MONET +

Výzvy postkvantové kryptografie v praxi

Mgr. Anežka Pejlová
Security Architect

Něco o MONET+

25+
Let na trhu

350+
zákazníků

300
zaměstnanců

6
Technologických divizí

€ 20 million
Obrat v roce 2022

20+
Zemí, ve kterých pracujeme

solutions by MONET+

Technologie

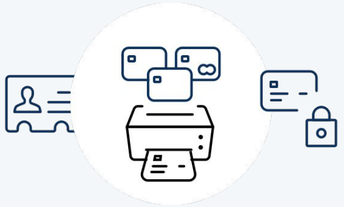
PKI

EMV platby

Smart cards

Mobile ID

Federované ID



Perso lab

solutions by **MONET +**

solutions by MONET+

Postkvantová kryptografie

Co je postkvantová kryptografie?

Výzva č. 1

solutions by MONET +

Postkvantová kryptografie (PQC)

- Kryptografie odolná vůči útokům o kvantové výpočetní síle
- využívá “těžké” problémy z jiných oblastí matematiky
  - samoopravné kódy
  - mřížky
  - hashovací funkce
  - polynomiální rovnice více proměnných
  - isogenie supersingulárních EC
- PQC algoritmy jsou proveditelné na klasických počítačích
  - vs. kvantová kryptografie

Dopady do klasické kryptografie

- Shorův algoritmus (1994)
  - Faktorizace přirozených čísel (RSA)
  - Diskrétní logaritmus (EC)
  - => Diffie-Hellman výměna klíčů

- Groverův algoritmus (1996)
  - Prohledávání stavového prostoru (délky klíčů, kolize)

Asymetrická kryptografie

Symetrická kryptografie

Které algoritmy použít?

