



The Redvers COBOL Signature software package includes Digital Signature Standard (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) capability and uses asymmetric encryption (PKI) with OAEP padding.

Main features:

- All code is 100% pure COBOL
- Runs on any COBOL platform
- Supports DSA and elliptic curve (ECDSA) signatures
- Complies with PKCS #1 v2.2: RSA Cryptography Standard
- Supports public/private keys up to 4096 bits, in hex or Base64
- Distributed in COBOL source code
- Efficient, professional and fully scalable
- Supports calls from batch or online (eg: CICS)
- **Free 30 day trial available**

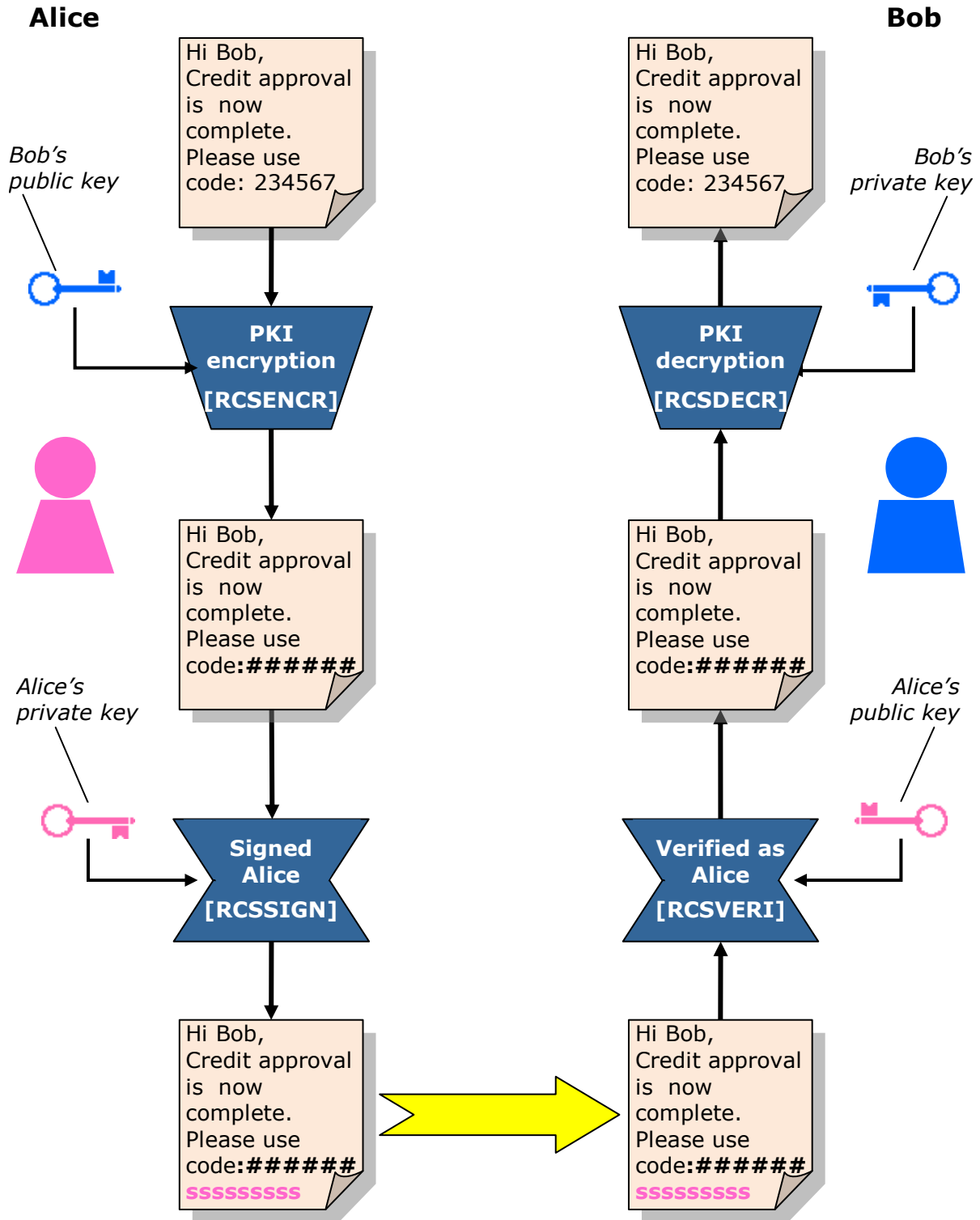
DSA signatures are created and verified as specified in [NIST FIPS PUB 186-4 Digital Signature Standard](#). ECDSA signatures conform to ANSI [ANS X9.62-2005 Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm \(ECDSA\)](#). Digital signatures provide assurance of the sender's identity and confirmation that the data received has not been altered by unauthorized activity.

