



SafeDoXX for Safe EXIM User Manual

SafeScript Limited.

© 2004 SafeScript Limited. All rights reserved.

Printed in India.

Publication date: 07 February 2004

SafeDoXX for Safe EXIM Version 1.0 User Manual

Trademark Notices

SafeDoXX™ and SAFE EXIM™ are registered trademarks of SafeScript Limited. Other trademarks and service marks in this document are the property of their respective owners.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photographic, audio, or otherwise) without prior written permission of SafeScript Limited. Notwithstanding the above, permission is granted to reproduce and distribute this document on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete form with attribution of the document to SafeScript Limited

Note: This document may describe features and/or functionality that are not present in your software or your service agreement. Contact your sales representative to learn more about what is available with this SafeScript product.

TABLE OF CONTENTS

I. Getting Started.....	1
A. What is SafeDoXX for Safe EXIM?	1
B. Who can use SafeDoXX for Safe EXIM?	1
C. What should I do with a Digitally Signed file?.....	1
D. What does DGFT do with a Digitally Signed file?.....	1
II. Before you start using SafeDoXX for Safe EXIM.....	2
III. Hardware and Software Requirements	2
IV. How do I Install SafeDoXX for Safe EXIM	2
V. How do I Un-Install SafeDoXX for Safe EXIM.....	5
VI. How do I Digitally Sign a file with SafeDoXX for Safe EXIM?	5
VII. Log Files	6
VIII. Frequently Asked Questions (FAQ's).....	7

I. Getting Started

A. What is SafeDoXX for Safe EXIM?

SafeDoXX for Safe EXIM is an easy-to-use Desktop Utility that enables Digital Signing of any File using a Safe EXIM Digital Certificate.

Today, the Indian legal framework accords the same significance to Digital Signatures on electronic documents as physical signatures on paper documents. Therefore, a user in India can leverage the benefits offered by the Indian Information Technology Act 2000 (IT Act 2000) by Digitally Signing electronic documents in lieu of traditional physical signatures and enjoy the same legal status as physical signatures, provided the Digital Certificate used has been issued by a licensed Certifying Authority.

B. Who can use SafeDoXX for Safe EXIM?

SafeDoXX for Safe EXIM can be used by Import and Export (EXIM) organizations that are registered with the Directorate General of Foreign Trade (DGFT) and have a valid Importer-Exporter Code (IEC). The EXIM organization is required to nominate an Authorized Employee to interact with the DGFT on behalf of the EXIM organization. This authorized employee would have SafeDoXX for Safe EXIM installed on his/her computer, with which he/she would Digitally Sign documents for upload on the DGFT website.

C. What should I do with a Digitally Signed file?

EXIM organizations are required to file several documents with the DGFT while applying for their duty-drawback licenses. Since DGFT permits the EXIM organizations to apply for their licenses online, DGFT has also permitted the EXIM organizations to send these accompanying documents electronically.

However, DGFT has stipulated that these electronic documents need to be Digitally Signed before they are uploaded onto the DGFT website.

Therefore, when applying online for their licenses, the EXIM organizations would need to use SafeDoXX for Safe EXIM to Digitally Sign all the accompanying documents and upload them to DGFT through their website.

D. What does DGFT do with a Digitally Signed file?

DGFT has incorporated an application on their website that automatically verifies the Digital Signature on a Digitally Signed file. This ensures that only documents Digitally Signed by a valid EXIM organization can be uploaded to DGFT through their website.

Once the Digitally Signed file is uploaded on DGFT's website, DGFT checks to see if the Digital Signature is valid, that the sender is authentic and that the original document has not been tampered with. DGFT then processes these documents for issuance of the licenses.

To find out more about Digital Certificates and Digital Signing, please read the FAQ section at the end of this document or visit <http://safeexim.safescrypt.com>.

II. Before you start using SafeDoXX for Safe EXIM

Step 1: Ensure that you have the USB Token software and drivers installed on your computer. Refer section 'Hardware and Software Requirements' for more details

Step 2: Ensure that you have a registered copy of SafeDoXX for Safe EXIM installed on your computer. Refer section 'Hardware and Software Requirements' for more details.

Step 3: Ensure that you have obtained your Safe EXIM Digital Certificate from SafeScript Ltd.