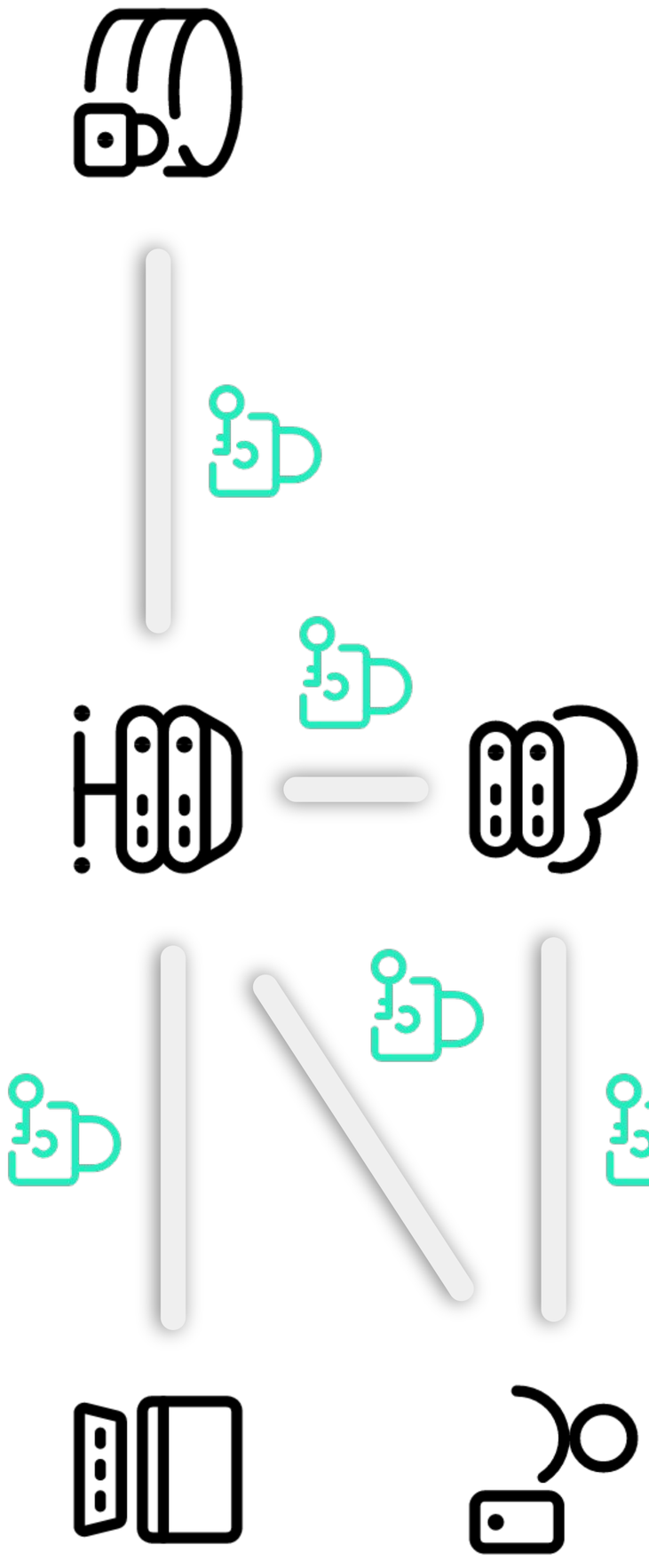
Výzva č. 2

NIST PQC Standardization

- 2016 - 23 podpisových + 59 PKE/KEM kandidátů
- 2022
  - vybrané algoritmy
    - podpisy (CRYSTALS-Dilithium, FALCON, SPHINCS+)
    - PKE/KEM (CRYSTALS-Kyber)
  - Round 4 pro “nemřížkové” PKE/KEM (BIKE, Classic McEliece, HQC)
  - Round 1 pro další podpisové algoritmy (40 kandidátů)
- 2023 - draft standardů
  - ML-DSA (CRYSTALS-Dilithium), SLH-DSA (SPHINCS+)
  - ML-KEM (CRYSTALS-Kyber)

Kde a co budeme měnit?

Výzva č. 3



Cryptographic inventory & Cryptoagility

- Aktivita identifikující všechna místa a účely, kde a proč je jaká kryptografie v systému použita
- Prerekvizita pro plánování a prioritizaci migrace
- Nejen kód, ale i dokumentace

- Design podporující rychlou adaptaci na nové kryptografické primitivy bez zásadních změn do systému
- Ideál - “drop-in” náhrady
- Pro kvantově zranitelné algoritmy prakticky nemožné

migration playbook

Půjde provést jednoduchou záměnu?

