

ClassifyIt 7.1

USER MANUAL

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

support@ugarbe.de
2026

Table of Contents

Article I. Introduction 4
Section 1.01 Why use ClassifyIt 4
Section 1.02 ClassifyIt Key Capabilities 5
Section 1.03 What is a Classification Marking 6
(a) Visual and Technical Classification Marking 7
(b) Translated Classification Markings 7
Section 1.04 How ClassifyIt integrates in Office Applications 8
Article II. ClassifyIt Functions 9
Section 2.01 ClassifyIt Menu 9
(a) Assign Metadata 10
Section 2.02 Release Form 11
Section 2.03 Review Date and Downgrade 12
Section 2.04 CryptIt – Word, PowerPoint, Excel 13
(a) Export PDF 13
(b) Export TDF 14
(c) Import TDF 15
(d) Certificate Management 15
Section 2.05 CryptIt – Outlook 18
(a) Encryption 18
(b) Save a Public Key 21
(a) Attach my Public Key 21
Article III. Windows Explorer 22
Section 3.01 Classify 22
Section 3.02 Show Classification 23
Section 3.03 Export as CI-TDF 23
Section 3.04 Opening a Container 23
Section 3.05 Export Original File 24
Section 3.06 Clear Classification 24
Section 3.07 Saving Changes into the Container 25
Section 3.08 Working Copies 26
Section 3.09 Classification on File Icons 26
Section 3.10 Certificate Password 27

Article IV. Public-Private Key Concept - how to use certificates 28
Article V. PDF Export 29
Article VI. Word Paragraph Marking 30
Article VII. PowerPoint Behaviour 33
Article VIII. Outlook Behaviour 34
Section 8.01 Email Without a Classification 34
Section 8.02 Quick Select in Outlook 34
Section 8.03 Email Started from Windows Explorer 35
Section 8.04 Email With Unapproved Attachment Type 35
Section 8.05 Reply or Forward with Lower Classification 36
Annex A – Certificate Exchange Walkthrough 37
Step 1 – Alice Generates Her Certificate 37
Step 2 – Alice Sends Her Public Key to Bob 37
Step 3 – Bob Imports Alice's Public Key 37
Step 4 – Bob Generates His Certificate and Sends It to Alice 38
Step 5 – Alice Encrypts for Bob Using Certificate Encryption 38
Step 6 – Bob Decrypts Alice's Message 38

Article I. Introduction

Section 1.01 Why use ClassifyIt

ClassifyIt is an information security support tool that enables users to apply policy-compliant classification markings to emails and documents, add data loss prevention information, and encrypt documents when distributing them over unprotected networks such as the Internet. ClassifyIt is designed to be powerful in its core functions and easy and intuitive for users and administrators.

Information security starts when writing or updating documents. Mark the document with a visible classification marking, such as SECRET, to ensure that you and others understand the sensitivity of the information within the document. ClassifyIt enforces classification marking and helps users select the correct marking.

Adding such a classification marking manually is possible without a tool, so the obvious and legitimate question is why use ClassifyIt? The answer depends on the kind of business and the size of your organisation. Very small companies might not require such a tool, although marking personal data might be a legal requirement (for example under GDPR) and a tool can help mark such data properly. Competitive, innovative and growing companies own and manage information that makes them unique, and this critical information must not become public or available to their competitors. ClassifyIt helps enforce a visual, human-readable marking as shown above, and adds a technical marking that supports DLP technologies.

The ISO 27001 standard requires the implementation of information classification. ClassifyIt is a highly flexible tool for supporting this requirement. Alongside the tool that enforces classification markings, policies and handling procedures are necessary to provide 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 documents, PowerPoint presentations and Excel spreadsheets. The markings are configured to comply with the company's or organisation's security policy and can be made interoperable with other companies' markings.

ClassifyIt supports classification **consistency** so that an email cannot have a lower classification than its attachments.

ClassifyIt supports the selection of **release** markings to ensure **compliance** with company and organisation security policies. Release markings can support internal and external authorisation to share sensitive data.

ClassifyIt supports adding **metadata** to documents to improve search engine results. Document availability is improved by this feature.

ClassifyIt supports **exporting** Office documents to PDF documents while preserving readable and machine-readable classification marking information.

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

ClassifyIt supports the **encryption** of documents and email attachments through verifiable and secure Trusted Data Format containers. Local support is currently in place for built-in protection (everyone with ClassifyIt can decrypt), PIN protection and certificate-based encryption.

ClassifyIt supports Windows Explorer: any file can be exported to a CI-TDF container from its context menu, a container opens with a double-click, and the icons of classified Office and PDF files and of containers show their classification.

Section 1.03 What is a Classification Marking

A classification marking is a textual label that defines, at a high level, the sensitivity of a document and how that document may be shared internally or externally to your organisation. In the context of ClassifyIt, the sensitivity is called the classification and the sharing statement is called the release.

Below is 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 conform to your organisation's information management policy, which sets the classifications and their meaning, as well as whether 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, optionally, a release marking. Your security administration or information management team defines those markings. For classifications there are normally between three and five categories, similar to those shown in the diagram above: OPEN, RESTRICTED or SECRET.

OPEN would apply to information that can be shared with everyone, where publishing such information on the internet would not reveal internal secrets of your organisation.

RESTRICTED would apply to information that has an official context within your own organisation or with external cooperation partners. This category could apply to information that would give competitors a certain but limited advantage if they became aware of it. Such information therefore needs to be protected with some care. Examples might include internal processes, certain price information or high-level technical information.

SECRET would apply to sensitive information that is very important to your organisation and must be handled with the highest care. This category could apply to information that would give competitors an advantage if they became aware of it. Such information therefore needs to be protected with the highest care. An example might be detailed technical information.

(a) Visual and Technical Classification Marking

ClassifyIt is a Data Loss Prevention (DLP) tool that adds and enforces visual classification markings shown as text within the document. ClassifyIt also adds technical classification markings stored in document properties. ClassifyIt ensures that the visual and technical markings have the same value. Technical markings can be used by software to identify the document classification and enforce whether the document can be provided to a recipient. Those technical markings are stored as key-value pairs, either as a custom property for documents or an x-header in an email. The default key is named: iCLASS, and the value assigned follows the syntax and semantic of the iCLASS standard.

The section above showed a SECRET classification marking with a release. The technical marking is represented in a JSON notation and the iCLASS standard looks like:

iCLASS = {"org": "UGARBE", "class": "S", "rel": ["MAN", "FIN"]}

The values for "class" and "rel" are configurable by the administrator and must match entries in the classification schema. In this notation S represents SECRET, MAN represents MANAGEMENT, and FIN represents FINANCE. "org" is a short code identifying the originating organisation, also configured by the administrator. In real configurations "org" and "rel" could be country codes or organisational codes, like EU or UN or NATO.

(b) Translated Classification Markings

For the visual classification marking, ClassifyIt allows the marking to be represented with a translation. This translation can be an additional visual line that standardises the classification marking. Such standardisation can be useful in international cooperation where the normal classification markings are not the same.

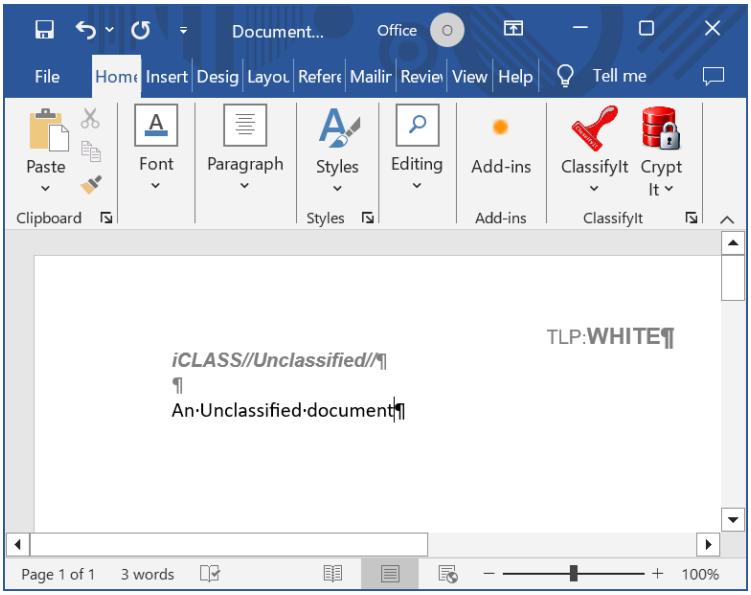
For more information, consult the case study on “International Classification – iCLASS”, available at https://classifyit.eu/case-study/iclass

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

TLP:WHITE
iCLASS//Unclassified//

Section 1.04 How ClassifyIt integrates in Office Applications

ClassifyIt integrates with Microsoft Outlook, Word, PowerPoint and Excel. If further applications are required, please contact the administrator, who can request this via support@ugarbe.de.



