

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.

eMails digital signieren unter Windows Mobile

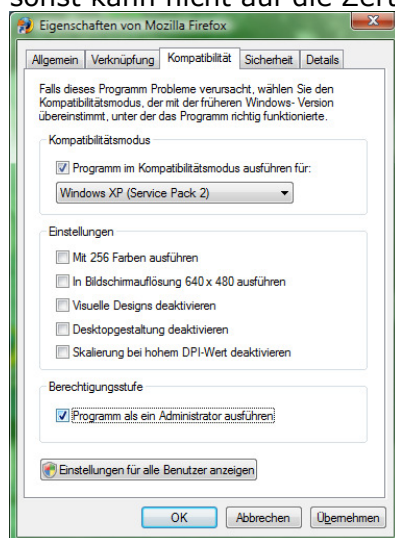
Den Absender einer eMail kann ja ziemlich jede Person ziemlich einfach fälschen. Wie kann man sich also absichern, zum Beispiel in der Geschäftskommunikation, dass das Gegenüber auch wirklich der oder diejenige ist? Seit 1995 gibt es dafür S/MIME (Englisch). Dabei wird, ganz vereinfacht gesagt, der Inhalt der eMail mit dem privaten Teil eines Zertifikat signiert und der öffentliche Teil davon angehängt, so dass die Empfängerseite dann mit dem öffentlichen Schlüssel prüfen kann, ob nichts an der eMail verändert wurde. Auch kann man damit auch gleich die ganze eMail verschlüsseln, wenn man den öffentlichen Schlüssel der Gegenseite kennt, und dann kann nur noch die Person, die den privaten Schlüssel besitzt, diese öffnen. Cool, oder?

Und wie bekommt man das nun auf Windows Mobile? Zu erst gibt es eine wichtige Grundvoraussetzung: Nur mit Exchange. Leider. Kein IMAP und kein POP3 wird dabei unterstützt, obschon es eigentlich in beiden Standards implementiert ist. Zweitens braucht man ein Zertifikat. Das kann man selber erstellen, z.B. mit OpenSSL und eine eigene Certificate Authority bilden, was aber wenig Sinn macht da dann jeder erst das Root-Zertifikat deines Servers herunterladen und diesem vertrauen muss, da dein eMail-Zertifikat auf diesem basiert. Also besorgt man sich von VeriSign, Thawte (beide Englisch) oder anderen grossen, offiziellen Autorisierungsstellen ein Zertifikat. CACert.org (Englisch) bietet leider keine gute Alternative, da auch hier erst das CACert-Root-Zertifikat installiert werden muss und auch das CACert-Prinzip nicht ganz unumstritten ist. Das ist aber hier offtopic.

Solche Zertifikatsausstellerfirmen verkaufen natürlich die Zertifikate, und das sogar ziemlich teuer. Wer jedoch darauf verzichten kann, dass im Zertifikat der eigene Name steht und nur die eMailadresse, und dass man damit keine Dateien, Programme oder sonstiges Signieren oder Verschlüsseln kann, ist mit dem gratis persönlichen eMail Zertifikat von Thawte (Englisch) gut bedient, darum nehme ich dies als Exempel. Im Folgenden nun also die Anleitung, wie man das bekommt, installiert und benutzt.

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.

Achtung: Das Zertifikaterstellen geht nicht im Internet Explorer 7 oder 8, nur im Internet Explorer 6 auf Windows XP. Deswegen entweder einen WinXP-Rechner mit einem alten Browser verwenden, einen Apple Macintosh mit OS X und Safari, oder den Mozilla Firefox 3, auch als [Portableapp](#) (Englisch). Ob voll installiert oder portabel, der Mozilla Firefox muss unter Vista (was ich hier als Beispiel aufführe, aber unter XP oder sonst wo funktioniert das ähnlich) im **Kompatibilitätsmodus für XP SP2** und als **Admin** laufen, sonst kann nicht auf die Zertifikatssteuerung zugegriffen werden:



Dann muss man zu erst einen Account bei Thawte einrichten:

Dazu geht man einfach auf <http://www.thawte.com/cgi/enroll/personal/step1.exe> (Englisch), liest sich die Terms and Conditions durch und bestätigt diese.

