Co je nového v oboru PKI

Vybrané téze

Ing. Miroslav Saferna
OIT

Národní úřad
pro kybernetickou
a informační bezpečnost

eIDAS – klíčové oblasti

nařízení Evropského Parlamentu a Rady (EU) č. 910/2014

(http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG)

- **Obsah kvalifikovaného certifikátu**

celého jména (CN) nově uváděno jak křestní jméno (G), tak příjmení (SN)

- položka **QCstatements**

(„prohlášení kvalifikovaného certifikátu“)

soukromý klíč umístěn v tzv. kvalifikovaném prostředku –QSCD

- **Vzájemná uznatelnost** (QC, QSCD)

„DE FACTO x DE JURE“

Erika Rumplíková <e.rumplikova@nukib.cz>

Národní úřad pro kybernetickou a informační bezpečnost

Vydal(a): I.CA Qualified 2 CA/RSA 02/2016

První certifikační autorita, a.s.

Platný od: 2017/08/16 15:11:45 +02'00'

Platný do: 2018/08/16 15:11:45 +02'00'

Zamýšlené použití: Digitální podpis, Neodvolatelnost, Ochrana e-mailu

Tento certifikát splňuje podmínky nařízení EU 910/2014, příloha I

Privátní klíč patřící k tomuto certifikátu je umístěn v zařízení QSCD (Qualified Signature Creation Device)

FIPS/NIST

- **FIPS 140-2** 03/2002

Security Requirements for Cryptographic Modules

- **FIPS 186-4** 10/2015

Digital signature standart (RSA 4096, DSA, ECC)

- **NIST Special Publication 800-133** 12/2012

Recommendation for Cryptographic Key Generation

https://csrc.nist.gov/publications/fips

O algoritmech

- Neexistuje žádný matematický důkaz, že daný algoritmus šifrovací metody je matematicky bezpečný
- Vědci jen spekulují, jak dlouho by bylo potřeba „strojového času“ k prolomení
- SHA -1. v první fázi 6500 let, v 2. fázi 110 let výkonu nejmodernějšího grafického procesoru

Google – spekulace jsou ošidné

$ sha1sum *
38762cf7f55934b34d179ae6a4c80cadccbb7f0a shattered-1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a shattered-2.pdf

RSA 2048 – dnes neuspokojivé

- SOG-IS Crypto Evaluation Scheme Agreed Cryptographic mechanism – v.1 z května 2016,
  - Str. 23, tabulka: Agreed RSA primitive sizes: Pro R se požaduje více než 3000 bitů.
  - Str. 11 nahoře: R – znamená Recommended (L znamená – legacy).

https://www.sogis.org/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.0.pdf

- Algorithms, key size and parameters report – 2014 ENISA (listopad 2014),
  - Str. 37, RSA problem, Future System Use, Near Term, 3072 b.,
  - Jinými slovy pro bezpečnost v blízké budoucnosti se doporučuje 3072b dlouhý RSA klíč.

https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report

Nově:

http://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

RSA 2048 – dnes neuspokojivé II.

- BSI-Technical Guide, BSI TR 02102-1, Cryptographic mechanism recommendation and Key lengths (leden 2018),
- Str. 24 – tabulka nahoře: 128 bitovou bezpečnost má RSA/DLP s délkou modulu 3200 bitů,
- Str. 25, třetí odstavec: Při zavádění nových systémů je potřeba používat větší délky asymetrických klíčů! Obvyklým požadavkem je dosažení 128 bitové bezpečnosti u všech komponent.

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=7

NSM Cryptographic Requirements

- STANDARD

RSA algorithm with key length of 2048 bits may be used until 2017-12-31.

- MODERATE(neutajované ale citlivé)

RSA algorithm with key length of 2048 bits may be used until 2019-12-31.

Note that the use of SHA-1 is not allowed

https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf

NÚKIB dnes doporučené algoritmy

- **ECC** s délkou klíče 384 a více
- Pokud je to možné **BRAINPOOL** křivky
- z bezpečnostního hlediska nejvhodnější vyšla ECC křivka: **brainpoolP384r1 (** kompromis**)**
- Prověřit „**Generátor náhodných čísel**“
- Nepoužívat **SHA-1**, případně (forezní audit) kombinovat s MD5

JAK NA TO ?