In all applications the ClassifyIt Menu is available. It comes with the ClassifyIt button to apply classifications to emails or documents, and the CryptIt button to encrypt, import and export documents and to support basic certificate operations.

Depending on the application, different functions are available under those main buttons. Both are split buttons, so there is a main function when pressing the top of the button and a menu when pressing the bottom of the button.

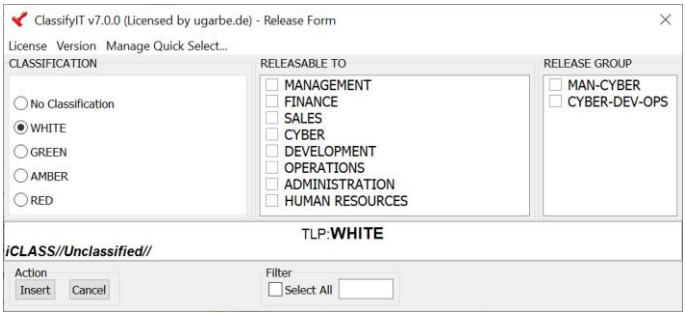
In Outlook the CryptIt component is slightly different because the main function of the button is to encrypt email attachments. In the other applications, CryptIt is mainly used to export the document to a secure and encrypted file type.

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.

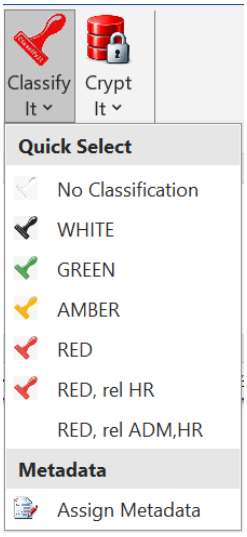
The ClassifyIt menu is a split button providing two functions. One is on the upper half and one is on the lower half of the button.



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). Insert applies the selected classification to the document; Cancel discards the selection.



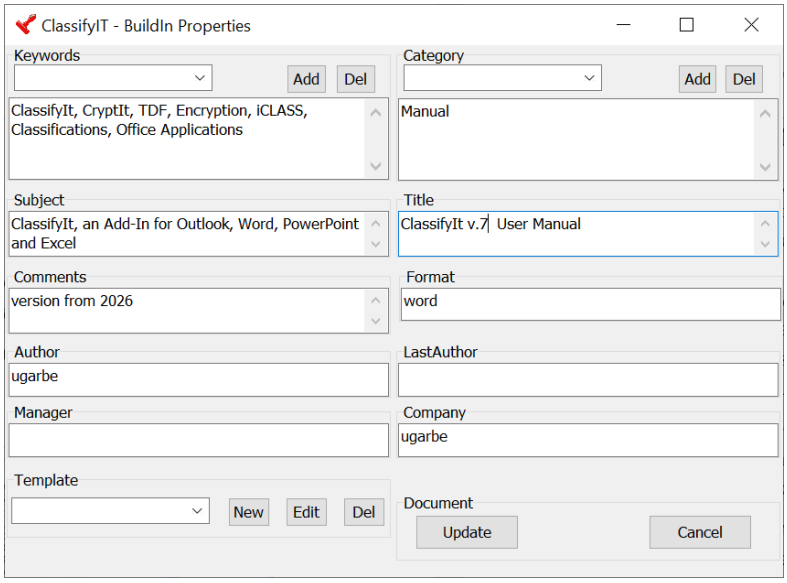
The lower half of the split button opens the integrated Quick Select menu. This menu provides a list of classification markings that are often used within the organisation. The number of entries is limited to 10 and is configurable (see Manage Quick Select below). If more entries are required, contact support@ugarbe.de. The Quick Select menu shows a display name for a particular classification marking and can include a classification and release marking. In essence, it provides a shortcut to frequently used classification markings. Example: REL, rel HR, could be the display name for RED REL: HUMAN RESOURCES. In addition metadata can be applied to word, spreadsheets and powerpoint documents.



(a) Assign Metadata



Assign Metadata opens the document properties dialog for the current document. In Word and Excel, users can maintain values such as title, subject, category, keywords, comments and related metadata; PowerPoint uses the same concept where supported by the host application. Predefined keywords and categories can be selected, or free text entered where the configuration permits; using predefined values keeps spelling and terminology consistent across documents, and templates can be used to apply a prepared set of properties to a document.



These properties help search, discovery and reuse. They do not replace the classification marking. The visible classification and the technical iCLASS marking remain the authoritative classification information.

When a document is exported to CI-TDF, ClassifyIt can include its properties as JSON in the separate 0.metadata entry. The signed manifest contains a hash used to verify those properties on import. These properties remain readable in clear text even when the document content is encrypted, so check them before sharing sensitive information.

Section 2.02 Release Form

The Release Form is the main ClassifyIt window for selecting the classification marking that is applied to the document. Select exactly one classification on the left. In the release column, tick the releases; the filter at the top right shows only the entries that contain the text you type, and ticked entries stay ticked while it hides them. The column's heading, RELEASE, opens a list: Clear selection removes every ticked release, also hidden ones; choosing a release group ticks all its releases - a group marked ✓ has all of them ticked already, and choosing it removes them. Depending on your organisation's configuration the form shows only the classification, or also releases, categories and dates.

The window title shows the version of ClassifyIt and whether it is licensed; About... shows the version, the license and the configuration in use. The Marking preview shows the marking exactly as it will be inserted. Insert - or Enter - applies it; Cancel - or Esc - closes the form without changing the document.

Levels without a release: for PUBLIC and UNCLASSIFIED markings (iCLASS P and U) no release can be selected - the release options are greyed out and an earlier selection is cleared. A release applies from the next higher level on.

Categories: if your organisation configures categories (for example STAFF or FINANCE), the Release Form shows a CATEGORY column. Select any number of them; they describe the kind of information. Categories cannot be selected for PUBLIC (iCLASS P). They appear in the visible marking and in the technical marking (iCLASS).

ONLY: where your organisation uses STANAG 4774 labels, an ONLY box is shown next to the category filter. With ONLY the selected categories restrict who may receive the information (for example STAFF ONLY); without it they are for information.

Review date and downgrade: in the Classify It dialog of a document or email - if your organisation configures it - the Release Form shows the review date and the scheduled change (downgrade), or one of them. The boxes show what the classification has. Tick the review date to record it with the classification and show it in the marking; for a marking without one, the organisation's default period is offered. For a downgrade, choose the lower classification (or the same classification and, with Release, a wider release) and its date; "(no downgrade)" means none. Both dates must lie in the future, and the downgrade must be lower than the current marking: a lower classification, or the same classification released to more nations.

Originator: whoever applies a marking becomes its originator - the marking carries your organisation's code, also for a document that came from another organisation.

Manage Quick Select... (bottom left) allows a user-specific selection and order for the Quick Select menu.

To add a Quick Select option, choose the classification and release options in the Release Form and click the Manage Quick Select button. The Manage Quick Select menu opens. With Add Current, the selected classification and release are added, and you are asked to add a display name (keep it short and precise). In addition, you can select any existing Quick Select marking and edit its name, delete it, or move it up or down in the list.

Quick Select and dates: a Quick Select entry sets the classification and release only; the document's review date, downgrade and categories stay as they are.

Section 2.03 Review Date and Downgrade

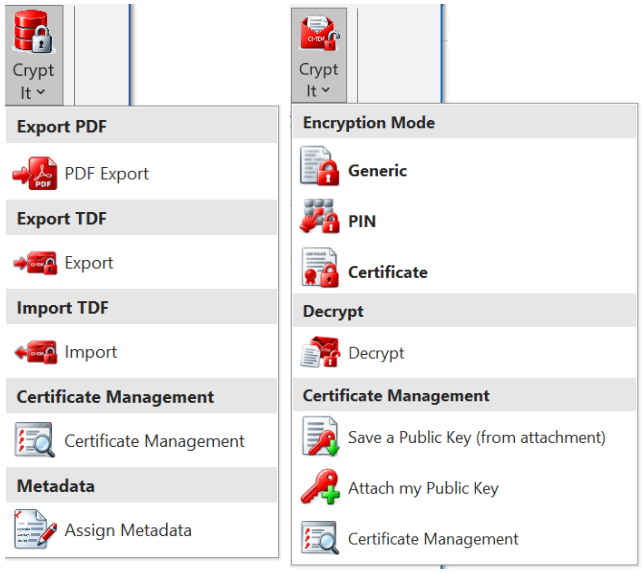
When you open a document in Word, Excel or PowerPoint that you may edit, ClassifyIt checks its dates:

Review date passed: ClassifyIt tells you and opens the Classify It dialog with the current marking and a new review date. Confirm or change the classification and click Insert. If you cancel, nothing changes and you are asked again the next time you open the document.

