Atestoj

★ Johan Swenker, 17 marto 2005 ★

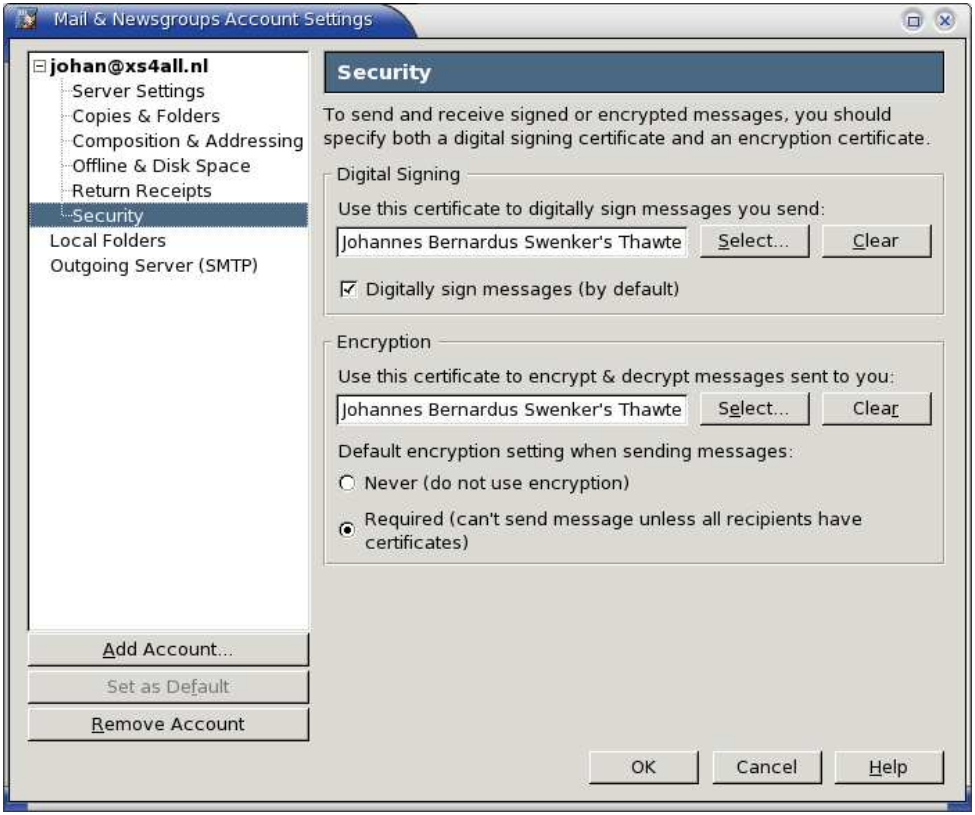
Kio signifas ateston

La angla vorto por tio pri kio mi parolos estas “certificate”. En la nederlanda ni uzas similan vorton: “certificaat”. Atesto similas pasporton. Per ambaŭ mi povas pruvi mian identecon. Per pasporto mi povas pruvi mian identecon en la reala mondo. Per atesto mi povas pruvi mian identecon en la virtuala mondo de Interreto.

Similaj vortoj estas aserti kaj certigi.

Retpoŝte uzi atestojn

Mi demonstracias pere de Mozilla. Mozilla ne nur estas interreta foliumilo, sed ankaŭ programo por legi kaj skribi retpoŝton. Aliaj homoj uzas Netscape, Eudora aŭ Outlook por prilabori retpoŝton. Outlook jes povas uzi atestojn. Eudora bezonas aldonan programaron por tio.



Ĉe la menuero sekureco mi povas alĝustigi 2 aferojn:

- ĉu mi volas uzi digitalajn subskribojn. Kaj se jes, kiun ateston mi volas uzi;
- ĉu mi volas ĉifri retmesaĝojn.

Por la demonstracio mi alĝustigis ĝin tiel ke mi forsendas ĉiujn mesaĝojn ĉifritaj. Kvankam la programo avertas min ke ĝi nur povas forsendi mesaĝojn kiam ĉiuj ricevontoj havas ateston.

Jen rigardu mian en–skatolon.

Interesa retpoŝta mesaĝo titolas: "*demonstratie ondertekening*". Kiam mi elektas tiun mesaĝon, Mozilla montras al mi ne nur la mesaĝon, sed ankaŭ piktogramon de plumo. Tiu plumo signifas ke la mesaĝo estas subskribita. Selektinte la plumon, mi povas legi kiu subskribis la retmesaĝon. Johannes Bernardus Swenker subskribis ĝin; lia retadreso estas Johan.Swenker@xs4all.nl; la firmao Thawte atestas ke la sendinto vere estas tiu Johan.

Por montri al vi ke atesto vere similas pasporton, mi nun montras al vi la ateston.

- ĝi estas de mi, simile kiel mia pasporto;
- pasportojn eldonas la urbestro, atastojn eldonas Thawte kaj aliaj firmaoj;
- ĝi validas nur limigitan tempon, tiel ke –post iom da tempo– mi denove devas doni foton kaj devas repagi;
- ĝi ne havas pasportan foton de mi, sed fingrospuron.

