IDGuard for Windows PC v 2.01
User manual

1 About IDGuard 2

1.1 Requirements, (un)installation 3

1.2 Registration 3

1.3 Using IDGuard on Palm OS® 4

2 First contact 5

3 Basic concepts 6

4 Useful tips 7

5 Attachments and Documents 10

6 Export/Import 11

7 Security 12

7.1 AES and security 12

7.2 Password strength 12

7.3 Implementation 13

8 Appendix 14

8.1 IDGuard CSV export format 14

8.2 How the synchronization works 15

1 About IDGuard

Resco 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 click 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 from prying eyes. What is even more important – IDGuard provides complete workbench incl. document opening, editing and saving.

Other advanced features

- Multiple data sources
- Import from / Export to several password managers
- Built-in attachment viewer
- 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 - if you loose it - there is no way to recover the stored data; even the Resco support team cannot help in such a case.

Cooperation with PDA

IDGuard can share its data with the Palm OS handhelds. You need to have Resco IDGuard for Palm OS on your handheld. More handheld platforms will be added in the future.

1.1 Requirements, (un)installation

System requirements

Windows 2000/ XP / Vista.

Installation using exe installer

Run the Installer and follow the instructions. The installer lets you install IDGuard desktop, user manual and the handheld components.

Installation using zip installer

- Select the folder where IDGuard should be installed. (This is not possible for the exe installer.)
- Unpack the zip contents into this folder and run IDGuardDesktop.exe.

Uninstallation

In case you used the exe installer, you can use Windows *Start Menu* > *Programs* > *Resco IDGuard* > *Uninstall*.
If you used zip installer, then simply delete the IDGuard folder.
IDGuard data (Data Sources) must be uninstalled manually. The easiest way is to delete them from the IDGuard menu.

1.2 Registration

IDGuard handheld versions come with a free 14-day trial; the desktop trial has no limitation.

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 purchasing the unlock key or by installing a trial of a higher version.

IDGuard can be purchased at the Resco web site or at several major resellers of the PDA software.

After the purchase, you will receive an unlock key which will allow unlimited use of the purchased version of the product.

No matter where you purchase the software, the license is valid for the Palm OS version, desktop PC version and for other platforms Resco may support in the future.

Normally you purchase IDGuard for your handheld device:

- Use the UserID of this device (HotsyncID, PPC owner name) for the purchase.
- Use the same UserID to register the IDGuard Desktop.

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. (A *major upgrade* means a change of the major version number. e.g., 1.10 -> 1.20 is a minor upgrade, while 1.20 -> 2.10 is a major upgrade.)

1.3 Using IDGuard on Palm OS®

Installation on the Palm OS® handheld

Resco IDGuard for Palm OS can be installed both from the exe- and zip-installers. You can even download the Palm OS application from the Resco web site.
To install IDGuard.prc onto your Palm OS device:

1. Double-click the prc file,
2. Hotsync.

Installation to a memory card

While it is possible, the card installation brings severe disadvantages:

Reminders and Hotsync won’t work and several other features (auto-lock, attachment launching) will be severely limited.

Upgrading from IDGuard for Palm OS v1

You need to upgrade the Data Source format; otherwise the synchronization will not work. IDGuard v2 will suggest that when opening the Data Source.

Uninstallation from Palm OS handheld

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

Synchronization between the Desktop and Palm OS

You need to install IDGuard conduit – a Hotsync plugin that takes care of the data synchronization. To do so, run IDGuard Desktop and open *Hotsync Setup* dialog (main menu). This tool allows you to set up all synchronization details, too.

Hotsync tips

- Hotsync will fail if the Data Source is being edited and contains unsaved changes.
- However, it is allowed to “view” the Data Source during a Hotsync. Any changes eventually coming from the device will be immediately shown.
- Check the contents of the Hotsync log (right click the Hotsync icon) to see the info about the IDGuard conduit activity.
- If you want to copy the Data Source (for example from PDA to PC), then open the *Hotsync Setup* dialog and select appropriate Hotsync action. (e.g. *Handheld overwrites Desktop*)
- If the IDGuard conduit is enabled, Hotsync itself does not back up the PDA Data Sources.
- If the conduit is disabled, the PDA Data Sources are backed up to the Palm Desktop backup folder the same way as the other RAM databases.
- Once the IDGuard conduit is installed, you can set it up also from the Hotsync manager: Right-click the Hotsync icon in the system tray, select *Custom…* etc.

2 First contact

When you launch IDGuard for the first time, you will be asked to setup the data storage – the Data Source.[1] IDGuard offers also the creation of the default templates and sample records. It is a good idea to select these options as they provide a convenient starting point.

