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 podpise
  - vyhláška 496/2004, o elektronických podatelnách…

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 ministerstvím informatiky, posléze ministerstvím 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

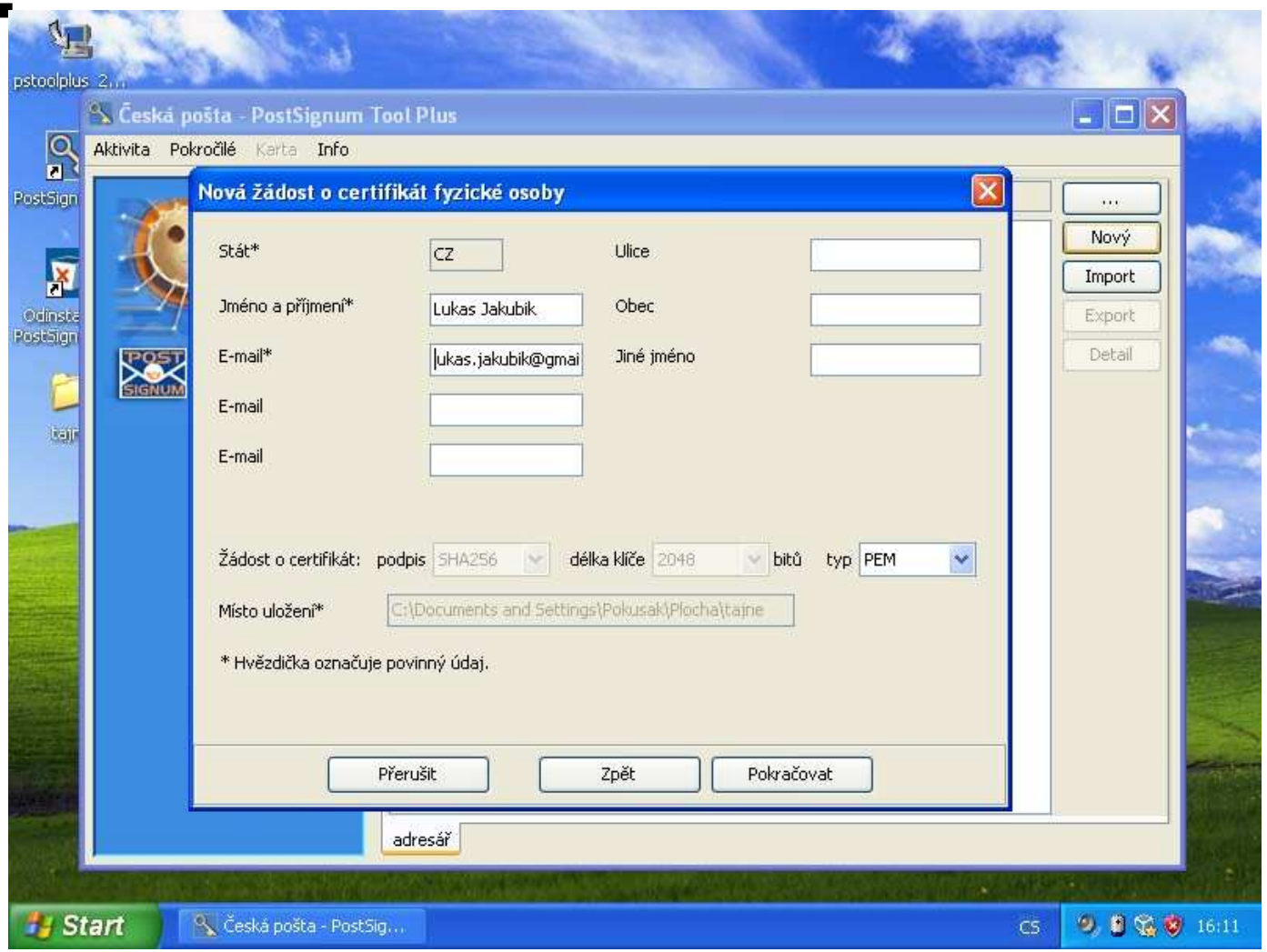
Požadavky k vydaní certifikátu

- 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