Nun müssen die grundlegenden Einstellungen getätigt werden:

1. Die Schriftkodierung muss gewählt werden. Für die Meisten ist „UTF-8 (best for UniCode)“ wohl das Beste. Aber auch „ISO-8859-1 (Latin 1)“ würde gehen mit Umlauten.
2. Namen und Geburtsdatum eintragen. Man muss ja älter als 13 sein.
3. Nationalität auswählen und
4. auf „Next“

Nun fragt Thawte nach der eMailadresse und ein paar anderen Daten wie dem Passwort. Daraufhin erhält man eine Bestätigung per eMail geschickt, die angeklickt und mit den entsprechenden Daten bestätigt werden muss:

[New Registration in Thawte's Personal Cert System]

Anmeldung für ein persönliches Zertifikat

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

If you are likely to enter characters that are not ASCII (ie accented characters) on this page or subsequent pages of the enrollment process, please choose a character encoding or charset from the drop-down list box below. If you are not sure what charset to choose click [here](#) to get a list of recommended charsets for languages. The default charset choice is the recommended charset for your browser language preference.

Charset For Text Input: UTF-8 (best for UniCode) 1.

Name und Staatsbürgerschaft

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: Jeanrenaud 2.

First Names or Given Names: Yves

Date Of Birth: Please give your date of birth. You need to specify the full year, including century. For example, "1973" or "1942".
15 März 1900

Nationality: Switzerland 3.

back next 4.

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.

Thawte Mail Ping

personal-cert-system@thawte.com

Die unnötigen Zeilennummern des Nachrichtentextes wurden automatisch entfernt.

Hi!

Hi!

Please use your browser to go to the following URL:

<https://www.thawte.com/cgi/enroll/personal/steps.exe>

Once you have connected successfully to the above address, you must copy and paste the "probe" and "ping" values below into the appropriate text boxes:

Probe:

Ping:

You should save this message until you have completed the enrollment process, just in case. But you MUST go to the above URL within 24 hours, or we will delete your request information and you'll have to start over!

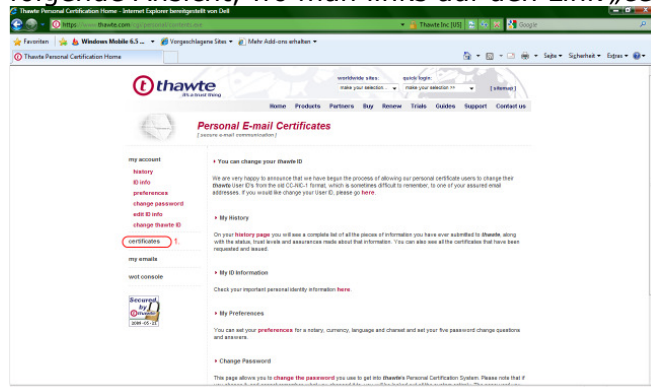
If you have problems completing the above please contact our support team by going to the following URL:

<https://www.thawte.com/cgi/support/contents.exe>

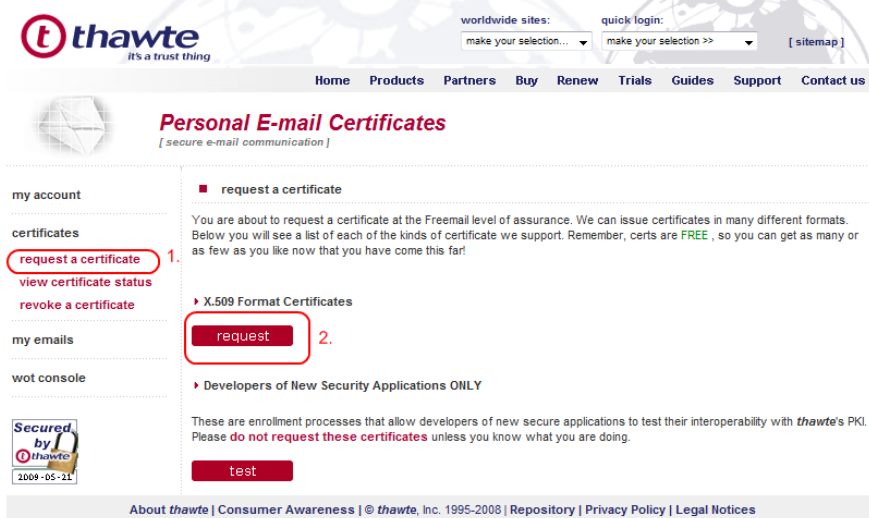
Regards,

The thawte team
thawte Certification

Nun kann man sich mit seiner bestätigten eMailadresse und dem Passwort <https://www.thawte.com/cgi/personal/contents.exe> (Englisch) einloggen und erhält folgende Ansicht, wo man links auf den Link „certificates“ klickt:



Dann auf 1. „request certificate“ und 2. unter „X.509 Format Certificates“ auf „request“:



Im Folgenden wählt man seinen Browser aus, damit das Zertifikat installiert werden kann:

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.

[certificates available for request]

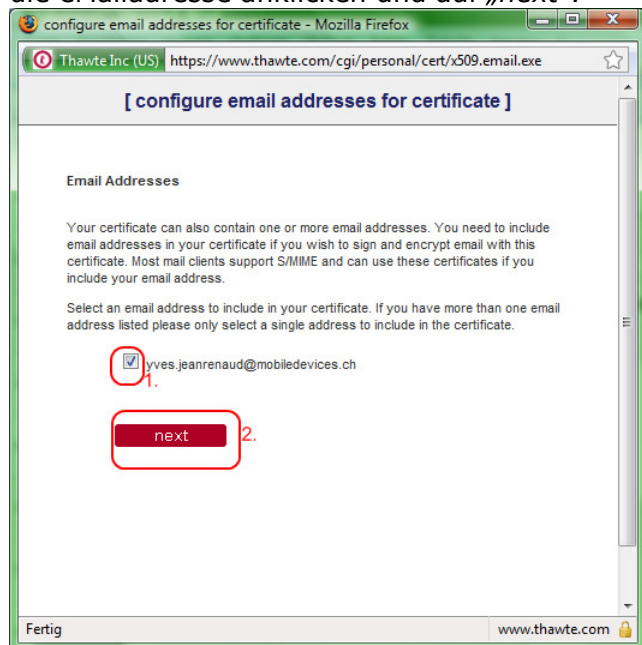
X.509 Format Certificates

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
- ☐ OperaSoftware Browser
- ☐ C2Net SafePassage Web Proxy

[request](#)

Dann bleibt die Auswahl auf „no employment information available“ und auf „next“, dann die eMailadresse anklicken und auf „next“:



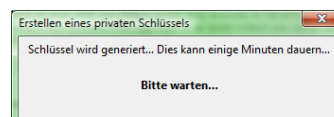
Wiederum „next“ und „accept“.

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.

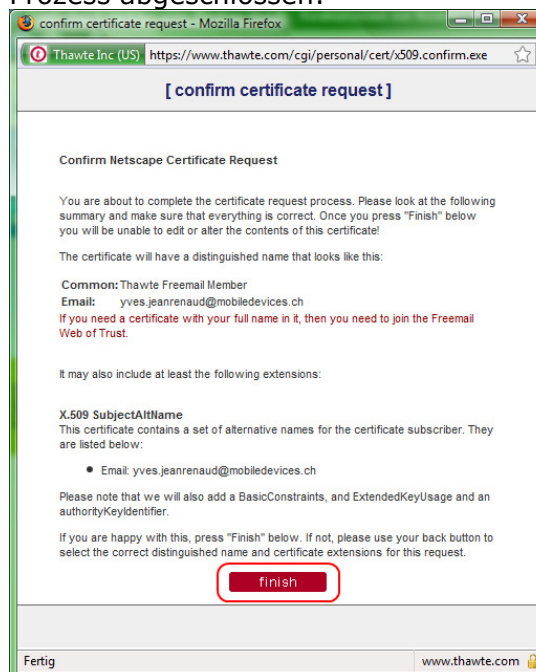
Public Key als „hochgradig“ auswählen und dann auf „next“:



Nun wird das Zertifikat erstellt:



Anschließend wird mit einem Klick auf „finish“ der Prozess abgeschlossen:



Dann holt man das Zertifikat ab:

Thawte Personal Cert Issued

Thawte Certificate Issuer [email-certs@thawte.com]

Die unnötigen Zeilenumbrüche des Nachrichtentextes wurden automatisch entfernt.

