

Používání certifikátů v elektronické poště

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

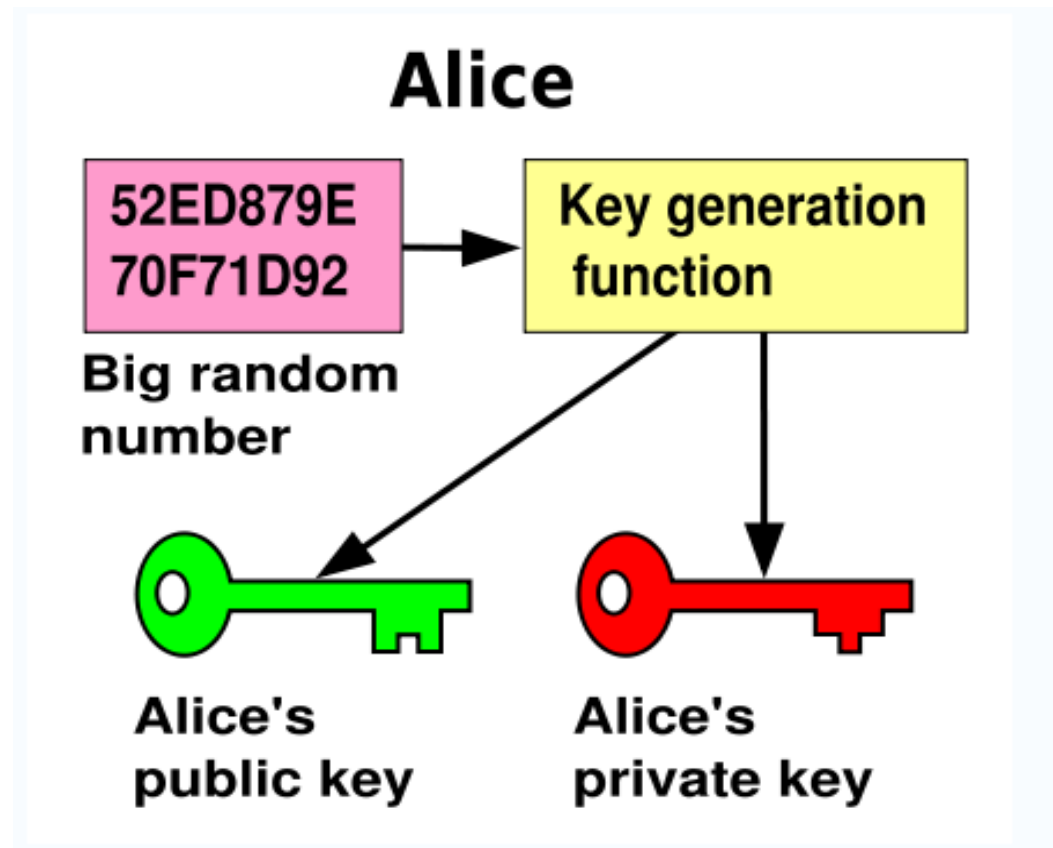
Jarda Kačer
jarda@kacer.biz

Český Warpstock 2007
Mladá Boleslav, 6.-7.10.2007

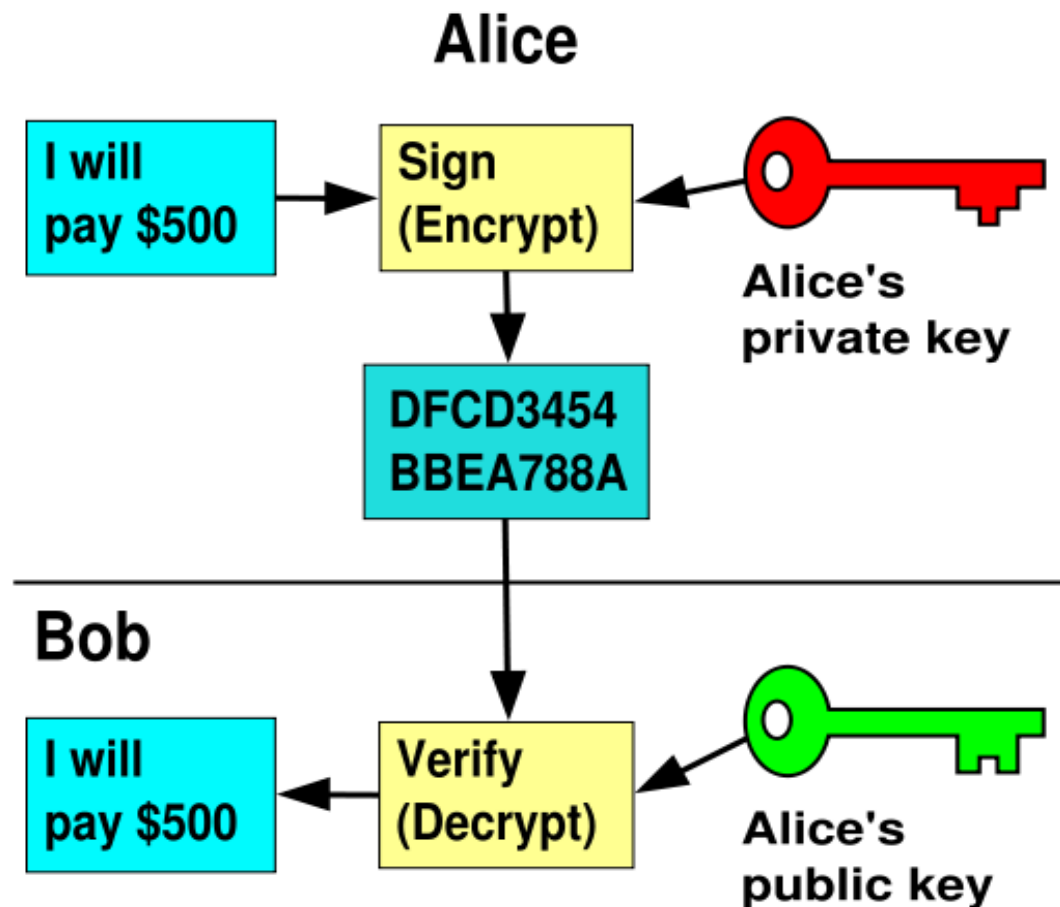
Co je to digitální podpis

- 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

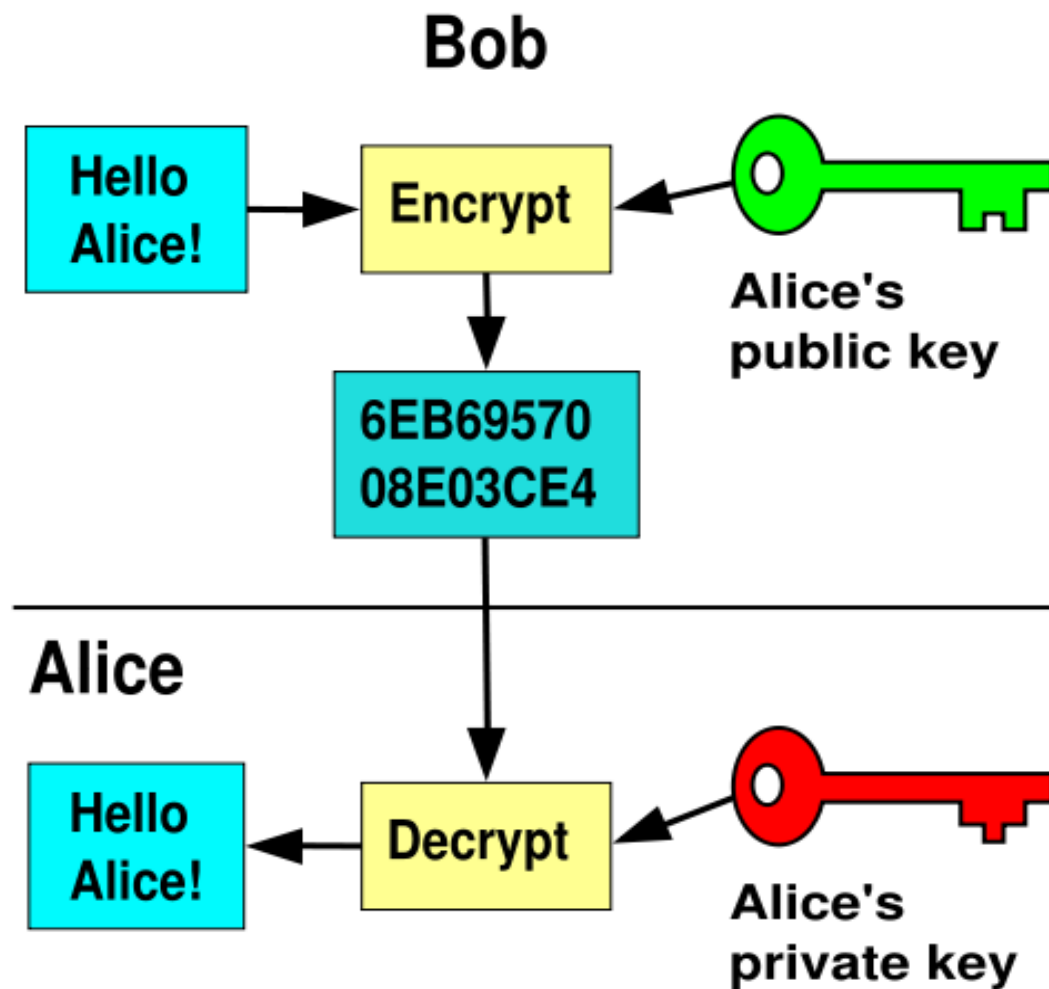


Digitální podpis – Podepsání



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 nainstalovány 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 submit your personal certificate application to **thawte**. By submitting these Terms and Conditions (certificate application) you are requesting that **thawte** issue a Personal Certificate (certificate) to you and are expressing your agreement to these terms.

TERMS OF USE FOR THAWTE PERSONAL CERTIFICATION 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 conditions then do not apply for, accept, or use such certificate(s). By clicking "Agree" below or by accepting or using a certificate, you agree to be 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 least 13 years old, but under 18, parental permission is required and all references to "you" shall include your parent(s). By clicking "Agree" 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** to enroll, please press "Next" below to sign up as a **thawte** Personal Certificate customer. You will then be able to request certificates to any of the most commonly used cryptographically-enabled applications available today - from Mozilla Firefox to Microsoft Outlook. Once again, thanks for choosing **thawte**.

By Clicking "Next" you agree to accept these Terms and Conditions. If you do not agree and accept these terms and conditions, do not click "Next".

[next](#)

https://www.thawte.com - New Registration

[New Registration in Thawte's Personal Certificate System]

Personal Cert System Enrollment

The first stage in this process is the establishment of your personal certificate information. This information will be captured only once and reused every time you request a certificate. It is difficult to change this information and information by us. **Please complete this enrollment ONCE only.**

If you are likely to enter characters that are not ASCII (e.g. non-English characters) on this page or subsequent pages of the enrollment process, please select an encoding or charset from the drop-down list box below. If you are unsure of what charset to choose click [here](#) to get a list of recommended charsets. The default charset choice is the recommended charset for your preference.

Charset For Text Input:

Name And Nationality

Please note that you need to be 13 years or older to enroll in the personal certificate 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

Nationality

[back](#) [next](#)

https://www.thawte.com - Requesting ID Information - SeatMonkey

[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

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



- [change password](#)
- [edit ID info](#)
- [change thawte ID](#)

certificates

my emails

wot console



a detailed status page for that entry.

