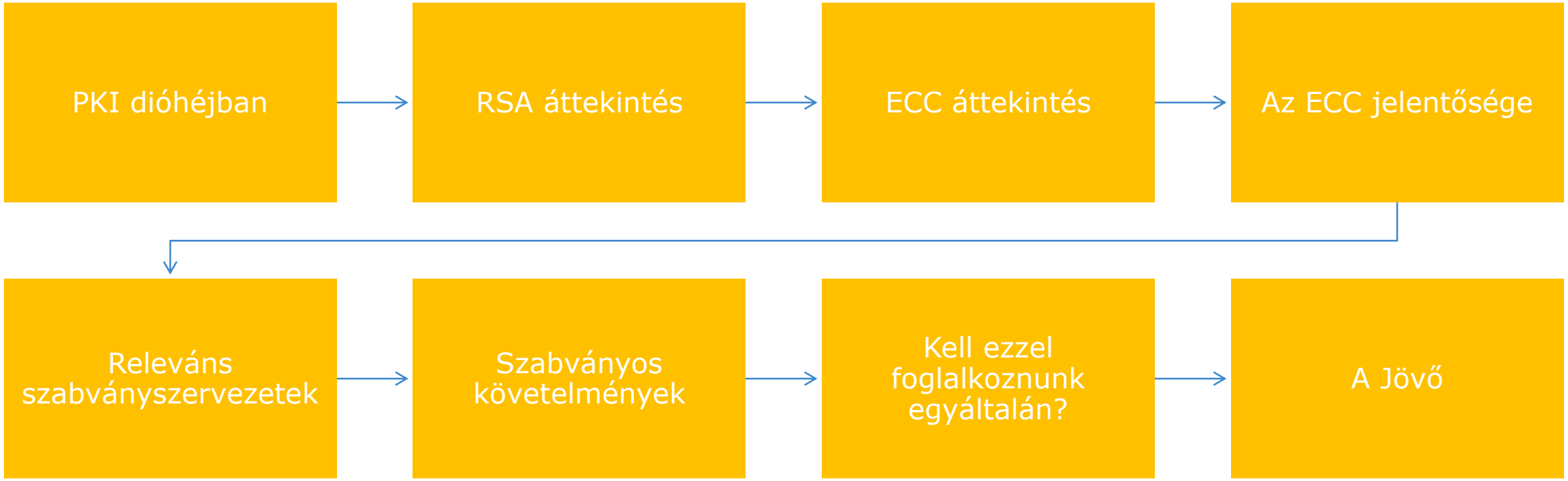
RSApokalipszis?

Meddig használhatjuk a megszokott algoritmusokat?

Rozgonyi Attila (Microsec)

Agenda


PKI dióhéjban
RSA áttekintés
ECC áttekintés
Az ECC jelentősége
Releváns szabványszervezetek
Szabványos követelmények
Kell ezzel foglalkoznunk egyáltalán?
A Jövő

PKI dióhéjban

- **magánkulcs** (csak a tulajdonos ismeri)
- **nyilvános kulcs** (bárki megismerheti)
- **aláírás** (hitelesítés): kódolás a magánkulccsal, ellenőrzés a nyilvános kulccsal
- **titkosítás**: kódolás a nyilvános kulccsal, visszafejtés a magánkulccsal
- *Csak akkor támaszkodhatunk egy nyilvános kulcsra, ha tudjuk, hogy ki birtokolja a hozzá tartozó magánkulcsot.*

PKI dióhéjban

- **Tanúsítvány**: aláírt igazolás arról, hogy egy nyilvános kulcs kihez tartozik
- **Hitelesítés-szolgáltató**: megbízható szervezet, kulcsokat és tanúsítványokat bocsát ki
- **Időbélyeg**: igazolja, hogy a dokumentum adott időpontban létezett
- **Időbélyegzés-szolgáltató**: időbélyegeket bocsát ki
- Jogszabály **bizonyító erő**t rendel hozzájuk

RSA áttekintés

- Algoritmust leíró első tanulmány: 1977
- Nagy számok prímtényezőkre bontásának problémáján (Integer Factorization Problem – **IFP**) alapul (egy nagy egész szám esetén nehéz megállapítani annak prímtényezőit)
  - Ha egy szám két nagy prímszám szorzata, akkor a faktorizáció erős számítógépekkel is beláthatatlan ideig tart.
- A mai napig világszerte elterjedt

