EXCEL MACRO SECURITY AND CERTIFICATES

Valid for ALLEVO XLSM - Master from Excel 2010

Technical documentation

Allevo

KERN

Table of Contents

1 Introduction 3

1.1 Allevo and Excel Macro Security and Certificates 3

1.2 Starting and working with the Allevo-Master 4

1.3 Offline-Process with MultiPage files 4

1.4 Trusted locations 5

2 KERN Certificate / Use signature in Allevo planning 6

2.1 Signature in Allevo Master 6

2.2 Installing the KERN certificate (public key) at the workstation 6

2.3 Installation of public key via Excel security query 8

3 Allevo Allevo with customer's own certificate 10

3.1 Overview / background 10

3.2 Creating your own certificate 10

3.3 Installing (and removing) the private key 11

3.4 Signing Allevo Master 11

3.5 Generating the public key 12

3.6 Installing the public key 12

4 Special case: Allevo MultiPage functions in offline mode 13

4.1 Background of the MultiPage Planning 13

4.2 Workstation for generating the offline files 13

4.3 Workstations for MultiPage planning 13

5 Appendix 14

5.1 Rolling out the Group Policy certificate 14

5.2 Displaying or removing installed certificate 14

5.3 Do not use Excel 4.0 Macros 15

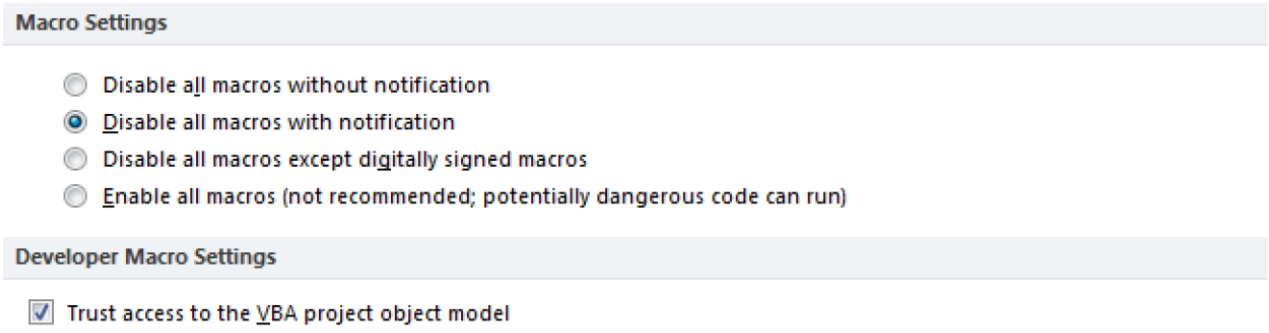
1 Introduction

1.1 Allevo and Excel Macro Security and Certificates

Allevo Master is provided in XLSM format (in older Allevo versions also XLS format).

XLSM is the standard format for workbooks with macros since Excel 2007. Allevo Master in this format is superior to the XLS format in terms of performance at startup (especially from Excel 2010). For this reason alone, XLSM should be the preferred format.

In order to avoid the danger of macros, companies are increasingly restrictive about the security regulations for executing Excel workbooks with macros. Excel 2010, for example, offers the following security settings as standard:



Picture 1-1: Excel Settings für macros

If the topmost option is active in the settings for macros, an Allevo master cannot be called up because VBA programs (macros) control a large part of the required functions.

With one of the middle options

- "Disable all macros with notification" or
- "Disable all macros except digitally signed macros".

only digitally signed Excel workbooks can be opened without a security warning. In the case of Allevo, the corresponding signature must therefore be entered in the master.

Note:	The setting option "Disable all macros with notification" is the sharper version of both (even if it is not directly visible in the text). In this case, all signed Excel files are accepted without further inquiry, all others are rejected (the option is therefore not clearly formulated).

For Allevo (and other applications with SAP Office Integration) the switch at "Trust access to the VBA project object model" should also be set (is only required for Allevo for marginal functions, e.g. displaying the VBA version of a master).
The documentation here describes how Allevo can be used comfortably even under increased security requirements. We distinguish two cases:

a. Normally, planning data are entered directly via the Allevo master. The call is made in in-place mode via SAP Office Integration (DOI) or via the Allevo Business Client (ABC). In this case, a certificate should ensure that Excel allows running the Allevo-Master.

b. Special case with MultiPage offline functions, where new Excel worksheets are created and these are stored on the hard disk as individual offline files. In this case, Excel unfortunately removes the signature; the associated files can no longer be accessed afterwards. In this case, a special copy routine or a customer-specific certificate can ensure that the offline files can also be created and retrieved in MultiPage mode.

