

طريقة تشفير ملف PDF

قبل البدء بتشفير اي ملف PDF يجب وصل التوكن الخاصة بالتوقيع الرقمي على الكمبيوتر ثم فتح الملف.

الغرض من التشفير:

تحويل المعلومات إلى شفرات غير مفهومة لمنع الأشخاص غير المرخص لهم من الإطلاع على المعلومات أو فهمها، لذلك يجب علينا قبل البدء بالتشفير معرفة الأشخاص الذين سيتم التشفير لهم بحيث يكونوا قادرين على فتح الملف عند استقبالهم له. وبالتالي هناك مرحلتين يجب القيام بهما من أجل هذه العملية.

1. **المرحلة الاولى:** وهي مرحلة ما قبل التشفير وفيها يتم تحميل المفتاح العام للشخص او الاشخاص المراد التشفير لهم ويتم ذلك باتباع الخطوات التالية:

- الدخول الى الموقع <https://ra.nans.gov.sy> فتظهر الصورة التالية:

أهلاً بكم في مركز التصديق الإلكتروني

وصف المشروع: بناء منظومة للتوقيع الرقمي مسؤولة عن منح وإدارة شهادات التصديق الرقمي للعاملين في الجهات العامة بصفتهم الوظيفية

الهدف من المشروع
اعتماد التوقيع الرقمي في المعاملات والمراسلات في الجهات العامة، التي تسمح بتبادل بيانات رقمية موثوقة لها نفس مصداقية الوثائق الرقمية تسهيل وتسريع تبادل المعلومات بين الجهات العامة
التخفيف من الحاجة إلى تبادل الوثائق الورقية الرسمية

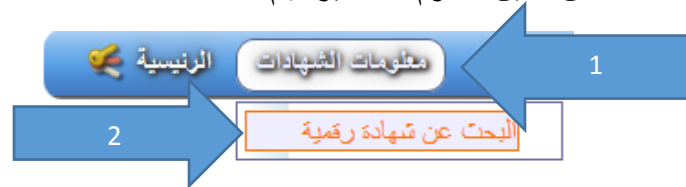
مخرجات المشروع
خدمة منح شهادات التصديق الرقمي للعاملين في الجهات العامة
اعتماد البريد الإلكتروني الحكومي الموثوق

للجهات الحكومية الراغبة بالحصول على شهادات رقمية من منظومة التوقيع الرقمي
يتم تقديم طلب من خلال البريد الإلكتروني пки@nans.gov.sy يتضمن مايلي:

- كتاب رسمي موجه للهيئة الوطنية لخدمات الشبكة، يشير لرغبة الجهة بالحصول على شهادات رقمية مع/ بدون حوامل إلكترونية مع تحديد الأسماء
- صورة هوية كل مستفيد من التوقيع الرقمي
- تعينة استمارة طلب شهادة توقيع رقمي

يمكن تحميل نموذج الاستمارة من [هنا](#)

- نختار القائمة معلومات الشهادة ثم البحث عن شهادة رقمية من اجل اختيار الشخص او مجموعة الاشخاص الذين سأقوم بالتشفير لهم



- بعد الضغط على البحث عن شهادة رقمية تظهر الصورة التالية:

يتم البحث باسم البريد الالكتروني

يتم البحث باسم الشخص ويتم وضعه بين * *

Name: *احبيب*

Emailaddress:

Distinguished Name:

Role:

Request Serial #:

OK Reset

- بعد كتابة اسم الشخص المراد التشفير له تظهر الصورة التالية وفيها جميع الاشخاص الذين في اسمائهم الاسم المراد البحث عنه، أو يتم البحث باستخدام البريد الالكتروني وفيه نحصل على اسم الشخص المراد التشفير له فقط.

