Introduction to Digital Certificates

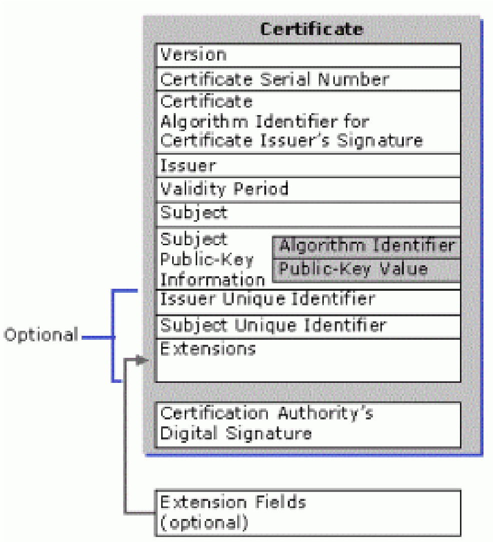
What is a digital certificate?

A digital signature or ID is more commonly known as a digital certificate. To digitally sign an Office document, you must have a current (not expired) digital certificate. Digital certificates are typically issued by a certificate authority (CA), which is a trusted third-party entity that issues digital certificates for use by other parties. There are many commercial third-party certificate authorities from which you can either purchase a digital certificate or obtain a free digital certificate. Many institutions, governments, and corporations can also issue their own certificates.

A digital certificate is necessary for a digital signature because it provides the public key that can be used to validate the private key that is associated with a digital signature. Digital certificates make it possible for digital signatures to be used as a way to authenticate digital information.

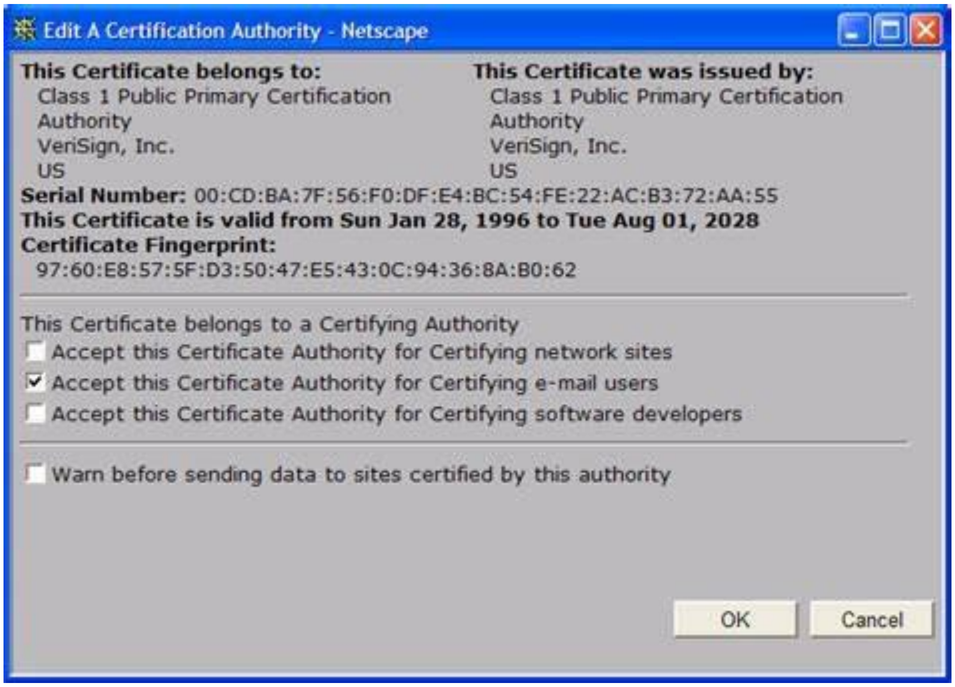
Digital certificates function similarly to identification cards such as passports and drivers' licenses. Digital certificates are issued by recognized (government) authorities. When someone requests a certificate, the authority verifies the identity of the requester, certifies that the requester meets all requirements to receive the certificate, and then issues it. When a digital certificate is presented to others, they can verify the identity of its owner because the certificate provides the following security benefits:

- It contains personal information to help identify and trace the owner.
- It contains the information that is required to identify and contact the issuing authority.
- It is designed to be tamper-resistant and difficult to counterfeit.
- It is issued by an authority that can revoke the identification card at any time (for example, if the card is misused or stolen).
- It can be checked for revocation by contacting the issuing authority.


Certificate
Version
Certificate Serial Number
Certificate Algorithm Identifier for Certificate Issuer's Signature
Issuer
Validity Period
Subject
Subject Public-Key Information
Algorithm Identifier
Public-Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Optional
Certification Authority's Digital Signature
Extension Fields (optional)

A digital certificate is necessary for a digital signature because it provides the public key that can be used to validate the private key that is associated with a digital signature. Digital certificates make it possible for digital signatures to be used as a way to authenticate digital information.

