

Signature

Code

Draft



سلطة التصديق الحكومي

الحامل الإلكتروني (ESMART TOKEN)

دليل الاستخدام

الإصدار: 1

التصنيف: مقيد

2019

			التغييرات
التاريخ	الإصدار	الشخص	ملاحظات

Ν

جدول المراجعات

التاريخ	الشخص	المنصب الوظيفي

				ESMART TOKEN	Page
					2
Page	Ν	Sign	Date		2

هذه الوثيقة تتضمن دليل الاستخدام للحامل الإلكتروني (ESMART TOKEN) المستخدم في سلطة التصديق الحكومي بمركز التصديق الإلكتروني في الهيئة

الوطنية لخدمات الشبكة

						Page
					ESMART TOKEN	2
Corrected	Page	Ν	Sign	Date		3

قبل استخدام الحامل يجب أولاً يجب تنصيب برامج التعريف والإدارة للحامل الإلكتروني (ESMART PKI)....

الآن سنشرح الخطوات اللازمة لاستخدام الحامل الإلكتروني على أنظمة ويندوز (Windows 7,8,10). نضع الحامل الإلكتروني في الحاسب ونفتح البرنامج ستظهر نافذة توضح معلومات الحامل (المأخذ، الاسم، الرقم التسلسلي، المصنّع، الموديل، حجم الذاكرة، عدد الجلسات، طول الرمز الشخصي، عدد المحاولات الفاشلة المسموحة): × - - - × = - × = = SMART* PKI Client 45.1

	Token	Data	Containers	Keys	Certificates	Tools	History	
∫ ^{™II}	🖬 Login Ini	tialize Token C	hange PIN Unlock	PIN				
ISBC ESMART Token 0	Reader							
	PKCS#11 Slot IE	•	1					
	Name		ISBC ESMA	RT Token 0				
	Token							
	Serial Number		3460A51C0	514A101				
	Label		PKIT-token					
	Manufacturer		ISBC					
	Model		ESMARTTO	ken GOST				
	Hardware Versio	m	2.5					
	Firmware Versio	n	0.0					
	Memory Size		72K					
	Maximum Numbe	er of Sessions	10					
	Minimal PIN Len	gth	4					
	Maximum PIN Le	ngth	8					
	Markup Version		2.1					
	Profile		Default 1.0					
	PIN Try Count		10					
	SO PIN Try Cou	nt	10					

للدخول إلى الحامل الإلكتروني واستخدامه يجب الضغط على زر Login وإدخال الرمز الشخصي Pin (default PIN: 12345678)

🥃 ESMART	PKI Client		Ø
	🥃 ESMART	Авторизация РІN или Віо	\otimes
ISBC ESMART Token 0	Re: PKC Nar Toł Seri Lab- Man Mod Han Firm Man Man Man Man Man Man Man So l	ли портиствуют совранённые отпачатки пальцев Введите PIN-код	ризоваться по PIN-коду

ESMART PKI Client 4.5.1

عندها ستظهر نافذة جديدة تمكننا من القيام بالكثير من العمليات: (تهيئة الحامل، مسح البيانات، تغيير الرمز الشخصي، فك قفل الحامل...).

إذا أردنا تهيئة الحامل ومسح كافة البيانات عليه نضغط Initialize Token وندخل SO PIN

(default SO PIN: 12345678)

						Pag
					ESMART TOKEN	4
Corrected	Page	Ν	Sign	Date		4

SMAR ESMAR	T[°] PKI Clie	nt					
	Token	Data	Containers	Keys	Certificates	Tools	History
ISBC ESMART Token 0	Logout I	nitialize Token	Clear Token Cha	nge PIN Unlock	PIN Enroll finger	rprints	
	PKCS#11 Slot IE	C	1				
	Token		3460A51C	C0514A101			

لتغيير الرمز الشخصي نضغط على الزر Change PIN وندخل الرمز الشخصي الجديد ونضغط على الزر OK.

Change PIN	×
() U	ser 🔘 SO
Old PIN	•••••
New PIN	•••••
Repeat New PIN	••••••
	Generate
	OK Cancel

لتوليد المفتاح الخاص على الحامل الإلكتروني نضغط على التبويب Keys ثم نضغط على Generate Key Pair:

Generate Key Pair		×
Key Pair Type	RSA	~
Key Size (bit)	1024	
	ОК	Cancel

نختار خوارزمية التوليد ونضغط OK ليتولد لدينا المفتاح الخاص على الحامل الإلكتروني...

