2MSecMail 1.3 PRO

Extra high Data security and secure e-mail client

http://www.sweb.cz/2msoft

2MSecMail 1.3 – data security and secure e-mail client

Product description:
This software is for creating **extra-high secure** messages with attachments. All items are compressed and separately encrypted by 256-bit strongest symmetric ciphering methods and algorithms. Result is one *.2ms file which can be send via e-mail to appropriate recipients even sending „Fingerprints" of each document to their „Fingerprint" e-mail address. „Fingerprint" address should be different than normal receive address.
This software uses also own Digital ID technology, for signing whole message. 2MSecMail is the world first software which allows include photo to the Digital signature !
One of extra advantage of this software is using quite smart principles for handling with passwords. This will be described later in this manual. Each group of users can use Groups for their communication. Messages created in one Group cannot be opened in second Group although they use same password.
All files with extension ***.2ms** can be automatically opened with the 2MsecMail application.
2MsecMail create 2ms files which are send via e-mail as attachment. After receiving such e-mail you simply click on the attachment and 2MsecMail automatically will start and require password. 2MsecMail can work directly together with SMTP server or collaborate with Microsoft MAPI.

Minimum system requirements

IBM PC compatible computer
CPU Intel Pentium 233
High color (16-bit color depth) resolution
64 MB RAM
50 MB free space on C drive
OS: Microsoft Windows 98 with DCOM98 installed

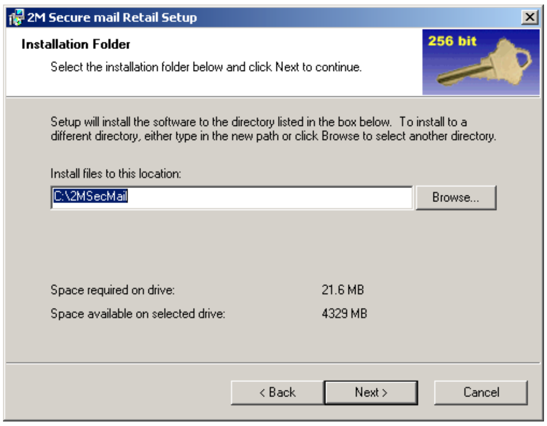
Recommended system

IBM PC compatible computer
CPU Intel Pentium III 600 MHz
True color (32-bit color depth) resolution
128 MB RAM
200 MB free on HDD
OS: Microsoft Windows 2000

Installation

Distribution contains one **setup.exe** file, which must be running under Windows 9x, NT4, Me, 2000 or XP.
Installation procedure is a standard one with possibility of choose for additional packages (Administrator and Tutorial)

Administrator package contain *Digital ID creator* and *Group creator*. All this will be in Admin directory.
Tutorial package contain tutorial message, Digital ID and keys. All this will be in Tutorial subdirectory. In DSK_A subdirectory are files which should be saved to diskette for tutorial purposes, like reading Key, SecKey or Digital ID …



2M Secure mail Retail Setup

Installation Folder

Select the installation folder below and click Next to continue.

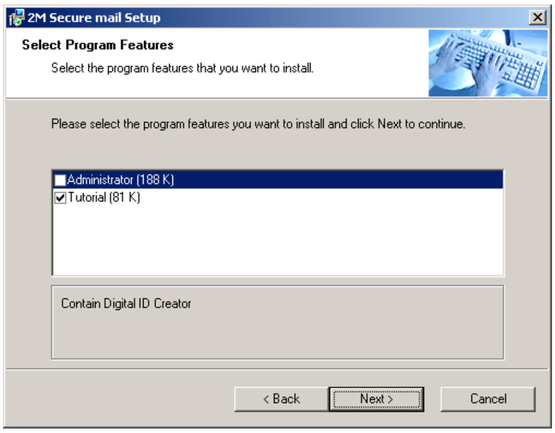
Setup will install the software to the directory listed in the box below. To install to a different directory, either type in the new path or click Browse to select another directory.

Install files to this location:

C:\2MSecMail

Space required on drive: 21.6 MB

Space available on selected drive: 4329 MB



2M Secure mail Setup

Select Program Features

Select the program features that you want to install.

Please select the program features you want to install and click Next to continue.

□ Administrator (188 K)

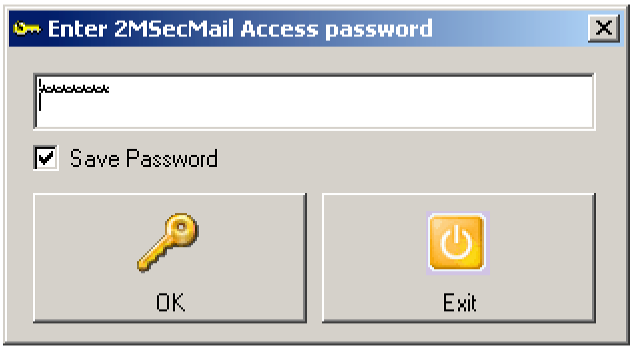
☑ Tutorial (81 K)

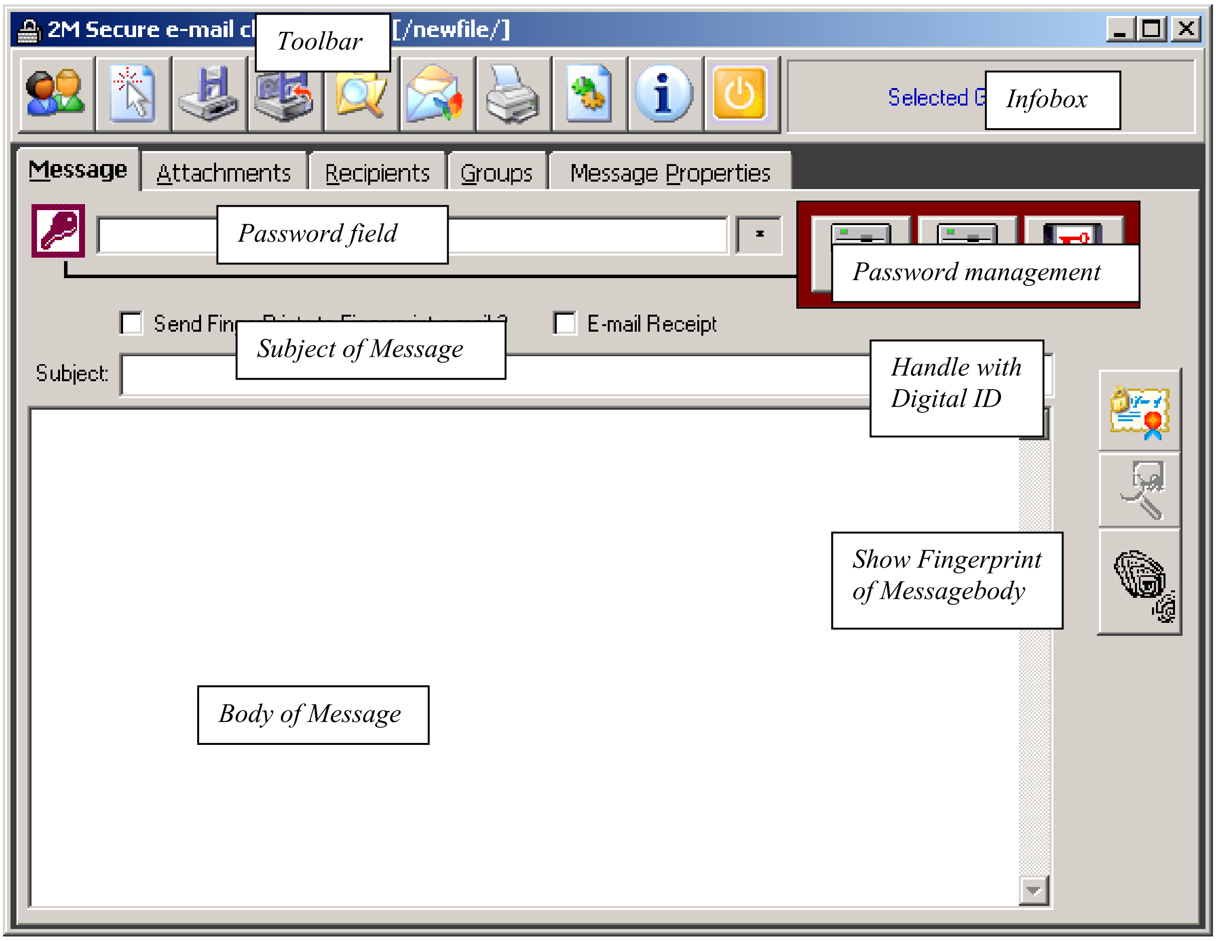
Contain Digital ID Creator

After installation process extension *.2ms will be automatically associated with 2MsecMail application. Also shortcut is created on the desktop.

Main screen

After start of the program user is required to enter access password. On base of this password is encrypted main database. Default password is "`start`". Never forgot the password otherwise you will be forced to reinstall software and you'll loose all contacts in Address book. The same is valid for Administrator tools like **Digital ID Creator** and **Group Manager**, but there is not possible to save the password.

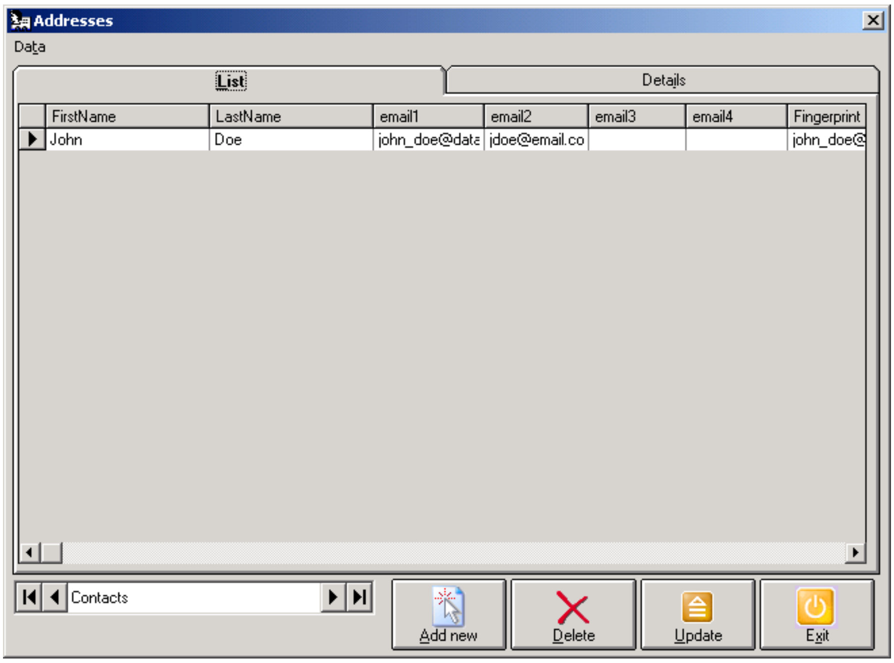




After startup of 2MSecMail user see this screen with Toolbar and tabbed dialog control.