Example of a Digital Certificate



This Certificate belongs to:
Class 1 Public Primary Certification Authority
VeriSign, Inc.
US

This Certificate was issued by:
Class 1 Public Primary Certification Authority
VeriSign, Inc.
US

Serial Number: 00:CD:BA:7F:56:F0:DF:E4:BC:54:FE:22:AC:B3:72:AA:55
This Certificate is valid from Sun Jan 28, 1996 to Tue Aug 01, 2028
Certificate Fingerprint:
97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62

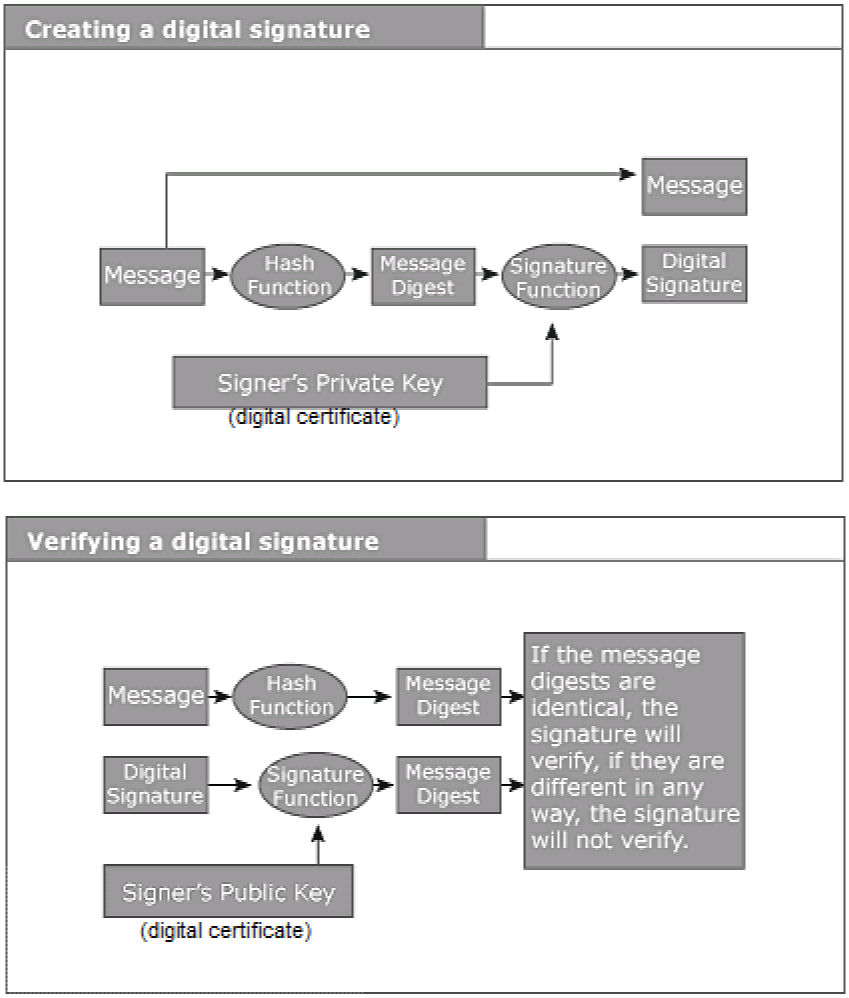
This Certificate belongs to a Certifying Authority
□ Accept this Certificate Authority for Certifying network sites
☑ Accept this Certificate Authority for Certifying e-mail users
□ Accept this Certificate Authority for Certifying software developers

□ Warn before sending data to sites certified by this authority

The use of a digital certificate to sign documents

When the signer uses a certificate to digitally sign a document, other people (known as relying parties) can trust the digital signature because they trust the CA has done their part to ensure the signer matches their digital identity.

So, technically speaking the difference between a digital signature and digital certificate is that a certificate binds a digital signature to an entity, whereas a digital signature is to ensure that a data/information remain secure from the point it was issued. In other words: digital certificates are used to verify the trustworthiness of a person (sender), while digital signatures are used to verify the trustworthiness of the data being sent.



Creating a digital signature using digital certificates (private key)

The difference between a digital signature and digital certificate

Digital business with digital *trustA* digital signature and a digital certificate, while both security measures, are different in the ways they are implemented and the background why they are implemented for. The technology industry loves to use acronyms and words that seem to either overlap with other similar words, or that are a slight variation on a word, but with widely different meanings. To understand more, these are the comparison Between Digital Signature vs Digital Certificate (Infographics)

