DocuArmor

A Security Suite

Portable Security

Compact enough to fit on a **USB drive** or **Android smart phone** and carry in your pocket. DocuArmor allows the user to encrypt and decrypt files by plugging in to any PC. It also runs on laptops, desktops, servers or Android phones version 2.1 or higher.

For a very low cost carry your data with confidence and prevent unwanted eyes from stealing your secrets. Learn more...

Secure SMS Texting

Using RSA 1024 bit encryption, DocuArmorPhone users can securely exchange text messages with each other. Simply exchange public certificates and your communications are safe from unauthorized access. Learn more…

Reclaim Your Privacy

With electronic mail and digital information, we have lost the expectation of privacy. Companies and organization regard electronic mail and information as their property and feel it is their right to intercept and read/view the messages and images. Using DocuArmor, individuals can easily encrypt their information and images restricting access from unwanted eyes. A strategic minded organization can purchase enterprise cryptography promoting individual privacy while educating members to protect their electronic corporate assets. Information espionage can occur at all levels resulting in costly damages which could be avoided by protecting assets with DocuArmor cryptographic technology.

Confidential Encrypted E-Mail

Avoid the embarrassment of sending an e-mail to the wrong person. DocuArmor technology allows you to encrypt any file for a specific person. If the encrypted document is inadvertently sent to the wrong person, the unintended recipient cannot read the information. Whether sending corporate strategy or exchanging sensitive material, the delivery is protected. Learn more...

Digital Signatures and Validation

How do you know who sent you a file or if it has been tampered with in route to you? With DocuArmor you can add your digital signature to any file. This enables the recipient to validate who signed a file before accepting it to be deciphered. The signature will not match if the file has been altered. Learn more...

Secure Delete

The secure delete feature will prevent hackers from recovering information from your disk. Any non-encrypted file that has been designated as a protected digital asset needs to be securely deleted after it has been encrypted. Any backup copies represent a security exposure so these should also be encrypted or securely deleted. Learn more...

Password Protection

Files are electronically encrypted and the keys used in ciphering are password protected.

Auto Lock Up

DocuArmor will automatically lock up after a default of 10 minutes of inactivity. The lock up timeout is customizable.

Easy for ALL User Levels

The highest security with the easiest interface, drag your files to the open vault and drop it in to encrypt your data. It's that simple.

No longer will you hear about companies who purchased an encryption package but lost information anyway because it was too difficult to use and did not provide adequate functions. Learn more...

Certificate Generation & Administration

The Enterprise version of DocuArmor includes an encryption key and certificate generation tool which allows corporations/organizations to easily manage each member's keys. Learn more...

Group Keys

This enterprise only feature allows the sharing of encrypted information to a collection of users such as a department, committee, inner circle, etc. A group Key store is distributed among participants allowing an individual to encrypt a single file that each member can decipher. Learn more...

CA Key Decryption

This enterprise only feature allows the owner of the CA Keys to decipher each member's encrypted files if the CA is the issuer of the member's keys. This feature provides for data recovery and collation of user's encrypted files. You can distribute a confidential survey to members and collate and decipher them with a single root key. Learn more...

Prevention and Safeguards

- DocuArmor keeps files protected during and after transmission thus eliminating the need to implement Secure Socket Layer (SSL) Networks.
- No one can read your encrypted mail or files as long as your vault is closed or keys are unloaded.
- Protect personal information to fulfill government regulations such as HIPAA.
- Strengthen your security against information thieves and pirates.
- Protection from Identity Theft

Highest Encryption and Performance

DocuArmor uses the highest symmetric encryption standard allowable in the United States. It can be customized for international use.

DocuArmor uses AES 256-bit encryption in CTR mode to protect your confidential information. It uses a combination of asymmetric (RSA) and symmetric keys to provide protection without losing performance.

No need to unnecessarily encrypt entire disks or volumes of data.

Strategic Advantage

Allows companies to assure clients that their private information remains confidential, thus providing a competitive edge for our users.

DocuArmor provides the granularity of encrypting any file type that ***requires*** protection.

Competition and Pricing

DocuArmor is competitively priced for both the single user edition and the corporate edition which includes key management tools for an enterprise.