III. Hardware and Software Requirements

The supported configurations for Hardware are: -

Intel-based PC, 133Mhz Pentium or faster

- Windows 98 running browser Internet Explorer 5.5+
- Win 2000 running browser Internet Explorer 6.0+
- WIN XP

-Internet Explorer with the above stated versions must support 128 bit Cipher Strength

- Min 32MB RAM
- Min 50MB free disk space

Hardware Support

- USB Port Token or Smart Card

IV. How do I Install SafeDoXX for Safe EXIM

Prior to installation ensure that all the required hardware and software components are installed.

- Insert the Safe EXIM CD in the CD-ROM drive of your system
- The user must navigate to the SafeDoXX for Safe EXIM directory on the CD and double click the executable file to start the installation. The installation wizard will guide you through the installation process
- After the installation is complete, a Registration Screen will be displayed. **Step 1** in this screen helps you generate the **Product Serial Number**. This is a 12 digit alpha-numeric code. Refer Image 1.

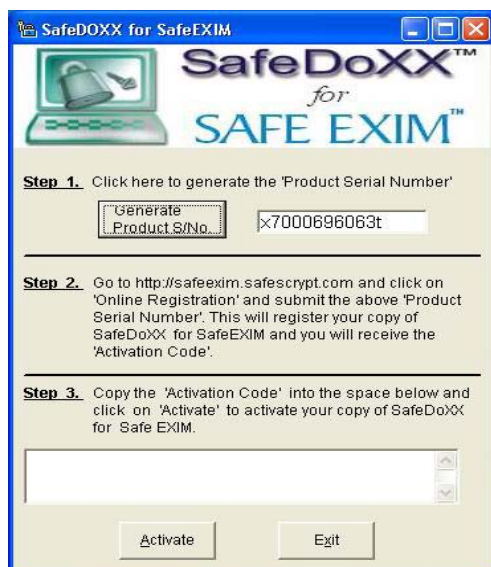



Image 1

- Please also keep the 16 digit **Token Redemption Number** from your Safe EXIM pack ready with you
- Visit the Online Registration page at <http://safeexim.safescrypt.com> and submit this Product Serial Number, the Token Redemption Number and your E-mail ID. Refer Image 2

SafeDoXX for Safe EXIM Online Registration



Please submit the required details below to
Register your copy of SafeDoXX for SafeEXIM

Product Serial Number * required	<input type="text"/>	The Product Serial Number is the number generated when you installed SafeDoXX for SafeEXIM. This number is case sensitive.
Token Redemption Number * required	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	The Token Redemption Number is the 16 digit number on the inside jacket of your SafeEXIM CD Cover. This number is case sensitive.
Email ID * required	<input type="text"/>	Your product Activation Code will be sent by E-mail to this ID. Please ensure that the E-mail ID is correct.
<input type="button" value="Register"/> <input type="button" value="Reset"/> <input type="button" value="Back"/>		

Image 2

- If successful, the Online Registration page will display a 128-character product **Activation Code**. Step 3 of the Registration Screen will have a text box where you must copy this Activation Code into SafeDoXX for Safe EXIM. Then click on the "Activate" button. The Activation Code will also be sent to you via e-mail. Refer Image 3.