We recommend that you setup also a password[2] and that the password is good enough so that it cannot be easily guessed.

Users who already use IDGuard on their handhelds may proceed differently and instead of creating a Data Source they can import it from the device. (See the chapter on synchronization.)

IDGuard window consists of three panes:

- **Record Tree** displays the record structure. Logically there are 3 levels: Categories, Templates and Records. However, you can use more complex category structure thus adding more levels to the tree.
- **Record List** shows the records belonging to the selected tree node.
- **Record View** displays the record content. Double-click onto this area to edit the record.

Start by adjusting the working environment to your needs – setup the window size and the proportions between the panes (do you see the movable splitters?), select the font etc.

A bit browsing through the tree and various menu options will reveal more than any help text. Most of the control elements are self-explaining and if you are not sure about the meaning of particular button, read the tooltip.

Double click some on record and do some editing. Test how the save/undo features work. Note that IDGuard offers two flavors of each – record-level save and global save (Data Source save; upper save button). As long you do not save the Data Source, the changes can be undone.

Now it is the right time to start entering your data. Just press the New Record button …

Later on we'll cover other topics including the synchronization with mobile devices.

[1] If you skip this step in the Welcome dialog, you can do so later – use the *Create Data Source* menu option.

[2] IDGuard can work without a password, too. In fact, it supplies then the default password "Resco".

3 Basic concepts

Data Source

Data Source denotes the database that stores your data. It is a single file[3] with protected content that is usually located on a standard place[4] so that it can be easily found during the synchronization.

You may create other data sources later when - for example - there will be a need to share part of the data with other persons.

Categories

Perhaps everybody will intuitively understand the meaning of the predefined categories:

- Business
- Personal
- Unfiled

The first two present broadly defined groups and you will mostly have no problem to assign your records to either of them. Nevertheless, you can define your own categories (Main menu > Categories) and even sub-categories. So for example you could create this category tree:

- Business
    - Clients
    - Company
- Private
- Unfiled

Unfiled category integrates records that – for some reason – have no assigned category[5].

Templates

Templates stand for the record types (credit card, web login...), i.e. they define the record structure – fields, labels and the mask attribute.[6] Each template has a name and an icon.

There is again the Unfiled template that is assigned to all records without a valid template.

Note the special **Free Text** template that does not use columns. It is here to store plain text.

Data Records

The records represent actual data items you are going to store – credit card description, data describing access to specific web site, etc. IDGuard records consist of:

- Record name
- Icon (default icon is inherited from the template, but this can be overridden)
- Template – defines the record fields
- Category (Private, Business etc.)
- Notes (any text)
- Attachments (Images, documents etc.)
- Reminder (Text the Windows displays at specified time instant)

[3] At least as long we talk about the „column“ data. The attachments are stored in separate files.
[4] Under the Windows *Documents And Settings* directory
[5] For example the record category could have been deleted.
[6] Maskable fields are dotted in the masked mode.

4 Useful tips

IDGuard look&feel

You can resize the application window, move the splitters between the panes, setup columns etc. All these changes are remembered and re-applied next time you'll start the IDGuard.

Getting help

Most buttons have tooltips.
Status bar shows prompts for the selected menu items.
F1 opens the online help.

IDGuard Locking

To prevent the situation that you forget to close the data, IDGuard locks itself after specified period of inactivity elapses. (*Options* dialog) To resume the work you need to repeat the login.

You can also use the manual locking – the *Lock Now* command accessible from the main menu. The same effect has the ESC key or the Lock icon.

Wrong password

After you enter a wrong password for the third time, IDGuard exits. This measure is here only to make the password guessing slower – you can restart IDGuard and continue.

Incremental Search

Text typed into the search box (top right corner) serves as a record filter. (Input focus must be either on the search box or on the record list.)

Sorting

(Details view only) You can sort the records by clicking on the respective column header.

Masking sensitive contents

Masking means replacing the field contents by a ••• symbol. To mask a field:

1. Edit the template and select the field as masked.
2. Press the mask button

Using Drag & Drop

- You can drag selected record and drop it onto the tree. This is a convenient way of assigning record categories or templates.
- Opening Data Source: You can drag a Data Source file and drop it onto the IDGuard.
- Creating a document record: Drag any file and drop it onto the record list.
- Adding an attachment: Drag any file and drop it onto the record view.

Global Undo

Any edit changes (even adding/deleting of the attachments) can be undone by pressing the ↶ button in the upper toolbar.[7]

[7] Note that for example Palm OS IDGuard cannot revert attachment deletion.

Using ESC key

ESC is interpreted as kind of negative action (undo, cancel, lock etc.) at several occasions. A few experiments will reveal if this property makes sense to you – most users like it.