Personal Identity Information

For more details on the assurance of your personal identity information, click [here](#).

Surname:	Kačer	Nationality:	Czech
Forenames:	Jaroslav	No Identity Number stored.	
Thawte ID:	JAROSLAV@KACER.BIZ	Date of Birth:	1978/04/19
Preferred Currency:	Czech Republic Koruna	Trust:	Untrusted

Employment Information

If your company uses the **thawte** Starter PKI for S/MIME and Client Authentication then you can have your title and position within the company certified, and can include this information in your certs. Click on your employment information to get detailed assurance information.

Employment Relationship: Trust:

No Employment Information.

Email Addresses

Your digital certificates can contain an email address, which is useful for S/MIME secure messaging. You need to have at least one trusted email address in the system before you can request certificates for S/MIME. You need to ping an email address before we can put it in your certificates. "Pinging" just means that **thawte** sends email to the address which requires a response from you. If you successfully respond, then we consider that email address "yours", in the sense that you can read email sent there.

Address:	Trust:	Date:
jaroslav@kacer.biz	Freemail	2007.05.17

Certificate Information

Below is a list of certificates you have requested, filtered if necessary. **You can select a certificate to view more status details.** You can change the filter on the list of certificates shown below by selecting the relevant certificate status from the dropdown box below and pressing "Filter". By default all the certificates you have ever requested are shown.

All Certificates Requested

Type:	Status:	Date:
Navigator:	Issued	Thu, 17 May, 2007, 19:53:15 GMT
Request Another		

Web of Trust Information

For a full list of your Web of Trust information [click here](#).

Vystavení certifikátu

thawte it's a trust thing

worldwide sites: [make your selection...] quick login: [make your selection >>]

Home Products Partners Buy Renew Trials Guides

Personal E-mail Certificates

[secure e-mail communication]

my account

certificates

- request a certificate
- view certificate status
- revoke a certificate

my emails

wot console

Secured by **thawte** 2007-10-01

About **thawte** | Consumer Awareness | © **thawte**, Inc. 1995-2006

[certificates available for request]

X.509 Format Certificates

For an X.509 certificate, please choose your software from the list below:

- Mozilla Firefox/Thunderbird, Netscape Communicator/Messenger
- Microsoft Internet Explorer, Outlook and Outlook Express
- Lotus Notes R5
- Opera Software Browser
- C2Net SafePassage Web Proxy

request

Home Products Partners Buy Renew Trials Guides Support Contact us

Personal E-mail Certificates

[secure e-mail communication]

my account

certificates

- request a certificate
- view certificate status
- revoke a certificate

my emails

wot console

Secured by **thawte** 2007-10-01

About **thawte** | Consumer Awareness | © **thawte**, Inc. 1995-2006 | Repository | Privacy Policy | Legal Notices

my account

You are about to request a certificate at the Freemail k...
Below you will see a list of each of the kinds of certifica...
as few as you like now that you have come this far!

request a certificate

view certificate status

revoke a certificate

request

test

view certificate status

Below is a list of certificates you have requested, filtered if necessary. **You can select a certificate to view more status details.** You can change the filter on the list of certificates shown below by selecting the relevant certificate status from the dropdown box below and pressing "Filter". By default all the certificates you have ever requested are shown.

All Certificates Requested filter

Type:	Status:	Date:
Navigator:	issued	Thu, 17 May, 2007, 19:53:15 GMT

Request Another

Odvolání certifikátu

The screenshot shows a web browser window with the address bar displaying "Choose Certificate to Revoke". The browser's toolbar includes various icons for bookmarks, cookies, CSS, forms, images, information, miscellaneous, outline, resize, tools, and view. The website header features the Thawte logo with the tagline "it's a trust thing" and navigation links for "Home", "Products", "Partners", "Buy", "Renew", "Trials", "Guides", "Support", and "Contact us". A "worldwide sites" dropdown menu is set to "make your selection..." and a "quick login" dropdown menu is set to "make your selection >>". A "[site map]" link is also present.

The main content area is titled "Personal E-mail Certificates" with the subtitle "[secure e-mail communication]". A sidebar on the left contains links for "my account", "certificates", "request a certificate", "view certificate status", "revoke a certificate", "my emails", and "wot console". The "certificates" section is expanded to show "revoke a certificate".

The "revoke a certificate" section contains the following text:

■ **revoke a certificate**

If you believe that your private key has been compromised, or you believe that the contents of a certificate are no longer accurate, then you should revoke the certificate. We sometimes revoke certificates automatically. **thawte** distributes a list of certificates that are invalid, called a Certificate Revocation List, to subscribers. It is also available off our web site, **here**. Attempting to use a revoked certificate will cause security alerts to be flagged.

Please choose the certificate you wish to revoke from the list of current, valid, unrevoked certificates below:

Navigator 2007.05.17 Serial: 148364293889966985095631578378163396499

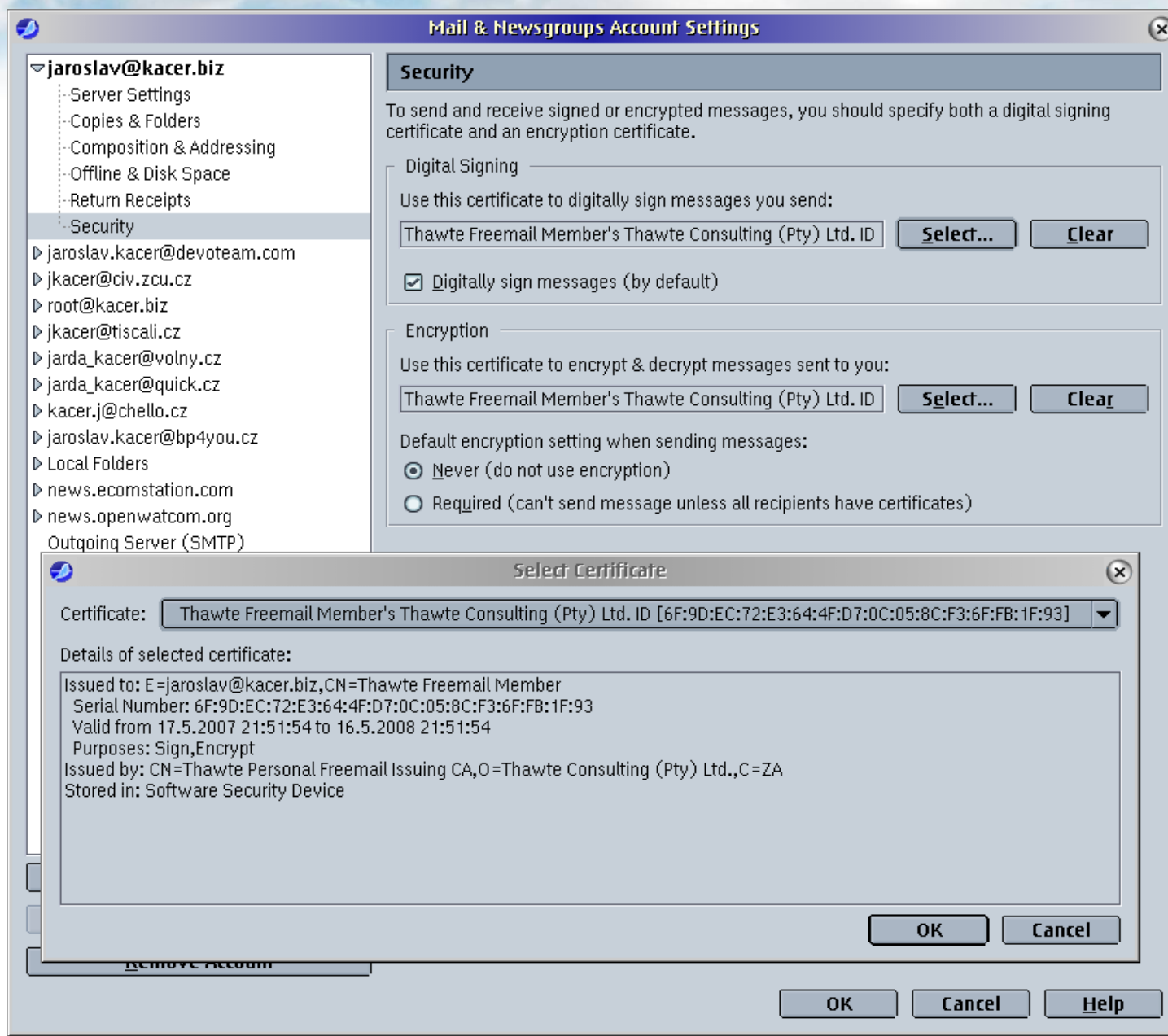
Clicking on a certificate will take you to a page that gives the exact contents of the cert and allows you to confirm revocation.

At the bottom left, there is a "Secured by Thawte" logo with the date "2007-10-01". The footer contains the text: "About **thawte** | Consumer Awareness | © **thawte**, Inc. 1995-2006 | Repository | Privacy Policy | Legal Notices".