The procedures described here for working with certificates correspond to standard recommendations e.g. from Microsoft when using VB programs. So it is actually not an Allevo-specific topic.

Especially in case (a) with in-place processing via DOI, SAP has the same basic conditions, e.g. when switching to the Excel display in a GR55 report or in the ALV.

1.2 Starting and working with the Allevo-Master

Normally, planning data are entered directly via the Allevo-Master. The start is made in in-place mode via SAP Office Integration or via the Allevo Business Client (ABC). In the case of increased security settings, a certificate should ensure that Excel allows the Allevo-Master to be called up.

When working in in-place mode, Allevo uses SAP Office Integration functions that various SAP applications (e.g. switching ALV display to Excel, Report Painter / Writer, GR55 with Office Integration) also used. Accordingly, there are some basic SAP notes on this topic:

- 816178 - RW: Excel macro security
- 1992004 - Report Writer: Validity of the digital signature in OI-Excel templates
- 696069 - No data display in Excel Inplace in ALV under Office 2003/XP
- 1567380 / 1425448 - Additional window when opening an Excel file with macros

1.3 Offline-Process with MultiPage files

Allevo offers offline functions to create and save individual Excel files together with suitable reference data.

If these files are created in the MultiPage mode of the Allevo, a separate worksheet is automatically created in the Excel file for each relevant object. Unfortunately, Excel loses the original signature of the Allevo master when saving these files (although nothing has changed in the VBA coding for which the signature is actually issued). Such a file can no longer be opened under Excel with increased security settings.

This special case occurs, for example, if the Allevo-Master is called via the MultiPage transactions (such as /ALLEVO/KSM) and the created MultiPage file is to be saved with reference data (the same case is using the Allevo Offline functions with "Export for Offline Planning" in Allevo-Cockpit).

To overcome this problem, Allevo offers a special function for copying sheets. It is activated via the "CopyMultiSheet" option in the Allevo master (see Excel manual). However, this method cannot always be used: e.g. not if the satellite areas are created as structured tables.

As an alternative to "CopyMultiSheet", you can user a customer-specific signature (see chapter 3.2).

Note:	This requirement for the use of a customer-specific signature also only exists for the in-place mode. The ABC automatically transfers a signature to the saved Excel file when "Save as" is called up (no further settings are required)

1.4 Trusted locations

Excel also offers the possibility of setting up so-called "Trusted locations" in the Security Centre. For Allevo, two use cases can be distinguished:

ABC mode: Setting up a "Trusted Location" in Excel can be helpful when the Allevo-Master starts from the ABC document mode. Only in this case the file directory can be declared as a Trusted Location with the Allevo-Master.

Inplace mode: when calling the Allevo-Master from SAP via Inplace mode, Trusted locations are NOT an option.

Explanation: the in-place mode uses basic functions of the SAP Office Integration (DOI), in which all called Office documents are temporarily copied into a local directory. Therefore, there is no central location for the storage of a called Allevo master. No matter whether the master is stored in the BDS or via the Allevo file management. When Excel starts in Inplace mode, the associated file is always stored temporarily according to the Windows temp settings, but such a temp directory cannot be classified as trustworthy on the Excel side.

In in-place mode, assignment of a Trusted Publisher by signature is therefore the only option. SAP provides this for their applications that are based on functions of SAP Office Integration, e.g. when switching to Excel in GR55 reports or applications for ALV (see e.g. SAP Note 1992004 - Report Writer: Validity of digital signature in OI Excel templates expired).

2 KERN Certificate / Use signature in Allevo planning

If the security settings of Excel only allow restrictive work with macros, a digital signature must be stored in the Allevo Master. Otherwise, it is not possible to call the Allevo Master via Excel (see notes in the first chapter).

