

The Cincom Smalltalk™ VisualWorks® Security Library

WHITE PAPER

Cincom in-depth analysis and review



SIMPLIFICATION THROUGH INNOVATION™



The Cincom Smalltalk VisualWorks Security Library

WHITE PAPER

Cincom in-depth analysis and review

Table of contents

| | |
|---|---|
| The need for data security | 1 |
| Cryptographic algorithms in VisualWorks | 1 |
| Cryptographic mechanisms in VisualWorks | 4 |
| Security frameworks in VisualWorks | 5 |
| Developing security applications in VisualWorks | 5 |
| Advantages of the VisualWorks security library | 6 |



The Cincom Smalltalk VisualWorks Security Library

The need for data security

Software developers are often required to add security features to their software to augment network security. The purpose of this extra security is to protect the integrity and ensure the privacy of sensitive data on a level that security applications such as firewalls on the network perimeter cannot. Not all data can be locked away. Sometimes it must be subject to public access, or transported across the internet via e-mail or web transactions. In these cases, the data is susceptible to access and tampering by unauthorized individuals. In addition, data within the protected confines of the enterprise is always vulnerable to internal access by unauthorized users misusing administrative privileges.

Encryption is an ideal method to protect confidentiality of data, no matter where it is stored or transported. The process converts data into an unreadable format, and then decrypts data by converting it back to the original readable data, only when accessed by an authorized user.

A wide range of practical cryptography and related security components have been implemented within VisualWorks to enable developers to quickly and easily incorporate a variety of security capabilities into their applications.

Cryptographic algorithms in VisualWorks

Encryption methods use an algorithm, also called a cipher, to perform encryption and decryption. These algorithms use a "key" to convert data into apparently random pieces, and to reassemble the data for access by authorized users. VisualWorks supports both of the common methods of encryption: symmetric key encryption, also called secret key encryption, and asymmetric key encryption, also called public key encryption. In addition, VisualWorks supports several hash algorithms, which represent another class of fundamental cryptographic algorithms.

Secret key encryption algorithms

In secret key encryption, the sender and receiver must have a single shared key set up in advance and kept secret from all other parties. The sender and the receiver use the same key for encryption and decryption.

The VisualWorks security library includes two types of secret key ciphers: block and stream. Block ciphers encrypt one full, fixed-size block at a time, and stream ciphers encrypt one byte at a time.

Block cipher implementations

VisualWorks provides implementations of three standard block ciphers:

AES: Advanced Encryption Standard (AES) is the National Institute of Standards (NIST) cipher (FIPS 197) based on the Rijndael algorithm. It is intended as a replacement for the DES standard (FIPS 46). AES encrypts 16-byte blocks and its key is 16, 24 or 32 bytes long.

Blowfish: Blowfish is a secret key block cipher providing a fast, free alternative to existing encryption algorithms. Blowfish was designed to work as a drop-in replacement for DES and IDEA encryption. Blowfish encrypts 8-byte blocks, and it takes a variable-length key from 32 bits to 448 bits.

DES: Digital Encryption Standard (DES) was the most common encryption during the 1980s, and although it has been increasingly supplanted by newer encryption schemes, such as AES, it remains a common encryption scheme. DES encrypts 8-byte blocks, and it takes a 56-bit (7-byte) key. This encryption standard is generally not recommended for new applications, and it should only be used for backward compatibility with legacy protocols and applications.

Stream cipher implementations

Stream ciphers operate on a single byte at a time. Using a key as seed, a random number generator (RNG) creates a key stream, which is used to encrypt the data. The same key stream is generated to decrypt the stream.

VisualWorks provides implementations of the popular ARC4 stream cipher.

ARC4: ARC4 uses a variable-length key up to 256 bytes. Beyond that, additional bytes are ignored. The algorithm generates a key stream from the key, which is then used for encryption and decryption.

Public key encryption algorithms

In public key encryption, there are two separate keys. A public key is published and enables any sender to perform encryption, while a separate private key is kept secret by the receiver to perform decryption. With this encryption method, the public key can be freely distributed, without concern about who has access.

Separate keys offer a significant advantage over secret key algorithms, because the private key does not need to be shared at all, significantly reducing the chance the key will be compromised. Moreover, the same key pair can be used for communication with many parties, who would otherwise require many different secret keys, posing a difficult key management challenge.