Serial	Common Name	Email
0xd0:18:49:81:e2:87:c3:fd:6b:5a	حبيب احمد غانم	h.ghanem@nans.gov.sy

نضغط هنا

يمكن وضع البريد الالكتروني بشكل كامل او الاكتفاء بجزء منه ويتم وضعه بين * *

Name:

Emailaddress: *h.ghanem*


Distinguished Name:

Role:

Request Serial #:


OK Reset

- ففي حال ظهور اكثر من نتيجة في البحث يجب تمييز الشهادة التي هي قيد الاستخدام حالياً عن الشهادة الملغية ويتم ذلك من خلال الضغط على Serial شهادة الشخص المراد فنظهر لنا احدى الحالات التالية:




حبيب احمد غانم
[0xd0:18:49:81:e2:87:c3:fd:6b:5a]

Issued By: NANS
Expiration on: Oct 19 06:36:28 2016 GMT
Profile: User
Status: **Valid** ← شهادة صالحة
[More Info...](#)



Habib Ghanem
[0x1b:ea:ca:37:ed:08:84:4b:66:94]

Issued By: NANS
Expiration on: Jan 23 10:10:00 2015 GMT
Profile: User
Status: **Revoked** ← شهادة ملغية
Reason: unspecified (ERR 2816)
[More Info...](#)



Habib Ghanem
[0x57:e9:51:4b:40:f5:f9:25:62:f1]

Issued By: NANS
Expiration on: Aug 26 10:40:50 2015 GMT
Profile: User
Status: **Expired** ← شهادة منتهية الصلاحية
[More Info...](#)

- بعد الضغط على Serial الشخص المراد التشفير له فتظهر الصورة التالية نلاحظ بان الشهادة Valid وبالتالي نقوم بتحميل المفتاح العام الخاص بهذه الشهادة:

حبيب احمد غانم
[0xd0:18:49:81:e2:87:c3:fd:6b:5a]

Issued By: NANS
Expiration on: Oct 19 06:36:28 2016 GMT
Profile: User
Status: Valid
More Info...

نضغط هنا

- بعد الضغط على More Info تظهر الرسالة التالية، نقوم بتحميل الشهادة باللاحقة Binary (cer) ثم نضغط على Get للتحميل.

md=viewCertFull;dataType=CERTIFICATE;key=982700247058364734729050;xsrf_protecti

OCSP - URI: http://ocsp.nans.gov.sy	
Netscape Cert Type	SSL Client, S/MIME
Netscape Comment	User Certificate of NANS
Authority Key Identifier	keyid:F3:96:4E:E0:6B:51:BB:A5:9F:71:FF:EC:AA:C5:14:C0:A6:FD:4D:1D
Basic Constraints	CA:FALSE
CRL Distribution Points	Full Name: URI: http://ra.nans.gov.sy/pki/pub/crl/cacrl.crl
Certificate Policies	Policy: 1.2.3.3.4 Policy: 1.2.3.3.5 Policy: 1.2.3.3.6 CPS: https://ca.nans.gov.sy/pki/pub/cps/basic
Extended Key Usage	TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
Issuer Alternative Name	email:pki@nans.gov.sy
Key Usage	Digital Signature, Non Repudiation, Key Encipherment
Subject Alternative Name	email:h.ghanem@nans.gov.sy
Subject Key Identifier	90:36:F3:72:C7:40:D4:F3:0B:F7:DF:7D:E2:81:FF:43:FC:C0:64:9C

Operations

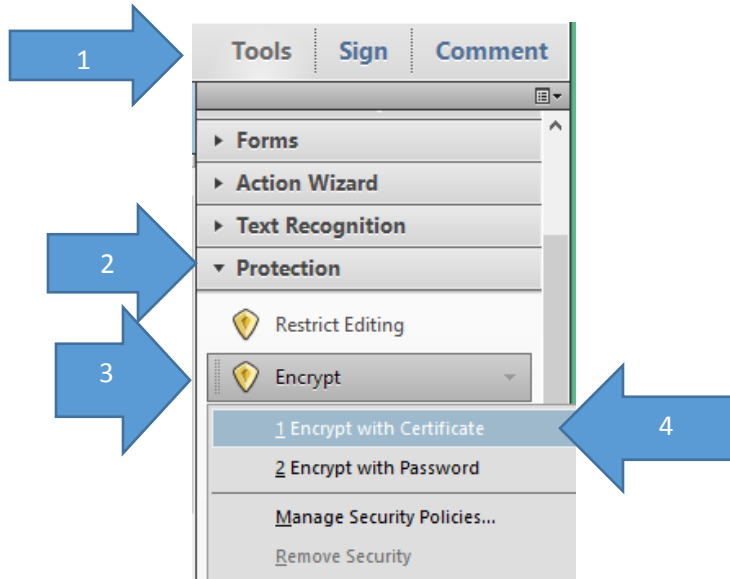
1 → Browser (selected) → Get → 3

2 → Binary (CER)

