Redvers Consulting Ltd

Redvers COBOL Signature

Das „Redvers COBOL Signature" Softwarepaket enthält die Funktionen Digital Signature Standard (DSA) und Elliptic Curve Digital Signature Algorithm (ECDSA) und verwendet asymmetrische Verschlüsselung mit OAEP-Padding.

Merkmale:

- Der gesamte Code ist 100% reines COBOL
- Läuft auf jedem Rechner, der COBOL ausführen kann
- Unterstützt DSA- und Elliptic Curve (ECDSA)- Signaturen
- Entspricht PKCS # 1 v2.2: RSA Kryptographiestandard
- Unterstützt öffentliche/private Schlüssel mit bis zu 4096 Bit in Hex oder Base64
- Wird als COBOL Quellprogramm lizensiert
- Effizient, professionell und skalierbar
- Kann im Batch-Modus oder Online (z.B. CICS) aufgerufen werden
- **Kostenlose 30-Tage-Demoversion**

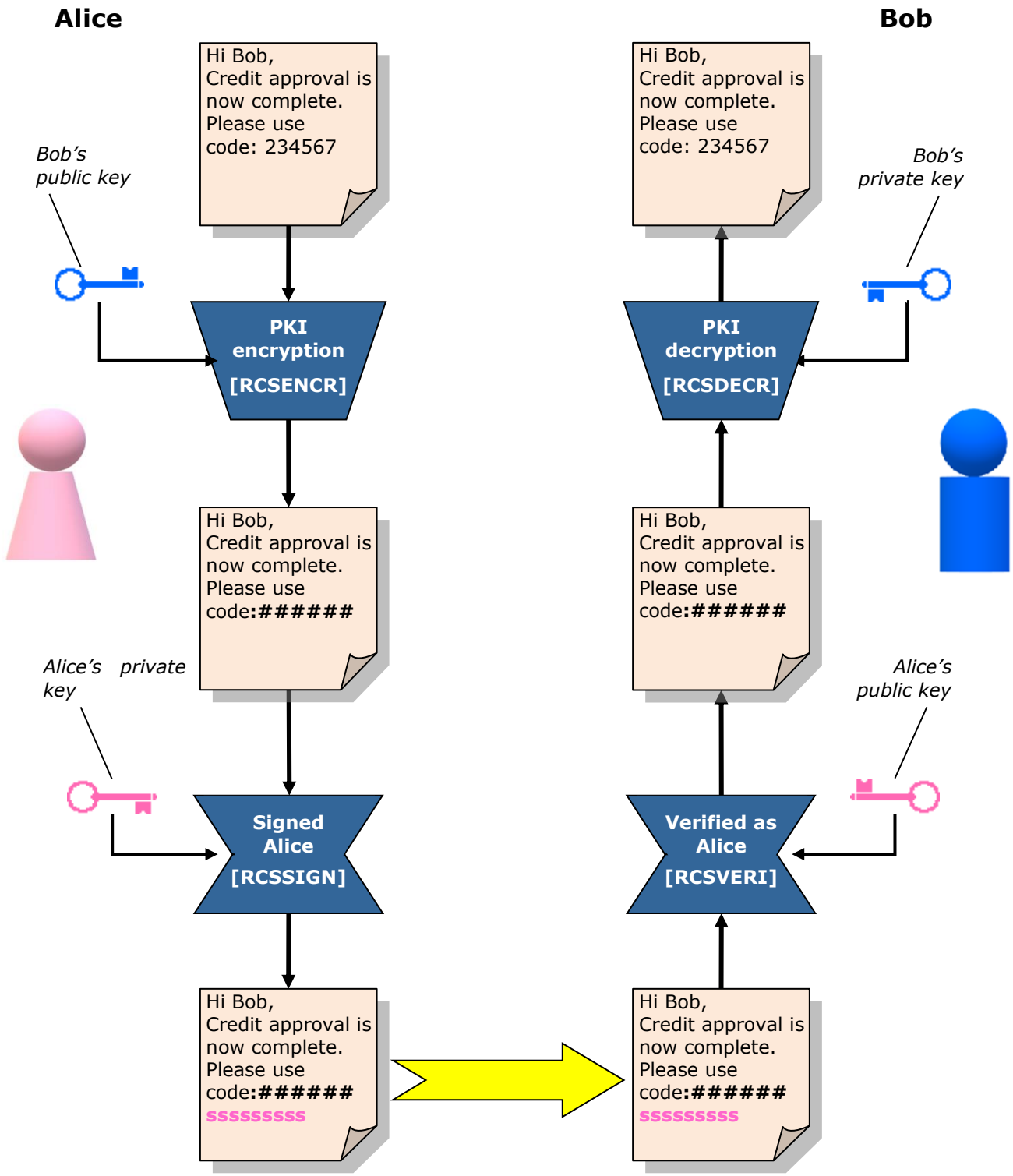
DSA-Signaturen werden gemäß NIST FIPS PUB 186-4 Digital Signature Standard erstellt und überprüft. ECDSA-Signaturen entsprechen ANSI ANS X9.62-2005 Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA). Digitale Signaturen gewährleisten die Identität des Absenders und bestätigen, dass die empfangenen Daten nicht durch unerlaubte Aktivitäten geändert wurden.