There are few if any competitors for this product, no one offers this much rich function for an economical price. Most competitors offer difficult and expensive solutions; Hard drive encryption, annual subscriptions for encryption keys and maintenance.

Editions

The Single User Edition allows individuals to secure and protect their private information. An Enterprise and Group Edition is available which extends the function of the Single User Edition to include certificate generation and administration. The Enterprise Edition can be purchased with or without enterprise database support.

Contact

Logical Answers Inc. also offers custom programming and support services to tailor products to your needs.

A single user license sells for only $25 (plus tax). For further information about this suite of products or for volume pricing please contact:

support@logicalanswers.com
Logical Answers Inc.
Troy, MI 48085
(248) 528-1742
web: http://www.logicalanswers.com

Portable Security

DocuArmor is architected to take advantage of the USB (Universal Serial Bus) Flash Drives and Android smart phone which are perfect for mobile professionals. Compact enough to fit on a USB drive or Android phone, carry it in your pocket and run the application directly on the phone or by plugging the USB drive in to a PC. (Works with any drive sized with at least 128 mb). DocuArmor provides the benefit of optionally separating the security keys from the files you want to protect. Using the application from an Android phone or USB drive allows the user to protect their files with confidence knowing that nobody can read them without their password protected keys.

The designed portability of DocuArmor allows the user to run the application directly on an Android phone or on *any* laptop or PC that has a USB port *without installing* the application on that PC. Additionally the user can secure files on either device and take them along. If anyone finds a lost or stolen Android phone or USB drive with DocuArmor, the secured files remain undecipherable.

Corporate volume licensing discounts are available. Each license is per user and can be installed on all their devices including desktops, laptops, Android phones and USB drives. This grants the user true mobility at an economical price.

Secure SMS Texting

DocuArmorPhone allows the user to take advantage of the SMS texting capabilities of their Android phone and exchange encrypted text message between other owners of the DocuArmorPhone app. All you need to do is exchange public certificates with other DocuArmorPhone users. Highlight and select the "**Secure Msging**" button to launch the SMS activity on your Android phone.

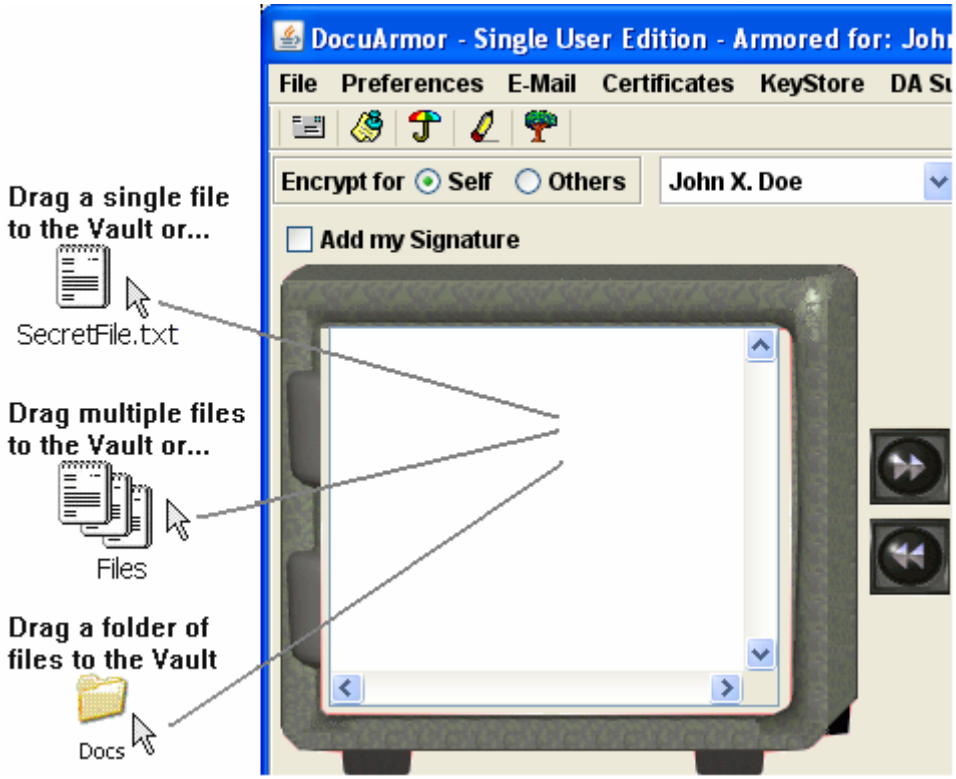
Secure Messaging Option

Secure Messaging Panel

Enter the user's phone number and message and it will be encrypted and sent. The message length is restricted to 110 characters