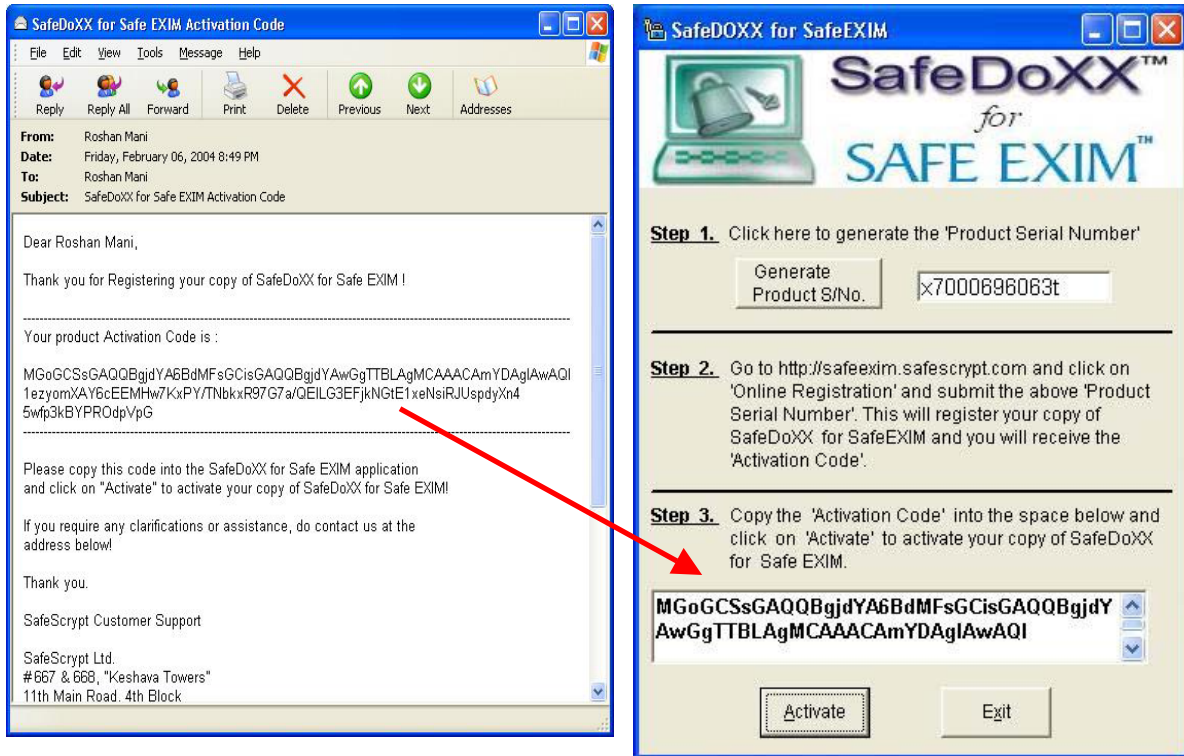


Image 3

- This will ensure that you have a licensed version of SafeDoXX for Safe EXIM. Without this registration step, SafeDoXX for Safe EXIM cannot be used. Refer Image 4

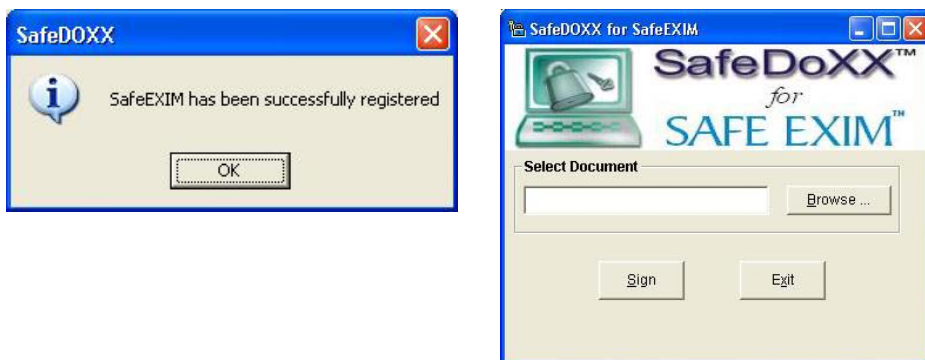


Image 4

- Once installation is complete, you may be asked to **restart** your computer. It is recommended that you restart your computer

V. How do I Un-Install SafeDoXX for Safe EXIM

When you uninstall SafeDoXX for Safe EXIM, please remember that if you need to reinstall and reuse the application, you will need to contact SafeScript and obtain an additional Registration Code. Without the registration step, SafeDoXX for Safe EXIM cannot be used.

Steps to Uninstall SafeDoXX for Safe EXIM

- Click on Start => Settings => Control Panel => Add and Remove Programs => Select SafeDoXX for Safe EXIM and click on "Add/Remove" button.
- Install Shield wizard will open. Select Remove and click on next to uninstall. You will get a message box "Do you want to completely remove the selected application and all of its components" Click on "Yes" on this message box to complete the uninstallation.

VI. How do I Digitally Sign a file with SafeDoXX for Safe EXIM?

1. Ensure that you have stored your Safe EXIM Digital Certificate on your USB Token and that the USB token is plugged into the USB port of your computer before you begin the Signing operation
2. Start SafeDoXX for Safe EXIM and click on the "Browse" button to select the file you want to Digitally Sign. Refer Image 5.

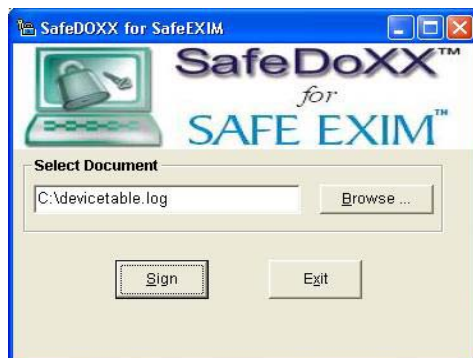


Image 5

3. Click on the "Sign" button to start the signing operation.
4. Select your Safe EXIM Digital Certificate from the certificate store. Refer Image 6.



