IDGuard for Palm OS® v 2.01
User manual

1 About IDGuard

Resco's IDGuard maintains your sensitive information such as user names, passwords, PINs, accounts, banking information, records, codes etc. Besides this personal information IDGuard can store images and other files (called attachments), whereby all stored data is securely encrypted and is accessible only by entering your password.

Basic features

- 10 predefined record types (templates)
- User-defined templates
- User-defined categories to group records into
- Record notes, reminders and attachments
- Auto-lock option
- Secure AES encryption
- Password generator

Secure Documents

You can create special document records containing just one file. When you tap such a record, the document will be opened in the associated application – viewer, reader etc.

Alternatively, you can attach files to any record. It works similarly to an e-mail application.

Whichever way you use, your documents will be secured before prying eyes. What is even more important – as long you use common file types (office documents, images, audio) – IDGuard provides the complete workbench incl. document opening, editing and saving.

Other advanced features

- Multiple data sources
- Import/Export to several password managers
- Direct camera control (take a photo of your credit card)
- Audio recorder (make a sound attachment with the built-in microphone)
- Built-in viewer and audio player (mp3, wav)
- Several GUI layouts (tree, list, icons etc.)

Security

IDGuard employs industry-standard AES encryption. According to crypto-experts, this encryption is good enough to survive dozens of years. Hence, you only need to concentrate on the weak point, which is your password.

IDGuard comes with a Password Generator that can measure the strength of your password.

The password is not stored anywhere and once you lose it, there is no way to recover the stored data; even the Resco support team cannot help in such a case.

1.1 Requirements, (un)installation, registration

System requirements

Any Palm OS 5+ PDA (**except Treo 600**) with at least 800K of free RAM.
An expansion card is required for the work with attachments. The amount of card space that is needed depends on the size of the attachments.

Installation

To install IDGuard:

- Add IDGuard.prc file to the Palm Desktop Install Tool:
  (Double-click the file, or drag the file onto the Install Tool window)
- Start HotSync on your Palm Handheld

IDGuard can be installed either to the internal memory or to a memory card.

In case of card installation reminder and auto-lock will not work.

Uninstallation

1. Delete the card data by deleting all attachments (or delete all accounts)
2. Delete IDGuard from the Palm Launcher.

Registration

IDGuard for Palm OS® comes with a free 14-day trial.

The trial is functionally identical with the full version except that it stops working after 14 days. You can get it working again either by either purchasing the unlock key or by installing a trial of a higher version.

After the purchase of the full product, you will receive an unlock key which will allow unlimited use of the purchased version of the product. Resco’s official policy is that the **upgrades** are free within one year from the date of the purchase or as long as the major product version does not change

1.2 Upgrading to IDGuard v2

Summary of the news implemented in the IDGuard v2:

- The Desktop component (Windows only)
- Layout: Background color, possible exclusion of the templates from the tree
- Internal viewer of the txt attachments
- More icons to select from

The most important extension is the ability to process the data on the desktop. As there is a separate manual explaining the desktop features, let's bring just a brief list of the steps you need to take:

- Install IDGuard for Palm OS v2 (the old version does not support the synchronization)
- Moreover, IDGuard must be installed into the main memory (RAM); otherwise the synchronization will not work.
- The old Data Sources must be upgraded to the new format. IDGuard offers this possibility in the Login dialog.
- Install IDGuard Desktop and the Hotsync conduit. (Hotsync setup dialog)
- Next Hotsync will copy the device Data Source(s) to the desktop. Since this moment the Hotsync will synchronize the changes between the PC and device Data Sources.

Note that **the upgrade to v2 is free** and the Desktop IDGuard accepts the same unlock code as used for the device version. (You need to type your device HotsyncID as the user name in the Desktop registration dialog.)

2 IDGuard tour

When you launch IDGuard for the first time, you will be asked to setup the data storage (data source):

- Data source name: You may keep predefined name “Default”. You may create another data source later, when there will be a need to share part of the data with other persons.
- Sample records and templates: these serve as convenient starting point, but you may decide to create everything yourself.
- Master passwords: We recommend that you setup a password (IDGuard can work also with non-encrypted data) and that the password is good enough so that it cannot be easily guessed.

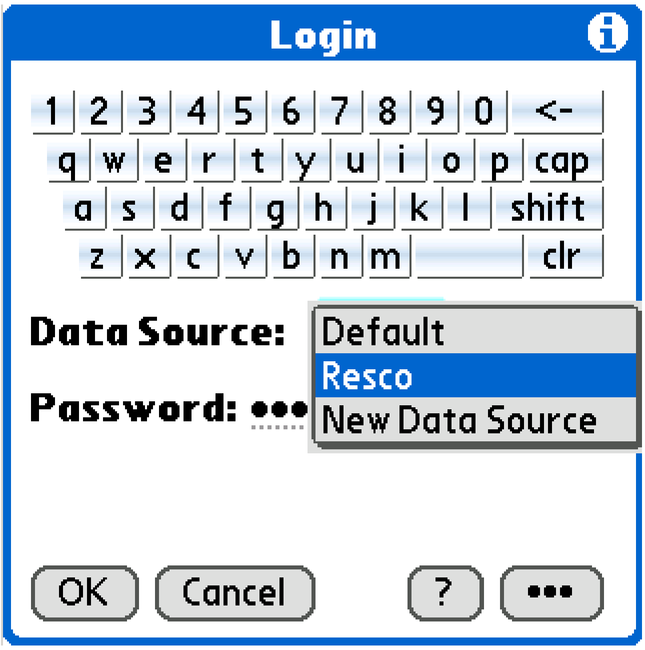


Figure 1 - Data Source selection (The buttons on the right side serve for hint and password masking)

Most people will probably work with just one data source. However, there are situations when maintaining more data sets comes handy. Figure 1 shows an example with multiple data sources. (“Default”and “Resco”)

You can change the password later (main menu, *Change Password* command). However, this procedure may take longer – especially if you have attachments.

(x) Upgrade Data Source version

IDGuard v2 shows this checkbox for old Data Sources created with IDGuard v1. Check this option if you want to synchronize with the Desktop IDGuard.