MICROSEC

RSA áttekintés

1. Sorsoljunk ki két prímszámot: *p* és *q*
2. Szorozzuk össze őket: ***m*** = *p* * *q*
3. Számítsuk ki: *f* = *(p-1)* * *(q-1)*
4. Válasszunk egy ***e*** számot, amelynek nincs 1-nél nagyobb közös osztója *f*-fel (relatív prímek).
5. Számítsuk ki ***d***-t úgy, hogy ***e*** * ***d*** adjon 1 maradékot *f*-fel osztva!

Ekkor egy matematikai tétel szerint bármilyen *x* számra igaz, hogy:
$(x^{e})^{d}$ maradéka ***m***-mel osztva = *x*

Nyilvános kulcs: ***m*** és ***e*** számpár

Magánkulcs: ***d*** szám

MICROSEC

ECC áttekintés

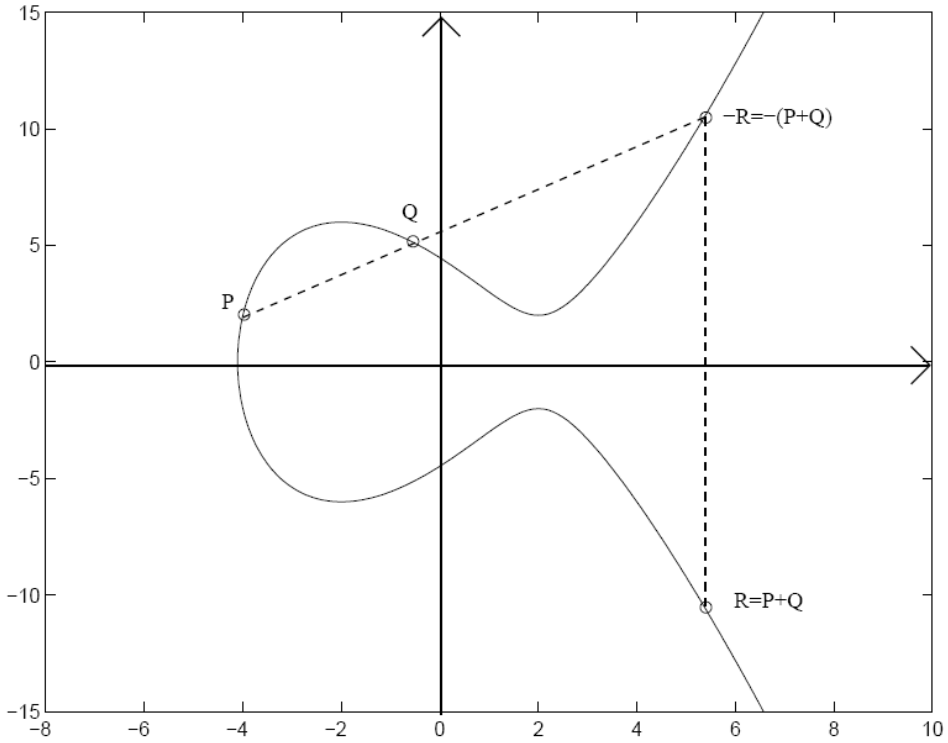
- ECC: Elliptikus görbéken alapuló kriptográfia (Elliptic Curve Cryptography)
- Egy elliptikus görbe a következő egyenlettel írható le:

$$y^2 = x^3 + ax + b$$

- Az elliptikus görbék pontjain matematikai műveleteket definiálhatunk:
- a görbe két pontjának összeadása
- a görbe egy pontjának szorzása egész számmal
- Ha Q a görbe egy pontja és k egész szám, akkor
  - Q és k*Q ismeretében
  - k meghatározása „nehéz” feladat. (Nem ismert rá hatékony algoritmus.)
- Ez az ún. diszkrét logaritmus probléma elliptikus görbéken értelmezett változata (ECDLP).