Image 6

5. Enter the password to your USB Token and click OK. Refer Image 7.



Image 7

6. Please wait while the Signing operation is completed.
7. Once the signing operation has been completed, a message box will be displayed that indicates the name and path of the digitally signed file. Refer Image 8.

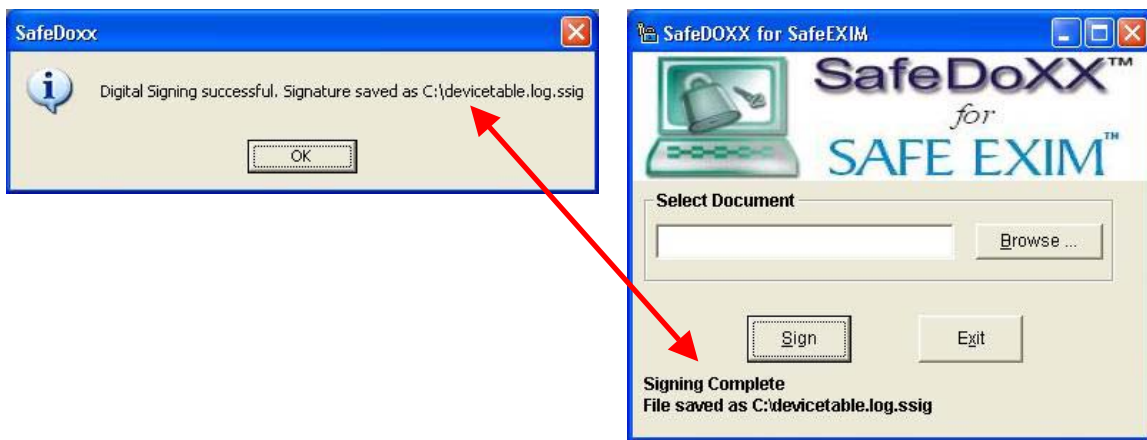


Image 8

8. Your Digitally Signed file will be stored in the same path as the original file and will have an extension of ".ssig"

Note: Your certificate store may hold more than one digital certificate. However, SafeDoXX for Safe EXIM will work only with a Safe EXIM Digital Certificate obtained from SafeScript Ltd.

VII. Log Files

SafeDoXX for Safe EXIM creates a Log File that logs all errors generated during the operation of SafeDoXX. This file is a text file and is stored in the same directory where SafeDoXX has been installed. To view the error log file at any time, navigate to the Installation Directory of SafeDoXX and locate the error file. Double click this file to open the log file in Windows Notepad.

If you would like to Backup your error log file, please make a copy of this log file in another location on your computer.

VIII. Frequently Asked Questions (FAQ's)

Challenges for Security

There are various challenges related to the security of electronic transactions:

- i. Confidentiality
- ii. Authentication
- iii. Integrity
- iv. Non-repudiation
- v. Interoperability / Universality

Confidentiality:

You want to be sure the information you are sending, such as credit card information when purchasing goods online, or sensitive business information in e-mail can't be read by anyone other than the intended recipient.

Integrity

You want to make sure no one has intercepted information and changed it in any way. So tampering of the information by anybody should be difficult and evident.

Authentication

You want to be able to check on the identity of users. For example, you wouldn't want a competitor to download your company information from an Extranet, or in the case of a very large financial transaction, you want to feel certain of who placed the order. As a user, you also want to be certain if you are buying goods from an online store, that the store is legitimate, and that you'll actually get the goods you are paying for.

Non-repudiation

In the real world, a contract with a written signature is generally binding. There is no real equivalent on the Internet. Someone might buy some stock over the Internet, the price falls, and then they say they never placed the order. There isn't a way to sign a contract electronically except with a certificate.

Interoperability

Finally, whatever solution you have needs to be interoperable and universal, because the benefits of this model is that everyone can work together and share information across the network transparently. The adoption of standards by Internet vendors has provided this interoperability.

What is PKI?

PKI essentially addresses just these challenges for secure electronic transactions.

