DIDISOFT
SOFTWARE SOLUTIONS
THAT FIT

DidiSoft OraRSA

RSA, CMS, S/MIME with PL/SQL methods inside the Oracle Database

DidiSoft OraRSA is an Oracle PL/SQL package providing cryptography methods that utilize the RSA algorithm and produce output in various IETF (Internet Engineering Task Force) standards like CMS (Cryptography Message Syntax), S/MIME (Secure Multipurpose Internet Mail extensions and X.509 certificates.

The package also enhances the capabilities of the standard UTL_SMTP PL/SQL package with support for sending S/MIME signed and encrypted emails.

All the cryptography operations are executed inside the database with no external applications involved.

Compatibility

The output and input of the package is fully compatible with all compliant software available on the market, including OpenSSL, Outlook, Thunderbird.

PRODUCT SUMMARY

- OpenRSA encryption inside Oracle© databases versions 11 and 12.
- Dedicated PL/SQL methods that work directly over the database columns.
- All the application logic is inside the database and no external applications are involved.
- Compliant with Internet Task Force standards and OpenSSL.
- Easy API with short learning curve.

DidiSoft OraPGP

OpenPGP encryption with PL/SQL methods inside the Oracle Database

Designed for Oracle Developers

The OraRSA package is designed to provide consistent PL/SQL methods for RSA cryptography. All the code is executed inside the Oracle© database memory space.

High security

The keys and X.509 certificates used with OpenRSA can be stored inside the Oracle© database and used directly from there, eliminating the need to access external files.

Support standards

RFC 5652 - Cryptographic Message Syntax (CMS)
RFC 5751 – S/MIME
RFC 2437 - RSA Cryptography

TECHNICAL SPECIFICATION

Oracle Database

Version 11 and 12

- ✓ Enterprise Edition
- ✓ Standard Edition
- ✓ Standard One

Programming Languages

PL/SQL

Public Key Algorithms

RSA, RSASSA-PSS

Public Key Format

PEM, DER, X.509, PKCS#12

Encryption Algorithms

AES 128/192/256, DES, 3-DES, Twofish, Blowfish, SAFER, Camellia 128/192/256

Signing Algorithms

SHA 256/384/512, SHA-1, MD-5, RIPEMD-160

Compression Algorithms

ZIP, BZIP2, ZLib

DidiSoft
www.didisoft.com

Tel: +1-256-907-7816
Fax: +1-256-907-7816

CORPORATE HEADQUARTERS
21 Dragovitza Str.
Apt. 120
Sofia 1000
Bulgaria, European Union (EU)

DidiSoft is a trusted leader in global business data protection. Over a decade DidiSoft has focused on providing encryption solutions to thousands of customers, including government agencies and financial institutions. Our software provides cost effective and easy to implement data protection solutions that is simple for IT to administer and operate.