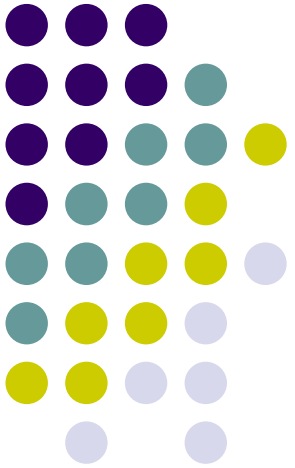
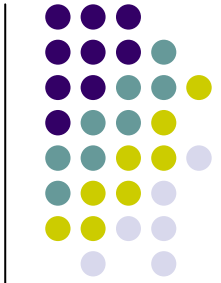
Length of cryptographic keys

Zdeněk Říha



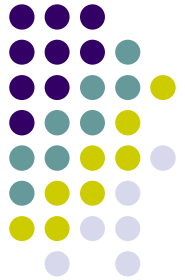
Security of RSA



- We choose randomly 2 primes and compute n and φ(n) :
  - **p, q**
  - **n = p·q**
  - **φ(n) = (p-1)(q-1).**
- **e** is chosen such that **gcd(e, φ(n)) = 1.**
- We compute **$d = e^{-1} \pmod{\varphi(n)}$.**
- Public key: **n, e.**
  Private parameters: **p, q, d.**
  Private key: **d.**

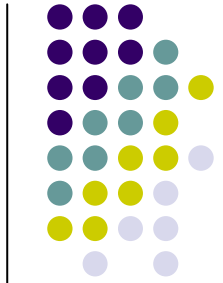
- Security of RSA cryptosystem is based on the problem of factoring large numbers
- If public **n** can be factored into **p** and **q**, we can calculate **φ(n)** and derive d from e.
- Integer factorization is taught at primary schools
- But when integers are very big it takes very long time even for fast computers to factor the number

Computational Security



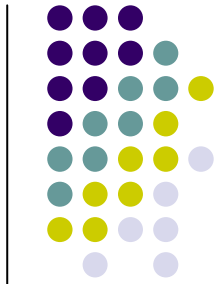
- Unconditional vs. computational security
- Security based on a hard problem
- The problem is solvable, but it takes impractically long time to solve
- The attacker cannot wait thousands/millions of years to break the encryption
- Our expectations can change:
  - Progress in the speed of HW
  - Progress in the efficiency of algorithms

History of RSA Security



- RSA is considered secure
  - But the key size does matter
- 1977: published in “Scientific American”
  - RSA-129 (129 decimal digits of modulus n)
  - Challenge of 100 dollars
  - 40 quadrillion years estimated to factor …
  - Factored in 1994
    - “The magic words are squeamish ossifrage.”

