PostSignum QCA

Qualified certificate, findings

Lukáš Jakubík
FI MU

2010

Motivation

- Qualified certificate provides a secure electronic signature of a person or organization under the Act
- Use for individuals and businesses
  - communication with state,
  - electronic submission before the submission of a hardcopy ...
- Legislation
  - § 227/2000 Coll. in revised, the electronic signature
  - Decree 496/2004, the electronic registrar ...

Qualification of certificate

- § 11 227/2000 Coll. novelized in 226/2002 Sb.
    - *In the area of public policy is to be used only advanced electronic signatures and qualified certificates issued by accredited certification service provider. This also applies to the exercise of public authority against natural and legal persons. If the advanced electronic signature based on a qualified certificate used in public authorities, professional certificate must contain such information that the person was clearly identifiable.*

PostSignum

- CA owned by Česká pošta, state-owned enterprise
- One of the three qualified CAs registered and accredited Ministry of informatics, then Ministry of interior
- Issues qualified certificates from 9 / 2005 and qualified time stamps from 7 / 2009
- Benefits
  - MPSV identification - the pseudonymous identification, unique number to the Ministry of labour and social affairs, Tax offices, Czech Social Security Administration and Employment offices
  - from 5 / 2010 included in the list of Microsoft Root CA
  - spread and accessibility of post offices with CzechPOINT
  - cheaper service (200 ~ 400 CZK), familiar surroundings