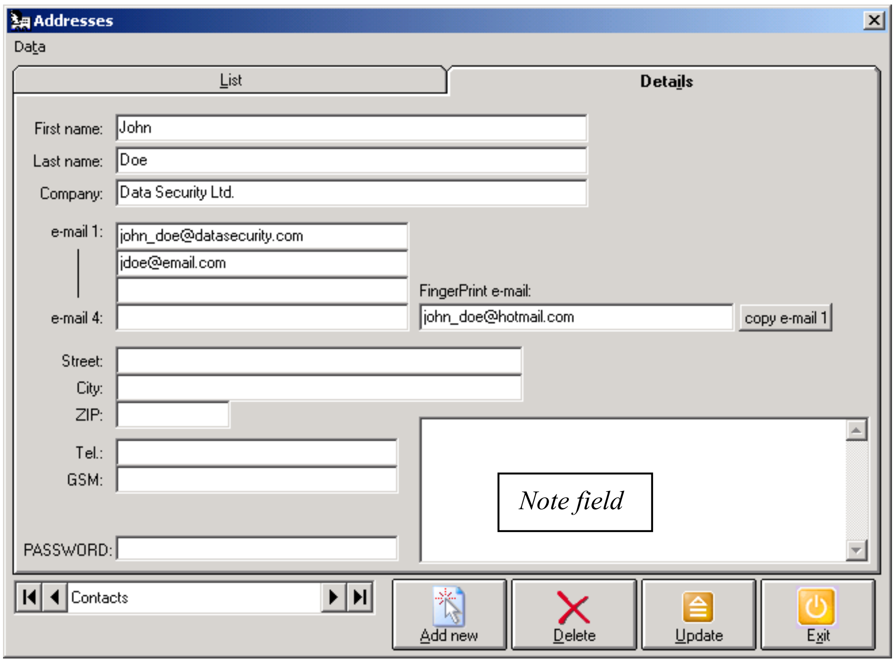
Toolbar Icon	F key	Description
👥	F2	Address book, see page 6.
🗋	F3	Create new empty message. This option will destroy the previous message without any warning even if is not saved!!!
💾		Save the message to fixed filename and path *AppDir*/OutFile/2msm.2ms
💾		Export (Save As) the message to required file name and path.
📂	F4	Open the *.2ms file
✉	F6	Send message via WinSock or MAPI
🖶		Print the message
⚙		Configuration of 2MSecMail
i		About box
⏻	F12	Exit the 2MSecMail

Address book



	FirstName	LastName	email1	email2	email3	email4	Fingerprint
▶	John	Doe	john_doe@data	jdoe@email.co			john_doe@

Address book, where user can add new one, Delete or update contacts.



First name: John

Last name: Doe

Company: Data Security Ltd.

e-mail 1: john_doe@datasecurity.com

jdoe@email.com

e-mail 4:

FingerPrint e-mail: john_doe@hotmail.com

Street:

City:

ZIP:

Tel.:

GSM:

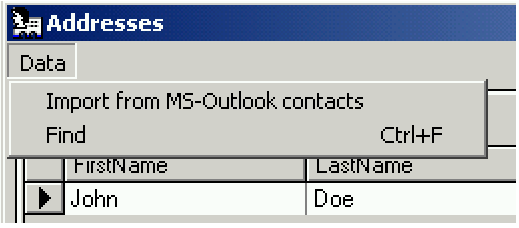
PASSWORD:

Fingerprint e-mail: address to which 2MSecMail will send file with Fingerprint information about Message and all attached documents.

*) *Fingerprint is unique hexadecimal key generated on base of special algorithm (SHA-1, MD5, SHA-256) from the source (text, File) and is unique for the exact text or file, that means that two same keys can not exist for different files or text even one byte has been changed.*

PASSWORD:
Here user can have notice about used password with communication with this people.

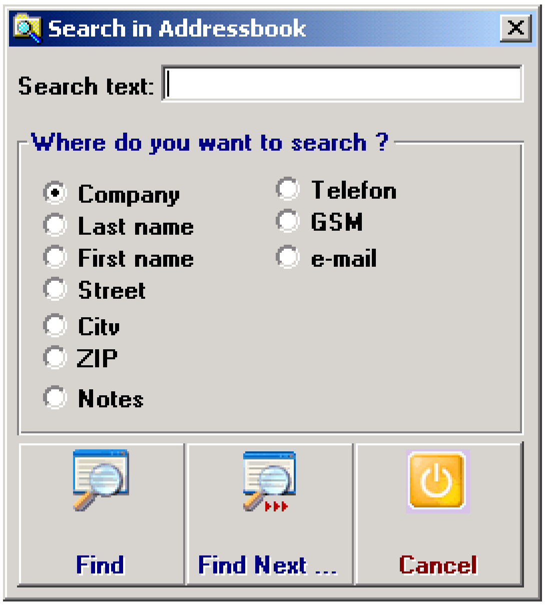
Menu “Data”:



FirstName	LastName
John	Doe

Import from MS-Outlook contacts: this menu option offers you import contact database from Microsoft Outlook database to 2MSecMail Address book.

Find:

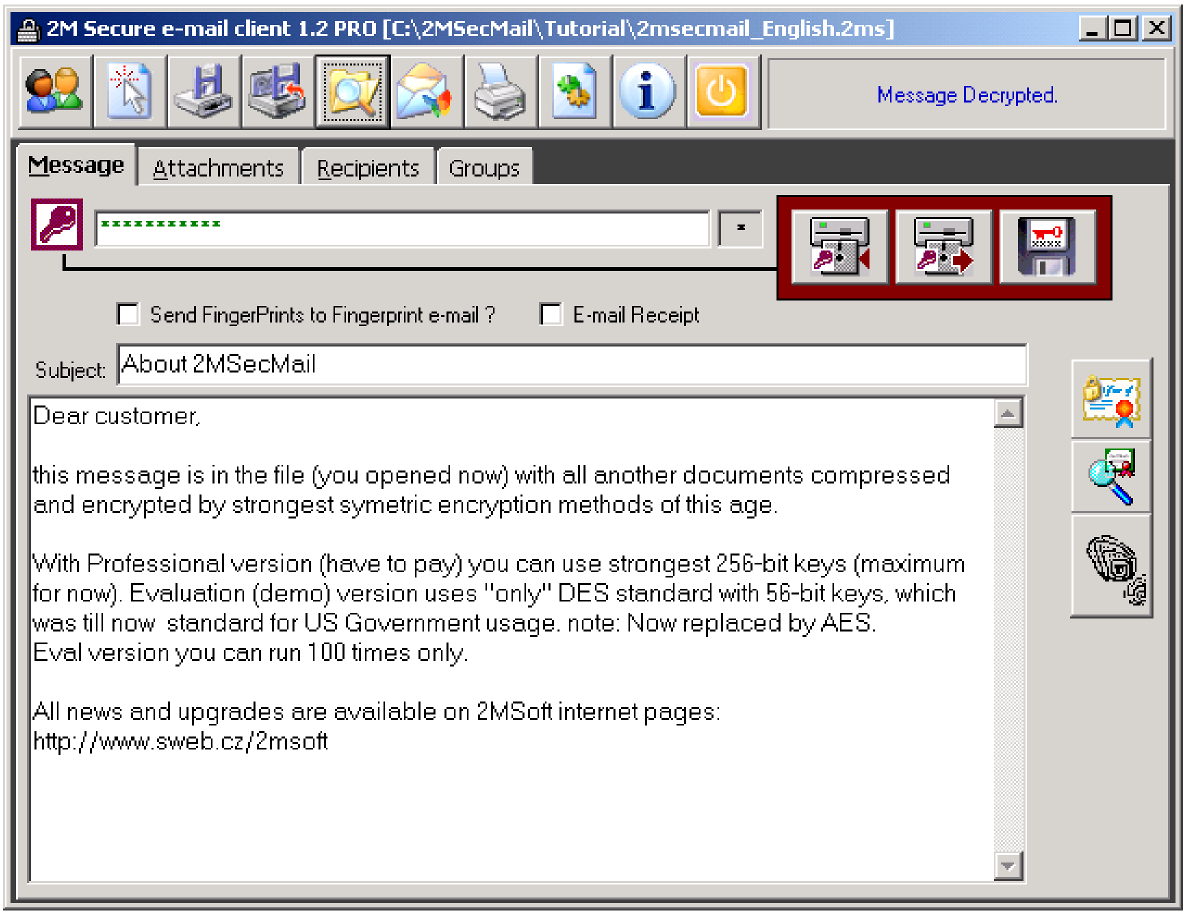


Search text:

Where do you want to search ?

● Company
○ Last name
○ First name
○ Street
○ City
○ ZIP
○ Notes
○ Telefon
○ GSM
○ e-mail

Type phrase you want to search on selected database field, like Company, Phone etc…



2M Secure e-mail client 1.2 PRO [C:\2MSecMail\Tutorial\2msecmail_English.2ms]
Message Decrypted.
Message
Attachments
Recipients
Groups

****

□ Send FingerPrints to Fingerprint e-mail ?

□ E-mail Receipt

Subject: About 2MSecMail

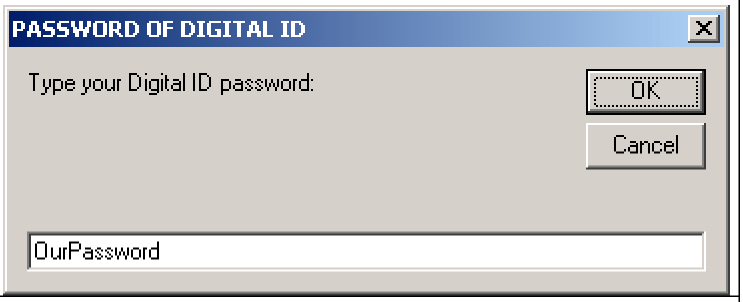
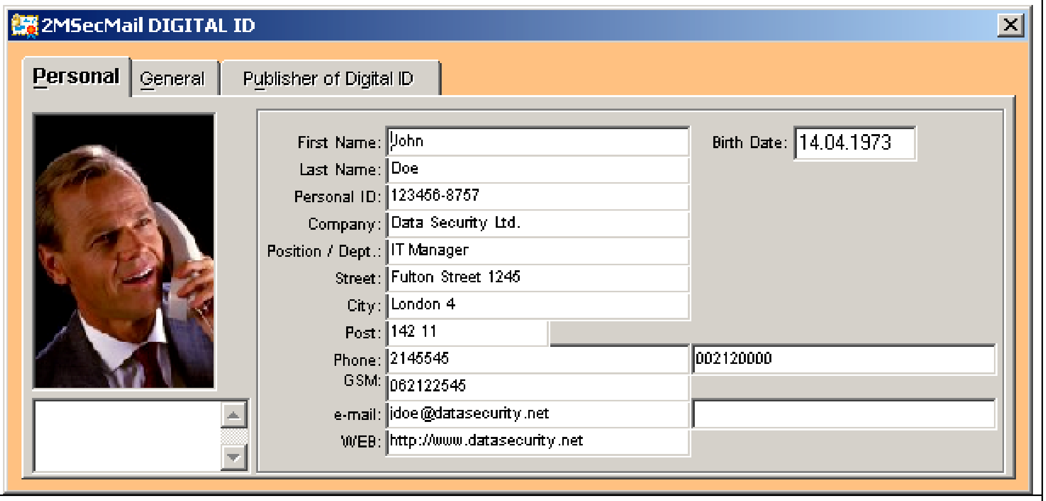
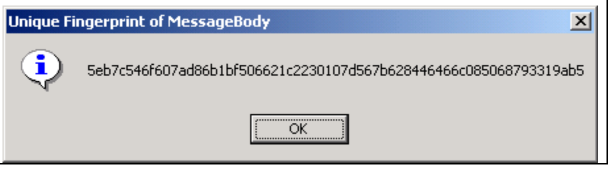
Dear customer,

this message is in the file (you opened now) with all another documents compressed and encrypted by strongest symetric encryption methods of this age.

With Professional version (have to pay) you can use strongest 256-bit keys (maximum for now). Evaluation (demo) version uses "only" DES standard with 56-bit keys, which was till now standard for US Government usage. note: Now replaced by AES.
Eval version you can run 100 times only.