Downgrade due: ClassifyIt tells you which classification the document has from the downgrade date on and opens the Classify It dialog with that classification preselected. Insert applies it, and the downgrade is removed from the marking; Cancel leaves the marking as it is.

Read-only documents and documents in Protected View are not checked. Nothing changes automatically: the marking that is applied stays valid until you change it. In PowerPoint the presentation's marking - that of the first slide - is checked.

Section 2.04 CryptIt – Word, PowerPoint, Excel



CryptIt is the main encryption menu for documents and email attachments. The menu is slightly different in Outlook and uses the second icon shown.

Word, PowerPoint and Excel provide CryptIt functions to export and import the current document, provide basic key management functions and allow metadata to be integrated into the document. The Outlook CryptIt functions are specialised for email and allow the encryption of attachments, the decryption of attachments and specific and general key management functions.

In Word, PowerPoint and Excel, pressing the upper part of the Crypt It button always starts the Export flow described below and asks for the encryption mode; unlike an email, a document has no persistent encrypted/decrypted state to toggle. The lower part of the button opens the Crypt It menu, which additionally offers PDF Export, Import and Certificate Management.

(a) Export PDF



The Export PDF function creates a PDF version of the current Office document. The document must be saved and classified before export. The PDF is created in the same folder as the source document and normally uses the same filename with the PDF extension.

The visible classification marking remains part of the exported PDF. ClassifyIt also stores the technical classification marking in the PDF metadata so that compatible checking tools can still identify the classification after export.

(b) Export TDF



The Export TDF function exports the current Word, PowerPoint or Excel document to a ClassifyIt Trusted Data Format container (CI-TDF). The CI-TDF container preserves the classification assertion and, depending on the selected mode, can also encrypt the document content. If the document has not been saved to disk yet, the export function will prompt you to save it first. The exported TDF file is created in the same folder, using the same file name with .tdf added.

When Export TDF is selected, ClassifyIt asks for the export mode. None creates an unencrypted CI-TDF container with integrity and classification information. Generic uses the preshared certificate built into ClassifyIt, so anyone with ClassifyIt can decrypt it, including users of shareware builds. PIN protects content with a password shared separately with recipients. Certificate encrypts for recipients whose public certificates are available in your local certificate folder; the sender is automatically included so that the sender can also decrypt the export.

Protection choices: the choices are named after who can open the container: No encryption (None), Anyone with ClassifyIt (Generic), Anyone with the PIN (PIN) and Selected recipients (Certificate). A short explanation below the choices tells what each one protects.

Recipients: in Certificate mode, ClassifyIt lists the public certificates in your certificate folder. Click a recipient to select it and click it again to deselect it; select as many recipients as needed. Your own certificate is always added. The same list is used for an export from Windows Explorer.

Shareware builds create signed, unencrypted CI-TDF containers regardless of the selected encryption mode. Read the encryption notice and check that your installation supports encryption before sending sensitive content. Shareware users can still decrypt supported files created by licensed users.

File limits: the stored payload must not exceed 256 MiB and the restored document must not exceed 512 MiB. If export reports a size limit, reduce the file size or split the content before exporting. If processing fails or is cancelled, the original attachment is retained; a send attempt requiring automatic attachment encryption is blocked until processing completes.

Legacy files: v7 does not decrypt older .cit files. Ask your administrator to recover them using a compatible older ClassifyIt installation and the original keys, then export the recovered content to CI-TDF. Keep the originals until recovery has been checked.

(c) Import TDF



The Import TDF function opens a CI-TDF container and restores the original unencrypted document. If the container is encrypted, ClassifyIt asks for the required decryption information. For PIN mode this is the PIN. For Certificate mode this is the private-key certificate and its password.

After import, ClassifyIt restores the classification from the verified container information. This prevents the user from relying only on the visual text in the document and keeps the technical classification information aligned with the imported content.

Each application imports only its own file types: Word documents, Excel workbooks and PowerPoint presentations. Open any other container from Windows Explorer (see Windows Explorer).

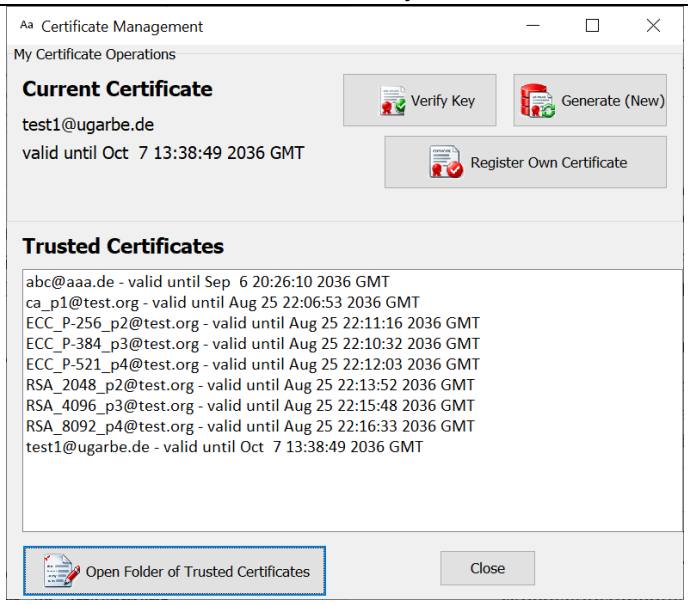
Confirm the sender: before a container is opened, ClassifyIt checks who signed it. If the signing certificate is not in your trusted certificates, ClassifyIt shows its owner and fingerprint and asks you to confirm the sender - compare the fingerprint, its words or its safety number with the sender by phone or in person. A container signed with the Generic key cannot identify its sender; confirm with the sender that they sent it.

Changes you save in the imported document are written back into the container (see Saving Changes into the Container).

Read-only or editing: before the document opens, ClassifyIt asks whether to open it read-only or for editing. A read-only document is not saved back into the container.

(d) Certificate Management

Certificate mode protects content so that only the intended recipients, identified by their certificates, can decrypt it; the sender's own certificate is always included so the sender can also open the protected container later. See Annex A - Certificate Exchange Walkthrough for a complete step-by-step example of generating, exchanging and using certificates.





All of the following actions are grouped behind a single entry, Certificate Management, in the Crypt It menu. Selecting it opens a dedicated window for managing your own certificate and the certificates you have received from colleagues.

Current Certificate: the top of the window shows the name and validity of the certificate you are currently using, so there is no need to open the certificate file itself to check this.



Verify Key: checks that the stored private key matches your certificate and that the password you enter is correct.



Generate (New): creates a new public-private key pair and certificate, replacing the current identity. The private key is protected by a password. Before replacing an identity, back up its certificate and private key securely and retain the password: older encrypted files still require the corresponding old private key.



Register Own Certificate: lets you select an existing certificate together with its matching private key (.pem, .crt or .cer). If the certificate is already in the certificate store, it is simply activated; otherwise it is imported first and then activated.



Trusted Certificates: the list below the buttons shows every certificate you have received from colleagues, together with its validity, so you can check whose public key is available before encrypting for them.

Certificate details: double-click a certificate, or right-click it, to see its owner, validity and fingerprint. The fingerprint is the SHA-256 value of the certificate, shown in three forms that say the same: as hexadecimal groups, as nine words and as a safety number of six groups of five digits. Your own fingerprint is shown at the top of the window with a Copy button, so that you can send it to colleagues.

Trust: a certificate in your trusted certificates is trusted both for encrypting to its owner and for accepting containers signed by its owner. Confirm a colleague's fingerprint by phone or in person before you add their certificate.

Signing: every container you create is signed with your own certificate, whichever mode you choose, so that recipients can see that it comes from you. ClassifyIt asks for your certificate password when it signs.