Die PKI-Verschlüsselungs- und OAEP-Auffülllogik entspricht den in den RSA Laboratories bereitgestellten Algorithmen PKCS #1 v2.2: RSA Cryptography Standard. Insbesondere werden RSAEP/RSADP zur Verschlüsselung/Entschlüsselung verwendet, und das RSA-OAEP-Auffüllen mit MGF1 wird zum Auffüllen und zur Maskenerzeugung verwendet. Bei der PKI-Verschlüsselung werden gemäß den Sicherheitsanforderungen der Anwendung öffentliche und private Schlüssel verwendet.

Die erforderliche Sicherheitsstufe für die Erzeugung / Verifizierung digitaler Signaturen und die PKI-Kryptografie hängt von der Länge der öffentlichen / privaten Schlüssel sowie von SHA-1- oder SHA-2-Hashing-Algorithmen ab. Schlüsselgrößen und Hash-Digest-Längen werden von der aufrufenden Anwendung angegeben, um sicherzustellen, dass die richtige Sicherheitsstufe beibehalten wird.

Überblick über die Funktionsweise

Das folgende Diagramm zeigt, wie vertrauliche Informationen mit das „**Redvers COBOL Signature**" Software verschlüsselt, signiert, gesendet, verifiziert und entschlüsselt werden können:



Die Redvers Signature Software führt standardmäßige Algorithmen für digitale Signaturen und asymmetrische Verschlüsselung aus, sodass Signaturen und Chiffretext von externen Institutionen überprüft und entschlüsselt werden können.

Technische Informationen

Das „**Redvers COBOL Signature**“ 2.2-Softwarepaket besteht aus:

- Ein Beispiel für ein aufrufendes COBOL-Programm (**RCSSAMP**).
- Vier zusätzliche Anwendungsprogramme zum verschlüsseln (**RCSENCR**), entschlüsseln (**RCSDECR**), unterschreiben (**RCSSIGN**) und überprüfen (**RCSVERI**).
- Zwei Unterprogramme von Redvers Consulting (**RCSCALC** und **RCSHASH**).

Alle diese Programme sollten in die Standard-Quellcodebibliothek kopiert und kompiliert werden. **RCSSAMP** muss zuletzt kompiliert und gelinkt werden, bevor die Ausführung des Testprogramms gestartet wird.

