ClassifyIT v.6.0

USER MANUAL

ClassifyIt, an Add-In for Outlook, Word, PowerPoint and Excel

support@ugarbe.de

2022

Table of Contents

Article I. Introduction 3
Section 1.01 Why to use ClassifyIt 3
Section 1.02 ClassifyIt Key Capabilities 4
Section 1.03 What is a Classification Marking 5
(a) Visual and Technical Classification Marking 6
(b) Translated Classification Markings 6
Section 1.04 How ClassifyIt integrates in Office Applications 7
Article II. ClassifyIt Functions 8
Section 2.01 ClassifyIt Menu 8
Section 2.02 Release Form 9
Section 2.03 CryptIt 10
(a) Use Cases – Encryption of Attachments 12
(b) Use Case – Company Wide Need-to-Know 12
(c) Use Case – Individual Need-to-Know 13
Section 2.04 Properties 15
Section 2.05 PDF Export 16
Article III. Public-Private Key Concept – how to use certificates 17
Article IV. Outlook Behaviour 19
Section 4.01 Email Without a Classification 19
Section 4.02 Email With Unapproved Attachment Type 19
Section 4.03 Reply or Forward with Lower Classification 19

Article I. Introduction

Section 1.01 Why to use ClassifyIt

ClassifyIt is an information security support tool which enables applying policy compliant classification markings to emails and documents, add data leak prevention information, and to encrypt documents when distributing them over unprotected networks (like the Internet). ClassifyIt is designed to be powerful on its core functions and easy and intuitive for the users and administrators.

Information security starts when writing or updating documents. Mark the document with a visible classification marking, like SECRET, to ensure you and others know about the sensitivity of the information within the document. ClassifyIt ( ) enforces and helps selecting the correct classification marking.

Adding such a classification marking manually is absolutely possible without a tool – so the obvious and legitimate question is why to use ClassifyIt? The answer is in the kind of business and size of your organisation. Very small companies might not require such a tool, although marking personnel data might be a legal requirement and a tool could help in marking such data properly, like the GDRP requirement. Competitive, innovative and growing companies owns and manages information which makes them unique and this critical information must not become public or available to their competitors. ClassifyIt helps and enforces a visual human readable marking as shown above and adds a technical marking supporting DLP technologies.

The ISO 27001 standard requires the implementation of Information Classifications. ClassifyIt is an absolute flexible tool to support this requirement. Around the tool which enforces classification markings (ClassifyIt), policy and handling procedures are necessary to have a common ruleset for your users.

Section 1.02 ClassifyIt Key Capabilities

ClassifyIt is a **Plug-In** for Microsoft Outlook, Word, PowerPoint and Excel applications, of the Microsoft Office Suite (2010 and higher).

ClassifyIt supports **Data Loss Prevention** (DLP) by enforcing or supporting the insertion of security classification markings. DLP is supported by readable security **markings** and non-readable information to emails (X-Header) and documents (properties). Both can support network security DLP measures through mailguards, web firewalls or other proxy mechanisms.

ClassifyIt supports the **enforcement** of **classification** markings on emails, word, slides and excel documents. The markings are configured to be compliant with the company's or organisation's security policy and can be made interoperable with other companies markings.

ClassifyIt supports the **coherence of email classifications** to prevent that the email could have a lower classification than its attachments.

ClassifyIt supports the selection of **release** markings to ensure company's and organisation's security policy compliant markings. Release can support internal as well as external authorisation to provide sensitive data.

ClassifyIt supports adding **meta-data** to documents to greatly improve search engines results. Document availability will be highly improved with this feature.

ClassifyIt supports the export of the Office documents to PDF formatted documents by enforcing and keeping the readable and non-readable classification marking information.

ClassifyIt supports **classification as a service** through central web control of configuration parameters.

ClassifyIt supports the **encryption** of email attachments, through built-in keys, user-passphrases or public/private keys.

Section 1.03 What is a Classification Marking

A Classification Marking is a textual label which defines at high level the sensitivity of a document (its information) and how this document could be shared internal or external to your organisation. In the context of ClassifyIt, the sensitivity is called the ***classification*** and a sharing statement the ***release***.