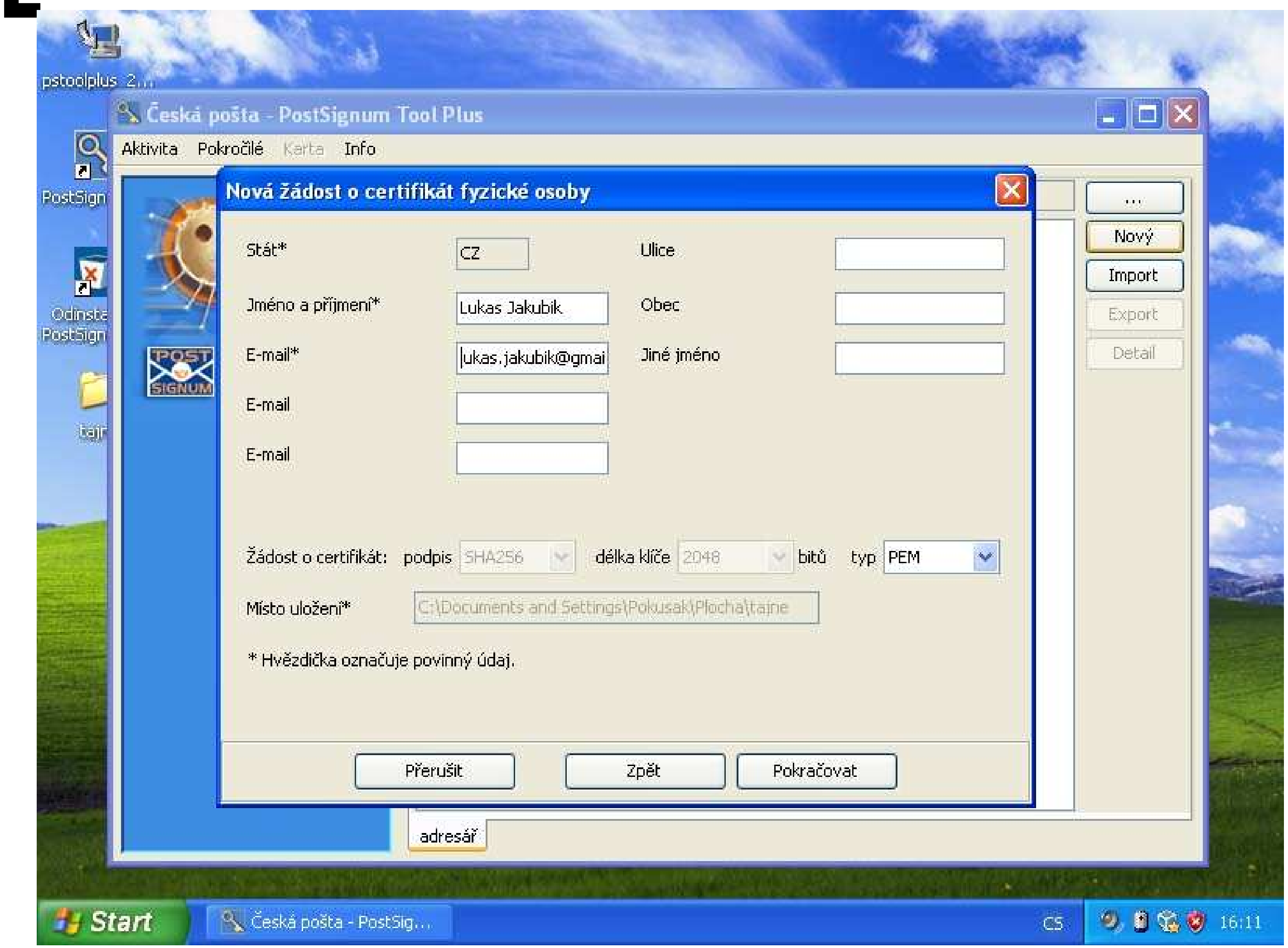
Requirements

- Generated key pair (online through IE / offline)
- Electronic certificate request, signed public key with private key pair (CMS)
- 2 completed copies of the Agreement on the Provision of Certification Services with Czech Post
- 2 completed paper forms containing attributes of requested certificate
- 2 identification cards
- Voucher / cash / maxkarta ~ no debetcard supported
- Time

Key generation

- Online generation in IE (rather) not tested
- Offline PostSignum Tool Plus is a portable application available for Windows, Linux and MacOS running the JRE
- It is suitable for the generation a key pair and then all types of certificate’s request, which gives PostSignum
- It uses the familiar file structure according to the PKCS, hidden in a password-protected directory
- ~ it means encrypted by "directory password"
- Password is loaded in the memory as long as you are working with the program