- Vhodný HSM
  - Např. **SafeNet Luna SA** (ECDSA, ECC Brainpool)
  - **SC4** HSM (Curve 25519)
- Vhodná karta (vč. kustomizace)
  - StarCos 3.5. (I.CA)
  - Gemalto (Java - Monet+)
- **Příslušný firmware (pkcs#11, csp knihovny)**

OpenSSL

- FIPS verze

  c:\OpenSSL\bin>openssl version

  OpenSSL 1.0.2j-fips 26 Sep 2016

- Libre SSL Verze 2.7.2
- OpenSSL Verze 1.1.1 beta3 TLS 1.3 (17.4.2018)

Seznam podporovaných křivek lze vypsat

C:\OpenSSL\bin>openssl ecparam -list_curves

C:\OpenSSL\bin>openssl list -public-key-algorithms

https://www.openssl.org/ http://www.libressl.org/

GUI nad OpenSSL

- XCA (multiplatformní) x509v3 extensions

  Windows, Linux , MAC

- Předpoklady pro SmardCard
  - OpenSC – driver čteček
  - PKCS#11 knihovny (firmware karet)
  - Personifikace karty (např. StarCos 3.5 pro ECC a CA)
- Ukázka použití (podle času a zájmu)
- Vhodné pro menší firmy

  http://hohnstaedt.de/xca/index.php

Enterprise GUI openXPKI

- ON Line RA/CA x509v3, openSSL a PERL
- Activ/Pasiv i Activ/Activ klastr
- WebUI s podporou všech hl. browserů
- Podpora HSM(např. Thales)
- Podpora SCEP a EST Enrollment Interface
- Konektory LDAP, SQL, WEB services..
- Podpora MySQL, Oracle,...
- Komerční support, školení a zákaznický vývoj

http://www.openxpki.org/ 100% OpenSource Apache2.0

FreeIPA

- Komplexní opensource řešení
- CA – DOGTAG (openssl, nss)
- RedHat DOGTAG nakonfiguroval s NSS (Mozilla)
- Default root a vydávající CA s RSA 2048
  (dnes již nedostačující bezpečnost)
- Jednáme s RedHat em o změně na ECC 384(512)

ROCA zranitelnost 10-2017

- **ROCA** se týkající se generování šifrovacích klíčů RSA v knihovně od Infineon Technologies AG
- Špatně napsaný Firmware – generátor náhodných čísel, postiženy i **TPM** čipy
- Postiženo Slovensko, Estonsko… – eObčanky

  Revokace všech dosud vydaných
- Otestováni

  https://keychest.net/roca#/

NSA BACK DOOR

- Diskreditace FIPS/NIST
- Problém přiznal MICROSOFT, CISCO, JUNIPER
- Problém i jistých ECC a to Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG)
- Edward Snowden 2013

https://www.wired.com/2013/09/nsa-backdoor/

https://www.infoworld.com/article/2608141/internet-privacy/snowden--the-nsa-planted-backdoors-in-cisco-products.html

https://www.schneier.com/blog/archives/2015/12/back_door_in_ju.html

Reakce NSA 8/2015

- Technicky podložené rozhodnutí

https://web.archive.org/web/20151123081120/https://www.nsa.gov/ia/programs/suiteb_cryptography

„V nejbližší době (blíže nespecifikováno) budou k dispozici kryptografické systémy odolné vůči kvantovým počítačům a pokud by někdo přecházel k Suite B eliptickým křivkám má počkat a přejít rovnou k těm odolným vůči kvantovým hrozbám, aby nevyhazoval peníze dvakrát za sebou.“

Reakce matematické veřejnosti

- https://jiggerwit.wordpress.com/2013/09/25/the-nsa-back-door-to-nist/

This article will be published in the *Notices of the American Mathematical Society*

