

# PostSignum QCA

**Kvalifikovaný certifikát, zkušenosti**

**Lukáš Jakubík  
FI MU  
2010**



# [ Motivace ]

---

- Kvalifikovaný certifikát umožňuje vytvořit zaručený elektronický podpis osoby nebo organizace podle zákona
- Použití pro fyzické osoby a podnikatele
  - komunikace se státní správou,
  - elektronické podání předcházející podání papírovému...
- Legislativa
  - § 227/2000 Sb. v znění novel, o elektronickém podpisu
  - vyhláška 496/2004, o elektronických podatelkách...

# Kvalifikovanost certifikátu

- § 11 zákona 227/2000 Sb. v znění 226/2002 Sb.
  - *V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb. To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je zaručený elektronický podpis založený na kvalifikovaném certifikátu užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná.*

# [ PostSignum



- CA vlastněna Českou poštou, s. p.
- Jedna ze tří kvalifikovaných CA registrovaných a akreditovaných ministerstvem informatiky, posléze ministerstvem vnitra
- Vydává kvalifikované certifikáty od 9/2005 a kvalifikované časové razítka od 7/2009
- Výhody
  - MPSV identifikátor – pseudonymní unikátní číslo klienta vůči MPSV, FÚ, ČSSZ a ÚP
  - od 5/2010 zařazena do seznamu Microsoft kořenových CA
  - rozšířenost a dostupnost na poštách s CzechPOINTem
  - levnější služby, známé prostředí

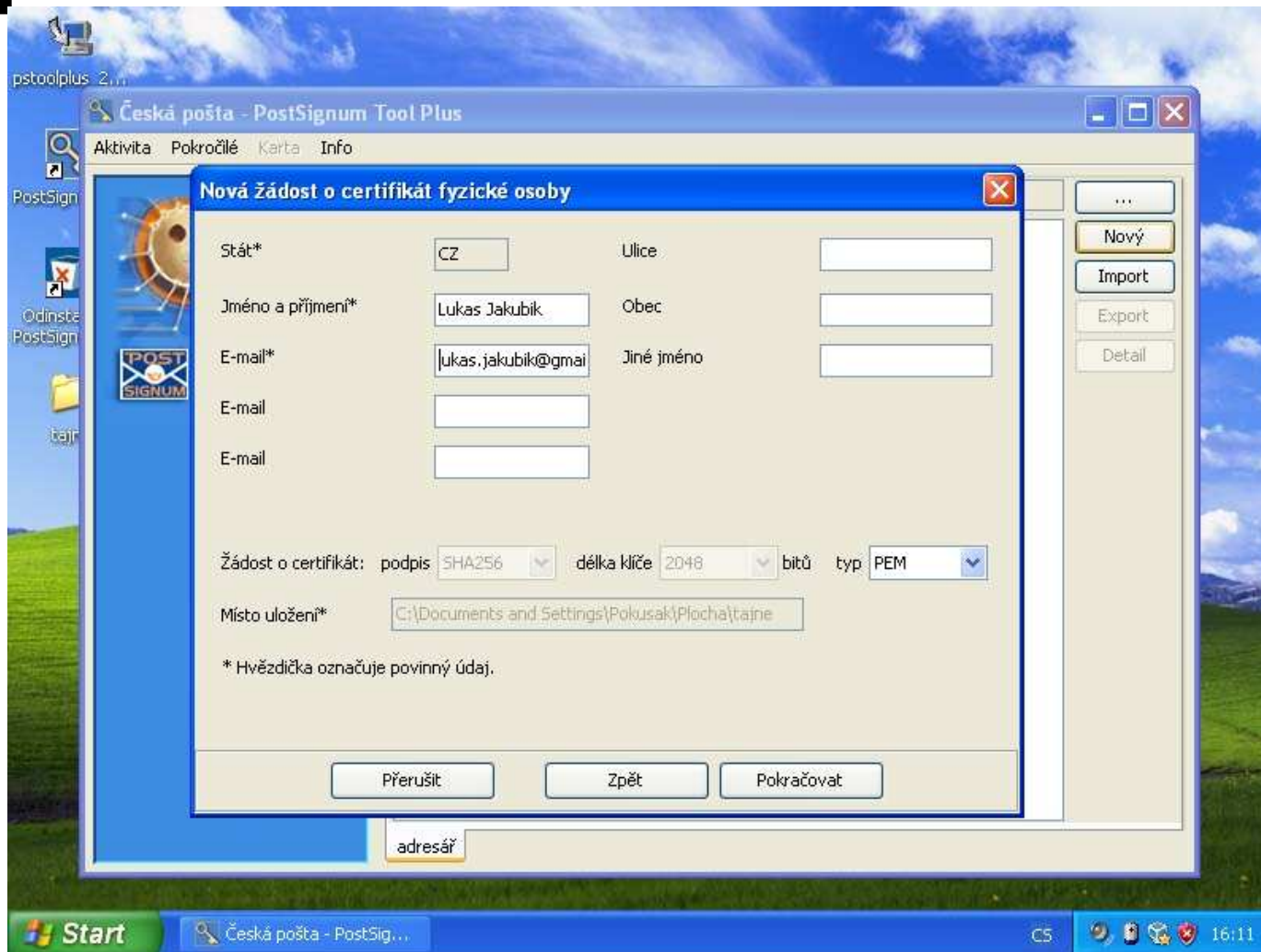
# [ Požadavky k vydání certifikátu ]