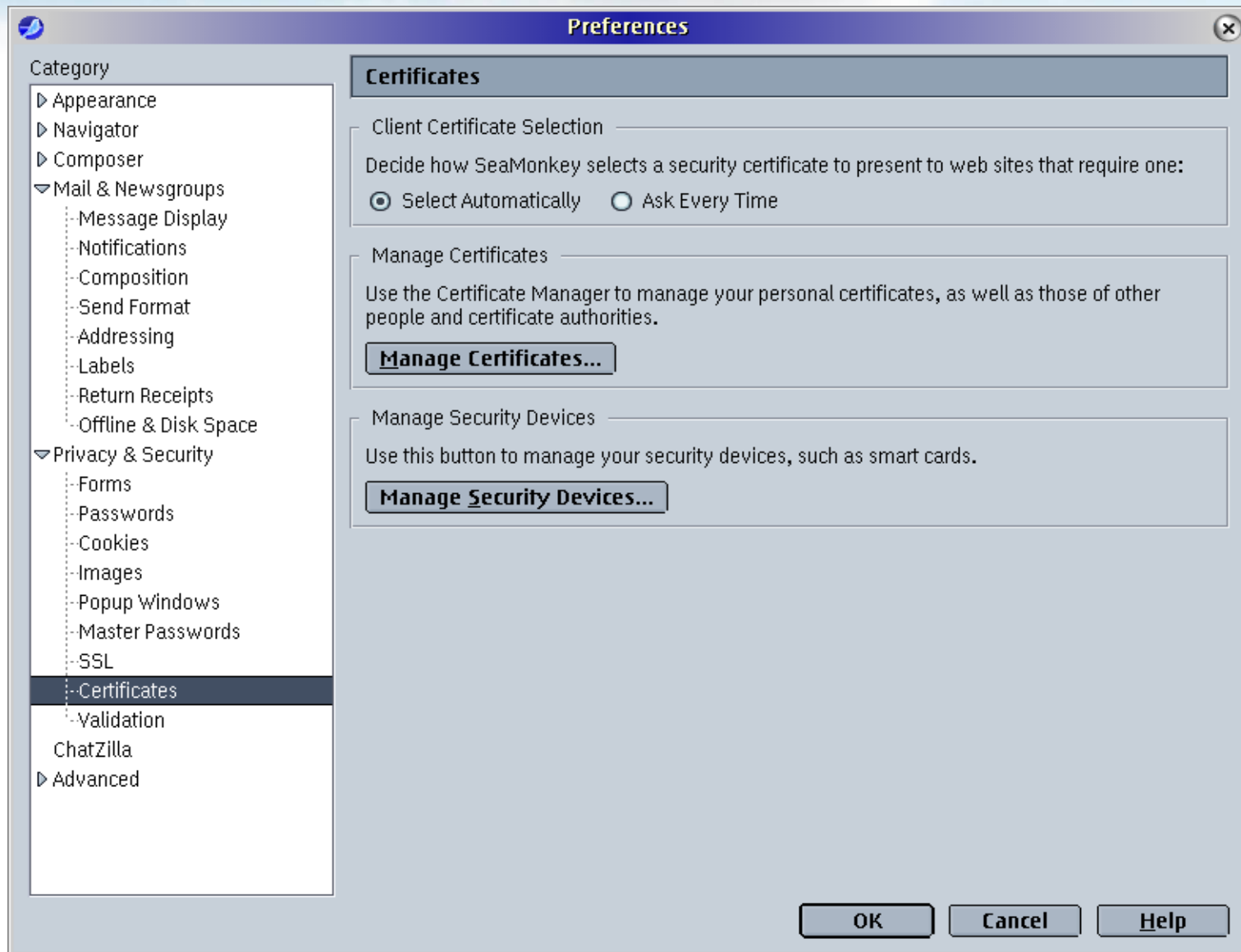
Thawte Web of Trust

- 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

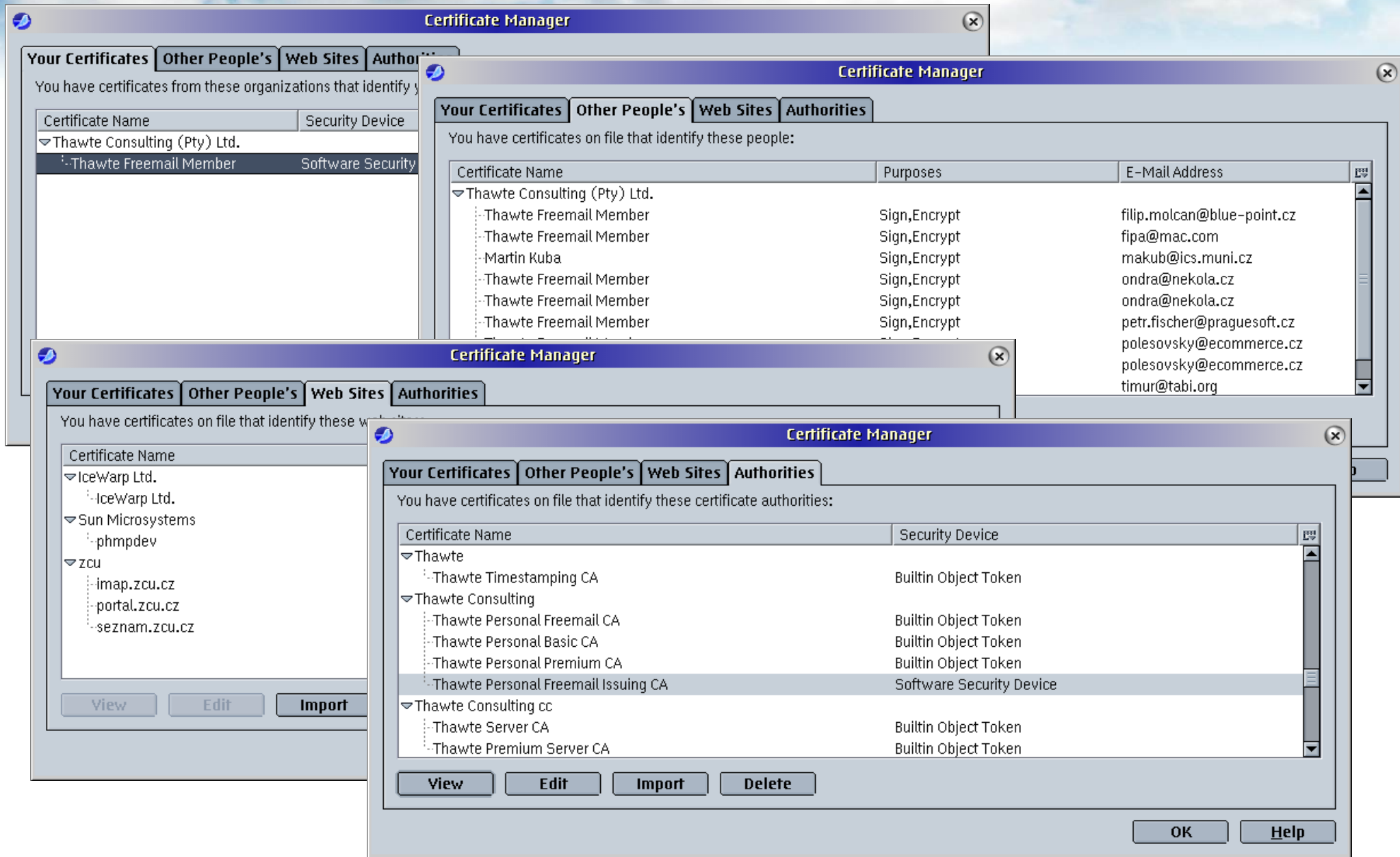
Výběr certifikátu pro použití



Úložiště certifikátů



Správce certifikátů



Detaily certifikátu

Certificate Viewer: "Thawte Freemail Member's Thawte Consulting (Pty) Ltd. ID

General | **Details**

This certificate has been verified for the following uses:
Email Signer Certificate
Email Recipient Certificate

Issued To

Common Name (CN)	Thawte Freemail Member
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	6F:9D:EC:72:E3:64:4F:D7:0C:05:8C:F3:6F:FB:1F:93