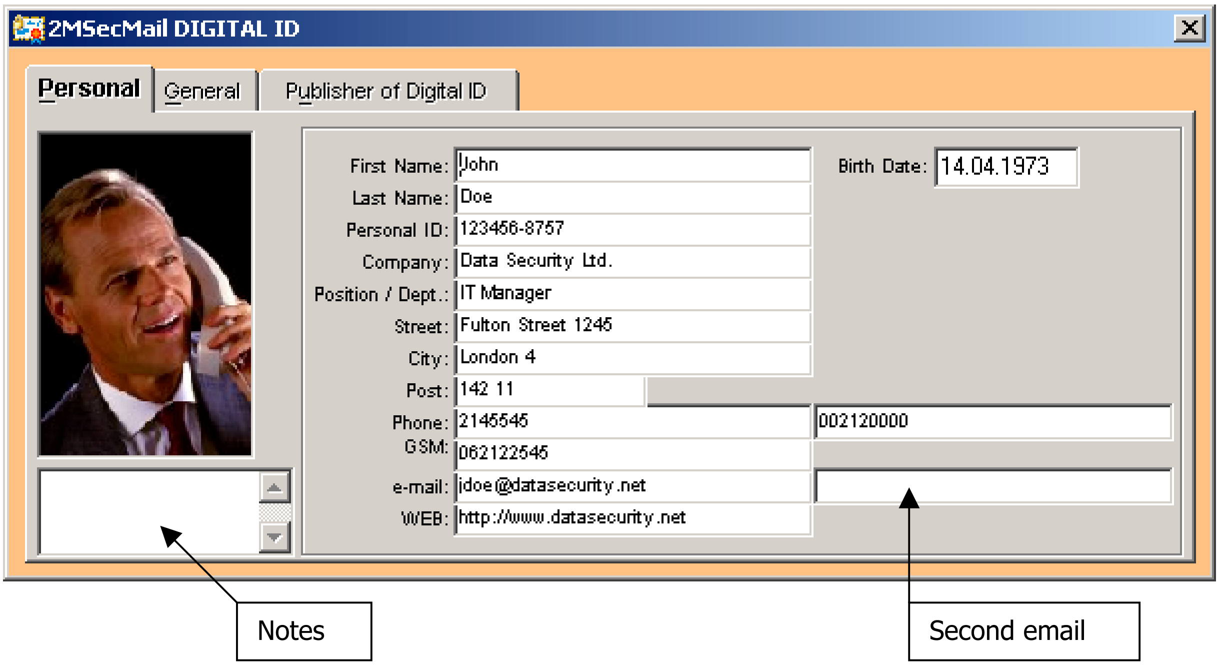
All news and upgrades are available on 2MSoft internet pages:
http://www.sweb.cz/2msoft

Screen example after opening Tutorial file

	Typed password will be saved to floppy drive, respectively to drive specified in Configuration
	Load key (password) from drive. User will never see the password. After importing the key (password), password field will be invisible.
	SecKey – Security key This combined password and diskette key. That means that message receiver can open message only if he/she knows password and have a diskette. SecKey depend on entered password.
	Import your Digital ID to the message. While opening the Digital ID file you'll be prompted for password, which encrypted DIG.ID, otherwise Digital ID can not be assigned to your message. Digital ID is kind of Digital signature.  PASSWORD OF DIGITAL ID Type your Digital ID password: OK Cancel OurPassword
	Example shows the Digital ID after pressing button with Magnifier.  2MSecMail DIGITAL ID Personal · General · Publisher of Digital ID First Name: John Birth Date: 14.04.1973 Last Name: Doe Personal ID: 123456-8757 Company: Data Security Ltd. Position / Dept.: IT Manager Street: Fulton Street 1245 City: London 4 Post: 142 11 Phone: 2145545 · 002120000 GSM: 062122545 e-mail: jdoe@datasecurity.net WEB: http://www.datasecurity.net
	Shows Fingerprint of the Message body  Unique Fingerprint of MessageBody 5eb7c546f607ad86b1bf506621c2230107d567b628446466c085068793319ab5 OK

Working with Digital ID

Next three pictures shows how Digital ID viewer looks like.



First Name: John

Last Name: Doe

Personal ID: 123456-8757

Company: Data Security Ltd.

Position / Dept.: IT Manager

Street: Fulton Street 1245

City: London 4

Post: 142 11

Phone: 2145545 002120000

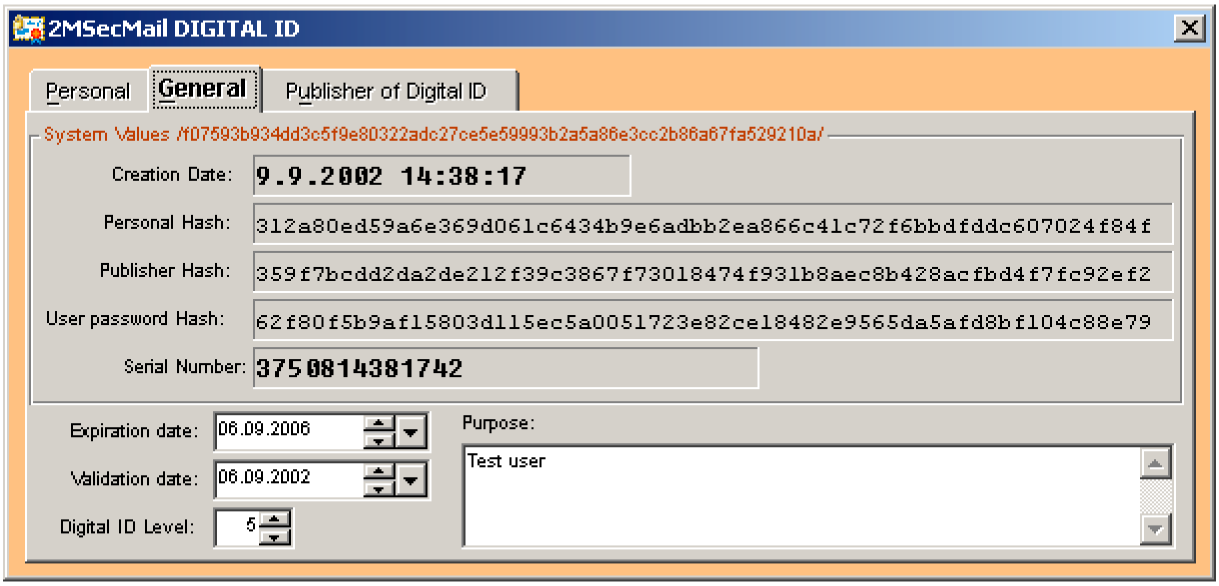
GSM: 062122545

e-mail: jdoe@datasecurity.net

WEB: http://www.datasecurity.net

Birth Date: 14.04.1973

One of interesting feature of 2MSecMail product is possibility include photo to the Digital signature !



System Values /f07593b934dd3c5f9e80322adc27ce5e59993b2a5a86e3cc2b86a67fa529210a/

Creation Date: 9.9.2002 14:38:17

Personal Hash: 312a80ed59a6e369d061c6434b9e6adbb2ea866c41c72f6bbdfddc607024f84f

Publisher Hash: 359f7bcdd2da2de212f39c3867f73018474f931b8aec8b428acfbd4f7fc92ef2

User password Hash: 62f80f5b9af15803d115ec5a0051723e82ce18482e9565da5afd8bf104c88e79

Serial Number: 3750814381742

Expiration date: 06.09.2006

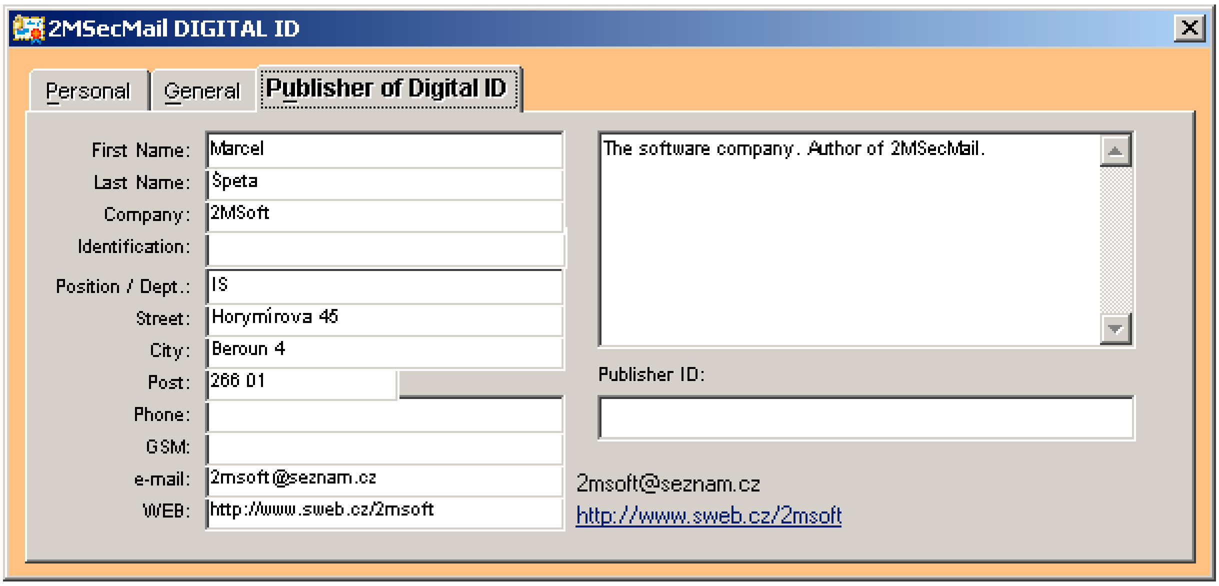
Validation date: 06.09.2002

Digital ID Level: 5

Purpose:

Test user

General information about Digital ID:
System Values caption is followed by General Fingerprint of Digital ID. Creation Date contain Date and Time of Dig.ID creation. Personal and Publisher Hash means fingerprint of collected information. Under this is Serial number of Digital ID. Digital Level can be from 0-5 depending of importance of it. Value 0 (Highest Level) can be Issued only by 2MSoft company.



First Name: Marcel

Last Name: Špeta

Company: 2MSoft

Identification:

Position / Dept.: IS

Street: Horymírova 45

City: Beroun 4

Post: 266 01

Phone:

GSM:

e-mail: 2msoft@seznam.cz

WEB: http://www.sweb.cz/2msoft

The software company. Author of 2MSecMail.

Publisher ID:

2msoft@seznam.cz

http://www.sweb.cz/2msoft

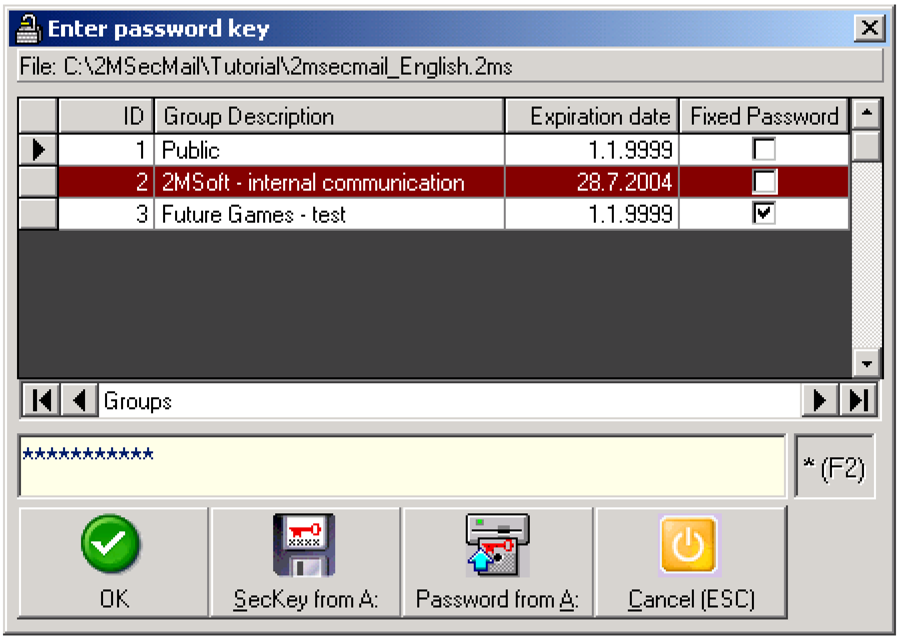
On right side of fields with e-mail and WEB information you'll find hyperlinks for immediate jumping to web pages or e-mail client.

