Používání certifikátů v elektronické poště

Podepisování a šifrování elektronické pošty za použití certifikátů od certifikační autority Thawte

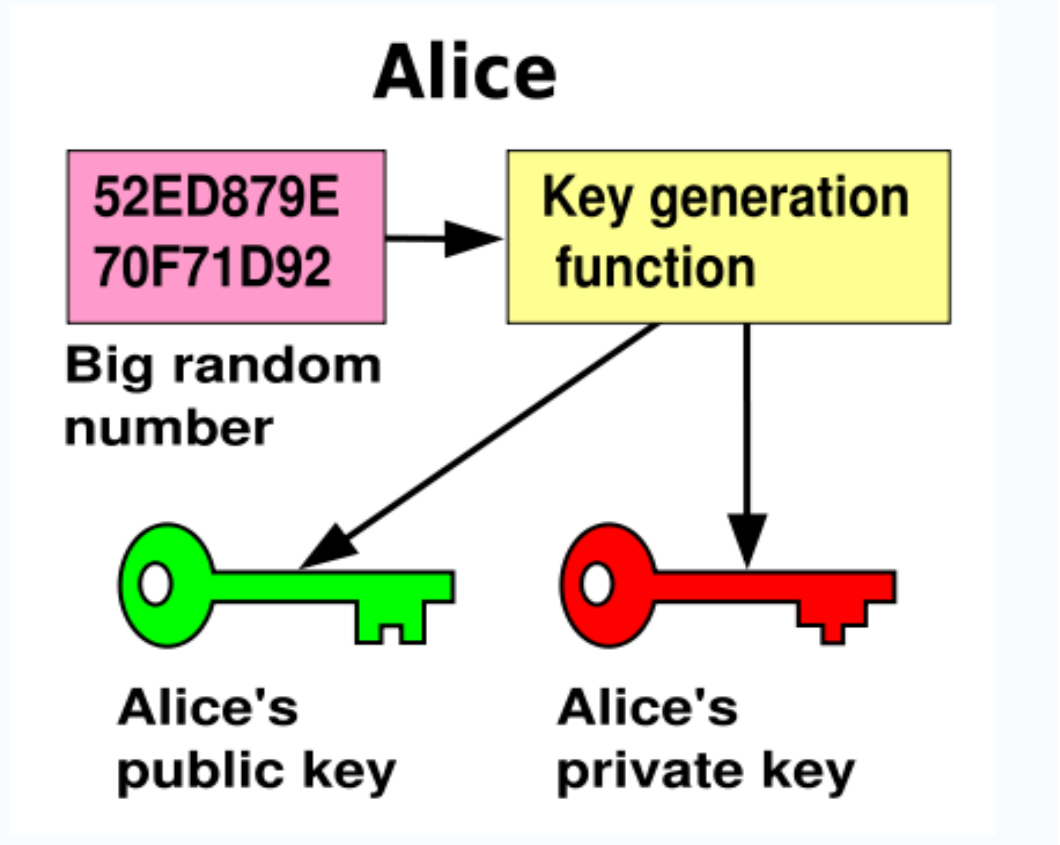
Jarda Kačer
jarda@kacer.biz

Český Warpstock 2007
Mladá Boleslav, 6.-7.10.2007

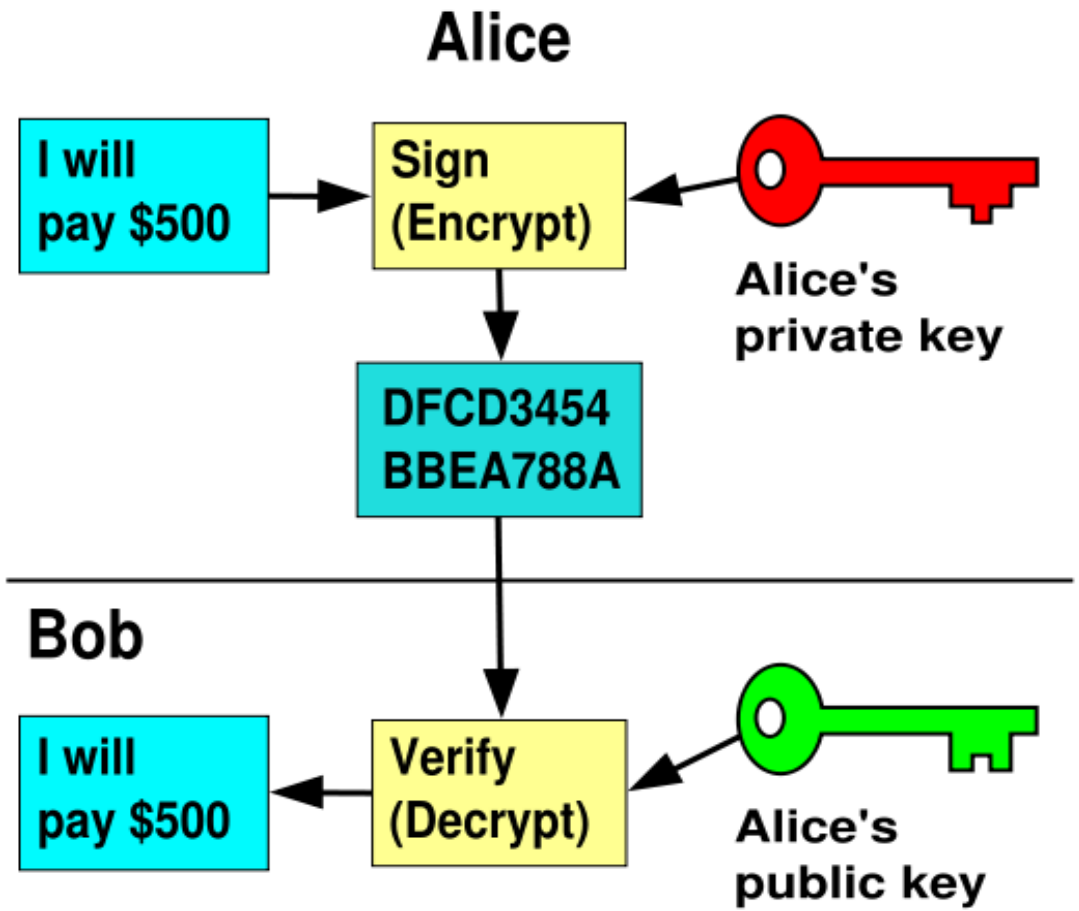
Co je to digitální podpis

- Typ asymetrické kryptografie, který poskytuje:
  - Autentifikaci
  - Nepopiratelnost
- Dva klíče, které jsou vygenerované najednou:
  - **Soukromý** – private – má ho pouze vlastník
  - **Veřejný** – public – může ho mít každý
- Algoritmy:
  - **Podpis**
  - **Ověření** podpisu

Digitální podpis – Výroba klíčů

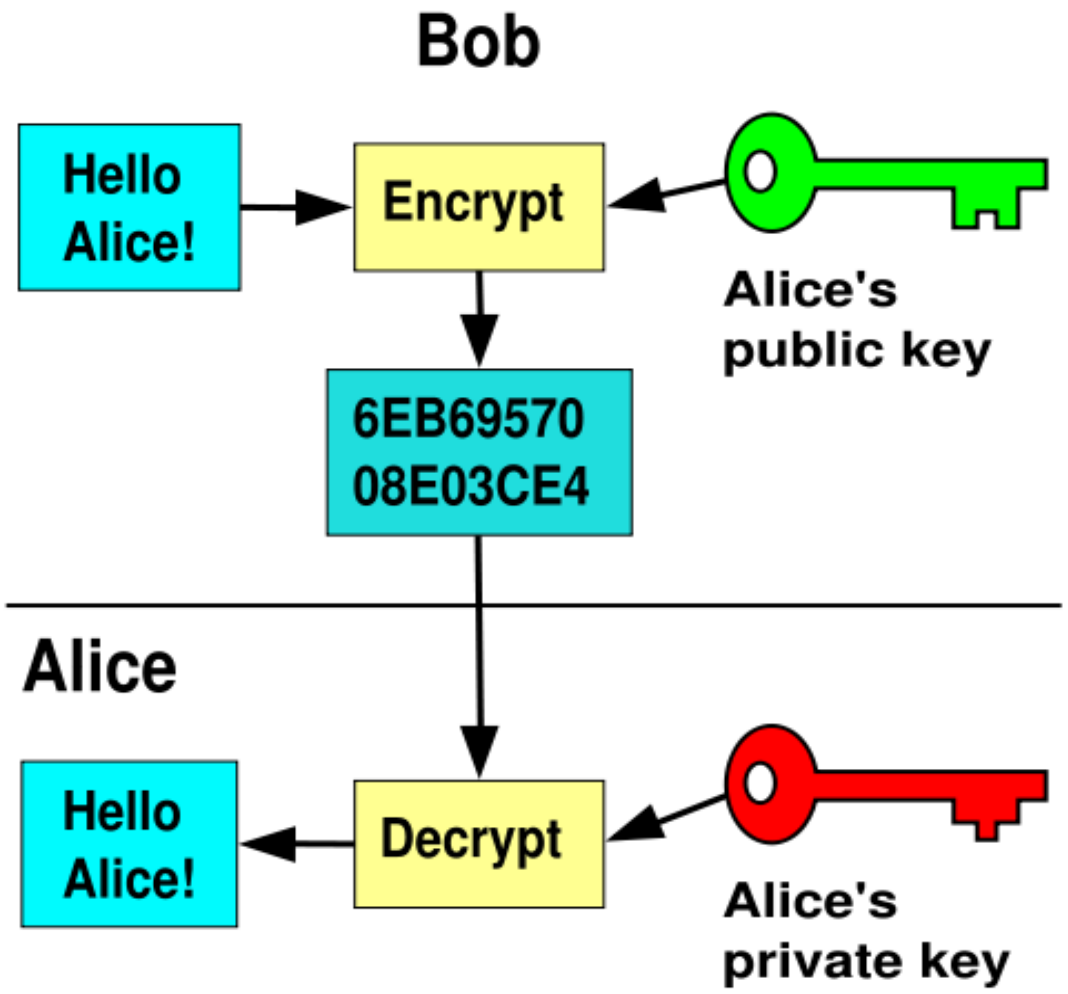


Digitální podpis – Podepsání



Většinou se podepisuje pouze hash zprávy, ne zpráva celá.