Below an example of a Classification Marking, where the classification is SECRET, and the release is MANAGEMENT and FINANCE. The classification marking is the label showing the classification and release, in this case:

Classification: SECRET
REL TO: MANAGEMENT\ \FINANCE

The label for such a classification marking must be conformant to your organisations information management policy which sets the classifications and their meaning as well as if your organisation requires release markings. The classification mainly represents the value of the information within a document and the release (if used) indicates approval to further distribute the document.

A classification marking contains a classification and optional a release marking. Your security administration or information management define those markings. For the classifications there are normally between three to fife categories, alike those shown on above diagram: OPEN, RESTRICTED or SECRET.

OPEN would apply to information which can be shared with everyone, so think about publishing of such information in the internet would not reveal internal secrets of your organisation.

RESTRICTED would apply to information which is of official context within your own organisation and with external cooperation partners. This category of classification could apply to information which would reveal a certain, but limited, advantage to competitors if those would be aware of the information. So, such information needs to be protected with some care. This might be internal processes, certain price information or high-level technical information.

SECRET would apply to sensitive information which is very important to your organisation and which must be handled with highest care. This category of classification could apply to information which would bring advantage to competitors if those would be aware of the information. So, such information needs to be protected with highest care. This might be detailed technical information.

(a) Visual and Technical Classification Marking

ClassifyIt is a data leakage protection tool (DLP) which adds and enforces visual classification markings which are shown as text within the document – ClassifyIt also adds technical classification markings which are stored in properties of the document. ClassifyIt ensures that the visual and technical markings are of the same value. Technical markings can be used by software to exactly identify the classification of the document and enforce if the document can be provided to a recipient or not.

The section above showed a SECRET classification marking with a release. The technical marking is represented in a JSON notation and might look like:

{“type”: “Normal”,
“x-class”: “S”,
“x-rel”: [“MAN”, “FIN”],
“app”: “email”}

The values for x-class and x-rel are configurable by the administrator. In this notation S represents SECRET, MAN represents MANAGEMENT and FIN represents FINANCE.

(b) Translated Classification Markings

For the visual Classification Marking, ClassifyIt allows to represent the marking with a translation. This translation could be an additional visual line which would standardise the classification marking. Such standardisation might be useful in international cooperations where the normal classification markings are not equal.

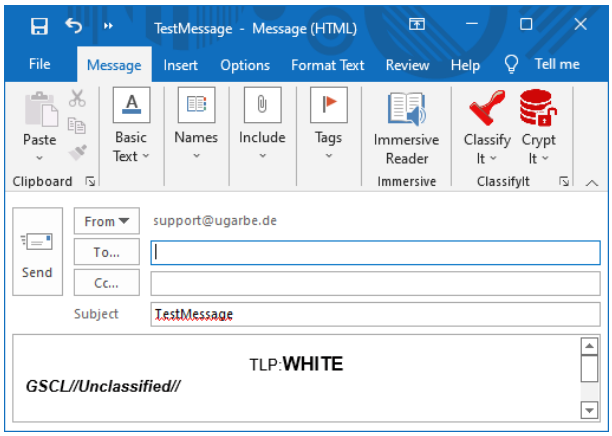
For more information consult the case study on Interoperability of Classification Markings, available on https://ugarbe.de

This document also uses the feature of a translated classification marking, following the notation of the Global Standardised Classification Label (GSCL).

TLP:WHITE
GSCL//Unclassified//

Section 1.04 How ClassifyIt integrates in Office Applications

ClassifyIt integrates in the Microsoft Office applications of Outlook, Word, PowerPoint and Excel. If further applications are required, please contact the administrator to request this to support@ugarbe.de