- vygenerovaný klíčový pár (online přes IE / offline)
- elektronická žádost o certifikát s veřejným klíčem podepsaná párovým soukromým klíčem (CMS)
- 2 vyplněné kopie smlouvy o poskytování certifikačních služeb s Českou poštou
- 2 vyplněné papírové formuláře, co bude uvedeno v polích certifikátu
- 2 doklady
- voucher / hotovost / maxkarta
- čas

# Generování klíčů a žádosti

- online generování v IE (raději) netestováno
- offline PostSignum Tool Plus je portabilní aplikace dostupná pro Win, Linux a MacOS běžící nad JRE
- je určena na generování klíčových páru a posléze žádostí o certifikát všech typů, které PostSignum vydává
- používá známe souborové struktury podle PKCS, skryté v adresáři chráněném heslem
- ~ šifrované “adresářovým heslem”
- heslo načteno v paměti během práce s programem

# Prostředí programu, Windows



# [ Obsah složky s klíči a žádosti ]

Address: Z:\certifikaty2010\ps05nastroje\tajne

File and Folder Tasks

Other Places

Details

**tajne**  
File Folder  
Date Modified: 24. října 2010, 10:34

5 objects (plus 2 hidden)

cert\_sign\_Lukas\_Jakubik\_1287670313852.ppk  
cert\_sign\_Lukas\_Jakubik\_1287670313852.req  
dir.info  
pair\_sign\_Lukas\_Jakubik\_1287670313852.p12  
user.info