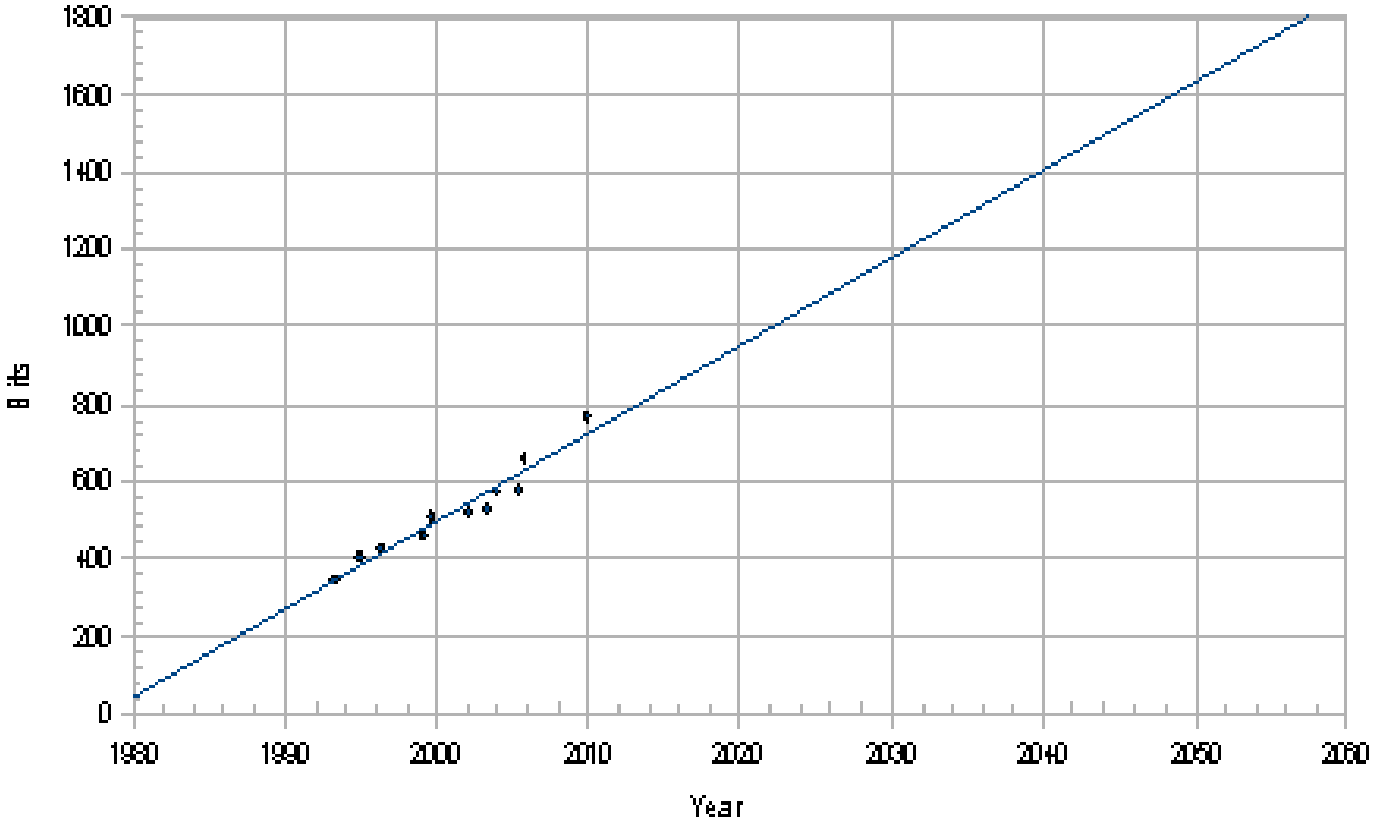
History of RSA Security II



- 1999
  - 512 bit integer was factorized
- 2005
  - 663 bit integer was factorized
- January 2010
  - 768 bit integer was factorized

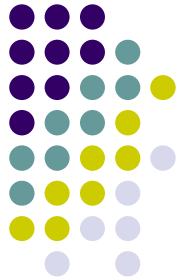
- 1024 bit integers are (probably) not factorable at the moment

Security of RSA



Source: P. Layland, RSA Security and Integer Factorization: The Thirty Years War from 1990 to 2020, IS2 2010, Praha

Key size



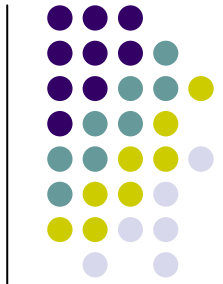
- Algorithms are public & keys must be secret
- Key must be large enough that a brute force attack is infeasible
- Depending on the algorithm used it is common to have different key sizes for the same level of security
  - Representing the level of security – number of combinations needed for the brute force attack
  - E.g. 1024 bit RSA key equivalent to 80 bit symmetric encryption key

Comparable strengths of cryptosystems

Bits of security	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA[19]	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Source:
NIST SP800

Security strengths of hash functions



Bits of Security	Digital Signatures and hash-only applications	HMAC	Key Derivation Functions[20]	Random Number Generation[21]	Other (To Be Determined)
80	SHA-1[22], SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	To Be Determined
112	SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
128	SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
192	SHA-384, SHA-512	SHA-224, SHA-256, SHA-384, SHA-512	SHA-224, SHA-256, SHA-384, SHA-512	SHA-224, SHA-256, SHA-384, SHA-512	
256	SHA-512	SHA-256, SHA-384, SHA-512	SHA-256, SHA-384, SHA-512	SHA-256, SHA-384, SHA-512	