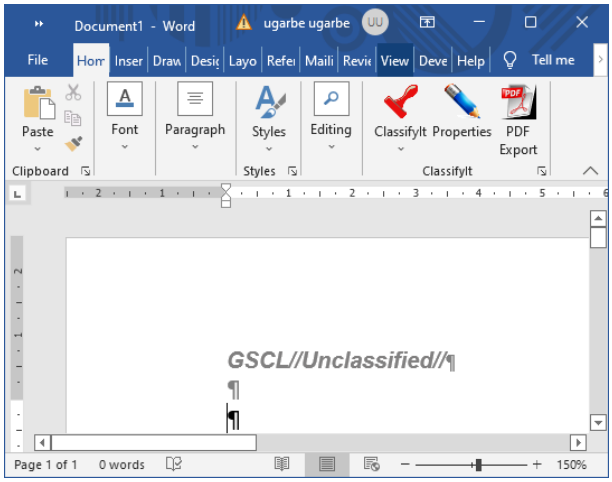


In all applications the ClassifyIt component is available to select and apply proper classification markings to the document. The ClassifyIt symbol is the red stamp.

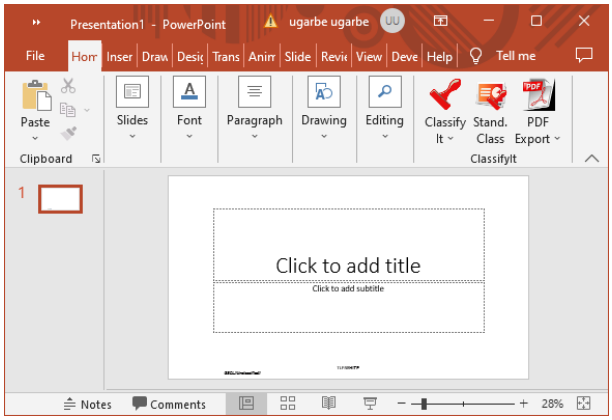
Pending the application one or two additional functions are integrated.

In Outlook the CryptIt component is available to support the encryption of email attachments. CryptIt is represented by the red database and lock symbol.

In Word and Excel two additional features are available to set and edit properties (meta-data) of the document and a PDF Export function. The PDF Export ensures that also the generated pdf file has the technical markings (properties) set.



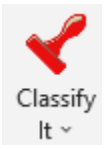
In PowerPoint also the PDF Export is available. In addition a standard classification can be selected, which will be applied to each new slide.



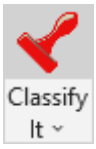
Article II. ClassifyIt Functions

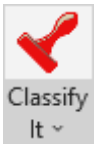
Section 2.01 ClassifyIt Menu

The ClassifyIt menu is available in all of the following applications: Outlook, Word, Excel and Powerpoint. In Outlook it is visible when opening an email.

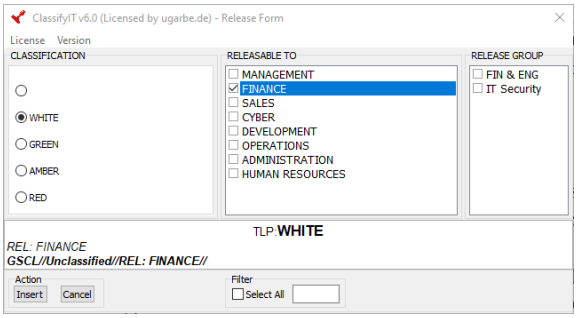


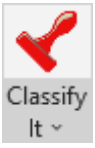
The ClassifyIt menu is a split button providing two functions. One at the upper half and one on the lower half of the button.



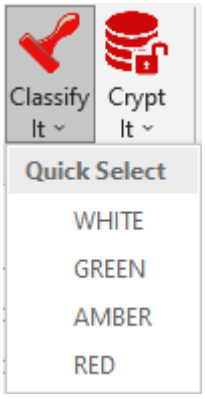


The upper half of the split button opens the full ClassifyIt menu, the Release Form. In this menu the full variety of classifications and release markings can be selected. It provides a preview of the selected classification marking and supports filtering and selection of release markings (see Section 2.02).