- الخطوات السابقة نحتاج لها مرة واحدة فقط في حالة كانت شهادة الشخص المراد التشفير له لا تزال في حالة Valid، حيث اننا نقوم بحفظ الشهادات التي تم تحميلها في مجلد معين للاستخدام لاحقا عند الحاجة.
- قد يأخذ ملف الشهادة المحملة اسم غير واضح مثل ____ .cer لذلك نقوم باعادة تسمية الشهادة باسم صاحب الشهادة.

2. المرحلة الثانية: وهي التشفير ويتم ذلك كمايلي:

- نذهب الى قائمة Tools من برنامج Adobe Acrobat XI Pro ثم Protection ثم Encrypt ثم Encrypt with Certificate كما هو موضح في الصورة:



- بعد ذلك تظهر النافذة التالية فنترك كل الخيارات كما هي ونضغط Next.

- بعد الضغط على Next تظهر النافذة التالية فنضغط على Ok.

Name	Issuer	Storage Mechanism	Expires
حبيب احمد غانم	TrustSy	Windows Certificate Store	2016.10.19 06:36:28 Z

- بعد ذلك تظهر النافذة التالية وفيها نقوم باضافة المفتاح العام للاشخاص الذين نريد تشفير الملف لهم ويتم ذلك بالضغط على Browse .

Update the list of intended recipients for documents secured using this policy. You can set document restrictions for a recipient by selecting the recipient and clicking "Permissions".

Name	Email
حبيب احمد غانم	

Search ...

Browse ...

Remove

Details ...

Permissions ...

نضغط هنا لاضافة مفاتيح عامة جديدة

Permissions

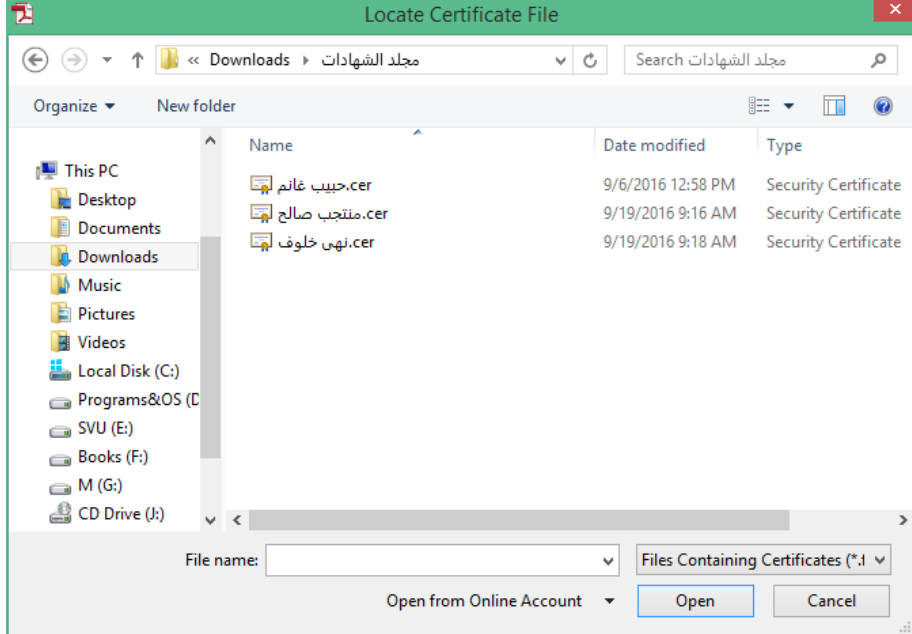
Change Security Settings:	Allowed
Changes:	Any except extracting pages
Printing:	High Resolution
Copying:	Allowed
Accessible:	Allowed

