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 الاشخاص 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 <u>https://ra.nans.gov.sy</u> فتظهر الصورة التالية:



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





 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.

	Seria	Cor	nmon Name	Email
0xd0:18:49:81:e2:87:c3:fd:6b:5a	نضبغط هنا	حبيب احمد غانم		h.ghanem@nans.gov.sy
			بد الالکتروني بشکل جزء منه ويتم وضعه	يمكن وضع البري كامل او الاكتفاء بـ
	Name		**(بين
	Emailaddress	*h.ghanem*		
	Distinguished Name			
	Role			
	Request Serial #			
		L		
	ОК			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 فتظهر لنا احدى الحالات التالية:





anem	1	
ca:37	:ed:08:84	:4b:66:94]
N	IANS	
J	an 23 10:10:0	0 2015 GMT
U	lser	
E	Revoked	شهادة ملغية
u	nspecified (RR 2816)
M	lore 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

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:



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

id=viewCertFull;dataType=CERTIFICATE;key=982700247058364734729050;xsrf_protectic C Search				
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			
1	Operations Browser Get 3 Browser Text PEM Binary (DER) Binary (CER) 2			

- 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
 تم Tools ثم Encrypt with Certificate كما هو موضح في الصورة:



بعد ذلك تظهر النافذة التالية فنترك كل الخيارات كماهي ونضغط Next.

Steps						
General settings Select regiments	Enter general name to conti	information for this Certificate Security policy. You must inue.	t enter at least the			
Summan	Save these	rattings as a policy				
Summary	Discard the	securitys as a poincy				
	() Distant the	se seeings area oppying				
	Policy name:	Encrypt with Certificate	max. 50 Characters			
	Description:	This policy will allow you to require access to a specific private key when opening a document.	max. 250 Characters			
	Select Document Components to Encrypt © Encrypt all document contents Carcypt all document contents except metadata (Acrobat 6 and later compatible) Encrypt only file attachments (Acrobat 7 and later compatible) All contents of the document will be encrypted, and search engines will not be able to access the document's metadata.					
	Ask for reci	pients when applying this policy porithm: 128-bit AES (Compatible with Acrobat 7.0 and la	ter) v			
	Cancel				< Back	Next >

بعد الضغط على Next تظهر النافذة التالية فنضغط على Ok.

	ى Ok.	هر النافذة الثالية فنضغط عد	د الضغط على Next نظ			
اسم من يقوم	Docum	ent Security - Digital ID Selection				
بتشفير الملف Plea once My Dig.	الملف encrypt the document. If you do not select your digital ID in this step, you will not be able to open the document once My Dig.					
Name	lssuer	Storage Mechanism	Expires			
حبيب احمد غانم	TrustSy	Windows Certificate Store	2016.10.19 06:36:28 Z			
Digital ID Selection Persistence	2		Add Digital ID Refresh			
Ask me which digital ID t	o use next time					
O Use this digital ID until I o	close the application					
○ Always use this digital ID						
Help			OK Cancel			

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

Vame	Email	Search	
حبيب احمد غاند			نىغط هنا لاضافة مفاتيح
		Browse	عامة جديدة
		Remove	
		Details	
		Permissions	
Permissions			
Change Security Settings:	Allowed		
Changes:	Any except extracting pages		
Printing:	High Resolution		
Copying:	Allowed		
Accessible:	Allowed		

 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.

1		Lo	ocate Certificat	e File				×
🔄 🌛 🖬 🕯 🐌	« Dow	لشهادات ∢ nloads∕	مجلد ا	v d	5	الشهادات Search	مجلد	Q,
Organize 🔻 New	v folder					l	= •	
This PC Desktop Documents Downloads Music Pictures Local Disk (C:) Programs&OS SVU (E:) Books (F:) M (G:) CD Drive (J:)	(C	Name cer جبيب غانم 🔄 منتجب صالح 🔄 cer،نهى خلوف 💭	ц Т		Dat 9/6 9/1 9/1	te modified /2016 12:58 PM 9/2016 9:16 AM 9/2016 9:18 AM	Type Security (Security (Security (Certificate Certificate
	File nan	ne:	Open from Online	e Account	¥ •	Files Containing Open) Certificate Can	s (*.1 ∨ Icel

 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.

Update the list of intended recipients restrictions for a recipient by selecting	for documents secured using this policy. the recipient and clicking "Permissions"	You can set document
	,	يتم الضغط هنا
Name	Email	Seal I I I I I I I I I I I I I I I I I I I
نهى محمد خلوف		من الفائمة
منتجب محمود صالح		Browse
حبيب احمد غانم		
		Remove
		Details
		Permissions

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

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

Acrobat Security	
Security settings will not be applied to the document until you save the document to continue to change security settings until you close the document.	t. You will be able
Do not show this message again	
	ОК

- 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.

