriented Architecture

The PROTECT architecture includes Oracle AS 10g, which provides a comprehensive SOA infrastructure that enables an organization to develop, wrap, orchestrate, provision, manage, secure, federate, discover, and access enterprise applications as services.

SOA is a software architecture that facilitates the development of enterprise applications as modular business services. The PROTECT architecture includes Oracle AS 10g, which provides a comprehensive SOA infrastructure that enables an organization to develop, wrap, orchestrate, provision, manage, secure, federate, discover, and access enterprise applications as services. Oracle AS 10g also supports event-driven computing, as a complement to service-oriented computing, to enable real time, sense-and-respond applications, such as RFID-based systems. These comprehensive capabilities provide an organization with a flexible enterprise application infrastructure.

Figure 10: Infrastructure Services



The PROTECT architecture provides a SOA infrastructure that enables a comprehensive runtime platform for web services including:

- Certified support for J2EE 1.3 and J2EE 1.4;
- Comprehensive support for J2EE services, including JTA, JCA, JMS, JNDI, JavaMail, MDB, and JAX-RPC;
- Comprehensive Web services infrastructure, including WS-I Basic Profile–compliant SOAP and WSDL generation tools, supporting SOAP 1.1 and 1.2, WSDL 1.1, and UDDI V2;
- A UDDI registry with support for Oracle's, Microsoft's, and IBM's UDDI browsers;
- A comprehensive SOA platform with support for WS-Reliability, WS-Addressing, WS-Security, and the WS-Coordination and Activation Framework (WS-CAF);
- A web services management console for logging, auditing, reliability, and security;
- Support for rpc/encoded and document/literal style web services; and
- Support for SOAP over JMS and HTTP.

Spatial Services

PROTECT solutions rely heavily on geospatial information. Data must be acquired from many sources, stored and organized into meaningful data models, and displayed effectively. Through Oracle Spatial and Oracle Locator, geographic and location data are managed in a native type within the Oracle Database 10g. Oracle Spatial is an option for Oracle Database 10g Enterprise Edition that provides advanced spatial features to support high-end GIS and location-based services (LBS) solutions. Oracle Locator is a feature of both the Oracle Database 10g Standard and Enterprise Editions that provides core location functionality needed by most customer applications to support a variety of LBS and third party GIS solutions.

Oracle MapViewer is an Oracle AS Java component and JDeveloper extension used for map rendering and viewing geospatial data managed by Oracle Spatial or Locator. Alternatively, data can be rendered by software from one of several GIS and LBS vendors. Almost all such software uses Oracle Spatial and/or Oracle Locator as its platform for data management.

Directory

A critical portion of the modern PROTECT infrastructure is the directory. Oracle Internet Directory is an LDAP service that combines the mission-critical strength of Oracle's database technology with the flexibility and compatibility of the LDAP Version Three directory standard. Oracle Internet Directory is a critical component of the Oracle Application Server's management and security infrastructure. It is also tightly integrated with the Oracle Database. In addition, Oracle Internet Directory's scalability, high availability and security features make it ideal for high volume and online service provider implementations.

Integration

Oracle Integration is a critical part of the PROTECT architecture. It connects PROTECT solutions to systems, devices and sensors inside and outside of the organization. It is composed of the following components:

- Enterprise Service Bus
- Process Management
- Partner Integration
- Activity Monitoring

Enterprise Service Bus

Oracle AS Interconnect is a simple and easy-to-use data integration product that provides full enterprise service bus (ESB) functionality for rapidly deploying integration solutions across the enterprise.

Process Management

Oracle AS BPEL Process Manager is a model-driven approach to business process management to develop, compose, and debug end-to-end business processes that span people, partners, and applications. Oracle offers the industry's first BPEL 1.1–compliant business process management engine. The BPEL Process Manager allows an organization to model business process definitions in a graphical modeling environment, to capture these definitions, and to execute them on Oracle's web services platform.

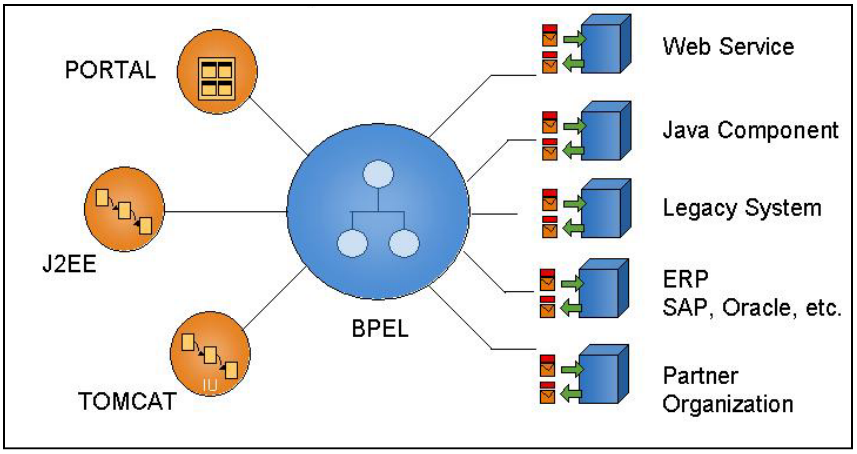


Figure 11: BPEL, the Orchestrator

Partner Integration

Oracle AS Integration Business-to-Business (B2B) is a complete B2B solution that supports leading industry protocols for comprehensive and rapid partner integration, including:

- Comprehensive trading partner management;
- Extensive protocol support; and
- Extensible architecture.