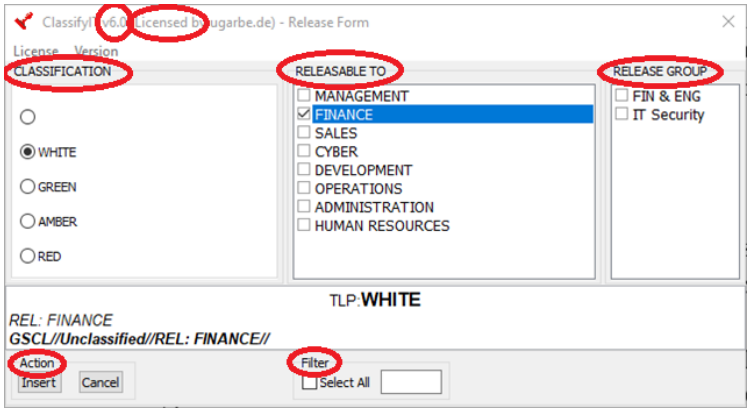




The lower half of the split button opens the integrated Quick Select menu. This menu provides a list of classification markings which are often used within the organisation. The number of entries is limited to 10 and is configurable by the administrator – if more entries are required contact support@ugarbe.de. The Quick Select menu shows a display name of a particular classification marking and can include classification and release. In essence it provides a shortcut to often used classification markings. (Example: W REL FIN, could be the display name for: WHITE REL: FINANCE).



Section 2.02 Release Form



The Release Form is the main ClassifyIt menu allowing the selection of a classification marking, which can be applied to the document. It provides some basic information, selection and action options.

At the top window frame the version of ClassifyIt is shown, as well as if the product is licensed and by whom. When support is required this information should be provided.

Below are the main selection options for selecting a Classification, Release and Release Group. Exactly **one classification** is to be selected – for a new document a default classification is set automatically, for an existing document the last classification is selected (this only applies to documents classified with ClassifyIt or interoperable other tools).

Any combination of **release** statements can be selected in the Releasable To selection menu. Using the Filter options below allows a selection/deselection of all release statements, and supports finding release statements (this is useful if there are many statements which don't fit in the window and are only selectable through a scrollbar).

The Release Group provides the option to add release statements to those already selected – this feature supports ease and consistency of more complex release statements – for example if documents are often/regularly released to a group of multiple partners a release group could be useful to support adding the x number of correct release statements.

The current classification marking with its formatting is shown on the lower part of the form. This is exactly how the marking will appear on the document when the Action insert is selected. With cancel the form can be exited without applying a new classification marking.

Section 2.03 CryptIt

CryptIt is the encryption menu for email attachments. It is integrated with ClassifyIt, however might be disabled by the administrator. It is only available in Outlook and allows the management of encryption options and the encryption and decryption of email attachments. Future versions might increase the CryptIt functionality and its availability to other applications.

In the Outlook Explorer (main window of Outlook) the CryptIt split button provides some certificate management functions of the user certificate and of imported public keys of other users.

Show My Certificate allows the user to see the name of his/her certificate.

Test My Certificate asks the user to enter the password of the certificate. If the password is not known, the certificate is useless and needs to be renewed. In this case other users need to be informed and the new public key of the certificate needs to be provided to them.

Generate My Certificate starts the process of generating a certificate for the user. The password protecting the private part of the certificate must be kept secret and must not be forgotten, otherwise the user will be not be able to decrypt data sent by others.

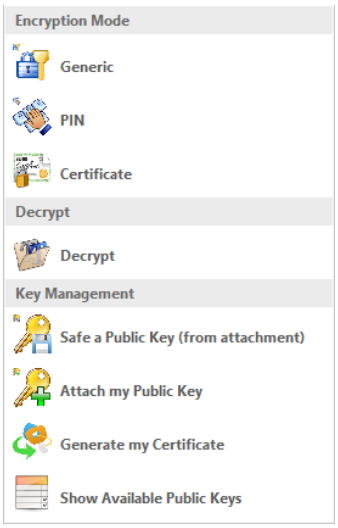
Show Available Public Keys, provides a list of users (their smtp-address) to whom certificate based encryption can be used.

In the Outlook Inspector (email window) CryptIt provides beside the certificate management functions encryption options for attachments of the edited email (new email, forward/reply to an email). The CryptIt symbol with the open lock indicates that attachments are not encrypted.