Note:	These requirements correspond to those that must also be observed in other SAP transactions when working with Excel inplace displays, for example, in the Report Writer (see, for example, SAP Note 1992004 for installing digital signatures when using Report Writer)

The following sections describe what to consider when installing and working with Allevo.

2.1 Signature in Allevo Master

In order to use the Allevo-Master with the macros, this master must be signed. This can be done via:

1. Signing of the Allevo-Master by Kern AG with a certificate from Kern AG. This certificate created with the certificate of DigiCert is trustworthy. In particular, it signs the VBA coding contained in the Allevo-Master.
   The public part of the certificate is delivered to the customer together with the signed Allevo Master.
2. Signing with the customer's certificate (how such a certificate can be generated is described as an example in the next chapter). In this case, the customer could also adjust the macros himself and then re-sign the master. The customer's own certificates can be used optionally without runtime limitation.

Official, trustworthy certificates (e.g. from DigiCert) always have a validity period, e.g. two years for the Kern AG certificate. Therefore, the signature in all relevant Allevo-Master files must be updated before the end of this period. The process is therefore comparable to signed templates that SAP delivers for ALV applications (see SAP Note 1686797) or Report Writer (see SAP Note1992004).

This maintenance of it may favor the use of a customer's own certificate (as described above as use case 2).

Note:	Certificates have to meet increasing security requirements and are accordingly further developed by the manufacturer (here DigiCert). Thus, from the end of 2015, the Kern AG certificate will also be available as SHA-256 Code Signing Certificate (as a replacement for the previously common SHA-1 certificate).

We will first describe the procedure for the application case (1). We describe now how to install the public part of the certificate in two ways.

2.2 Installing the KERN certificate (public key) at the workstation

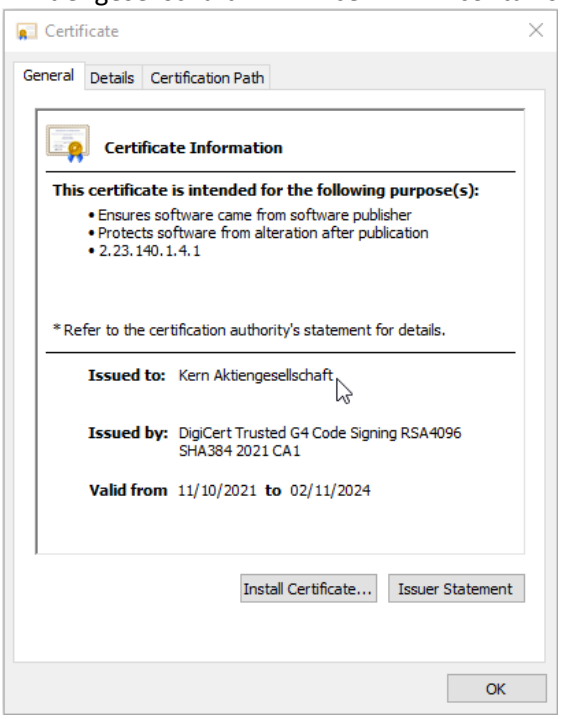
To ensure that the workbooks starts without a security warning, the Kern AG **public certificate** must be installed in the "Trusted Issuers" certificate store at the customer.

This certificate must be installed on all workstations where Allevo is used (controller and planner). The installation can be called up manually at each workstation; in network environments, the system administrator can of course roll out the certificate centrally.

Note:	Until 2015 the previous SHA-1 certificates were delivered under the name "KernAktiengesellschaftXXXX.cer" (again with XXXX as expiration year). The additionally delivered files "DigiCert Trusted Root G4.cer" and "DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1.cer" are only required in special cases (see section 5.2). In this case the installation could also be carried out using the programme "Kern Zertifikat Setup.msi", whereby all relevant steps described below for manual installation were carried out automatically.