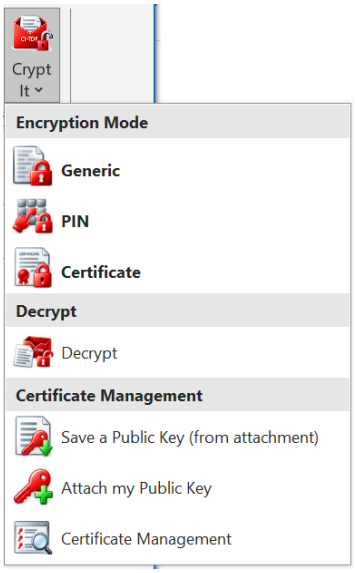
Open Folder of Trusted Certificates: opens %APPDATA%\Certificates, which stores your own certificate and private key and the public certificates imported from colleagues. Protect private keys and their passwords, and keep a secure recovery backup.

Choosing recipients: when you protect a file for selected recipients, tick everyone who should be able to open it - a click on a name ticks or clears it, like a click on its box.

Section 2.05 CryptIt – Outlook



CryptIt in Outlook is the encryption menu for email attachments. Unlike the document-based CryptIt menu in Word, Excel and PowerPoint, it works directly on the attachments of the currently open or selected email, and also provides the key-management entries needed to exchange certificates by email.



The CryptIt split button has two parts. The lower part opens the CryptIt menu, where you first choose an encryption mode - Generic, PIN or Certificate. The upper part then encrypts the current attachments using that mode. Once the attachments are encrypted, pressing the upper part again decrypts them: ClassifyIt detects the current state automatically, so the same button serves for both directions.



Generic Encryption: encrypts attachments using the preshared certificate built into ClassifyIt. Any ClassifyIt installation can decrypt them, including shareware builds. This mode is convenient for broad exchange but is not recipient-specific.



PIN Encryption: encrypts attachments with a PIN chosen by the sender. The PIN must be communicated separately from the encrypted email.



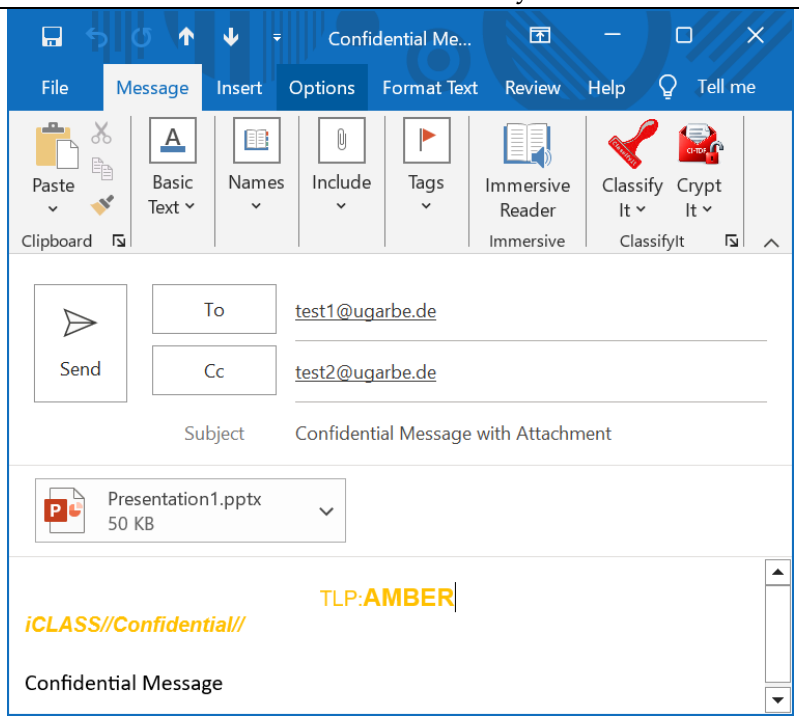
Certificate Encryption: encrypts attachments for the selected recipients' public keys. Only recipients with the matching private key can decrypt the attachments. Certificate files are named after the recipient's SMTP email address - for example, the certificate for surname.name@company.com is named surname.name@company.com.crt.

(a) Encryption

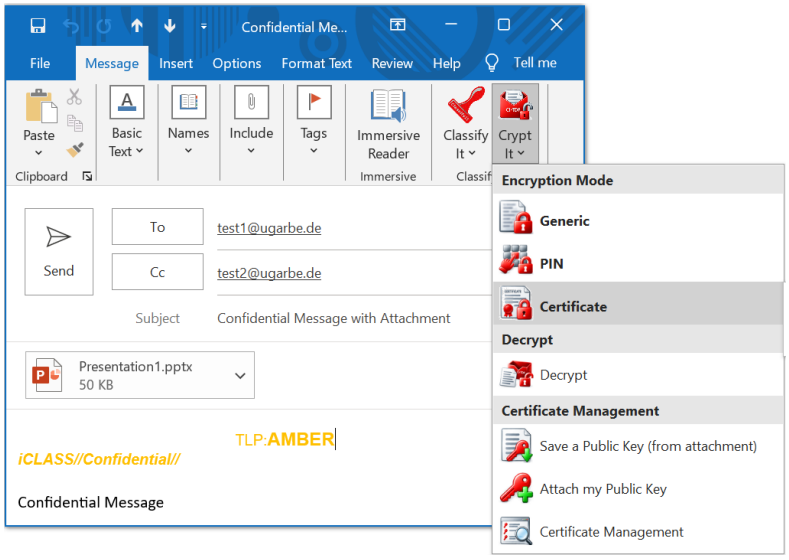
For encrypting attachments, select any of the three modes. When using Certificate Encryption, make sure the recipients are already in the To and/or Cc field, and that you hold the corresponding certificate for each of them in your certificate store.

The following example shows how to encrypt an attachment with Certificate Encryption for two users, test1@ugarbe.de and test2@ugarbe.de. For the second user we have not yet received the public certificate, so we will receive a warning message.

The email has a .pptx attachment and the two recipients already added.

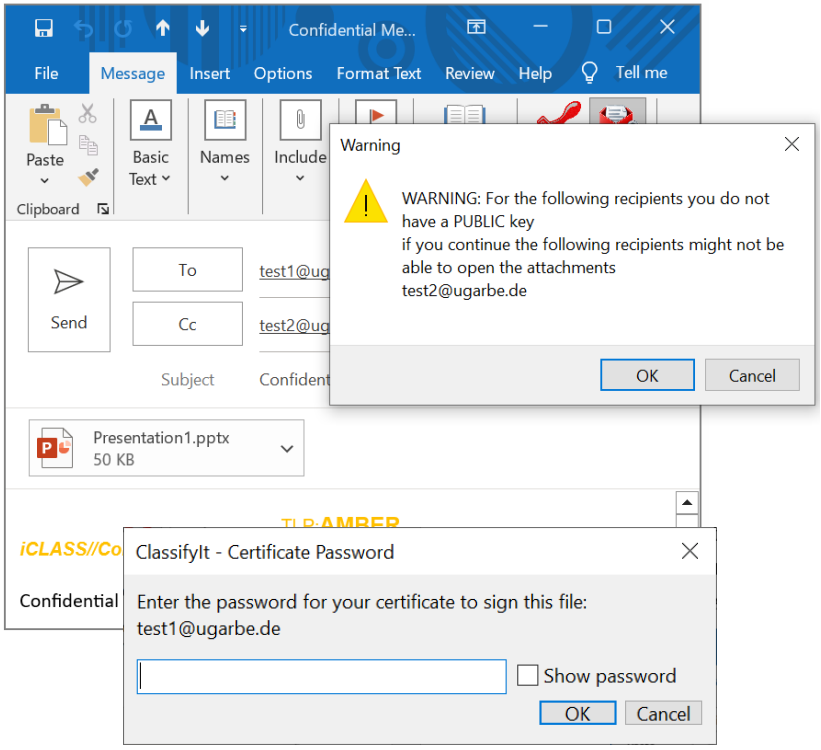


Next, open the Encryption Mode menu and choose Certificate.



ClassifyIt shows a warning that the public key for test2@ugarbe.de is not available.

Continuing will encrypt the attachment, but test2@ugarbe.de will not be able to decrypt it.