cert\_sign\_Lukas\_Jakubik\_1...0\ps05nastroje\tajne) - GVIM

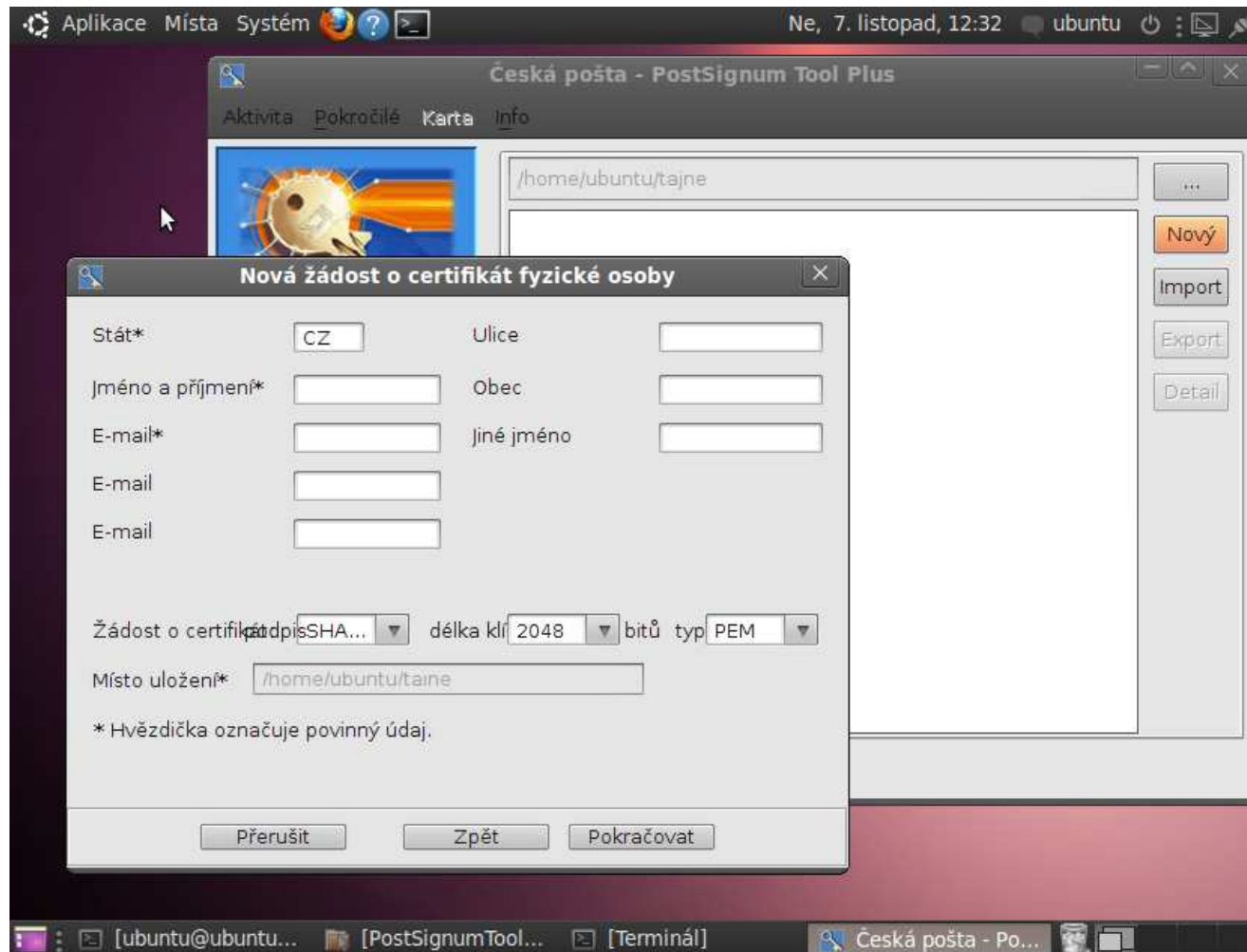
```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: DES-EDE3-CBC,D19DEC04872C07E7  
[  
X6vT9J401PiuJ6Au19jVBSewuNWqLnznFiU/8nIJ88W+qtpaUQX1Dm+WayDaJX  
4,0-1 Začátek
```