Digitální podpis – Šifrování



Co to je certifikát

- Ve velkém měřítku je výměna klíčů „každý s každým“ neefektivní
- Certifikát je tvrzení o vzájemném **spojení** nějaké **identity** s **veřejným klíčem**
- Vystavuje ho někdo, komu se věří
  - Certifikační autorita v PKI systémech
  - Ostatní uživatelé v sítích vzájemné důvěry
- Vystavovatel ho **podepisuje svým soukromým klíčem**
- Může být odvolán – CRL

Hierarchie certifikátů

- Certifikáty se mohou řetězit
- Ten, kdo vystavil někomu certifikát, má svůj vystavený také od někoho
- Stromová struktura s kořenem
- Kořenovému certifikátu se apriori věří
  - Certifikáty naimportovány přímo v softwaru při nainstalování

Co to je certifikační autorita

- Vystavuje certifikáty ostatním
- Věří se jí – Trusted third party
- Příklady:
  - VeriSign
  - Thawte
  - GeoTrust
  - Comodo
  - Vlastní CA pro firmu, univerzitu – Problém: Pro ostatní není možno ověřit platnost

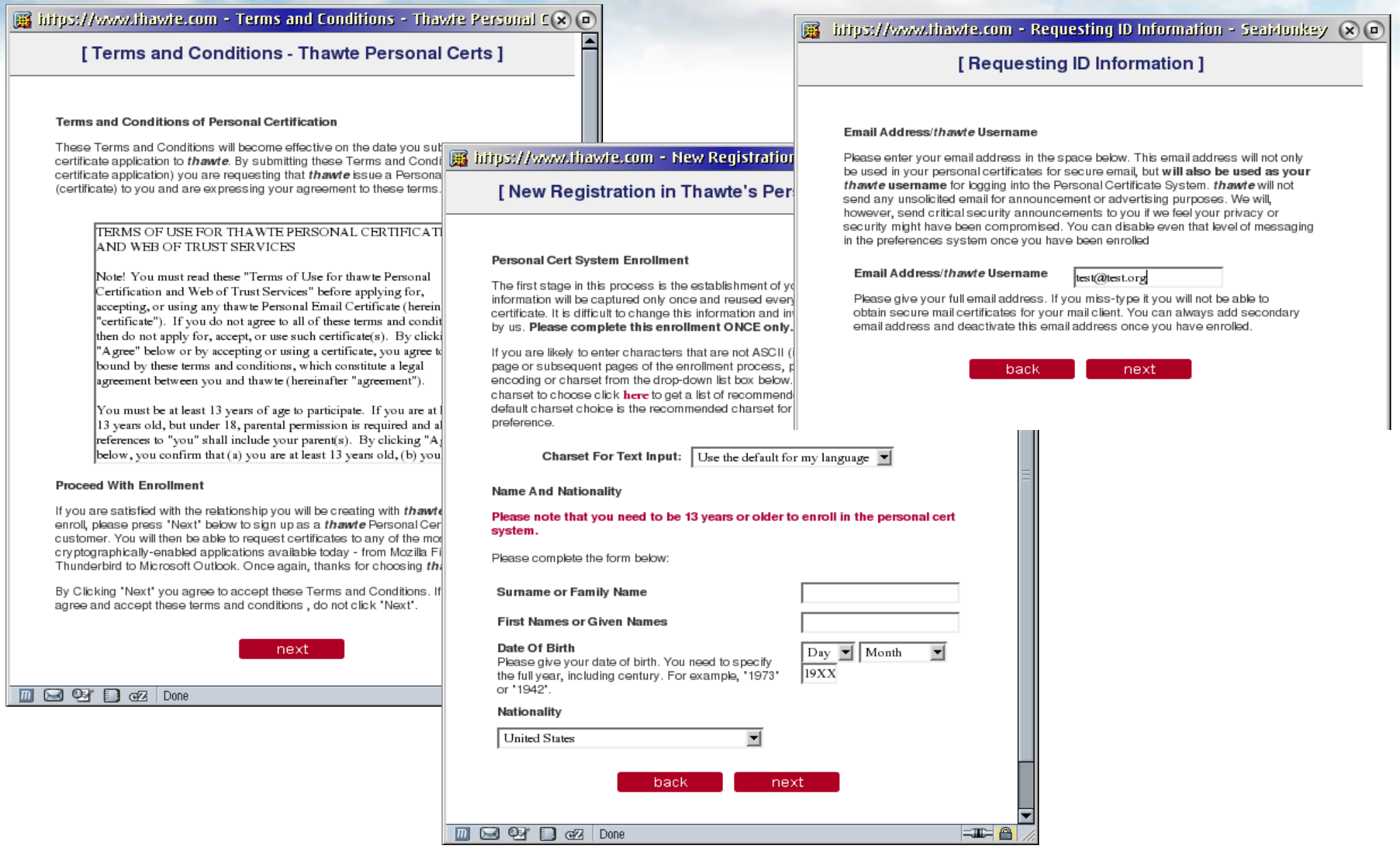
Proč Thawte?

- Vystavuje certifikáty pro podpis a šifrování pošty zdarma
- Její certifikáty jsou standardně ve většině programů – Mozilla FF/TB/SM, MS Outlook, …
- Založena v r. 1995 Markem Shuttleworthem v Jižní Africe
- V r. 1999 koupena VeriSignem
- Vystavěla navíc tzv. Web of Trust

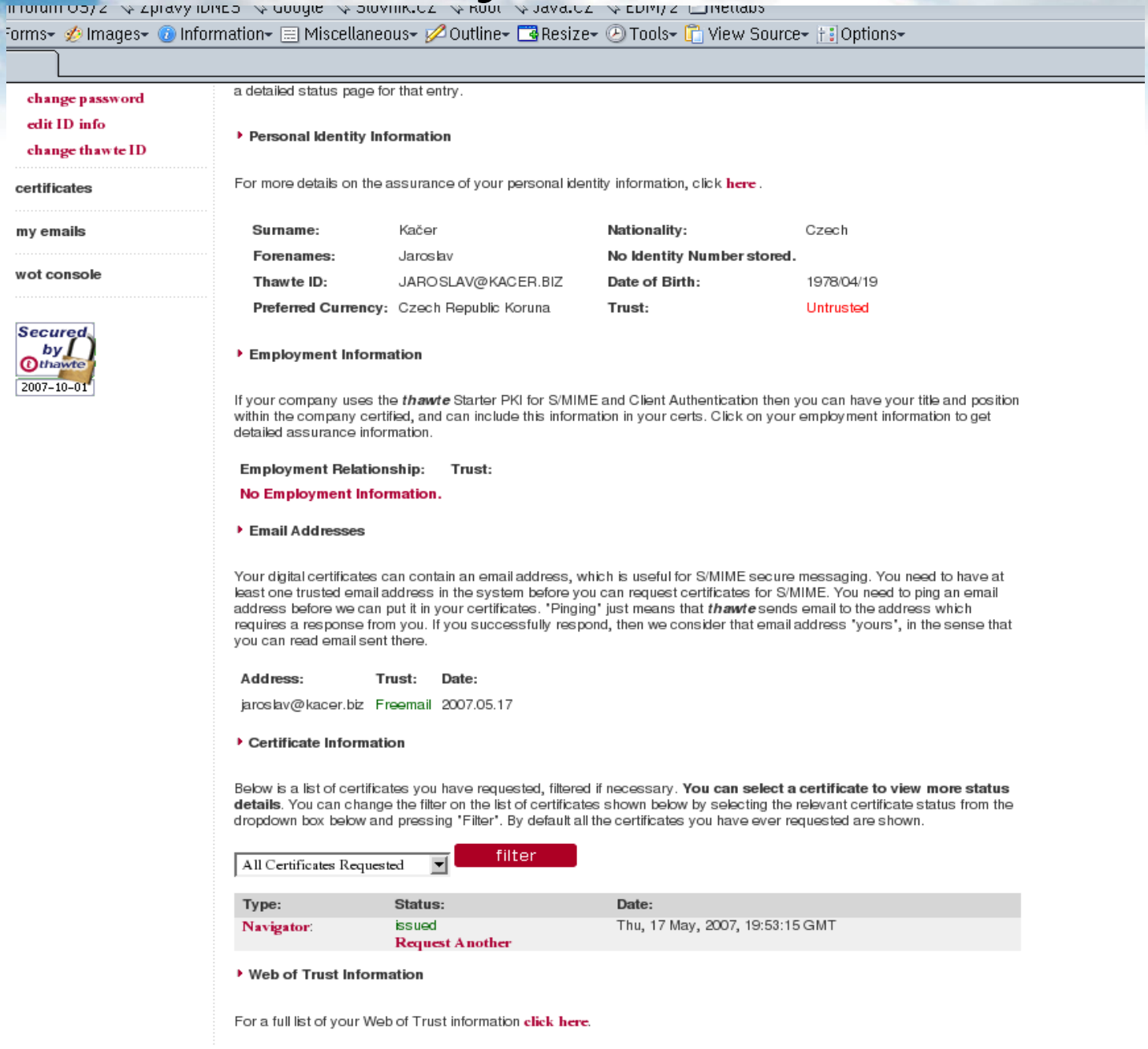
Jak dostat certifikát

- Nejdříve je třeba mít u Thawte konto
- Vázáno na emailovou adresu
- Později lze přidat i skutečné jméno, viz dále Web of Trust
- Thawte generuje oba klíče i certifikát
- Verze pro více programů: Mozilla XXX, MS XXX, Opera, Lotus Notes, ...