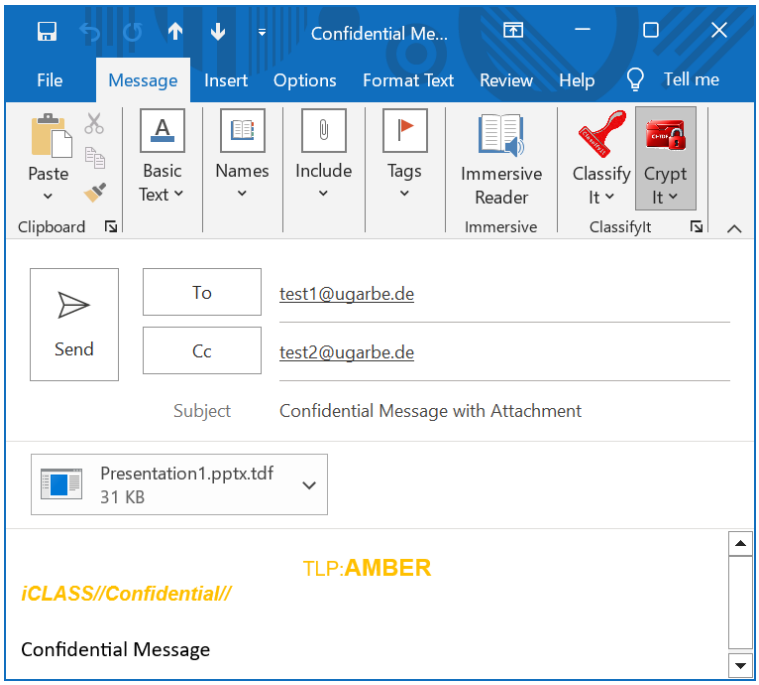


After the warning, enter the password protecting your own private key - in this example, the sender is also test1@ugarbe.de.

If the password is correct, the attachment is encrypted and can only be decrypted by test1@ugarbe.de.

The CryptIt icon now shows as closed, indicating the attachment is encrypted, and the .pptx file has become a .tdf file.

Adding additional attachments will automatically encrypt those as well.



(b) Save a Public Key


Save a Public Key: imports signed public-certificate packages ending in .crt.tdf and public certificates attached as .pem, .crt, .cer or .public files. ClassifyIt can offer to import an unrecognised certificate when you open the email. Private-key files must not be shared or imported as public certificates.

(a) Attach my Public Key


Attach My Public Key: adds your public certificate as a signed, unencrypted <certificate-name>.crt.tdf package. ClassifyIt may ask for the password protecting your private key to sign the package; the private key itself is never included. Recipients use Save a Public Key to verify and import the public certificate. Organisation-specific mail filtering can still affect delivery.

Article III. Windows Explorer

ClassifyIt brings CI-TDF to Windows Explorer, without opening an Office application. The commands are carried out by ClassifyItTool, which the setup installs together with the add-in.

Section 3.01 Classify

Right-click one or more Word, Excel, PowerPoint or PDF files and choose ClassifyIt > Classify File... (on Windows 11 under Show more options). Choose one classification in the Release Form; ClassifyIt writes it into each file - where its program and other ClassifyIt installations read it - and the file's icon shows its stamp. When a Word, Excel or PowerPoint file classified this way is opened, ClassifyIt offers to apply the visible marking.

STANAG 4774: Where your organisation uses STANAG 4774 labels, Classify File also writes the label into each file - in Word, Excel and PowerPoint files the same label part Office writes when you save, in PDFs their metadata.

Signing (STANAG 4778): where your organisation uses STANAG 4774 labels, a finished Word, Excel or PowerPoint file can be signed: right-click it and choose ClassifyIt > Sign Classification (STANAG 4778). The label is then bound to every part of the document - text, headers and footers, pictures, document properties - and signed with your certificate (the password is asked once per session). Sign when the document is finished and closed: a later change makes the signature fail, and saving in Office removes it, because the saved document no longer matches it - sign again after closing. Classify File signs as well, and Outlook signs the Word, Excel and PowerPoint attachments of an email when it is sent - only the attached copies, your files stay as they are. Without your own certificate the files keep the label without a signature. Show Assertions shows the result: valid (with the signer and whether the signer is in your trusted certificates), changed since signing (with the parts that changed), invalid, or not signed.

Text files from a container: a .txt.tdf, .csv.tdf, .json.tdf or other text container opens in your text editor. Many editors keep their own unencrypted copy of open files - also of unsaved changes - for their next start, and close without asking to save. ClassifyIt tells you so when you open such a file, with the settings to switch this off in your editor (e.g. Notepad, Notepad++). Press Ctrl+S before you close the file: ClassifyIt then offers to save it back into the container. "OK, don't show this again" hides the message for the future.

A file that is classified already - in its application, by a PDF export or here before -

keeps its classification: ClassifyIt lists it and leaves it unchanged. Change it in its application.

Section 3.02 Show Classification

ClassifyIt > Show Classification shows the classification of the selected Word, Excel, PowerPoint, PDF and CI-TDF files as your configuration names it: classification, originator, release, categories, review date and downgrade. A container is not opened for this; its classification is verified when it is opened.

The window: Show Classification and Show Assertions open a window with the ClassifyIt stamp in the title bar and on the taskbar; it stays in front of Explorer until you close it.

Section 3.03 Export as CI-TDF

Right-click one or more files and choose ClassifyIt > Export to TDF... (on Windows 11 under Show more options). Each file is protected as a container next to it, named <file name>.tdf; the original files are not changed.

A file that already carries a ClassifyIt classification keeps exactly that classification, even if it comes from another organisation. For the other files you choose one classification in the Release Form; it is written into the copy inside the container, and when that document is first opened in Word, Excel or PowerPoint, ClassifyIt offers to apply the visible marking.

Then choose the encryption mode - None, Generic, PIN or Certificate - as for an export from Office. Several selected files are exported together, with one classification and one mode.

No mode is preselected. Generic only scrambles the file: everyone with ClassifyIt can open it - choose PIN or Certificate to protect the content. If a container of the same name exists in the folder, ClassifyIt asks before replacing it.

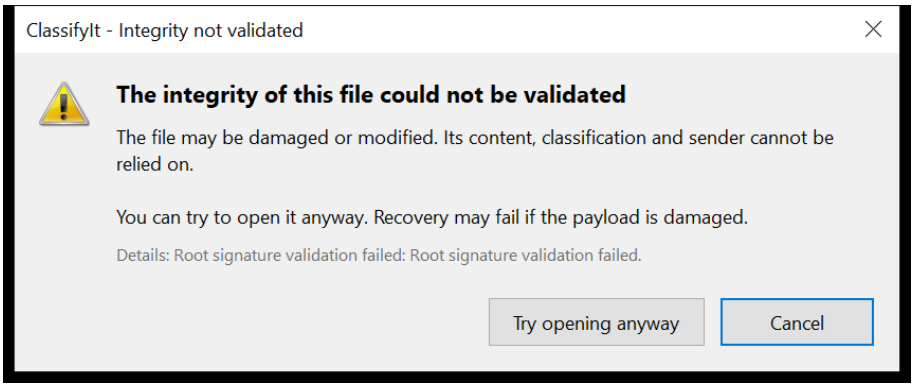
Section 3.04 Opening a Container

Double-click a .tdf file. ClassifyIt verifies the container, asks you to confirm the sender if the signing certificate is not trusted (see Certificate Management), asks for the PIN or your certificate password if needed, and opens the file with its program. The decrypted file is kept in a local working folder, not next to the container.

If the file inside is a program, script or shortcut (for example .exe, .js or .lnk), ClassifyIt warns before opening it - open it only if you trust the sender and

expected the file. A container downloaded from the internet or saved from an email passes this mark on to the opened file: Office opens it in Protected View, and Windows warns before running a program.

Damaged or changed container: if ClassifyIt cannot validate a container - its signature, its manifest or its classification no longer match - it warns that the content, classification and sender cannot be relied on. Cancel is the default. Try opening anyway opens the file if its content can still be recovered: the sender is then not confirmed, the working copy keeps the warning, and it can never overwrite the original container - save it as a new container instead. If the content itself is damaged, it cannot be opened.



The warning for a container whose integrity cannot be validated.

Section 3.05 Export Original File

Right-click a .tdf file and choose ClassifyIt > Export Original File to save the file inside, verified, next to the container under its original name - for example to keep it or to pass it on. If a file of that name exists in the folder, ClassifyIt asks before replacing it. The exported file is no longer protected by the container; an Office or PDF file keeps its classification.

Section 3.06 Clear Classification

ClassifyIt > Clear Classification removes the stored classification of Word, Excel, PowerPoint and PDF files. The visible marking stays in the document until it is opened.

On opening: when such a file is opened next in Word, Excel or PowerPoint, ClassifyIt explains that its classification was cleared and offers to remove the visible marking too: in Word the marking in headers and footers, in Excel the matching header and footer text, in PowerPoint the marking on the slides. Paragraph markings and text typed by hand stay - check the document before you

share it. A read-only document is only reported; ClassifyIt asks again once it can be edited.

