vshosting

NIS2

Praktická příprava, technicky i právně

Václav Steiner

+420 246 035 835

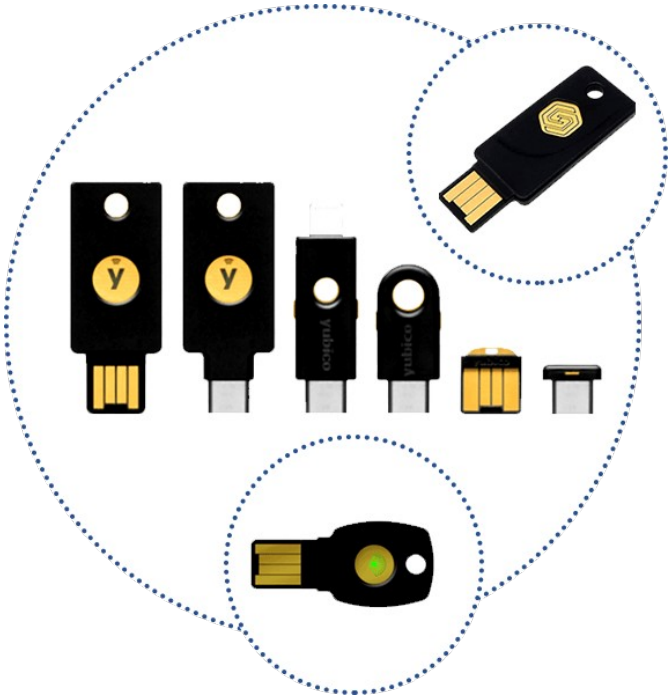
konzultace@vshosting.cz

vshosting

Hesla dle NIS2

- STRIKTNĚJŠÍ PRAVIDLA PRO POUŽÍVÁNÍ HESEL
- PRAVIDLO 12-17-22
- PRAVIDLA PRO ZMĚNU HESLA + ČASOVÉ ROZMEZÍ
- » PŘIHLAŠOVÁNÍ POMOCÍ DVOUFAKTOROVÉ AUTENTIZACE, EV. POMOCÍ KRYPTOGRAFICKÝCH KLÍČŮ/CERTIFIKÁTŮ