ECC áttekintés

geometriai definíció



algebrai definíció

$$x_3 = s^2 - x_1 - x_2$$
$$y_3 = s(x_1 - x_3) - y_1$$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

MICROSEC

Az ECC jelentősége

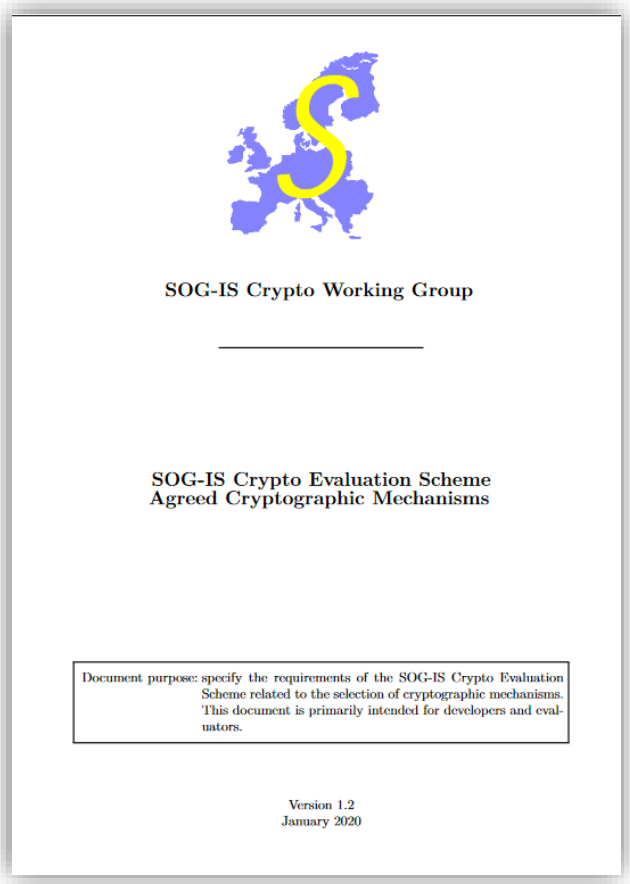
- Kisebb kulcsmérettel nyújt hasonló biztonságot, mint az RSA
- 2048 bit RSA ~ 224 bit ECC
- 3072 bit RSA ~ 256 bit ECC
- Igaz, nagyon-nagyon nehéz összehasonlítani két algoritmus biztonságát
- IFP (RSA): már a régi görögök is...
- ECDLP (ECC): 1985 óta (Koblitz, Miller)
- Kisebbek a kulcsok, de bonyolultabbak a műveletek
- Az ECC más alapokon nyugszik, mint az RSA
- Kriptográfiai alkalmazásokban nem valós számok feletti görbéket szokás alkalmazni (GF(p), GF(2^m)).

Releváns szabványszervezetek

- PKI területen rengeteg szabvány és szabványszervezet
  - Felhasználás célja, területi hatály stb. szempontjából különbözhetnek
- Az Európai Unióban (x19 xxx szabványcsalád):
- CEN (Comité Européen de Normalisation)
- **ETSI** (European Telecommunications Standards Institute)
- Globálisan:
- IETF (Internet Engineering Task Force) - pl. RFC 5280, RFC 6960 stb.
- ISO (International Organization for Standardization)
- CA/Browser Forum
- CSC (Cloud Signature Consortium)

Szabványos követelmények – SOG-IS Agreed Cryptographic Mechanisms

- SOG-IS egyezmény: 92/242/EEC (EGK Tanács határozat)
- Agreed Cryptographic Mechanisms: SOG-IS (Crypto Evaluation Scheme sémában) résztvevők által elismert kriptográfiai mechanizmusok meghatározása
- ETSI is erre a dokumentumra támaszkodik
- Legacy és recommended kategória
- Kétévente új verzió - idén esedékes



SOG-IS Crypto Working Group

SOG-IS Crypto Evaluation Scheme
Agreed Cryptographic Mechanisms

Document purpose: specify the requirements of the SOG-IS Crypto Evaluation Scheme related to the selection of cryptographic mechanisms. This document is primarily intended for developers and evaluators.