Program GUI, Windows



Česká pošta - PostSignum Tool Plus

Nová žádost o certifikát fyzické osoby

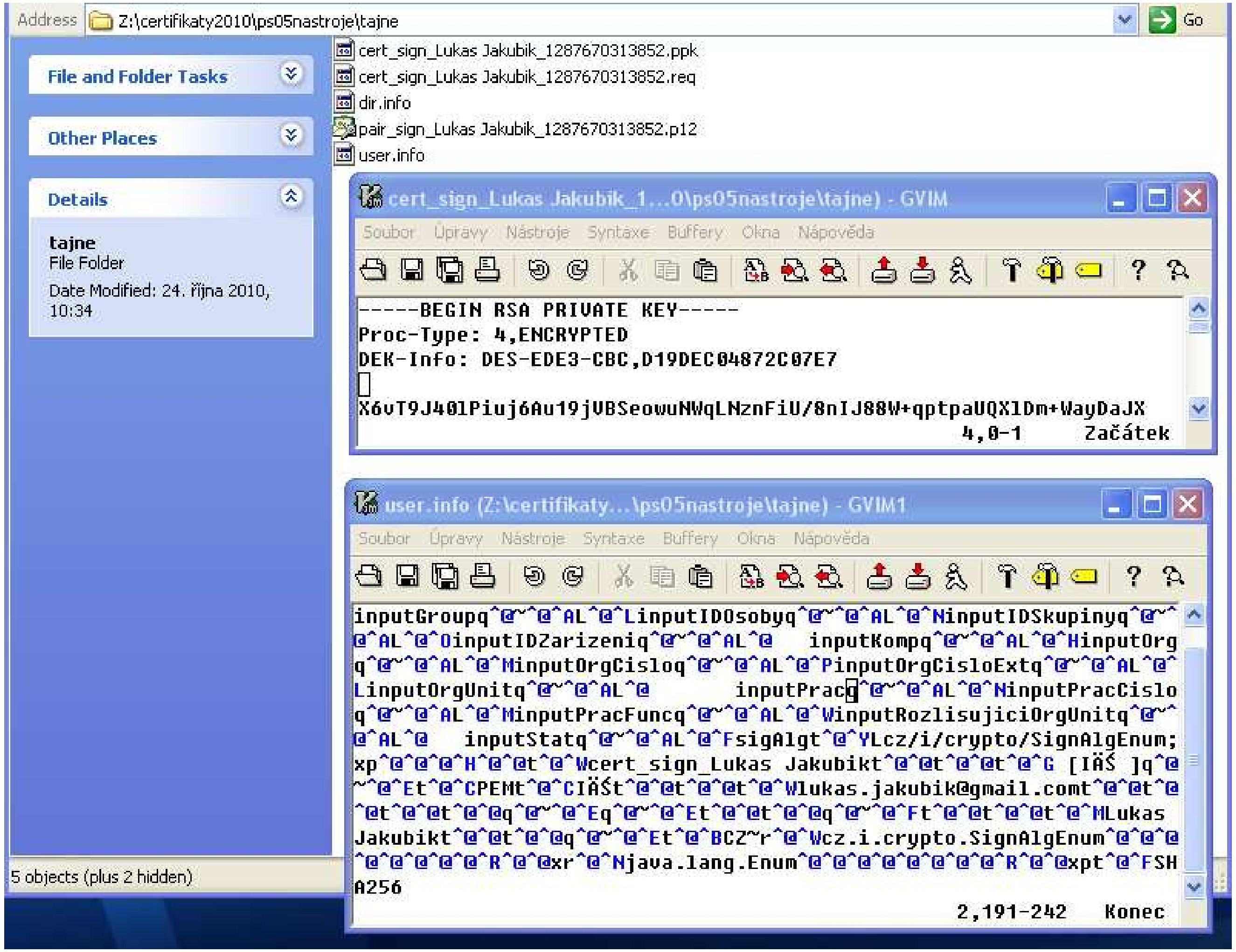
Stát*	CZ	Ulice	
Jméno a příjmení*	Lukas Jakubik	Obec	
E-mail*	lukas.jakubik@gmai	Jiné jméno	
E-mail			
E-mail			

Žádost o certifikát: podpis SHA256 délka klíče 2048 bitů typ PEM

Místo uložení* C:\Documents and Settings\Pokusak\Plocha\tajne

* Hvězdička označuje povinný údaj.

Folder content



Z:\certifikaty2010\ps05nastroje\tajne

- cert_sign_Lukas Jakubik_1287670313852.ppk
- cert_sign_Lukas Jakubik_1287670313852.req
- dir.info
- pair_sign_Lukas Jakubik_1287670313852.p12
- user.info

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

5 objects (plus 2 hidden)