Am: Yves Jeanrenaud

Hello,

This is an automated message to let you know that we have just issued your personal certificate. You can retrieve it at:

<https://www.thawte.com/cgi/personal/cert/deliver.exe?serial=>

Remember, you will need your Thawte ID and password to access the Personal Certification System. You also need to be running the same browser, on the same machine, logged in as the same user, as you were when you made the request.

Note Netscape users: When fetch is clicked, nothing appears on the page, however the certificate is automatically downloaded into your browser.

Please have a look at the following solutions for download instructions:

<http://search.thawte.com/thawte/solution.jsp?id=vs10585>

Thanks for choosing Thawte!

The Customer Services Team
Thawte

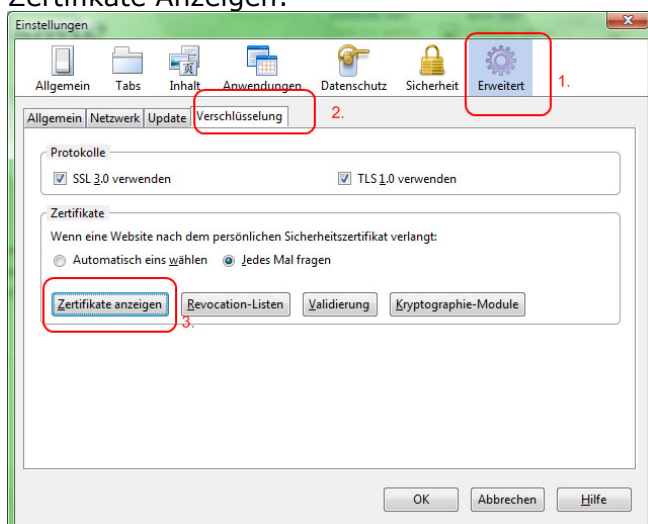
und speichert es im Schlüsselbund des

Firefox.

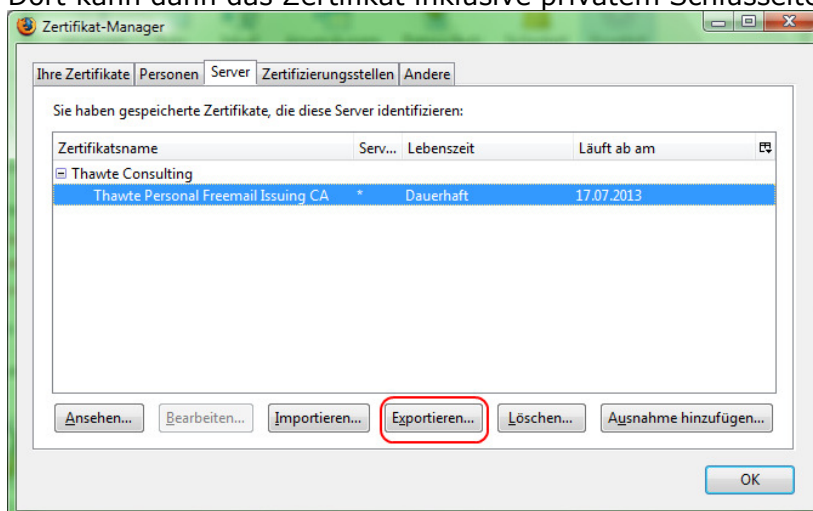
Nun muss das Zertifikat ja noch aus dem Firefox-Speicher raus. Wie also nun weiter?

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.