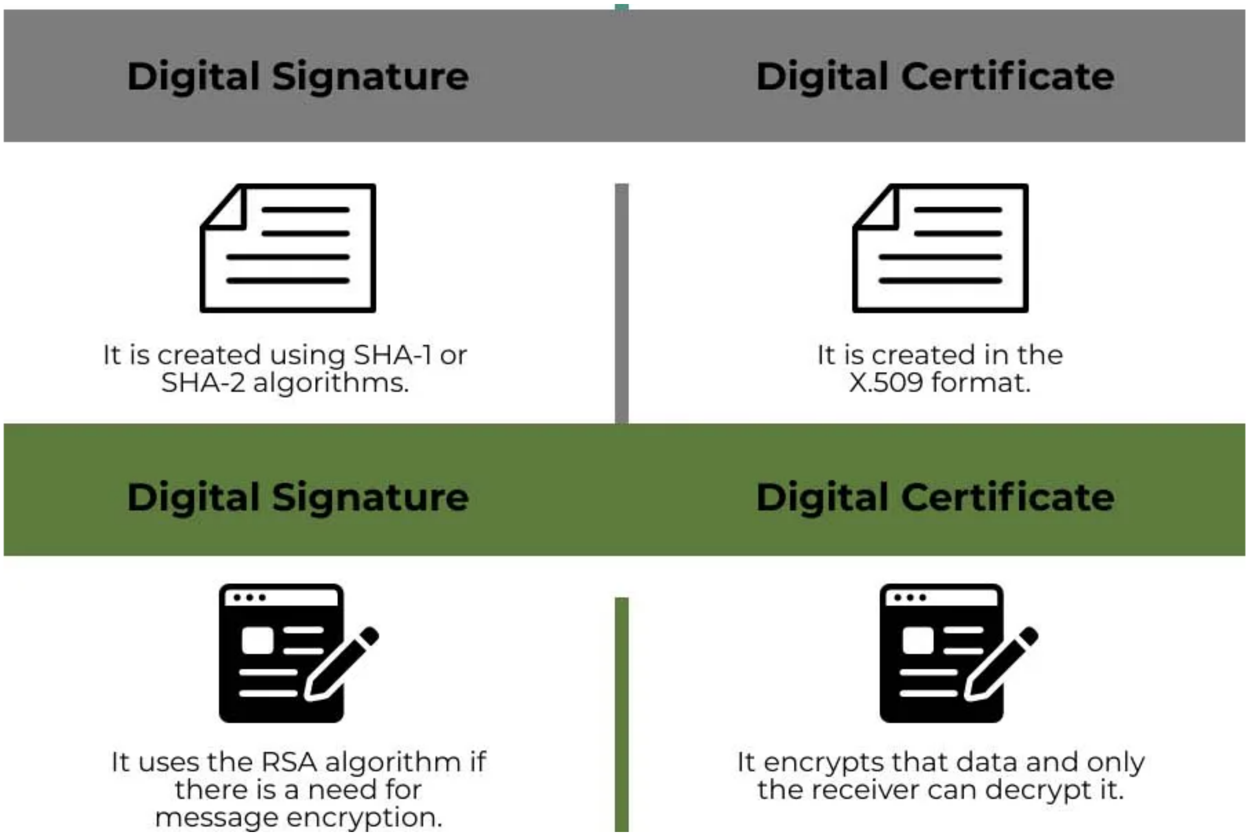
Digital Signature	Digital Certificate
It verifies the identity of the document.	It verifies the identity of the ownership of an online medium.
Digital Signature	**Digital Certificate**
It is issued to a specific individual by an authorized agency.	It is issued after the background check of the applicant by the Certificate Authority(CA).
Digital Signature	**Digital Certificate**
It ensures that the signer cannot non-repudiate the signed document.	It ensures that two parties who are exchanging the information are secured.
Digital Signature	**Digital Certificate**
It works on DSS (Digital Signature Standard).	It works on the principles of public-key cryptography standards.

Digital Signature	Digital Certificate
The digital signature uses a mathematical function (Hashing function).	It contains personal information to help in identifying the trace of the owner.

Digital Signature	Digital Certificate
It is widely used for avoiding forging the document.	It is used in an online transaction for the trustworthiness of the data and the sender.

Digital Signature	Digital Certificate
It is an attachment to a document that can be viewed as a signature.	It is a medium to prove the holder's identity for a particular transaction.

Digital Signature	Digital Certificate
It ensures the sender and the receiver have the same document containing the same data.	It builds the trust between the user and the business (Certificate holder).



Digital Signature

Digital Certificate

It is created using SHA-1 or SHA-2 algorithms.

It is created in the X.509 format.

Digital Signature

Digital Certificate

It uses the RSA algorithm if there is a need for message encryption.

It encrypts that data and only the receiver can decrypt it.

Key Difference Between Digital Signature vs Digital Certificate

Let us discuss some of the major key differences between Digital Signature and Digital Certificate:

- The digital signature is used to identify the owner of the document whereas the digital certificate is a document that identifies the identity of the organization.
- The digital signature is signed created by the signer's private key and verified by the public key of a signer whereas digital certificate is issued by a third party and an end-user can check its validity and authenticity.
- The digital signature uses a mathematical function (Hashing function) wherein a Digital certificate contains personal information to help in identifying the trace of the owner.
- A digital signature is created using DSS (Digital Signature Standard) whereas digital certificate works on the principles of public-key cryptography standards.
- A digital signature uses the RSA algorithm when there is a need for message encryption whereas digital certificate is proof that the data transmission will be on the secured layer and in an encrypted way.
- Digital signatures are used to validate the sent data whereas digital certificates are used to validate the identity of the sender.
- With a digital certificate, an end user may have a relationship with the sender whereas in the digital certificate the end user trusts the third party and does not have a relationship with the business owner or the entity.

Digital Signature vs Digital Certificate Comparison Table

Let’s discuss the top comparison between Digital Signature vs Digital Certificate:

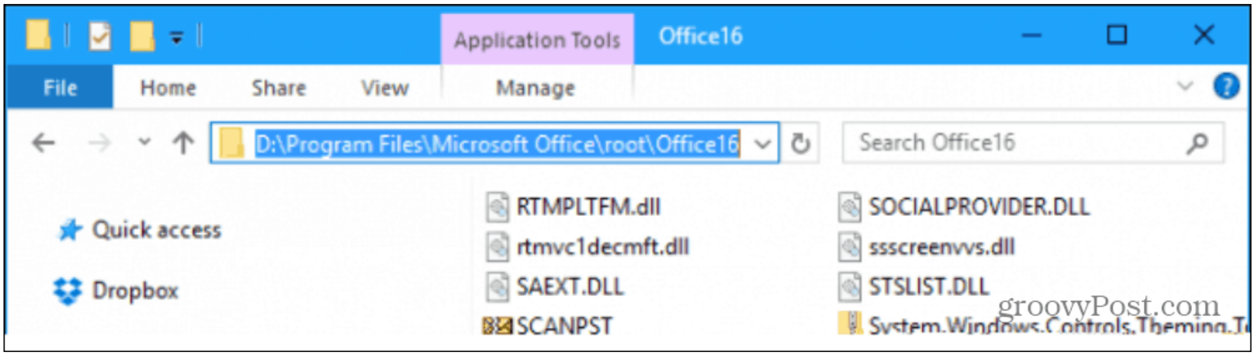
Digital Signature	Digital Certificate
It verifies the identity of the document.	It verifies the identity of the ownership of an online medium.
It is issued to a specific individual by an authorized agency.	It is issued after the background check of the applicant by the Certificate Authority(CA).
It ensures that the signer cannot non-repudiate the signed document.	It ensures that two parties who are exchanging the information are secured.
It works on DSS (Digital Signature Standard)	It works on the principles of public-key cryptography standards.
The digital signature uses a mathematical function (Hashing function).	It contains personal information to help in identifying the trace of the owner.
It is widely used for avoiding forging the document.	It is used in an online transaction for the trustworthiness of the data and the sender.
It is an attachment to a document that can be viewed as a signature.	It is a medium to prove the holder’s identity for a particular transaction.
It ensures the sender and the receiver have the same document containing the same data.	It builds the trust between the user and the business (Certificate holder).
It is created using SHA-1 or SHA-2 algorithms.	It is created in the X.509 format.
It uses the RSA algorithm if there is a need for message encryption.	It encrypts that data and only the receiver can decrypt it.

How to Create a Self-Signed Digital Certificate in Microsoft Office 2016

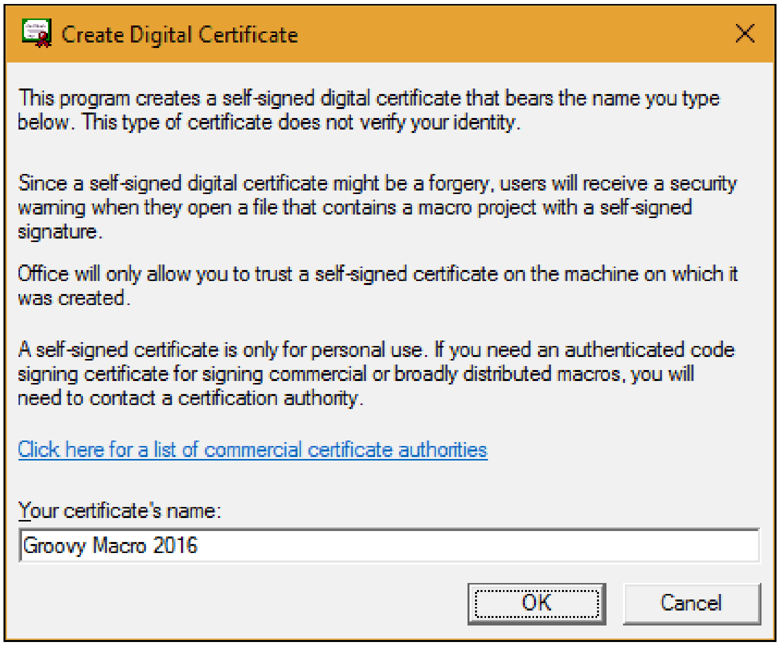
One of the most compelling parts of the Microsoft Office productivity suite for power users is automating functionality using Visual Basic for Application code. Applications such as Word, Excel, and Outlook can be used to create Macros. Macros are small bits of programming code used for performing repetitive tasks. In versions of Office before 2007, VBA support was notorious for being exploited. Since then, Microsoft has enhanced the security within the suite, limiting the impact of rogue code causing potential damage.

Setup Self-Signed Digital Certificate in Office 2016 Applications

The Digital Certificate for VBA Projects can now be found within **Program Files > Microsoft Office > root > Office16**.



Double click the SELFCERT file, enter a name for your Digital Certificate, then click OK.


Create Digital Certificate

This program creates a self-signed digital certificate that bears the name you type below. This type of certificate does not verify your identity.

Since a self-signed digital certificate might be a forgery, users will receive a security warning when they open a file that contains a macro project with a self-signed signature.