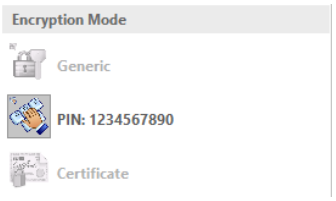
If the encryption method is selected (see below) and the upper part of the split button is pressed, the attachments of the email will be encrypted and the CryptIt split button shows this by the closed lock. Pressing again the upper part of the button will decrypt the attachments again, and the open lock is shown again.

In the Outlook Inspector (email) the CryptIt split button provides functions to select an encryption mode and to support the key management of certificates (see above).

The Encryption Mode must be selected before attachments can be encrypted. CryptIt provides three options. The encryption for the attachment is at all times at the same strength with an AES-256 algorithm, which is very strong.



The most convenient encryption mode is the ***Generic*** option. When the mode is selected it is highlighted and no other mode can be selected. To change the Generic mode needs to be un-selected by pressing it again, and then any mode can be selected. In Generic mode the attachments will be encrypted without any additional secret. As such anyone who receives the email and has CryptIt installed can decrypt the attachment.



Higher security (need-to-know) can be achieved by selecting the ***PIN*** mode. When selected, a PIN will be set by the user and displayed in the mode. The PIN should be at least 10 characters long. For the recipient to be able to decrypt the attachments, he/she needs to know the PIN, which should be provided through another means, for instance through a phone call, or something agreed beforehand.

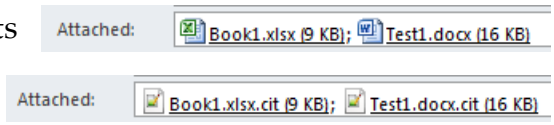
Highest security (need-to-know) can be achieved by selecting the Certificate mode. To use this mode the user needs to generate a certificate AND needs to receive beforehand the public keys from the recipients (background on certificates can be found at Article III). In order to receive certificate encrypted attachments, the other party needs your Public key. To ease handling you can attach your Public Key to an email to send it to others by using the Key Management function ***Attach my Public Key***.

Public keys are named with the email address added with the word public, e.g. support@ugarbe.de.public. If a received email contains a public key as an attachment CryptIt can import this through the Key Management function ***Safe a Public Key***. Once imported you can encrypt attachments for that recipient.

(a) Use Cases – Encryption of Attachments

The CryptIt module supports the encryption of attachments. This and the following use cases illustrate when to use the which encryption mode. All encryption modes encrypt the data with the same strong encryption to keep the confidentiality of the data/information at a very high level. The "only" difference is the method of providing a key to the intended recipient(s) to be able to decrypt the attachment(s). Whoever has this key can read the content of the attachment(s) so protection of the key is important. The encryption modes provide different methods of providing this decryption key to the recipients.

When encryption is activated attachments are encrypted and receive the new file extension .cit as shown in the example where an Excel and Word file become encrypted.



In order to encrypt select first the encryption mode through the CryptIt menu, and then press the CryptIt button (upper part). When encryption is active all current attachments are encrypted. When new attachments are added also those become encrypted, with the exception when encrypting in the Certificate mode.

The three encryption modes support different need-to-know scenarios of the data. When encrypted in the Generic mode everyone who receives the email and has CryptIt installed, can decrypt the attachment and read the content. When encrypted in the PIN mode the recipient(s) need to receive the PIN to be able to decrypt the attachments. When encrypted in Certificate mode only those in the recipient list and where the public key is available, can decrypt the attachments.

(b) Use Case – Company Wide Need-to-Know

Generic encryption is typically used for a huge amount of recipients who have a common need-to-know for the data/information within the attachments. The only thing the recipients need is the installation of CryptIt. The decryption key is managed within CryptIt and does not need any user intervention.

This mode is very easy and is recommended for company data which is for a wider amount of recipients within the company.

Adding recipients or attachments is no problem in this mode.

(c) Use Case – Individual Need-to-Know

PIN and Certificate encryption are typically used when exchanging sensitive data which must be available to certain individuals only.