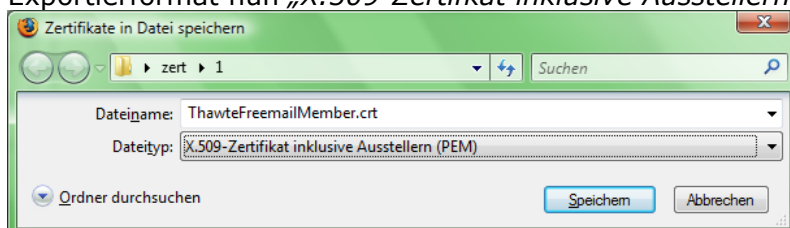
Einfach im Menü unter Extras>Einstellungen auf 1. Erweitert. 2. Verschlüsselung und 3. Zertifikate Anzeigen:



Dort kann dann das Zertifikat inklusive privatem Schlüsselteil exportiert werden:



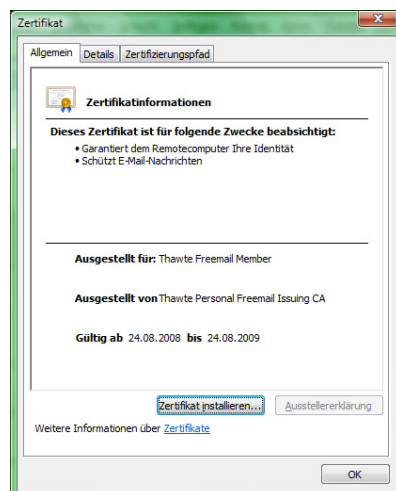
Warum das bei mir unter Server auftaucht, weiss ich nicht. Scheint ein Fehler zu sein. Jedenfalls wählt man als Exportierformat nun „X.509-Zertifikat inklusive Ausstellern (PEM)“:



Bei der Abfrage unbedingt das Zertifikat mit einem **guten** Passwort schützen, schliesslich ist hierin der private Schlüssel vorhanden!

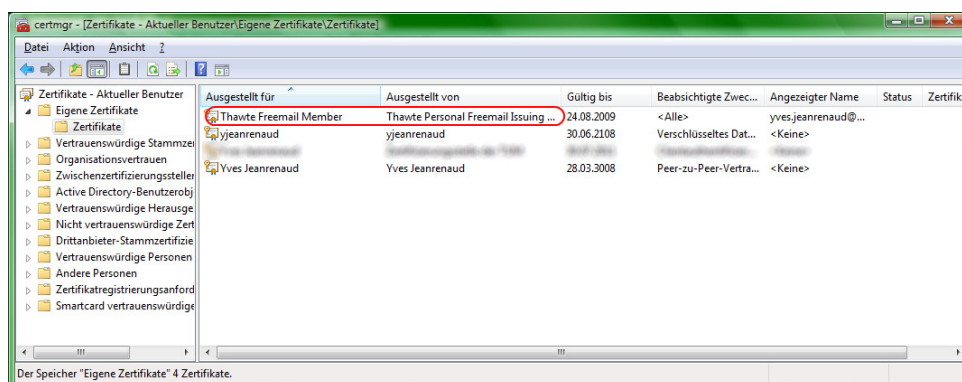
Dieses Zertifikat nun in den Windows Zertifikatsschlüsselbund importieren durch Doppelklick und „Zertifikat installieren...“ und dann einfach alles automatisch machen lassen:

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.



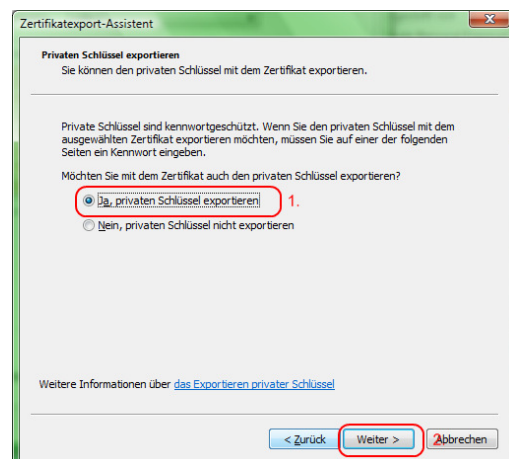
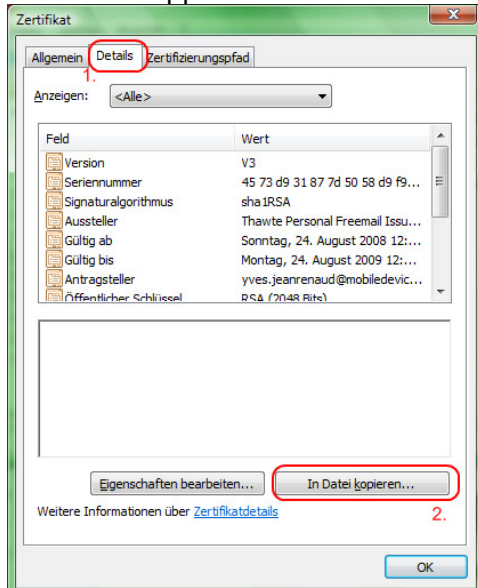
Nun kann das Zertifikat in ein PocketPC-kompatibles Format exportieren.

