DocuArmorPhone

Encryption with Secure SMS Texting

Portable Security

Compact enough to fit on an **Android Smart phone** and carry in your pocket. DocuArmorPhone allows the user to encrypt and decrypt files. It runs on Android 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, users can securely exchange text messages with each other. Simply exchange public certificates and your communications are safe from unauthorized access. Learn more…

Easy Encryption for ALL User Levels

DocuArmorPhone provides a high level of security with an easy to use interface. Select a file and hit the encryption button. 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...

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 DocuArmorPhone, 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 DocuArmorPhone cryptographic technology.

Confidential Encrypted E-Mail

Avoid the embarrassment of sending an e-mail to the wrong person. DocuArmorPhone 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.

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 DocuArmorPhone 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...

Securely Deleting Files

The secure delete feature prevents hackers from recovering information from your phone. Any non-encrypted file that has been designated as a protected digital asset needs to be securely deleted after it has been encrypted. Learn more...

Password Protection

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

Prevention and Safeguards

- DocuArmorPhone 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 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

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

DocuArmorPhone uses AES 256-bit encryption 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.

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

Competition and Pricing

DocuArmorPhone 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.

Contact

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

DocuArmorPhone is INCLUDED as part of the DocuArmor suite of secure applications which sells for only $25.00. 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

DocuArmorPhone is architected to take advantage of Android Smart Phones V2.1 and is perfect for individuals and mobile professionals. Compact enough to fit on an Android Phone carry it in your pocket and run the application directly. DocuArmorPhone app allows the user to protect their files on their phone with confidence knowing that nobody can read them without their password protected keys.

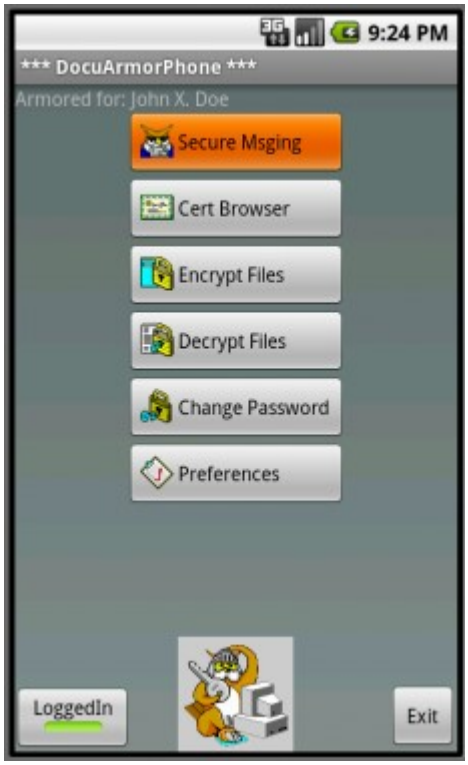
The designed portability of DocuArmorPhone allows the user to run the application on Android phones with operating system at 2.1 or higher. The user can secure files on the phone and take them along. If anyone finds a lost or stolen Android phone with DocuArmorPhone, the secured files remain undecipherable.

CYA - Cover Your Assets!

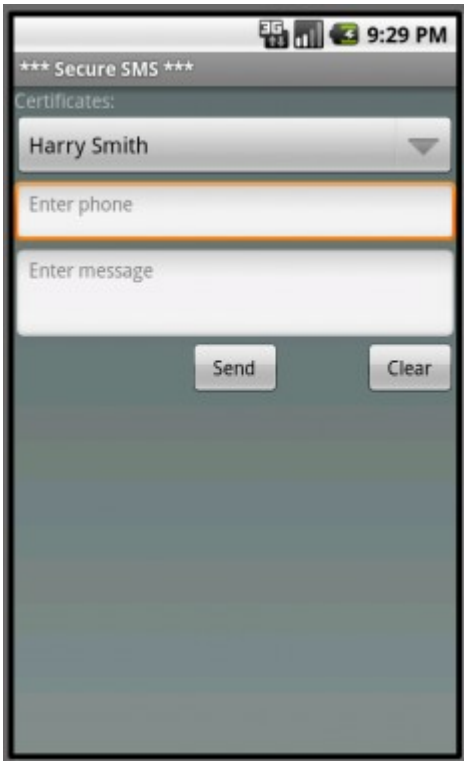
Each license is per user and can be installed on all their Android phones. This grants the user true mobility at an economical price.

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

Protecting Your Assets

DocuArmorPhone allows the encryption of all file types: text, word processing, images, etc. The certificate holds the key (known as the public key) used to encrypt any file; your certificate is what you give to others so they can send you encrypted messages or files. The key store holds the complimentary key (known as the private key) used to decipher that file. The encryption is based on the latest RSA algorithms.

File names will default to name of the chosen file(s) with the alias and AES/ASG extension added. For example, if the current user alias is johndoe, a file named:

myfile.txt

Will be encrypted as:

…/Encrypted/**myfile.txt*.johndoe_nnnn.AES***

If the signature is included it will be encrypted as:

…/Encrypted/**myfile.txt*.johndoe_nnnn.ASG***

Encrypt Files Option

Highlight and select the "**Encrypt Files**" button to launch the encrypt activity on your Android phone.

You can encrypt a file for yourself or another person if you have their certificate. You can also add your signature to the encrypted file by checking the "Add Signature" box. You can select a file to encrypt or edit and encrypt a new text note. To select file to encrypt, highlight and select the "**Encrypt File**" button.

Encrypt a Selected File

File Chooser Activity

The File Chooser will appear allowing you to select a file from internal or external memory. You can navigate to various directories and go back by hitting the "**Parent Dir**" button. Once you select a file, you will see a message box showing the file is being encrypted.

Encrypt File Message

After the DocuArmorPhone app finishes encrypting the file, it will be displayed in the list. You can delete the encrypted file or select another file for encryption.

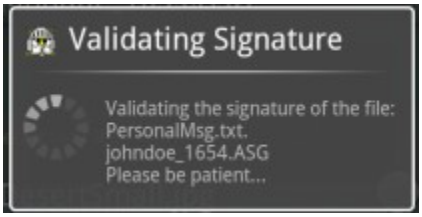
Encrypt File Results

Who Sent the Message?

To determine which person has included a digital signature in a received file, DocuArmorPhone 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. Select a file with the **ASG** extension and select the "**Verify Signature**" button.

Verifying Signature

After hitting the button a message box will appear displaying the file being validated. If the signature is valid a dialogue box will appear asking the user if the file should be decrypted as well.



Validate Signature Message

Valid Signature Dialogue

Selecting the "Yes" button will decrypt the encrypted file and it will appear in the list.

Securely Deleting Files

The technique to securely delete any non-encrypted file is to overwrite it one or more times. The secure delete will prevent file recovery with software products and make it extremely difficult for a hacker to recover the file using expensive specialized magnetic disc readers. Any backup represents a security exposure so these should also be securely deleted.

Even though the DocuArmorPhone app uses the secure deletion technique, the introduction of solid state drives poses an exposure to decrypted files (see next section). It is recommended to keep unencrypted files to a minimum on a phone and keep all your confidential data encrypted.

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.