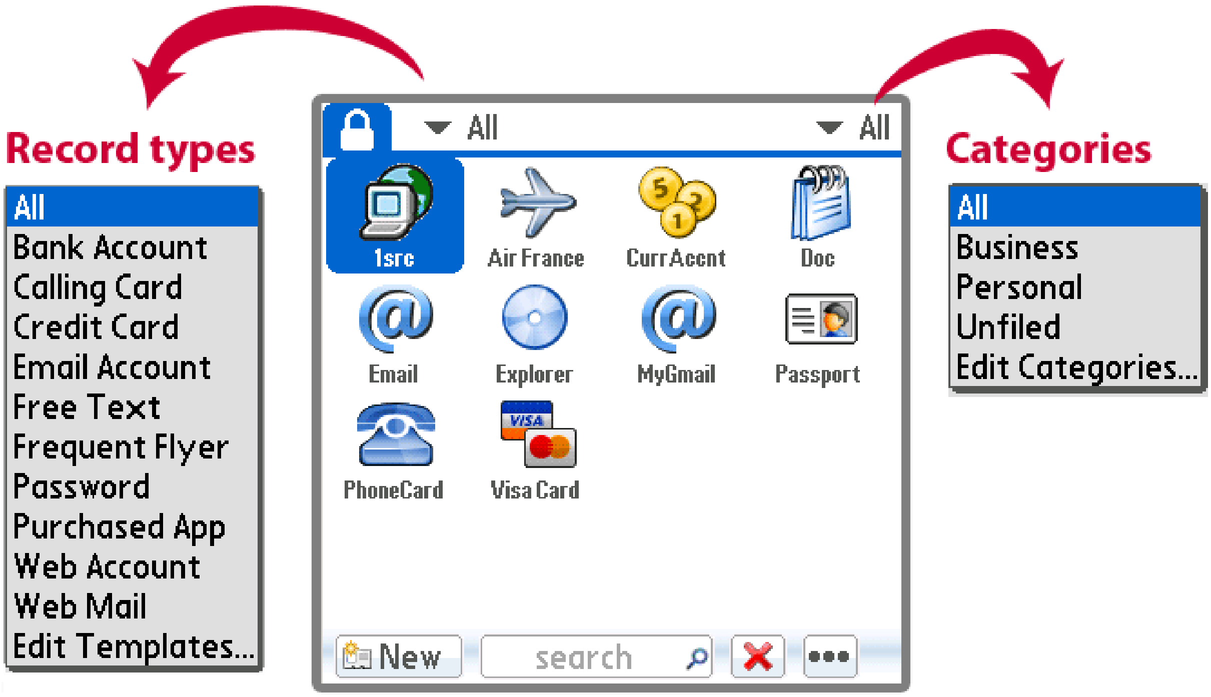


Figure 2 - Main screen - Icon View (IDGuard v1.20 contains also button for toggling icons/list)

Figure 2 shows the situation after you create your first data source. You will see a couple of sample records, predefined record types and categories. Both record types and categories can be used as filters.

The buttons at the bottom allow to:

- Create a new record
- Search for a record by typing the first character(s) – this works similarly to the Treo Phone application
- Delete a selected record
- The last button serves for masking and you will see its meaning later.

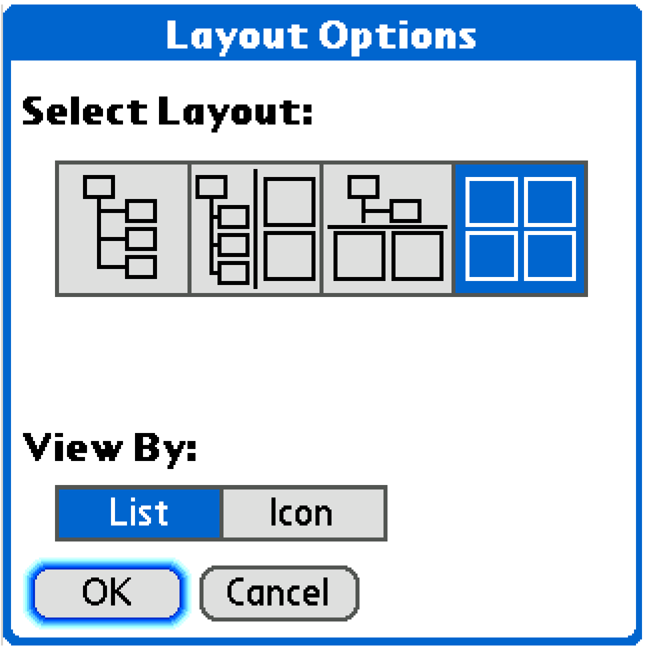
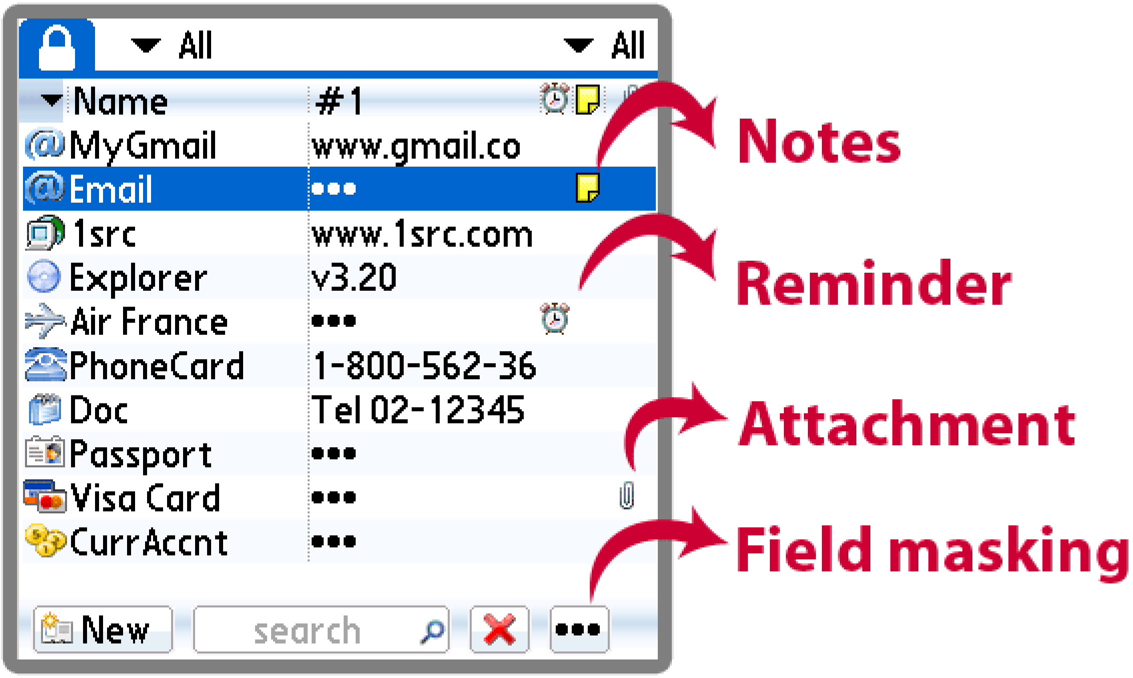


Figure 3 - IDGuard layouts

As the Figure 3 shows, you can select several alternative layouts depending on your preferences - as a tree, as a list, as icons, or any combination.