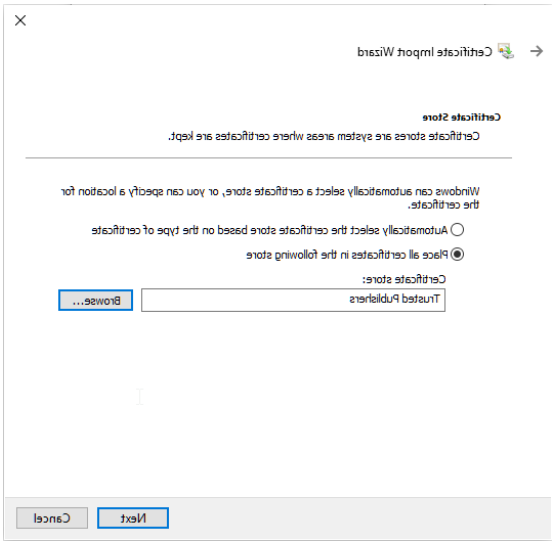
The manual installation at the workplace works as follows:

- Double click on file "**KernAgCodeSigning256_XXXX.cer**" (or "KernAgCodeSigning256_XXXX.cer" or "KernAktiengesellschaftXXXXXX.cer" contains information about the certificate)



Picture 2-1: Information about the KERN Certificate

- [Install Certificate...] leads to the Welcome dialog, which you confirm with [Next].
- Then select the certificate store: select [**Save all certificates to the following store**] and click [Browse].
- In the following list, select and accept "Trusted Publishers".



Picture 2-2: Kern certificate with store „Trusted Publisher“

- Select [Next], and in the next screen, select [Finish].
- Finally, appears the message "The import operation was successful“.

Kern AG is registered as a "trustworthy publisher". To display all installed certificates and publishers, see the notes in the appendix (section 5.2).

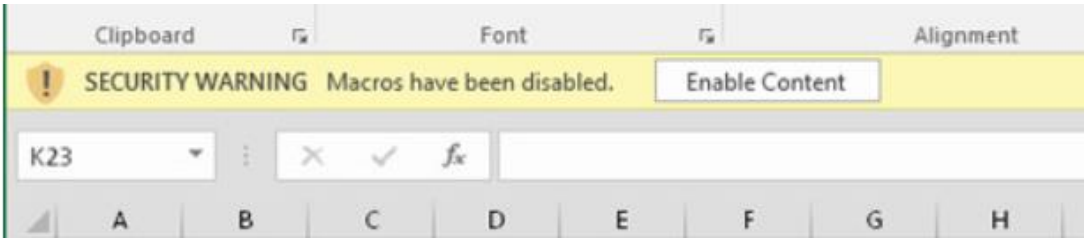
Alternatively, the certificate can also be installed directly via the signed Excel template (as an additional Excel function for macro warnings, which is described in the next section).

Note: If the certificate is installed in a different memory, an error message "the publisher of this certificate could not be found" will be displayed. In this case, please repeat the installation with the "Trusted publisher" memory.

2.3 Installation of public key via Excel security query

A public key can also be installed directly via a signed Excel master: as an alternative to the procedure described in the last section 2.2. This variant is a more complicated way, but can be useful if the key is to be stored directly at individual workstations.

If the Excel macro security is set to the second level ("Disable macros with notification"), the following security warning appears when a signed Allevo-Master starts:



Picture 2-3: Excel security warning for XLSM file with macros and signature

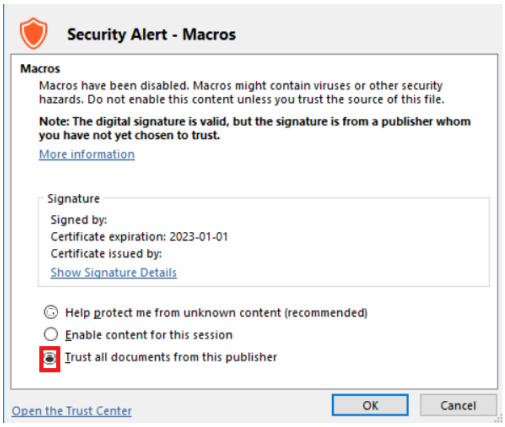
This message appears every time an Excel file opens as long as the public part of the corresponding certificate is not installed on the local computer.

The following steps are necessary to avoid notification:

- Click on "Macros have been disabled”

- Select "Advanced options" under "Enable content”

- Trust all documents from this publisher



- Finish with OK

After these steps, the public part of the certificate is installed in the Trusted Issuers store. The next time you open the Excel file, the security warning from above should no longer appear.

3 Allevo Allevo with customer's own certificate

3.1 Overview / background

In some cases, it may be good to use a customer's own certificate instead of the KERN certificate described in the previous section.

