

## Database Security

# Protected Grid Computing with ORACLE Database



**Described Version:** ORACLE Database 10g Enterprise

**Also applicable for:** ORACLE Database 10g Standard

**Target platforms:** Windows Vista/XP/2000, Linux

**MARX hardware:** CrypToken M2048 / MX2048 JCOP



### Database Security and Compliance!

Oracle Database 10g builds upon the powerful security features delivered in Oracle9i to bring state-of-the-art capabilities to address rapidly emerging requirements in the areas of privacy, regulatory compliance, and data consolidation.

New features include column based access controls with Virtual Private Database, enhancements to Fine Grained Auditing, support for the AES algorithm for database encryption, expanded support for PKI and integration of Oracle Label Security with Oracle Identity Management. A new feature in Oracle Database 10g Release 2 is Transparent Data Encryption, part of Oracle Advanced Security. The CrypToken simplifies and secures your Oracle database protection scheme.

- **Mobile and secure certificate storage**
- **Enhanced security with two-factor authentication**
- **Authentication with X.509 certificates**
- **Safe against phishing and password theft**

# Table of Contents

<b>1. Oracle Overview.....</b>	<b>2</b>
<b>2. Authentication and security for Oracle based solutions.....</b>	<b>3</b>
2.1 Oracle Advanced Security.....	3
2.2 PKCS #12 Support.....	3
2.3 PKCS#11 support, Smartcards/Hardware Security modules.....	3
2.4 Oracle Database Security: Oracle Identity Management.....	4
2.5 Oracle Fusion Middleware.....	4
<b>3. CryptToken: cryptographic hardware for Oracle-based security solutions....</b>	<b>5</b>

## 1. Oracle Overview

Oracle (<http://www.oracle.com>) is one of the world's largest enterprise software companies offering solutions for every tier of business-database, middleware, business intelligence, business applications, and collaboration. The most known Oracle products are Oracle Database and Oracle Fusion Middleware.

**Oracle Database** (<http://www.oracle.com/database/index.html>) offers enterprise-class performance, scalability and reliability on clustered and single-server configurations. It provides comprehensive features to support the most demanding transaction processing, business intelligence, and content management applications. Oracle Database delivers protect from server failure, site failure or human error, secures data with unique row-level security, fine grained auditing, and transparent data encryption, includes high-performance data warehousing, online analytic processing, and data mining features for Windows, Linux, and UNIX servers.

Oracle's next-generation enterprise computing platform – **Fusion** (<http://www.oracle.com/products/middleware/index.html>) – is being designed to enable incremental adoption of a powerful, flexible, service-oriented IT infrastructure without the disruption associated with a wholesale platform upgrade. It contains Application Server, Collaboration Suite, Developer Tools, Identity Management and other deliberate solutions.

Oracle also supplies a wide range of business solutions and applications generally known as **Oracle Applications** (<http://www.oracle.com/applications/home.html>) like Oracle E-Business Suite, Siebel, Peoplesoft Enterprise, Financial Management, Human Capital Management, and others.

## 2. Authentication and security for Oracle based solutions

Oracle recommends, if possible, using Oracle Advanced Security (an option to the Enterprise Edition of Oracle Database) with network authentication services (such as Kerberos), token cards, smart cards or X.509 certificates.

### 2.1 Oracle Advanced Security

Oracle Advanced Security provides the ability for businesses to leverage their existing security infrastructures such as Kerberos, PKI and RADIUS for strong authentication services.

<http://www.oracle.com/technology/deploy/security/database-security/advanced-security/index.html>

PKI support includes the ability to check X.509v3 certificate revocations using Certificate Revocation Lists stored in the file system, Oracle Internet Directory or using CRL Distribution Points. In addition, Oracle database servers or database clients can use PKI credentials, stored in smart cards, with the PKCS #11.

### 2.2 PKCS #12 Support

PKCS #12 standard support allows the public key credentials sharing with other user applications such as browsers. Oracle Advanced Security supports X.509 certificates stored in **PKCS #12** containers, making the Oracle Wallet interoperable with third party applications like Netscape Communicator 4.x and Microsoft Internet Explorer 5.x, and providing wallet portability across operating systems. Users who have existing PKI credentials may export them in PKCS#12 format and reuse them in Oracle Wallet Manager, and vice versa. PKCS#12 thus increases interoperability and reduces the cost of PKI deployment for organizations.

### 2.3 PKCS#11 support, Smartcards/Hardware Security modules

An Oracle Wallet is a software container that holds the private key and other trust points of the certificate. Oracle Advanced Security supports PKCS#11 industry standard. This allows the private keys that were previously stored on the file system to be created and stored in secure devices such as Hardware Security Modules or Smart Cards that are available in the market.

Oracle Advanced Security 10g Release 2 and later versions provides deeper integration with PKCS#11 enabling interoperability with pre-provisioned certificates on hardware devices.

See the following link for details:

Oracle 11:

<http://www.oracle.com/technology/deploy/security/database-security/pdf/advanced-security-11g-whitepaper.pdf>

Oracle 10g Release 2:

[http://www.oracle.com/technology/tech/windows/wp/Oracle\\_DB\\_10g\\_Security\\_WP.pdf](http://www.oracle.com/technology/tech/windows/wp/Oracle_DB_10g_Security_WP.pdf)

The similar information can be found in the “Oracle Advanced Security” datasheet:

*Certificate Based Authentication*

*OracleAS supports mutual authentication or server authentication with certificates. Users can use certificates that have been provisioned without using Oracle Wallet Manager as long as they are in the*

## 2. Authentication and security for Oracle based solutions 4

standard PKCS#12 format. The private key and/or certificates can reside in a smart card or a hardware security module that supports the standard PKCS#11 interface.