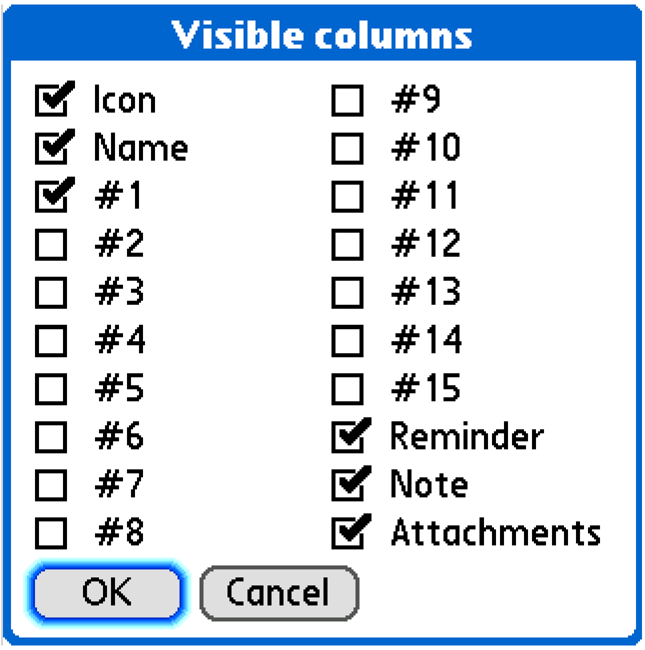


Name	#1
MyGmail	www.gmail.co
Email	●●●
1src	www.1src.com
Explorer	v3.20
Air France	●●●
PhoneCard	1-800-562-36
Doc	Tel 02-12345
Passport	●●●
Visa Card	●●●
CurrAccnt	●●●

Figure 4 - List View (IDGuard v1.20 contains also button for toggling icons/list)

For example, Figure 4 shows another layout - the list view. Visible columns are specified through the Column Selection dialog. Every record can have various add-ons such as notes or attachments – we'll talk about them later.

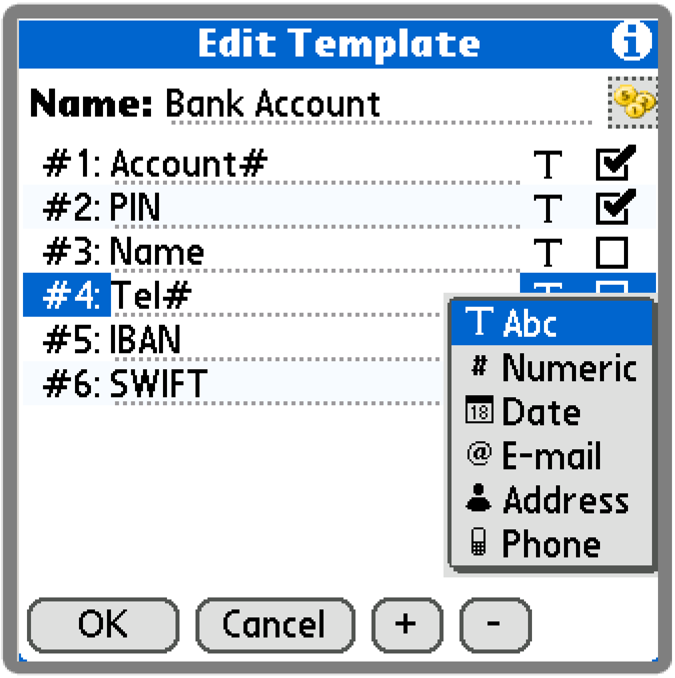
You see also the effect of the mask button. It decides whether the sensitive fields (as specified by the record template) are shown or masked as dots.



Visible columns

☑ Icon
☑ Name
☑ #1
□ #2
□ #3
□ #4
□ #5
□ #6
□ #7
□ #8
□ #9
□ #10
□ #11
□ #12
□ #13
□ #14
□ #15
☑ Reminder
☑ Note
☑ Attachments

Figure 5 - Column selection for the List View



Edit Template

Name: Bank Account

#1: Account# T ☑

#2: PIN T ☑

#3: Name T □

#4: Tel#

#5: IBAN

#6: SWIFT

Figure 6 - Record template specifying 6 columns

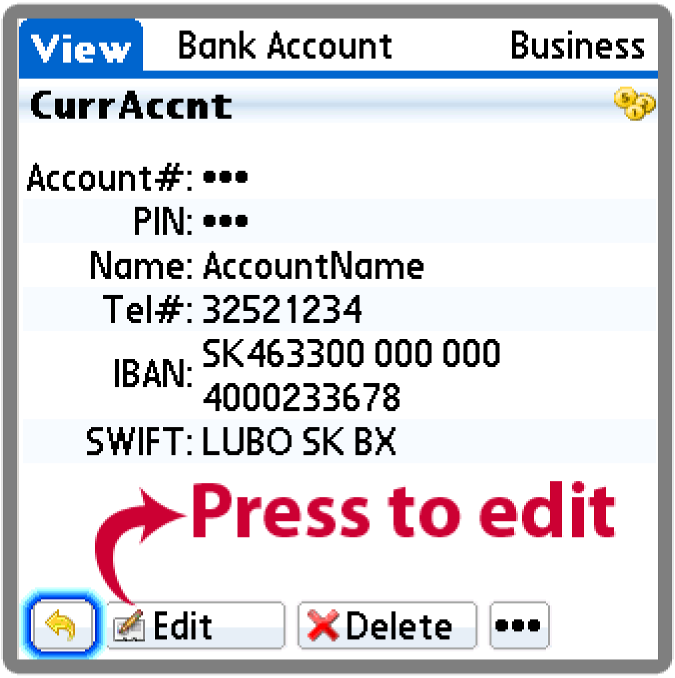
Every data record belongs to a template. The template specifies the column attributes:

- Column name,
- Data type ranging from Text up to the Phone number. Data type influences data editor used. E.g. if you select Phone, the record editor lets you use phone number lookup in the Address book.
- Mask attributes: Selection denotes sensitive fields that can be masked as shown in Figure 4.

Note there is a special **Free Text** template that does not use columns. It is something similar as if you used the Palm Memo application.

Columns are added/deleted using +/- buttons. You can use up to 15 columns.

The icon (top right corner) serves as the default icon for new records assigned to this template.



View Bank Account Business

CurrAccnt

Account#: •••

PIN: •••

Name: AccountName

Tel#: 32521234

IBAN: SK463300 000 000 4000233678

SWIFT: LUBO SK BX

Press to edit

Figure 7 - Record Preview

By tapping a record icon you open the record preview. You can open the record editor, delete the record, and mask/unmask the sensitive fields.

Although not shown in the figure, the record preview also shows:

- Notes: By tapping the note you open the notes viewer.
- Attachments: By tapping an attachment you get a choice to open (save, delete) the attachment. Opening means showing the file in Documents To Go (for DOC/XLS…), Resco Viewer (for a jpg image) etc. It depends on the attachment type and the software you have on your PDA. (More details later.)
- Reminder: This is an alarm consisting of an exact time instant and a text. The purpose is to remind the user that something needs to be done, e.g., that a web login has expired.

If you want to modify the record (edit the notes, add attachments etc.), you need to tap the *Edit* button.

All attachment types are shown schematically in the next figure.