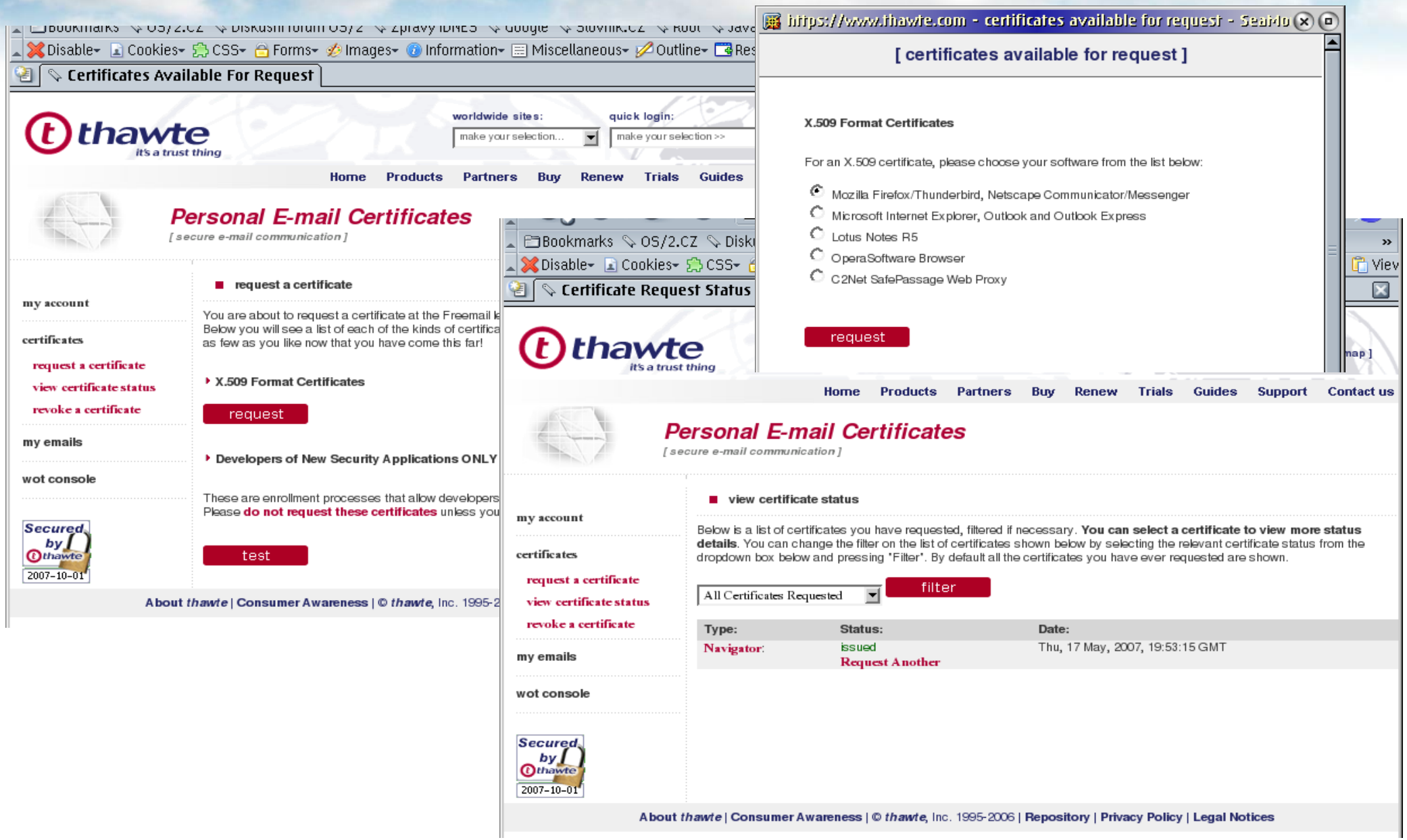
Registrace


https://www.thawte.com - Terms and Conditions - Thawte Personal C
[Terms and Conditions - Thawte Personal Certs]
Terms and Conditions of Personal Certification
These Terms and Conditions will become effective on the date you sut
certificate application to thawte. By submitting these Terms and Condi
certificate application) you are requesting that thawte issue a Persona
(certificate) to you and are expressing your agreement to these terms.
TERMS OF USE FOR THAWTE PERSONAL CERTIFICATI
AND WEB OF TRUST SERVICES
Note! You must read these "Terms of Use for thawte Personal
Certification and Web of Trust Services" before applying for,
accepting, or using any thawte Personal Email Certificate (herein
"certificate"). If you do not agree to all of these terms and condit
then do not apply for, accept, or use such certificate(s). By clicki
"Agree" below or by accepting or using a certificate, you agree t
bound by these terms and conditions, which constitute a legal
agreement between you and thawte (hereinafter "agreement").
You must be at least 13 years of age to participate. If you are at l
13 years old, but under 18, parental permission is required and al
references to "you" shall include your parent(s). By clicking "A
below, you confirm that (a) you are at least 13 years old, (b) you
Proceed With Enrollment
If you are satisfied with the relationship you will be creating with thawte
enroll, please press "Next" below to sign up as a thawte Personal Cer
customer. You will then be able to request certificates to any of the mo
cryptographically-enabled applications available today - from Mozilla Fi
Thunderbird to Microsoft Outlook. Once again, thanks for choosing th
By Clicking "Next" you agree to accept these Terms and Conditions. If
agree and accept these terms and conditions , do not click "Next".
next
Done
https://www.thawte.com - New Registration
[New Registration in Thawte's Per
Personal Cert System Enrollment
The first stage in this process is the establishment of yo
information will be captured only once and reused every
certificate. It is difficult to change this information and in
by us. Please complete this enrollment ONCE only.
If you are likely to enter characters that are not ASCII (
page or subsequent pages of the enrollment process, p
encoding or charset from the drop-down list box below.
charset to choose click here to get a list of recommend
default charset choice is the recommended charset for
preference.
Charset For Text Input: Use the default for my language
Name And Nationality
Please note that you need to be 13 years or older to enroll in the personal cert system.
Please complete the form below:
Surname or Family Name
First Names or Given Names
Date Of Birth
Please give your date of birth. You need to specify the full year, including century. For example, "1973" or "1942".
Day
Month
19XX
Nationality
United States
back
next
Done
https://www.thawte.com - Requesting ID Information - SeaMonkey
[Requesting ID Information]
Email Address/thawte Username
Please enter your email address in the space below. This email address will not only be used in your personal certificates for secure email, but will also be used as your thawte username for logging into the Personal Certificate System. thawte will not send any unsolicited email for announcement or advertising purposes. We will, however, send critical security announcements to you if we feel your privacy or security might have been compromised. You can disable even that level of messaging in the preferences system once you have been enrolled
Email Address/thawte Username
test@test.org
Please give your full email address. If you miss-type it you will not be able to obtain secure mail certificates for your mail client. You can always add secondary email address and deactivate this email address once you have enrolled.
back
next