user.info (Z:\certifikaty...\ps05nastroje\tajne) - GVIM1

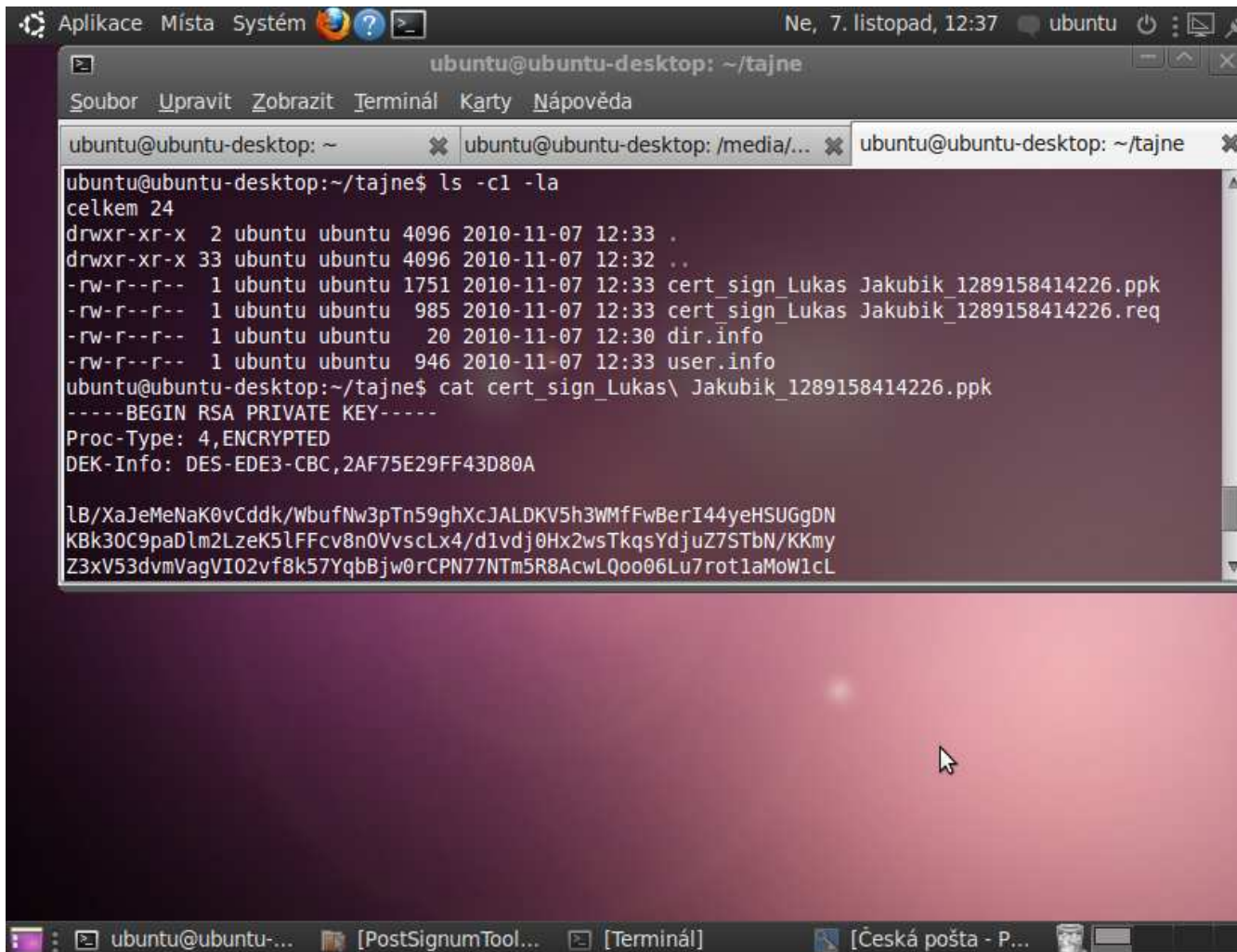
```
inputGroupq^@^@AL^@^@LinutID0sobyq^@^@AL^@^@NinputIDSkupinyq^@^@  
^@AL^@^@0inputIDZarizeniq^@^@AL^@^@ inputKompq^@^@AL^@^@HinputOrg  
q^@^@AL^@^@MinutOrgCisloq^@^@AL^@^@PinutOrgCisloExtq^@^@AL^@^@  
LinutOrgUnitq^@^@AL^@^@ inputPracq^@^@AL^@^@NinputPracCislo  
q^@^@AL^@^@MinutPracFuncq^@^@AL^@^@WinutRozlisujiciOrgUnitq^@^@  
^@AL^@^@ inputStatq^@^@AL^@^@FsigAlgt^@^@Vlcz/i/crypto/SignAlgEnum;  
xp^@^@H^@^@t^@^@Wcert_sign_Lukas_Jakubikt^@^@t^@^@t^@^@G [IÁŠ ]q^@^@  
~^@^@Et^@^@CPEMt^@^@CIÁSt^@^@t^@^@t^@^@Wlukas.jakubik@gmail.comt^@^@t^@^@  
^@t^@^@t^@^@q^@^@Eq^@^@Et^@^@t^@^@q^@^@Ft^@^@t^@^@t^@^@MLukas  
Jakubikt^@^@t^@^@q^@^@Et^@^@BCZ~r^@^@Wcz.i.crypto.SignAlgEnum^@^@t^@^@  
^@^@t^@^@R^@^@xr^@^@Njava.lang.Enum^@^@t^@^@t^@^@R^@^@xpt^@^@FSH  
A256  
2,191-242 Konec
```