Double Click

- To modify a field double-click it in the record view. (Bottom pane) Can be also used for the notes.
- You can double-click also the record in the record list – effect is the same.
- However, if you double-click a document record, it gets opened in the associated application.

Using the Clipboard

Record list – Details view: Right-click the column > Popup menu > Copy to Clipboard

The same procedure can be used in the record view

Text pasted to the clipboard is cleared when the Data Source is closed or locked.

Reminders

A reminder is a kind of alarm consisting of an exact time instant and suitable text. The purpose is to remind the user that something needs to be done – for example a web login has expired. To set up a reminder select suitable record and press the ⏰ icon.

Notes:

- For reminders to work the Task Scheduler service must be running on your system. (For W2000 use Control Panel > Administrative Tools > Services.)
- Reminders ere entries in the system Task Scheduler. (Accessible from the Control Panel.)

Web links

By clicking a web link, the link will be opened in the web browser. E-mail addresses work similarly.

Password editor

If the field label starts with “passw” and if you click this label in the record view, you get the password editor.

Change indicator

The rightmost pane of the status bar serves as the change indicator.

🔄 icon (Sync conflicts)

IDGuard shows this icon if the synchronization ended with conflicts, i.e. both sides modified the data in such a way that it is impossible to automatically select the correct possibility. You need to press the icon and “finalize the synchronization” manually. Until this is done, any further synchronization (of this Data Source) is refused.

This manual sync should be done on the desktop; the next synchronization will apply the changes to the handheld.

Sync Against…

This menu command can be used to synchronize two desktop Data Sources. The rules are more or less the same as when you synchronize against a device.

⚠ icon (open attachments)

This icon appears when there are attachments that need to be closed. (See the chapter on attachments.) Click the icon and decide what to do.

(x) Data Sources shared by all users

This is one of the key decisions you have to take in the Options dialog. Technically this option decides whether the data is stored in the “current user” folder or under “all users”.

If several users will access the Data Source, you should use the second option. Otherwise it in fact does not matter – just do not modify this setting or you will see different Data Sources.

Printing the record(s)

Use the preview commands – they contain the Print command in the menu.

Data Source cloning

represents a way how to create and exact copy of the opened Data Source.

5 Attachments and Documents

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.

To add an attachment: Either press the 📎 icon or drag the file onto the record area.

To restore original attached file: Right-click the attachment and select *Save As*.[8]

Every attachment is encrypted and is as safe as the rest of your data. There is an important moment you should know about:

- Microsoft Word does not understand encrypted doc file
- Media player cannot play encrypted mp3
- Etc. No foreign application understands the encryption.

This means that the attachments must be temporarily decrypted before “viewing” them.

“Native” attachments

IDGuard understands some commonly used formats:

- jpg, bmp, tif and png images (internal viewer)
- pdf, xml and html files (Internet Explorer ActiveX control)
- txt files (internal editor)

These attachments can be opened directly in the IDGuard and present no security risks.

“Foreign” attachments

The rest must undergo a complex process that is similar to opening a zipped file from a file manager. When you double-click an attachment, IDGuard will:

1. Decrypt the attachment to a temporary location.
2. Open the decrypted file in the associated application.[9]
3. Those, who expect that IDGuard will trace what happens next, will be disappointed. This is basically impossible. Instead, IDGuard issues kind of a warning by showing the 📎⚠ icon. Tap it and you’ll get a list of opened attachments with further options. (Discard the file or re-import the changes.)

Documents

The “documents” were invented to simplify the attachment processing.

To create a document - simply drag a file onto the record list. Or use menu -> *New Document* and browse for the file. In both cases you get the same result - a new record that inherited the name and the icon of the original file. When you tap the record, it gets opened.

Technically speaking the documents:

- Use predefined template called Document
- Share the name of the attached file (unless you redefine it)
- Use the icon of the associated viewer/editor.

Of course, the document record is like any other record, i.e. you can attach notes, reminders etc. However, the main purpose is to simplify the access to the stored files.

[8] More advanced users can use a zipper and open the encrypted attachment directly from the IDGuard storage.

[9] Of course, you can right-click the attachment and select the application yourself.

6 Export/Import

Data Export

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 format is 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* 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'. (You may want to select "All" category for this action.)

Finally you need to select the file where the output will be stored. (Press the [**…**] button.)

In all cases the output is **not encrypted**

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.

Data Import

While the Data Import 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.
- CSV format ignores attachments. CSV serves 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[10], Adarian and KeePass. Note that you first need 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.

[10] Only vID format is supported.

7 Security

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.

7.1 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

7.2 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.