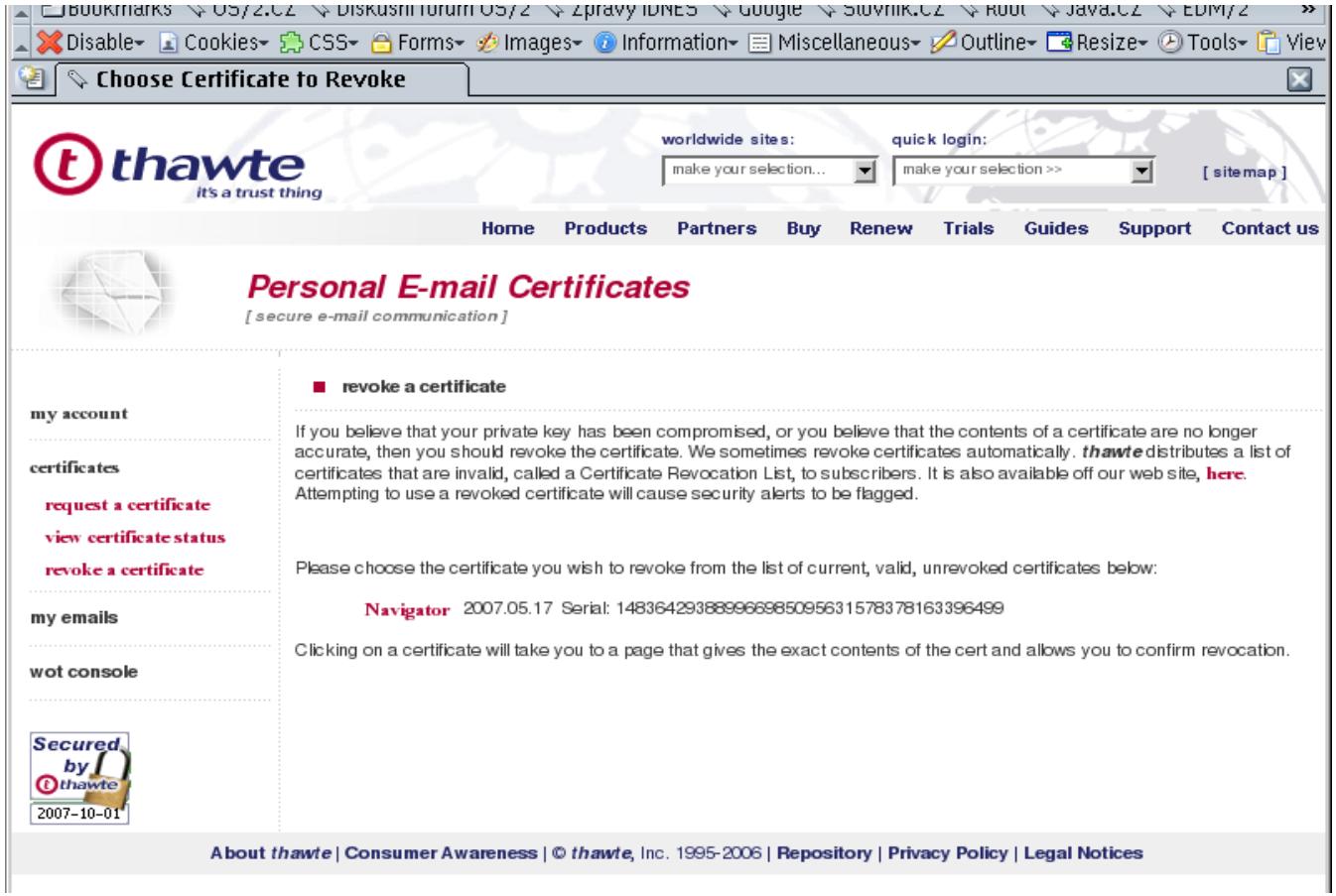
Detaily uživatele



Vystavení certifikátu



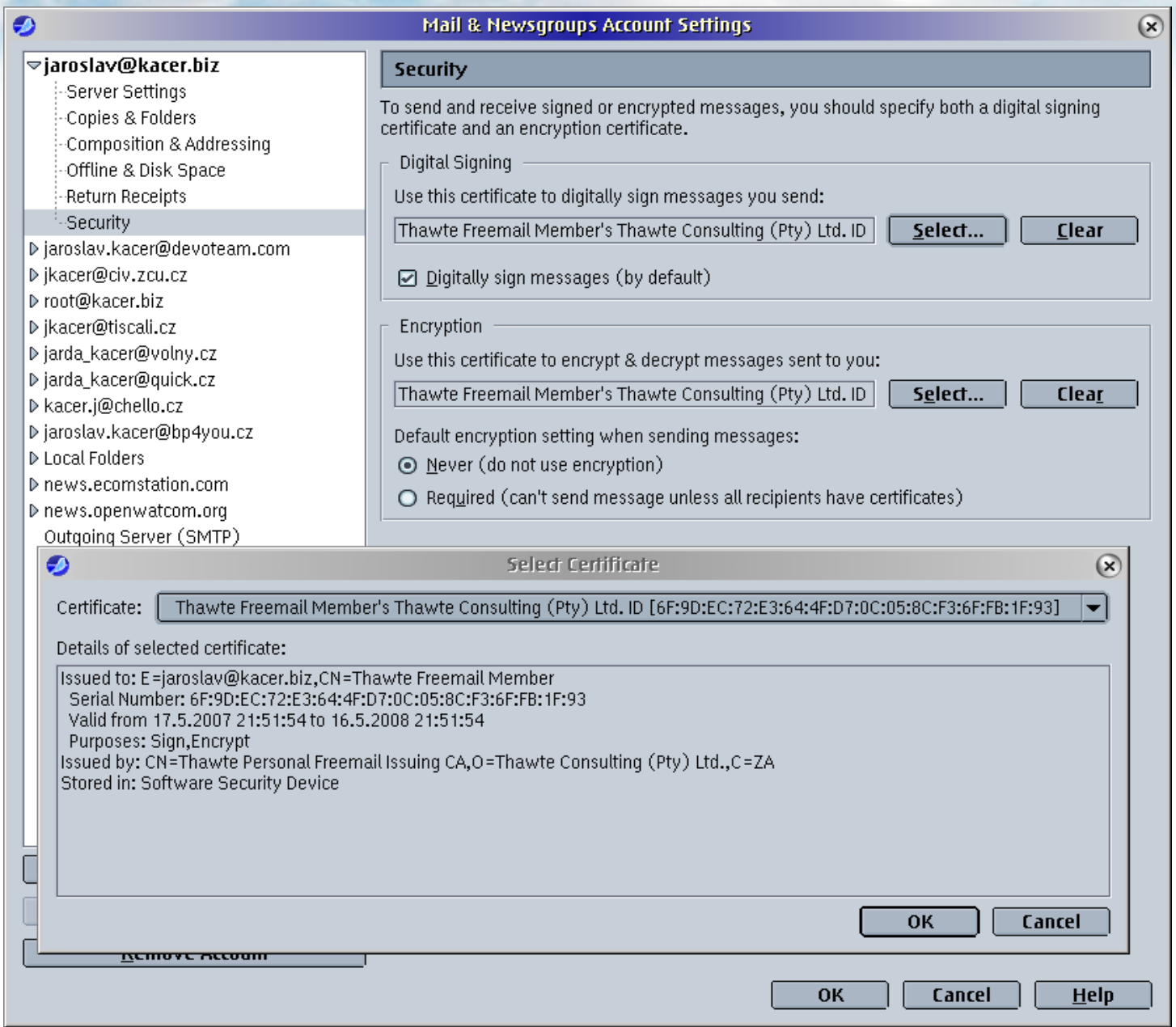
Odvolání certifikátu



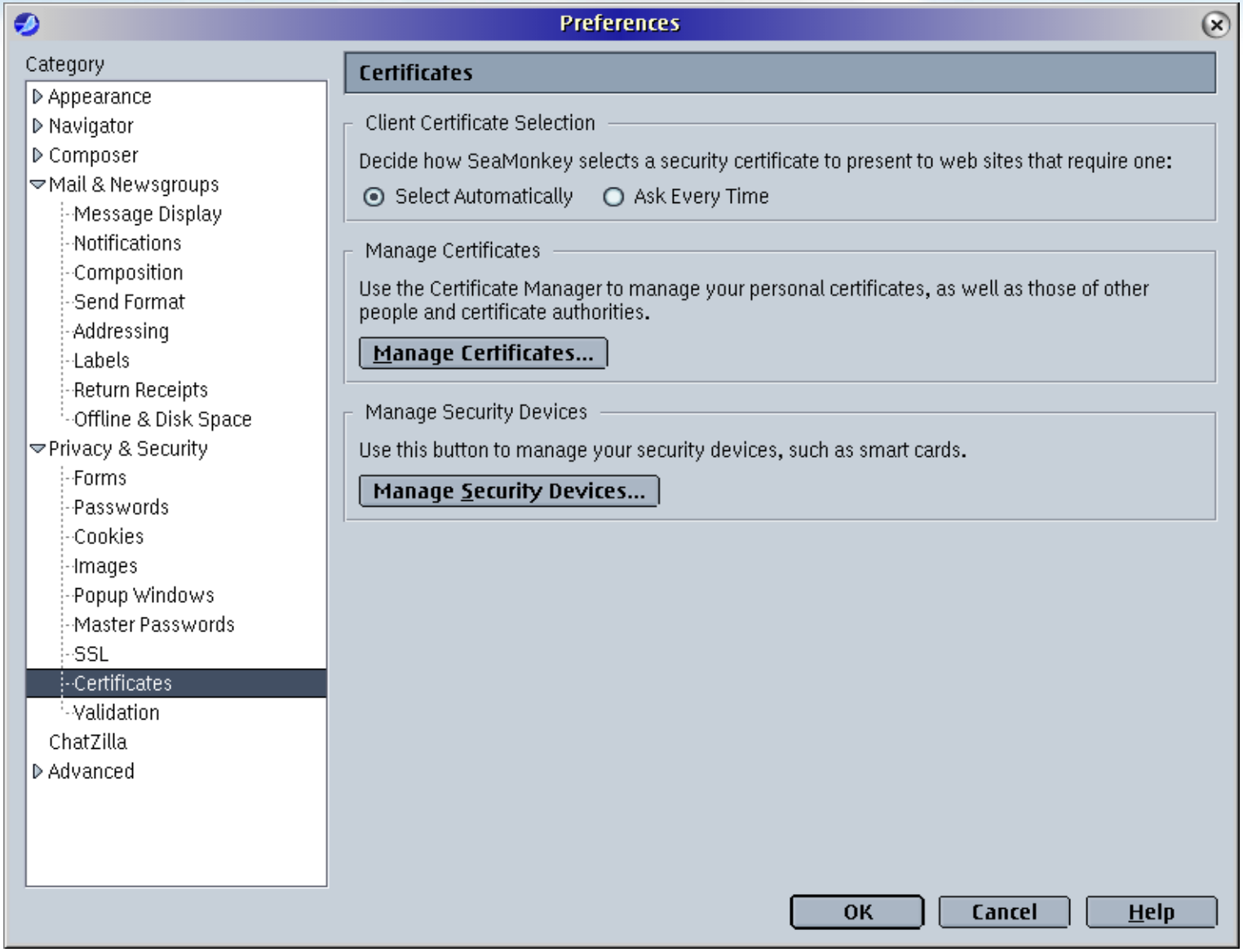
Thawte Web of Trust

- Nejdříve je součástí certifikátu jen emailová adresa, jméno uživatele = „Thawte Freemail Member“
- Existuje síť Thawte notářů, každý může přidělit určitý počet bodů
  - Nutno zaregistrovat na webu 2 doklady
  - Pak obcházet notáře
  - Po 50 bodech nárok na jméno – nový certifikát
  - Po 100 bodech se člověk stává notářem