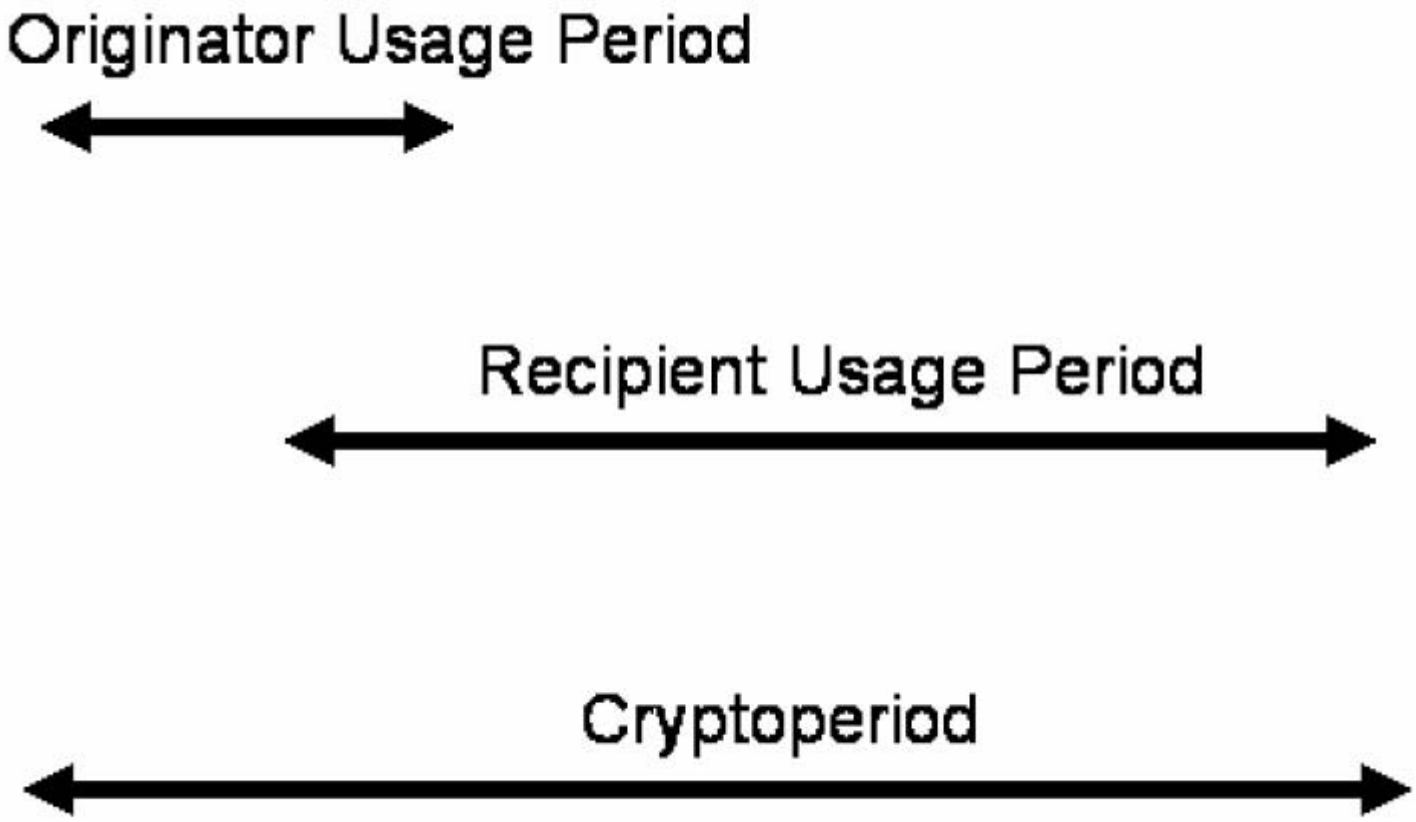
Source:
NIST SP800

Recommended key sizes

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[23] 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$; $N = 160$	Min.: $k=1024$	Min.: $f=160$
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: $k=2048$	Min.: $f=224$
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: $k=3072$	Min.: $f=256$