	Token	Data	Containers	Keys	Certificates	Tools	History
	Logout	Refresh Save Key	Generate Key	Generate Key Pai	r View Delet	e Certificate Re	quest
ISBC ESMART Token 0	⊞ 🗞 RSA K	ey Pair (73e94c82-	d374-4d1f-a896-c7	1dc95f44f5); Key Si	ze, bits: 1024		

عند تحديد هذه المفتاح ستظهر لدينا مجموعة من الخيارات الإضافية (حفظ المفتاح، إظهار المفتاح، حذف المفتاح، إنشاء طلب لشهادة مرتبط بهذا المفتاح). والآن يمكننا إنشاء ملف طلب الشهادة بالضغط على التبويب Certificate Request

							Pag
						ESMART TOKEN	_
ſ	Corrected	Page	Ν	Sign	Date		5

Certificate Request				\times
Data				
Person	Organization			
Name				
Surname				
Given Name				
E-mail				
Title				
Organizational Uni	t			
Organization				
Address				
Locality				
State				
Country	Russian Federation (RU) \sim			
INN				
OGRN				
OGRNIP				
SNILS				
Unstructured name	le			
Extensions	No ~			<u>_</u>
Subject Alternative	e Name	Certificate Templa	ate OID	
E-mail		Template OID		
IPv4		Major Version		
DNS		Minor Version		

نملأ البيانات المطلوبة (يجب إدخال بيانات الاسم والبريد الإلكتروني على الأقل) ونضغط Generate فيظهر الطلب في الجانب الأيمن، نضغط Save to File لحفظ ملف.

نرسل ملف الطلب إلى سلطة التصديق لتوقيعه والحصول على المفتاح العام.

لاستيراد هذا الملف نضغط على التبويب Certificates ثم نضغط Add ونختار الملف المطلوب لتصبح لدينا شهادة شخصية يمكن استخدامها لاحقاً...

😻 ESMART PKI Client 4.5.1									
🥃 ESMART	PKI Clier	nt							
	Token	Data	Containers	Keys	Certificates	Tools	History		
J ^{HI}	B Logout Refresh Add View Delete Certificate CN-ahmad odiem, SURNAME-ahmad, GIVENNAME-adiem, OU=NANS, O=ECC, STREET=Sahara, L=Qudsaya, ST=Damascus, C=SY								

كيف سنستخدم الشهادة الموجودة على الحامل الإلكتروني لتوقيع ملف والتحقق من هذا التوقيع؟

						Page
					ESMART TOKEN	(
Corrected	Page	Ν	Sign	Date		0

لتوقيع ملف نضغط على التبويب Tools

	Token	Data	Containers	Keys	Certificates	Tools	History		
State State	a Logout								
ISBC ESMART Token 0	Digital signatur	9							
		Certificate	CN=ahmad odiem	, SURNAME=ahma	d, GIVENNAME=od	liem, OU=NANS, O	ECC, STREET=Sal	nara, L=Qudsaya, S	T=Damascus, C=SY 🛛 🗸
		File	C:\Users\Dell\Desk	top\Token_Test.pd	lf				X
								Detached	Sign
	Digital signatur	e verification							
		Signature file							X
	(if signat	Source file ure is detached)							X
	Verify certi	ficate chain 🕕							
	CRL	directory 🛈							X
									Verify

نختار الشهادة التي نريد التوقيع بها (يمكن وضع أكثر من شهادة على نفس الحامل) ونختار الملف الذي نريد توقيعه ثم نضغط Sign

File being signed	
File path	C:\Users\Dell\Desktop
File name	Token_Test.pdf
Size	664.7 KB
File creation time	2019-10-10 08:47:49
File modification time	2019-10-10 08:47:50
Checksum (SHA-256)	FC5709C2419641C5F803301BC3D1A12C53CA460A3507A5FE0A1EF11AEED77F1B
Certificate	
Subject	CN=ahmad odiem, SURNAME=ahmad, GIVENNAME=odiem, OU=NANS, O=ECC, STREET=Sahar
Serial Number	23198514A4A31BAD6DD2
(
`	

تظهر نافذة عليها اسم الملف وحجمه و Checksum وكذلك الشهادة مع رقمها التسلسلي، نضغط Sign سيتولد لدينا ملف التوقيع بلاحقة P7s نحفظه على جهازنا.

الآن كيف يمكن التحقق من صحة التوقيع لملف ما...؟

للتأكد من صحة توقيع ملف ما، ننتقل إلى القسم Digital signature verification نختار ملف التوقيع (P7s.) والملف المراد التحقق منه ونضغط Verify عندها ستظهر نافذة تؤكد صحة التوقيع وأن البيانات لم يطرأ عليها أي تغيير وتظهر كذلك مالك الشهادة والجهة المصدرة للشهادة وصلاحيتها ورقمها التسلسلي...وفي حال عدم صحة التوقيع ستظهر رسالة تبيّن أن التوقيع غير صالح وأن البيانات قد يكون قد طرأ عيها تغيير.

						Pag
					ESMART TOKEN	7
Corrected	Page	Ν	Sign	Date		

😻 File signature verification

Signature	
Authenticity	Signature is valid. Data was not changed.
Certificate	
Owner	ahmad odiem
Issuer	C=SY,O=Operations,OU=ECC,CN=Com. Root CA
Valid from	2019-10-10 06:06:10
Valid till	2019-11-09 06:06:10
Serial Number	23198514A4A31BAD6DD2

ОК

						D
						Page
					ESMART TOKEN	0
Corrected	Page	e N	Sign	Date		8

Х