A PKI (public key infrastructure) enables users of a basically non-secure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair. This key pair is obtained and shared through a trusted authority. Public key infrastructure provides **digital certificates** that identify individuals or organizations and directory services that store and, when necessary, revoke these certificates. Public key infrastructure uses **public key cryptography**, which is the most common method on the Internet for authenticating a message sender or encrypting and decrypting a message. This is also sometimes referred to as asymmetric cryptography. PKI provides users with a means of conducting electronic transactions and electronic correspondence that ensures confidentiality, integrity of information, authentication, access control, and non-repudiation.

Types of cryptography

Symmetric Key Cryptography

Symmetric, or secret key, cryptography is where you use the SAME "key" (think of this as a mathematical formula) to both encrypt and decrypt data. This is the kind of cryptography used in WW-II, where code was "cracked" by the enemy so confidential information about troop movements could be gathered. To summarize Symmetric Key Cryptography Assuming to users Bob and Alice, if Bob wants to send Alice an encrypted messages · Bob has one secret key · If Alice wants to send Bob a secret message · Bob Sends Alice a copy of his secret key · Alice encrypts message with Bob's secret key · Bob decrypts message with his secret key

Problems:

1. How does Bob get secret key to Alice?
2. What if Alice is a double agent?
3. What if Alice, Bob, Charley, & Dan need to exchange messages? Need n! Keys

With single-key cryptography you have the problems of how to share the secret key -- how does Bob get the secret key to Alice safely, and of managing a large number of secret keys. Moreover if too many people share the same secret key, then if even one of them is bad, a mole, all messages are compromised. So A Better method: Public Key Cryptography

Public Key Cryptography

In public key cryptography, public and private keys are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory). Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it

What is a Digital Certificate?

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a Certification Authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signature), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

Certification Authority

A certificate authority (CA) is an authority that works as a trusted third party to validate the identity of a user/organization, and issues certificates attesting to the identity of the user/organization. Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

What is a Digital Signature?

A digital signature functions for electronic documents like a handwritten signature does for printed documents. The signature is an un-forgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming the signature was forged.

In other words, digital signatures enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message

A Digital ID is issued by a Certification Authority (CA) and signed with the CA's private key.

A Digital ID typically contains at a minimum, the Owner's public key, Owner's name, Expiration date of the public key, Name of the issuer (the CA that issued the Digital ID), Serial number of the Digital ID and Digital signature of the issuer. The most widely accepted format for Digital IDs is defined by the CCITT X.509 international standard; thus certificates can be read or written by any application complying with X.509. Further refinements are found in the PKCS standards and the PEM standard.

In other words, digital signatures enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message

How legal is it all?

India is one of a select band of nations that has Digital Signature Legislation. The Act grants Digital Signatures issued by a licensed Certifying Authority in India the same status as a Physical Signature. The technology specified to deploy Digital Signatures is Public Key Infrastructure (PKI).

What is a Certification Revocation List (CRL)?

The CRL is a list of subscribers paired with digital certificate status. A CRL allows clients and servers to check whether the entity they are dealing with has a valid certificate. The CRL is a binary file and contains the following information: A list of revoked certificates and the reason for their revocation, The issuer of the CRL, When it was issued · When the next version of the CRL will be published The CRL is created and published on a periodic basis, often determined by settings in the CA software. You must have the current CRL when verifying signatures or encrypting data. As the CRL is a file, your application must retrieve a new CRL if the copy on its local system is outdated.

What is a Cryptographic Service Provider?

The Cryptographic Service Provider (CSP) is the software that generates the public/private key pair, which is the basis of digital certificate technology. The CSP also performs all cryptographic operations such as encryption and digital signature.

What is an Algorithm?

The term algorithm (pronounced al-go-rith-um) is a procedure or formula for solving a problem. A computer program can be viewed as an elaborate algorithm. In mathematics and computer science, an algorithm usually means a small procedure that solves a recurrent problem.

What is a hash algorithm?

A hash function is a math equation that uses text (such as an e-mail message) to create a code called a message digest. Examples of well-known hash functions are MD4, MD5, and SHA. A hash function used for digital authentication must have certain properties that make it secure enough for cryptographic use. Specifically, it must be infeasible to find: · Text that hashes to a given value. That is, if you know the message digest, you should not be able to figure out the message. · Two distinct messages that hash to the same value The ability to find a message that hashes to a given value would enable an attacker to substitute a fake message for a real message that was signed. It would also enable someone to falsely disown a message by claiming that he or she actually signed a different

message hashing to the same value, thus violating the non-repudiation property of digital signatures. The ability to find two distinct messages that hash to the same value could enable an attack whereby someone is tricked into signing a message that hashes to the same value as another message with a quite different meaning.