Differences:

- When the VBA code is adjust, the Allevo Master is signed via an in-house standard process (e.g. by the same department that is responsible for other Excel applications). If necessary, even an already existing certificate is used.
- The DigiCert KERN certificate must be updated every 2 years; other providers may have different periods.

If the Allevo module is used for offline planning together with a so-called MultiPage master, an in-house signature must be used due to the Microsoft system (see following chapter).

In the following steps, the handling Allevo and customer's own certificate is explained by way of example.

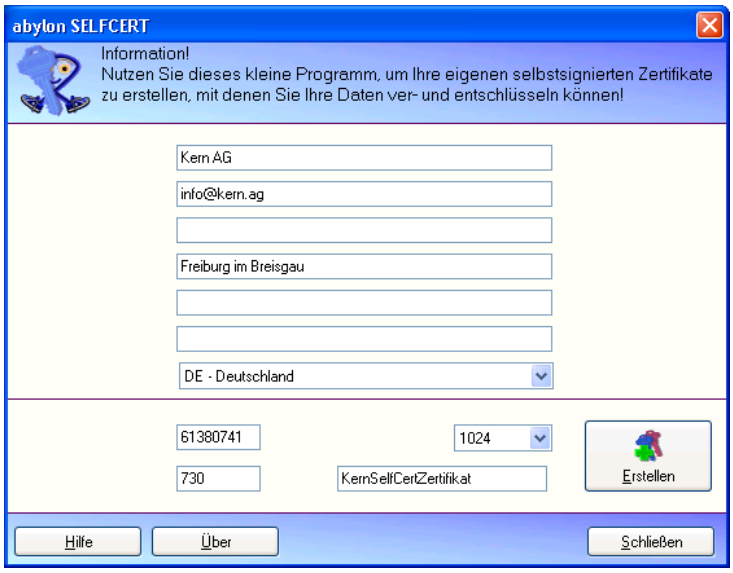
3.2 Creating your own certificate

The Kern AG certificate was created with a root certificate from DigiCert for signing VBA Coding: the "Extended Key Usage" (EKU) is set to "codeSigning" (OID: 1.3.6.1.5.5.7.3.3).

When purchasing a company-owned certificate, make sure that it is intended for signing VBA.

For in-house use, however, a root certificate is not necessarily required. Instead, the programme "Abylon SelfCert" can be used to create a certificate (download from http://www.abylonsoft.de/selfcert). Thereby a certificate is generated, which is intended for VBA coding from the outset. The necessary steps:

- "Abylon SelfCert" is a Windows application, which can be obtained by download from the homepage of the manufacturer.
- After installation and start of the application, the required company-specific information is entered:



Picture 3-1: Company specific information about the customer certificate

- The [Create] button prompts you to enter a password
- In the next step the private key of the certificate is stored in a PFX file.
- By confirming the following dialogue with "Yes", you will automatically be guided to the installation of the key on the local computer.
  However, this installation can also be started by double clicking on the PFX file (as described below)-

Note:	We have just described the procedure using "Abylon SelfCert": if Allevo-MultiPage files are only created on a single workstation, you can alternatively use the program "Selfcert.exe", which is included in the installation package of Microsoft Office.

3.3 Installing (and removing) the private key

The private key of the certificate stored in the PFX file must be installed on all workstations where Allevo workbooks for multi-planning are created (normally the controller workstation).

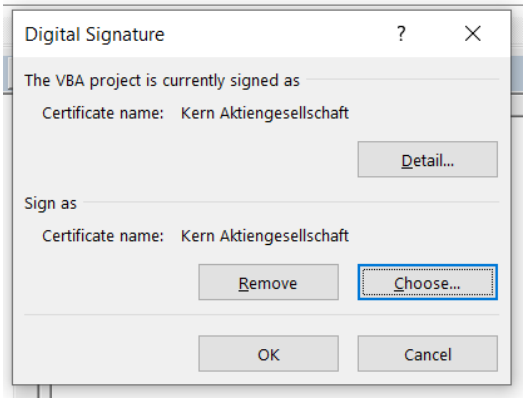
- Double-click on the PFX file and confirm Welcome with [Next].
- Confirm the PFX file with [Next].
- Enter the password defined when creating the certificate.
- The certificate store can be selected automatically with [Next] or manually with [Save all certificates in the following store] and [Browse] in "Own certificates".
- After [Finish] and the success message, the certificate is installed and documents can be signed.
- Now the sentence "You have a private key for this certificate" must appear at the very bottom of the certificate properties, tab General

To remove a private key, program certmgr.msc can be helpful: the installed keys can be found under "Own certificates >> Certificates" (if necessary delete the relevant entry via context menu).