Einfach Start und „**cemgr.msc**“ ausführen. Dort unter eigene Zertifikate die Zertifikate anzeigen lassen: Dort sind Zertifikate zur Dateiverschlüsselung etc, die interessieren uns natürlich alle nicht, sondern das „*Thawte Freemail Member*“:

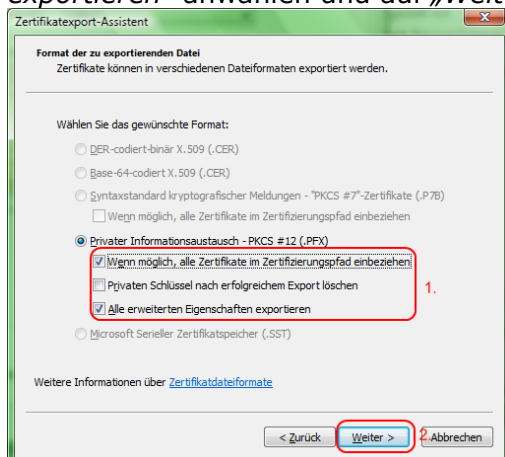


Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.

Dort mit Doppelklick öffnen und unter „Details“ einfach „In Datei kopieren...“ auswählen:

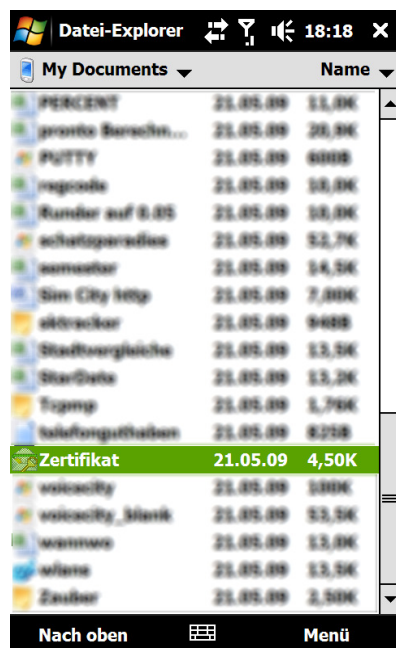


Dann auf „Weiter>“, „Ja, privaten Schlüssel exportieren“ und „Weiter>“
Nun „Privater Informationsaustausch – PKCS 12 (.PFX)“ und „Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen“ sowie „Alle erweiterten Eigenschaften exportieren“ anwählen und auf „Weiter>“:

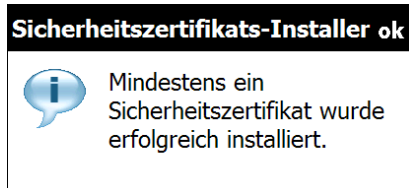


Wiederum wird man nach einem Passwort gefragt mit dem die Datei geschützt werden soll und anschliessend nach dem Dateinamen. Nun hat man eine Datei, die auf **.PFX** endet. Diese enthält den ganzen Schlüsselsatz, privat und öffentlich, also gebt wirklich Sorge zu der Datei. Am besten, ihr zieht eine Kopie auf eine CD und versteckt diese irgendwo sicher, vor allem getrennt vom Passwort.