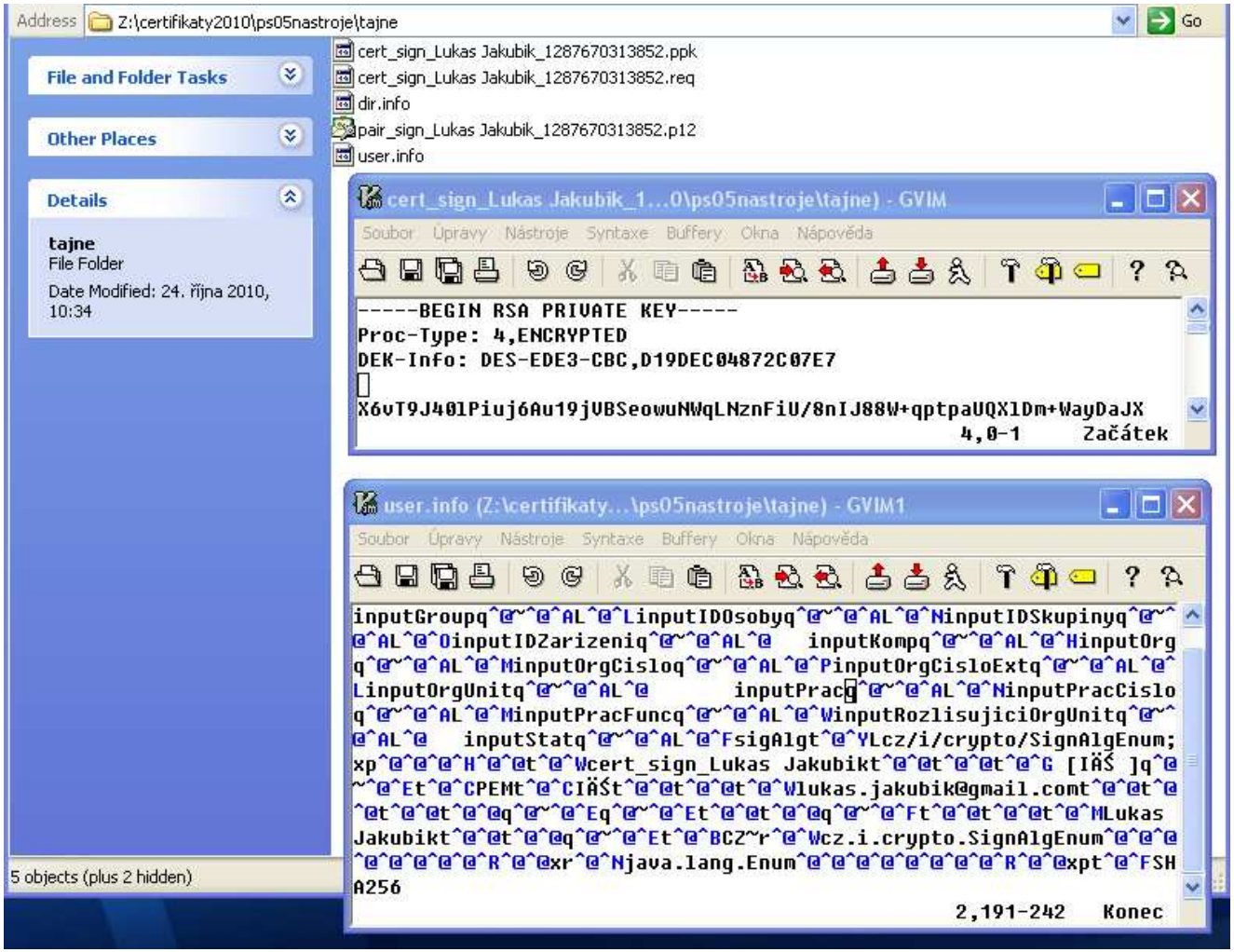
Generování klíčů a žádosti

- 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

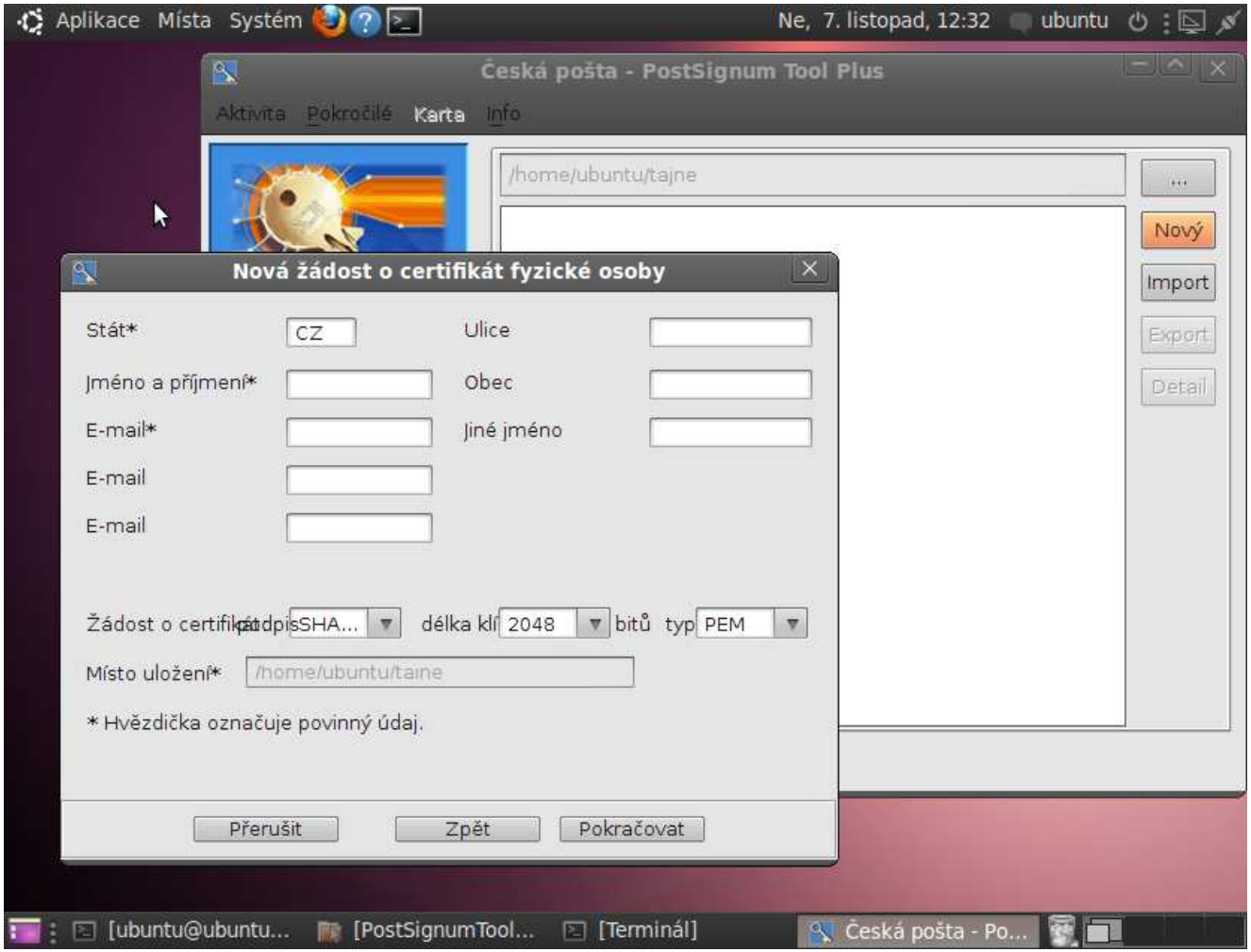
