

# GoldMine 6.5 Digital IDs

Copyright © 2004 FrontRange Solutions, Inc.

---

**Author:** Charles Courchaine

**Department:** Technical Support

**Created:** March 16, 2004

**Last Updated:** April 18, 2004

## Copyright

*Copyright © 2004 FrontRange Solutions Inc. All Rights Reserved. GoldMine, HEAT, and other FrontRange products and brands are registered trademarks or trademarks of FrontRange Solutions Inc. in the U.S. and/or other countries. Other products and brands are registered trademarks or trademarks of their respective owners/companies.*

*USE OF THE SOFTWARE DESCRIBED IN THIS PAPER AND ITS RELATED USER DOCUMENTATION ARE SUBJECT TO THE TERMS AND CONDITIONS OF THE APPLICABLE END-USER LICENSE AGREEMENT (EULA).*

The information contained in this document is provided “as is” without warranty of any kind. To the maximum extent permitted by applicable law, FrontRange Solutions disclaims all warranties, either expressed or implied, including the warranties for merchantability and fitness for a particular purpose; and in no event shall FrontRange Solutions or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if advised of the possibility of such damages.

# Table of Contents

COPYRIGHT .....	2
<b>DIGITAL ID BACKGROUND .....</b>	<b>4</b>
DIGITAL ID USES.....	4
PUBLIC AND PRIVATE KEYS .....	4
LEVELS OF SECURITY .....	5
SHARING PUBLIC KEYS .....	5
<b>EXPORTING DIGITAL IDS FROM WINDOWS FOR USE WITH GOLDMINE.....</b>	<b>6</b>
BACKGROUND: .....	6
METHOD 1: WINDOWS 2000/XP Pro/2003 .....	6
METHOD 2: MICROSOFT OUTLOOK EXPRESS.....	7
METHOD 3: MICROSOFT OUTLOOK XP (2002) .....	7
<b>USING DIGITAL IDS WITH GOLDMINE.....</b>	<b>8</b>
IMPORT THE DIGITAL ID INTO GOLDMINE: .....	8
SECURITY TAB OPTIONS .....	8
<i>Signature Settings</i> .....	8
<i>Encryption Settings</i> .....	8
<i>Other Settings</i> .....	8
ENCRYPTING EMAIL .....	9
SIGNING EMAIL .....	9

# Digital ID Background

If you and your contact use digital IDs to verify your signatures and/or to send encrypted e-mail messages, GoldMine allows you to configure your **Internet Preferences** and the **Record Properties>>Contact Details>>Digital IDs** to include the necessary information for S/MIME enabled e-mail.

Your digital ID, also known as a digital certificate, is a file sent along with an e-mail message identifying you as the authentic sender. Digital ID certificates are files issued by a certified security authority, such as VeriSign, Inc., or from your Microsoft Exchange Server administrator. Digital IDs have an expiration date and must be renewed periodically to remain valid. A digital ID you send to someone typically contains the following information:

- Your name and e-mail address as a digital signature
- Your public key (Public and private keys are discussed below)
- Expiration date of the public key
- Name of the Certification Authority (CA) who issued your Digital ID
- Serial number of the Digital ID
- Digital signature of the CA

## Digital ID Uses

E-mail applications use digital IDs in several ways. One way is as a digital signature. A digital signature provides security by verifying that the message originated from a specific person and that the message has not been altered. A signature does not guarantee that the message has not been read, only unaltered. The second way the digital ID works is as a message encryption method. Digital ID encryption scrambles a message with a recipient-specific algorithm.

## Public and Private Keys

Digital ID encryption uses a system of key pairs. Key pairs include a public key, used to encrypt a message, and a private key, used to decrypt a message. The sender of a secure e-mail must have the recipient's public key to encrypt the message. Then, when the message is received, it is decrypted using the recipient's matching private key.

Using GoldMine you can exchange encrypted e-mail messages with a contact. To do this, you must have the contact's digital ID that includes his public key and he must have your digital ID that includes your public key. Then, in GoldMine, you must import the contact's Digital ID using the contact's **Record Properties>>Contact Details>>Digital IDs** tab and import your Digital ID using your **Internet Preferences>>More Options>>Security** tab.