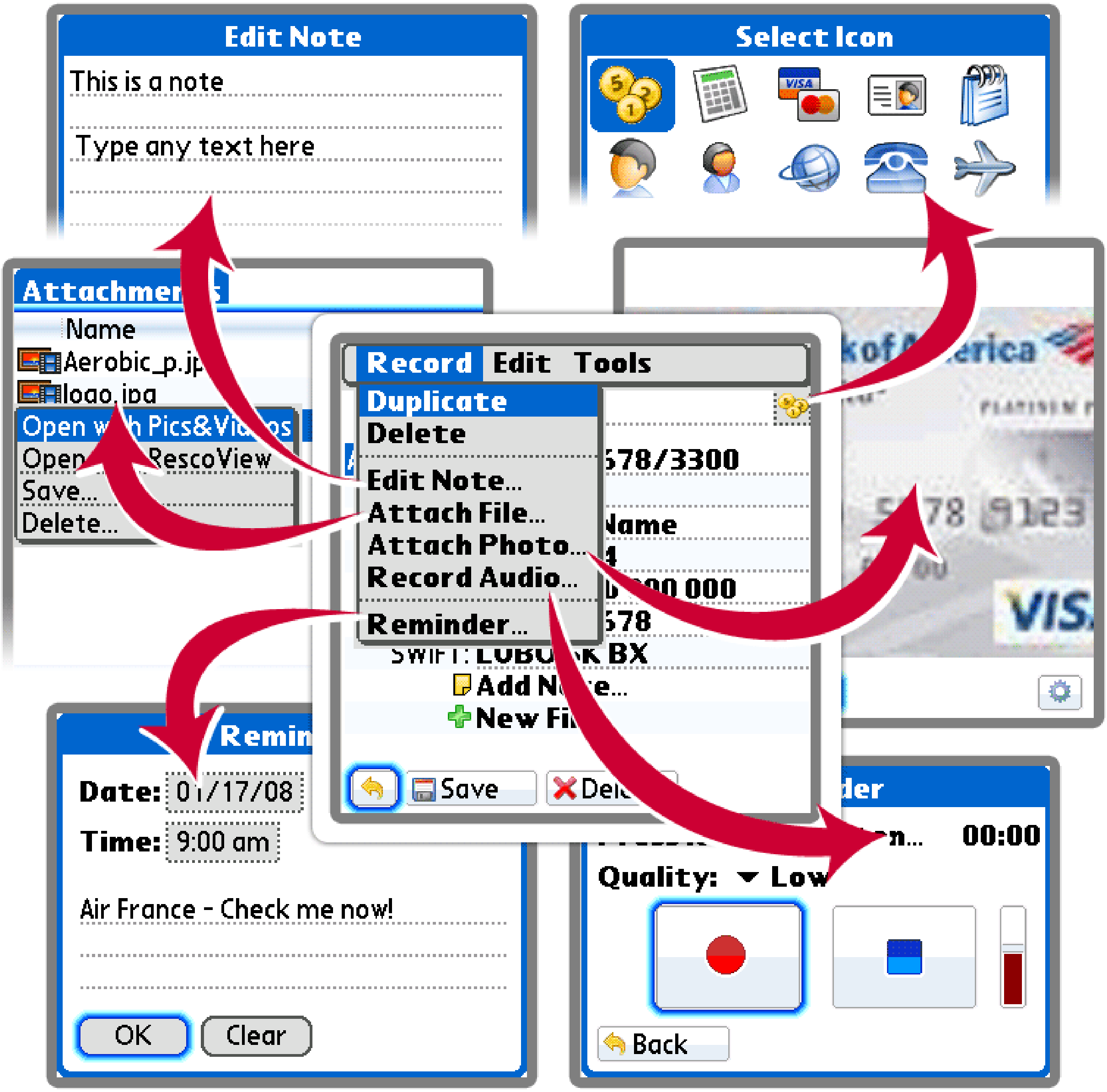


Figure 8 - Record Editor

As already mentioned, the records consist of the textual information (organized into columns) plus optional notes, attachments and a reminder. Although you can add any file as an attachment, there are two special attachment types that receive extended support:

- Camera photo: If you have a PDA equipped with a camera, you can make a photo and attach it to the record.
- An audio attachment: If your PDA supports audio recording, you can make a sound attachment. The interface will be familiar to the users who use to work with audio recording. It enables also the testing of the recorded sound. Note that the reply quality depends very much on the processor speed and even more on the speed of your SD card.

3 Safety

The safety of the stored data is the key factor of any password manager. We shall explain here the storage scheme used in the IDGuard as well as potential risks the user should be aware of.

3.1 AES and security

IDGuard uses AES (Advanced Encryption Standard) encryption.

AES is a symmetric key encryption technique adopted as common standard for safe encryption.

When talking about security, there is no such thing as absolutely secure algorithm; any code can eventually be broken. A better way to think of this is to consider the cost and time needed to break the code. (Remember the old good DES algorithm? It was considered as secure for years until the computers improved to the extent that the costs of the code breaking decreased to a reasonable value.)

To illustrate AES safety this way, here is a citation from a security expert (2004):

“Correctly implemented AES-128 is likely to protect against a million dollar budget for 50+ years and against individual budgets for at least another 10 years.“

To conclude, computer security and user practices are much more important than crypto algorithm! By far the most critical thing is the quality of the password. (At least have 8 characters and use a mixture of uppercase and lowercase letters combined with special characters.)

3.2 Password strength

The key to the secure encryption scheme is a good password.

Here is how Wikipedia defines a weak password:

A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, and words based on the user name or common variations on these themes. Passwords that can be easily guessed by acquaintances of the user, such as a birth date and pet's name, are also considered weak.

Examples of weak passwords:

- Can be guessed: admin, 1234, aaaa, nbusr123
- Common names: susan
- Known from keyboards: asdf, qwerty
- *12/3/75* -- date, possibly of personal importance (birthday, anniversary)
- p@$$\/\/0rd - cracking tools are pre-programmed for such letter ciphers

Here is the definition of the strong password:

A strong password is sufficiently long, random, or otherwise producible only by the user who chose it, such that successfully guessing it will require more time than the password cracker is willing to use guessing it. The length of time deemed to be too long will vary with the attacker … and the value of the password to the attacker. A student's password might not be worth more than a few seconds of computer time, while a password controlling access to a large bank's electronic money transfer system might be worth many weeks of computer time.

Examples of strong passwords:

- *t3wahSetyeT4*
- *EPOcsoRYG5%4pp@.djr*

(Note: because these passwords have been published (in this document), they are not strong anymore.)

For those who wish to learn more: http://en.wikipedia.org/wiki/Password_strength

Password strength meter in IDGuard

Note the change password dialog contains a color bar under the Password field. Its color and length corresponds to the password quality: The longer the bar, the better the password.

3.3 Implementation

The "column data" is stored in a RAM database with individual records AES-encrypted. There is no other tool that could read this database.