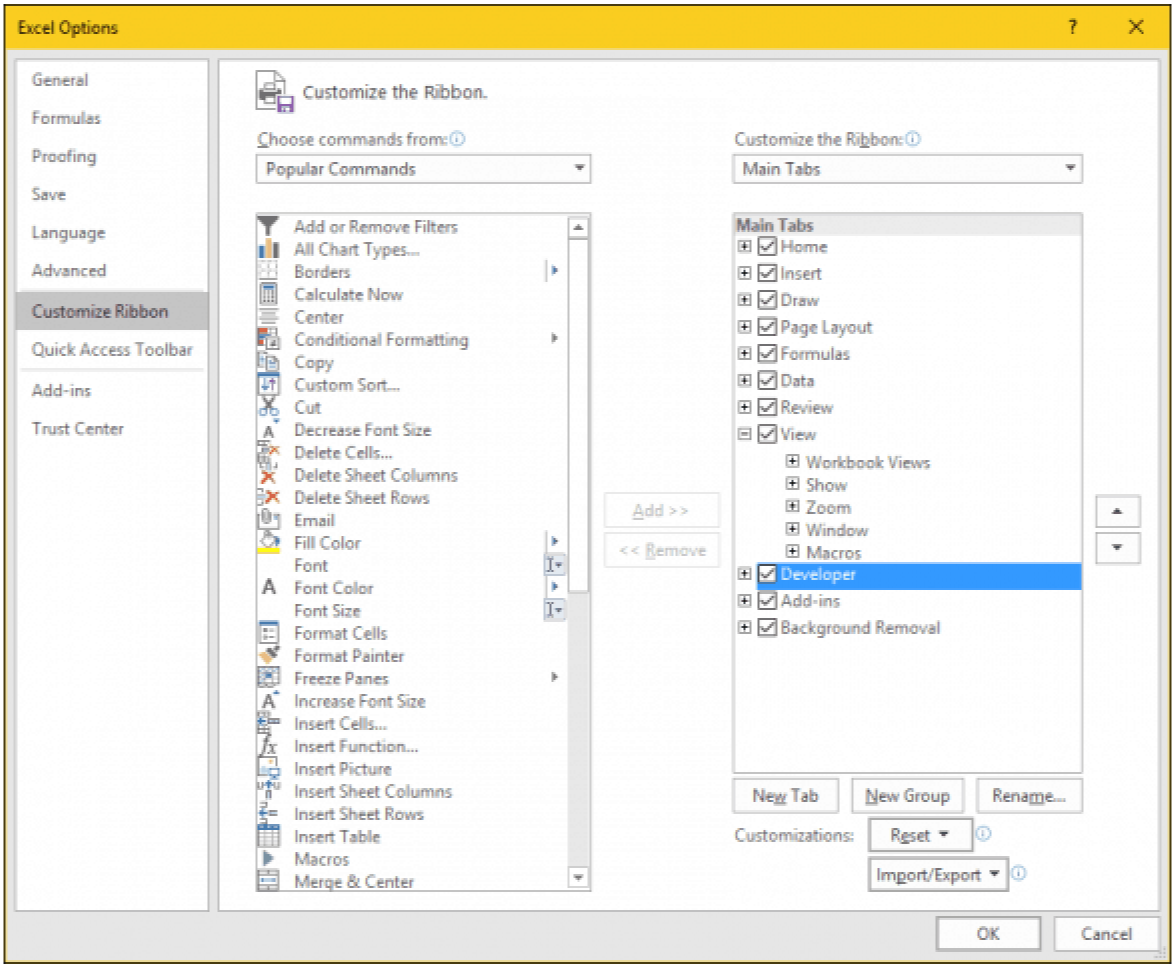
Office will only allow you to trust a self-signed certificate on the machine on which it was created.

A self-signed certificate is only for personal use. If you need an authenticated code signing certificate for signing commercial or broadly distributed macros, you will need to contact a certification authority.

Click here for a list of commercial certificate authorities

Your certificate's name: Groovy Macro 2016

Launch any of the Office applications you would like to use the digital certificate in. For this article, I am going to use Excel. The first thing you will need to do is enable the *Developer* tab. Click File > Options > Customize Ribbon > check the box *Developer* then click OK.



Excel Options

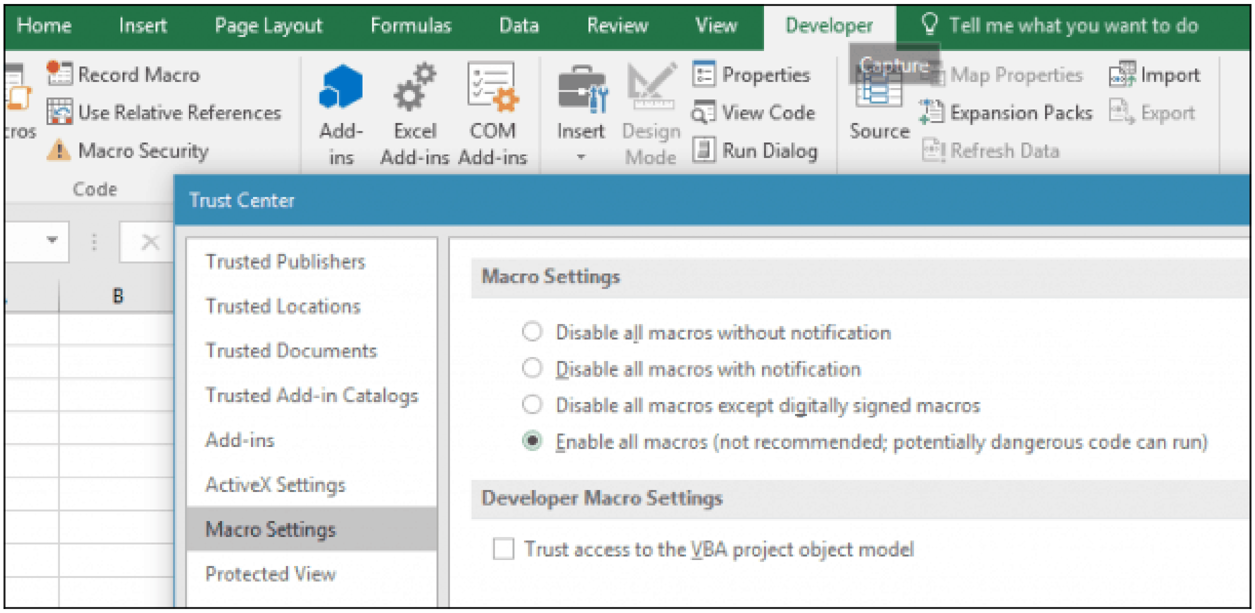
Customize the Ribbon.