Prostředí programu, Windows



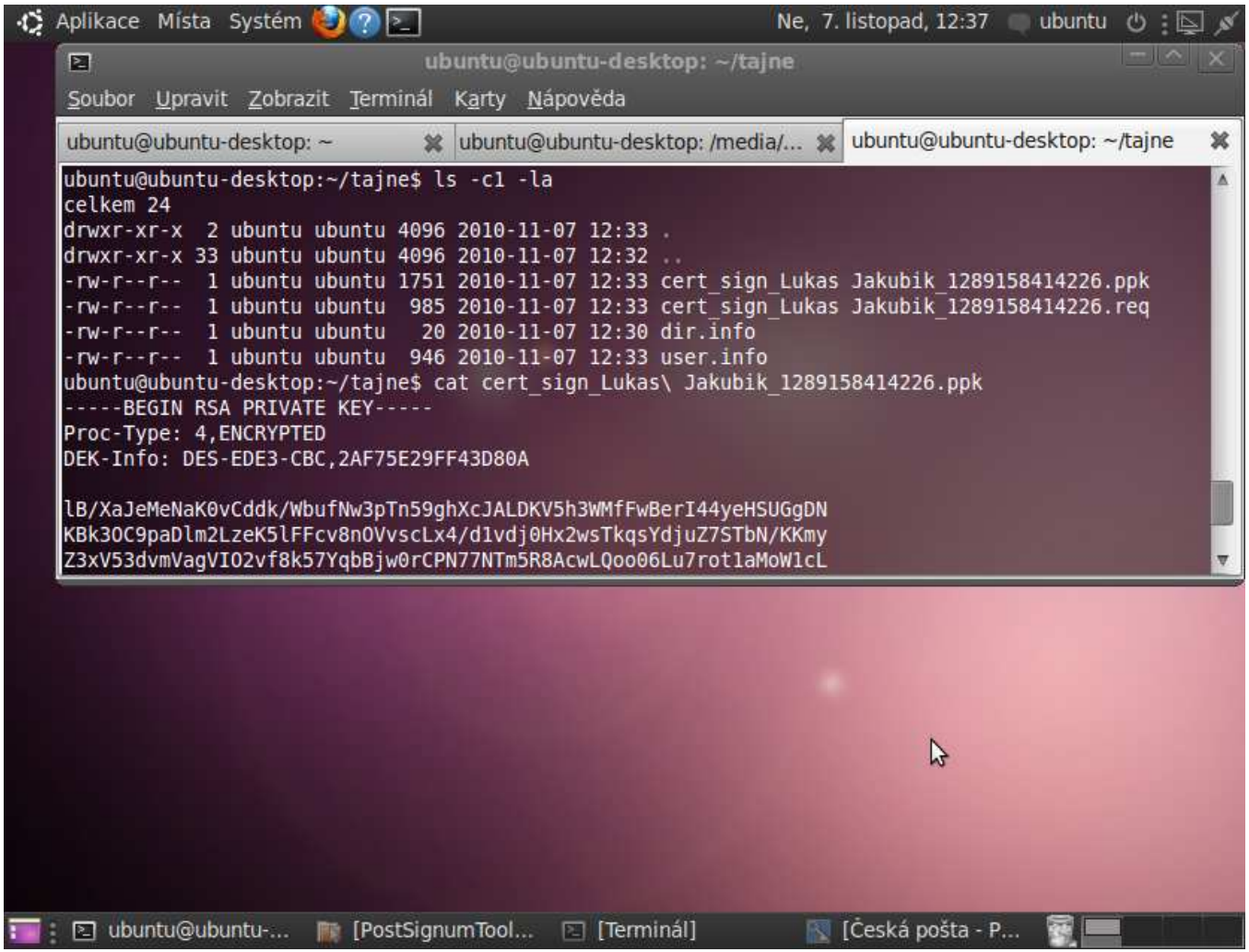
Obsah složky s klíči a žádosti



Prostředí programu, Ubuntu



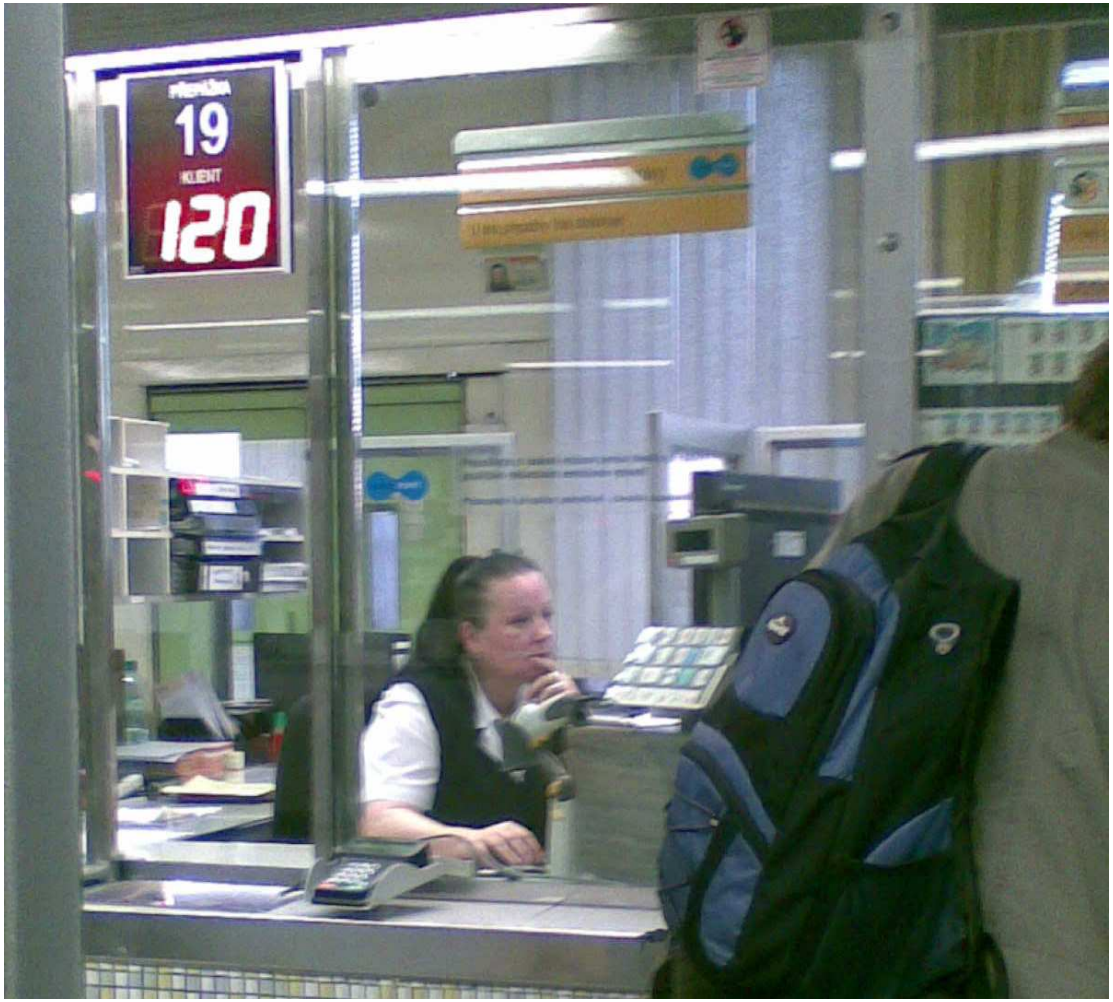
Obsah složky s klíči a žádosti



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 kvalifikovany certifikat byl vydan podle zakona 227/2000Sb. a navaznych 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
- …