Section 3.07 Saving Changes into the Container

When you save the opened file, ClassifyIt writes the changes back into the container. For Word, Excel and PowerPoint documents the add-in does this; for all other files - for example text files, PDFs or pictures - ClassifyIt watches the file and writes it back each time the program has saved it. The container keeps its protection:

None, Generic and PIN: the container is overwritten after a warning at every save; for a PIN container the PIN is asked again and checked.

Organisation: a container from another organisation is saved back like your own, after the same warning, which names the organisation it comes from. A Certificate container keeps its recipients.

Classification: the container gets the classification the document has when you save it. If you change the classification, that is your responsibility - ClassifyIt does not stop a lower class or a wider release. To keep the original unchanged, choose Save as new container: the new container and the file name in its manifest get the name you choose.

Changes not saved into the container: if your changes cannot be written back - you decline, the integrity of the original could not be validated, or an error occurs - ClassifyIt tells you why, and you choose: Retry; Save as new container (you name it, and later saves go into the new container); Keep for later (the working copy is kept, and you are asked again the next time you start the application); or Discard changes, after a confirmation. Changes in a working copy are never deleted without asking.

Changed elsewhere: if someone else saved the container after you opened the document, the warning says so, and No is the default - choose Save as new container to keep both versions.

Save As in the program creates a copy outside the container, which is not encrypted. Word and Excel warn before this happens. PowerPoint does not tell ClassifyIt whether you chose Save or Save As, so it asks at every save of a document from a container whether to continue; No, the default, cancels the save.

State on the Crypt It button: while a document from a container is open in Word, Excel or PowerPoint, the Crypt It button shows its state instead of its name: TDF (saved), TDF (unsaved), TDF (saving) just after a save, TDF (discarded) after you

discarded your changes, TDF (not verified) after an integrity warning, or TDF (check) if the container is missing or was changed elsewhere. A save you cancel leaves it at TDF (unsaved). Point to it to see the container and the full state; click it for an explanation. Its menu keeps the other functions.

Section 3.08 Working Copies

Decrypted working copies are deleted as soon as no program uses them any more: Word, Excel and PowerPoint copies when the application is closed, other files at the latest 15 minutes after their last use, and all of them when you sign out. Editors with tabs show only the active tab's file name; a file in another tab may therefore be deleted after 15 minutes. When you save it, the editor writes it again and it is still written back into the container. A working copy with changes that are not in its container is kept until you have decided what to do with them: ClassifyIt offers them again when you start Word, Excel or PowerPoint, and, for other files, the next time you use ClassifyIt from Windows Explorer.

Section 3.09 Classification on File Icons

Classified Word, Excel, PowerPoint and PDF files show a stamp in the top right corner of their icon, and so do CI-TDF containers, which also show the icon of the file inside, in a frame of the classification's colour. The stamp is the one your configuration defines for the file's class - also for a file classified by another nation or organisation: a German VS-VERTRAULICH (C) document shows your stamp for C.

A ring around the stamp shows that the file's review date has passed or its downgrade is due. Explorer shows it when the folder is opened or refreshed.

Class not in your configuration: a class your configuration does not have - for example O (Official) or T (Top Secret) - is not shown as another class. Such a file gets a rounded square with an "i" (for iCLASS) in the colour of that class on classifyit.eu/iclass.

Previews: Word, Excel and PowerPoint files saved with a preview picture show it in the larger Explorer views. For a classified file the stamp sits in the top right corner, as on the icons; the program's small logo stays bottom right. Files without a preview picture show their icon with the stamp.



Class in your policy:
its stamp

Class not in your policy:
iCLASS square (O)

Class not in your policy:
iCLASS square (T)

Review date passed:
amber ring

Previews in Windows Explorer: the stamp of a class, the iCLASS square for classes not in the configuration, and the ring of a due review date.

Out-of-date icons: if icons or previews look out of date - for example after ClassifyIt was installed or updated, or its configuration changed - run ClassifyItTool restartshell. It restarts Windows Explorer, empties its icon and preview caches and reopens your folder windows.

Network drives: files on network drives get their stamp a moment after the folder opens. If that is slow on your network, right-click any file and choose ClassifyIt > Hide stamps on network drives; Show stamps on network drives turns them on again. Your administrator may have set this for the computer - then it cannot be changed.

Section 3.10 Certificate Password

When you open or create several certificate-protected containers from Windows Explorer, your certificate password is asked once and remembered for 15 minutes.

Article IV. Public-Private Key Concept - how to use certificates

A public-key certificate contains a public key and identifying information. Its matching private key is stored separately, must stay secret and is protected by a password. Share only the public certificate so that other users can encrypt information for you.

When Bob wants to receive certificate-encrypted data, he generates a certificate, keeps its private key and sends the public certificate to Alice. Alice imports it and encrypts for Bob. Bob can decrypt using his private key and password; ClassifyIt also includes Alice's own certificate so that she can reopen her export.

The public key does not need to be protected as a secret. It can be sent by email or made available through another trusted distribution method. The private key and its password must be protected carefully. If the private key is lost or the password is forgotten, encrypted information for that key can no longer be decrypted.

For regular certificate-based exchange, each participant should generate a certificate, share the public key with communication partners and import the public keys received from others. Once this preparation is complete, certificate mode is reliable and convenient for recurring need-to-know exchange.

Article V. PDF Export



In Word, Excel and PowerPoint, ClassifyIt can export the current document to PDF. The source document must be saved and classified before export. The PDF is created in the same folder as the source document and normally uses the same filename with the PDF extension.

The exported PDF keeps the visible classification marking and stores the technical classification marking in PDF metadata. This supports later checks by ClassifyIt and by compatible DLP or inspection tools.

The PDF is saved next to the document - for a document opened from a CI-TDF container, next to the container. If a PDF of the same name exists, ClassifyIt asks before replacing it. The same applies to Export TDF.

Article VI. Word Paragraph Marking

Paragraph marking is a beta feature and should only be enabled by the administrator in test environments. When enabled, Word shows paragraph marking commands in the ClassifyIt menu. Selected paragraphs can receive individual markings in addition to the document classification. Keep paragraphMarking disabled for production deployment.

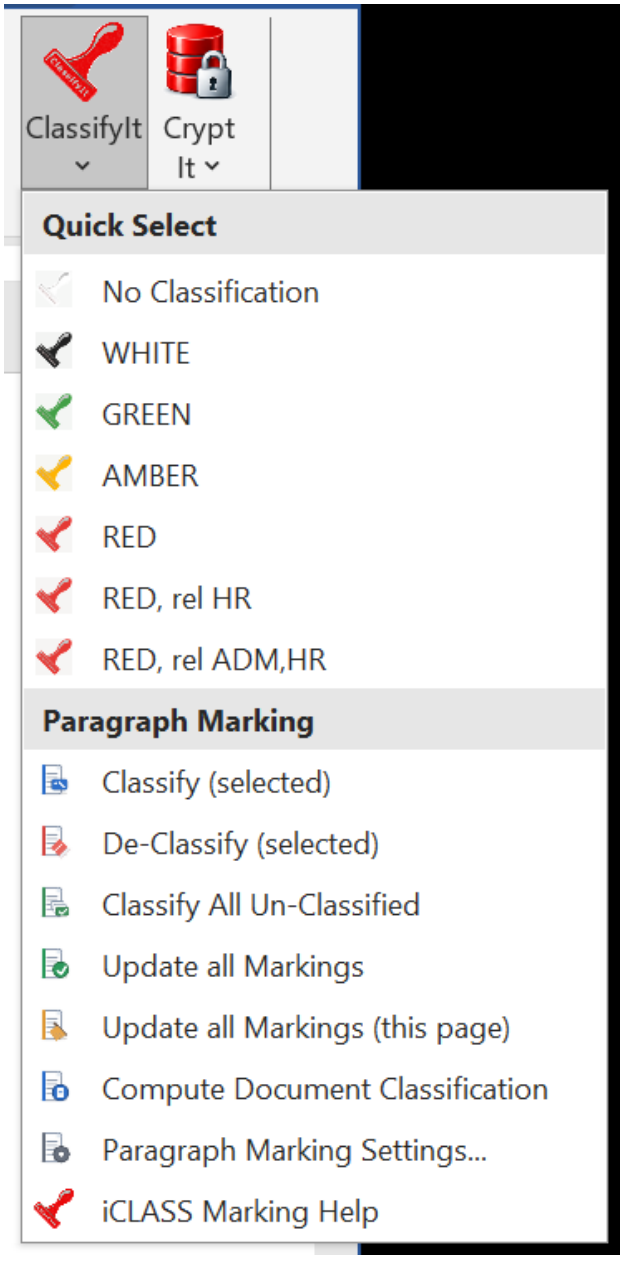


Figure 5-1. Word ClassifyIt menu with paragraph marking commands enabled.