Activity Monitoring

Oracle AS Integration Business Activity Monitoring (BAM) is an event-driven platform for aggregating, correlating, and presenting events in the enterprise within a context understood by the organization. It enables an organization to collect, filter, correlate, and aggregate events from a range of different event and data sources, including sensor-based networks that generate millions of events. Oracle AS Integration BAM interprets those events into meaningful business events that are actionable or that provide visibility into the enterprise.

Oracle Integration also exploits the batch processing and data-cleansing capabilities of Oracle Warehouse Builder to deliver a single source of truth for important information assets. It interoperates seamlessly with Oracle Portal to create composite applications involving enterprise business processes and data. And it provides comprehensive monitoring and management using Oracle Enterprise Manager.

Sensor/RFID

Driven by advances in RFID technology, many agencies and organizations currently use sensors to collect a wide variety of data. The PROTECT business solutions recognize the need for organizations to improve their use of sensors and to better utilize the data collected by those sensors. Thus, the Oracle Edge Server is another important component of the Integration layer of the PROTECT architecture.

The PROTECT business solutions recognize the need for organizations to improve their use of sensors and to better utilize the data collected by those sensors.

A component of the Oracle AS, the Oracle Edge Server collects data from a wide variety of sensors and provides customized filters for each of the different types of sensors. The filtered data generates events, including XML-based messages that can be fed into the rest of the Integration layer. The filtered data can thus be passed to any backend systems, such as warehouse management systems. Results can also be fed back to partners, such as suppliers, to instantly adjust the real time supply chain.

The Oracle Edge Server can also interface with sensors used for many other scenarios, such as the temperature, motion or location sensors used for asset security management. In each case, the data can be transformed, routed, analyzed and used to drive alerts or complex business processes.

Data Hub

Oracle is uniquely able to provide data models and data services for delivery and analysis of real world scenarios in a secure manner.

One of the major obstacles facing organizations today is working with data from multiple sources. The Data Hub layer defined for the PROTECT architecture provides the functionality needed to capture, maintain, and analyze data that is obtained from various and multiple data source locations. This data can then be disseminated across the organization or analyzed by the various BI tools.

The PROTECT Oracle Data Hub layer consists of tools to instantiate domain specific data models. Examples of these data models are:

- Global Justice XML Data Model (Global JXDM) (for law enforcement agencies);
- HL7 3.0 RIM (for healthcare data); or
- Oracle Trading Community Architecture (TCA) model (for any entity, organization, or location’s modeling needs);

Increasingly, vendors are moving to an XML standard for data interchange. In this case, the data definitions are well defined, including hierarchical structure and cross-links.

The Oracle XML DB feature of the Oracle Database allows XML data models to be directly mapped into the database. These XML data models can then be accessed by both XML native tools and SQL-based queries. An organization can then easily build applications and analysis on top of an XML-based standard data model.

PROTECT includes tools to automatically generate such data models for industry standard XML schemas. These tools greatly reduce the costs of adopting XML-based data models as the foundation for interoperability with other organizations. Oracle is adopting a number of these data models as solutions in the Oracle Data Hub strategy.

CONCLUSION

A pre-integrated stack that is constantly tested together, the PROTECT architecture greatly reduces the complexity and manageability of the PROTECT business solutions. Ensuring that developing and managing PROTECT solutions is modular and scalable, the layered architecture implements best practices for building enterprise solutions. Further, by adhering to standard APIs throughout the stack, PROTECT solutions maintain their flexibility while protecting the customer's investment.

Ensuring that developing and managing PROTECT solutions is modular and scalable, the layered architecture implements best practices for building enterprise solutions.

With an extensive background in secure data handling from years in the intelligence and military agencies, Oracle offers the most secure and complete software infrastructure for both protecting and sharing sensitive information. This data can include unstructured text, XML standard models, image, or spatial data. All can be acquired, managed, processed and accessed according to the exact needs of the data and the community that utilizes it. Examples of very sensitive data that the PROTECT solutions can manage include:

- Patient health data;
- Criminal identities, evidence, and witness information;
- Pre-strike terrorism patterns; and
- Air strike tasking orders.

Finally, Oracle plans to greatly extend the capabilities of Trusted Information Sharing in the future. Users of the PROTECT solutions will be able to easily take advantage of these new features to extend both the strength and reach of their information systems. This will be very important as organizations continue to extend their cooperation with larger virtual communities of partners.

ORACLE

Oracle PROTECT: Solutions for Homeland Security Solution Architecture
June 2005
Author: Paul Silverstein
Contributing Author: Julie Greenspoon

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

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.