Choose commands from: Popular Commands

Customize the Ribbon: Main Tabs

Main Tabs
- ☑ Home
- ☑ Insert
- ☑ Draw
- ☑ Page Layout
- ☑ Formulas
- ☑ Data
- ☑ Review
- ☑ View
  - Workbook Views
  - Show
  - Zoom
  - Window
  - Macros
- ☑ Developer
- ☑ Add-ins
- ☑ Background Removal

Select the Developer tab, then click the *Macro Security* button within the *Code* group, select the *Enable all Macros* radio box, then click *OK*.



Trust Center

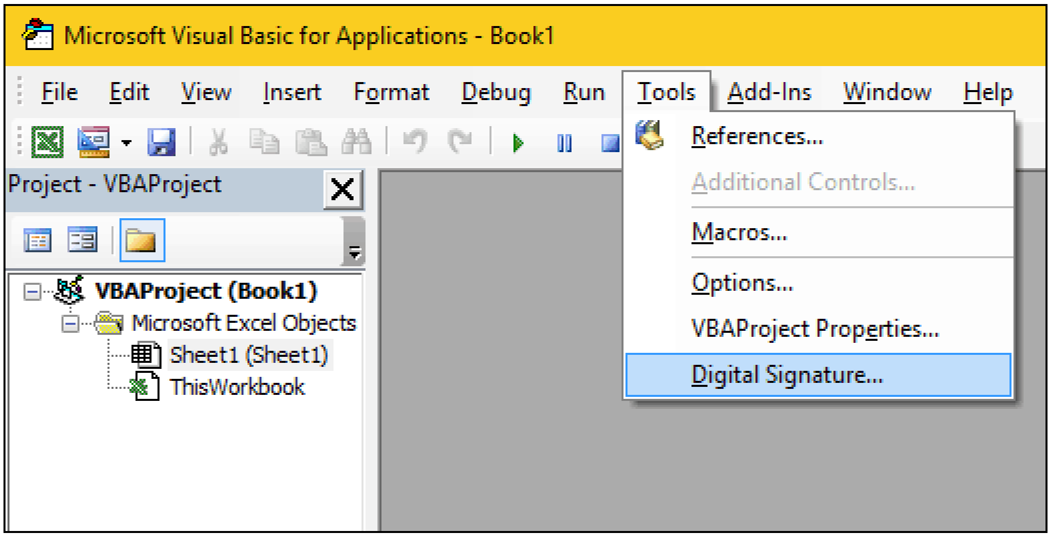
Macro Settings

○ Disable all macros without notification
○ Disable all macros with notification
○ Disable all macros except digitally signed macros
● Enable all macros (not recommended; potentially dangerous code can run)

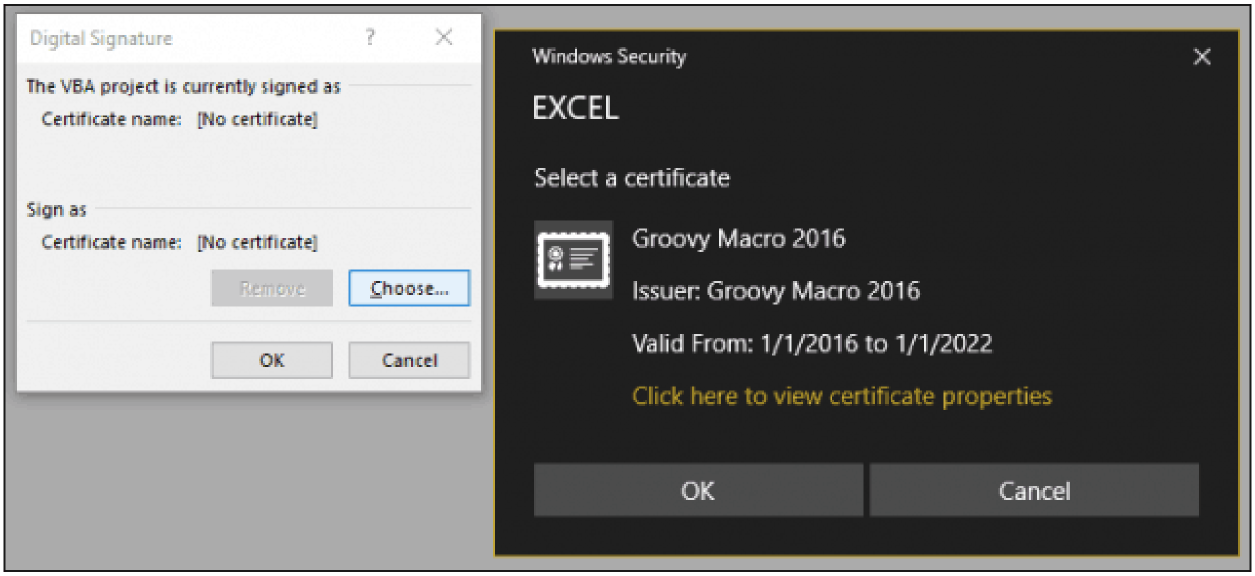
Developer Macro Settings

□ Trust access to the VBA project object model

Within the *Code* group, click *Visual Basic*. The Visual Basic for Applications component will be launched. Next, click Tools, then click Digital Signature.



Click Choose, the recently created digital certificate will be presented. Click OK, then proceed to save your project.