Classify selected paragraphs: applies a paragraph classification to the current selection.



Classify all unmarked paragraphs: adds paragraph markings where no paragraph marking is currently present.



Clear paragraph markings: removes paragraph markings from the selected paragraphs.



Refresh paragraph markings: updates the visible paragraph markings in the document.



Document classification from paragraphs: calculates or verifies the document classification based on paragraph markings where this is enabled by policy.



Paragraph settings: opens the paragraph marking settings dialog.

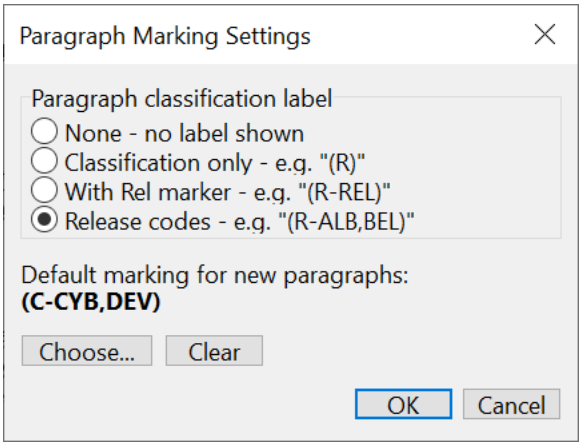


Figure 5-2. Paragraph marking settings.

Paragraph markings are shown beside the relevant paragraph in a compact iCLASS-style notation. Depending on policy, release codes can be hidden, shown generically, or shown with the actual release markings.

Document classification from paragraphs follows the same rule as a PowerPoint presentation: the document gets the highest classification of its paragraphs, and only the releases that all paragraphs above UNCLASSIFIED have in common. PUBLIC and UNCLASSIFIED paragraphs are ignored for the release.

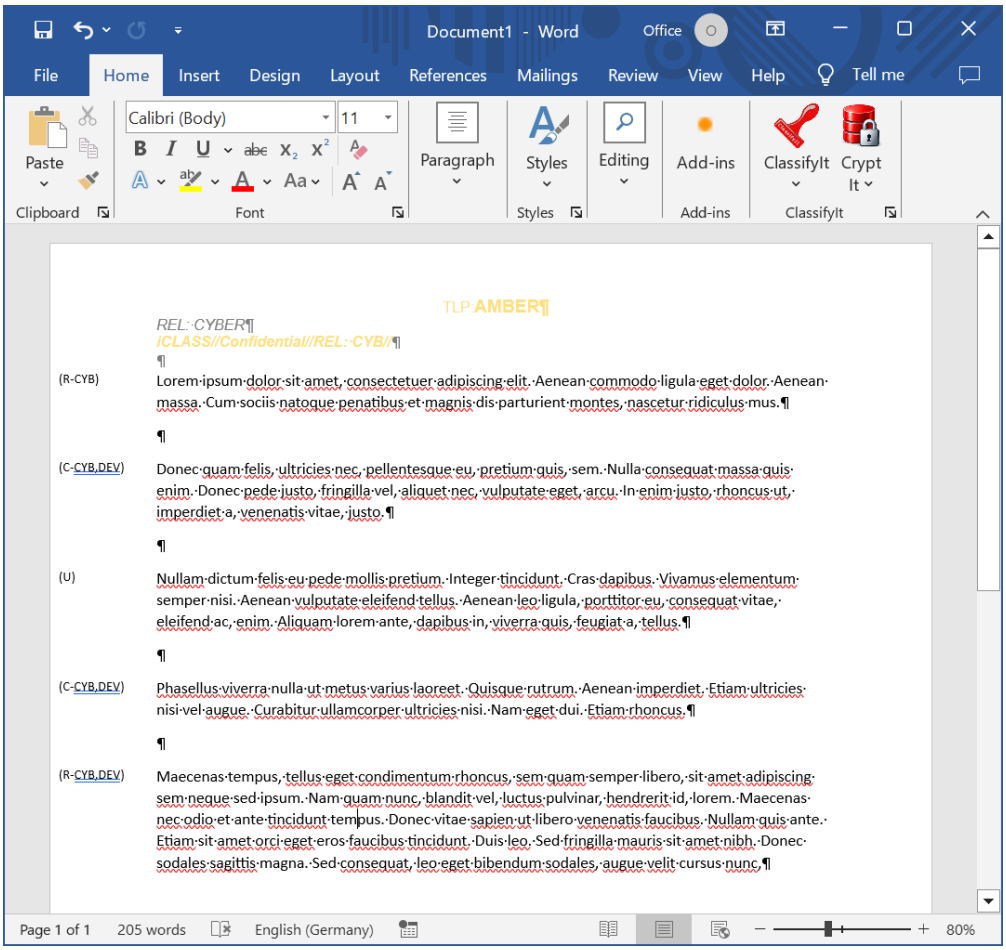


Figure 5-3. Example Word document with paragraph markings.

Article VII. PowerPoint Behaviour

In PowerPoint each slide carries its own classification marking, and the first slide carries the classification of the whole presentation. When a classified presentation is saved, ClassifyIt checks the first slide against the other slides:

Lower: the first slide must not be classified lower than any other slide. If it is, the presentation is not saved and you are asked to correct it.

Higher: if the first slide is classified higher than all other slides, a note is shown and the presentation is saved.

Release: for the slides above UNCLASSIFIED, the first slide must not release to more than all of them allow in common - if it does, the presentation is not saved. If it releases to less, a note is shown.

PUBLIC and UNCLASSIFIED: these slides carry no release and are ignored for the release check.

The CheckClass button in the ClassifyIt menu runs the same check at any time, without saving.

Article VIII. Outlook Behaviour

Section 8.01 Email Without a Classification

Depending on the configuration, Outlook emails may not be sent without a classification. If the user tries to send an unclassified email, ClassifyIt informs the user and opens the classification menu so that a valid marking can be selected.

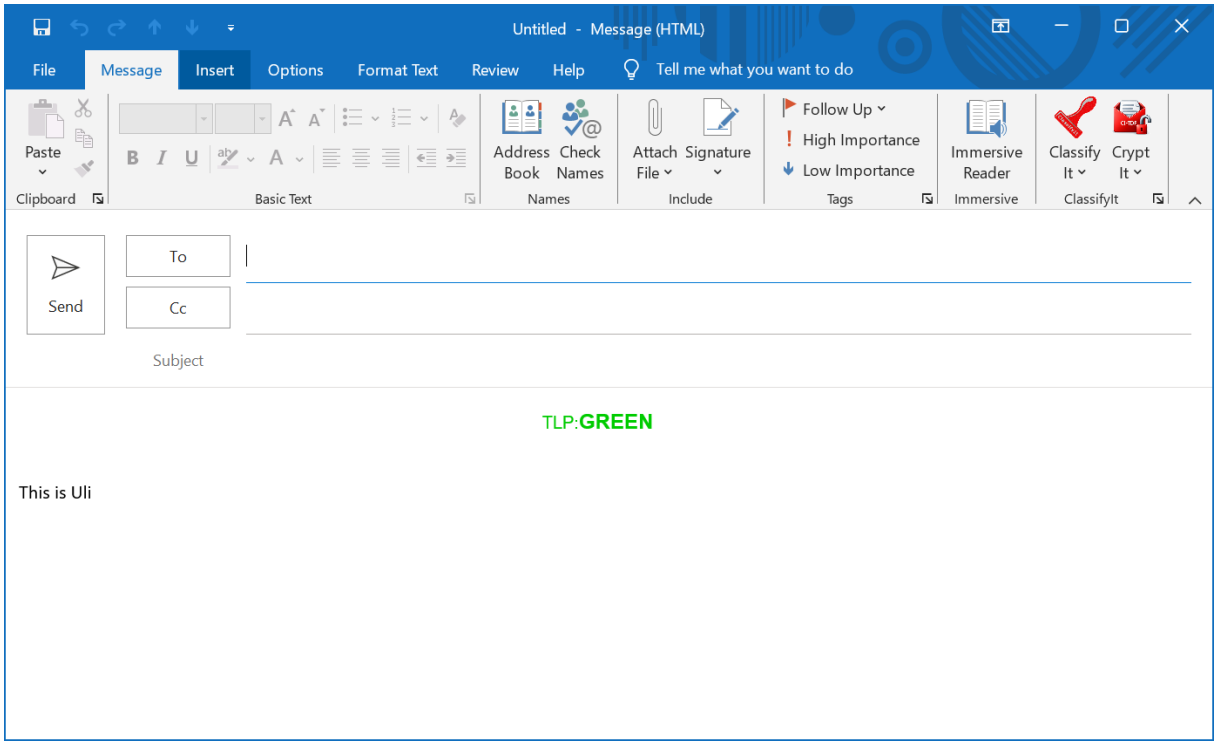


Figure 6-1. New Outlook email with the ClassifyIt menu available.

