DIGITAL SIGNATURE MANUAL

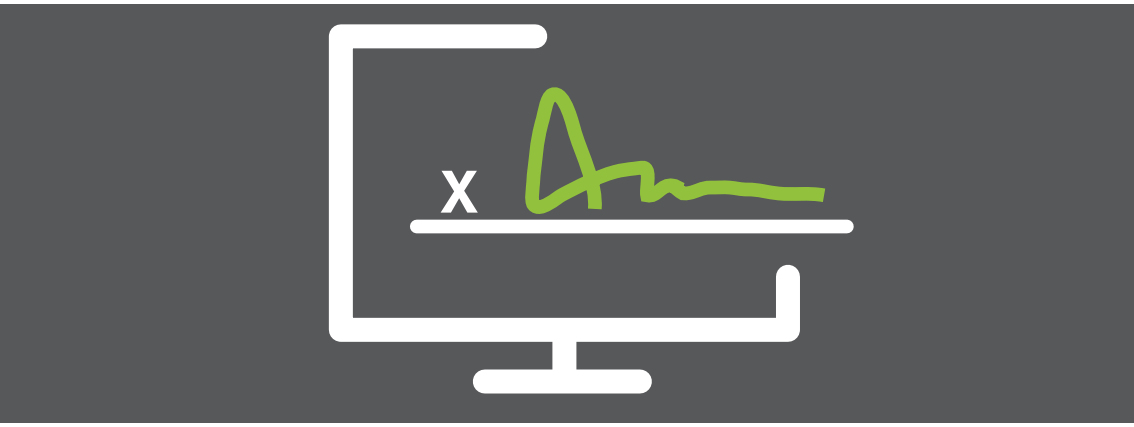
Investor Service Center
مركز خدمات المستثمرين

3 Salah Salem Street, Nasr City, Cairo, Egypt
Call Center: 16035
investment@miic.gov.eg
www.miic.gov.eg
MIICEgypt


ISC
Investor
Service Center
مركز خدمات المستثمرين

Table of Contents

What is a Digital Signature?



A digital signature is a convenient, time-saving, and secure way of signing electronic documents for transactions, contracts, images, official documents, etc. may be digitally signed and sent in seconds.

Digital signatures are created using two separate keys - one is private, and the other is public. The private key is used by the signatory to sign the document, which is encrypted and stored in the document. Any user that accesses the document thereafter can view the signature using the public key.

For the first time in Egypt, the Ministry of Investment and International Cooperation is pioneering this technology in the public sector in an effort to improve business transactions between government entities as well as the private sector.

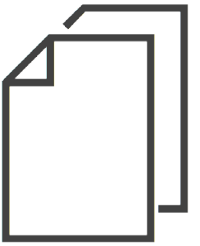
Required Documents

In order to apply for a digital signature, you will need to have the following:

National identification card, or passport for non-Egyptians

Application fee of 700 EGP

Additionally, there is the option to include your job title and company in your digital signature. To do so, please also bring the following documents:



- Copy of the company's commercial register
- Copy of the company's tax ID card
- Copy of the company's commercial license
- Copy of the company contract and it's legal form
- A signed and stamped HR letter

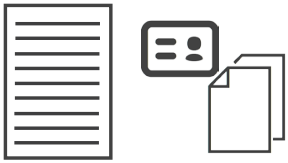
How to Apply

To apply for the digital signature, bring the required documents to the third floor of the Investment Service Center.

1.

Select a queue number and head to the Digital Signature counter to fill out the application form

2.

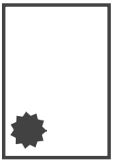


Submit the completed form along with your identification documents to the operator

3.

The operator will process your application form. After confirming your personal details, please sign.

4.



After paying the fees, the operator will hand you your token and certificate once it has been issued

Upon certificate issuance you shall receive the following:

- A Hardware Token
- A Sealed Pin Number Slip
- An Original Copy of Digital Signature Contract
- A CD with the Installation Software and Guide

Certificate Installation

The first step to utilizing your digital signature is to install the root certificates.

The root certificates are issued by the certificate authority (CA).

To download and install the root certificate, kindly refer to either one of the following websites:

Egypt Trust
https://www.egypttrust.com/download

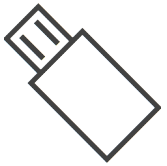
MCDR
http://www.mcdr-ca.com/Download.aspx

And select the required certificate to download.

User Manual

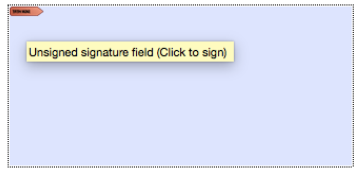
Once you have installed the certificates, follow the instructions below to sign your official documents electronically.

1.



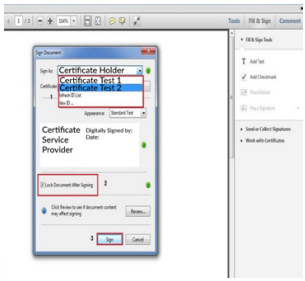
Insert your token in a USB port on your computer.

2.