The VBA project is currently signed as

Certificate name: [No certificate]

Sign as

Certificate name: [No certificate]

EXCEL

Select a certificate

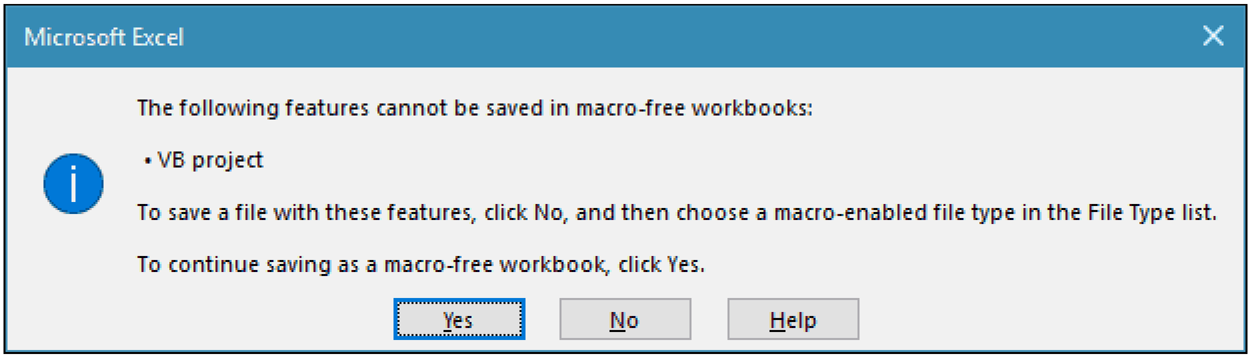
Groovy Macro 2016

Issuer: Groovy Macro 2016

Valid From: 1/1/2016 to 1/1/2022

Ensuring your Macros Work

I noted earlier; Microsoft has made security changes to how Macros work in Office applications over the years. Saving your Macro’s is not allowed in a standard workbook or document.



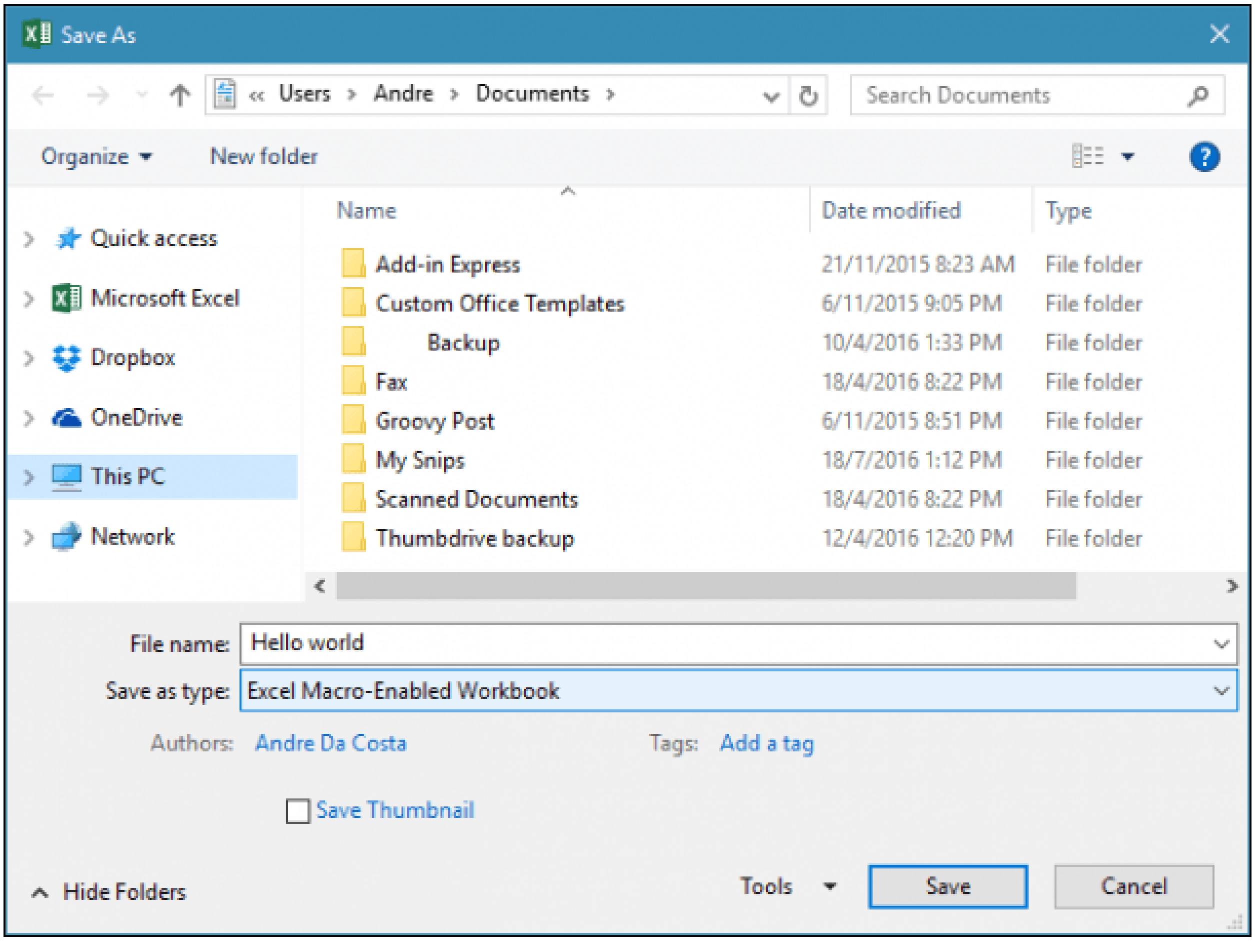
The following features cannot be saved in macro-free workbooks:

- VB project

To save a file with these features, click No, and then choose a macro-enabled file type in the File Type list.

