www.kotobarabia.com

قانون التوقيع الإلكتروني (واللائحة التنفيذية)

قانون

التوقيع الإلكتروني

(واللائحة التنفيذية)

طبقا لقوانين الملكية الفكرية

جميع حقوق النشر و التوزيع الالكتروني لمذا المصنف محفوظة لكتب عربية. يحظر نقل أو إعادة بيع اى جزء من خذا المصنف و بثه الكترونيا (عبر الانترنت أو للمكتبات الالكترونية أو الاقراص المحجة أو اى وسيلة أخرى) دون الحصول على إذن كتابي من كتب عربية. حقوق الطبع الو رقى محفوظة للمؤلف أو ناشره طبقا للتعاقدات السارية.

فهيرس

-	
-	
	قرارات وزارة الاتصالات وتكنولوجيا المعلومات
-	
-	
_	
_	_

:"

: : ()

: ()

: ()

· : ()

: ()

.

: ()

: () () () () ()

() () () () () () ()

() () () () () ()

() () () ()

() () () () () () () () () () () ()

() () () () () ()

() ()

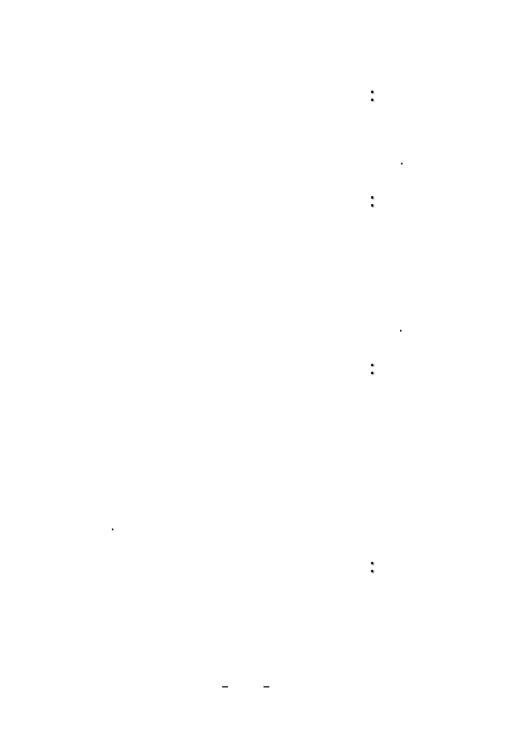
:

- -

()	
()	
. ()	
. ()	
. ()	
. ()	

				()
				()
			:	
	-	-		

() () () ()





;
()
()
()

:

:

- -

()
...
()
...

:

:

· _ _ () () ()
. ()
. ()

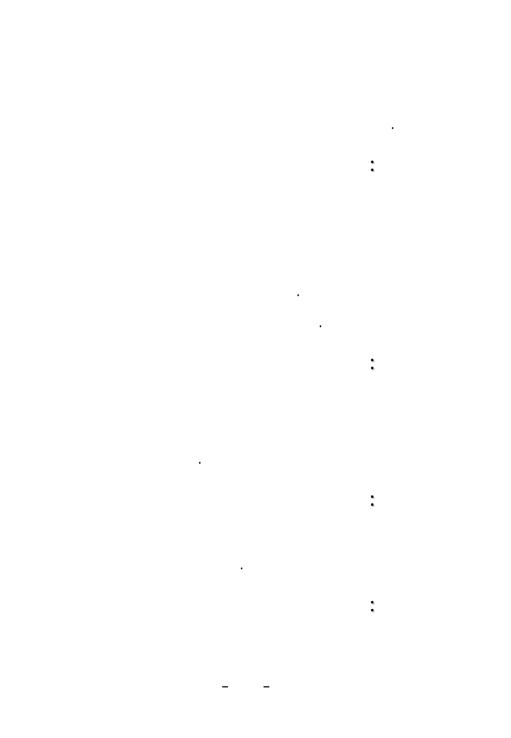
.

.