Version 1.2
January 2020

Szabványos követelmények – SOG-IS Agreed Cryptographic Mechanisms

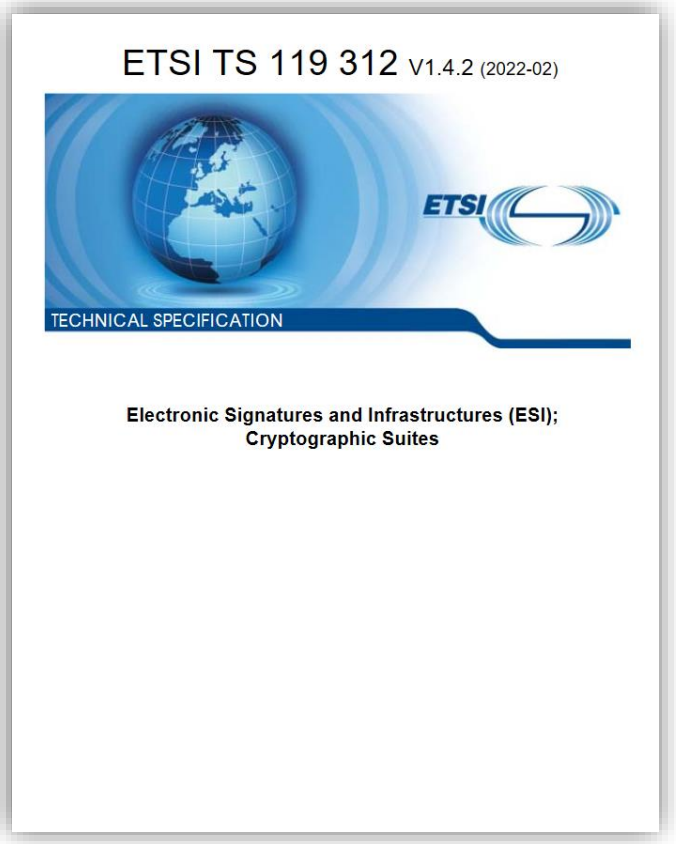
- 23. o Agreed RSA primitive sizes táblázat + 28. o, Agreed Digital Signature Schemes táblázat:
- **EC-DSA: Ajánlott**
- **RSA:**
  - 1900 > 3000 bites kulcsmérettel **2025-ig használható (gyakoribb)**
  - **3000 bites kulcsméret felett ajánlott**, de:
- RSA Padding:
  - PKCS#1v1.5 : **Default legacy, 2027-ig használható (gyakoribb)**
  - **PSS: Ajánlott**

Agreed RSA primitive sizes.

Primitive	Parameters' sizes	R/L	Notes
RSA	$n \geq 3000$, $\log_2(e) > 16$	R	
	$n \geq 1900$, $\log_2(e) > 16$	L [2025]	27-LegacyRSA

Szabványos követelmények – ETSI TS 119 312 (AlgoPaper)

- Az EU irányadó szabványa
- Leginkább SOG-IS követelményeken alapul
- Kétévente felülvizsgálat (+ rendkívüli esetben is – ilyenkor azonnali felülvizsgálat)
- Szintén véghatáridőket rendel az algoritmusokhoz



Szabványos követelmények – ETSI TS 119 312 (AlgoPaper)

- 9. táblázat:
- **ECDSA** szintén **ajánlott**
- **RSA-2048 szintén legkésőbb 2025 végéig használható** → három évre kiadott aláíró tanúsítványokat pl. már érinti januártól
- **PKCS#1v1.5 padding szintén legkésőbb 2027 végéig használható**

Table 9: Recommended signature suites for algorithm resistance during X years (was table 12 in version 1.1.1)

Entry name of the signature suite	1 year	3 years	6 years
sha256-with-rsa	≥ 1 900	≥ 1 900	not recommended
sha384-with-rsa	≥ 1 900	≥ 1 900	not recommended
sha512-with-rsa	≥ 1 900	≥ 1 900	not recommended
rsa-pss with mgf1SHA-256Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-384Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-512Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA3-Identifier	≥ 1 900	≥ 1 900	≥ 3 000
sha256-with-dsa	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	3 072
sha224-with-ecdsa	legacy		not recommended
sha2-with-ecdsa	recommended		
sha2-with-ecsdsa	recommended		
sha3-with-ecdsa	recommended		
sha3-with-ecsdsa	recommended		

Kell ezzel foglalkoznunk végfelhasználóként?