Public key algorithms are significantly slower than secret key algorithms, however, and therefore are rarely used directly for data encryption. Instead, public key algorithms are usually used in tandem with secret key algorithms. First, a random secret key is generated and used to encrypt the data. Then, the secret key is encrypted using the public key algorithm and attached to the encrypted data. Only the holder of the corresponding private key can recover the secret key and decrypt the data.

Public key algorithms can also be used for digital signatures to authenticate communication and to ensure data integrity. A digital signature employs public key cryptography to validate the source of a document and to provide evidence as to whether a document was tampered with.

The VisualWorks security library offers three standard implementations of public key algorithms including DSA, RSA and the DH key agreement.

Digital Signature Algorithm (DSA)

DSA is a public key algorithm developed by the United States government and is used only for creating digital signatures. DSA does not encrypt or decrypt data.

RSA algorithm

RSA is a public key algorithm that can be used for both encryption and digital signing. It is often used to encrypt the key for a secret key algorithm, while the secret key is used to encrypt and decrypt the actual data. The encrypted data and encrypted key constitute a "digital envelope."

RSA can also be used for digital signing of a message. A message encrypted with a private key constitutes a digital signature because only the holder of that private key could have produced that encrypted message, provided the key has been kept secure. The corresponding public key is used to verify the signature, and since the key is public, anyone is able to perform this test.

Diffie-Hellman (DH) key agreement

DH is a public key algorithm that does not encrypt or sign a message. Instead, it allows remote parties to establish a shared secret value over an unprotected channel by exchanging public information. From that shared secret value, the two parties each create a secret session key to use for encrypting and decrypting a message.

Hash algorithms

Secure hash algorithms provide a fingerprint that uniquely identifies data. These algorithms are used to verify file integrity. By storing a hash of the file and periodically rehashing the file and comparing the digests, the user can determine if the file has been modified. Hashes are also used to generate a message digest for message authentication, and they can be employed by a pseudo random number generator (PRNG).

VisualWorks provides implementations of the popular MD5 and SHA hash algorithms, in the classes MD5, SHA (implementing SHA-1) and SHA-256 (implementing 256-bit SHA).

MD5

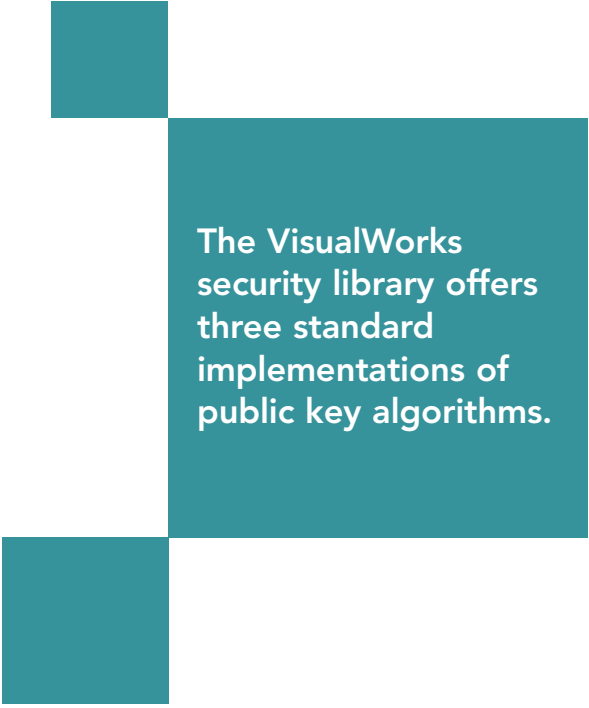
The MD5 algorithm produces a 16-byte (128-bit) message digest used to validate data integrity.

SHA

The SHA-1 algorithm produces a 160-bit message digest and is therefore considered a stronger algorithm than MD5. SHA-1 is utilized in a broad range of popular security applications and protocols.

SHA-256

The SHA-256 hashing algorithm extends the size of the digest to 256 bits for heightened security.



The VisualWorks
security library offers
three standard
implementations of
public key algorithms.

Cryptographic mechanisms in VisualWorks

Cryptographic algorithms presented in the previous section are used to build higher-level mechanisms for specific security objectives. The VisualWorks security library also offers a variety of other mechanisms including hash-based message authentication, pseudo random number generators, password-based cryptography and secure storage of private keys.

HMAC

HMAC, or hash-based message authentication code, is an extension of the SHA or MD5 secure hash algorithms used for validating the integrity of a message using a shared secret key. In VisualWorks, HMAC uses either MD5 or SHA-1 hashing algorithms.