# Prostředí programu, Ubuntu



# Obsah složky s klíči a žádosti



```
ubuntu@ubuntu-desktop: ~/tajne
Soubor Upravit Zobrazit Terminál Karty Nápověda

ubuntu@ubuntu-desktop: ~
ubuntu@ubuntu-desktop: /media/...
ubuntu@ubuntu-desktop: ~/tajne

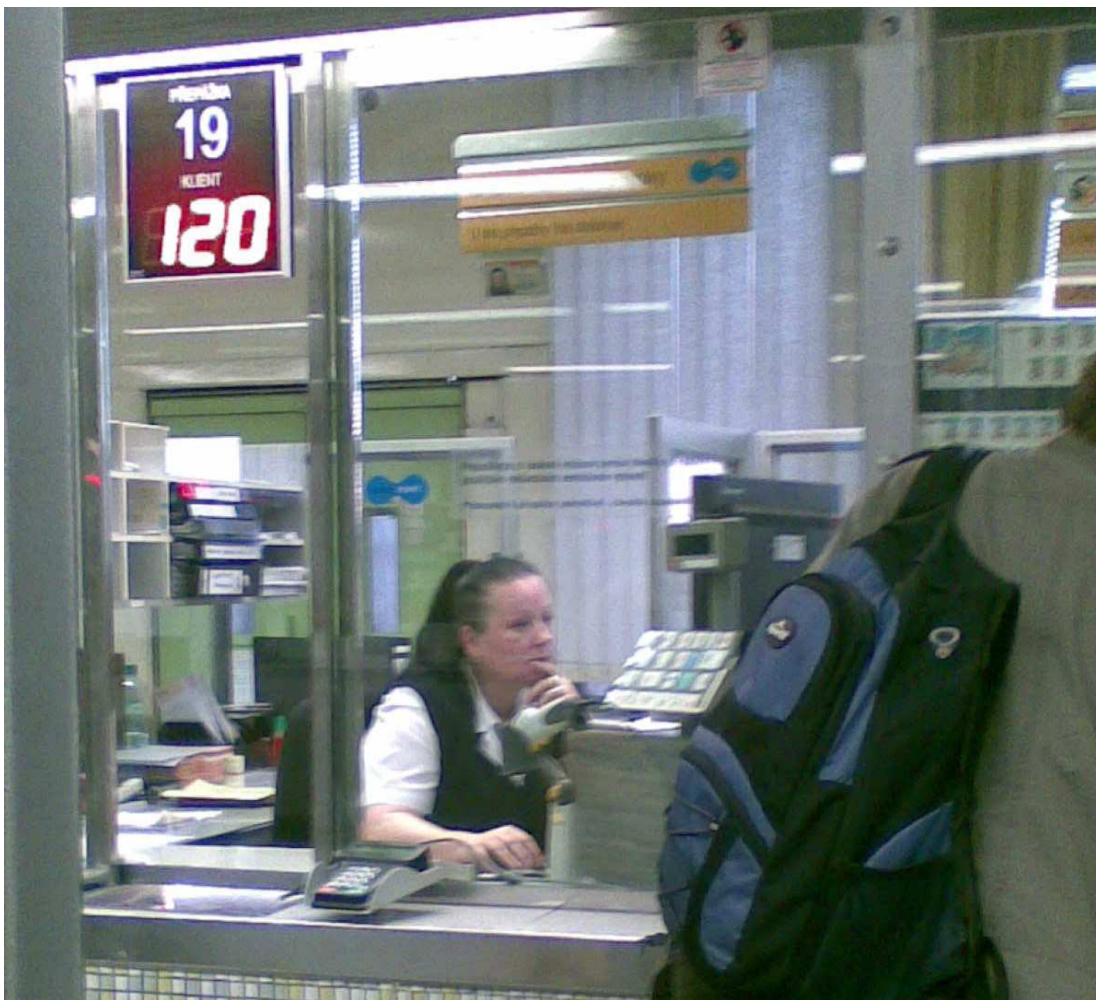
ubuntu@ubuntu-desktop:~/tajne$ ls -cl -la
celkem 24
drwxr-xr-x  2 ubuntu ubuntu 4096 2010-11-07 12:33 .
drwxr-xr-x 33 ubuntu ubuntu 4096 2010-11-07 12:32 ..
-rw-r--r--  1 ubuntu ubuntu 1751 2010-11-07 12:33 cert_sign_Lukas_Jakubik_1289158414226.ppk
-rw-r--r--  1 ubuntu ubuntu  985 2010-11-07 12:33 cert_sign_Lukas_Jakubik_1289158414226.req
-rw-r--r--  1 ubuntu ubuntu   20 2010-11-07 12:30 dir.info
-rw-r--r--  1 ubuntu ubuntu  946 2010-11-07 12:33 user.info
ubuntu@ubuntu-desktop:~/tajne$ cat cert_sign_Lukas\ Jakubik_1289158414226.ppk
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,2AF75E29FF43D80A

lB/XaJeMeNaK0vCddk/wbufNw3pTn59ghXcJALDKV5h3WMfFwBerI44yeHSUGgDN
KBk30C9paDl2LzeK5lFFcv8n0VvscLx4/d1vdj0Hx2wsTkqsYdjuZ7STbN/KKmy
Z3xV53dvmVagVI02vf8k57YqbJw0rCPN77NTm5R8AcwLQoo06Lu7rot1aMoW1cL
```