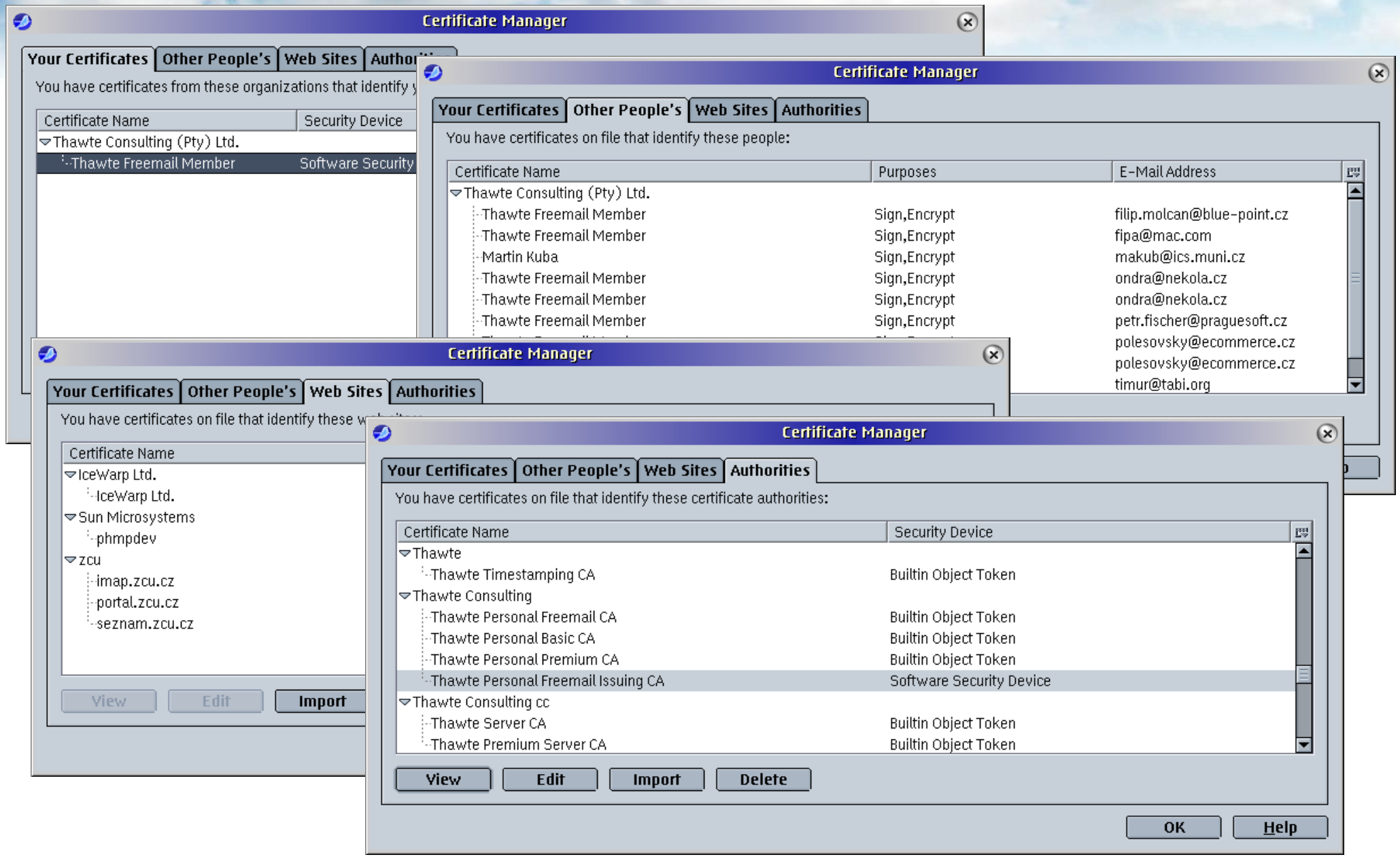
Výběr certifikátu pro použití



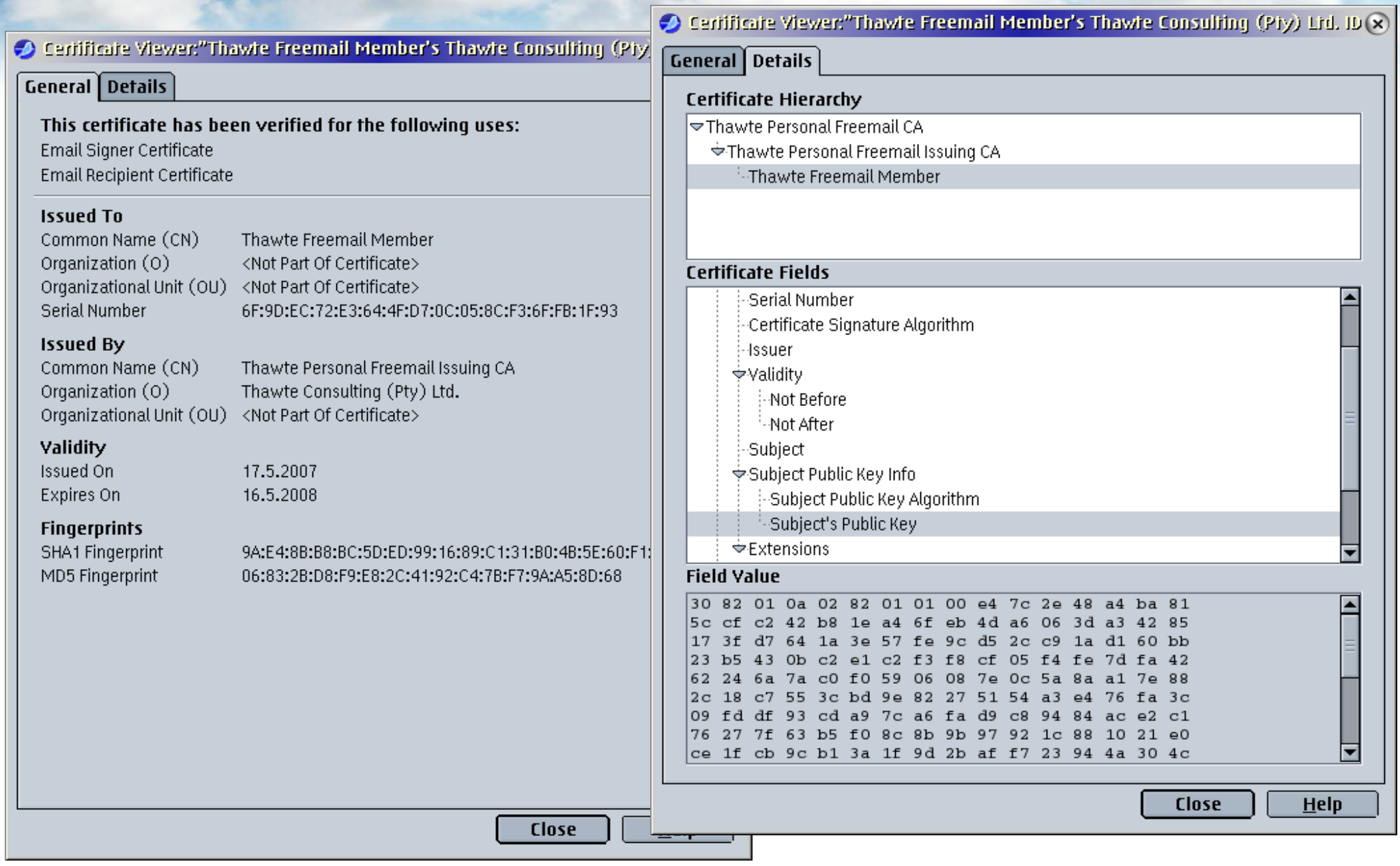
Úložiště certifikátů



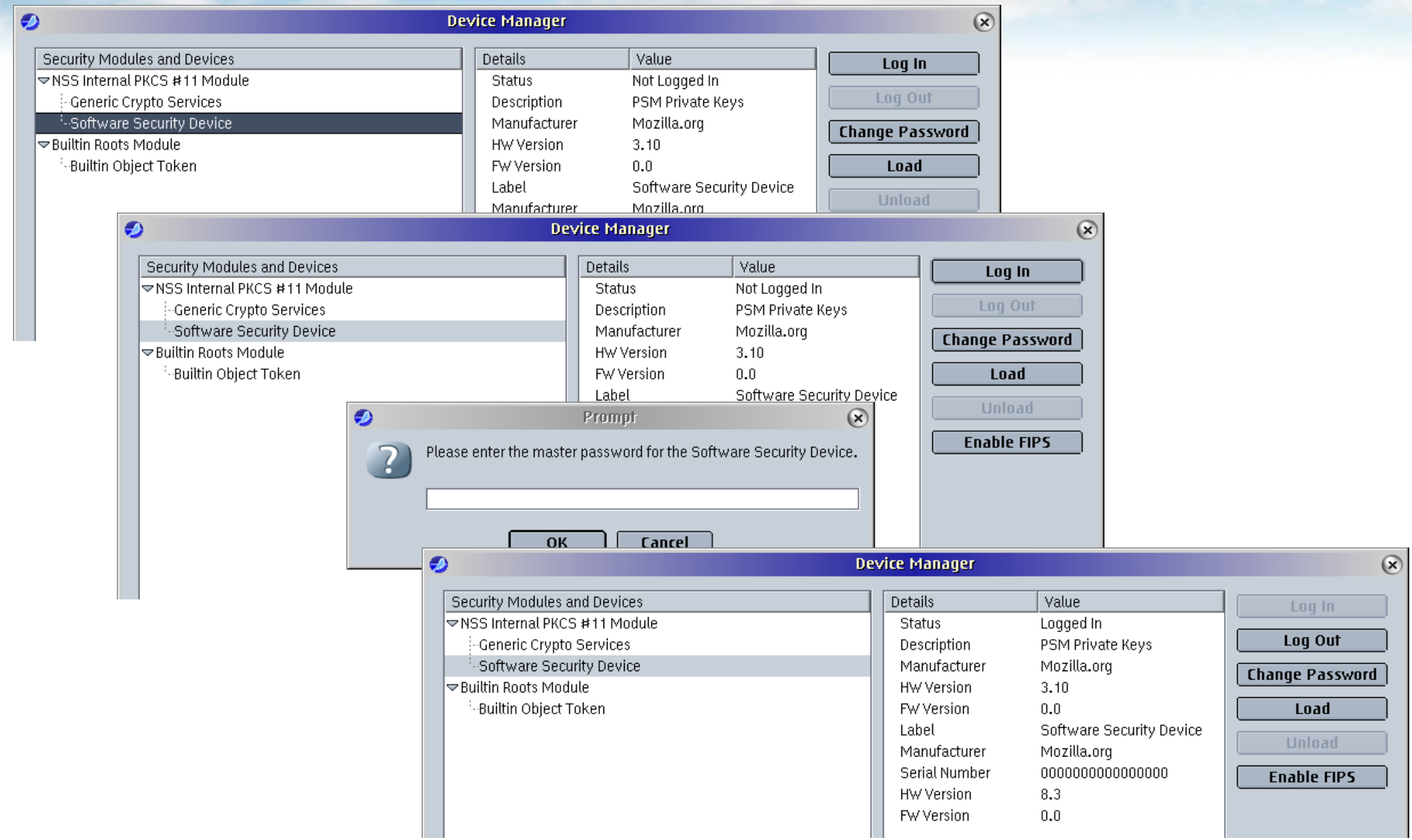
Správce certifikátů



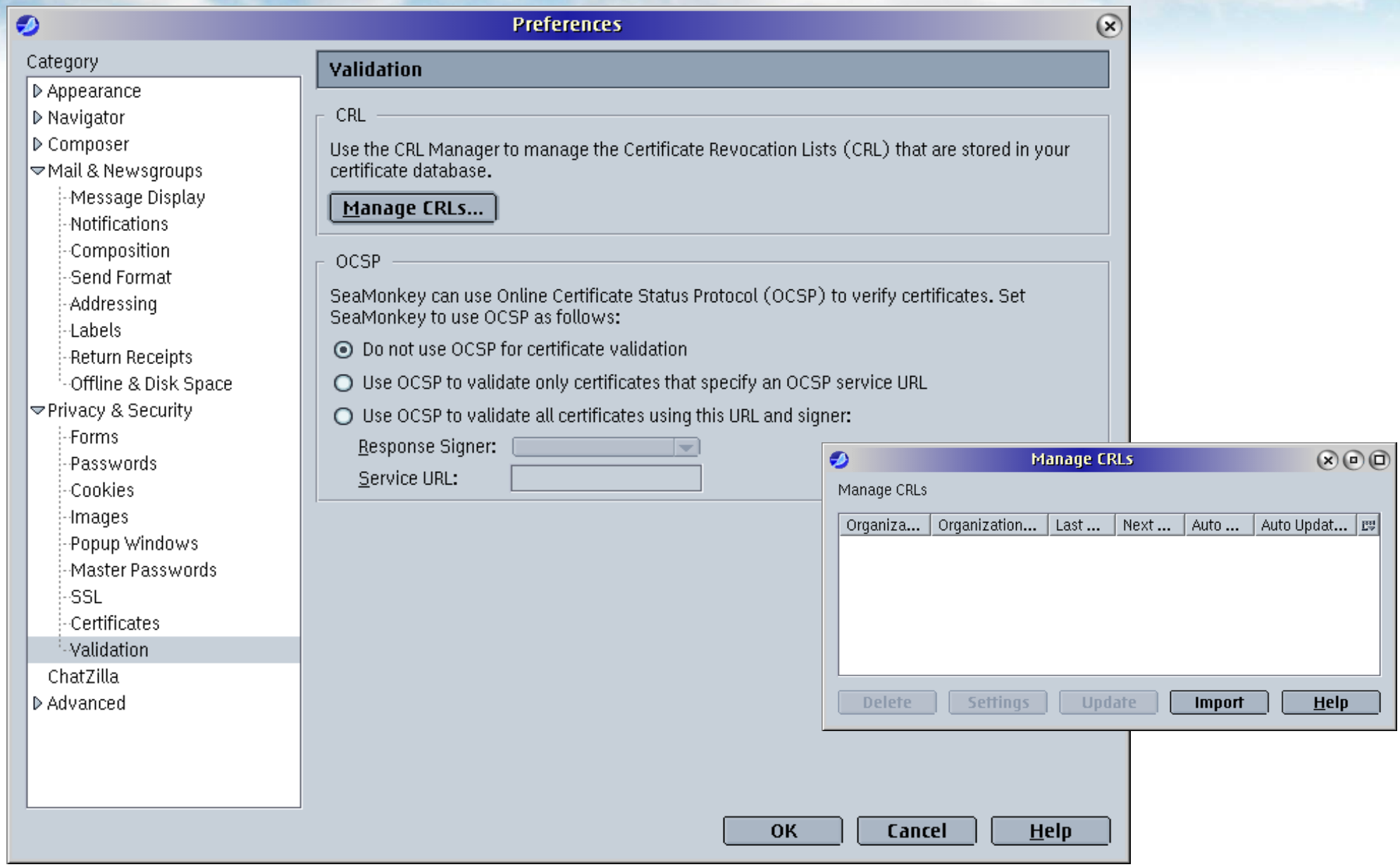