- Detailně popsaná problematika a spekulace nad důvody NSA

https://eprint.iacr.org/2015/1018.pdf

IACR - International Association for Cryptologic Research

https://www.root.cz/clanky/vestime-co-dokaze-nsa-rozlousknout/

- Vyzývá k revizi Suite B a …

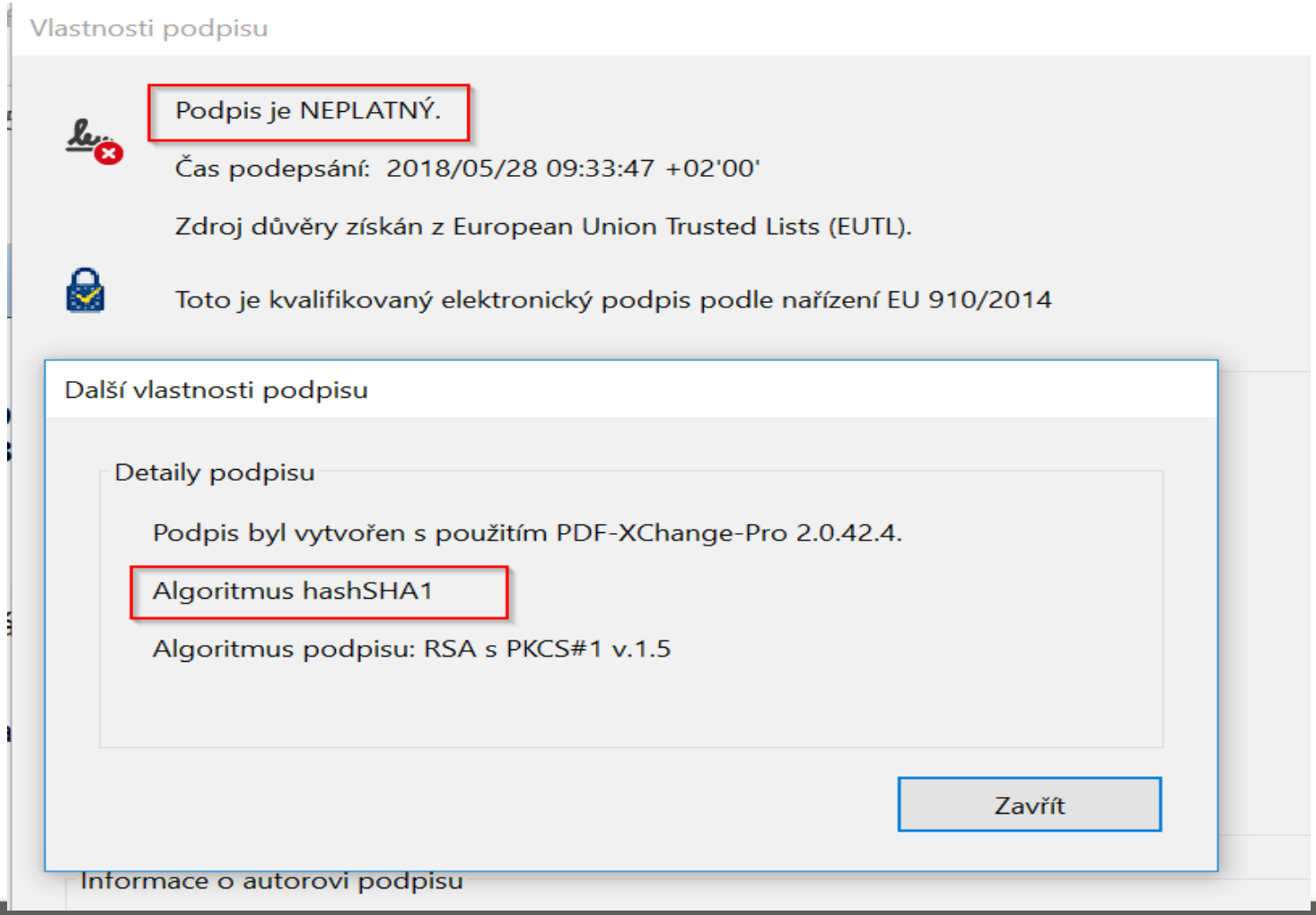
„…**Revised Suite B allows 3072-bit RSA but only P-384 and not P-256 for ECC…**“

Reakce IT světa

- SHA-1 2017 - konec v Chrome, Firefoxu, Safari i MS Explorer a Edge
- DNSSEC přechod od RSA k ECDSA (2017-2018)
- OpenSSH – Curve25519 na základu ECDH (2014)
- TSL 1.2, 1.3 - Curve25519
- Curve25519

https://www.root.cz/clanky/bernsteinovy-elipticke-krivky/

Prakticky Acrobat Reader DC



Google DNS s algoritmem 25519

- Známá služba Google Public DNS oznámila podporu validace DNSSEC podpisů využívajících algoritmus Ed25519. Použití tohoto algoritmu v DNSSECu bylo standardizováno v RFC 8080, které vyšlo v únoru 2017.
- Až doposud byly v DNSSECu podporovány pouze eliptické křivky z dílny amerického Národního ústavu standardů a technologie (NIST), konkrétně křivky P-256 a P-384, přičemž první jmenovaná je zároveň nejpoužívanější křivka v českém DNSSECu, na kterou v červnu přešla i celá doména .cz
- Algoritmus Ed25519 je založen na křivce Curve25519, kterou navrhl tým odborníků v čele s Danielem J. Bernsteinem.