· :

- -

			:		
				()	
	-	-			



()

اللائحة التنفيذية

1 1

:

•

·

.() (1)

()

. () ()

· ()

-

·

-. -

·

.

/

- -

1 1

()

- -

	()
		()	
	()
_		-	

(voip) .(vpn) .(sms) .(gprs)

() • () • () 1



()

•

.

()

•

/

: -

.

: -

: -

: -

•

: -

•

•

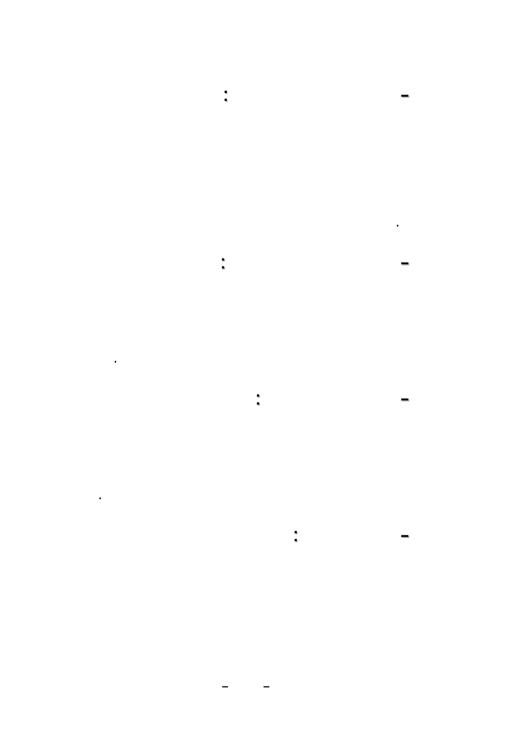
:

.

; -

.

:(



(smart tokens)

.

•

. _



:

: -

•

: -

•

· : -

•

() () () () () () () ()

		()
()		
	•	()
		.(bit)
(hardware security	()	modules)
	()	. ()

. ()

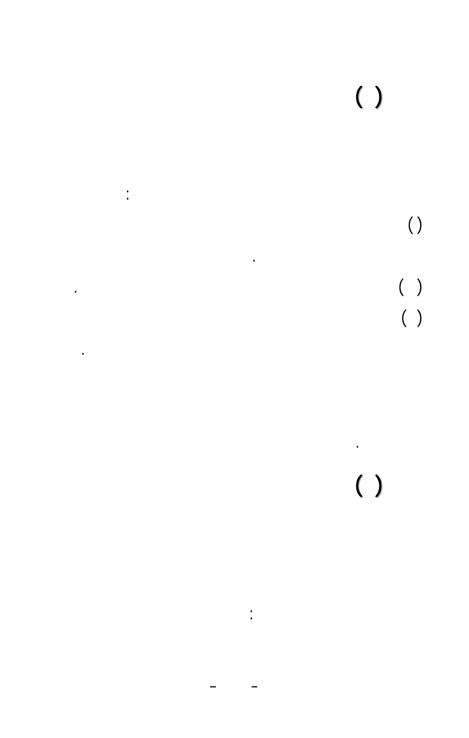
. ()

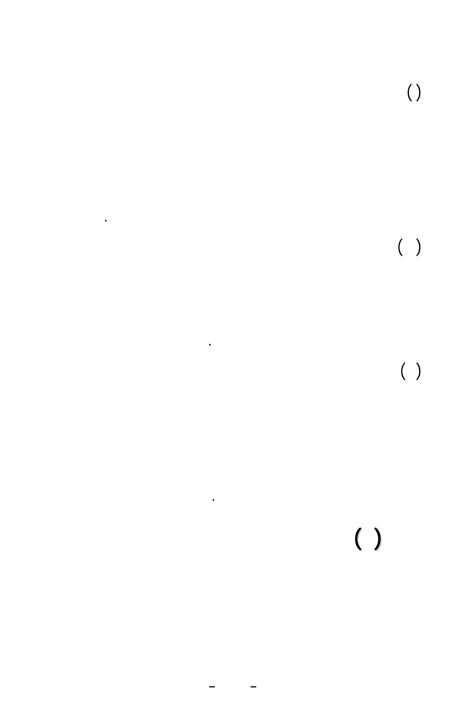
()