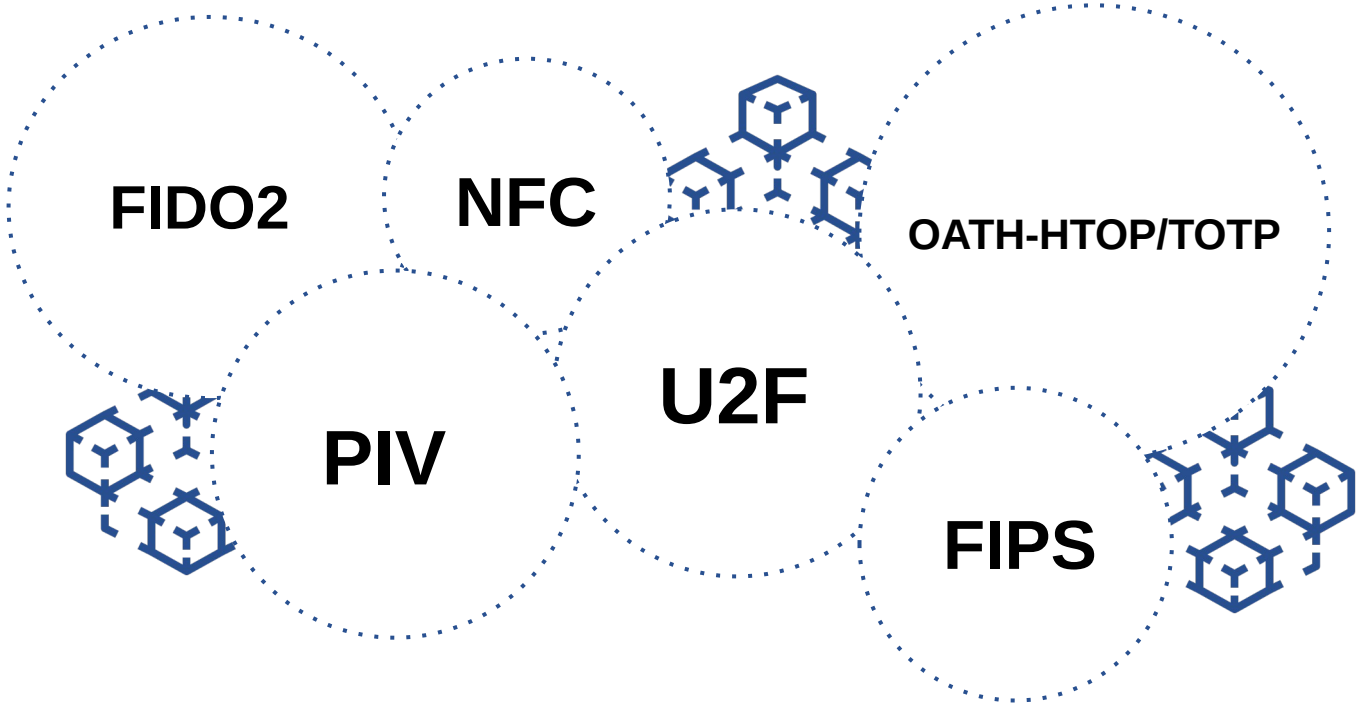
Bezpečnostní tokeny



- GOTRUST IDEM KEY
- YUBIKEY SECURITY KEY
- YUBIKEY 5, YUBIKEY 5 NANO, YUBIKEY BIO
- FEITIAN EPASS, FEITAN BIOPASS
- A DALŠÍ...

V čem se liší?

Zkratky a technologie



Původní token

- GEMALTO IDBRIDGE K50 USB TOKEN
- OPENPGP KARTA
- PRIVÁTNÍ KLÍČ ULOŽEN JEN V KLÍČENCE
- ODEMČENÍ POMOCÍ PIN KÓDU

NAŠE POUŽITÍ:

- PRO PŘIHLÁŠENÍ NA LINUXOVÉ SERVERY, ALGORITMUS RSA-3072
- ŠIFROVÁNÍ E-MAILŮ POMOCÍ PGP

Nový bezpečnostní token

YUBIKEY 5 NFC (USB-A / USB-C)

- SSH KLÍČ S ALGORITMEM ED25519
- ZVÝŠENÍ BEZPEČNOSTI, RYCHLEJŠÍ PŘIHLÁŠENÍ K SERVERŮM
- I NADÁLE MOŽNOST ŠIFROVAT E-MAILY
- \+ DVOUFAKTOROVÁ/VÍCEFAKTOROVÁ AUTENTIZACE

FIDO2

- VYCHÁZÍ Z FIDO U2F
- CTAP (CLIENT TO AUTHENTICATOR PROTOCOL)
  WEBAUTHN (OVĚŘOVÁNÍ NA WEBU)
- \+ RŮZNÉ ÚROVNĚ CERTIFIKACE (L1, L2, L3)

PROČ JE FIDO2 OBLÍBENÉ?

- ASYMETRICKÁ KRYPTOGRAFIE
- FYZICKÝ PŘÍSTUP K TOKENU
- PIN NEBO BIOMETRIKA

Jak funguje FIDO2

- REGISTRACE TOKENU
- AUTENTIZACE

Keycloak

- OPEN SOURCE IDENTITY AND ACCESS MANAGEMENT

https://www.keycloak.org/

REALIZUJE

1. REGISTRACI TOKENU + VAZBU NA OPRÁVNĚNÍ
2. PŘIHLAŠOVÁNÍ K WEBOVÝM SLUŽBÁM

K čemu dalšímu token použít?

- PŘIHLAŠOVÁNÍ DO SVÉHO PC
- ODEMYKÁNÍ ZAŠIFROVANÉHO DISKU
- ODEMYKÁNÍ KLÍČENKY S HESLY
- ŠIFROVÁNÍ E-MAILŮ

K ČEMU NELZE?

- ULOŽENÍ KVALIFIKOVANÉHO CERTIFIKÁTU

vshosting

Prostor pro dotazy

Václav Steiner

+420 246 035 835

konzultace@vshosting.cz

vshosting