Výhody křivky Curve25519, 448

První vlastností je rigidnost výběru parametrů křivky.

Křivka je imunní proti **časovým, hyperthreading a cachovacím postranním kanálům**, protože se implementace **vyhýbá větvení závislém na vstupu**, nepoužívá indexy pole závislé na vstupu ani jiné instrukce s časováním závislým na vstupu.

https://cs.wikipedia.org/wiki/Curve25519, https://cr.yp.to/ecdh.html,

Seznam uživatelů https://

https://ianix.com/pub/curve25519-deployment.htmlR

RFC 8080

Soft HSM projekt openDNSSEC

- V rámci projektu openDNSSEC vznikl Soft HSM
- Je bezpečné použít Soft HSM pro ROOT CA ?

https://www.opendnssec.org/2017/07/softhsm-2-3-0

HSM a JAVA API

- Oracle poskytuje knihovnu PKCS#11 v rámci Java Cryptographic API.
- Většina HSM používá JAVA API ve svých HSM
- Je známo, že Thales nCipher HSM ji používá také
- Java Crypto API keytool – export PK ?

https://security.stackexchange.com/questions/51691/root-certificate-from-an-ca-company-which-can-be-encrpyted-by-softhsm

HSM Thales ?

Postup generování a přenos chráněných pomocí HSM klíčů pro Azure Key Vault

How to generate and transfer HSM-protected keys for Azure Key Vault

Pro jistotu při použití Azure Key Vault, můžete importovat nebo generovat klíče v modulech hardwarového zabezpečení (HSM), které nikdy neopustí hranice modulu hardwarového zabezpečení. Tento scénář se často označuje jako *přineste si vlastní klíč*, nebo BYOK. Moduly hardwarového zabezpečení jsou ověřené podle standardu FIPS 140-2 Level 2. Služba Azure Key Vault využívá moduly hardwarového zabezpečení Thales nShield řady chrání vaše klíče.

Pomocí informací v tomto tématu vám pomohou plánovat, generovat a potom přeneste svůj vlastní klíče chráněné HSM pro použití s Azure Key Vault.

Tato funkce není dostupná pro Azure China.

Post kvantové algoritmy Microsoft

- Microsoft přidal do openVPN post-kvantové kryptografické algoritmy

  https://github.com/Microsoft/PQCrypto-VPN

- Práce jsou sponsorována Microsoft Research Security and Cryptography, jako část post-quantum cryptography projectu.