Easy to Use Encryption

DocuArmor allows the user to encipher files of any type such as Microsoft Word or Excel documents, pictures in any format, plain text, program and executables, etc. Simply drag a file(s) to the vault image and drop it on any point within its grey shaded area. Additionally, one can select the encrypt option under the file menu and a file prompter will appear to select a file to encrypt.



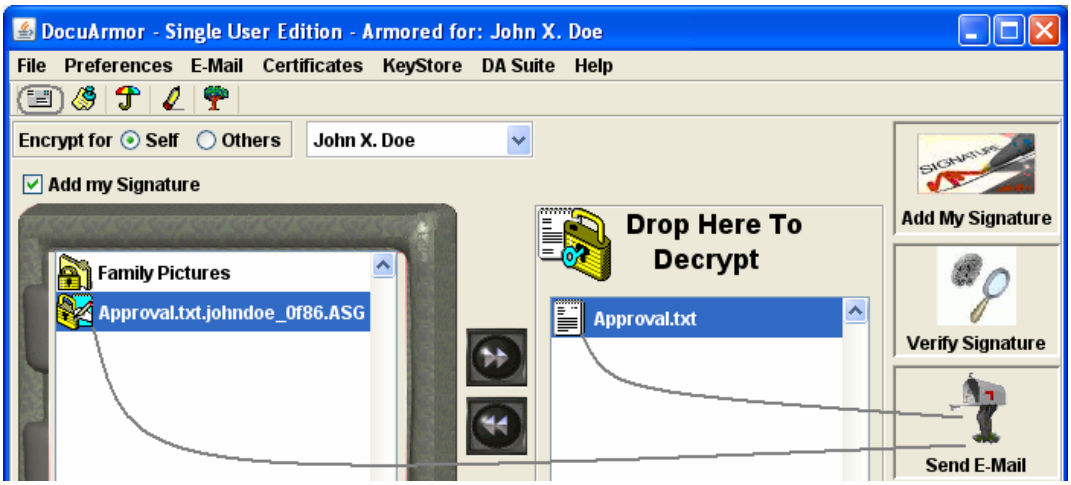
Dragging a file to encrypt

After selecting a file to encrypt, a prompt will appear giving you the option to remove the original source file. The encrypted file will appear inside the vault as a file with a lock.

Encrypted file in the Vault

Confidential Encrypted E-Mail

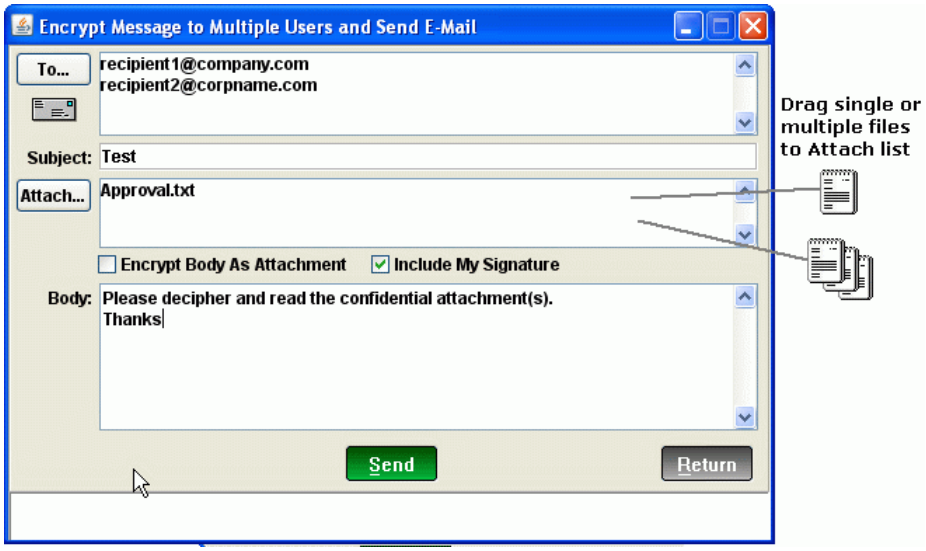
DocuArmor allows you to drag one or more non-encrypted or encrypted files to the e-mail area labeled "**Send E-Mail**" and you'll be prompted with an e-mail window to send the attached files.