The PIN mode requires a password (PIN) to be selected by the sender and which the recipient(s) need to receive. Sending the PIN with the same email as the attachments is not a good idea, as then everyone receiving the email can decrypt the attachments. Agreeing on the PIN prior of sending encrypted data, or providing the PIN afterwards through telephone calls or text messages would be required so that the intended recipients can decrypt and read the attachments. PIN mode is mainly used for spontaneous exchange of data with recipients with whom only rarely encrypted data exchange is required.

Although the PIN mode works very easy, there is minor administrative work required to ensure the PIN is available to the recipients, it is also prone for error when the PIN is entered wrongly or transmitted wrongly.

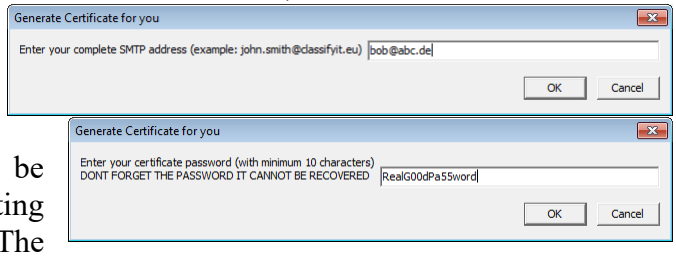
Adding recipients and attachments when encryption is activated is no problem.

For regular exchange of encrypted data the Certificate mode is best, although some administrative work is required in preparation before encrypted data can be exchanged. Once this is done, the method is very reliable and easy to use. To become familiar with certificate based encryption, and in particular with private and public keys, consider reading *Article III*.

In preparation of Certificate based encryption all participants need to generate certificates, which consist of a private and a public key and then distribute the public keys to each other. CryptIt supports these actions as illustrated below.

(i) Generate Public-Private Key-Pair

The CryptIt function ***Generate My Certificate*** guides the user through two steps to create their Public-Private Key-Pair (in other words, the certificate). First the user needs to select his/her email address (SMTP address) which is used for the identity of the key-pair. Second a secure password for the Private Key protection. This password must not be forgotten, and is needed when decrypting certificate based encryption. The password cannot be recovered.



The Public-Private Key-Pair is stored at the user's folder \AppData\Roaming\cli_certs\ .

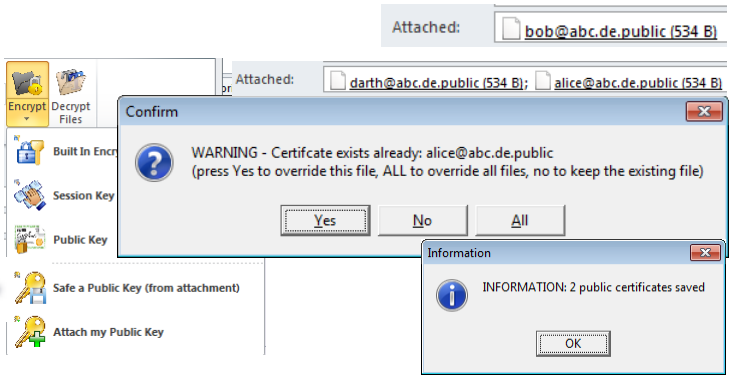
The Public Key is saved in the file: email-address.public (e.g. bob@abc.de.public). The Private Key with the file-extension .private (e.g. bob@abc.de.private). Note: the same folder stores the public keys of other users who did provide their keys and which have been imported.

(ii) Send Public Key

To provide the Public Key to others by email, use the CryptIt function ***Attach My Public Key***. The Public Key of the user is added to the email as an attachment.

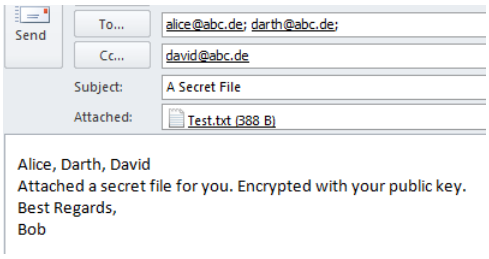
(iii) Receive Public Keys

When receiving an email with Public Keys from other users, the Public Keys can be automatically saved by selecting ***Safe a Public Key (from attachment)***. This function also works for multiple keys. If a Public Key is already in the key store, then CryptIt will warn and ask if the previous key(s) should be overwritten. At the end CryptIt informs how many Public Keys (Certificates) have been saved.