Publisher of Digital ID – all information about issuer of Dig.ID

Publisher ID can be obtained only from 2Msoft company. That means that Publisher information has been checked and approved by 2MSoft. Publisher required this ID must go in contact with 2MSoft and send all required documents or physically visit 2MSoft office. After that Publisher will get electronic key where gets Publisher ID and Digital ID Level 0. This kind of service is charged. See 2MSoft internet pages.

Password entering & Group choice

For Tutorial purposes use Public group and password “OurPassword”.



Enter password key

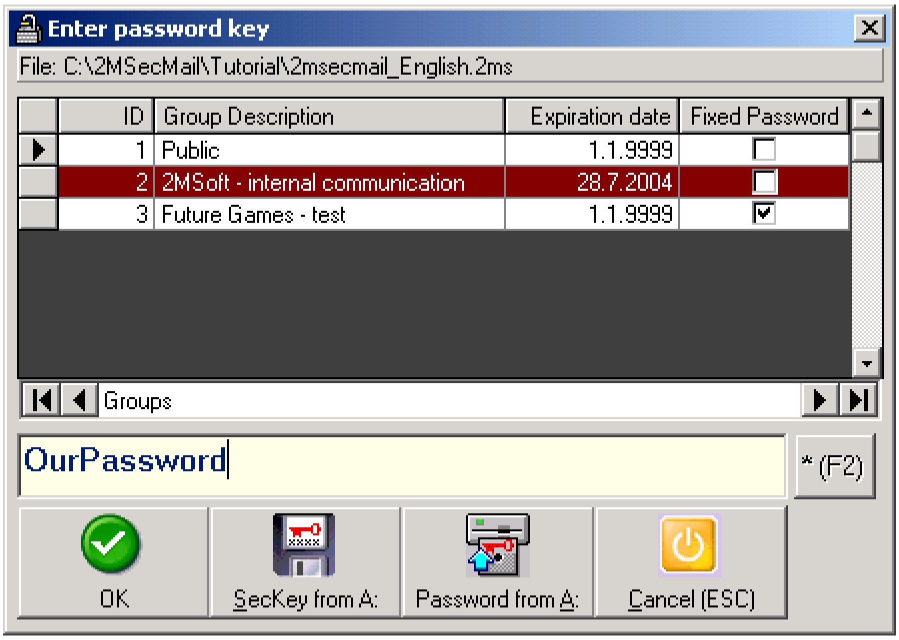
File: C:\2MSecMail\Tutorial\2msecmail_English.2ms

ID	Group Description	Expiration date	Fixed Password
1	Public	1.1.9999	□
2	2MSoft - internal communication	28.7.2004	□
3	Future Games - test	1.1.9999	☑

Groups

****

F2 key make entering of your password visible



Enter password key

File: C:\2MSecMail\Tutorial\2msecmail_English.2ms

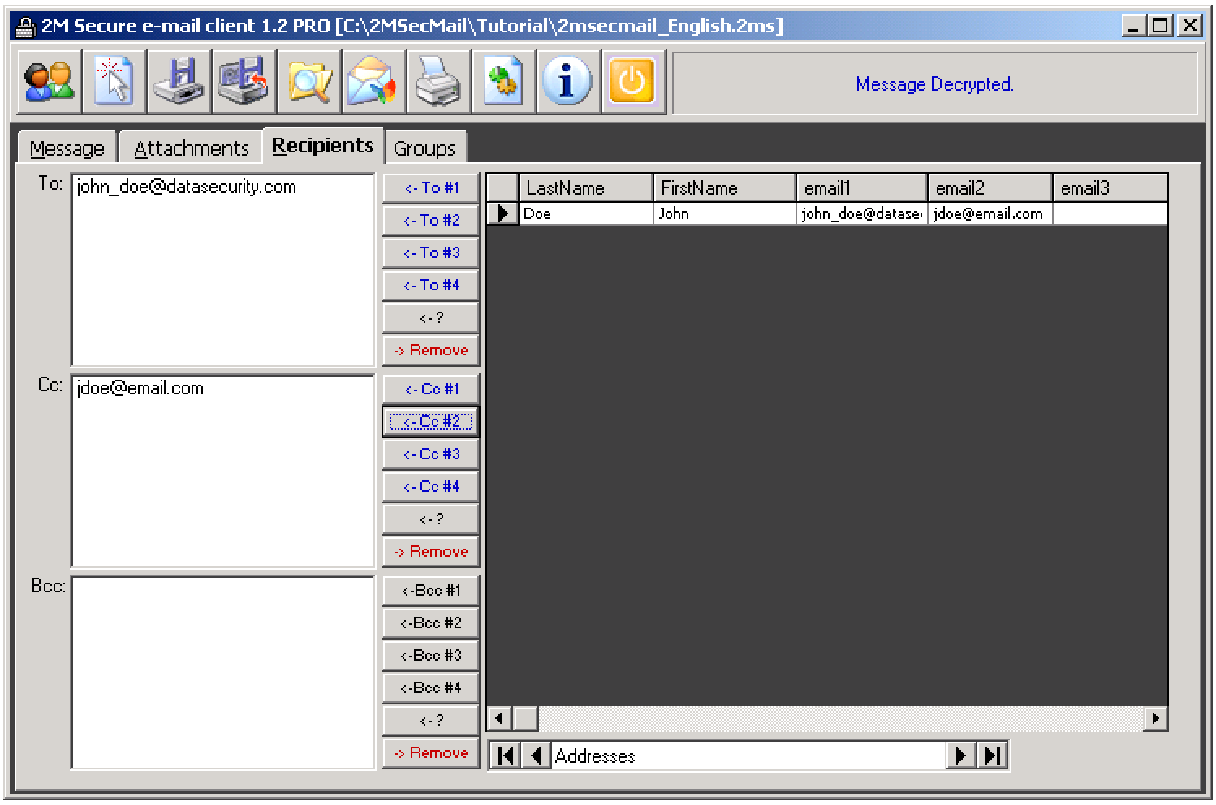
ID	Group Description	Expiration date	Fixed Password
1	Public	1.1.9999	□
2	2MSoft - internal communication	28.7.2004	□
3	Future Games - test	1.1.9999	☑

Groups

OurPassword

Instead of typing the password you can also use diskette key, and import such key directly from drive you specified in Configuration. Keep in mind, that the password imported from diskette, user will never see. But is possible to encrypt the message with this same password, but user will never know the password. SecKey is working similar, but required also entering the password. This option is most secure for document exchange.

Recipients



2M Secure e-mail client 1.2 PRO [C:\2MSecMail\Tutorial\2msecmail_English.2ms]

Message Decrypted.

To: john_doe@datasecurity.com

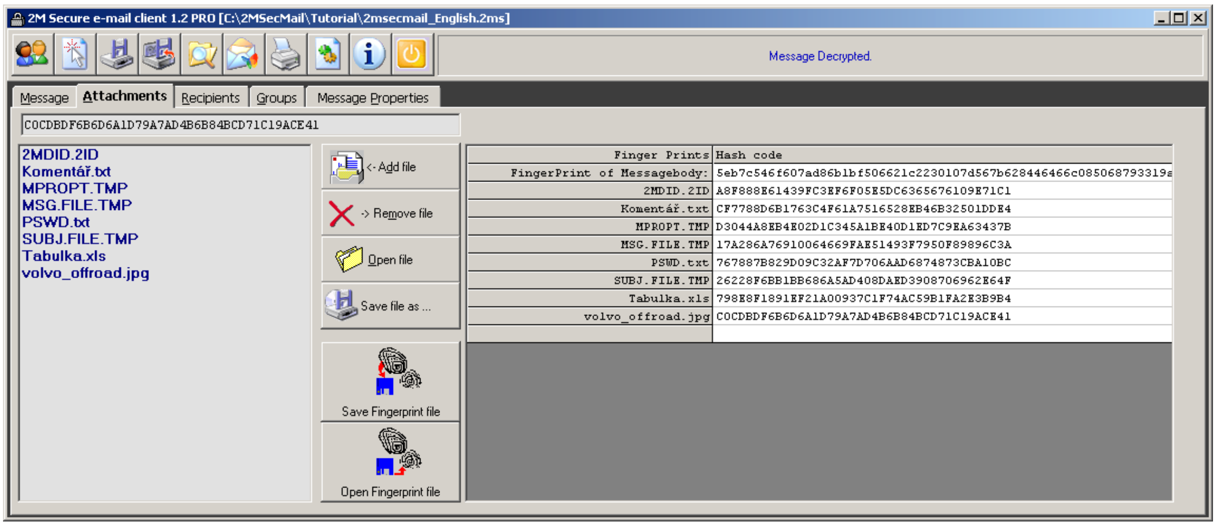
Cc: jdoe@email.com

Bcc:

	LastName	FirstName	email1	email2	email3
▶	Doe	John	john_doe@datase	jdoe@email.com	

Left table contain all contacts from Address book. Simply select required person and click to button for assigning e-mail address to appropriate list. In Address book user can have up to 4 e-mail address per person + Fingerprint e-mail. That's why exists buttons with **<-To #** *1 – 4*.
Button with **<-?** Means that user can enter whatever wants. Remove button delete selected address from the list.

Attachments



2M Secure e-mail client 1.2 PRO [C:\2MSecMail\Tutorial\2msecmail_English.2ms]

Message Decrypted.

C0CDBDF6B6D6A1D79A7AD4B6B84BCD71C19ACE41

2MDID.2ID
Komentář.txt
MPROPT.TMP
MSG.FILE.TMP
PSWD.txt
SUBJ.FILE.TMP
Tabulka.xls
volvo_offroad.jpg

Finger Prints	Hash code
FingerPrint of Messagebody:	5eb7c546f607ad86b1bf506621c2230107d567b628446466c085068793319a
2MDID.2ID	A8F888E61439FC3EF6F05E5DC6365676109E71C1
Komentář.txt	CF7788D6B1763C4F61A7516528EB46B32501DDE4
MPROPT.TMP	D3044A8EB4E02D1C345A1BE40D1ED7C9EA63437B
MSG.FILE.TMP	17A286A76910064669FAE51493F7950F89896C3A
PSWD.txt	767887B829D09C32AF7D706AAD6874873CBA10BC
SUBJ.FILE.TMP	26228F6BB1BB686A5AD408DAED3908706962E64F
Tabulka.xls	798E8F1891EF21A00937C1F74AC59B1FA2E3B9B4
volvo_offroad.jpg	C0CDBDF6B6D6A1D79A7AD4B6B84BCD71C19ACE41

Example screen with opened Fingerprint) file, which was received separately. This is for checking if the content of the message has not been changed.*

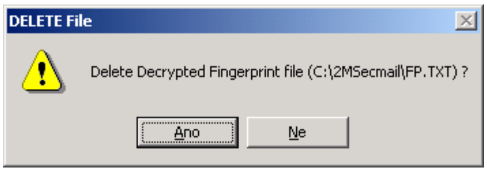
**) Explanation in section Address book*

In this Tab user can assign attachment files by clicking on <- Add file button. Also if you open Windows Explorer user can use Drag & Drop technology to copy files into the message. Simply Drag and Drop on FileList control.