- Legfőképpen szolgáltatóra vonatkozó követelmények, de az esetleges problémák (pl. idő előtti törés stb.) elkerülése szempontjából már január előtt is érdemes:

- Olyan időbélyegzőt használnunk, amely már valamely biztonságos, jelenleg kivezetési időhatár nélkül használható **algoritmuson alapul**, mint pl. az **ECC.** Ha jelenleg nem ilyen megoldást használunk, érdemes a szolgáltatónál ECC alapú megoldás iránt érdeklődnünk.

- Olyan **aláírás-létrehozó és -ellenőrző programot** választanunk, amely képes az ECC algoritmus kezelésére. Amennyiben nem vagyunk biztosak abban, hogy a programunk képes-e ECC-t kezelni, használjuk az ingyenesen letölthető e-Szignó kliens program legfrissebb verzióját.

- Ha gyakran fogadunk be elektronikus aláírásokat vagy egyéb, időbélyegzett állományokat, **felkészülnünk** arra, hogy egyre több ECC alapú megoldással találkozunk majd, ugyanis a jövőben a szolgáltatóknak is kötelező lesz ezek alkalmazása.

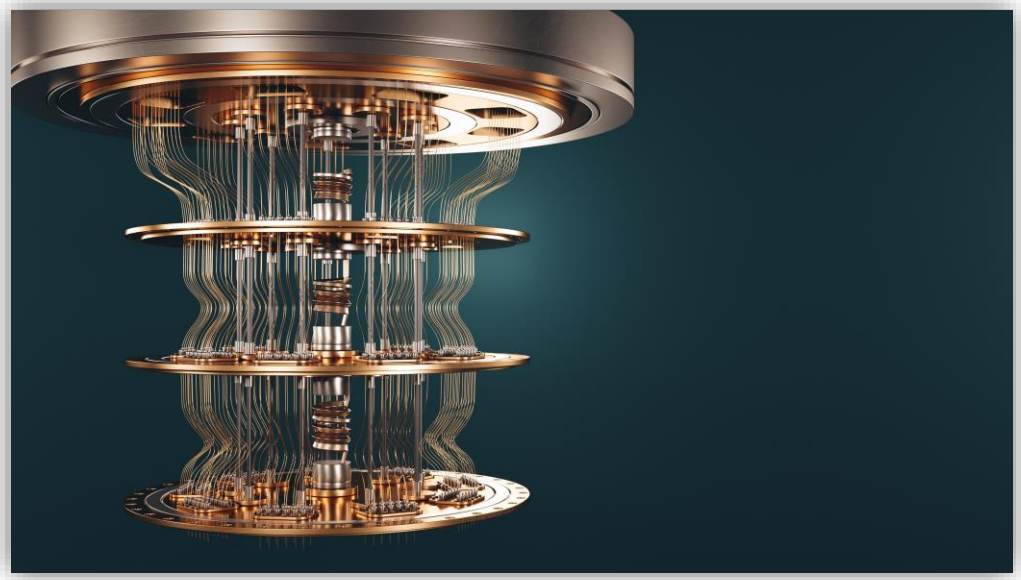
- Ha jelenleg RSA-2048 időbélyeget használunk, akkor a megőrzési célnak megfelelően a hosszú távú megőrzés biztosítása érdekében **elkezdenünk felülidőbélyegezni** ECC algoritmuson alapuló időbélyeggel az RSA-val időbélyegzett dokumentumainkat, ahol szükséges.

Microsec e-Szignó ECC alapú időbélyegző

- 2019 óta EC alapú időbélyegzés
- Évente 250.000.000 létrehozott időbélyeg
- Magas performancia (500 db/mp)
- 11 év érvényességi idő
- Demo időbélyegzés szolgáltatás: https://teszt.e-szigno.hu/tsa
- Performancia teszt: https://e-szigno.hu/idobelyeg-performancia-teszt

A Jövő

- Kvantumszámítógépek?
- IBM: 2025-re 4000 qubites hardver (jelenleg 127)
- Peter Shor (1994): *Shor's algorithm* – faktorizáció polinom időn belül
- ~5 év, mire mostani legacy kategóriás algoritmusok törhetnek
- Megoldás: poszt-kvantum kriptográfia (FALCON, Rainbow stb.)
  - NIST verseny: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions



Köszönöm a figyelmet!

Rozgonyi Attila

PKI szakértő

Microsec Zrt.

rozgonyi.attila@microsec.hu