(iv) Certificate based Encryption

To encrypt attachments with the Certificate mode, one needs to make sure that all recipients are in the To, Cc or BCC field, **before** the encryption is conducted, otherwise the attachment will not be encrypted for the later recipients. Also for all recipients one needs the public key, otherwise when there are users where no public key is available those will not be able to decrypt the attachments.



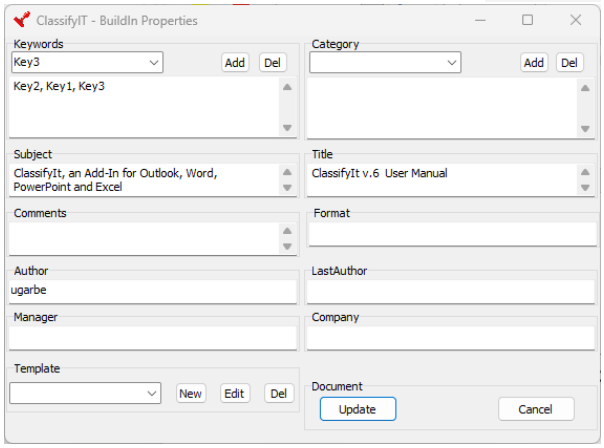
So after all recipients are selected, and the Certificate mode has been selected the attachments can be encrypted. CryptIt checks if all public keys of the recipients are available and if not provides a warning with those recipients for whom no public key is available. If confirmed to continue the attachments are encrypted for those recipients where a private key had been imported. In the example there is no public key for david@abc.de (CC field) and CryptIt warns the user.

Adding attachments when encryption is activated is no problem, but adding additional users would require to decrypt, select Certificate mode again and encrypt again.

Section 2.04 Properties

In Word and Excel, ClassifyIt supports the management of properties, like keywords and categories.

The **Properties** function opens a form to manage the standard properties of a document (word, excel). Providing properties to documents helps organising and finding them back through search engines. Users can define a list of Keywords and Categories. Those can then be selected from the list or added as free-text. Using the list has the benefit of correct spelling and reuse of the same keywords as appropriate.



Beside the benefit of organising consistent keywords and categories for documents, ClassifyIt allows the organisation of templates, which allow the use of the those properties (metadata) also in other documents.

Section 2.05 PDF Export

In Word, Excel and PowerPoint, ClassifyIt supports the export of the document to the PDF format. Using PDF Export fully supports the remanence of the technical security markings.

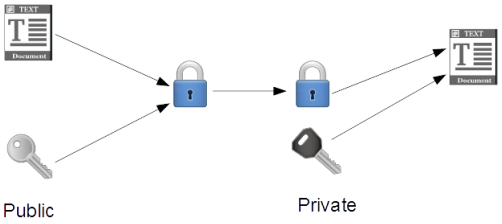
Creating the PDF is a one-click operation. The PDF is automatically stored in the same folder of the original document, for instance the word document, and has the same name. A balloon message informs the user that the action was successful and highlights where the file is saved.

If the original document is not saved when PDF Export is used, then the user needs to save the document beforehand.

Article III. Public-Private Key Concept – how to use certificates

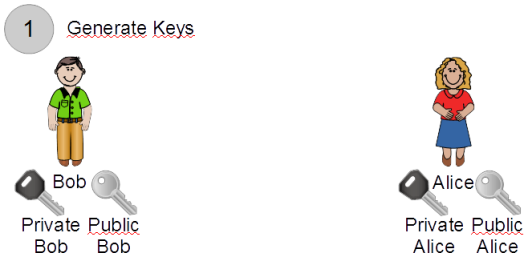
A Certificate is a pair of two keys, plus a number of attributes like the name of the owner, the date of generation, the validity date and so on. When the user Bob generates his certificate those two keys are generated. One key is a private key, which must be kept secret by Bob, and the second key is a public key which should be made available to anyone Bob needs to encrypt data with. The public key could be posted on a site where anyone has access to.