# [ Podání žádosti o certifikát ]

- žádost o certifikát se podává osobně
- zaměstnankyně zkontroluje papírové náležitosti, doklady (zhotoví kopie) a ve svém systému
  - vyplní smluvní strany i pro budoucí spolupráci
  - vyplní žádost o certifikát podle formuláře
  - nahraje z USB flash disku elektronickou žádost
  - vyplní složité revokační heslo
  - vystaví potvrzení o vydání certifikátu s vytištěným revokačním heslem 😊
  - usmívá se a docela jí to jde (2 úspěchy z cca 5 denně)
- podepisují se všechny smlouvy a formuláře
- certifikát bude zveřejněn / doručen na webu

# [ Prostředí QCA ]



# [ Vydaný certifikát, atributy ]

- Certificate:
- ...
- Signature Algorithm: sha256WithRSAEncryption
- Issuer: C=CZ, O=\xC4\x8Cesk\xC3\xA1 po\xC5\xA1ta, s.p. [I\xC4\x8C 47114983], CN=PostSignum Qualified CA 2
- Validity
- Not Before: Oct 21 16:46:00 2010 GMT
- Not After : Oct 21 16:46:00 2011 GMT
- Subject: C=CZ, OU=P250905, CN=Lukas Jakubik/serialNumber=P250905
- Subject Public Key Info:
- Public Key Algorithm: rsaEncryption
- RSA Public Key: (2048 bit)
- Modulus (2048 bit)
- ...

# [ Vydaný certifikát, atributy ]

- ...
- X509v3 extensions:
  - X509v3 Subject Alternative Name:
    - email:lukas.jakubik@gmail.com,
    - othername:<unsupported>, othername:<unsupported>
  - X509v3 Basic Constraints:
    - CA:FALSE
  - X509v3 Certificate Policies:
    - Policy: 2.23.134.1.4.1.7.200
  - User Notice:
    - Explicit Text: Tento kvalifikovaný certifikát byl vydan podle zákona 227/2000Sb. a navazných predpisu./This qualified certificate was issued according to Law No 227/2000Coll. and related regulations
  - CPS: <http://www.postsignum.cz>
  - X509v3 Key Usage: critical
    - Digital Signature, Non Repudiation, Key Encipherment
- ...