Drag File(s) to E-Mail Icon

A second option allows the user to press the "Letter" icon on the toolbar to initiate sending encrypted attachments. An e-mail window prompt will appear allowing you to e-mail attachments to multiple users.

The e-mail application will allow you to add one or more recipients, a subject title, multiple attachments, and a short note that can optionally be encrypted as an attachment. You can select an individual recipient and alter the e-mail by hitting enter key. A prompt will appear allowing you to alter the e-mail address. You can *remove* any recipient by select them and pressing the delete key.



Send E-Mail with Attachments

Each recipient is associated with a certificate which is used to encrypt each attachment and the body if the "Encrypt Body..." checkbox is selected. Additionally, the owner's digital signature will be added to each attachment if the "Include My Signature" checkbox is selected.

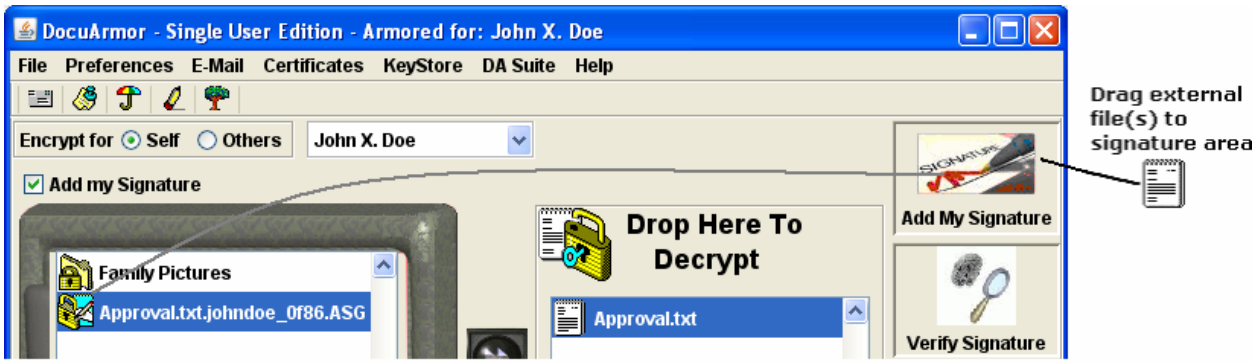
After pressing the send key, each recipient will receive attachments that only they can decipher. This is one of the safest techniques for sending encrypted information to a relative, friend or associate, ensuring that only they can view the information and preventing unauthorized access.

If the attachment is digitally signed, then the sender can be authenticated as well as detecting any tampering with the information.

Digital Signatures on a Document

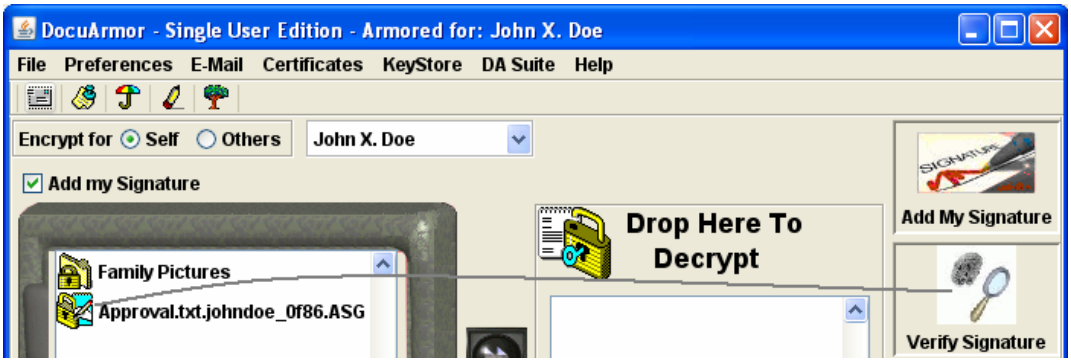
There has always been a need to determine who sent a message. A digital signature allows the receiver to verify the sender by using the sender's public certificate. Once the receiver has validated the sender's signature (the date signed is also provided) they can then choose to decrypt the message.