The file can be opened in appropriate application by Open file button or by double click in file list. "Save file as …" exports the selected file wherever user wants.

Save Fingerprint file This function generate Fingerprints of Message body and all attached files to *.cfp file, which can be distributed. Please be aware that *.cfp file can be opened only if correct password is typed in password field. Fingerprint file is not depending on selected Group.

Open Fingerprint file This button open the *.cfp file. Prior opening file user must type correct password for Fingerprint file. After successfully opening of the file you will be prompted



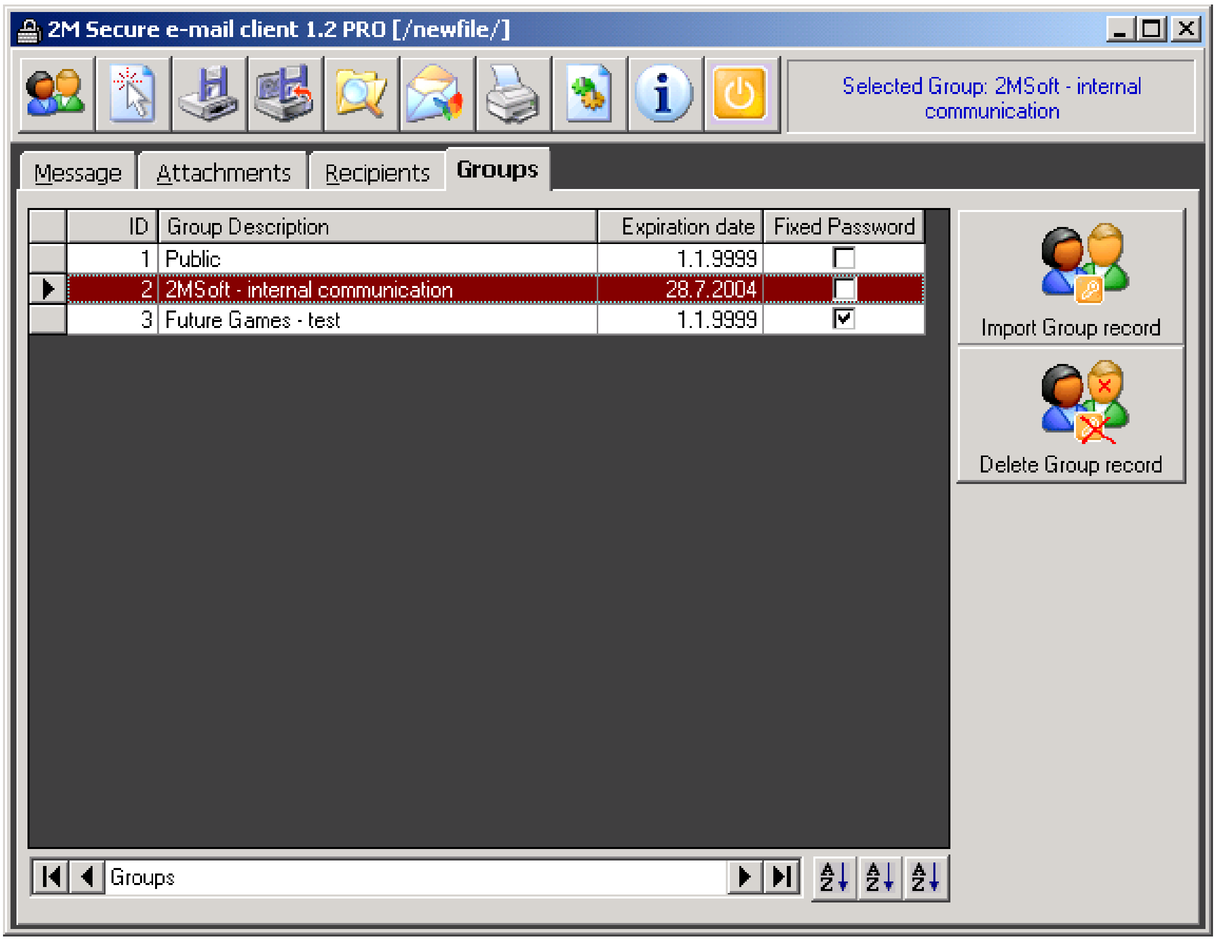
DELETE File

Delete Decrypted Fingerprint file (C:\2MSecmail\FP.TXT) ?

For deleting FP.TXT file. This TXT file is decrypted Fingerprint file. If you do not wish use information from this file press Enter or click Ok to delete of this file, otherwise press No. Table with unique hash codes and filenames will appear on left side of window.

Group usage

Administrator package contain utility for creating Groups, details are described later.
2MSecMail can import file with Group definition, which will be added to the list.
If user select Group other than Public, then the message (*.2ms file) will be encrypted by little bit different method. That means that only members of Group (all of them must have imported Group definition file) can communicate to each other. No one else can open it although he/she knows the password.



2M Secure e-mail client 1.2 PRO [/newfile/]

Selected Group: 2MSoft - internal communication

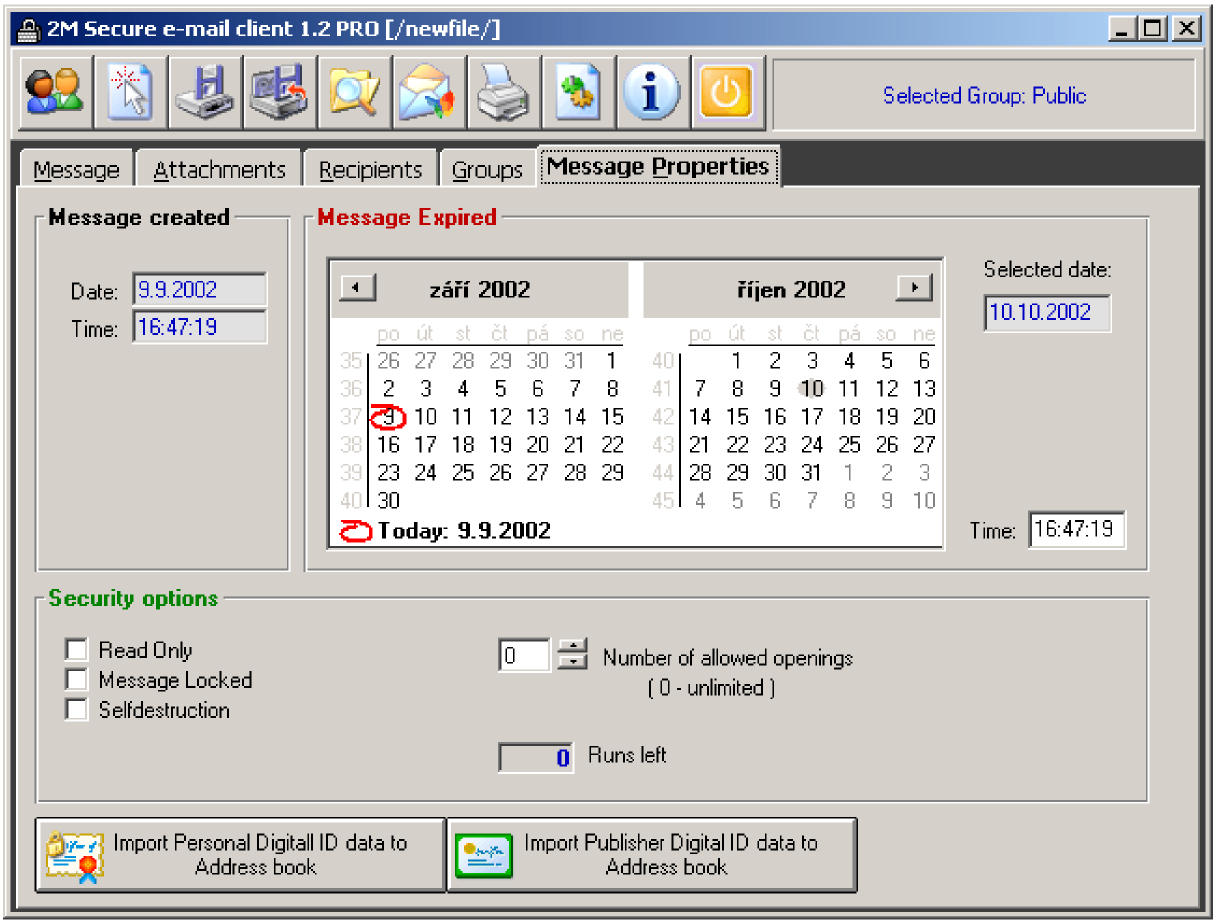
ID	Group Description	Expiration date	Fixed Password
1	Public	1.1.9999	□
2	2MSoft - internal communication	28.7.2004	□
3	Future Games - test	1.1.9999	☑

**) Note: The "Public" Group is not possible to delete*

Expiration date – if user wanted use Group after date expired, then the system will notify user about this and will not continue until another Group is selected.
Fixed Password – is nice function, that Admin define Group with Fixed password, so nobody in this Group will not use any typed password. All members of this Group can free read *.2ms files (!)

AZ↓ - sort Groups by 3 categories. Group Description, Expiration date, ID

Message properties



Selected Group: Public

Message created

Date: 9.9.2002

Time: 16:47:19

Message Expired

	po	út	st	čt	pá	so	ne
září 2002							
35	26	27	28	29	30	31	1
36	2	3	4	5	6	7	8
37	9	10	11	12	13	14	15
38	16	17	18	19	20	21	22
39	23	24	25	26	27	28	29
40	30						

	po	út	st	čt	pá	so	ne
říjen 2002							
40		1	2	3	4	5	6
41	7	8	9	10	11	12	13
42	14	15	16	17	18	19	20
43	21	22	23	24	25	26	27
44	28	29	30	31	1	2	3
45	4	5	6	7	8	9	10

Today: 9.9.2002

Selected date: 10.10.2002

Time: 16:47:19

Security options

□ Read Only
□ Message Locked
□ Selfdestruction

0 Number of allowed openings (0 - unlimited)

0 Runs left

Import Personal Digitall ID data to Address book
Import Publisher Digital ID data to Address book

One of very interesting feature of 2MSecMail. Each file (Message) contain Date and Time of creation (saving or export). Opening file (Message) on computer with Date and Time less than Creation Date and time is NOT possible! User can define Expiration date and time. After that Date and time nobody can open the message. Expiration date can be easily chosen from Calendar.

Also Security options advanced the feature:

Read Only mode – means user can only see the message and open attachments. No print or export is possible. Adding files is forbidden. After checking this mode, automatically Message Locked is checked also.