# [ Certifikační politika ]

- Certifikační politika definuje především způsob vydání certifikátu, další správu, použití, akceptaci, ukončení platnosti, zneplatnění atd.
- Struktura politiky je dána mezinárodně RFC 3647, posléze v ČR přebráno do vyhlášky 378/2006
- PostSignum CP pro QCA z 1/2010
  - 3. Identifikace a autentizace – k certifikaci, k revokaci
  - 4. Životní cyklus certifikátu – OCSP
  - 6. Technická bezpečnost – zajištění QCA
  - 7. Profily certifikátu – tabulkové přehledy vlastností
  - 9. Ostatní obchodní a právní záležitosti – zřeknutí se zodpovědnosti 😊

# [ Certifikační politika, zkušenosti ]

- správná verze smlouvy, tedy pro fyzické nepodnikající osoby je důležitá
- znalost CP v celém rozsahu (naštěstí) nelze od zaměstnankyň očekávat
  - 3.1.4 Pravidla pro interpretaci různých forem jmen
  - .. do žádostí o certifikáty přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech. Transkripce, jako například odstranění diakritiky, není možná..
  - ~ Lukáš Jakubík má i tak CN=Lukas Jakubik
- certifikát může být zneplatněn z rozhodnutí manažera QCA nebo ministerstva



# Validace certifikátu

http://tsl.gov.cz/certiq/vysledek.jsp?results=2

MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

Úvodní stránka  
Návod k aplikaci  
Seznam TSL

### Certifikát

Soubor: QCA1090640.pem  
Vystaveno pro: SERIALNUMBER=P250905, CN=Lukas Jakubik, OU=P250905, C=CZ  
Sériové číslo certifikátu: 1090640  
Vystavitel: CN=PostSignum Qualified CA 2,O=Česká pošta, s.p. [IČ 47114983],C=CZ  
Platnost od: 21.10.2010 18:46 CEST  
Platnost do: 21.10.2011 18:46 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 01.11.2010 v 12.17 (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

Aplikaci provozuje [Ministerstvo vnitra ČR](#) | Aplikaci vytvořil [MathAn Praha, s.r.o.](#) Forma uveřejňovaných informací je v souladu s vyhláškou č. 64/2008 Sb. (Vyhláška o přístupnosti).  
Verze aplikace: 1.0.9

# [ Shrnutí ]

- Lukáš Nevosád, 2005
  - *I přes složitost procesu jeho získání hodnotím počin České pošty kladně a věřím, že přispěje k masivnějšímu využívání e-podpisu v ČR. Nemohu se ovšem ubránit dojmu, že celý proces by se dal výrazně zjednodušit a automatizovat.*
  - *Skutečně je nutné vynaložit 12 fyzických podpisů na jeden elektronický?*
- Lukáš Jakubík, 2010
  - *Pořídit si kvalifikovaný certifikát není nijak náročné, ale napoprvé se povede úspěšně dokončit postup jen připraveným. K průběhu procesu nelze nic vytknout, myslím, že na poště má cesta k elektronickému podpisu dokonce docela lidskou tvář.*
  - *Už jsou zapotřebí jen 8 až 10 podpisů 😊*
- Děkuji za pozornost

# [ Odkazy ]

---

- Sbíрка zákonů
- [http://www.postsignum.cz/offline\\_generovani\\_zadosti.html](http://www.postsignum.cz/offline_generovani_zadosti.html)
- <http://tools.ietf.org/html/rfc3647>
- <http://www.mvcr.cz/clanek/informace-k-pouzivani-kvalifikovanych-certifikatu-pro-elektronicky-podpis-a-zaroven-pro-autentizaci-a-sifrovani.aspx>
- <http://www.mvcr.cz/clanek/aktualni-situace-v-oblasti-uznavani-zahranicnich-kvalifikovanych-certifikatu.aspx>
- <http://www.lupa.cz/clanky/jak-jsem-si-poridil-elektronicky-podpis-ceske-posty/>