Section 8.02 Quick Select in Outlook

Quick Select provides shortcuts for frequently used markings. The entries are configured by the organisation and can also be adjusted by the user where this is allowed. Selecting an entry immediately applies the corresponding classification and release marking.

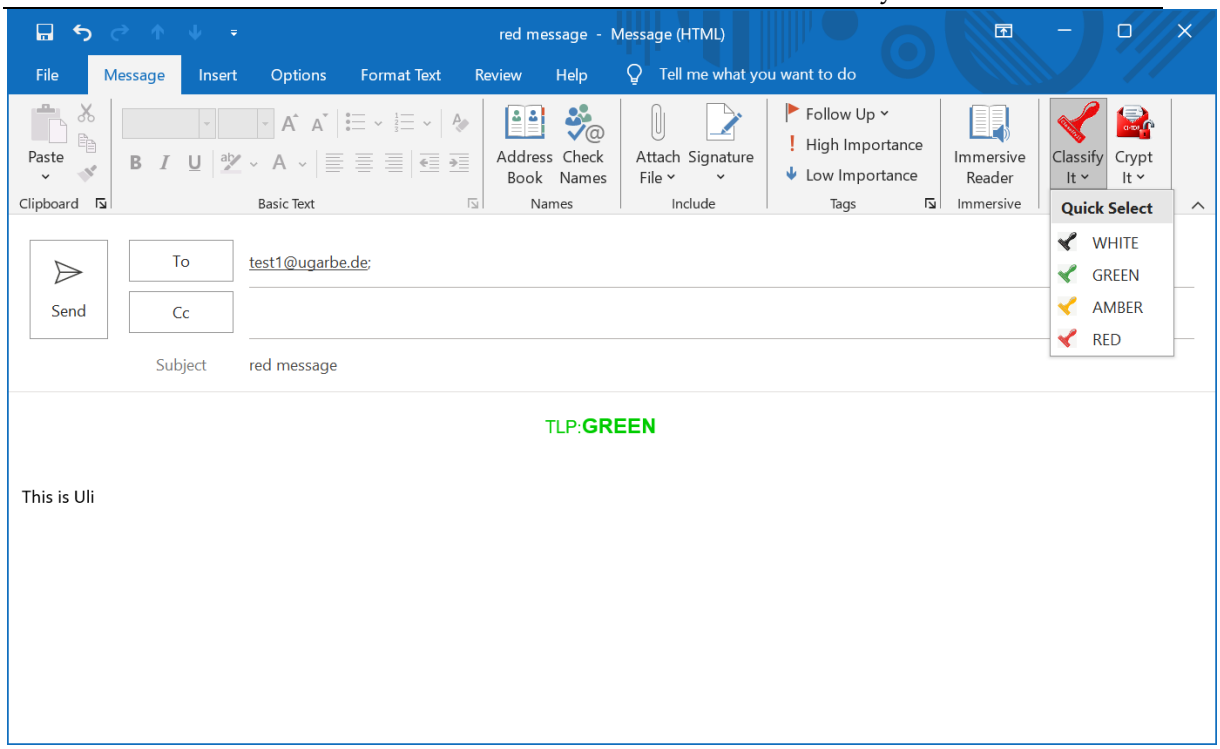


Figure 6-2. Quick Select menu used to apply a frequently used marking.

Section 8.03 Email Started from Windows Explorer

ClassifyIt places the classification marking at the top of the email body in a protected area, so that it cannot be changed or deleted by mistake while you write.

An email started with Send to > Mail recipient in Windows Explorer opens in plain-text format, in which this protected area cannot be created. ClassifyIt then writes the marking as normal text. It can be edited, but ClassifyIt checks it when the email is sent: if it was changed, the email is not sent and the classification is applied again.

To have the protected area, switch the email to HTML or Rich Text (Format Text > Format) and apply the classification again. The recipient receives the marking as text in either case.

Section 8.04 Email With Unapproved Attachment Type

ClassifyIt can block or warn about attachment file types that are not authorised by policy. If a user attempts to send an email with an unapproved attachment type, ClassifyIt displays a message identifying the attachment that must be removed or replaced.

Section 8.05 Reply or Forward with Lower Classification

When replying to or forwarding an email, ClassifyIt can compare the new email classification with the original email and its attachments. Depending on policy, a lower classification can either trigger a warning or block sending until the classification is corrected.

If attachment checking is enabled, ClassifyIt can also compare the email classification with the classification of attached Office documents and exported PDFs. This helps prevent sending an email whose marking is lower than the information it contains.

A reply or forward is marked by you: it carries your organisation's code and no review date or downgrade. The categories of the original email, and ONLY, must be kept - ClassifyIt checks this when the marking is applied and when the email is sent.

Annex A – Certificate Exchange Walkthrough

This annex walks through a complete certificate exchange between two colleagues, Alice and Bob, from generating their certificates to encrypting a document for each other. It builds on the concepts introduced in Public-Private Key Concept - how to use certificates, and on Certificate Management described under CryptIt.

Step 1 – Alice Generates Her Certificate



Generate (New): Alice opens the Crypt It menu (in Outlook, Word, Excel or PowerPoint) and selects Certificate Management. In the Certificate Management window she clicks Generate (New). ClassifyIt creates a new public-private key pair and asks Alice for a password that will protect her private key.

Alice chooses a strong password and keeps a secure backup of her certificate, private key and recovery information. Losing the key or password can make files encrypted for that key inaccessible. Her new certificate is now shown as Current Certificate.

Step 2 – Alice Sends Her Public Key to Bob



Attach My Public Key: in a new email to Bob, Alice selects Attach My Public Key from the Crypt It menu. ClassifyIt creates a signed, unencrypted .crt.tdf certificate package and may request her private-key password to sign it. Only her public certificate is attached; her private key remains on her computer.

Alice sends the email to Bob. The public key is safe to send this way: only the matching private key, which never leaves Alice's computer, can decrypt information encrypted with it.

Step 3 – Bob Imports Alice's Public Key



Save a Public Key: when Bob opens the email, ClassifyIt can offer to import Alice's .crt.tdf package; alternatively, he selects Save a Public Key (from attachment) in the Crypt It menu. ClassifyIt verifies the package before copying the public certificate into the local certificate folder.

Alice's public certificate appears in Bob's Trusted Certificates list together with its validity. A valid package signature proves that the package matches the enclosed signing certificate; confirm the certificate owner's identity through your organisation's trusted exchange procedure before relying on it.

Step 4 – Bob Generates His Certificate and Sends It to Alice

Bob repeats Step 1: he opens Certificate Management and clicks Generate (New) to create his own certificate and password. He then repeats Step 2, attaching his public key to an email to Alice using Attach My Public Key. When Alice receives it, she imports it the same way Bob did in Step 3, either automatically or via Save a Public Key (from attachment).

Alice and Bob now hold their own password-protected private keys and each other's public certificates. They can reuse these certificates for subsequent exchanges, but must exchange updated public certificates when identities are replaced or renewed.

Step 5 – Alice Encrypts for Bob Using Certificate Encryption



Certificate: in Outlook, Alice adds Bob to the email recipients and selects Certificate mode. For a Word, Excel or PowerPoint export, she selects Bob's certificate in the recipient-selection dialog. Bob's certificate, received from him in Step 4, is now available.

In Outlook, Alice attaches the file(s) she wants to protect and then presses the upper part of the Crypt It button to encrypt the attachments. In Word, Excel or PowerPoint, the same Certificate mode is used with Export instead, to protect the current document as a CI-TDF container. Alice sends the encrypted email or container to Bob.

Step 6 – Bob Decrypts Alice's Message

Bob opens the email and presses the upper part of Crypt It to decrypt its attachments, or uses Import for a CI-TDF document. His matching private key and password unlock the content. ClassifyIt automatically included Alice's certificate during encryption, so she can also decrypt with her own private key and password. Other recipients need a private key corresponding to a certificate included when the file was encrypted.

Once this one-time exchange of public keys is complete, Alice and Bob can repeat Steps 5 and 6 as often as required, in either direction, without exchanging keys again. If either certificate is replaced (for example, after Generate (New) is used again) or expires, the exchange in Steps 1 to 4 must be repeated before Certificate mode can be used between them again.