Výzva č. 4

solutions by MONET +

Velikost klíčů a podpisů/zpráv

RSA

EC

DH

ECDH

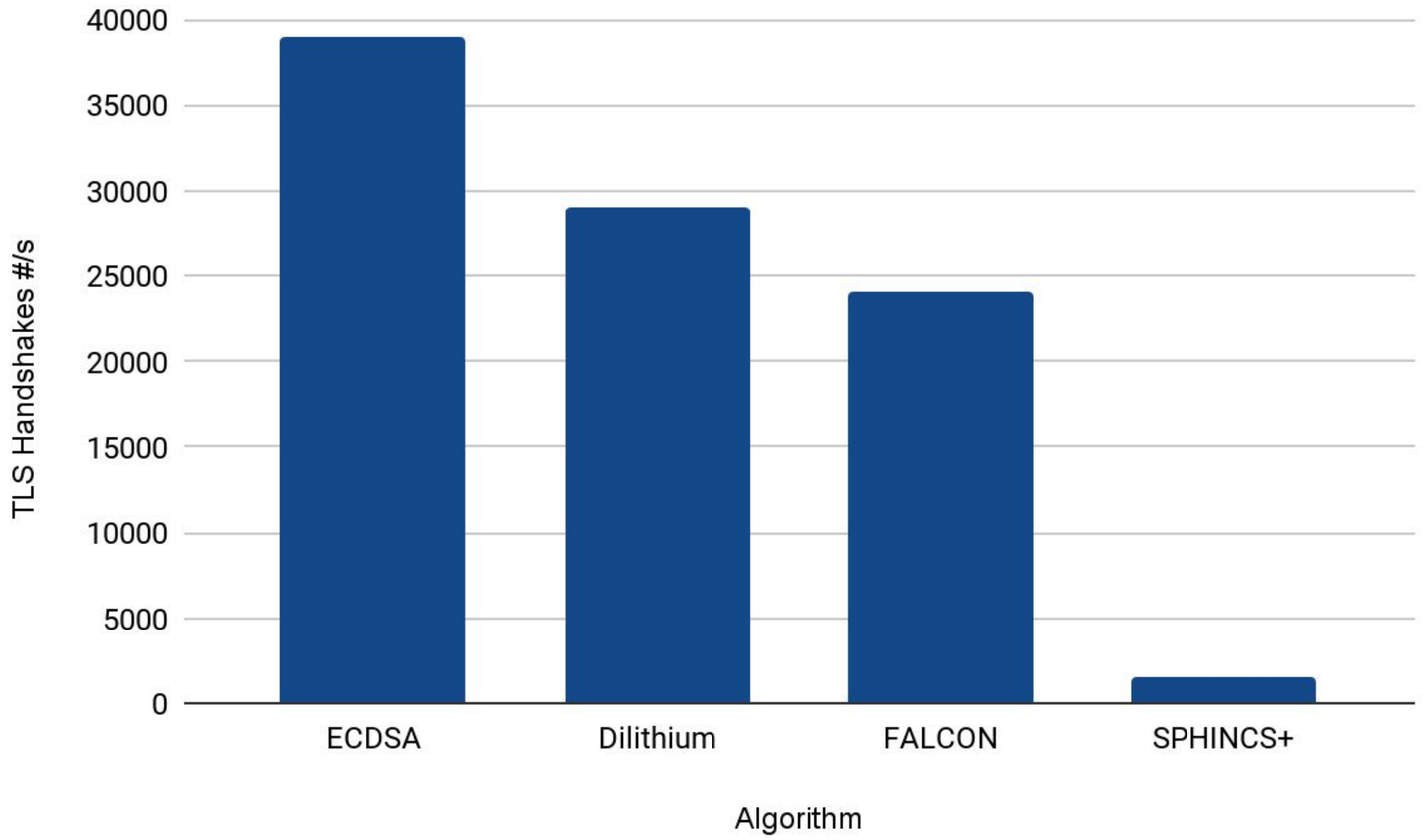
Dilithium 3x 2x

FALCON 3x

SPHINCS+ 8x

KYBER 4,5x

Rychlost generování podpisů



Porovnání klasických a PQ algoritmů

- Značně se liší v parametrech
  - Velikost klíčů i zpráv/podpisů
  - Rychlost operací
  - Výkon a škálování implementace
- Různé aplikace <= různé PQ algoritmy stejného typu

- Komplikovaná aktualizace v HW komponentách

Jak budeme migrovat?

Výzva č. 5

Migrační strategie

- Přímá
  - Výměna klasického algoritmu za PQC
  - Jednodušší, lepší integrace, efektivnější
  - Pokud důvěřujeme PQC
- Hybridní
  - Výměna za složený podpis klasický+PQC
  - Concatenated vs. Nested vs. Composite
  - Odolné vůči prolomení jednoho z přístupů
  - Komplikovaná interoperabilita

Jak se k tomu tedy postavit?

Výzva č. 6

Mosca’s Theorem

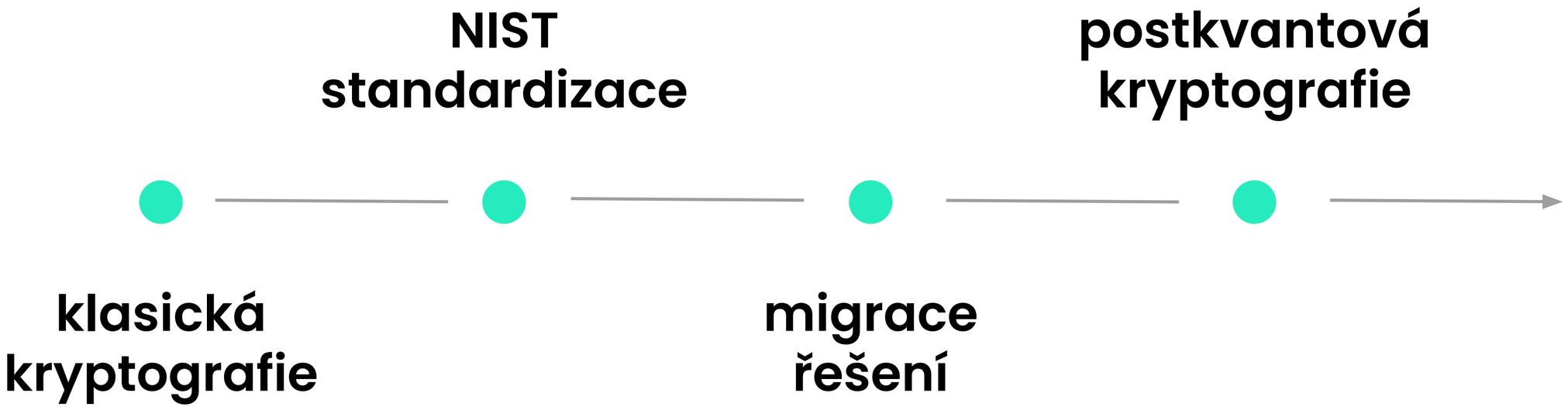
Y = Migration Time

X = Security Shelf life

Z = Time to compromise

Pokud X + Y > Z pak může dojít ke kompromitaci!

Timeline



PQC v praxi

MONET +

Signal

ENTRUST

chrome

Děkuji!

Potřebujete vyřešit kryptografii
ve vaší organizaci?

Kontaktujte nás.

www.proid.cz | info@proid.cz