Issued By

Common Name (CN)	Thawte Personal Freemail Issuing CA
Organization (O)	Thawte Consulting (Pty) Ltd.
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	17.5.2007
Expires On	16.5.2008

Fingerprints

SHA1 Fingerprint	9A:E4:8B:B8:BC:5D:ED:99:16:89:C1:31:B0:4B:5E:60:F1:
MD5 Fingerprint	06:83:2B:D8:F9:E8:2C:41:92:C4:7B:F7:9A:A5:8D:68

Close

Certificate Viewer: "Thawte Freemail Member's Thawte Consulting (Pty) Ltd. ID

General | **Details**

Certificate Hierarchy

- Thawte Personal Freemail CA
 - Thawte Personal Freemail Issuing CA
 - Thawte Freemail Member

Certificate Fields

- Serial Number
- Certificate Signature Algorithm
- Issuer
- Validity
 - Not Before
 - Not After
- Subject
- Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key
- Extensions

Field Value

```
30 82 01 0a 02 82 01 01 00 e4 7c 2e 48 a4 ba 81
5c cf c2 42 b8 1e a4 6f eb 4d a6 06 3d a3 42 85
17 3f d7 64 1a 3e 57 fe 9c d5 2c c9 1a d1 60 bb
23 b5 43 0b c2 e1 c2 f3 f8 cf 05 f4 fe 7d fa 42
62 24 6a 7a c0 f0 59 06 08 7e 0c 5a 8a a1 7e 88
2c 18 c7 55 3c bd 9e 82 27 51 54 a3 e4 76 fa 3c
09 fd df 93 cd a9 7c a6 fa d9 c8 94 84 ac e2 c1
76 27 7f 63 b5 f0 8c 8b 9b 97 92 1c 88 10 21 e0
ce 1f cb 9c b1 3a 1f 9d 2b af f7 23 94 4a 30 4c
```

Close **Help**

Software Security Device

The image displays three overlapping screenshots of the 'Device Manager' application, illustrating the process of logging in to a Software Security Device.

Top Screenshot: The 'Software Security Device' is selected in the left pane. The 'Details' pane shows the following information:

Details	Value
Status	Not Logged In
Description	PSM Private Keys
Manufacturer	Mozilla.org
HW Version	3.10
FW Version	0.0
Label	Software Security Device
Manufacturer	Mozilla.org

Buttons on the right include: Log In, Log Out, Change Password, Load, and Unload.

Middle Screenshot: A 'Prompt' dialog box is displayed over the Device Manager, asking for the master password:

Please enter the master password for the Software Security Device.

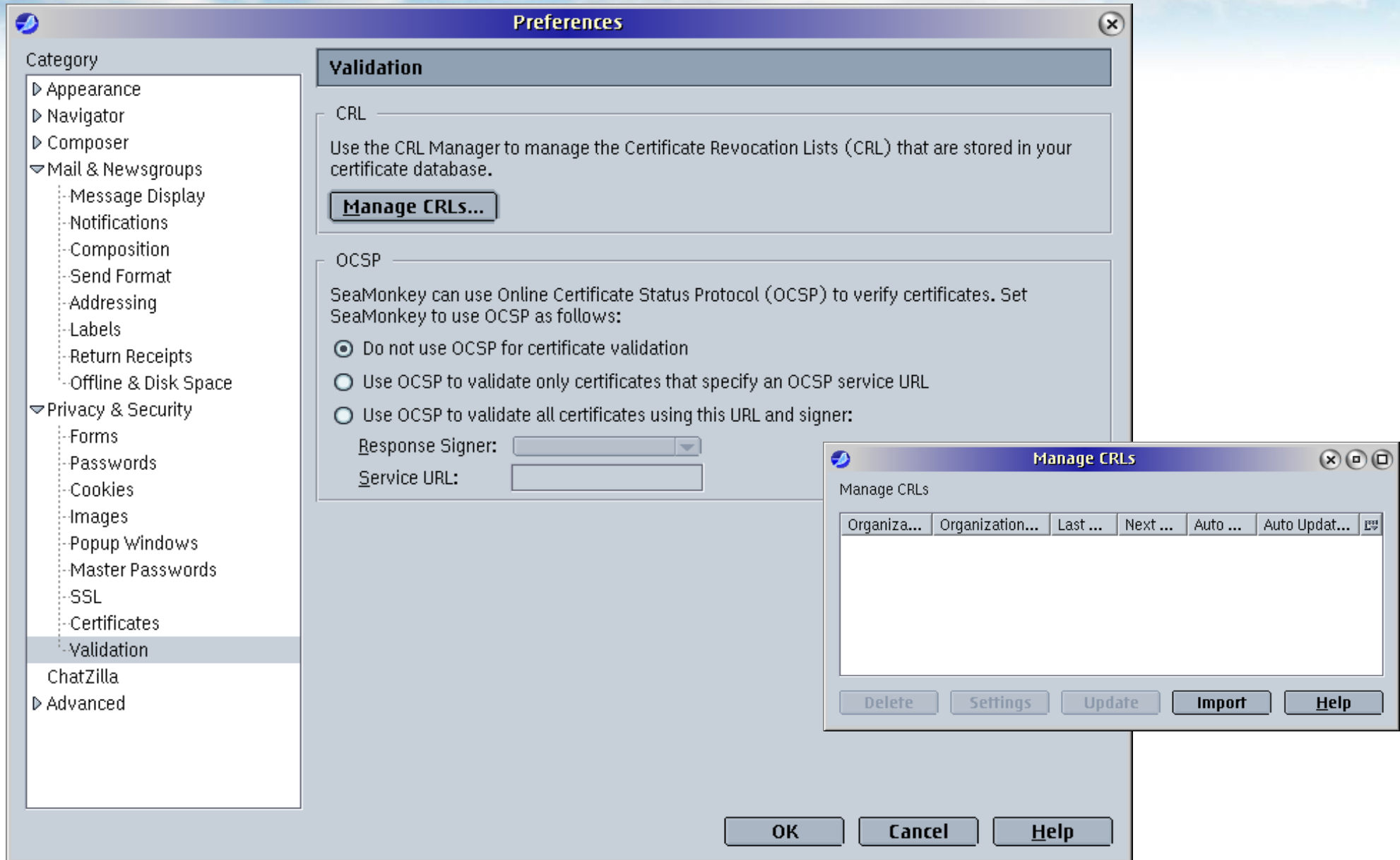
Buttons: OK, Cancel

Bottom Screenshot: The 'Software Security Device' is now logged in. The 'Details' pane shows the following information:

Details	Value
Status	Logged In
Description	PSM Private Keys
Manufacturer	Mozilla.org
HW Version	3.10
FW Version	0.0
Label	Software Security Device
Manufacturer	Mozilla.org
Serial Number	0000000000000000
HW Version	8.3
FW Version	0.0

Buttons on the right include: Log In, Log Out, Change Password, Load, Unload, and Enable FIPS.

Ověřování certifikátů



Přišel podepsaný email...

The screenshot shows the SeaMonkey email client interface. The window title is "Re: web - Inbox for jaroslav@kacer.biz - SeaMonkey". The menu bar includes "Tools", "Window", and "Help". The toolbar contains icons for "Reply", "Reply All", "Forward", "Next", "Junk", and "Delete". A "Message Security" dialog box is open, displaying the following information:

Message Is Signed
This message includes a valid digital signature. The message has not been altered since it was sent.
Signed by: Thawte Freemail Member
Email address: fipa@mac.com
Certificate issued by: Thawte Personal Freemail Issuing CA
[View Signature Certificate](#)

Message Not Encrypted
This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

Buttons: OK, Help

The background email header shows:

Subject: Re: web
From: Filip Molcan <fipa@mac.com>
Date: 17.9.2007 19:52
To: Jaroslav Kačer <jaroslav@kacer.biz>

The email body contains the text:

ahoj,

On 17.9.2007, at 19:48, Jaroslav Kačer wrote:

Vsimnul jsem si, ze nam ale nejak zmizel Warpstock 2006. Na tom FTP je nejakej soubor warpstock2006.tar.bz, neni ten obsah nahodou v nem? Ja ze bych ho stahnul, rozpakoval a nasazel to tam...

At the bottom right, the status bar shows "Unread: 0 Total: 23".

Posíláme email s podpisem a šifrovaně

The screenshot shows an email client window titled "Compose: Ukazak na Warpstock - Zadost o podepsany a zasifrovany email". The email is addressed to Filip Molčan (fipa@mac.com) and is signed and encrypted. A "Message Security" dialog box is open, displaying the encryption status and a table of certificates.

From: Jaroslav Kačer <jaroslav@kacer.biz>
To: "Filip Molčan (OS/2, @Mac)" <fipa@mac.com>
Subject: Ukazak na Warpstock - Zadost o podepsany a zasifrovany email

Attachments:

Message Security

Please note: Subject lines of email messages are never encrypted.

The contents of your message will be sent as follows:

Digitally signed: Yes
Encrypted: Yes

Certificates:

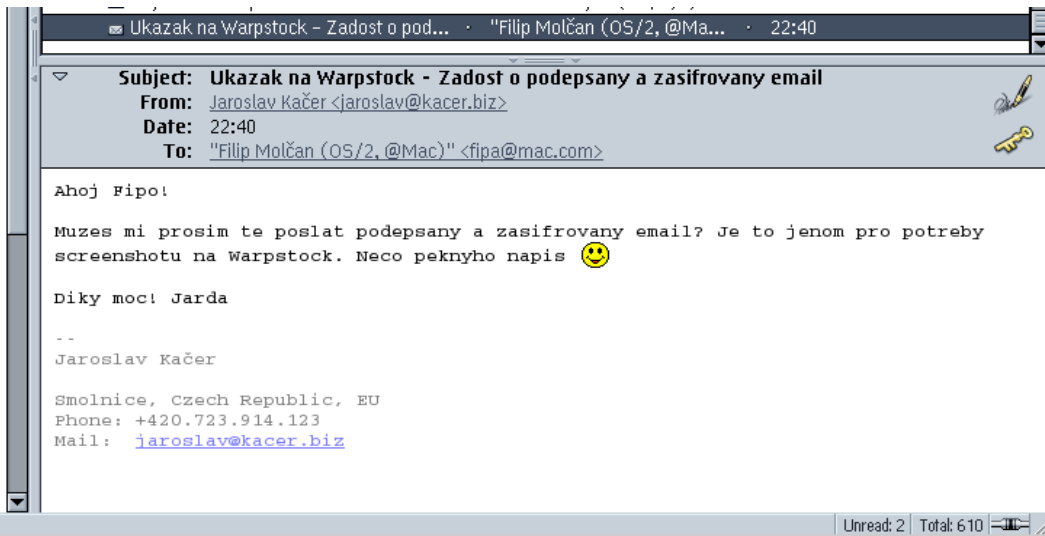
Recipient	Status	Issued	Expires
fipa@mac.com	Valid	11.10.2006	11.10.2007