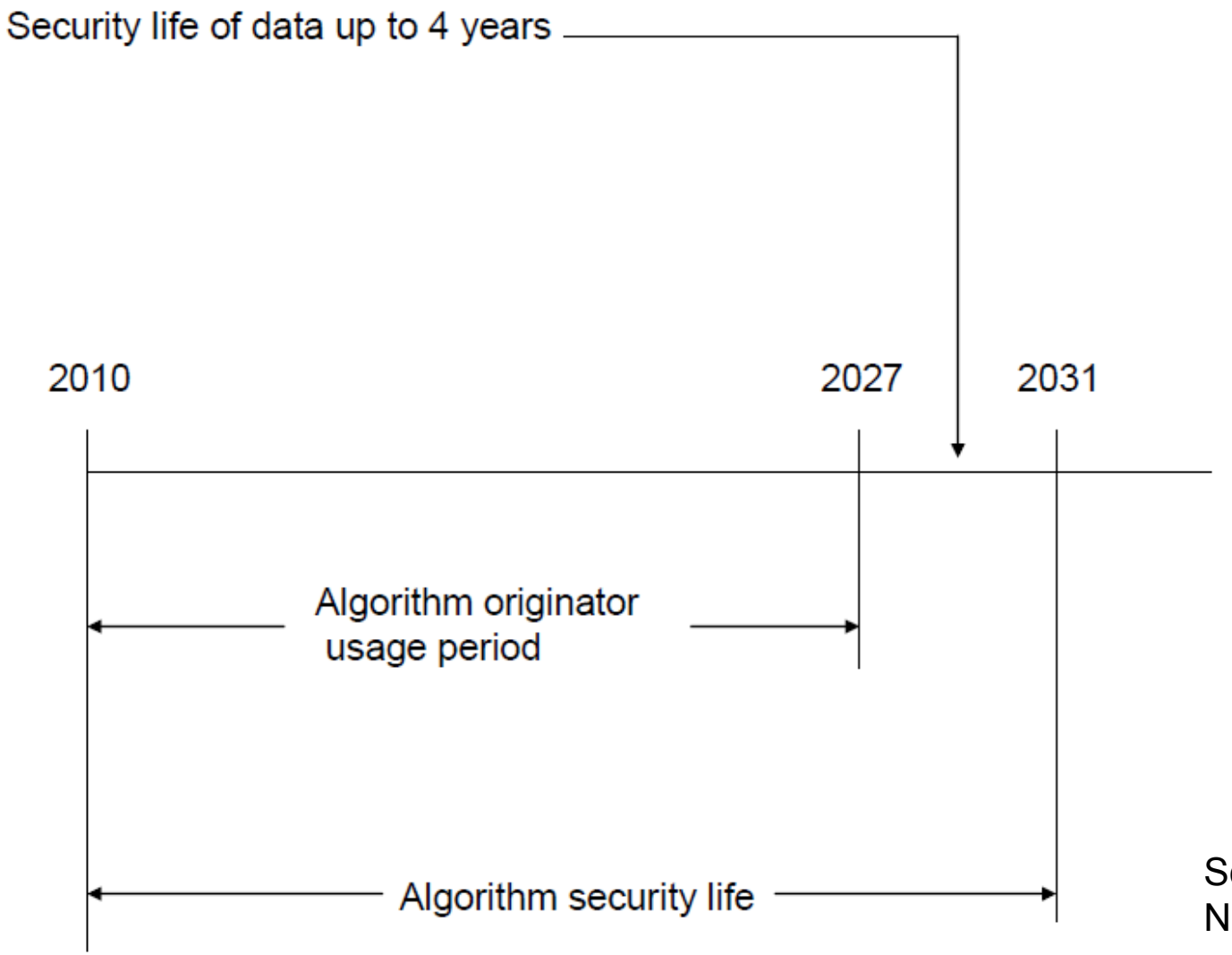
Source:
NIST SP800

Crypto period



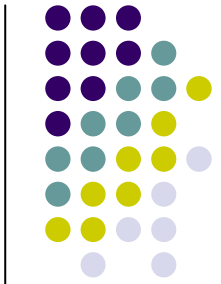
Source:
NIST SP800

Crypto period example



Source:
NIST SP800

Recommended crypto periods



Key Type	Cryptoperiod	
	Originator Usage Period (OUP)	Recipient Usage Period
1. Private Signature Key	1-3 years	
2. Public Signature Key	Several years (depends on key size)	
3. Symmetric Authentication Key	≤ 2 years	≤ OUP + 3 years
4. Private Authentication Key	1-2 years	
5. Public Authentication Key	1-2 years	
6. Symmetric Data Encryption Keys	≤ 2 years	≤ OUP + 3 years

Source:NIST SP800

ETSI recommendation (RSA)

Parameter	1 year	3 years	6 years	10 years (speculative)
MinModLen	1 024	1 536	2 048	?
ErrProb	2^{-80}	2^{-80}	2^{-100}	2^{-100}
SeedEntropy/EntropyBits	80	80	100	?