DocuArmor provides two ways of adding your digital signature. The **Include My Signature on Encryption** will include the signature on new notes and encryptions. Another technique is to add a signature include dragging an encrypted file from the vault or an external file to the **"Add My Signature"** image.



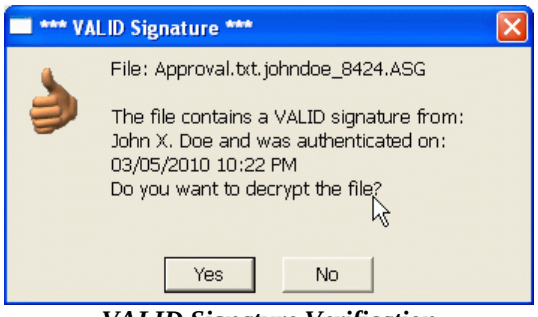
Drag File to Add Digital Signature

To determine which person has included a digital signature in a received file, DocuArmor uses the person's public key to authenticate the digital signature. Any file with the extension, **SGN** or **ASG** can be checked for signature verification. Drag the selected file to the **"Check Signature"** image to verify the digital signature.



Verifying the Signature of a Document

After the file is dropped, validation takes place and the user is notified whether or not the signature is valid.

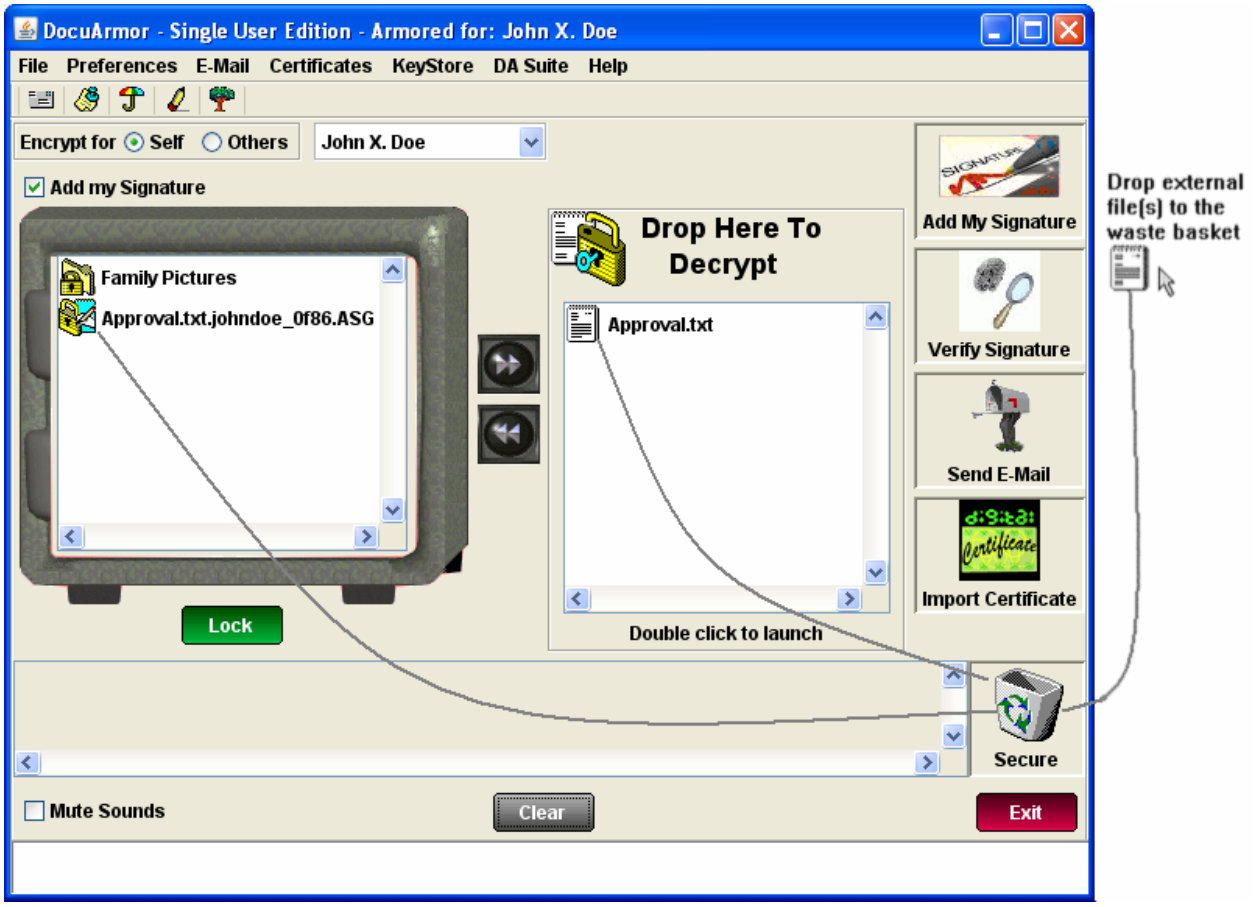


VALID Signature Verification

The person who signed the file will be displayed along with a timestamp. The user will have the option to decrypt the file.

Secure File Deletion

Any file (encrypted or non-encrypted) can be securely deleted by dragging and dropping them to into the ***Waste Basket*** icon. Please note that the user will be prompted to verify the delete. The secure delete will prevent any recovery of the file unless you have made a prior backup.



Dragging Files to Secure Delete

Be careful when deleting **encrypted** files because you will **NOT** be able to recover them. Make sure you do not need them or a have a backup copy.

Solid State Drives (SSD)

Solid state drives pose a potential flaw to secure file deletion. When attempting to over-write a page from a file on a solid state drive with a hex pattern, it marks the original page as invalid and writes the new data to a new or previously used page. At some point the original page will be over written.