With a Public-Private Key-Pair the following is possible. A text (or any kind of file) can be encrypted with the Public Key, the encrypted text can be transferred anywhere and can only be decrypted with the Private Key.

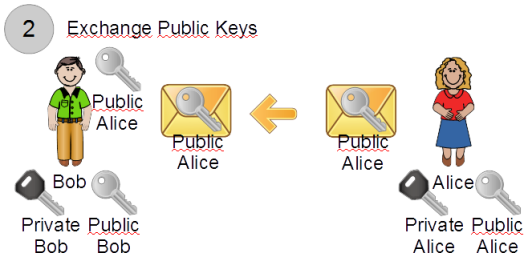


CryptIt Certificate based encryption uses this concept for an easy and very secure encryption of attachments providing the necessary Public-Private Keypairs and the necessary administration of those keys. The following shows an example where Bob and Alice use Public-Private Keypairs to exchange safely data between each other.

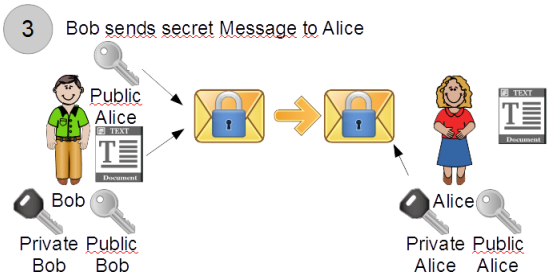
First Bob and Alice need to produce each their Public-Private Keypair. Each key is unique and receives a unique name. In this example Bob generates the Private Bob and Public Bob keys. Alice generates the Private Alice and Public Alice keys. CryptIt can generate those keys with the name of the email address of the user.



Then Bob and Alice can share their Public Keys. This can be done in any way and does not require a special protection of the key. In this example Alice sends her Public key to Bob as an email attachment. CryptIt provides this function to attach the Private Key to an email and when receiving a Private Key to store it appropriately.



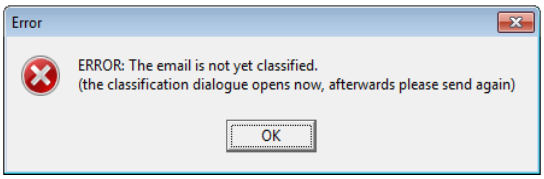
Now everything is in place so that Bob and Alice can exchange in a secure way secret messages. In this example Bob can send Alice a secret message, since he has Alice's Public Key. Bob encrypts the secret message with Alice's Public Key and sends the message by email to Alice. Alice has her Private Key and decrypts the message (no one else can do this!). CryptIt integrates the encryption and decryption of email attachments with one click.



To finalise this example. Consider that Darth had access to the Public Key of Alice and to the encrypted message from Bob to Alice. Darth can't do anything to get access to the secret message. Darth would need the Private Key of Alice, which Alice protects properly.

Article IV. Outlook Behaviour

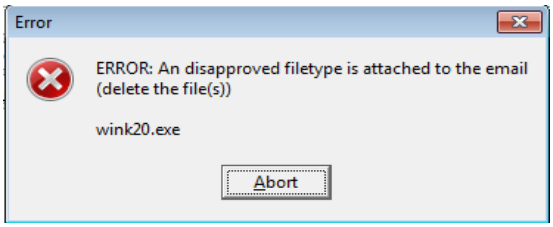
Section 4.01 Email Without a Classification



Emails which have not entered a classification through ClassifyIt cannot be sent by users. If the user tries to send an unclassified email the user is informed and the classification menu opens.

Section 4.02 Email With Unapproved Attachment Type

When users want to send Emails with attachment types which are not authorised an error message is generated listing the attachment(s) which are not authorised.



Section 4.03 Reply or Forward with Lower Classification

Replying or Forwarding emails with a lower classification result either in a warning which the user can ignore or in an error the user has to correct. The behaviour depends on the information security policy and is configurable in ClassifyIt.