cert_sign_Lukas Jakubik_1...0\ps05nastroje\tajne) - GVIM

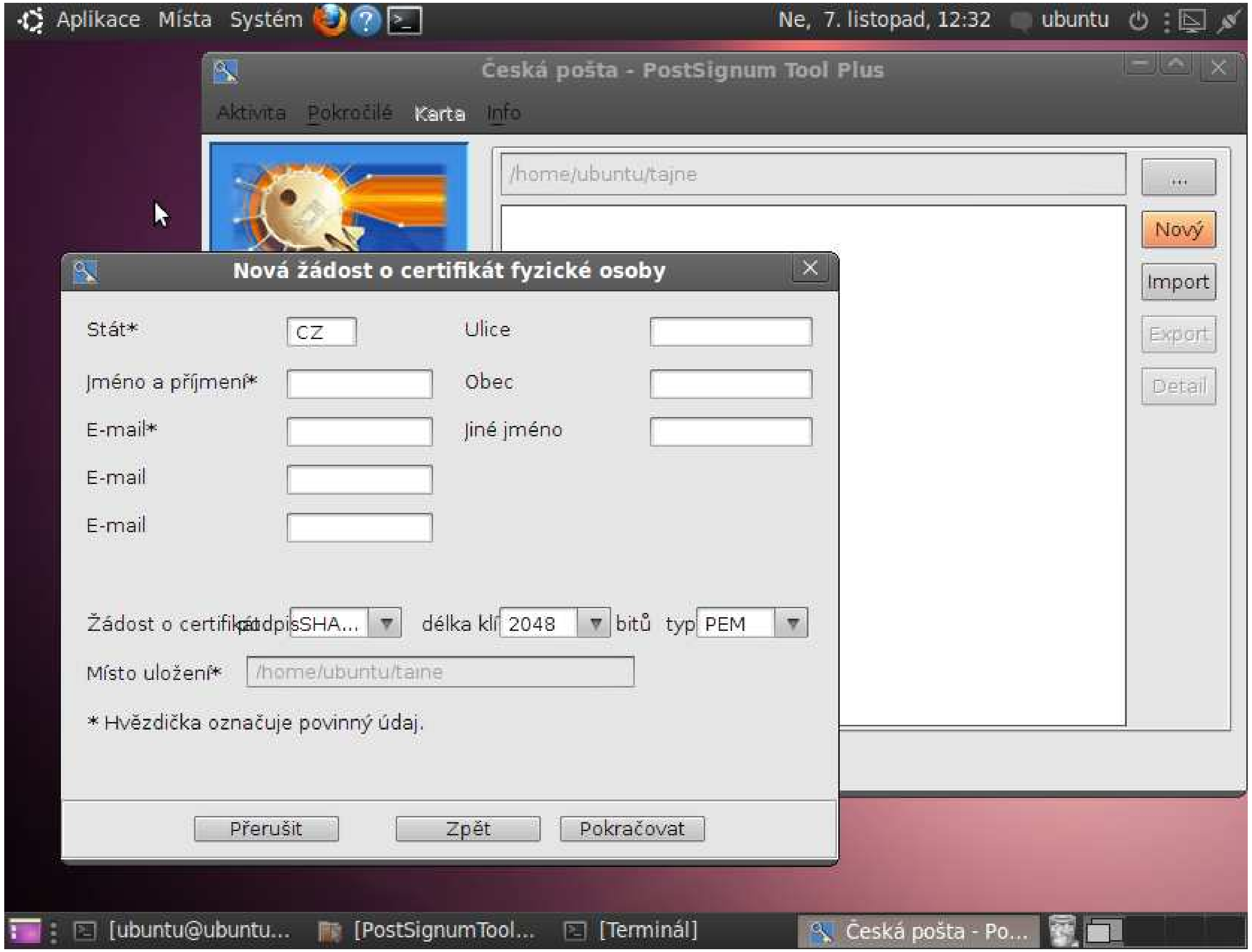
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D19DEC04872C07E7

X6vT9J40lPiuj6Au19jVBSeowuNWqLNznFiU/8nIJ88W+qptpaUQXlDm+WayDaJX
                                             4,0-1      Začátek
```

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