3.4 Signing Allevo Master

On a computer where the certificate private key is installed, all Allevo Masters are now signed. This is done as follows:

- Open the XLSM - Master by double-clicking it.
- Start the VBA Editor by pressing the Alt and F11 keys simultaneously.
- Select the VBA project belonging to the master in the list on the left side of the VBA Editor.
- Menu Extras>Digital signature... opens



Picture 3-2: Digital signature in Allevo Master

- Press [Remove] to remove the core signature if necessary
- Press [Choose] to select your own certificate and press OK to confirm
- Confirm with OK and save the master.

- Include the master via the SAP transactions OAOR or via file management (see Allevo manual)

Based on this Allevo-Master, the MultiPage planning files for the Allevo-Offline planning can now be generated. In each Excel planning file, which is now created and saved using Allevo functions, **the signature is also retained**.

3.5 Generating the public key

The public key is generated on the same computer on which the private key of the certificate has been installed. This is done as follows:

- In Windows Start>Run, enter the command CertMgr.msc
- In the certificate tree Certificates>Own Certificates>Select Certificates
- elect the previously created certificate and start the export via Menu>Action>All tasks>Export...
- With Next > Next > Continue, enter the file name and finish saving the public key of the certificate in a CER file.

3.6 Installing the public key

The public key must now be installed on all workstations where Allevo is called. The installation must be done in two stores: as "Trusted Root Certification Authorities" and "Trusted Publishers“

- On the computer on which the certificate is to be installed, right-click on the CER file previously created and select "Install Certificate.
- Welcome confirm with [Next].
- Select "Trusted Root Certification Authorities" as the certificate store using [Save all certificates in the following store] and [Browse].
- Continue and Finish.
- It must now be confirmed that a certificate without a root certificate is to be trusted.
- Right-click on the CER file again and select "Install Certificate" to start the installation.
- Welcome confirm with [Next].
- Select "Trusted Issuers" as the certificate store with [Save all certificates in the following store] and [Browse].
- Continue and Finish.

Afterwards, all Allevo Excel files created with a self-signed multi - or single - master should be accessible without a security prompt.

4 Special case: Allevo MultiPage functions in offline mode

4.1 Background of the MultiPage Planning

Allevo offers offline functions where individual Excel files are created and saved together with matching reference data. If these files are created in the so-called "MultiPage mode" of Allevo, a separate worksheet is automatically created for each relevant object in the exported Excel folder. Due to Microsoft functionalities, the original signature of the Allevo-Master is unfortunately lost when saving these files (although the VBA coding for which the signature is actually issued has not changed).

To overcome this problem, Allevo offers a special function for copying sheets. It is activated via the "CopyMultiSheet" option in the Allevo master (see Excel manual). However, this method cannot always be used: e.g. not if the satellite areas are created as Structured Tables or if high performance is required.

In order to be able to work comfortably with Allevo in this case, a customer-specific signature can be used (with public and private key): if the corresponding private key is installed on the workstation where the offline file is saved, the signature is also preserved for MultiPage documents.

The necessary steps are described below.

Note:	The requirement to use a customer-specific signature together with MultiPage offline files only exists for the in-place mode. The ABC mode automatically transfers a signature to the saved Excel file when "Save as" is called up (no further settings are required)

4.2 Workstation for generating the offline files

A customised certificate for Microsoft Office VBA coding is required at workstations for creating offline workbooks in Allevo MultiPage mode.

Procedure:

- If such a certificate does not yet exist at the customer's premises, it should be issued as described in section 3.2 above (but its use should always be coordinated with the in-house IT department).
- The private key of the certificate stored in the PFX file must be installed on all workstations on which Excel workbooks for offline MultiPage planning are created (normally the workstation of the controller). See section 3.3 above.