PKI encryption and OAEP padding logic complies with algorithms provided in the RSA Laboratories [PKCS #1 v2.2: RSA Cryptography Standard](#). Specifically, RSAEP/RSADP are used for encryption/decryption and RSA-OAEP padding with MGF1 is used in padding and mask generation. PKI encryption uses public and private keys, according to application security requirements.

The required security level for digital signature generation/verification and PKI cryptography depends on the length of public/private keys as well as SHA-1 or SHA-2 hashing algorithms. Key sizes and hash digest lengths are specified by the calling application to ensure the correct security level is maintained.

How it Works

The diagram below shows how confidential information may be encrypted, signed, sent, verified and decrypted using **Redvers COBOL Signature** software.



The Redvers Signature Software runs standard digital signature and asymmetric encryption algorithms, so that signatures and ciphertext can be verified and decrypted by outside institutions.

Technical Information

The **Redvers COBOL Signature** (2.2) software package consists of:

- A sample COBOL calling application program (**RCSSAMP**).
- Four additional application programs to encrypt (**RCSENCR**), decrypt (**RCSDECR**), sign (**RCSSIGN**) and verify (**RCSVERI**).
- Two Redvers Consulting subroutines (**RCSCALC** and **RCSHASH**).

All these programs should be copied to the standard source code library and compiled. **RCSSAMP** will need to be compiled and linked last, before starting the trial.

Redvers COBOL Signature programs can be run on EBCDIC or ASCII character encoded platforms, using big or little endian binary formats. Data exchange between subroutines uses a common communication block containing left justified, space filled parameters in hexadecimal or Base64 formats.

All subroutine storage areas containing confidential information are initialized before control is returned to the calling application.

Included within the software is the Redvers calculator subroutine **RCSCALC**. This routine performs the modulated exponential calculations, modular inverse functions, scalar arithmetic and data conversion within the encryption/signature processes.

Also included is the Redvers hashing subroutine **RCSHASH**, which runs SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 algorithms.

RCSCALC and **RCSHASH** may be used by clients for other technical application requirements without charge.

If key lengths or algorithms are required that are not currently listed in the calling parameters, please contact your account manager or use our **Contact** page to request an enhancement.

The Product Package

A perpetual license for the **Redvers COBOL Signature** software can be provided for a one-off fee. Alternatively, the software can be leased on an annual basis for 20% of the perpetual license cost (minimum two years).

All licenses include:

- Product source code
- Sample COBOL calling programs
- User Guide
- Corporate level software license
- Money back guarantee
- Product upgrades and support via email*

Additional options:

- 24 x 7 telephone hotline support
- Software escrow agreement with Software Escrow Solutions

Licensed software and documents are shipped in the form of email attachments unless otherwise requested. Installation is performed by copying the source code text into your COBOL source code library and running your standard site compiler.

Full pricing details can be found at:

https://www.redversconsulting.com/cobol_signature_pricing.php

* Free for the first year followed by a minimal annual fee.

About Redvers Consulting

Redvers Consulting provide niche software products for the integration, modernization and security of COBOL applications. Our clients are primarily large financial institutions in Europe and North America, although we also have customers in many other business and geographical areas.

Our ability to deliver software in COBOL source code form, gives customers reliable, efficient and perfectly integrated solutions to business needs. Source code distribution also means our software will run on all hardware platforms and operating systems: *EBCDIC, ASCII, big endian or little endian*.

Redvers Consulting have received many business awards over the years, including winning the **Best use of Technology** category in the Thames Gateway Business Awards. We are also business partners with **IBM, Micro Focus** and **Fujitsu**.

Our client list includes:

Agora (FR)
ANZ (AUS)
BAE Systems (USA)
Canada Life Assurance (UK)
Deutsche Bank (USA)
Deutsche Rentenversicherung Bund (DE)
FirstBank (USA)
Fiserv (USA)
GMAC Insurance (USA)
Hanesbrands (USA)
John Deere (USA)
LBS / Finanz Informatik (DE)
J P Morgan (USA)
Oppenheimer (USA)
Pacific Gas (USA)
Network Rail (UK)
R+V Allgemeine Versicherung (DE)
Sasktel (CAN)
SEB (DE)
Standard Life Assurance (UK)
Suncorp (AUS)
SunGard / FIS (USA)
WorkSafeBC (CAN)
Zurich Insurance (UK & CHE)

Contact: <https://www.redversconsulting.com/contact.php>

Development Office:

Redvers Consulting Ltd
16-18 Woodford Road,
London E7 0HA,
UK

Tel: +44 (0)208 522 7404

Accounts Office:

Redvers Consulting Ltd
1st Floor, 48 Dangan Rd,
London E11 2RF,
UK

Tel: +44 (0)870 922 0633

German Office:

Redvers Consulting Ltd
Scharfeneckweg 2,
50739 Köln,
Deutschland

Tel: +49 (0)221 1704 9000