Detaily certifikátu



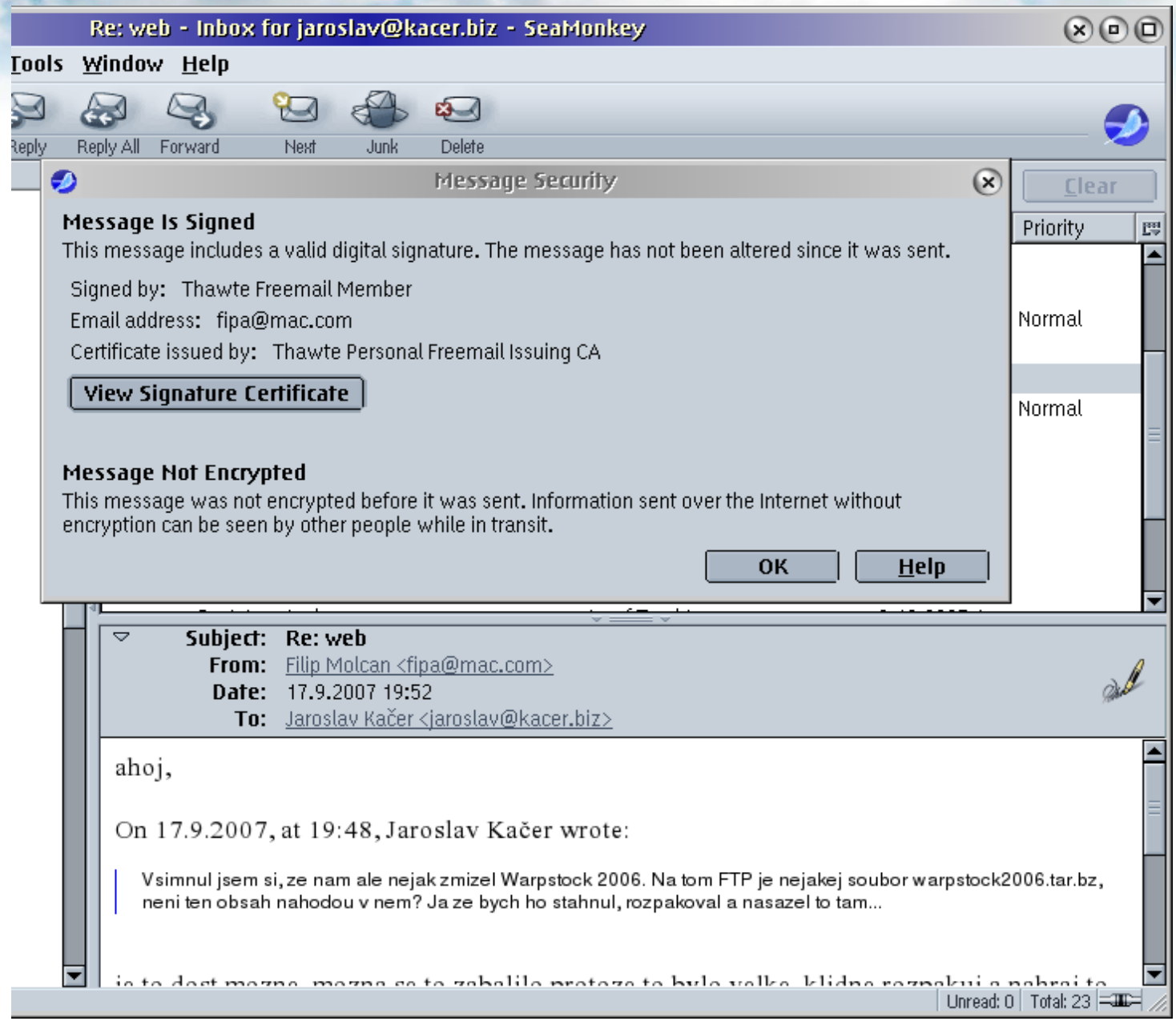
Software Security Device



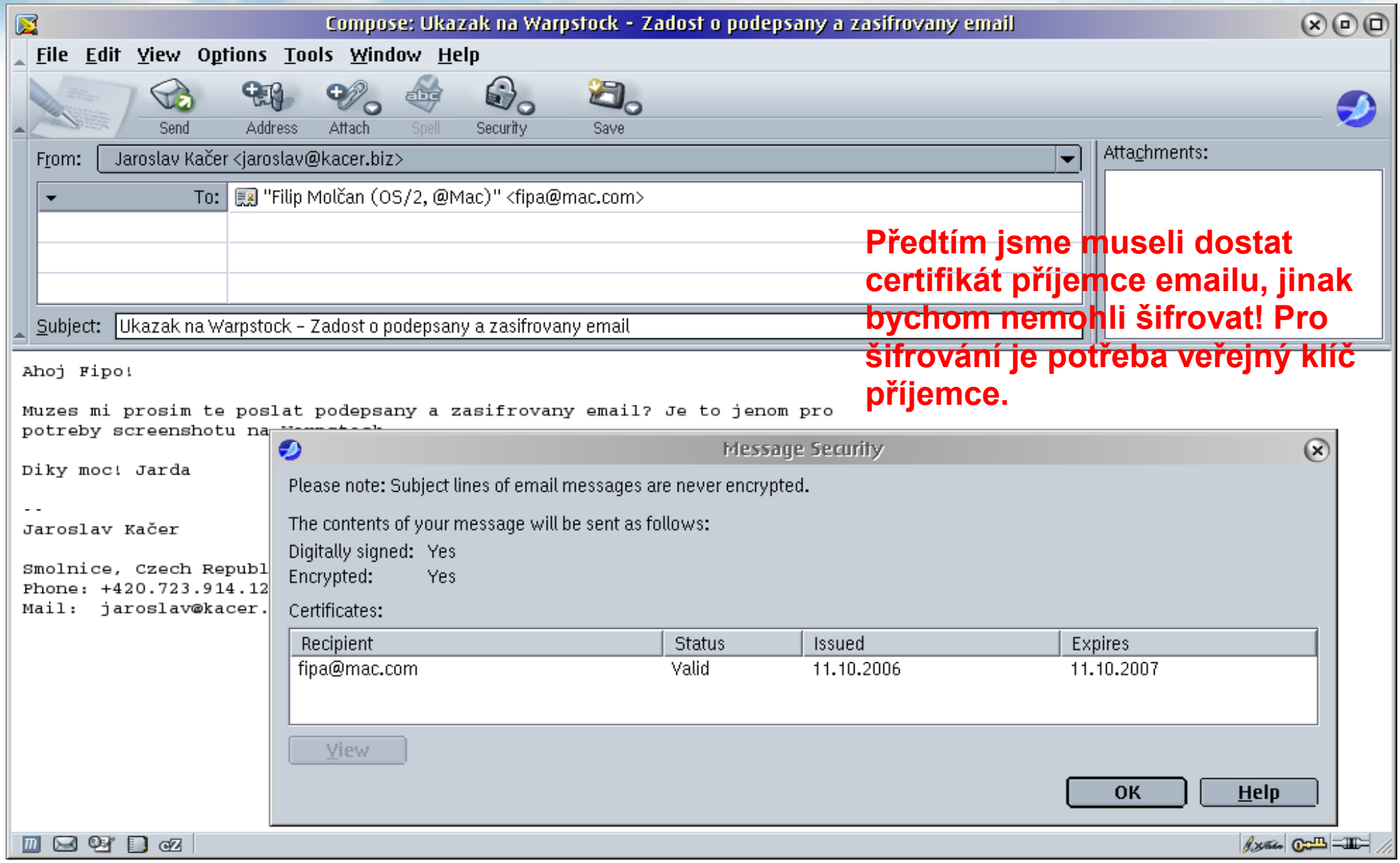
Ověřování certifikátů



Přišel podepsaný email...

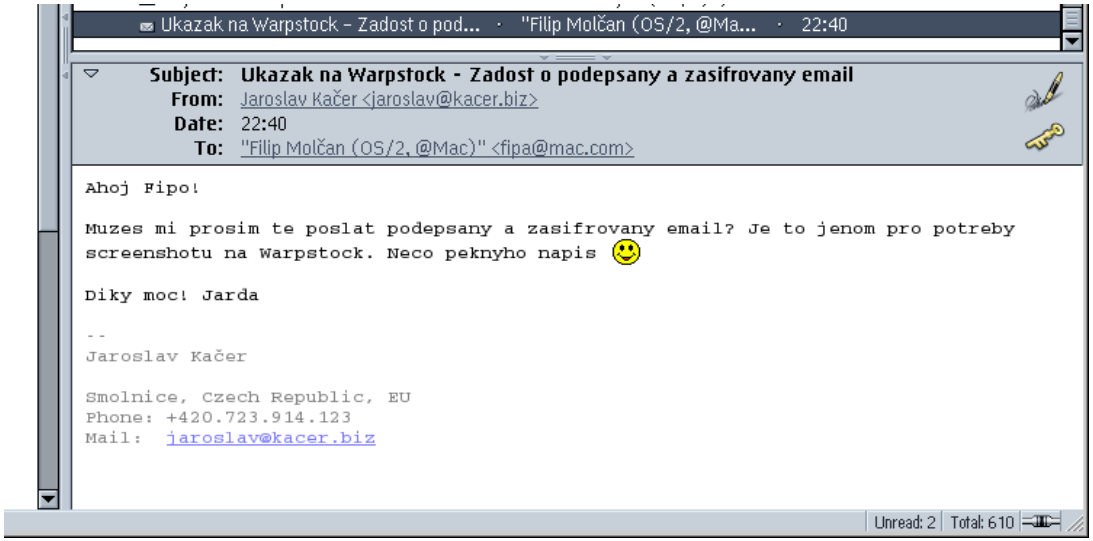