For example, when you send an encrypted message to a contact, it is encrypted in GoldMine using the public key he provided to you and then, when he receives the message, it is decrypted by his e-mail application using his private key. Conversely, when a contact sends you an

encrypted message it is encrypted by the sender's e-mail application with your public key (that you provided earlier). When you receive the message, it is decrypted using your private key.

## Levels of Security

- **Signed:** The message is signed with the sender's private key. The private key is not sent, it is used to create a unique identifier for the message that can be verified with your public key. Sending a message with a digital signature confirms that the message was sent by the sender listed in the From address and is unaltered.
- **Encrypted:** The message is sent encrypted with the recipient's public key. The recipient provided you with his public key before you send the message. When a message is encrypted, the body and any attachments are gibberish to anyone who does not have the recipient's private key. Only the recipient should have his private key. An encrypted message does not guarantee to the recipient that the sender is the name in the From address.
- **Signed and Encrypted:** The message is signed with the sender's private key, confirming for the recipient that the message was sent by the sender in the From address and unaltered, and it is encrypted with the recipient's public key and then decrypted with their private key when he receives the message.

## Sharing Public Keys

For security reasons you should not share your private key; however, you can and need to share your public key with contacts, if you want to receive encrypted mail, in two ways:

**Digital ID Signature:** Your Digital ID is attached to any message that includes a Digital ID Signature. The recipient can then extract it and import it into his e-mail application. For example, in Outlook the user can right-click on the sender's name on a message and add the contact to his existing contacts. The digital ID certificate is included.

**Export:** You can export your Digital ID send it to a contact who can then import the file into their e-mail application. For example, in Outlook the file is imported on the contact's Certificate tab.

# Exporting Digital IDs from Windows for use with GoldMine

## Background:

When a certificate is obtained from VeriSign or a similar authority, it is usually downloaded and deposited directly into Windows' certificate store; it is not typically saved as a certificate file. GoldMine cannot access the Windows' certificate store and must import the certificate into its own certificate store. In order to accomplish this, the certificate along with private key must be exported to a file and imported into GoldMine. Methods for accomplishing this are detailed below:

- Method 1 is for Microsoft Windows 2000/XP Professional/2003
- Method 2 is for using Microsoft Outlook Express to export the file
- Method 3 is for using Microsoft Outlook XP (2002) to export the file.

## Method 1: MS Windows 2000/XP Pro/2003

1. Click **Start>>Run**. Type **mmc** and press **Enter**.
2. Select **File(Console in Microsoft Windows 2000)>>Add/Remove Snap-in (Ctrl + m)**.
3. Click **Add**
4. Click **Certificates** and then click **Add**.
5. Leave *My user account* selected and click **Finish**.
6. Click **Close**.
7. Click **OK**.
8. Expand *Certificates – Current user*.
9. Expand *Personal*.
10. Highlight your certificate.
11. Right click your certificate and choose **All Tasks>>Export**.
12. Click **Next**.
13. Select **Export the private key** and click **Next**.
14. Select **Include all certificates in path if possible** and click **Next**.
15. Enter a password for the certificate and click **Next**.
16. Enter a path with file name for the certificate and click **Next**.
17. Click **Finish**.
18. You should receive a message stating export was successful.
19. Close the management console, do not save changes.
20. Import the certificate into GoldMine (See Section on importing a certificate into GoldMine)

## Method 2: Microsoft Outlook Express

1. Open Outlook Express.
2. Select **Tools>>Options**.
3. Click the **Security** tab.
4. Click **Digital IDs...**
5. Highlight the user's ID.
6. Click **Export**.
7. In the Certificate Export Wizard click **Next**.
8. Leave **Yes export the private key** selected and click **Next**.
9. Select **Include all certificates in the certification path** and click **Next**.
10. Enter a password for the certificate and click **Next**.
11. Enter a path with file name for the certificate and click **Next**
12. Click **Finish**.
13. You should receive a message stating export was successful.
14. Click **Close** in the certificates window.
15. Click **Cancel** in the options window.
16. Close Microsoft Outlook Express.
17. Import the certificate into GoldMine (See Section on importing a certificate into GoldMine)

