Oracle Security Developer Tools (OSDT)
August 2008
Items

• Introduction
• OSDT 10g Architecture
• Business Benefits
• Oracle Products Currently Using OSDT 10g
• OSDT 10g APIs Description
• OSDT 11g Sneak Preview
Introduction

- Oracle Security Developer Tools (OSDT) is a set of Java libraries that developers use to secure enterprise applications
- OSDT is delivered as a set of JARs shipped as part of the Oracle Application Server
- OSDT is one of the SDKs making up Oracle Platform Security Services (OPSS)
  - Other OPSS SDKs include key store management, identity services, etc.
OSDT 10g Architecture

Note: Lower layers enable higher layers. For example, XML Security is used to sign and/or encrypt SAML assertions and/or WS-Security headers.

Note: Deprecated in 10g. Part of JCE in 11g.
**Business Benefits**

- Standards-compliant
  - Java, XML
- Certified
  - Oracle’s Crypto Engine is FIPS 140-2 Level 1 certified
- Proven
  - Used by several Oracle products
  - Deployed at hundreds of customer sites worldwide since 1996
- Interoperable
  - OASIS / W3C / LAP interop events
- Readily available
  - The OSDT JARs are installed with the Oracle Application Server in `ORACLE_HOME` (OC4J and WebLogic Server)
- Extensible
  - Modular architecture, portable, scalable, easily integrated with enterprise applications
Oracle Products Currently Using OSDT

- **Oracle Applications**
  - Global Mapping; GI (Image Process Management); Payment; XDO (XML Publisher); Workflow, BPEL
  - Oracle Collaboration Suite (Email)

- **Application Server**
  - OC4J (Web Services security stack)
  - Available on WebLogic Server (10.3 and later)

- **Platform Security**
  - JPS; SSL Configuration; Oracle Wallet (used by Oracle Identity Management products, Oracle EM and the Oracle Database Server)

- **Oracle Products**
  - Oracle Web Services Manager (OWSM); Business Integration (B2B); Oracle Portal; Oracle Identity Federation (OIF)
OSDT APIs
Oracle Crypto

- Provides core algorithms for cryptography in Java
  - RSA, DSA and EC public key cryptosystem
  - RC4 stream cipher
  - AES, DES and Triple-DES encryption
  - MD5 and SHA message digests
  - Diffie-Hellman Key Agreement
  - Pseudo-Random Number Generators (PRNG)

- Highlights
  - Public key and symmetric encryption, key exchange, message digests, and pseudo-random number generation
  - ASN1 parsing
  - Appropriate for applets and applications
  - JCE 1.2.1 provider available
  - Lightweight infrastructure for portability and thin code size
  - FIPS 140-2 Level 1 Certified
  - 100% Java, with no native methods
  - Portability to all Java platforms: JDK 1.1, 1.2, 1.3, 1.4, 1.5
Cryptoki (For information only: Deprecated)

- HSM & Smart Card Integration
  - Transparently integrates cryptographic hardware for performance or secure key storage
  - Works with any PKCS#11 compliant tokens
  - Helps building secure Java applets / applications that offer token-based authentication and digital signatures provided by smartcards
  - Supports Chrysalis, Eracom, nCipher, Rainbow, Sun, Thales accelerators and HSMs
  - ACS, Aladdin, Arcot, Celocom, Datakey, Giesecke & Devrient, GemPlus, Rainbow iKey, Schlumberger, Spyrus smartcards and authN tokens
- Deprecated in 10gR3
  - Currently available through JCE
Oracle JCE Provider
Java Cryptography Extensions

• Sun’s JCE provides cryptographic extensions to Sun’s Java Cryptography Architecture (JCA), a framework for developing and accessing cryptographic functionality for the Java platform

• Oracle JCE Provider is a concrete implementation of a subset of the cryptographic services defined in JCE
CMS

Cryptographic Message Syntax

• CMS defines data protection schemes that allow for secure message envelopes
• Fundamental technology underpinning non-XML digital signatures
• Highlights
  • Supports signed, digested, authenticated, encrypted, enveloped, compressed data, signed receipts and timestamps
  • Compliant with RFC 2630 and PKCS#7
  • Stream I/O support for efficiently securing large data sizes
  • Unlimited levels of secure content wrapping
  • Pure Java implementation
  • Optional PKCS#11 support for hardware accelerators and smartcards
S/MIME
Secure / Multipurpose Internet Mail Extensions

- Security enhancements to the MIME email standard based on RSA Data Security
- Interoperable with other S/MIME compliant products, such as Mozilla Mail and Microsoft Outlook
- Highlights
  - S/MIME v2, v3 and v3.1 support plus support for Enhanced Security Services (RFC 2634) such as digital receipts
  - Supports EDI-INT AS1 and AS2 enabling the secure exchange of EDI over the Internet
  - JavaMail-compliant API portable to all Java platforms
  - Optional PKCS#11 support for hardware accelerators and smartcards
PKI