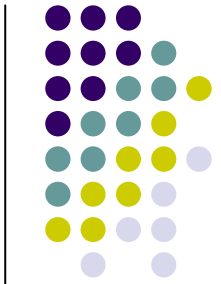
- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended key sizes for RSA
- Starting date: 2006

ETSI recommendation (RSA)

entry name of the padding scheme	1 year	3 years	6 years	10 years (speculative)
PKCS#1-v1.5	usable/n.a	usable/n.a.	usable/n.a.	unusable/n.a.
PKCS#1-v2.1	usable/n.a	usable/n.a	usable/n.a.	unusable/n.a.
PKCS#1-PSS	usable/64	usable/64	usable/64	usable/64
ISO-DS 2	usable/64	usable/64	usable/64	usable/64
ISO-DS 3	usable	usable	usable	usable
ISO-DIN-RN	usable/64	usable/64	usable/64	usable/64

- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended padding schemes for RSA
- Starting date: 2006

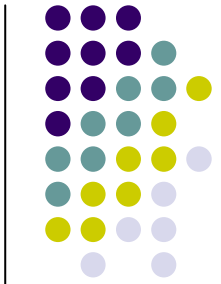
ETSI recommendation (DSA)



Parameter	1 year	3 years	6 years	10 years (speculative)
pMinLen	1 024	1 536	2 048	2 048
qMinLen	160	160	224	224
ErrProb	2^{-80}	2^{-80}	2^{-100}	2^{-100}
SeedEntropy/EntropyBits	80	80	100	100

- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended key sizes for DSA
- Starting date: 2006

ETSI recommendation (ECDSA)



Parameter	1 year	3 years	6 years	10 years (speculative)
pMinLen	-	-	-	?
qMinLen	160	160	224	?
r0Min	104	104	104	?
MinClass	200	200	200	?
ErrProb	2^{-80}	2^{-80}	2^{-100}	2^{-100}
SeedEntropy/EntropyBits	80	80	100	?

- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended key sizes for ECDSA
- Starting date: 2006

ETSI recommendation (hash functions)

entry name of the hash function	1 year	3 years	6 years	10 years (speculative)
sha1	usable	unknown	unusable	unusable
ripemd160	usable	usable	unusable	unusable
sha224	usable	usable	usable	unknown
sha256	usable	usable	usable	unknown
sha384	usable	usable	usable	usable
sha512	usable	usable	usable	usable
Whirlpool	usable	usable	usable	usable
NOTE: The listed hash functions are expected to be 2nd pre-image resistant and pre-image resistant for a longer period of time.				

- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended hash functions
- Starting date: 2006

ETSI recommendation

Entry name of the signature suite	1 years	3 years	6 years	10 years
sha1-with-rsa	1 024	unknown	not recommended	
sha256-with-rsa	1 024	1 536	2 048	2 048
RSASSA-PSS with mgf1SHA-1Identifier	1 024	1 536	2 048	2 048
RSASSA-PSS with mgf1SHA-224Identifier	1 024	1 536	2 048	2 048
RSASSA-PSS with mgf1SHA-256Identifier	1 024	1 536	2 048	2 048
sha1-with-dsa	1 024	unknown	not recommended	
sha1-with-ecdsa	163	unknown	not recommended	
sha224-with-ecdsa	224	224	224	224
sha256-with-ecdsa	256	256	256	256

- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended signature schemes
- Starting date: 2006

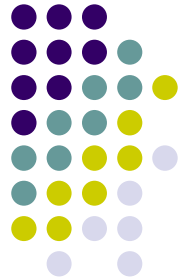
Česká republika & EU & ETSI

- EU
  - SMĚRNICE 1999/93/EC EVROPSKÉHO PARLAMENTU A RADY ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
- ČR
  - Zákon č. 227/2000 Sb. o elektronickém podpisu
  - Několikrát novelizován
  - Podzákonné předpisy
    - Nařízení vlády č. 495/2004 Sb, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
    - Vyhláška č. 496/2004 Sb. k elektronickým podatelnám
    - Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb

Česká republika & EU & ETSI

- Vyhláška č. 378/2006 Sb.
  - „používá důvěryhodné systémy a postupy, které splňují požadavky standardu pro tyto systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky“
  - 1. CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements.
    - „Security requirements for TWSs also include a minimum set of requirements to be fulfilled by the signature algorithms and their parameters allowed for use by CSPs. These requirements are provided in [ALGO].“
    - [ALGO] ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

Stanovisko MV ČR



- „V návaznosti na směrnici ES č. 1999/93/EC o zásadách Společenství pro elektronické podpisy a v ní obsažený princip vzájemného uznávání kvalifikovaných certifikátů vydaných v kterémkoliv členském státu EU je nezbytné vycházet z dokumentu ALGO paper, který stanoví, že od 1. 1. 2010 je algoritmus SHA-1 „unusable“ a je tedy nezbytné ukončit jeho používání pro oblast elektronického podpisu a zahájit přechod na bezpečnější algoritmy třídy SHA-2. Česká republika patří k těm členským státům, ve kterých je tento přechod rozložen do delšího časového období. Je však nezbytné jej realizovat, a tak zachovat důvěru uživatelů v bezpečnost elektronického podpisu.“

  - poskytovatelé certifikačních služeb přestanou vydávat kvalifikované certifikáty s algoritmem SHA-1 nejpozději do 31. 12. 2009,
  - poskytovatelé certifikačních služeb zahájí vydávání kvalifikovaných certifikátů s hashovací funkcí třídy SHA-2 nejpozději 1. 1. 2010 (mohou tak však učinit kdykoliv dříve); tato změna se samozřejmě týká i vydávání kořenových certifikátů, kterými poskytovatel certifikačních služeb označuje jím vydané certifikáty,
  - aplikace, ve kterých je elektronický podpis používán, musí podporovat nejpozději od 1. 1. 2010 všechny algoritmy třídy SHA-2,
  - podpora algoritmu SHA-1 musí být v aplikacích zachována minimálně do 31.12.2010

Zdroj: MV ČR

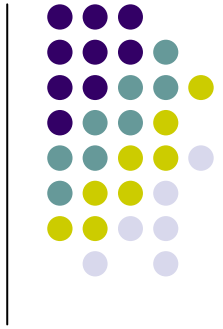
Dohoda českých akreditovaných CA

- „Kvalifikované certifikáty s hashovací funkcí třídy SHA-2, které začnou vydávat nejpozději od 1. ledna 2010, budou všichni tři poskytovatelé přednostně nabízet s hashovací funkcí SHA-256 v kombinaci s algoritmem RSA s délkou klíče 2048 bitů. Poskytovatel certifikačních služeb může na základě vlastního rozhodnutí a základě požadavků svých zákazníků vydávat kvalifikované certifikáty i s některou z dalších funkcí z rodiny SHA-2, tj. SHA-224, SHA-384 nebo SHA-512.“

  - Ministerstvo vnitra nemá námitek proti této dohodě. Tvůrce aplikací pracujících se zaručeným elektronickým podpisem založeném na kvalifikovaném certifikátu je však nutné upozornit, že je nezbytné vytvořit prostředí pro akceptování všech čtyř hashovacích funkcí rodiny SHA-2, a to i s ohledem na akceptaci kvalifikovaných certifikátů vydaných v jiných členských státech EU

Zdroj: MV ČR

Akreditované CA



- První certifikační autorita, a. s.
- Česká pošta, s. p.,
- eldentity a. s.,

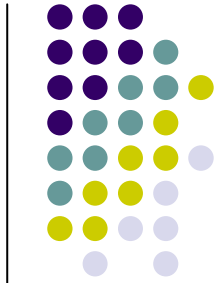
Zdroj: MV ČR

Poslední změny zákona

- „Za elektronický podpis splňující požadavky odstavce 1 se považuje rovněž zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb usazeném v některém z členských států Evropské unie, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb, jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled.“

Zdroj:
§ 11 zákona 227/2000 Sb.