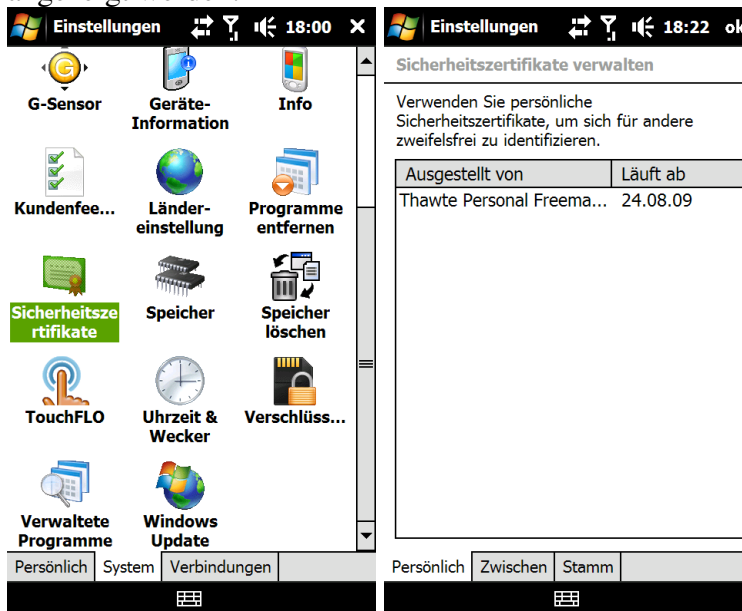
Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.



Die PFX kann nun auf den PocketPC kopiert und dort im DateiExplorer geöffnet werden. Man wird nach dem Passwort gefragt und anschliessend ist das Zertifikat installiert:



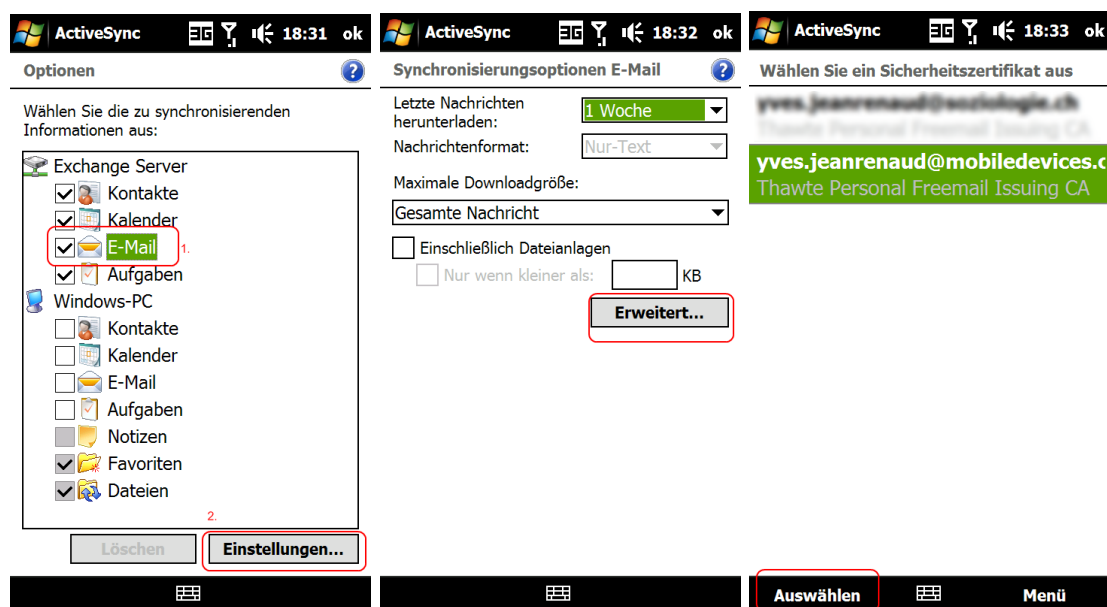
Unter Einstellungen>Sicherheitszertifikate kann dies nun angezeigt werden:



Nun kann die PFX-Datei wieder gelöscht werden.