```
inputGroupq^@~^@^AL^@^LinputIDOsobyq^@~^@^AL^@^NinputIDSkupinyq^@~^
@^AL^@^OinputIDZarizeniq^@~^@^AL^@   inputKompq^@~^@^AL^@^HinputOrg
q^@~^@^AL^@^MinputOrgCisloq^@~^@^AL^@^PinputOrgCisloExtq^@~^@^AL^@^
LinputOrgUnitq^@~^@^AL^@          inputPracq^@~^@^AL^@^NinputPracCislo
q^@~^@^AL^@^MinputPracFuncq^@~^@^AL^@^WinputRozlisujiciOrgUnitq^@~^
@^AL^@   inputStatq^@~^@^AL^@^FsigAlgt^@^YLcz/i/crypto/SignAlgEnum;
xp^@^@^@^H^@^@t^@^Wcert_sign_Lukas Jakubikt^@^@t^@^@t^@^G [IĂŚ ]q^@
~^@^Et^@^CPEMt^@^CIĂŚt^@^@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^@^@^@
^@^@^@^@^@^R^@^@xr^@^Njava.lang.Enum^@^@^@^@^@^@^@^@^R^@^@xpt^@^FSH
A256
                                              2,191-242    Konec
```

Program GUI, Ubuntu



Aplikace Místa Systém
Ne, 7. listopad, 12:32
ubuntu
Česká pošta - PostSignum Tool Plus
Aktivita Pokročilé Karta Info
/home/ubuntu/tajne
...
Nový
Import
Export
Detail
[ubuntu@ubuntu... [PostSignumTool... [Terminál] Česká pošta - Po...

Nová žádost o certifikát fyzické osoby

Stát* CZ

Ulice

Jméno a příjmení*

Obec

E-mail*

Jiné jméno

E-mail

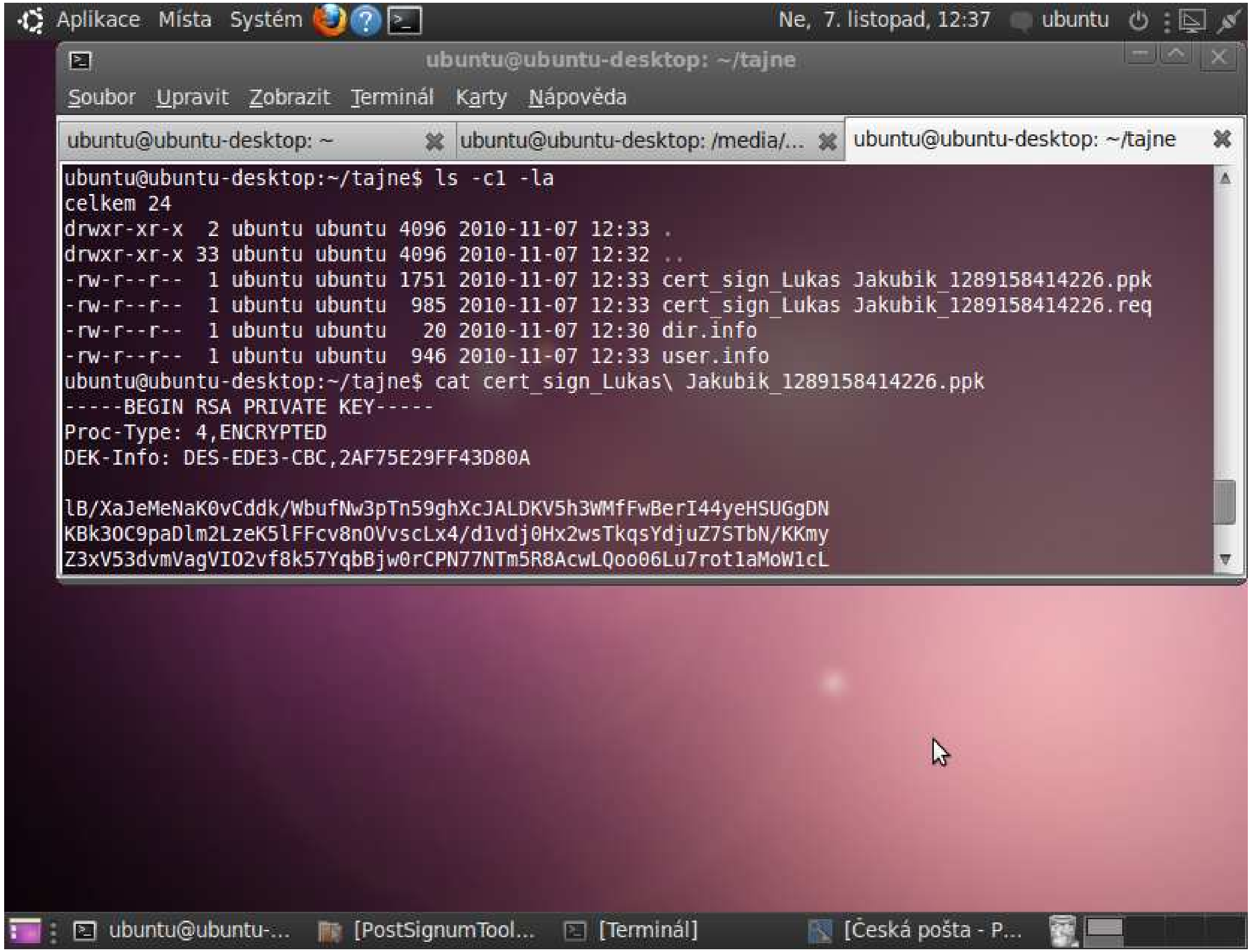
E-mail

Žádost o certifikát podpis SHA... délka klíč 2048 bitů typ PEM