„**Redvers COBOL Signature**“ Programme können auf Plattformen mit EBCDIC- oder ASCII-codierten Zeichen unter Verwendung von Big- oder Little-Endian-Binärformaten ausgeführt werden. Der Datenaustausch zwischen Unterroutinen verwendet einen gemeinsamen Kommunikationsblock, der linksbündige, mit Leerzeichen gefüllte Parameter im Hexadezimal- oder Base64-Format enthält. Alle Unterprogramm-Speicherbereiche, die vertrauliche Informationen enthalten, werden initialisiert, bevor die Steuerung an die aufrufende Anwendung zurückgegeben wird.

In der Software ist das Redvers-Rechner-Unterprogramm **RCSCALC** enthalten. Diese Routine führt die modulierten Exponentialberechnungen, modularen Inversfunktionen, Skalararithmetik und Datenkonvertierung innerhalb der Verschlüsselungs-/Signaturprozesse durch. Ebenfalls enthalten ist die Redvers-Hashing-Subroutine **RCSHASH**, auf der die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512 ausgeführt werden. **RCSCALC** und **RCSHASH** können von Kunden kostenlos für andere technische Anwendungsanforderungen verwendet werden.

Wenn Schlüssellängen oder Algorithmen erforderlich sind, die derzeit nicht in den Parametern des rufenden Programms aufgeführt sind, wenden Sie sich an Ihren Kundenberater oder fordern Sie auf unserer **Kontaktseite** eine Anpassung an.

Das Produktangebot

Eine Dauerlizenz für das „**Redvers COBOL Signature**” kann für eine einmalige Gebühr erworben werden. Alternativ kann die Software auch gemietet werden für eine jährliche Gebühr, die 20% des Betrags der Dauerlizenz beträgt.

Für diesen Betrag erhalten Sie:

- den Quellcode (verschlüsselt)
- Beispiel für rufende Programme
- Handbücher
- eine unternehmensweit gültige Softwarelizenz
- Geld-zurück-Garantie
- Softwareupgrades und Support per E-Mail*

Zusätzliche Optionen:

- telefonischer Support rund um die Uhr
- Software Escrow / Quellcodehinterlegung bei Software Escrow Solutions.

Die aufgeführte Software und Handbücher werden als Textdateien und PDF E-Mail-Anhänge geliefert, wenn keine abweichenden Vereinbarungen getroffen wurden. Sie werden installiert, indem Sie den Quelltext manuell in Ihre COBOL Quelltextbibliothek kopieren, und dann mit Ihrem üblichen Compiler kompilieren und linken.

Ausführliche Informationen zu den Preisen finden Sie auf:
https://www.cobol.de/cobol_signature_pricing.php

*Kostenlos für das erste Jahrmit einer geringen jährlichen Folgegebühr.

Über Redvers Consulting

Redvers Consulting bietet seit 1988 erstklassige Produkte und Dienstleistungen für COBOL-Anwendungen. Unser Ansatz, die Software als Quellcode auszuliefern, ermöglicht unseren Kunden die Erfüllung ihrer geschäftlichen Anforderungen mit einer zuverlässigen, effizienten und perfekt integrierten Lösung.

Unsere Kunden sind überwiegend große Finanzdienstleister in Großbritannien und den USA. In zunehmendem Maße sind wir im deutschsprachigen Raum und auch in anderen Branchen tätig.

Da unsere Software als verschlüsselter Quellcode ausgeliefert wird, bieten wir Unterstützung für alle Hardwareplattformen und Betriebssysteme, für die ein COBOL-Compiler existiert - EBCDIC, ASCII, big endian und little endian.

Einige unserer Kunden:

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)
Landesbank Hessen Thüringen (DE)
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)

Kontakt: https://www.cobol.de/contact.php

Deutsches Büro:

Redvers Consulting Ltd
Scharfeneckweg 2,
50739 Köln,
Deutschland

Tel: +49 (0)221 1704 9000

Hauptbüro:

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

Tel: +44 (0)870 922 0633

Entwicklungsbüro:

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

Tel: +44 (0)208 522 7404