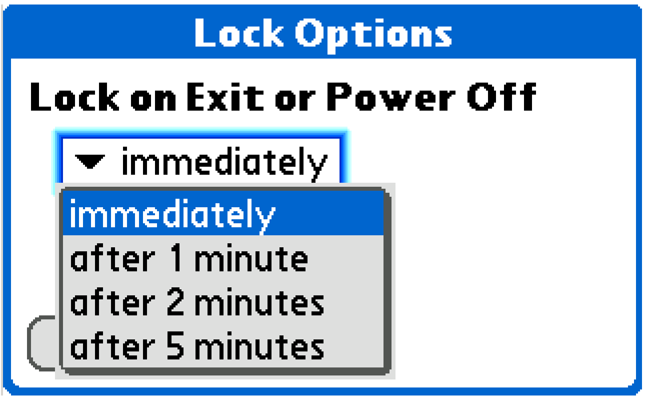
Attachments are stored on the card under the folder named /Palm/Launcher/IDGuard/__EXStore. The chosen implementation for attachments is a zip format **compatible with WinZip, 7Zip, PowerArchiver, Resco Explorer,** etc. This means that any of the above zippers can be used to open the attachments – with the correct password, of course. (Note that older ZIP-utilities mostly do not support AES encryption and thus will not be able to unzip IDGuard archives.)

Attachment processing (viewing, editing) also implies security risks, as the attachments must be temporarily decrypted. This topic is discussed in the chapter about attachments.

Backup sets include a copy of the encrypted password database as well as copy of all attachments. It means they are as safe as the original IDGuard data.

Note for the Resco Viewer users: Encryption used in IDGuard is safer, but slower.

3.4 Data locks



Lock Options

Lock on Exit or Power Off

▼ immediately

Figure 9 - Lock Options

To prevent the situation that you forget to close the data, IDGuard locks itself after the device powers off and specified period of inactivity elapses. To resume the work you need to repeat the login.

The reverse holds true as well: when you exit and then restart IDGuard within the specified auto-lock period, no login is needed.

The option “immediately” provides highest safety (every power off and every exit means new login), while the remaining options leave you more freedom.

You can use also the manual locking – the *Lock now* command accessible from the main menu.

4 Attachments

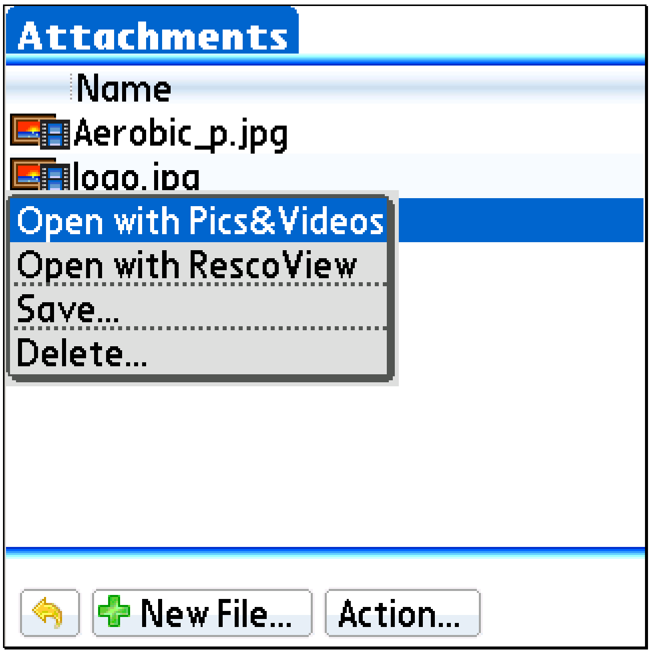


Figure 10 - Attachments

The work with attachments resembles an e-mail program: You can attach any number of files; the attachments can be saved, deleted, or viewed with appropriate application.

As was already demonstrated, IDGuard supports special attachment types – photos made with the built-in camera and sounds recorded with IDGuard.

Every attachment is stored in an AES-encrypted zip file.[1] It means the stored attachment is as safe as the rest of your data.

When you are attaching a file, you get a question "**Delete the original?**" If you answer *yes* (recommended answer because the original file is not encrypted), the file being attached will be deleted after successful import and you will have to use IDGuard to open it. If you answer *no* or if the import fails, the original file will remain intact.

You can any time restore original attached file by tapping the attachment and selecting the *Save* command. More advanced users can use a zipper and open the encrypted attachment residing in the folder /Palm/Launcher/IDGuard/__EXStore/.

There is an important moment you should know about:

- Documents To Go does not understand AES-encrypted doc file
- Pocket Tunes cannot play AES encrypted mp3
- Etc. No foreign application understands the encryption.

This means that these attachments must be temporarily decrypted before passing them to the respective application. We'll explain how it is done in the following chapter.

[1] Corollary: Unless an already compressed file is used (mp3, jpg), the stored attachment size will be substantially smaller than the original.

4.1 Launching an attachment

It looks simple: A jpg image gets opened in Resco Viewer, a doc gets opened by Word To Go, etc.

What is happening behind the scenes is that Resco Viewer tells Palm OS that it can process the images and Documents To Go tells the same about the doc files. This is called an association.

When you tap an attachment:

1. IDGuard will offer you all apps that can process that file.[2] (e.g. you can have two viewers.)
2. After you select the right application, IDGuard will decrypt the attachment and pass it to the application.
3. When the processing is done, IDGuard will check if the attachment was modified. If yes, the attachment will be encrypted and stored.
4. Finally the decrypted attachment gets deleted.

It’s quite complex, but that’s not the whole story. The next problem is how to tell the launched application that it has to open our attachment.

4.2 Safe vs. unsafe applications

Well, some apps understand such request. These apps work exactly as explained above, i.e. more or less **safely**.

- Documents To Go, MobiOffice
- Repligo
- PalmPDF
- Resco Viewer
- Blazer, NetFront, Eudora, Universe 3
- Kinoma
- TCPMP
- (Pocket Tunes, AeroPlayer and MMPlayer could be added to the list in case of user interest. However, IDGuard has its own mp3 player.)

The remaining applications can be used only with a trick:

The decrypted attachment is sent to the application similarly as if it was beamed. The application will accept the data (provided it supports the beam receive) and somehow process it. The user might have the impression that everything works, but the typical consequence is a decrypted attachment saved on an unknown place. That’s way these applications are considered as **unsafe**.

[2] Note that apps installed on the card should never be listed. If they are, then a) it is a bug of that application, b) you can expect a crash due to another Palm OS bug.

5 Documents

The attachments explained in the previous chapter provide a powerful tool, yet their use is a bit too tedious for the most typical cases. You need to create a general record and fill a few items and only then define an attachment. The “documents” were invented to simplify this procedure. Here are the two simple steps you need to do:

1. Select the menu option *New Document*. This will open a card browser.
2. Select a card file (a Word document, an image etc.) that should be stored in IDGuard.

That’s it. You have just created a new item that securely stores the selected document.