The Allevo masters used must be signed as described in section 3.4. These signatures are then no longer lost when offline MultiPage files are created.

4.3 Workstations for MultiPage planning

In order to now plan with the created Excel files, the public key of the previously created certificate must be installed on the workstations used. Afterwards, all Excel files created with a self-signed multi or single master should be accessible without a security prompt.

The installation is described in section 3.6 above.

5 Appendix

5.1 Rolling out the Group Policy certificate

Certificates are important login information. Administrators may not want users to be able to decide for themselves, which certificates are trusted and which are not.

In such cases, the decision as to whether or not to trust a particular certificate is made by administrators or persons who are familiar with that certificate and its implications for the organisation.

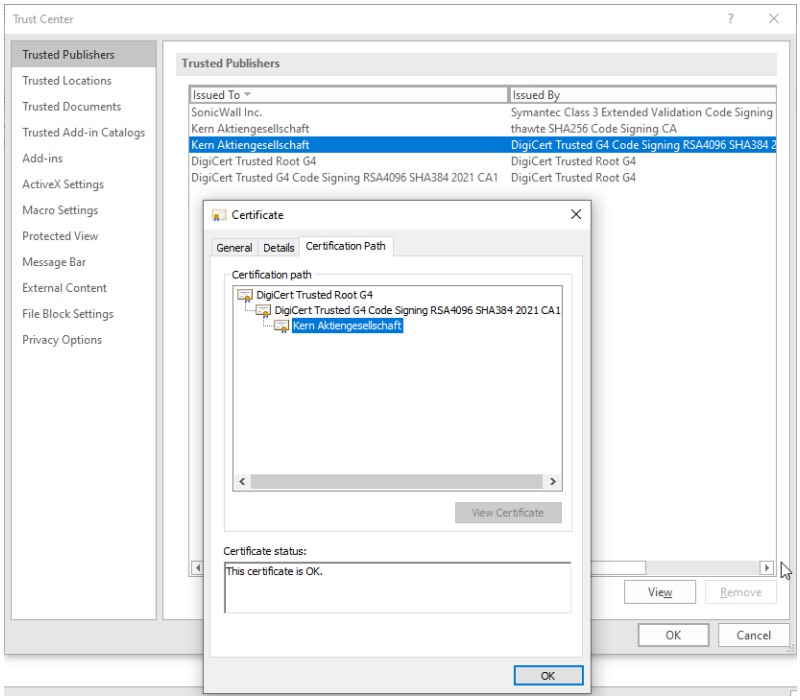
The certificate is then also distributed on the administrator's initiative using group policies. For further details see:

http://technet.microsoft.com/de-de/library/cc772491%28WS.10%29.aspx

5.2 Displaying or removing installed certificate

With program **certmgr.msc** you can view the installed certificates on the local computer. Execute via START > RUN on Windows PC.

Alternatively, you can also make the display via the Excel Security Centre; select "Trusted Publishers" there“.



Picture 5-1: View or remove installed certificates

Individual certificates can also be removed here. In the detailed data for the certificate, pay particular attention to the certification path, which should look like the one shown in the figure above.

Note: If the main branch "DigiCert Trusted Root G4" is missing, "DigiCert Trusted Root G4.cer" must be installed first, but here with the option "Select certificate store automatically". If the branch "DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1“ below "DigiCert Trusted Root G4" is missing in the certification path to "Kern Aktiongesellschaft", please additionally install the file "DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1.cer"; (again with the option "Select certificate store automatically"). Afterwards the path should be completely visible.

5.3 Do not use Excel 4.0 Macros

If Excel 4.0 macros are included in xls or xlsm, the security question may be displayed even for signed documents. In this case, the macros should be removed and replaced with current functions.

Excel 4.0 macros are e.g. CELL and FILES. These can be contained in formulas e.g. in named areas. In formula in the spreadsheet these functions do not present a problem.

A complete list of critical macros could not be created so far. Here there is a list: https://d13ot9o61jdzpp.cloudfront.net/files/Excel%204.0%20Macro%20Functions%20Reference.pdf

Note: if such macros are used in the master, the signature is lost when the master is called up. Normally you can recognize this by the fact that the Allevo-Ribbon does not appear anymore or the security warning (as shown in the following chapter).