DSSRandom PRNG

Many operations involved in cryptographic security rely on secure random values. For example, generating secure keys for secret and public key ciphers relies on a high-quality random number generator or pseudo random number generator. The security of generated keys is based on the quality of the generators.

For security applications, VisualWorks offers the DSSRandom PRNG, which implements the algorithm specified in the DSS standard (FIPS 186-2). DSSRandom, a cryptographically strong PRNG suitable for use in secure applications, is an implementation of the random number generator for the Digital Signature Algorithm.

PKCS5: password-based cryptography

Many applications use passwords as part of the security system. PKCS5 is the RSA recommendation for a password-based encryption standard, which is implemented in VisualWorks in the PBC class.

PKCS5 applies to both message encryption and message authentication. The VisualWorks implementation includes both encryption and message authentication and implements both version 1 and version 2 of the recommendation. Version 1 is recommended only for compatibility with old applications, and version 2 is recommended for all new applications.

PKCS8: secure storage of private keys

PKCS8 is used to store RSA or DSA private keys in a file using a format specified by the Public Key Cryptography Standard (PKCS) #8 and encrypts it using a password. This standard format for private keys can be used to import or export keys to be used in other applications.



Security frameworks in VisualWorks

VisualWorks also supports several standard security frameworks including SSL protocol, X.509 certificates and ASN.1.

SSL protocol

Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting data securely via the internet. VisualWorks provides full support for the use of SSL to secure application communications.

X.509 certificates

Authentication of a public key is performed using X.509 certificates. The VisualWorks security library allows for easy integration of X.509 certificates into any application.

ASN.1

ASN.1 defines standard methods of encoding arbitrary data in bytes so that they can be stored in a file or transferred over a network connection between communicating applications. ASN.1 is used in many of the RFCs that define internet protocols. For example, the structure of X.509 certificates is defined using ASN.1.

Developing security applications in VisualWorks

Developers can use the components in the VisualWorks security library to:

- Secure web communications
- Secure e-mail protocols and messages
- Keep data confidential
- Ensure data integrity
- Authenticate communicating parties
- Sign application code

In addition, VisualWorks provides out-of-the-box support for the HTTPS protocol to secure web communication via the SSL framework available in the VisualWorks security library. This feature can be used transparently, in the same way VisualWorks is used to establish an HTTP connection, automatically integrating the SSL framework for security.

VisualWorks provides out-of-the-box support for the HTTPS protocol to secure web communication via the SSL framework available in the VisualWorks security library.

Advantages of the VisualWorks security library

Cross-platform portability

Security applications in VisualWorks benefit from the environment's portability across a wide range of platforms. Applications developed in VisualWorks can run on Windows, Linux, UNIX, Mac OS/X and even mobile platforms like Windows CE – without requiring any modification to the code.

Ease of use

The VisualWorks security library and the entire environment are easy to learn and use. Security components simply plug into any application and work together automatically. Changes to applications can be made effortlessly at any point in the development cycle without impact, and developers even have the option to universally apply changes throughout an application in real time.

Simple API

The VisualWorks API is designed to be as straightforward and simple as possible.

Speed

Developers can develop, test and deploy security applications in VisualWorks in a fraction of the time required by other development environments.

Comprehensive coverage

The VisualWorks security library offers extensive coverage of security components, delivering all the tools a developer needs to secure applications.

Built for Smalltalk

The components in the VisualWorks security library are completely implemented in Smalltalk, built specifically for the VisualWorks environment. Developers have all the source code at their fingertips, making VisualWorks security components easy to plug into any application, debug and reuse.

Quality of implementation

All the components in the VisualWorks security library are designed by Smalltalk experts with the level of quality Cincom and VisualWorks are known for.

Compliance

All components in the VisualWorks security library are built to comply with the latest security standards.

Cincom support

VisualWorks security components are backed by Cincom's commitment to serving the Smalltalk community with the highest-quality development tools and 24/7/365 technical support.

Cincom, the Quadrant Logo, Cincom Smalltalk, VisualWorks, and Simplification Through Innovation are trademarks or registered trademarks of Cincom Systems, Inc. All other trademarks belong to their respective companies.

© 2006 Cincom Systems, Inc.
FORM CS060421-2 5/06
Printed in U.S.A.
All Rights Reserved

World Headquarters • Cincinnati, OH USA • US 1-800-2CINCOM
Fax 1-513-612-2000 • International 1-513-612-2769
E-mail info@cincom.com • www.cincom.com • <http://smalltalk.cincom.com>