US Federal Goverment - dnes

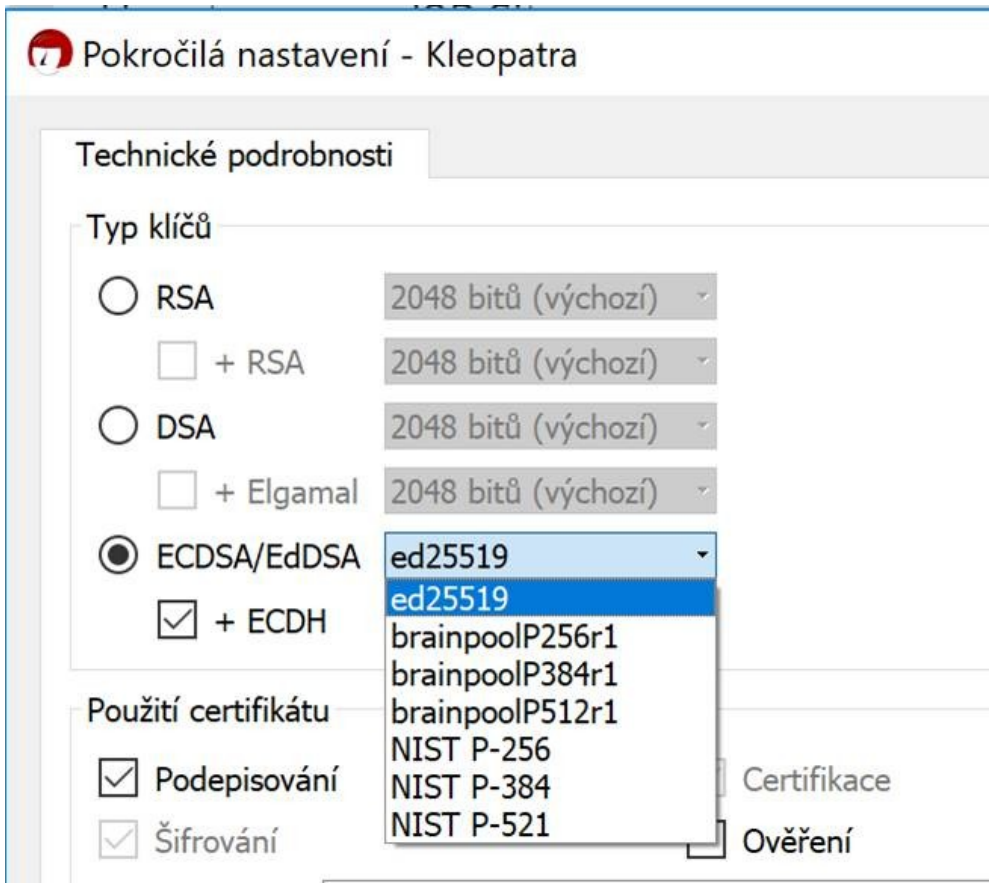
In 2017, NIST announced that

Curve25519 and **Curve448** would be added to **Special Publication 800-186**,

which specifies approved elliptic curves for use by the US Federal Government.

Both are described in RFC 7748

GPG - dnes




```
C:\Users\safm>gpg --full-generate-key --expert
gpg (GnuPG) 2.2.6; Copyright (C) 2018 Free Softu
This is free software: you are free to change a
There is NO WARRANTY, to the extent permitted by

Prosím, vyberte druh klíče, který chcete:
   (1) RSA a RSA (implicitní)
   (2) DSA a Elgamal
   (3) DSA (pouze pro podpis)
   (4) RSA (pouze pro podpis)
   (7) DSA (nastavit si vlastní použití)
   (8) RSA (nastavit si vlastní použití)
   (9) ECC a ECC
   (10) ECC (pouze pro podpis)
   (11) ECC (nastavit si vlastní použití)
   (13) Existující klíč
Váš výběr? 9
Prosím, vyberte, kterou eliptickou křivku chcete
   (1) Curve 25519
   (3) NIST P-256
   (4) NIST P-384
   (5) NIST P-521
   (6) Brainpool P-256
   (7) Brainpool P-384
   (8) Brainpool P-512
   (9) secp256k1
Váš výběr?
```

Státní správa - dnes

- Státní portály na http (ARES, RUIAN)- změnit na https
- Spisová služba (staré verze PDF konvertoru založené na SHA-1)

takový e-podpis je označen jako neplatný, aktualizovat konvertory, aby nepoužívaly SHA-1

- NEN – aktualizovat Metodické pokyny – „Principy práce s certifikáty v NEN“ z pohledu eIDASu (pfx, p12) – export a toto:

…Privátní klíč by měl mít k dispozici pouze minimálnímu počtu osob a měl by být do doby otevírání nabídek bezpečně uložen …

…Použití certifikátu v rámci otevírání nabídek v systému NEN znamená jeho použití jednotlivými členy komise otevírání nabídek. Případně sdělení PINu/hesla při použití tokenu nebo systémového úložiště.

Evropa dnes

- V Německu vznikne agentura pro kybernetickou bezpečnost
- Německo je znepokojeno svou závislostí na amerických technologiích poté, poté co E.S. odhalil rozsáhlé tajné sledování komunikace lidí americkou NSA.
- Horst Seehofer – ministr vnitra 29.8.2018

https://www.novinky.cz/internet-a-pc/bezpecnost/481902-v-nemecku-vznikne-agentura-pro-kybernetickou-bezpecnost.html

Závěr

Budoucnost je v ECC.

Variantní jsou typy křivek.

Rigidní bezpečné parametry.

(Ne)máme vhodné karty

a k nim dostupný FirmWare.

Dny RSA jsou sečteny.

Děkuji za pozornost

15.11.2018

m.saferna@nukib.cz

Zpracováno pro ors.slu.cz