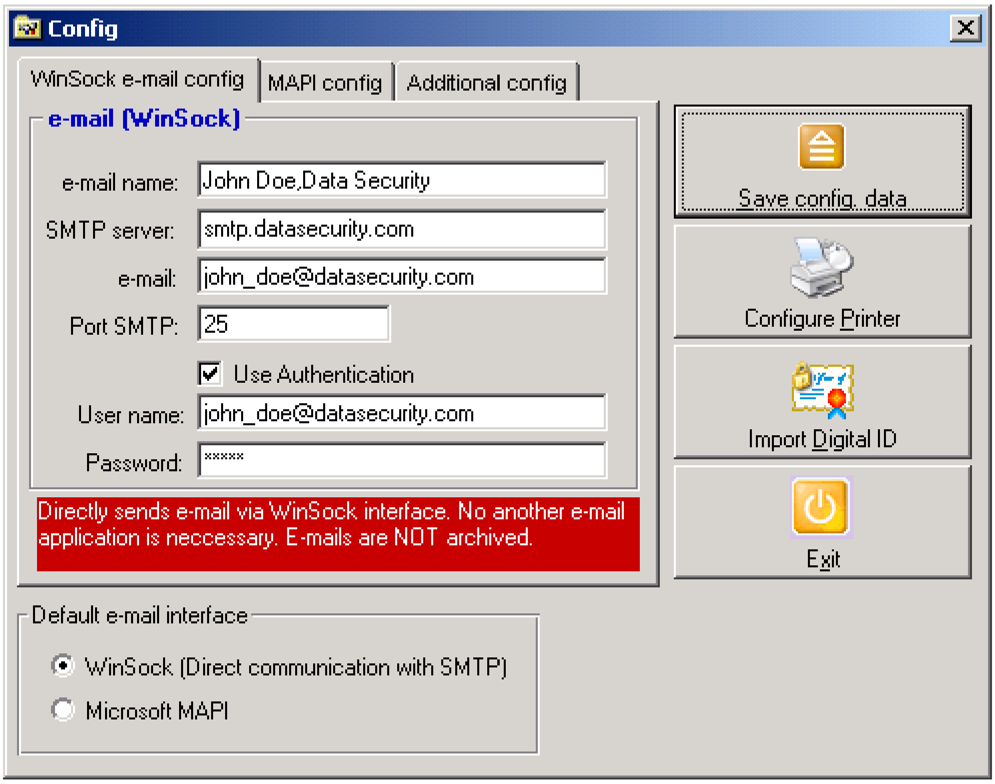
Message Locked – means everything is possible except changing Password, Subject and body of message. Adding files is forbidden.

Self-destruction – means that file (Message) after Expire or abandoned Run counter will destroy the message file!

Number of allowed openings – quite clear. How many times can be message opened. *Note: Keep in mind that if message is too large and Counter>0 then the opening of message will be double time longer, because first time must be message opened and decrypted, then must save new counter value and immediately save back with encryption.*

Import Personal or **Publisher Digital ID data to Address book** – if you have already opened Digital ID file, you can import data like name, company, address and emails to your Address book. For example good function to get all data about sender of message you've received ;-)

Configuration



e-mail (WinSock)

e-mail name: John Doe,Data Security

SMTP server: smtp.datasecurity.com

e-mail: john_doe@datasecurity.com

Port SMTP: 25

☑ Use Authentication

User name: john_doe@datasecurity.com

Password: *****

Directly sends e-mail via WinSock interface. No another e-mail application is neccessary. E-mails are NOT archived.

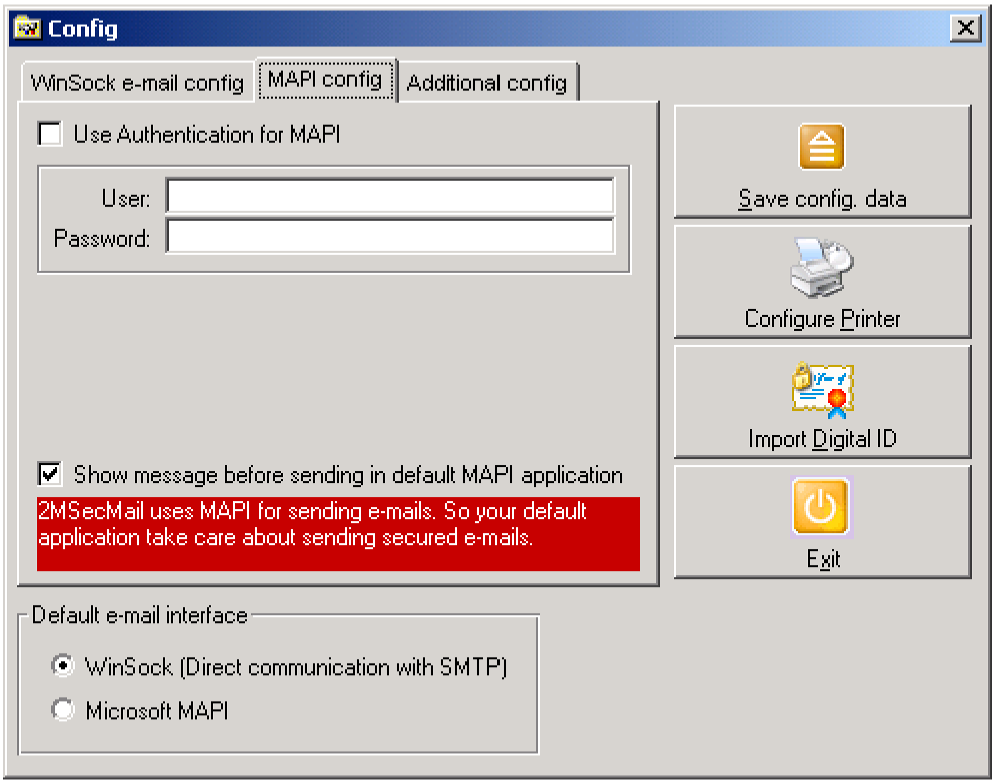
Default e-mail interface

● WinSock (Direct communication with SMTP)

○ Microsoft MAPI

First Tab offer to user config WinSock environment. First of all user should know what kind of connection can or will use.
WinSock – direct connection to SMTP server. Usually works only if connected to the internet via Analog or ISDN modem. While sending message user must be connected to the internet. Settings should be consulted with your Network administrator.

MAPI – uses standard Microsoft mail environment like MS Outlook Express, MS-Outlook. When sending, connection to the internet is not necessary.



☐ Use Authentication for MAPI

User:

Password:

☑ Show message before sending in default MAPI application

2MSecMail uses MAPI for sending e-mails. So your default application take care about sending secured e-mails.

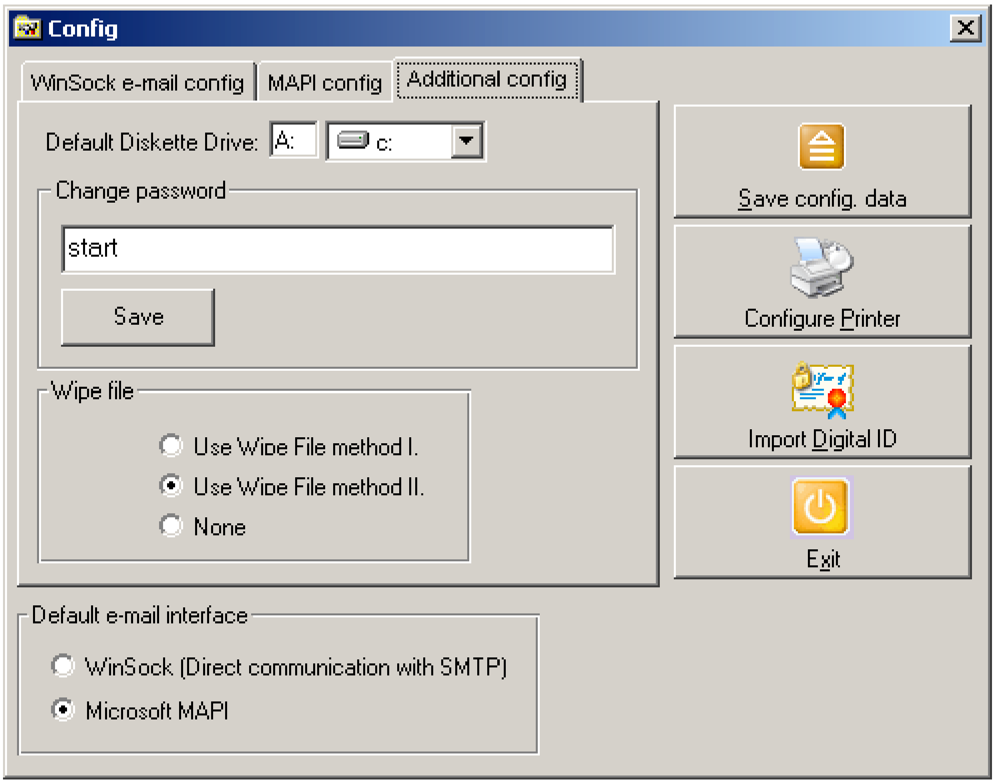
Default e-mail interface

● WinSock (Direct communication with SMTP)

○ Microsoft MAPI

Checkbox "Show message before …" – after sending message from 2MSecMail user will be prompted in MAPI default Mail application *) for editing and sending message.

*) In *Control panel* and *Internet Options* user can define in folder *Programs* which application is default for handling e-mails in user environment. Ask your administrator in case of some questions.



Default Diskette Drive: A: c:

Change password

start

Wipe file

○ Use Wipe File method I.

● Use Wipe File method II.

○ None

Default e-mail interface

○ WinSock (Direct communication with SMTP)

● Microsoft MAPI

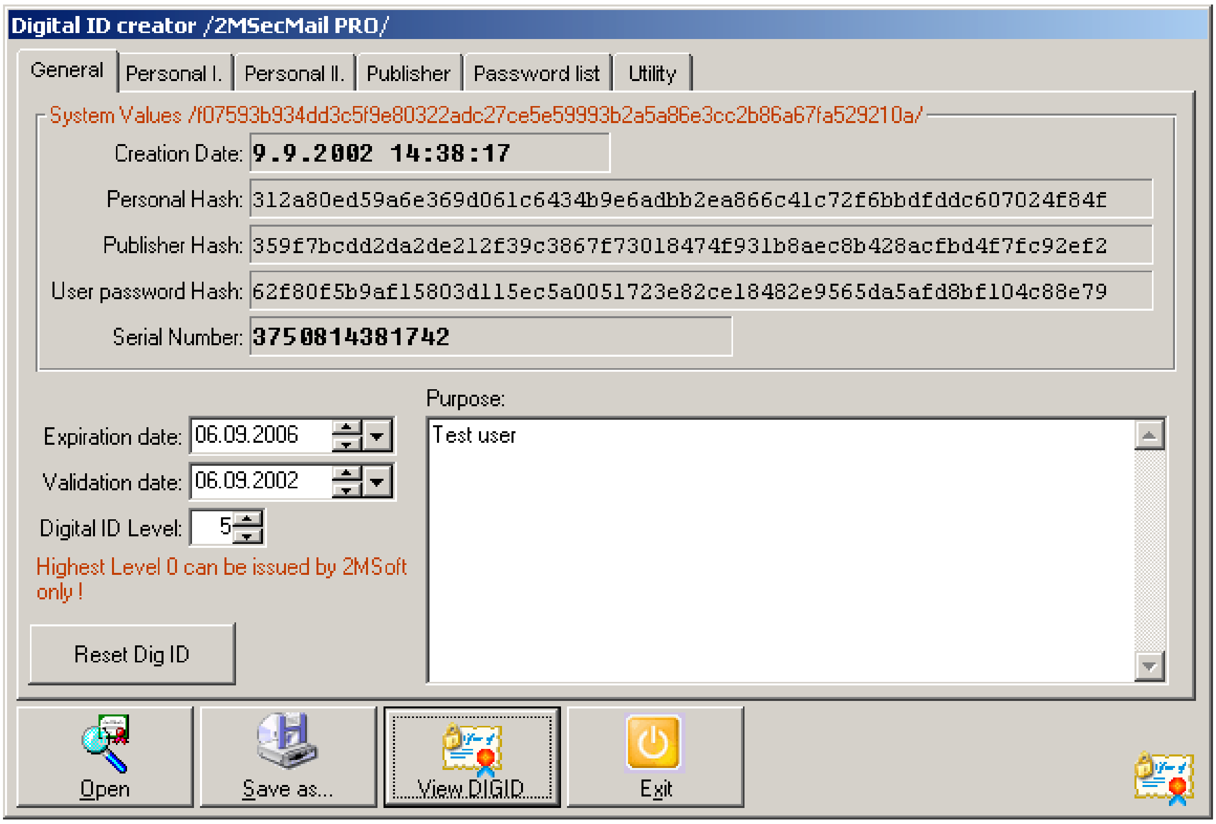
Here user can define Diskette drive (can be also Hard drive), but keys will be saved to the root of drive.