Public Key Infrastructure

- Comprehensive range of protocols covering the entire certificate lifecycle for public key infrastructure development
- Allows for incremental PKI deployment with maximum flexibility and ease of integration
- Integrates with PKCS#11 cryptographic hardware
- Supported protocols
  - CMP/CRMF: Certificate Management Protocols (protocol used for certificate creation and management) and its companion specification Certificate Request Message Format (syntax used to construct a request for a certificate to a Certificate Authority); the Oracle CMP/CRMF API provides classes that implement CMP as described in RFC 2510 and CRMF as described in RFC 2511
  - OCSP: Online Certificate Status Protocol (protocol used to obtain the revocation status of a certificate – OCSP is an alternative to Certificate Revocation Lists); the Oracle OCSP API helps developers construct both standard OCSP requests and responses
  - TSP: Time Stamping Protocol (used to support non-repudiation); the Oracle TSP API provides an example implementation of a TSA server to use for testing TSP request messages, or as a basis for developing your own time stamping service
  - LDAP: Light Weight Directory Access Protocol (certificates are often stored in an LDAP directory and accessed as needed by requesting applications and services); the Oracle LDAP API helps developers validate a user’s certificate in an LDAP directory, and add, retrieve, delete a certificate from an LDAP directory
- Key pair / certificate generation utilities
XML Security

XML Signature and XML Encryption

- Core security tool for XML Digital Signatures and Encryption
- Complies with the W3C XML security recommendations
  - XML Signature, XML Encryption,
  - Transforms: Canonicalization 1.0, exclusive canonicalization, decrypt transform, XPath filter transform and enveloped signature transform
- Compatibility with JAXP 1.1-compliant software and hardware XML parsers and XSLT engines
  - Certified to work with Oracle/BEA, Apache, IBM, and Sun XML parsers)
- Integrates with smart cards and hardware security modules for secure key storage
- Can be deployed in any JRE 1.2+ application environment
SAML
Security Assertion Markup Language

• SAML enables cross-domain, interoperable exchange of security information (authentication, attributes, authorization) among trusted partners with disparate access management systems and applications
• The Oracle SAML API provides supporting tools, documentation, and sample programs to assist developers of SAML-compliant Java security services
  • Oracle SAML can be integrated into existing Java solutions, including applets, applications, EJBs, servlets, and JSPs
• Oracle SAML supports
  • SAML 1.0/1.1 and 2.0 specifications
  • SAML-based single sign-on (SSO), attribute, metadata, enhanced client proxy, and federated identity profiles
• Integrated security features includes XML security
• Integrates with smart cards and hardware security modules for secure key storage
• Can be deployed in any JRE 1.2+ application environment
XKMS
XML Key Management Specification

• XKMS defines protocols for distributing and registering public keys
  • Applications or web services supporting XKMS don't have to deploy a PKI solution locally; the application or web service sends XML requests (in SOAP messages) to PKI components installed at a trusted third-party site (e.g., Verisign) which executes the XML requests on behalf of the requesting party

• The Oracle XKMS API provides
  • Simplified access to PKI functionality: developers can easily deploy robust application functionality by deploying secure, lightweight client software
  • Support for complete key / certificate life cycle: helps enterprise applications locate, retrieve, and validate signature and encryption keys using lightweight web services infrastructure
  • Secure XKMS messages using the Oracle XML Security API
  • Support for JAXP 1.1-compliant XML parsers
WS-Security 1.0

Web Services Security

- WS-Security specifies SOAP security extensions that provide confidentiality using XML Encryption and data integrity using XML Signature
- WS-Security also includes profiles that specify how to insert different types of binary and XML security tokens in WS-Security headers for authentication and authorization purposes
- The Oracle WS-Security API supports the following profiles
  - Username Token 1.0
  - X.509 Certificate Token 1.0
  - SAML 1.x Token (committee draft)
  - Kerberos Token (committed draft)
Liberty Alliance

- The Liberty Alliance Project is an international organization that defines open identity standards, business and deployment guidelines, and best practices for managing security, access control and privacy
- The Oracle Liberty API allows Java developers to design and develop single sign-on (SSO) and federated identity management (FIM) solutions
  - Conforms to the Liberty Alliance ID-FF 1.1 and 1.2 specifications
  - Can be integrated into any existing Java solution, including applets, applications, EJBs, servlets, JSPs
OSDT JARs, OSDT Samples and Documentation

- **OSDT JARs Location**
  - `oracle_home/jlib/osdt_*.jar`
  - `jdeveloper/jlib/osdt_*.jar`

- **Samples for each API are available here:**

- **Documentation (Reference Guide (PDF) and JavaDocs for each API) is available here:**
  - [http://download.oracle.com/docs/cd/B28196_01/nav/docindex.htm](http://download.oracle.com/docs/cd/B28196_01/nav/docindex.htm)
OSDT 11g Sneak Preview
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.
OSDT 11g Architecture (2009)

Note: Lower layers enable higher layers. For example, XML Security is used to sign and/or encrypt SAML assertions and/or WS-Security headers.

(*) XML Security includes interface and implementation. For implementation, JSR 105 / 106 can be used (instead of Oracle’s implementation).

Note: Ships with OSDT 11gR1, but deprecated.