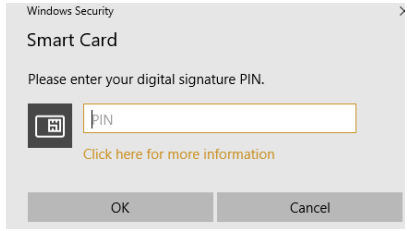
Open the PDF document and click on the empty box designated for your signature.

3.



Click on “Sign as” and choose your certificate. Then click “sign”.

4.



Enter your pin code in the box then click OK.

5.

Now the document is digitally signed.

Revocation Process

Your digital signature token is in a sense as crucial and as important as your National ID card & your Bank ATM card. In the event of losing, misplacing, or damaging your digital signature token, you must notify your Certificate Service Provider (CSP).

1.

Contact your service provider
Egypt Trust: 22668856 or 22665855
MCDR: 25971666

2.

The operator will ask a few questions to verify your identity and revoke your digital signature certificate.

3.

The revoked certificate will be published on the certification revocation list (CRL) online.

Frequently Asked Questions

What is a digital signature?

A digital signature is a convenient, time-saving, and secure way of signing electronic documents.

What is an electronic document?

An electronic document is any document that is generated or stored on a computer, such as a letter, a contract, or a will. In addition, an electronic document can be an image, such as a blueprint, a survey plat, a drawing, or even a photograph. A digital signature can be used to sign these documents.

Does that mean that the authenticity of any electronic document can be verified by a digital signature?

Yes, the verfication will provide and ensure the following:
- Authentication and nonrepudiation
- Certificate path
- Validity of the certificate
- That the signed content has not been altered

What is it like to sign an electronic document?

It's a simple process and may vary slightly in the software you use, but your digital signature software does all the work. You select the signature option, then select the document, and finally enter your pin code. Everything is accomplished electronically; you do not take a pen in hand and sign a paper.

What is a certificate? What does it mean to "publish" a certificate?

A certificate is a computer-based record that identifies the subscriber, contains the public key, and is digitally signed by the certification authority. The digital signature certificate must be associated with both a private key and a public key. When you publish the certificate, you identify yourself to the certification authority by providing it with your public key.

How am I identified as the signer?

When you use your digital signature software, you create a matched pair of keys. One is the "private" key. The private key is used only by you and is required during the signing process.

The second key is the "public" key. The public key is available for use by anyone wishing to authenticate documents you sign. The public key will "read" the digital signature created by the private key and verify the authenticity of documents created with it. It would be similar to the process of accessing a safety deposit box. Your key must work with the bank's key before opening the box.

Who creates the public and private keys?

The digital certificates used to apply digital signatures are comprised of public and private keys. As the names suggest, public keys can be freely shared and are used to verify digital signatures, while private keys are kept secret and are used to create digital signatures.

The key-pair is generated by the Certificate Authority (CA) who issues the digital certificate. The private key is generated on the device (e.g., token) that requests the certificate, so the CA never has access to the private key.

What are the responsibilities and the liability of a digital signature certificate subscriber?

The subscriber is responsible for the following:
- Safeguarding access to the token and the pin code.
- Informing the CSP in case token is lost/ stolen/ damaged.

Does my recipient need special software to receive my digitally signed document?

Recipients of digitally signed document don't need any additional software to verify the signature beyond what they'd normally need to open the document. For example, digitally signed PDF can open in Adobe Reader and digitally signed Microsoft Word document can open in Word. The recipient needs to trust the CA chain by installing these certificates as per the certificate installation steps.

Can a digital signature be forged?

We like to think that a handwritten signature is unique to the signer and to the piece of paper which hold it. What if someone produces a good likeness of your handwritten signature? Or, what if on a long contract, someone changes the text of the pages previous to the signature page? In these instances, the signature is valid, but the document has been altered.

With digital signatures, forgery is next to impossible – much more difficult than forging a handwritten signature. First, a digital signature is more of a process than just affixing a signature. For example, when the document is "digitally signed," the digital software scans the document and creates a calculation which represents the document. This calculation becomes part of the "digital signature." When the recipient verifies the signature, a similar process is carried out. The sender's and the receiver's calculations are then compared. If the results are the same, the signature is valid; if they are different, the signature is invalid.

How do I know if my certificate is valid?

The subscriber could open the token management middle- ware and insert the pin code to view the certificate details and review certificates validity.

Also, the Certificate Revocation List (CRL) is a list that is regularly updated, maintained and published online by CSP and includes all revoked (blacklisted) certificates and subscribers could search their certificates by using the serial number to make sure it is not revoked.

Egypt Trust: http://mpkicrl.egypttrust.com/INVESTORSCA/LatestCRL.crl

MCDR: http://www.mcdr-ca.com/Download.aspx
and select MCDR- Certificate Revocation List - (CRL)

When signing a document / email, a crucial step of the verifying process is checking the serial number of your certificate against the CRL, to make sure that your certificate is valid and not revoked.


ISC
Investor
Service Center
مركز خدمات المستثمرين

3 Salah Salem Street, Nasr City, Cairo, Egypt
Call Center: **16035**
investment@miic.gov.eg
www.miic.gov.eg
MIICEgypt


وزارة الاستثمار والتعاون الدولي
Ministry of Investment and International Cooperation
جمهورية مصر العربية