Cancel

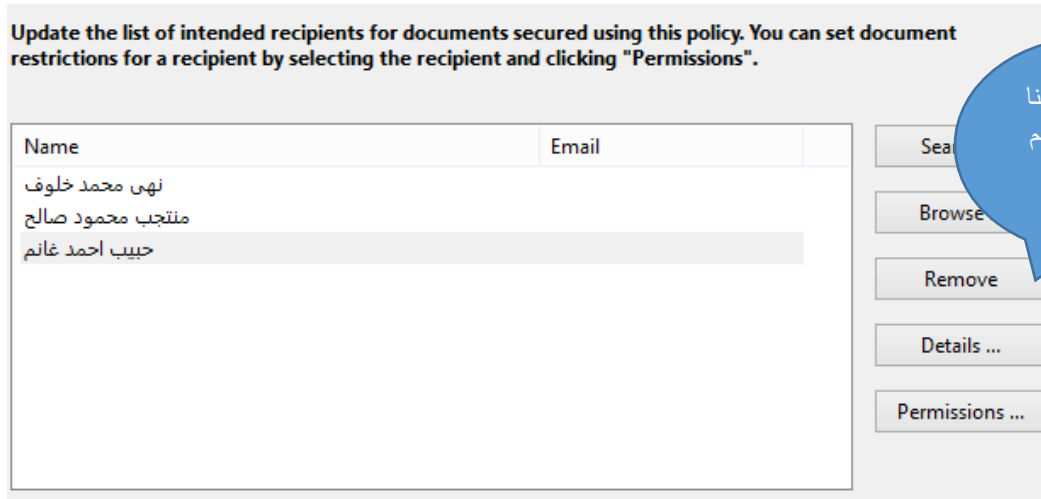
< Back

Next >

- بعد الضغط على Browse تظهر النافذة التالية فنذهب الى المجلد الذي قمت بوضع الشهادات فيه ونختار الاشخاص الذين أريد التشفير لهم حيث تتم اضافة كل شخص بالنقر نقرا مزدوجاً على الاسم.

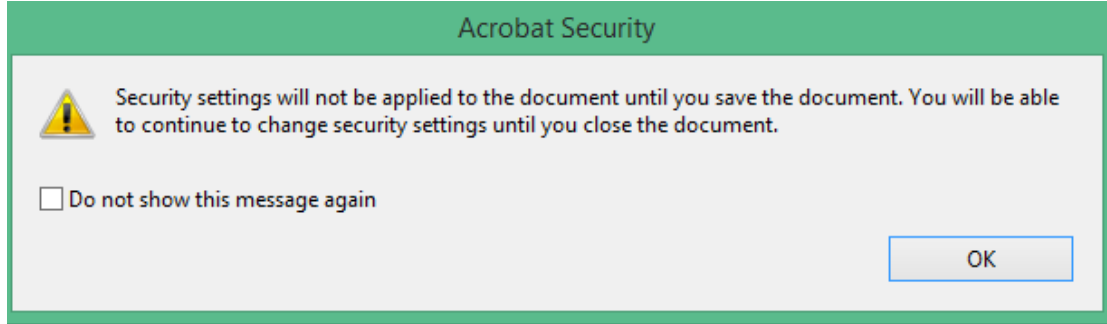


- بعد اضافة الاسماء تظهر كما في الصورة التالية وبالتالي فان كل الاشخاص الموجودين ضمن القائمة التالية سيتم تشفير الملف لهم وبالتالي هم فقط من يستطيعون فتح الملف.



- يمكن حذف اي اسم وذلك بتحديد الاسم ثم الضغط على Remove.

- بعد الانتهاء نضغط على Next ثم Finish فتظهر الرسالة التالية بانه لن يتم تطبيق اعدادات الامان الجديدة قبل ان نقوم بحفظ الملف لذلك نقوم بالضغط على Ok ثم نحفظ الملف.



- ملاحظة: ان حذف اسم من قام بتشفير الملف من قائمة الاسماء الذين سنقوم بتشفير الملف لهم يعني انه لن يستطيع فتح هذا الملف بعد تشفيره لذلك نرى اسمه دائما موجود وبشكل افتراضي ضمن القائمة مع امكانية حذفه.
- وعند محاولة فتح الملف من قبل اي شخص لم نقم بتشفير الملف له سوف تظهر الرسالة التالية، وهي رسالة تفيد بان الملف مشفر ولا يستطيع اي شخص فتح هذا الملف الا من تم التشفير له.