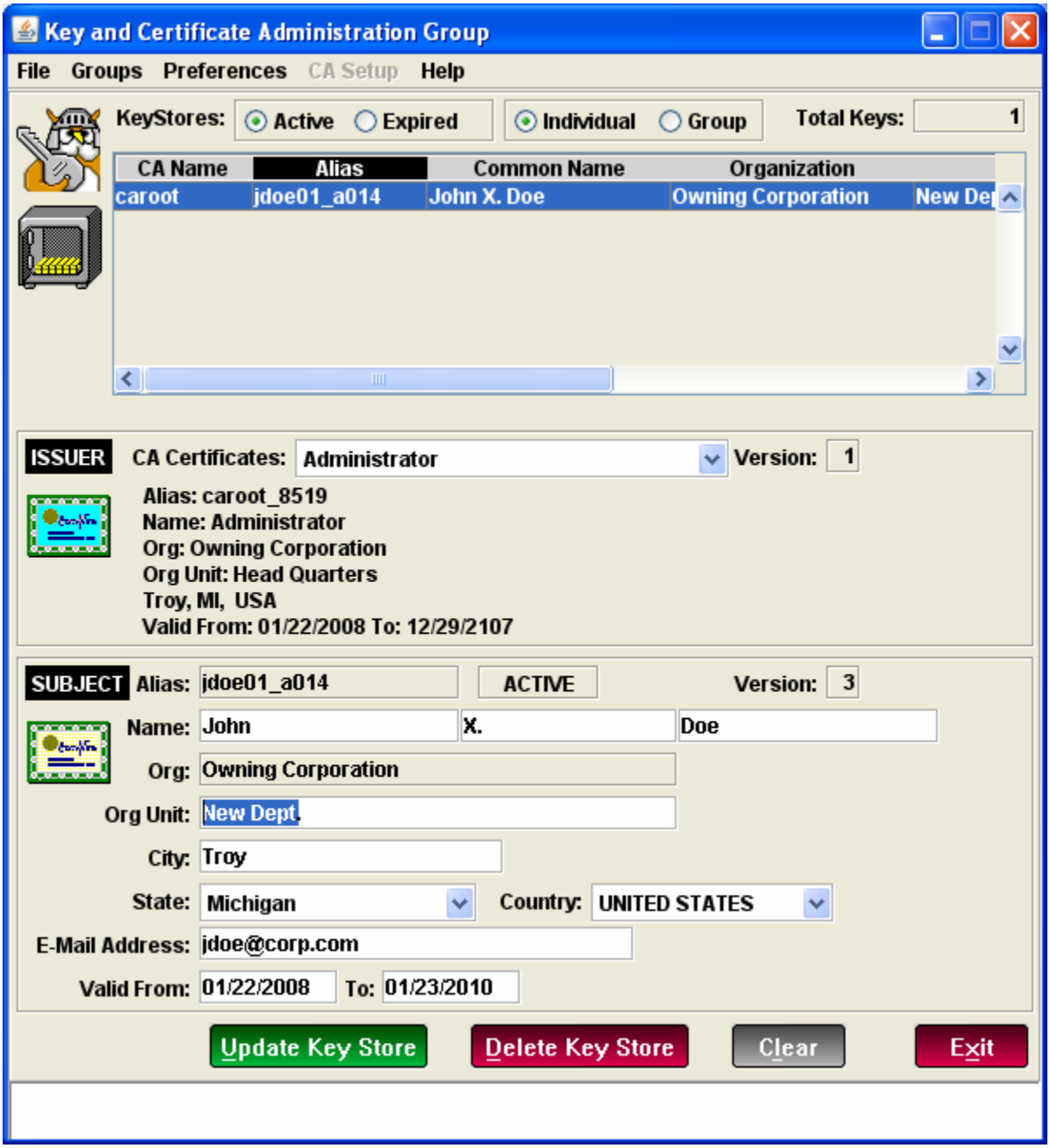
How does one address secure deletion on a solid state drive? You can delete the file and then create a file of hex patterns that is large enough to take up the remaining free space on the solid state drive. Once the file is created and written, it can be deleted to free up the space again. This technique should force the overwriting of data from previously deleted files. However, if the solid state drive is large, it may take a long time to perform the one pass erasure. It can take 2.5 minutes to wipe 100 million bytes so if the size of a solid state drive is in the gigabytes, each erasure of a gigabyte would last 25 minutes.

Keep in mind that a hacker would have a difficult time piecing together the remnants of a deleted file unless its removal was recent. This only applies to decrypted files since encrypted files are protected regardless of being deleted or not.

Solid state drives are typically found in mobile devices such as flash drives and phones.

Key Store Certificate Generation

The security administrator can generate a Certifying Authority (CA) certificate for the whole company or develop a corporate hierarchy of CA certificates. Once the administrator selects a CA certificate the employee encryption keys (key stores) and certificates can be generated.