Oracle 11:

[http://www.oracle.com/technology/deploy/security/database-security/pdf/ds\\_security\\_db\\_advanced\\_security.pdf](http://www.oracle.com/technology/deploy/security/database-security/pdf/ds_security_db_advanced_security.pdf)

Oracle 10g Release 2:

[http://www.oracle.com/technology/deploy/security/as\\_security/pdf/appserversec\\_10gr2\\_datasheet.pdf](http://www.oracle.com/technology/deploy/security/as_security/pdf/appserversec_10gr2_datasheet.pdf)

### 2.4 Oracle Database Security: Oracle Identity Management

Oracle Database Security can be integrated with enterprise-scale Oracle Identity Management which allows enterprises to manage end-to-end lifecycle of user identities across all enterprise resources and experience the full power of Enterprise Single Sign-On.

(<http://www.oracle.com/products/middleware/identity-management/identity-management.html>)

Oracle Identity Management is a member of the Oracle Fusion Middleware family of products and provides integrated identity administration, single sign-on, centralized policy management and a compliance-reporting framework for applications. It supports a wide variety of authentication mechanisms - for example HTML Forms, X.509 certificates, and smart cards - and has a flexible administration framework for creating, managing, or customizing access control policies.

Authentication control and policy enforcement is provided out of the box for a wide variety of web servers, application servers, and packaged applications running on nearly any flavor of operating system, including Windows, SUSE Linux, RedHat Linux, Solaris, AIX, and HP-UX.

### 2.5 Oracle Fusion Middleware

Oracle Fusion Middleware is a family of Oracle software solutions (Oracle Application Server is a member of the Oracle Fusion Middleware family of products e.g.).

See the following link for more details on Oracle Fusion Middleware:

<http://www.oracle.com/products/middleware/index.html>

As already mentioned Oracle Fusion Middleware security is based on Oracle Identity Management solution. Combined with Oracle Strong Authentication Solutions it allows to use smart cards for users authentication:

<http://www.oracle.com/products/middleware/identity-management/strong-authentication.html>

### 3. CrypToken: cryptographic hardware for Oracle-based security solutions

MARX® CryptoTech LP provides comprehensive support for PKI / X.509 industry standards in its CrypToken product series. The CrypToken supports both Microsoft Windows Cryptographic Services and RSA Labs' Public Key Cryptographic Standards; the two most widely adopted cryptographic interfaces.

It allows direct usage of CrypTokens for X.509 certificates secure storage and manipulation, strong authentication, digital signatures and data encryption in Oracle Advanced Security and Identity Management solutions.

MARX offers two models of CrypToken: CrypToken M2048 (with MULTOS operating system) and CrypToken MX2048 (with JavaCard operating system). Due to Microsoft CryptoAPI comprehensive support both of them can be straightforwardly used in Active Directory-based security solutions.

The CrypToken is equipped with SafeSign middleware. SafeSign is a powerful and cost effective Public Key middleware solution for USB Tokens and Smart Cards.

It's our business to protect yours

## The CrypToken is ideal for...

- Online Banking: Secure Internet banking and financial transactions.
- VPN: Virtual Private Network control from remote locations.
- eGovernment: Access control to confidential information.
- Email: Encryption and digital signature of confidential emails.
- eCommerce: Secure B2B/B2C authentication.
- RAS and network logon: Access for authorized users only.
- WebSecurity: Secure web portal and internet and intranet identification.
- DataSecurity: Encryption of sensitive information.



Get your CrypToken Evaluation Kit:

[www.cryptoken.com/eval](http://www.cryptoken.com/eval)  
+49(0)8403 9295-14

### Comparison table CrypToken M2048 and CrypToken MX2048

Features	M2048	MX2048
Token operating system	MULTOS	JavaCard
Operation	Driverless, if CCID OS used	
Certification smart card chip	EAL 5+ EMV, ISO7816	EAL 4+, EMV, ISO7816, JavaCard 2.3.1, GlobalPlatform 2.1.1
Controller chip certification	WHQL (Microsoft), HBCI (Home Banking Computer Interface), EMV, ISO7816	
Smart card chip	Infineon SLE66xx series	SmartMX/JCOP21
Cryptographic standards supported	PKCS#11v2.01, MS-CAPI	
Operating systems supported	Windows Vista/XP/2000, Linux, MacOS X	Windows Vista/XP/2000, Linux, MacOS X
Memory (total)	64 KByte	72 KByte
Casing & LED	Metal Designer Case, LED (duo color green/red, for „stand by/activity“), eye for key ring/lanyard	
Electrical certifications	FCC, CE, RWTUEV	FCC, CE, RWTUEV
Dimensions	0.51" x 0.32" x 1.38" (13 x 8 x 35 mm)	0.51" x 0.32" x 1.38" (13 x 8 x 35 mm)
Weight	0.326 oz (9,25g)	0.326 oz (9,25g)

#### CrypToken certifications



All trademarks used in this document are property of their respective owners.

#### MARX CryptoTech Germany

Vohburger Strasse 68  
D-85104 Wackerstein  
Phone: +49 (0) 8403 9295-14  
Fax: +49 (0) 8403 929529  
contact@cryptoken.com

#### MARX CryptoTech LP

4485 Tench Road #310  
Suwanee, GA 30024 U.S.A.  
Phone: (+1) 770 904 0369  
Fax: (+1) 770 904 3893  
info@cryptotech.com

[www.cryptoken.com](http://www.cryptoken.com)