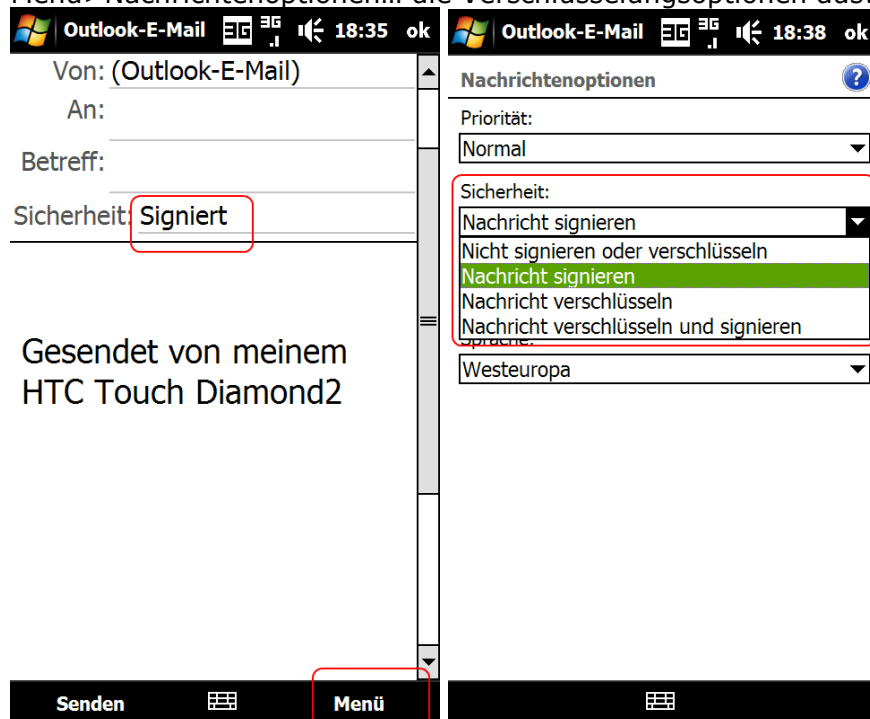
Aber das hilft uns ja alles noch nichts, wenn wir damit keine eMails signieren können. Also einfach unter ActiveSync>Menü>Optionen>Exchange Server „E-Mail“ auswählen und auf „Einstellungen...“, dann „Erweitert...“ und dann kann man das Häkchen bei „Alle ausgehenden E-Mails signieren“ und auf „Sicherheitszertifikat auswählen...“. Bestätigen und fertig.

Titel	EMAILS DIGITAL SIGNIEREN UNTER WINDOWS MOBILE
Autor	Yves Jeanrenaud (yves.jeanrenaud@mobiledevices.ch – nur für Feedback/Fehler! Kein Support!)
Aktualisiert	21.5.2009
Copyright	Dieses Dokument darf nicht ohne die ausdrückliche Erlaubnis des Autors oder von der Administration von mobiledevices.ch vervielfältigt werden, als Schulungsunterlage genutzt werden, auf anderen Website veröffentlicht werden, einzelne Teile daraus kopiert werden oder angepasst werden.



The screenshot shows the 'Optionen' (Options) screen in Windows Mobile. The 'Exchange Server' section is expanded, and 'E-Mail' is selected. The 'Synchronisierungsoptionen E-Mail' (Email Synchronization Options) screen is also visible, showing settings for 'Letzte Nachrichten herunterladen' (Last messages to download) set to '1 Woche' (1 week), 'Nachrichtenformat' (Message format) set to 'Nur-Text' (Text only), and 'Maximale Downloadgröße' (Maximum download size) set to 'Gesamte Nachricht' (Entire message). The 'Erweitert...' (Advanced...) button is highlighted.

Nun kann auch bei jeder eMail via Exchange ausgewählt und angezeigt werden, ob verschlüsselt oder signiert werden kann. Unter Sicherheit steht nun „Signiert“ und unter Menü>Nachrichtenoptionen... die Verschlüsselungsoptionen auswählen:



The screenshot shows the 'Outlook-E-Mail' screen. The 'Sicherheit' (Security) field is set to 'Signiert' (Signed). The 'Menü' (Menu) button is highlighted. The 'Nachrichtenoptionen' (Message Options) screen is also visible, showing settings for 'Priorität' (Priority) set to 'Normal', 'Sicherheit' (Security) set to 'Nachricht signieren' (Sign message), and 'Sprache' (Language) set to 'Westeuropa' (Western Europe).

Nun können alle sicher sein, dass die eMail auch von euch stammt!