When you tap the item, it gets opened in the selected viewer, e.g.

- A Word document will be opened in the Word To Go (Mobi Office),
- An image will be shown in Resco Viewer
- etc.

Except the preview, the documents can be

- Sent: The decrypted document will be sent using selected channel (BT, e-mail etc.),
- Saved: Use to extract the decrypted document and store it to selected card folder.

The documents have a few specifics:

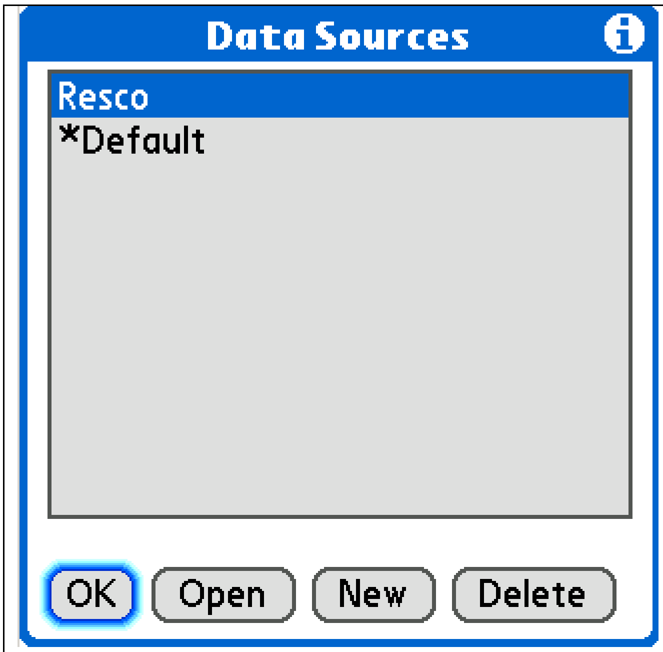
- They use predefined template called Document
- The share the name of the attached file (unless you redefine it)
- They use the icon of the associated handler, i.e. a .doc file will display Documents To Go icon etc.

Of course, the document record is like any other record, i.e. you can attach the notes or any other file or even define the textual information. However, the main purpose of the Document template is to facilitate the one-tap access to the stored documents.

As far the document viewing is concerned the restrictions described in the Attachments chapter apply, mainly the paragraph Safe vs. unsafe applications.

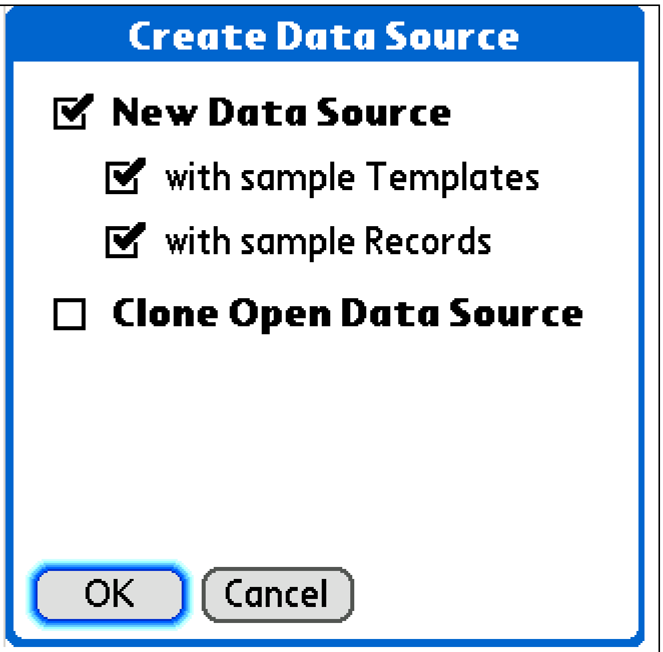
6 Other topics

6.1 Data Sources



Resco
*Default

Figure 11 - Data Source selection



☑ New Data Source

☑ with sample Templates

☑ with sample Records

□ Clone Open Data Source

Figure 12 - Data Source creation

You can work with several databases, each protected by its own password. The selection is done either in the initial login or from the Data Sources dialog.

Fig. 11 shows a situation with one private data source (Default) and one shared data source (Resco). Asterisk marks the data source that is opened at given instant.

The dialog offers basic tools for the maintenance of the data sources, namely the creation and deletion.

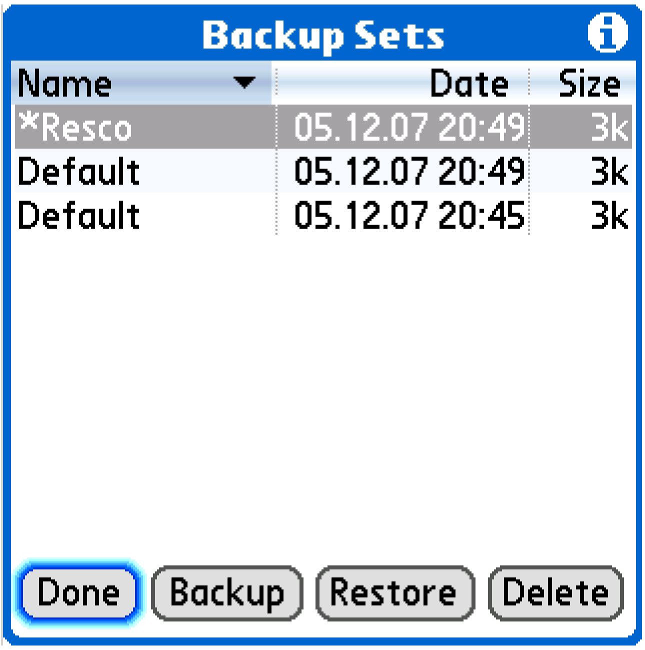
When you create a new data source, you have two options:

- To create a new data source (optionally populated with sample records), or
- To duplicate (clone) opened data source.

As far the data source sharing is concerned, there are two options:

- Export / Import
- Backup / Restore

6.2 Backup/Restore



Name	Date	Size
*Resco	05.12.07 20:49	3k
Default	05.12.07 20:49	3k
Default	05.12.07 20:45	3k

Figure 13 - Backup/Restore

The opened data source can be backed up. The result of this process is a backup set and it contains complete data source data – records, templates, attachments etc.

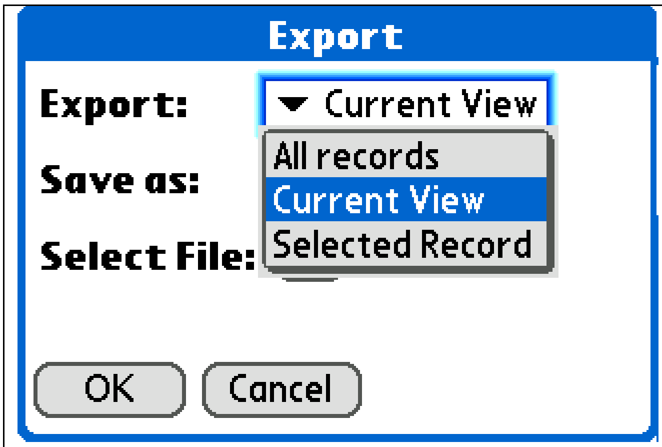
You can manipulate the backup sets similarly to a standard backup program:

- *Backup* button creates a new backup set (copy of the opened data source)
- *Delete* button removes selected backup set
- *Restore* restores the data source to the state stored in the selected backup set. It does not matter whether the restored data source exists or whether it is opened. If the data source doesn't exist anymore restore command creates it once again.