To continue saving as a macro-free workbook, click Yes.

Instead, users must correctly choose Macro-Enabled as the file type when saving.



Name	Date modified	Type
Add-in Express	21/11/2015 8:23 AM	File folder
Custom Office Templates	6/11/2015 9:05 PM	File folder
Backup	10/4/2016 1:33 PM	File folder
Fax	18/4/2016 8:22 PM	File folder
Groovy Post	6/11/2015 8:51 PM	File folder
My Snips	18/7/2016 1:12 PM	File folder
Scanned Documents	18/4/2016 8:22 PM	File folder
Thumbdrive backup	12/4/2016 12:20 PM	File folder

File name: Hello world

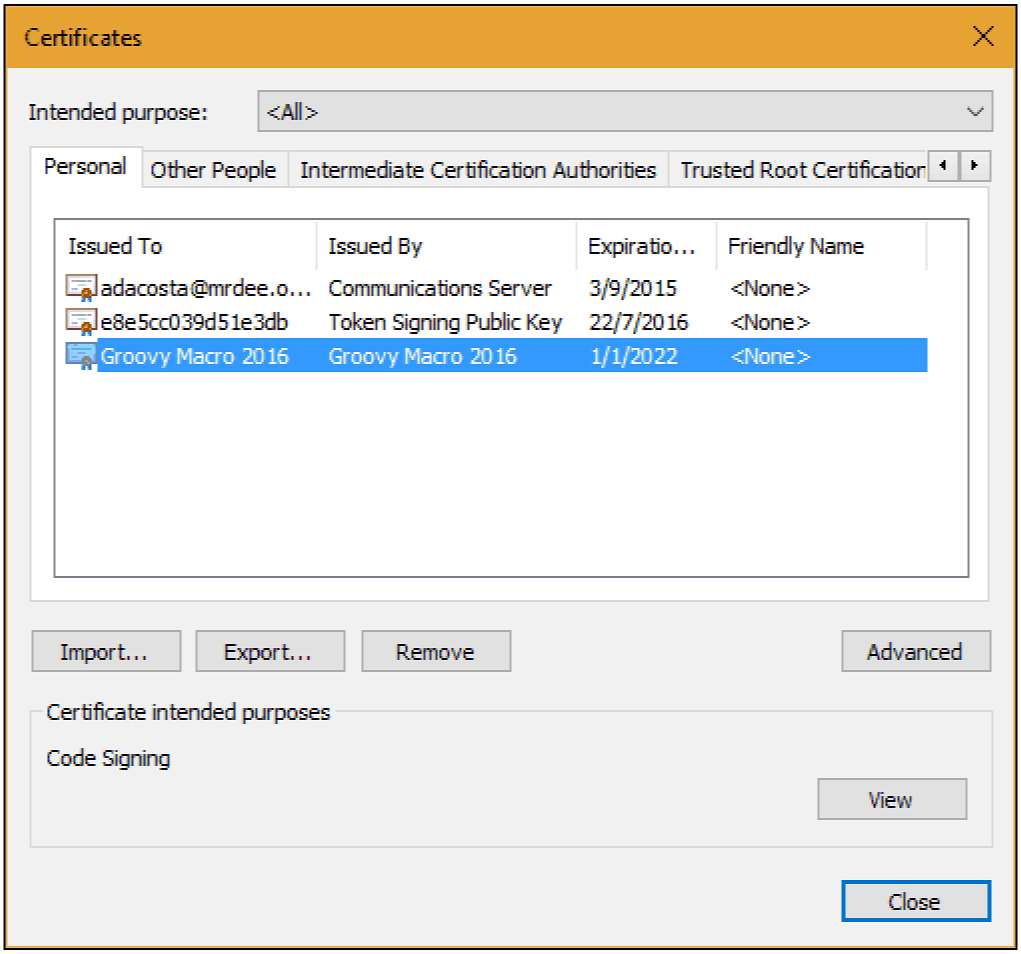
Save as type: Excel Macro-Enabled Workbook

Authors: Andre Da Costa

Tags: Add a tag

□ Save Thumbnail

Users can manage their signed certificate by using launching Internet Options. First, click Start, then **type:** *internet options*, hit Enter on your keyboard, select the *Content* tab, then click *Manage Certificates*. Here you have the choice of deleting or exporting your certificate for use on another computer.



Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
adacosta@mrdee.o...	Communications Server	3/9/2015	<None>
e8e5cc039d51e3db	Token Signing Public Key	22/7/2016	<None>
Groovy Macro 2016	Groovy Macro 2016	1/1/2022	<None>

Certificate intended purposes

Code Signing

Sources:

How to Create a Self-Signed Digital Certificate in Microsoft Office 2016 (groovypost.com)

What is Digital Certificate? | A Technology Overview from Comodo

PowerPoint Presentation (globalsign.com)

What is a Digital Signature? (techtarget.com)

What Is a Digital Signature (and How Does it Work) | Signaturely

The difference between a digital signature and digital certificate » AET Europe