Change password – after installation of 2MsecMail is as default password "start". Here user can change the password. The current password is displayed in text box.
If you forget the password then doesn't exist any way how to get main database back!

Wipe file – this is method how destroy file which should be erased from hard drive. Method I is the slowest one, but most secure. No one can undelete temp or other file and make reconstruction. For this method is necessary to have fast computer (Pentium III 600 MHz). Method II use little bit less secure method but much faster than Method I. Recommended use at least Method I. (!).
None – means that files are only deleted but not destroyed at all, so hacker can find them undelete on you PC. This method is fastest.

Import Digital ID – when you receive your Digital ID on the diskette or by e-mail from your Administrator, here you can import this Digital ID as your default one. Most secure solution is open Digital ID from the diskette each time you are assigning DigID to your message. If you keep diskette on safe place then nobody can make a copy and Digital ID is really yours. Administrator is having one copy as well.
Import function require password of Digital ID. Then is displayed in the Digital ID Viewer and after that saved as default – default.2id file.

Digital ID creator (Administrator kit)



System Values /f07593b934dd3c5f9e80322adc27ce5e59993b2a5a86e3cc2b86a67fa529210a/

Creation Date: 9.9.2002 14:38:17

Personal Hash: 312a80ed59a6e369d061c6434b9e6adbb2ea866c41c72f6bbdfddc607024f84f

Publisher Hash: 359f7bcdd2da2de212f39c3867f73018474f931b8aec8b428acfbd4f7fc92ef2

User password Hash: 62f80f5b9af15803d115ec5a0051723e82ce18482e9565da5afd8bf104c88e79

Serial Number: 3750814381742

Expiration date: 06.09.2006

Validation date: 06.09.2002

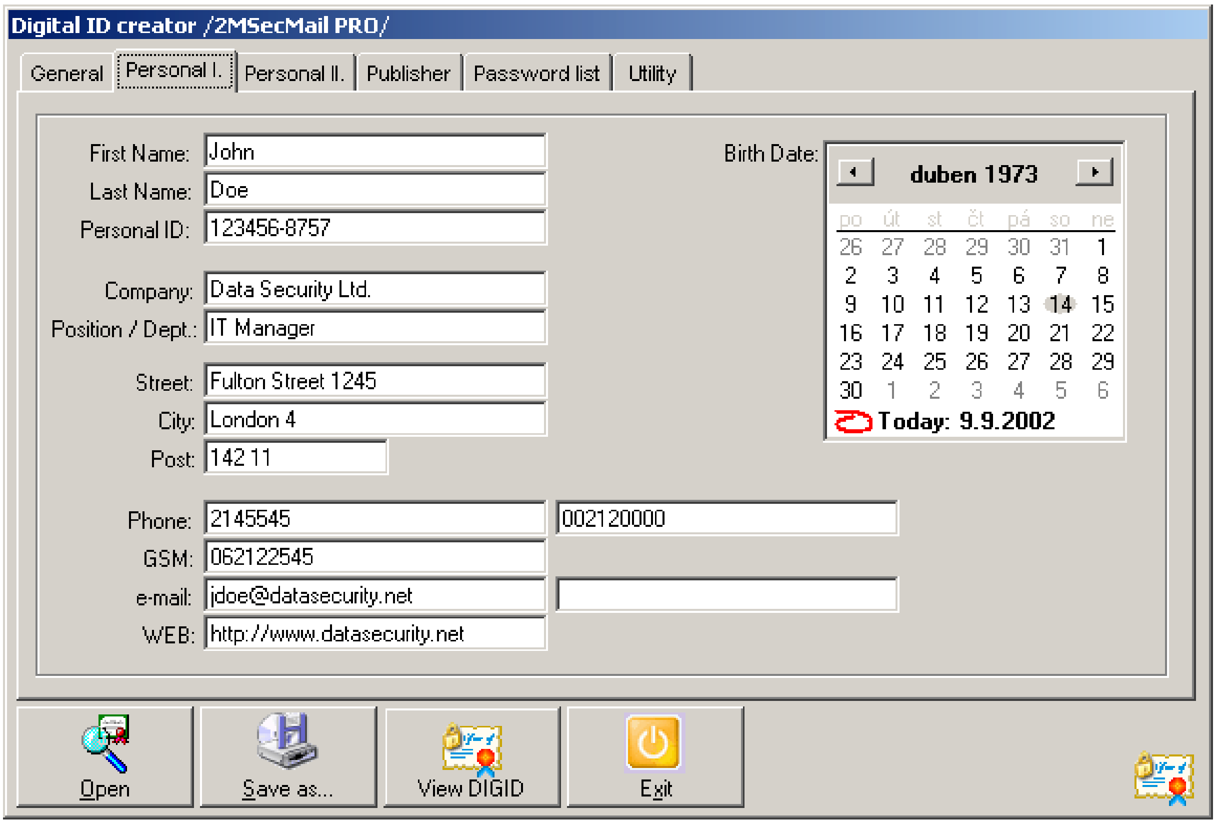
Digital ID Level: 5

Highest Level 0 can be issued by 2MSoft only !

Purpose:

Test user

Digital ID Creator is for creating Digital ID for users. This tool should have only Administrator. This creator is accessible via password of administrator. After installation the default password is "`start`". First Tab contain General information. Expiration date - after this date this Digital ID can't be imported or viewed in 2MSecMail. Of course can be opened in this tool. Each Digital ID depend of selected password from Tab "Password list".



First Name: John
Last Name: Doe
Personal ID: 123456-8757

Company: Data Security Ltd.
Position / Dept.: IT Manager

Street: Fulton Street 1245
City: London 4
Post: 142 11

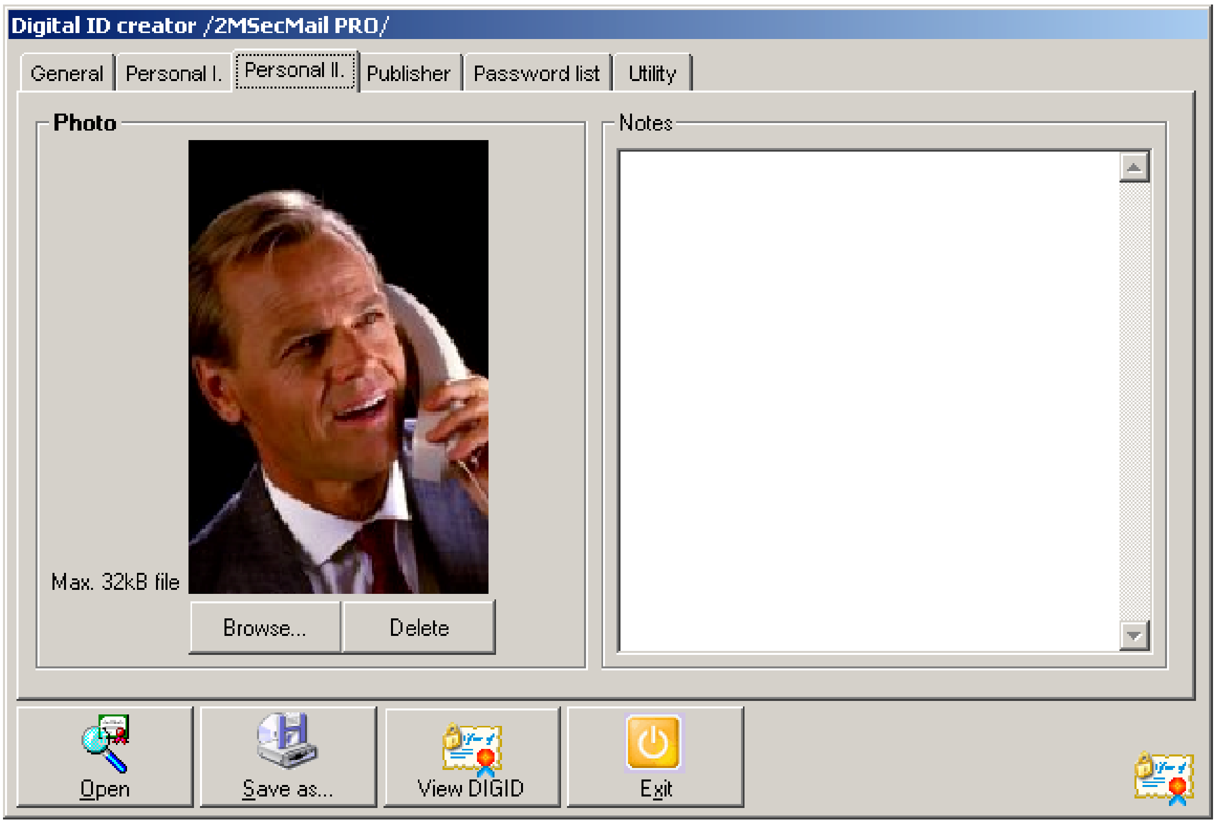
Phone: 2145545 002120000
GSM: 062122545
e-mail: jdoe@datasecurity.net
WEB: http://www.datasecurity.net

Birth Date: duben 1973

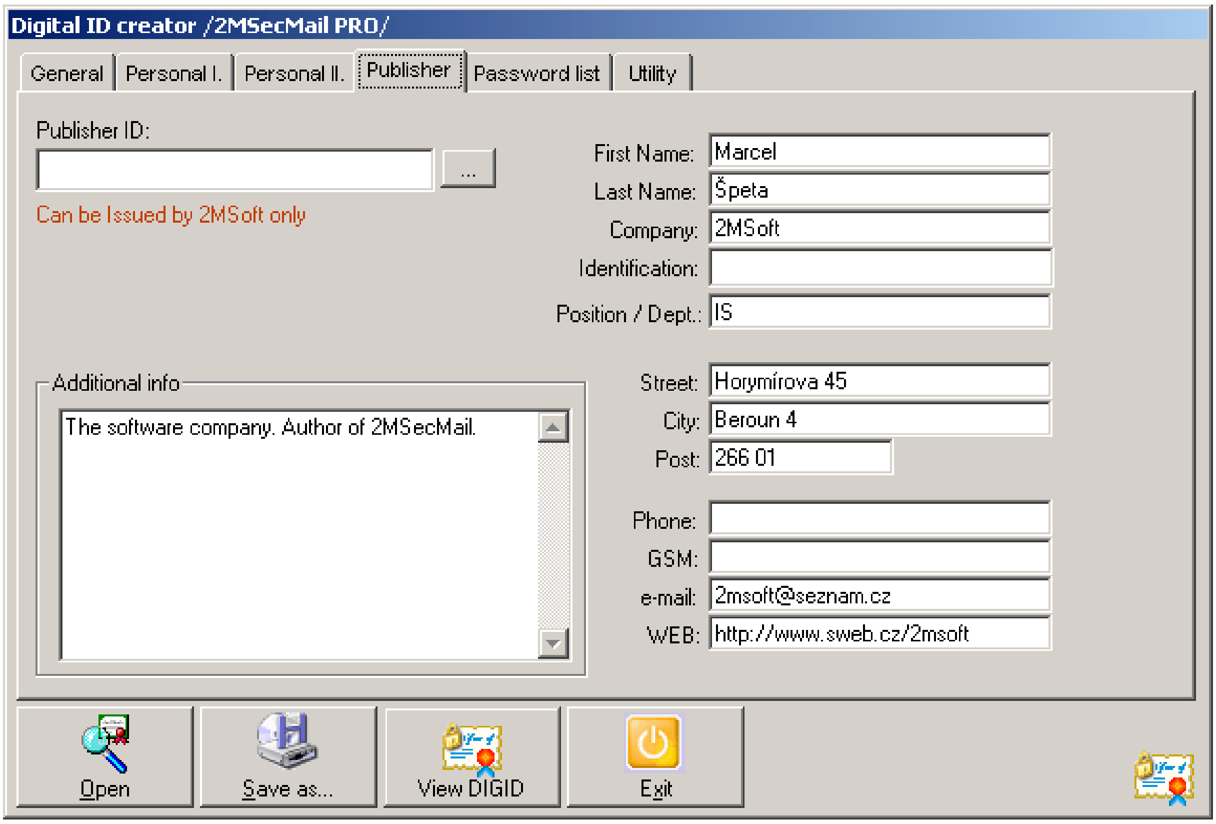
po	út	st	čt	pá	so	ne
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Today: 9.9.2002

Here administrator can fill out all Personal information



In this section can be assigned Photo from JPG,GIF or BMP file which doesn't exceed 32kB. Delete means deletion from Digital ID - not from disk !