Backup sets are stored under /Palm/Launcher/IDGuard/Backups card folder. Each backup set contains a copy of the (encrypted) password database and copies of all attachments. (Encrypted as well.)

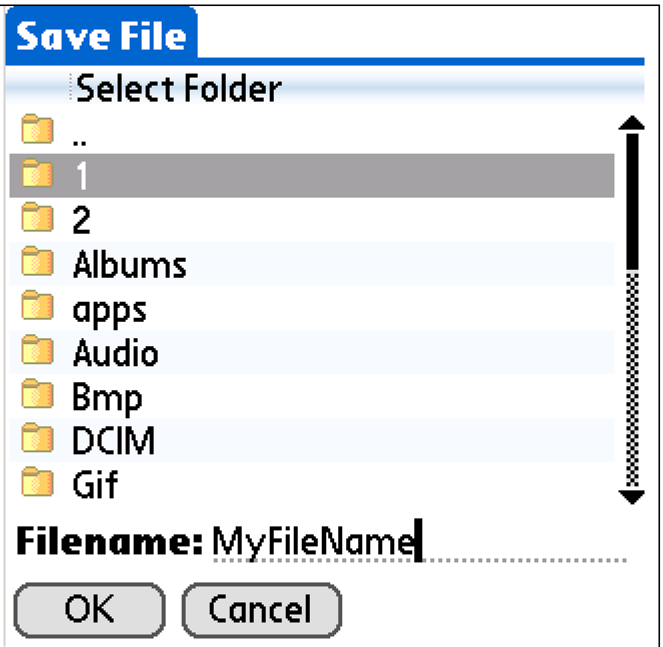
Backup sets present a convenient way for the data sharing.

6.3 Data Export



Export: Current View

Figure 14 - Data Export



Filename: MyFileName

Figure 15 - Save File dialog

Export dialog lets you save the data in a format that might be used for alternative purposes:

- HTML is suitable for presentation in a web browser. The attachments are displayed as file names only – the data is not included.
- CSV produces format suitable for spreadsheet processors. It has similar limitations as HTML.
- XML is a loss-less format. It contains categories, templates and textual data. You can optionally include also the attachments – the checkbox *Include Attachments* (displayed for XML output format only) serves for this purpose. You can display the XML output in any web browser.

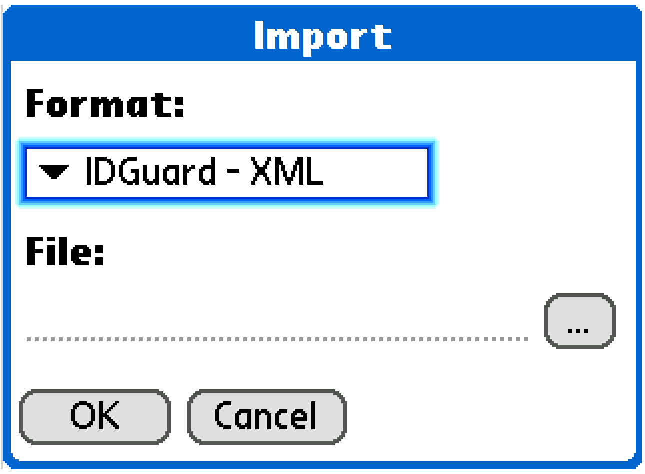
You can save all records or just part of the data. For example if you specify incremental filter a* (i.e. you type '*a*' into the search box), then export of the *Current View* will output all records with names starting with 'a'.

Finally you need to select the file where the output will be stored. By pressing the [**…**] button you get the Save File dialog, where you need to select the output folder and the file name. (Note that you don't need to enter html/xml/csv file suffix; IDGuard will do it for you.)

In all cases the output is **not encrypted**. (The future upgrades will come also with encrypted export.)

XML format has another advantage – the output can be used for the reverse operation, i.e. the Import. This makes it a tool for data sharing.

6.4 Data Import



Import

Format:

▾ IDGuard - XML

File:

Figure 16 - Data Import

While the Data Import logically looks like a reverse operation to Export, it is only partially true:

- IDGuard XML exports can be imported and the result is 1:1 replication of the original.
- IDGuard CSV export/import works similarly except the attachments are ignored. CSV format was added as a mean of data exchange with other password managers, hence attachments would cause more harm than use.
- HTML files cannot be imported.

On the other hand, Import can be used to take over data produced by other password managers – currently SplashID[3], Adarian and KeePass. Note that you need first to export unencrypted data from the foreign data manager. (Encrypted data cannot be imported, as the programs do not understand each other's protection schemes.)

What to do if you need to import another (unsupported) format? If you are not afraid of editing CSV files, you can modify the foreign file to the IDGuard CSV format (see the Appendix) and import it this way.

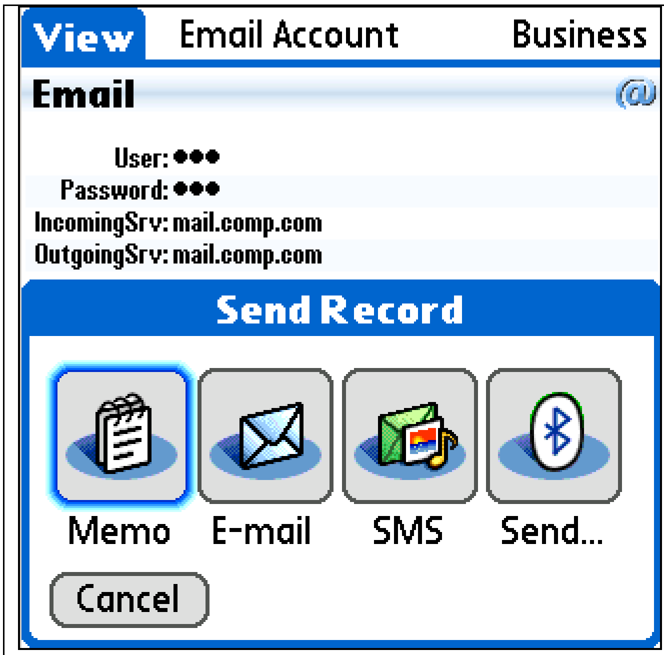
Imported data is merged with the opened data source. Of course, you can import into an empty database and escape potential conflicts this way.

The import procedure consists of two steps:

- Selection of the import format
- Selection of the file containing the data to be imported. Although you can type the file path manually, the button [**...**] provides the easiest way – the file browser.