Posíláme email s podpisem a šifrovaně



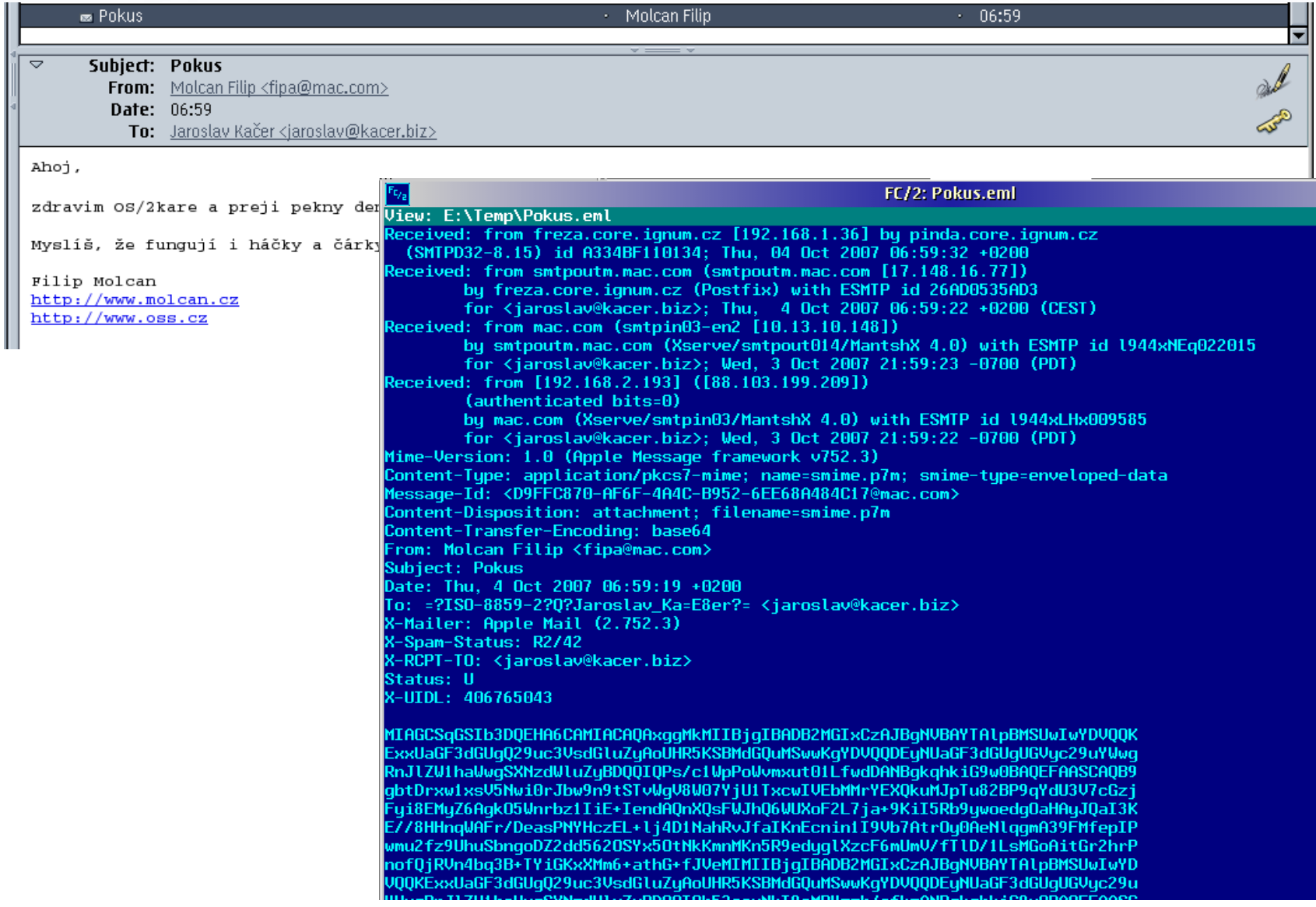
Předtím jsme museli dostat certifikát příjemce emailu, jinak bychom nemohli šifrovat! Pro šifrování je potřeba veřejný klíč příjemce.