Jak na to v praxi



- Každá země EU vydává seznam důvěryhodných certifikačních služeb
  - TSL: Trusted Services List
- Ne každá země však takový seznam digitálně podepisuje …
- Seznam je k dispozici mimo jiné na http://tsl.gov.cz/
  - Řada odkazů na lidsky čitelné a strojově zpracovatelně (XML) TSL seznamy zemí EU

Seznam TSL

Seznam TSL

Seznam TSL členských států EU byl načten z internetové adresy **https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml** 20.09.2010 v 08.16 (CET). Jedná se o čas serveru, na kterém je provozována tato aplikace. Čas serveru je synchronizován s NTP serverem time.ufe.cz (stratum 1). Příští aktualizace seznamu proběhne 20.09.2010 v 09.16 (CET)

Seznam TSL

Stát	URL strojově zpracovatelného TSL	URL lidsky čitelného TSL
Belgie (BE)	http://tsl.belgium.be/tsl-be.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://tsl.belgium.be/tsl-be.pdf
Bulharsko (BG)	Není k dispozici	http://www.crc.bg/section.php?lang=en&id=31
Česká republika (CZ)	http://tsl.gov.cz/publ/TSL_CZ.xtsl	http://tsl.gov.cz/publ/TSL_CZ.pdf
Dánsko (DK)	http://www.itst.dk/digitale-losninger/digital-signatur/in... TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://www.itst.dk/digitale-losninger/digital-signatur/in...
Estonsko (EE)	http://sr.riik.ee/tsl/estonian-tsl.xml TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://sr.riik.ee/tsl/estonian-tsl.pdf
Finsko (FI)	http://www.ficora.fi/attachments/suomiry/5m5T1qldW/truste... Formát XML souboru není dle specifikace XML.	http://www.ficora.fi/attachments/suomiry/5m5Sl2GEj/truste...
Francie (FR)	http://references.modernisation.gouv.fr/sites/default/fil... TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://references.modernisation.gouv.fr/sites/default/fil...

Služba MV ČR: CertIQ

- Určí, zda certifikát byl vydán jako kvalifikovaný v nějaké zemi EU

Certifikát

Soubor: cert10569926.cer
Vystaveno pro: SERIALNUMBER=ICA - 10134279, EMAILADDRESS=tupa.irena@tiscali.cz, OU=PORTALZP-ZZ, O=MUD. Irena Tupá, L="Žatec, Javorová 2692, 43801", CN=MUD. Irena Tupá, C=CZ
Sériové číslo certifikátu: 10569926
Vystavitel: OU=I.CA - Accredited Provider of Certification Services,O=První certifikační autorita\, a.s.,CN=I.CA - Qualified Certification Authority\, 09/2009,C=CZ
Platnost od: 20.09.2010 10:37 CEST
Platnost do: 20.09.2011 10:37 CEST

Výsledek ověření, zda se jedná o kvalifikovaný certifikát*

* kvalifikovaný certifikát ve smyslu směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy, resp. zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

Na základě informací dostupných v TSL zveřejněných členskými státy lze tento certifikát považovat za kvalifikovaný.

Porovnání proběhlo oproti TSL dostupným 20.09.2010 v 21.17 (CET). Jedná se o čas serveru, na kterém je provozována tato aplikace. Čas serveru je synchronizován s NTP serverem time.ufe.cz (stratum 1).

Tato aplikace ověřuje pouze, zda je certifikát kvalifikovaný, neověřuje však jeho platnost.

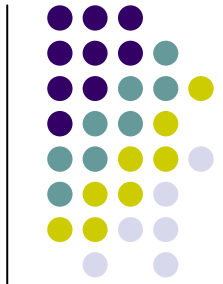
Služby, kterým odpovídá zadaný certifikát

	Stát	Vydavatel
1.	CZ	Ministerstvo vnitra České republiky

ICAO recommendation

- International Civil Aviation Organization
  - Electronic passports
  - Data signed by the issuing country to protect integrity
  - One CA per country, certificates issued for entities producing passports (so called Document Signers).
  - Standard validity of passports: 10 years

ICAO recommendations



- RSA (UK, CZ, France, …)
  - Padding: PKCS#1 v1.5, PSS (recommended)
  - For CA: min 3072 bits
  - For DS: min 2048 bits
- DSA
  - For CA: min 3072/256 bits
  - For DS: min 2048/224 bits
- ECDSA (Germany, Switzerland, …)
  - For CA: min 256 bits
  - For DS: min 224 bits
- Hash functions
  - SHA-1, SHA-2

Source: ICAO Doc. 9303

ICAO recommendations

- “It is therefore RECOMMENDED that the maximum period the Document Signer Key is used to sign passport documents be three months. For States that generate large numbers of MRTDs, several current document signing keys MAY be issued at any given time.”

Source: ICAO Doc. 9303