()

.()

()





() () () . ()

() () () () ()

() . () () () () ()

_ _

() () () ()

() () () (() ()

. () () . ()

· ()

()

() ()

(web site) ()

					()
					()
()				
		-	-		

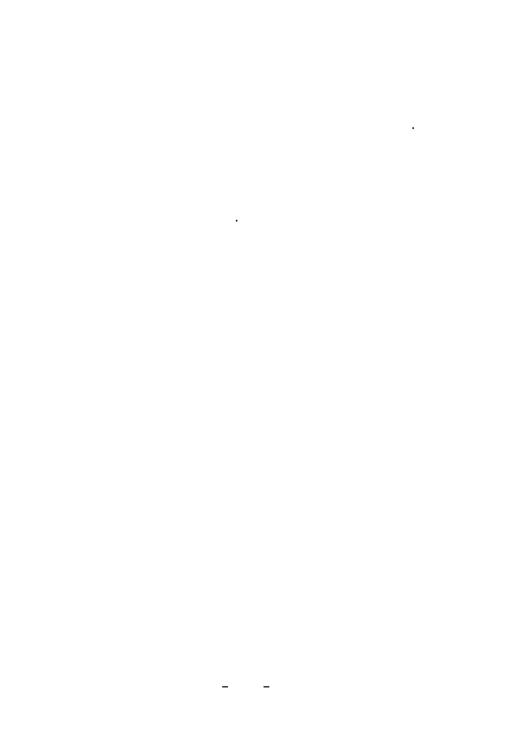
()

.

()

•

()



(-)

Pki technology

- The profiles rpf pki operational management protocols must be based on pkix (x. 509 based pki).
- The profile for qualified certificates must be based on x. 509 (rfc 3739).
- At least one of the following algorithms must be deployed:
 - Symmetric algorithms (AES, {N} DES, CAST5, BLOWFISH, TWOFISH, IDEA etc).
 - o Asymmetric algorithms (DSA, RSA, ELGAMAL, RC {N} etc).
 - o Hash algorithms (MD5, SHA-1 224 etc).

- Minimum RSA/ DS A key length must be at least 1024 bits until the end of 2006. ncreaing the length to 2048 bits is recommended with a view to guaranteeing long term security levels.
- Abaseline certificate policy for service providers issuing qualified certificates should be written according frame work RFC 3647.

(-)

Hardware security modules

For e-signature creation and verification product and in trustworthy hardware devices used as secure signature creation devices, it is required it have concurrent acceptance and usage of FIBS 140 – 1 level 3 or higher or equivalent standard such as suitable protection profile based on common criteria (iso 15408).

(–)

Smart cards

Smart cards are able to store private esignature keys for acard holder without delivering the key to outside world. Therefore the calculation of the signature algorithm as well as its storage is proformed in ahighly secure environment inside asmart card thus, it is required to have smart card (reader/readerless/ contactless) which use the most advanced security standard avaible in the market.

Security evalution ITSEC E4 OR NIST FIPS x.509v3 certificates Iso 7816

Cryptographic algorithms must include RSA. SHA-1

MICROSOFT PC/SC Recommende: capi-

Microsoft cryptographic Recommended: pkcs #11 Recommended: pkcs #5

(interface) (syntax standard)

(-)

Security standards

- general security management codes of practice, such as BS7799-2 (british standard, information security management system specification with guidance for use) and its guidance ISO/IEC 17799 (recommended) < or equivalent standard.

Operation standards

Recommended: ETSI (the European telecommunications standards institute) TS 101 456 v 1.2.1 (2002 – 04) policy requirements for certification authorities issuing qualified certification, specifically chapter 7 which covers the following parts:

- certification practice statement.
- Key management life cycle.
- Certificate management life cyrcle.
- CA management and operation. Or equivalent standard.