## Method 3: Microsoft Outlook XP (2002)

1. Open Microsoft Outlook.
2. Select **Tools>>Options>>Security**.
3. Click **Import/Export** under the Digital IDs section.
4. Choose **Export your Digital ID to a file**.
5. Click **Select**.
6. Highlight the certificate and click **OK**.
7. Browse to or enter a path with filename.
8. Enter a password and confirm it.
9. Click **OK**
10. You should receive a message stating export was successful.
11. Click **Cancel** in the options window.
12. Close Microsoft Outlook.
13. Import the certificate into GoldMine (See Section on importing a certificate into GoldMine)

# Using Digital IDs with GoldMine

## Import the Digital ID into GoldMine:

1. Go to **Edit>>Preferences>>Internet**, click **More Options** and select the **Security** tab.
2. Click the **DigitalID(s)...** button and choose import.
3. Enter the path and filename (or browse to the file) that you previously exported.
4. Enter in and confirm the password you exported the certificate with and click **OK**.
5. Your certificate will then appear in the list box, and click **OK**.

## Security Tab Options

Access these settings by going to **Edit>>Preferences>>Internet**, click **More Options** and select the **Security** tab.

### *Signature Settings*

**Sign ALL outgoing E-mail with a Digital ID, by default:** Sends all your e-mail messages with your digital ID. The message is sent with a signature, but it is not encoded (clear text). This allows recipients who cannot support S/MIME to read the message.

**Encode any outgoing E-mail signed with a Digital ID (Recipients required to have S/MIME to read 'opaque' messages):** Sends outgoing e-mail messages signed with your digital ID as S/MIME encoded (opaque). Older e-mail clients that do not support S/MIME will not be able to read the body of this type of e-mail message. You can also sign individual messages by selecting **Sign with Digital ID** on the Edit E-mail toolbar.

### *Encryption Settings*

To encrypt all outgoing messages by default, select **Encrypt ALL outgoing E-mail, by default (Recipients' Certificates are required in advance)**. Selecting this option encrypts outgoing messages with your contact's digital ID. Even with this option selected, you can select **Do not Encrypt** on the encryption menu on the Edit E-mail toolbar. If you do not select this option, you can still encrypt individual messages by selecting **Encrypt Messages** on the Edit E-mail toolbar.

### *Other Settings*

**Import new/updated certificates for ALL incoming signed E-mails, by default:** Automatically imports the digital ID on all signed incoming messages into the contact's **Record Properties>>Contact Details>>Digital IDs** tab. If the contact sends you the digital ID as an attached file you can save it and manually import it for that contact. Go to that contact in GoldMine and go to **Edit>>Record Properties>>Contact Details>>Digital IDs** tab. On that tab select import and enter the path and file name (or browse to where you saved the file) and enter a name that you want to display for that digital ID.

**Save ALL incoming S/MIME e-mails as 'clear' messages:** Saves all S/MIME encoded (opaque) messages and all encrypted messages as clear text, or not encoded. As clear-text messages, all GoldMine users with access to the e-mail record can read the messages. If this option is not selected, the messages are saved as they were received. Whenever a GoldMine user, either the recipient or another user, wants to read the e-mail message, he will need to enter the password for the private key of the GoldMine recipient. Remember, for security reasons, only the recipient should know the password for his private key.

If you do not select this setting, encrypted messages from contacts will be unreadable by other users on the History and Pending tabs. Carefully consider the consequences before clearing this option. Also note that encrypting the message after retrieval with GoldMine's encryption and then clearing GoldMine's encryption also removes the S/MIME encryption and saves the message as clear text.

## **Encrypting Email**

1. Create an email message (ctrl+shift+e)
2. Click the **Encrypt Message** button from the message tool bar
3. Click **Encrypt using Digital ID**

If the recipient is not a contact or you do not have a digital certificate (public key) on file for that contact GoldMine will inform you that you cannot send an S/MIME encrypted message to that contact.

## **Signing Email**

1. Create an email message (ctrl+shift+e)
2. Click **Sign with Digital ID** from the message tool bar

GoldMine will sign the email with your private key; if the recipient has your public key, they will be able to verify that the message is unaltered. If the recipient does not have your public key then they will only be able to verify that the message originated from you. Additionally, the recipient's email client must support S/MIME to view the message.