[3] Two SplashID formats are supported: Either vID file created by SplashID desktop or the live SplashID database from your device. Support for CSV format was omitted as it provides the worst results.

6.5 Sending record



Email

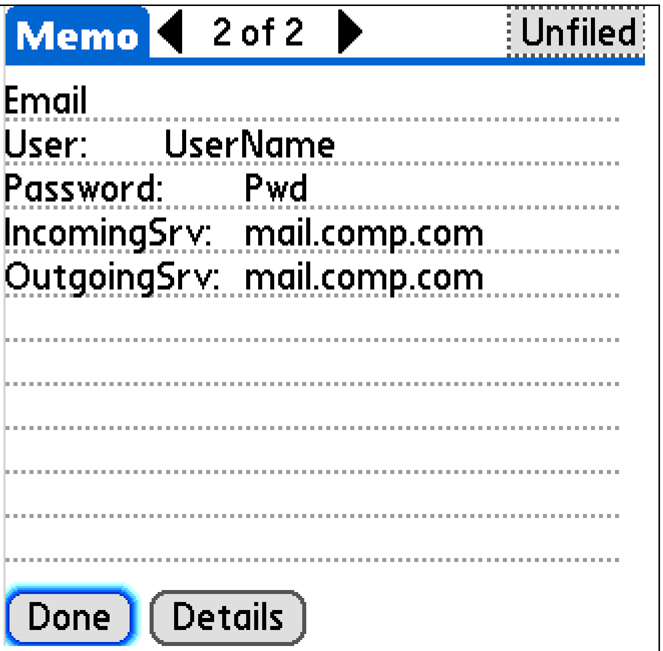
User: ●●●

Password: ●●●

IncomingSrv: mail.comp.com

OutgoingSrv: mail.comp.com

Figure 17 - Record sending



Email

User: UserName

Password: Pwd

IncomingSrv: mail.comp.com

OutgoingSrv: mail.comp.com

Figure 18 - Record sent as memo

If you want to share particular record, you can use also *Send Record* command. Above figures show an example – sending as memo. As you can see, the result is the record contents written as plain text; notes and attachments are ignored.

The other options provide similar functionality:

- *E-mail* will open the default OS Mail package (usually Versamail), fill the message body and lets you finish the e-mail.
- *SMS* will create an SMS message with similar contents as the above memo. You have to select the sender and eventually modify the message text.
- *Send* stands for all transfer means you have installed on your PDA. Typically it is Beam (sending using Infrared), Bluetooth, Versamail, Snappermail, Messaging etc. In all cases IDGuard creates a txt file (similar to the memo you see above) and passes it to the transfer medium you chose. It means for example:
    - Sending a txt file via Bluetooth. (The receiving device must be able to process txt files.)
    - Creating an e-mail with attached txt file.
    - Etc.

7 Appendix

7.1 IDGuard Messages

- **Delete Original?**

You get this question when creating a new document entry or adding an attachment. IDGuard imports the file into the secure storage and asks what to do with the original file. The recommended answer is *yes*, i.e. deleting the unprotected document instance. You can any time restore the original document using the *Save* command.

- **Could not recover launched file "...file name..."**
... error message ...
Delete?

Decrypted document passed to a document editor was modified, but the attempt to import the changes back to IDGuard failed.
You can either delete the file or do another corrective action outside of IDGuard.

- **Could not recover launched file "...file name..."**
File not found.

Just a warning: Decrypted document passed to a document editor was not found.
An example when this happens: The user renamed the document in the editor.

- **You have to log-in to recover the launched file.**
Delete instead?
A decrypted attachment needs to be re-imported into the IDGuard storage. If you cancel the login, the file will remain unsecured. IDGuard offers you an automatic deletion of the file.

- **Backup set name in use.**
Please wait 1 minute and retry.

Backup set name is created from the data source name and the current time expressed in minutes. You cannot make two backup sets within a minute, as they would share the same name.

- **Launched from card!**
Reminders and delayed locking will not work!

Due to the Palm OS limitations the applications installed onto the card do not receive system messages, for example such apps are not awaken when specified time elapses.

- **Can't duplicate a document**
The document nodes cannot be duplicated. This is just an artificial limitation introduced to reduce the confusion.

- **Delete Attachment … name …**
Warning: The delete is irreversible.
When you edit a record, you still can cancel the changes by pressing the *Back* icon. However, changes on the attachment level cannot be reverted.

7.2 IDGuard CSV export format

As the users demanded import of various csv formats and because every program uses its own scheme, we decided to publish our format. In many cases it is relatively easy to modify csv export from another password manager to fit to the IDGuard scheme.

Find below an informal format description. It is best understood when compared to a real exported file.

First line must be:
Resco IDGuard export v2.0

Template lines are optional and have the format
T,label,fieldName1,,,,,,,,,,,,,,,label,fieldName16, fieldMask, iconID

fieldName == charData[|dataType]
dataType == Optional: { 0-Text, 1-Number, 2-Date, 3-Email, 4-Address, 5-Phone }
filedMask == bitmask of maskable fields (0 = nothing masked)
iconID == 3001, 3002… 3025 (icons from Select Icon dialog)

Data rows have the format:
F,label,field1,,,,,,,,,,,,,,,field16, note, category

Fields, note and category can be empty.
The record is assigned to the last successfully imported template or is added to Unfiled if there was no template defined yet.
The note can span multiple lines; any internal comma characters must be escaped.

Examples

Example with templates and categories	Resco IDGuard export v2.0 T,Calling Card,Access#|0,PIN|0,,,,,,,,,,,,,,,2,3009 F,PhoneCard,1-800-562-3621,123456,,,,,,,,,,,,,,,,Unfiled T,Credit Card,Card #|0,CV2|0,Valid Thru|0,Name|0,PIN|0,Bank|0,,,,,,,,,,,49,3003 F,Visa Card,3333 1111 2222 4444,,10/09,MyName,1111,CSOB,,,,,,,,,,,Unfiled T,Email Account,User|0,Password|0,IncomingSrv|0,OutgoingSrv|0,,,,,,,,,,,,,3,3018 F,Email,UserName,Pwd,mail.comp.com,mail.comp.com,,,,,,,,,,,,,Unfiled T,Frequent Flyer,Number|0,Name|0,Date|0,,,,,,,,,,,,,,1,3010 F,Air France,123456,MyName,"Sep-11,2007",,,,,,,,,,,,,,Unfiled
The same data without templates and categories	Resco IDGuard export v2.0 F,PhoneCard,1-800-562-3621,123456,,,,,,,,,,,,,,,, F,Visa Card,3333 1111 2222 4444,,10/09,NameOnCard,1111,CSOB,,,,,,,,,,,, F,Email,UserName,Pwd,mail.comp.com,mail.comp.com,,,,,,,,,,,,,, F,Air France,123456,MyName,"Sep-11,2007",,,,,,,,,,,,,,,