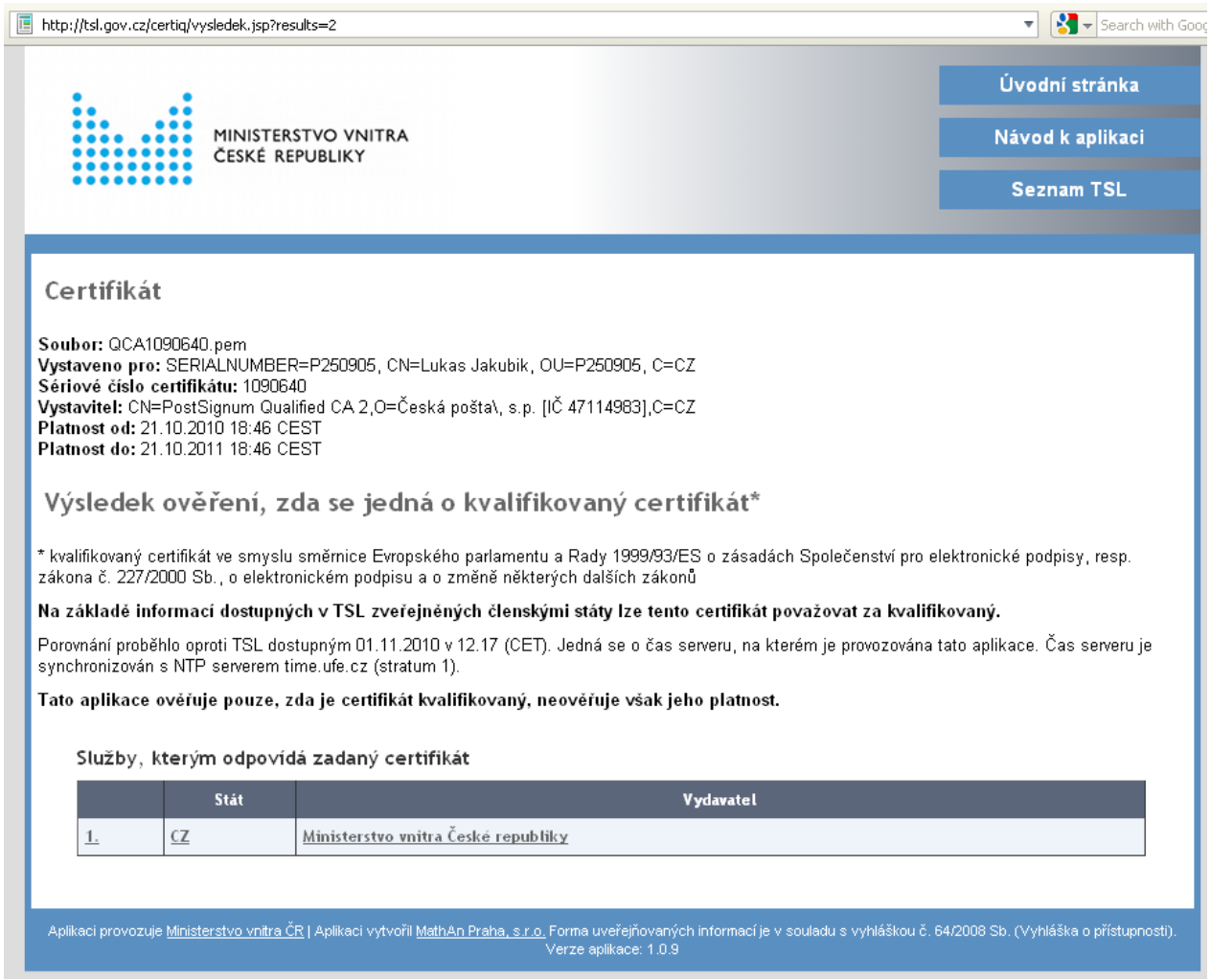
Certifikační politika

- 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



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

- Sbírka zákonů
- 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/