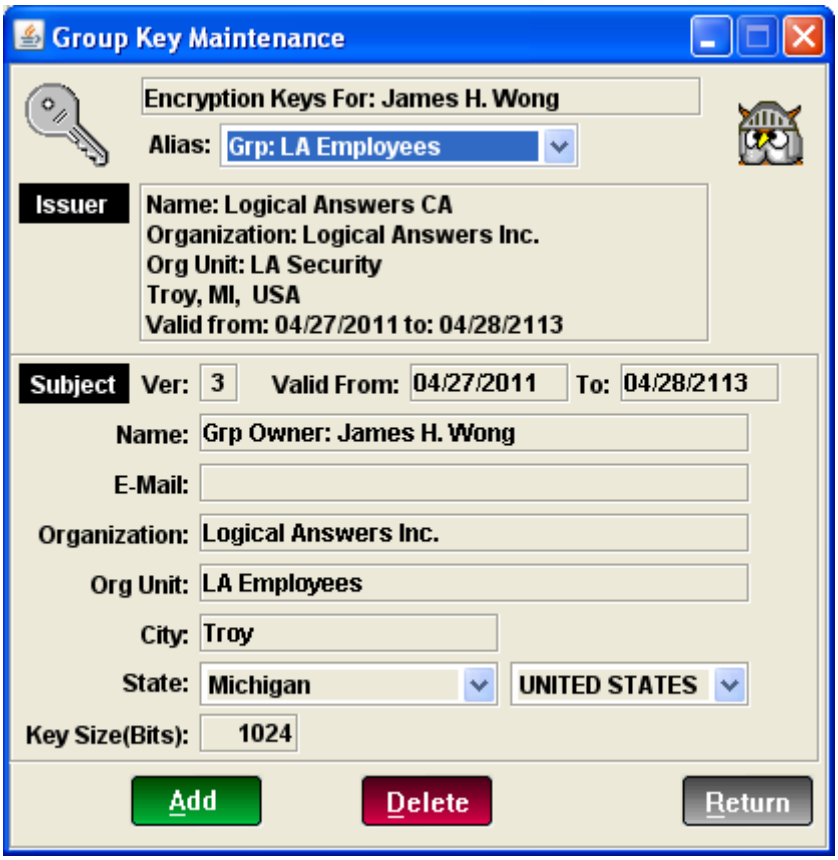
Generating an Employee Key Store

After the key store is generated, the administrator can update it with any corrections or leave it as is and distribute it to the corporate recipient.

The administrator can optionally purge the key store if they are practicing or the key store is no longer required. Key stores can also be "*expired*" through the update function. See the *KeyAdminUser.pdf* for detailed information.

Group Key Stores (Enterprise)

Group key stores are used to distribute encrypted information to a collection of users such as a department, committee, inner circle, etc. A group key store is a special file that is generated via the **Key Administration Enterprise** application. Its file name is prefixed with the phrase **"g_"** such as g_employees_nnnn.jks. After a group key store is created, it is distributed to the appropriate members by the administrator. The administrator should encrypt the group key store prior to distributing to each group member. When the group key store is received by the user, it must be added to their current security keys. Dropping an encrypted group key store onto the ***Decrypt area*** of DocuArmor will cause the group key store to be decrypted and copied to the la\daShared\KeyStore directory and the certificate to the la\daShared\PubCerts directory. Once the key store has been decrypted it is available to merge into an individual's key store. These group keys are shared by a collection of related users and a message encrypted with the public certificate can be deciphered by all members holding a copy of the group key.



Viewing/Deleting Group Key

The Group Key Maintenance module provides an alias drop down list which allows the user to select individual and group certificates for viewing or purging. When a group certificate is selected, the **Delete** button is enabled. If the user presses the delete button, the key will be removed making retrieval impossible until another copy of the group key is received.

Using CA Keys to Decipher Files (Enterprise)

Encryption keys/certificates generated with the enterprise tool, Key Administration, are "issued" by a **c**ertificate **a**uthority (**CA**) and retain a copy of the CA certificate (see Key Store Administration for more detail). During the encryption of a file, the CA certificate's public key is included during the ciphering of the symmetric key. This provides the owners of the CA keys/certificate the ability to decipher any user's encrypted files whose keys are issued by the CA. The CA owner can drag a user's encrypted file to the decryption area and the file will be deciphered. The most common uses for this feature are the recovery of information and collation of protected data.

Information Recovery

When an organization requires information that is encrypted by a member, what can the organization do if the member is not available? If the unavailability of the member is temporary, the organization can wait till the member returns. If the absence is permanent, the organization can have owner of the CA decipher the files or use a copy of the user's keys to decipher the files.

If an employee that leave the organization, the information they've encrypted can be collected and analyzed for possible re-distribution such as sales leads. Parents can purchase the DocuArmor Group edition and be the CA owners while their children can use the encryption keys issued by them. Parents can decipher their children's encrypted files in case of emergencies.

Collating Protected Data

To gather protected information from members of an organization, each member can encrypt the information with their own keys and send a copy to the CA owner. The CA owner can read each file from the different members. Alternatively, each member can encrypt their data for a specific member and send it to them, but would need to digitally sign it to identify their file. If there is a question of the veracity of any encrypted member file, digital signatures would eliminate the exposure.

A teacher can be the CA owner and the students can provide homework assignments, daily work, and tests to the teacher for grading.