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

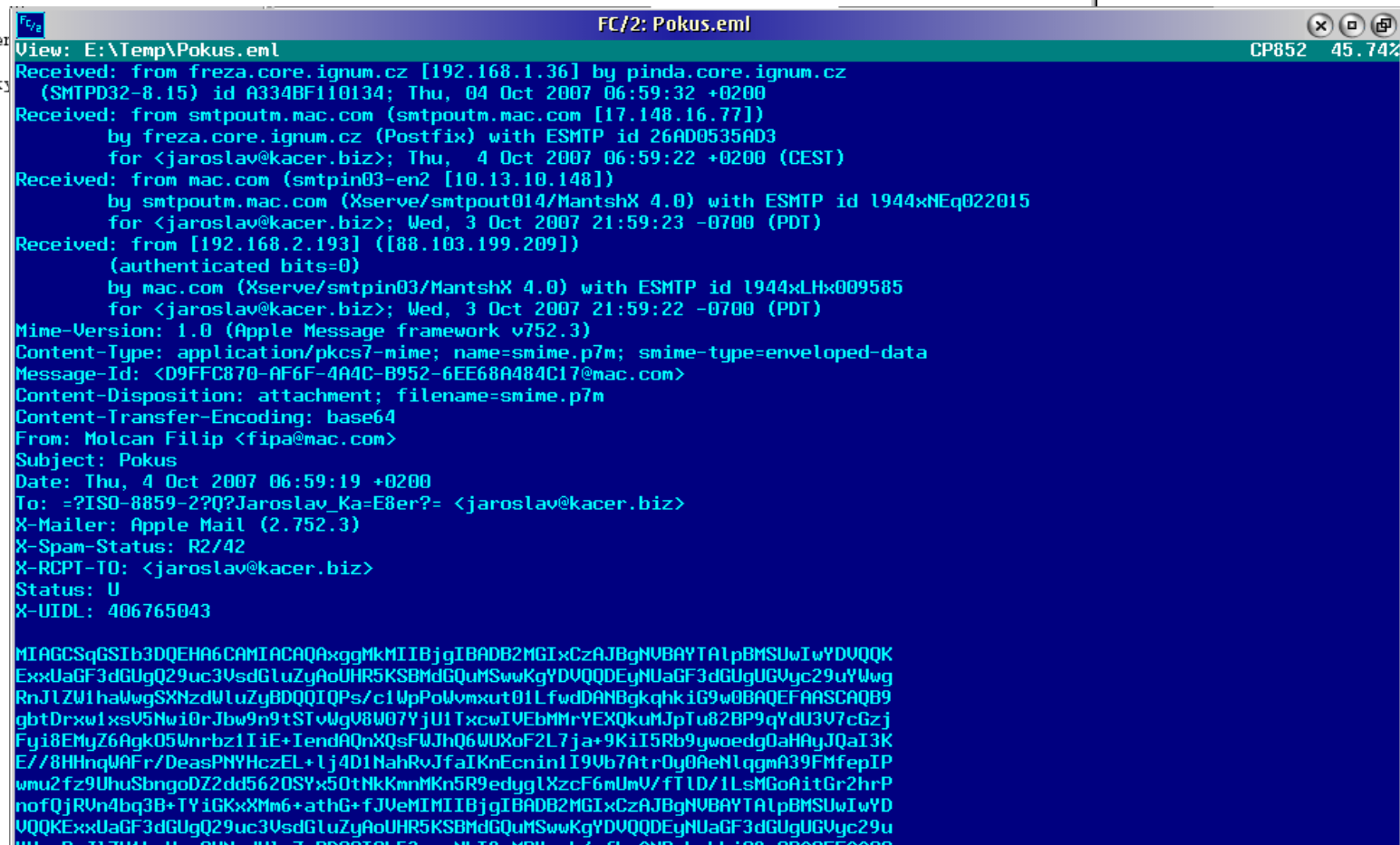
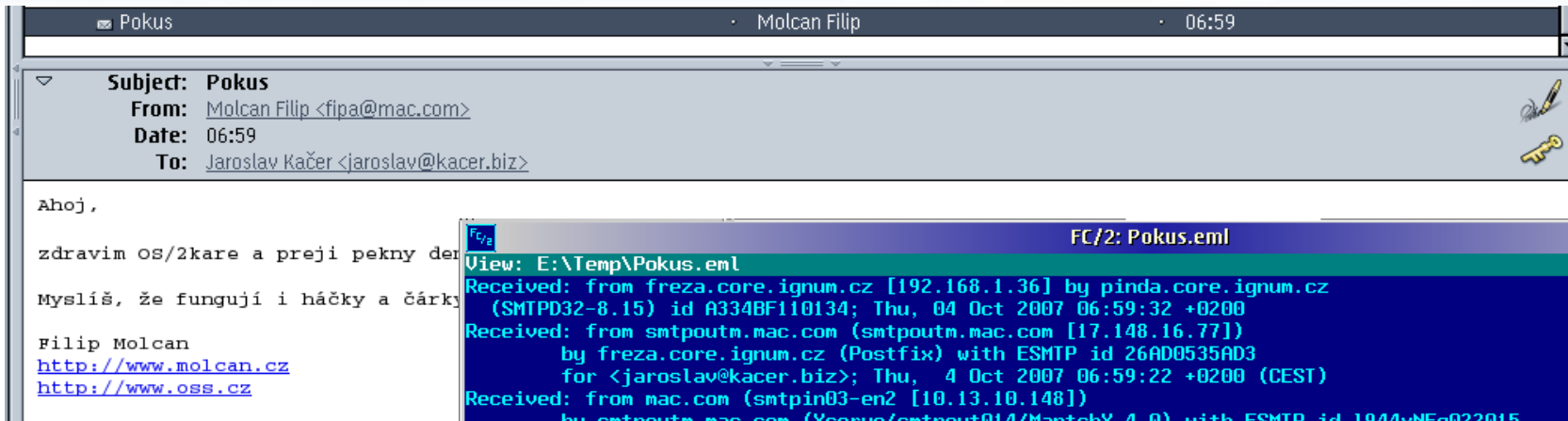
Ahoj Fipo!
Muzes mi prosim te poslat podepsany a zasifrovany email? Je to jenom pro potreby screenshotu na Warpstock.
Diky moc! Jarda
--
Jaroslav Kačer
Smolnice, Czech Republ
Phone: +420.723.914.12
Mail: jaroslav@kacer.

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



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!