SHA1

The Secure Hash Algorithm (SHA), the algorithm specified in the Secure Hash Standard (SHS, FIPS 180), was developed by NIST is a revision to SHA that was published in 1994; the revision corrected an unpublished flaw in SHA. SHA-1 is also described in the ANSI X9.30 (part 2) standard. The algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5 but the larger message digest makes it more secure against brute-force collision and inversion attacks.

MD5

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is unique to that specific data as a fingerprint is to the specific individual.

What is a message digest?

A message digest is the results you get when you run text (such as an e-mail message) through a hash algorithm. A message digest concisely represents a longer message or document. You can think of a message digest as the "digital fingerprint" of a larger document. A message digest is used to create a digital signature that's unique to a particular document. A message digest does not reveal the contents of a document. That is, if you can view the message digest, you cannot figure out what the original message was. MD2, MD4 and MD5 (MD stands for Message Digest) are widely used hash functions designed specifically for cryptographic use. They produce 128-bit digests and there is no known attack faster than exhaustive search.

What algorithm does SafeDoXX for Safe EXIM use?

SafeDoXX for Safe EXIM uses the SHA1 algorithm to create the message digest of a particular document. It then uses the RSA algorithm in combination with a Safe EXIM Digital Certificate to Digitally Sign the message digest to create the Digital Signature for that particular document. These algorithms are built into SafeDoXX for Safe EXIM and are also commonly found in popular internet applications such as Internet Explorer and Netscape Navigator.

How does SafeDoXX for Safe EXIM use my Digital Certificate?

When you use a USB token to store your Digital Certificate, a copy of the public key is also maintained in the Certificate Store of the Internet Explorer browser on your computer. When performing a signing operation, SafeDoXX for Safe EXIM looks into this certificate store for your private key and finds only your public key there. However, along with the public key there will also be a corresponding registry entry that identifies the location of your private key as being in the USB Token. SafeDoXX for Safe EXIM then sends the message digest to the USB Token where the private key is used for the signing operation.

What if I can't find my Safe EXIM Digital Certificate in the Internet Explorer (IE) certificate store on my computer?

If you have installed the USB Token software and drivers properly on your computer and if you are able to view the contents of your USB Token through the Token software, then you unplug your token from your computer and plug it back in. This should cause the Digital Certificate to be copied into the IE certificate store. If you still cannot see your Digital Certificate in your IE certificate store, then login into your USB Token through the Token software, select your Digital Certificate and then do a "copy to System" operation. This will cause the Digital Certificate to be copied into the IE certificate store. If this also fails, then please contact us at SafeScript for technical assistance.

Note: During this copying operation, only the Public Key and the digital certificate are copied out of the USB Token. Your private key never leaves the USB Token at any time.

What is the size of the Digital Signature created by SafeDoXX for Safe EXIM?

Digital Signatures created with SafeDoXX for Safe EXIM increase the size of the original file by around 4 to 5 Kilo Bytes (KB's).

What happens when you Digitally Sign a file with SafeDoXX for Safe EXIM?

When you digitally sign information, you are giving the recipients the ability to determine that the contents of the document have not been altered since you signed it. In other words, data integrity is guaranteed. Even if there is a minor alteration in digitally signed information, the verification process fails, and warning recipients that the information has changed since it was signed.

In order to sign a file, you must have a public/private key pair and a certificate associated with the pair. When you sign a file, first a message digest is created of that file. A message digest is essentially a digital fingerprint of a specific file. It is created using the Hash Algorithm that you specify e.g. MD4, MD5 or SHA1. The message digest is then encrypted using your private key. The resultant file is your Digital Signature for that specific file. The signature and a copy of the original file are placed into one file. The recipient can then verify the signature to establish your identity and data integrity of the file. If the file has been altered, then the verification process fails.

What happens when you verify a Digitally Signed file?

A digitally signed file can be verified to check Data Integrity, Certificate Trust, Certificate Validity and Certificate Revocation Status.

Data Integrity: The data signed by the sender and data received by the recipient is same

Certificate Validity: The certificate has not expired

Certificate Revocation Status: The certificate is not revoked. A Certificate revocation List (CRL) is published on CA's site and the certificate is validated against it