Místo uložení* /home/ubuntu/tajne

* Hvězdička označuje povinný údaj.

Folder content



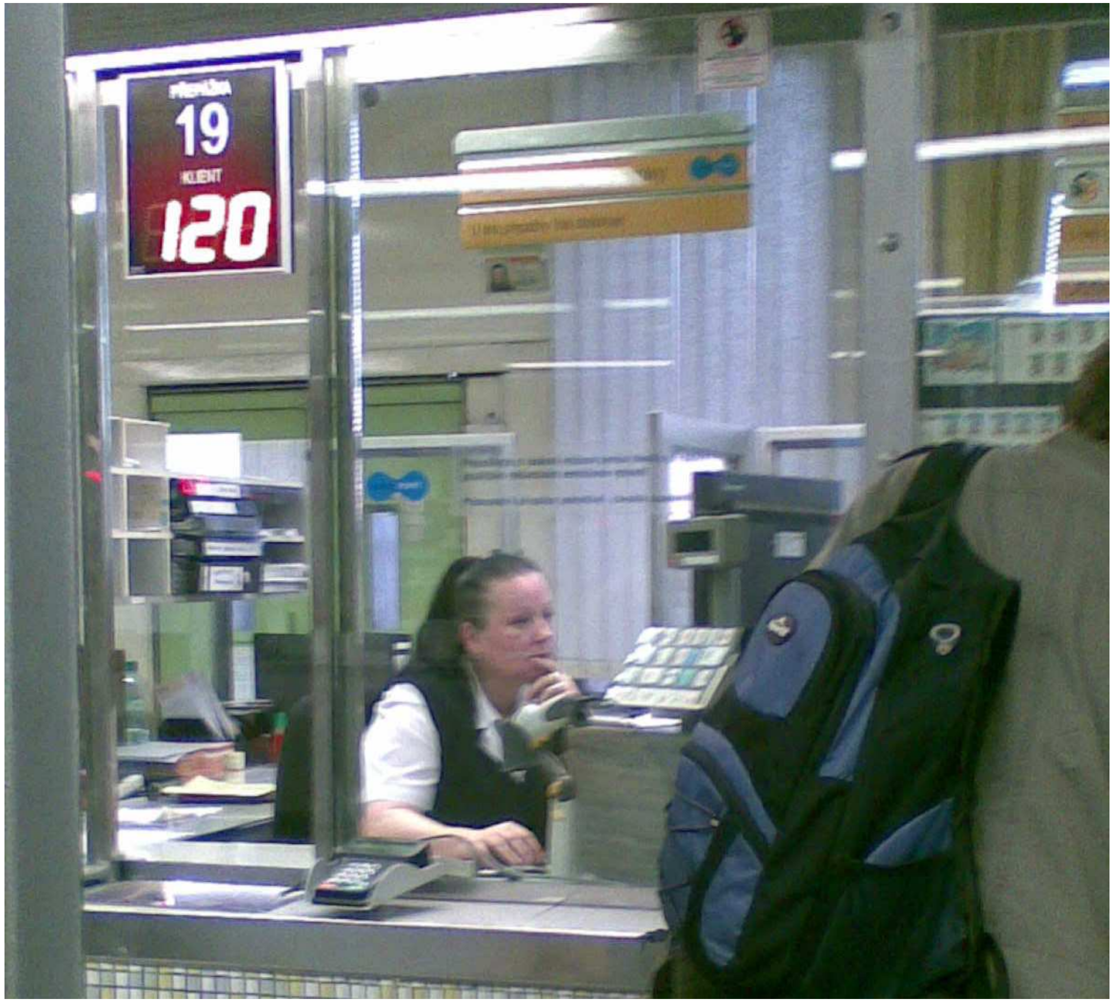
```
ubuntu@ubuntu-desktop:~/tajne$ ls -cl -la
celkem 24
drwxr-xr-x  2 ubuntu ubuntu 4096 2010-11-07 12:33 .
drwxr-xr-x 33 ubuntu ubuntu 4096 2010-11-07 12:32 ..
-rw-r--r--  1 ubuntu ubuntu 1751 2010-11-07 12:33 cert_sign_Lukas Jakubik_1289158414226.ppk
-rw-r--r--  1 ubuntu ubuntu  985 2010-11-07 12:33 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
KBk3OC9paDlm2LzeK5lFFcv8nOVvscLx4/d1vdj0Hx2wsTkqsYdjuZ7STbN/KKmy
Z3xV53dvmVagVIO2vf8k57YqbBjw0rCPN77NTm5R8AcwLQoo06Lu7rot1aMoW1cL
```

Certificate’s request procedure

- Certificate’s request shall be filed in person
- Worker checks the paper formalities documents (makes a copy) and in her system
  - filled parties for future cooperation
  - complete the application form for a certificate under
  - loaded from a USB flash drive electronic application
  - complete revocation strong password
  - a certificate of issuing a certificate printed with that strong password ☺
  - she is nice and skilled (2 successes from about 5 per day)
- Signing all agreements and forms
- Certificate will be released / delivered on the Web