Šifrovaný email v Sent složce

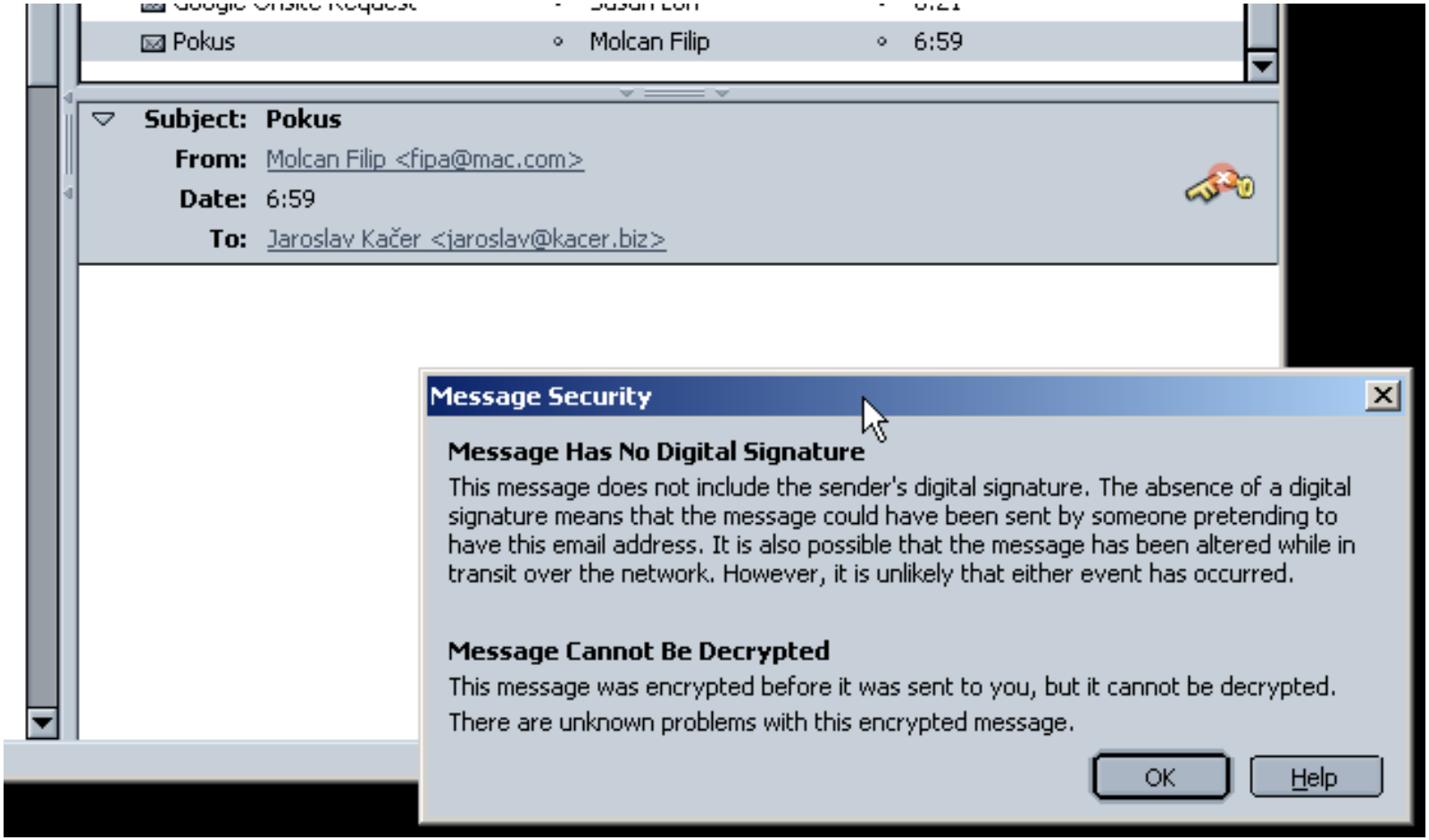


- Je uložen zašifrovaně
  - Přesto ho lze v Mozille přečíst (???)
  - V nějakých jiných programech ho přečíst nelze: webová poštovní aplikace apod.

Šifrovaný email na příjmu


Pokus · Molcan Filip · 06:59
Subject: Pokus
From: Molcan Filip <fipa@mac.com>
Date: 06:59
To: Jaroslav Kačer <jaroslav@kacer.biz>
Ahoj,
zdravim OS/2kare a preji pekny der
Myslíš, že fungují i háčky a čárky
Filip Molcan
http://www.molcan.cz
http://www.oss.cz
FC/2: Pokus.eml
View: E:\Temp\Pokus.eml CP852 45.74%
Received: from freza.core.ignum.cz [192.168.1.36] by pinda.core.ignum.cz
(SMTPD32-8.15) id A334BF110134; Thu, 04 Oct 2007 06:59:32 +0200
Received: from smtpoutm.mac.com (smtpoutm.mac.com [17.148.16.77])
by freza.core.ignum.cz (Postfix) with ESMTP id 26AD0535AD3
for <jaroslav@kacer.biz>; Thu, 4 Oct 2007 06:59:22 +0200 (CEST)
Received: from mac.com (smtpin03-en2 [10.13.10.148])
by smtpoutm.mac.com (Xserve/smtpout014/MantshX 4.0) with ESMTP id l944xNEq022015
for <jaroslav@kacer.biz>; Wed, 3 Oct 2007 21:59:23 -0700 (PDT)
Received: from [192.168.2.193] ([88.103.199.209])
(authenticated bits=0)
by mac.com (Xserve/smtpin03/MantshX 4.0) with ESMTP id l944xLHx009585
for <jaroslav@kacer.biz>; Wed, 3 Oct 2007 21:59:22 -0700 (PDT)
Mime-Version: 1.0 (Apple Message framework v752.3)
Content-Type: application/pkcs7-mime; name=smime.p7m; smime-type=enveloped-data
Message-Id: <D9FFC870-AF6F-4A4C-B952-6EE68A484C17@mac.com>
Content-Disposition: attachment; filename=smime.p7m
Content-Transfer-Encoding: base64
From: Molcan Filip <fipa@mac.com>
Subject: Pokus
Date: Thu, 4 Oct 2007 06:59:19 +0200
To: =?ISO-8859-2?Q?Jaroslav_Ka=E8er?= <jaroslav@kacer.biz>
X-Mailer: Apple Mail (2.752.3)
X-Spam-Status: R2/42
X-RCPT-TO: <jaroslav@kacer.biz>
Status: U
X-UIDL: 406765043
MIAGCSqGSIb3DQEHA6CAMIACAQAxggMkMIIBjgIBADB2MGIxCzAJBgNVBAYTAlpBMSUwIwYDVQQK
ExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMSwwKgYDVQQDEyNUaGF3dGUgUGVyc29uYWwg
RnJlZW1haWwgSXNzdWluZyBDQQIQPs/c1WpPoWvmxut01LfwdDANBgkqhkiG9w0BAQEFAASCAQB9
gbtDrxw1xsV5Nwi0rJbw9n9tSTvWgV8W07YjU1TxcwIVEbMMrYEXQkuMJpTu82BP9qYdU3V7cGzj
Fyi8EMyZ6AgkO5Wnrbz1IiE+IendAQnXQsFWJhQ6WUXoF2L7ja+9KiI5Rb9ywoedgOaHAyJQaI3K
E//8HHnqWAFr/DeasPNYHczEL+lj4D1NahRvJfaIKnEcnin1I9Vb7AtrOy0AeNlqgmA39FMfepIP
wmu2fz9UhuSbngoDZ2dd562OSYx5OtNkKmnMKn5R9edyglXzcF6mUmV/fTlD/1LsMGoAitGr2hrP
nofQjRVn4bq3B+TYiGKxXMm6+athG+fJVeMIMIIBjgIBADB2MGIxCzAJBgNVBAYTAlpBMSUwIwYD
VQQKExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMSwwKgYDVQQDEyNUaGF3dGUgUGVyc29u
```
```

Bez certifikátu nelze přečíst



Pozor!

- Nešifrují se hlavičky emailu, pouze tělo
- Vlastnost zašifrování se ztrácí:
  - Vytištěním na papír, screenshotem :-)
  - Uložením na disk u některých emailových klientů; Mozilla uloží mail v zašifrované podobě
  - Forward jako nový nešifrovaný email
    - Pokud se forwarduje zašifrovaný email, Mozilla sama zapne šifrování. Pak musíme mít veřejný klíč příjemce.
    - Pokud šifrování forwardu vypneme, příjemce dostane i původní zprávu (např. jako přílohu), i když nebyla původně určena jemu.

Závěr

- Je to zdarma
- Funguje to perfektně i na OS/2
- Přispívá k image pisatele
  - Stojí si za tím, co píše

Používejte digitální podpis!