Publisher ID:

Can be Issued by 2MSoft only

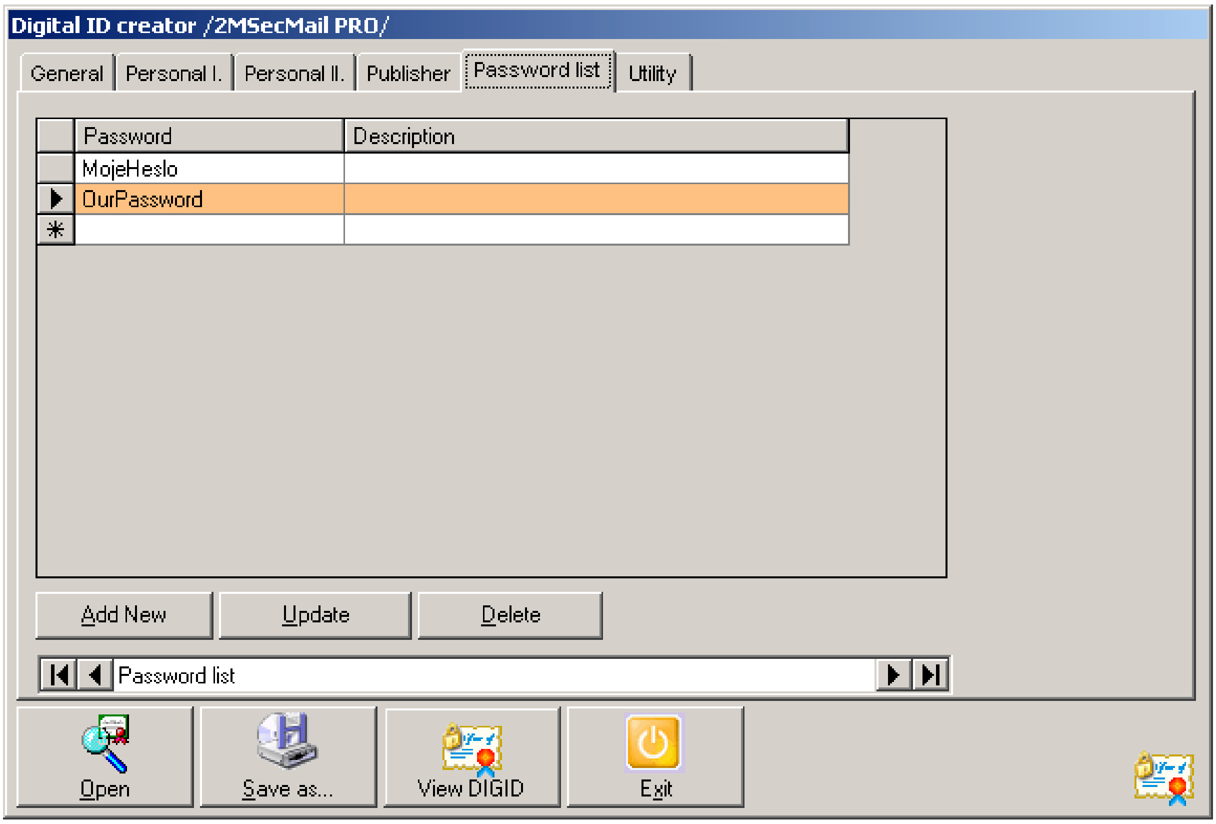
First Name: Marcel
Last Name: Špeta
Company: 2MSoft
Identification:
Position / Dept.: IS

Additional info: The software company. Author of 2MSecMail.

Street: Horymírova 45
City: Beroun 4
Post: 266 01

Phone:
GSM:
e-mail: 2msoft@seznam.cz
WEB: http://www.sweb.cz/2msoft

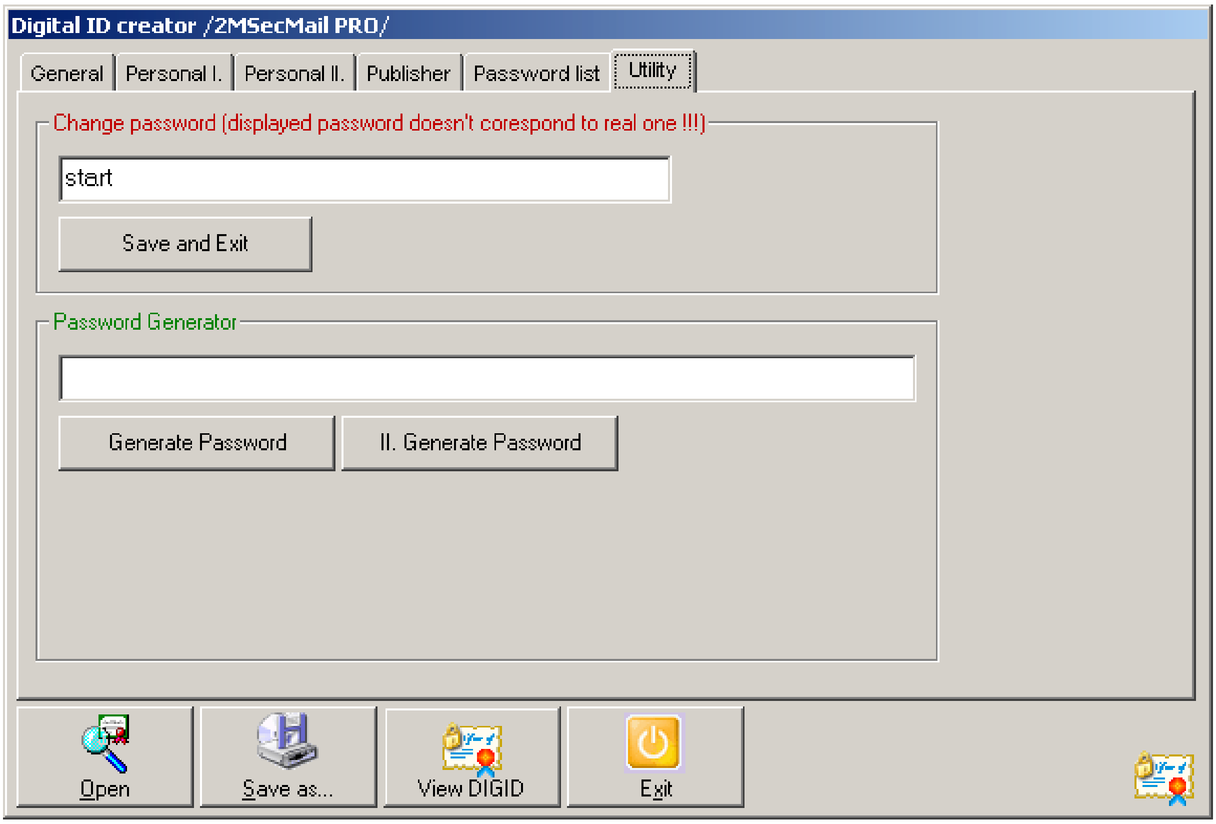
All information about Publisher. Publisher ID can be obtained from 2MSoft only. More details see page 10 – 11.



Digital ID creator /2MSecMail PRO/

Password	Description
MojeHeslo	
OurPassword	

Digital ID will be encrypted by defined password from password database. User must know the Password otherwise can't assign Digital ID to his/her message.

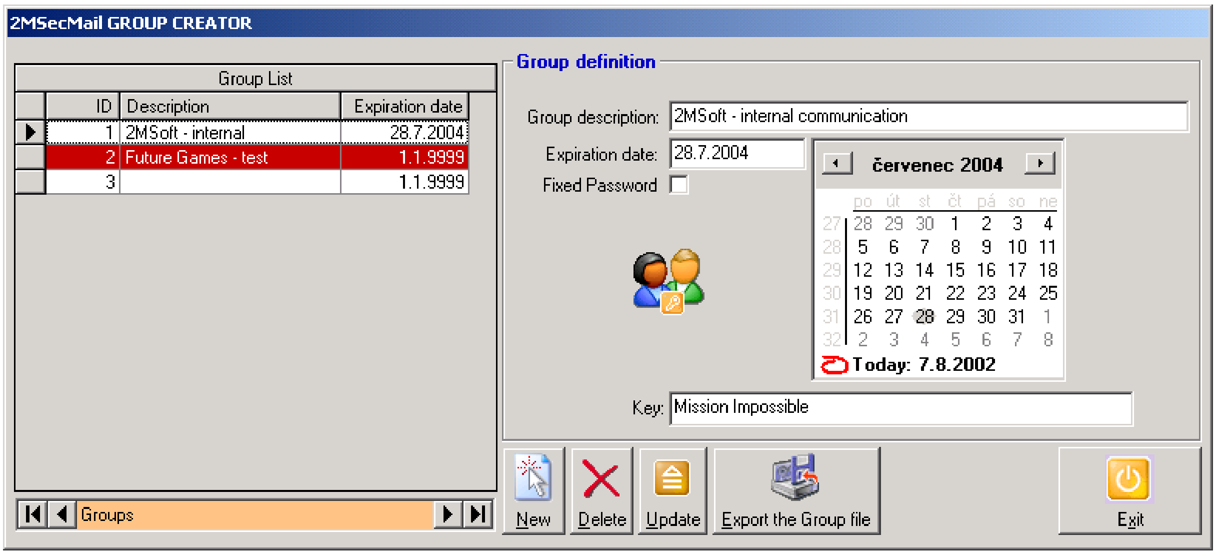


start

In the **Utility** folder user can change the application password. When saved then application must restart.

Password Generator is tool for randomly selection from vocabulary of English words. Button “II. Generate…” generate password on base of vocabulary and special algorithm. This password can be transferred via Microsoft Windows Clipboard to Password list or any another application.

Group Manager (Administrator kit)



2MSecMail GROUP CREATOR

Group List

ID	Description	Expiration date
1	2MSoft - internal	28.7.2004
2	Future Games - test	1.1.9999
3		1.1.9999

Group definition

Group description: 2MSoft - internal communication

Expiration date: 28.7.2004

Fixed Password □

červenec 2004

	po	út	st	čt	pá	so	ne
27	28	29	30	1	2	3	4
28	5	6	7	8	9	10	11
29	12	13	14	15	16	17	18
30	19	20	21	22	23	24	25
31	26	27	28	29	30	31	1
32	2	3	4	5	6	7	8

Today: 7.8.2002

Key: Mission Impossible

This tool creates Group definition. In calendar Admin can select Expiration date, choose if Group is using fixed password and must define the Key. Key should be secret information.

Fixed password make Group that members will not use their own password but generated one in this Group. All members of this Group can free communicate to each other without typing password.

File extension description

***.2ms**	Message / document encrypted by 2MSecMail. All files are compressed and encrypted there.
***.2id**	Digital ID file
***.2mg**	Group definition file
***.cfp**	Fingerprint file
KEY.DAT	Diskette key
SKEY.DAT	SecKey