Workspace of QCA



Issued certificate, attributes

- 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)
- …

Issued certificate, attributes

- …
- 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
- …

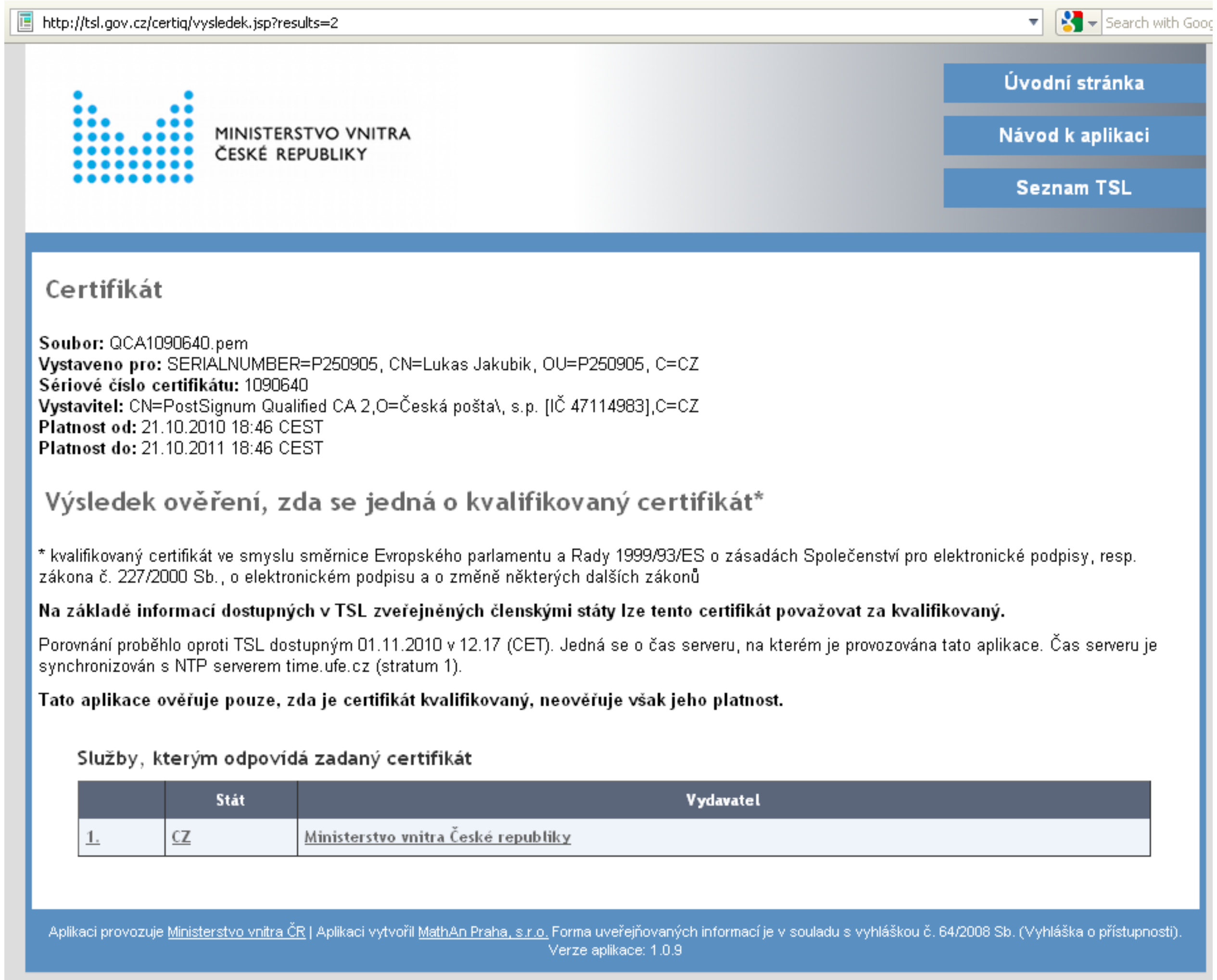
Certification policy

- Certificate Policy defines the way of issuing a certificate, the next administration, use, acceptance, termination, revocation, etc.
- The structure of international politics is given RFC 3647, later taken over by local Decree 378/2006
- Example: PostSignum CP for QCA from 1 / 2010
  - 3rd Identification and authentication – the certification, the revocation
  - 4th Certificate Life Cycle – OCSP not provided
  - 6th Technical safety – ensuring the QCA
  - 7th Certificate profile – a table showing the properties
  - 9th Other business and legal affairs - disclaimer

Certification policy, findings

- The right version of the agreement, that is a person not conducting business is important
- Knowledge of the policies in full (thankfully) can not be expected from workers
  - 3.1.4 Rules for interpreting various name forms
  - *... to transmit requests for certificates in the form in which they are listed in the submitted documents. Transcription, such as the removal of diacritics, it is not possible …*
  - ~ Lukáš Jakubík has the CN = Lukas Jakubik
- Certificate may be revoked by decision of the manager of QCA or the staff of Ministry of interior

Certification validation



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

Conclusion

- Lukáš Nevosád, 2005
  - *Despite the complexity of the process of obtaining evaluate the achievement of the Czech Post in the affirmative and I believe it will contribute to spread use of e-signatures in the country. But I can not resist the impression that the whole process could be greatly simplified and automated.*
  - *Indeed, it is necessary to spend 12 signatures per electronic signatures?*
- Lukáš Jakubík, 2010
  - *Getting a qualified certificate is not a hard time, but the process will complete successfully only prepared. The course of the process is beyond reproach, I think the post office has a path to the electronic signature even quite human face.*
  - *It is needed only 8-10 signatures…*

- Thank you for your attention

Links

- Collection of laws
- 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/