7.3 Implementation

The Data Source is kind of a database with individual records AES-encrypted. There is no other tool that could read this database.

Attachments are stored in separate disk files (1 attachment = 1 file), every one AES-encrypted. The chosen implementation for attachments is a zip format **compatible with WinZip, 7Zip, PowerArchiver,** 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.

Attachments are stored on the fixed location under your Documents and Settings folder structure. The full path looks like

c:\Documents and Settings\<user>\Application Data\IDGuard

Note, however, that the folder *Application Data* is hidden; hence you might have problems in looking for it.

8 Appendix

8.1 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",,,,,,,,,,,,,,,

8.2 How the synchronization works

In the following we shall refer to the typical scenario – synchronization between the PC and handheld Data Source. However, most considerations are valid also for the remaining cases, for example for the synchronization between two Data Sources on the same PC.

Data Source pairing

This refers to the question, which databases should be synchronized. The most obvious answer – those having the same name – is basically wrong. Or at least dangerous as it allows data exchange between possibly unrelated objects that just happen to have the same name. (How many users will keep the default Data Source name?)

The correct answer is that the databases must establish a contact – they must be paired. The pairing is realized by exchanging a unique token that cannot be generated under different circumstances. Both databases store this token and verify it before any synchronization trial.

At present IDGuard allows two ways of Data Source pairing:

- Cloning a database. (I.e. cloned databases can be synchronized.)
- One-way synchronization (see below)

Other Data Sources cannot be synchronized, even if they had the same name.

Synchronization types

On the most general level there are four synchronization types:

- True synchronization, i.e. replicating the changes made on one end to the other end
- Handheld overwrites desktop
- Desktop overwrites handheld
- Do nothing

The last three types are obvious and – strictly speaking – they do not represent the synchronization. However, there are good reasons to list them:

- They are commonly used by the synchronization managers (such as Palm OS Hotsync)
- One-way copy is a convenient way of establishing the Data Source pairing. (I.e. such Data Sources can be synchronized in the future.)
- It is a useful option. Sometimes you know that the differences between both sides are too complex and a one-way copy is simply the best solution.

Since now we shall talk about the first sync type only – the true synchronization.

Sync session

Once the two databases were synchronized, they maintain a sync session consisting of:

- Unique database ID (result of pairing)
- Anchor, which is basically the (GMT) time of the last synchronization.

The synchronization will be refused if any of these values differ.

Well, the time comparison presents actually a problem as any machine might have wrong system time. IDGuard tolerates differences up to a few minutes to account for this possibility.

The reason behind the time comparison will become clear later. For the time being note that it is not allowed to synchronize a live Data Source against a Data Source restored from backup. The reason - the time comparison will fail. (Provided there was a sync since the backup was created.)

Sync algorithm

The data at the disposal:

- The time of the last synchronization (T0)
- Each record has a unique ID (records are compared by this ID) and stores the time of the last modification.

Let's consider the synchronization between the Data Sources DS_A and DS_B. IDGuard goes record by record. So for example this consideration is done for every record from DS_A:

If the record (i.e. its ID) is not found on the other side (DS_B):

- If it is older than T0, then it must have been deleted from DS_B.[11] Such record will be deleted from DS_A, too.
- Otherwise we have a conflict[12] and nothing is done. (For this record, of course. The synchronization goes on with other records.)

If the record exists on both sides, then IDGuard decides based on the record modification date: The newer record gets copied to the opposite side. (The latest wins.)

Note that the real algorithm is much more complex as it applies additional rules for templates and categories.[13] However, the above text explains the main idea and the concept of a conflict in particular.

Conflicts

As explained above, synchronization might fail due to unresolved conflicts. In such cases IDGuard displays the icon in the upper toolbar to remind the user that his intervention is needed. The user has to click on the icon and take needed decisions, i.e. to select which of the two Data Sources contains correct data in all cases that could not be resolved automatically.

As long as unresolved conflicts exist, no further synchronization is possible.

Attachments

Attachments represent a problem in itself. They are stored outside of the password database. Even larger problem present mobile devices that usually store the attachments on the (removable) expansion card. What should for example happen when the user swaps the expansion card before the synchronization?

IDGuard implements only additive attachment synchronization. It first determines if the device uses the correct card. If yes, the attachments are synchronized except one thing – they are never deleted. The user must perform the delete manually – on both sides, of course.

[11] Remember that the situation at the instant T0 was identical; hence the record existed at both sides then!

[12] The record was modified at DS_A and deleted from DS_B. Because Data Sources do not store deleted records (imagine the problems when synchronizing into a triangle), we do not know in which order the actions happened.

[13] For example categories are compared by name and are never deleted.