Alia interesa mesaĝo estas la respondo. Unue Mozilla rifuzas montri ĝin. Fakte ĝi ne povas montri ĝin. La mesaĝo estas ĉifrita. Nur mia privata ŝlosilo povas deĉifri ĝin. Se mi perdas la ŝlosilon, mi neniam plu povas legi la mesaĝon. Ankaŭ la ŝlosilo mem estas ĉifrita. Mozilla nun bezonas la kodon por deĉifri la ŝlosilon. Se mi forgesas tiun kodon, mi fakte perdas la ŝlosilon.

Kiam mi nun selektas la piktogramon de plumo aŭ ŝlosilo, Mozilla klarigas ke ne eblas ke aliaj personoj legis la mesaĝon ĉar ĝi estis ĉifrita.

Mozilla nun scias mian privatan ŝlosilon. Mi volas ke ĝi demandu ĝin denove. Tial mi haltas kaj relanĉas Mozilla-n.

Kiel mi jam montris, mi subskribas kaj ĉifras ĉiujn mesaĝojn. Mi nun montras kiel tio funkcias.

Mi sendos retmesaĝon al Johan.Swenker @xs4all.nl. Per la butono "*security*" mi povas vidi ke ĉio estas en ordo. Mozilla havas validan ateston por la ricevonto. Do ĉifrado eblas. Mi sendos la mesaĝon ankaŭ al wvganswk@xs4all.nl. Kiam mi denove demandas ĉu ĉio estas en ordo, Mozilla indikas ke ĝi ne havas

ateston de Wil. Ĉifrado do ne eblas. Kiam mi volas forsendi ĝin, Mozilla laŭte protestas. Mi eĉ ne povas konservi ĝin. Do, Wil vi ne ricevos la mesaĝon. Kiam mi denove provas forsendi ĝin, Mozilla demandas la kodon por deĉifri mian privatan ŝlosilon. Ĝi estas bezonata por subskribi la mesaĝon. Nun Mozilla povas forsendi la retmesaĝon, almenaŭ se mi havus retaliron.

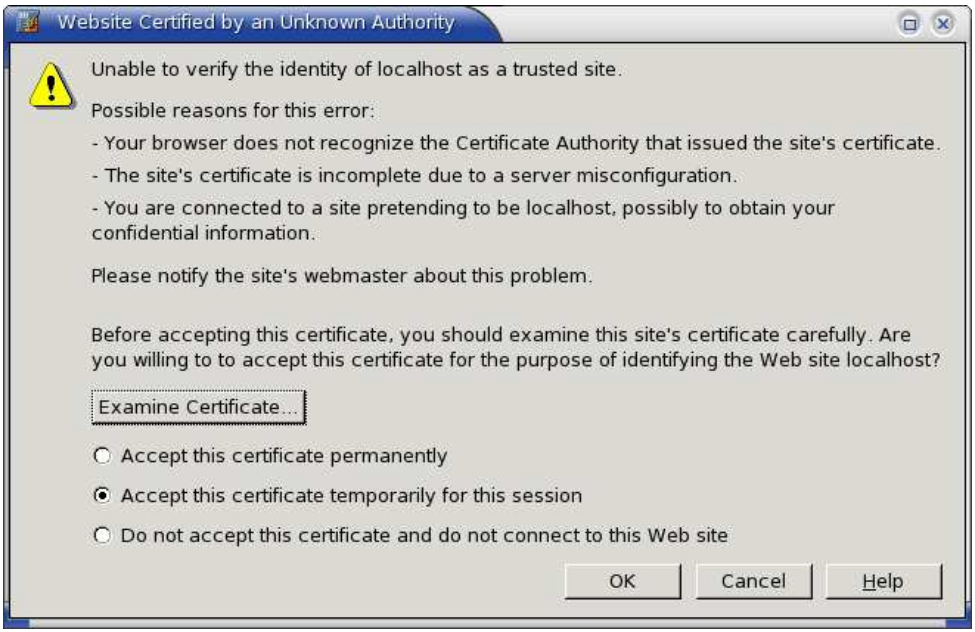
Uzi atestojn ĉe retejoj

Je kelkaj retejoj oni povas uzi atestojn anstataŭ pasvortojn. Multaj retejoj mem uzas atestojn por pruvi ilian identecon. Precipe retbankoj, sed ankaŭ retbutikoj devas pruvi ke ili vere estas mia banko aŭ tiu altkvalita butiko.

Mi montras ambaŭ per la retejo localhost.

Localhost estas retejo, simile al lernu.net. Ĝi estas loka al mia komputilo. Mi do ne bezonas la cetero de Interreto por demonstracii. Je localhost estas kelkaj ekzemploj pri atestoj.

Localhost mem provas identigi sin per sia atesto. Mozilla ne povas kontroli la identecon de localhost.



Estas tri eblaj kaŭzoj:

- la foliumilo ne rekonas la eldonanto de la atesto;
- la retservilo malbone funkcias;
- alia retejo ŝajnigas sin kiel localhost.

Kiam mi montras al vi la ateston de localhost, vi vidas ke la eldonanto ne estas konata, almenaŭ ne al Mozilla. Mi akceptas la ateston kaj daŭrigas la komunikadon kun localhost. La ŝloseto sube en la fenestro nun estas ŝlosita.

La ŝloseto signifas ke la identeco de la retejo estas kontrolita kaj ke la komunikiĝo estas ĉifrita. Mi do sen hezitoj povas sendi la nombron de mia kreditkarto aŭ mian pasvorton al tiu retejo.

La publika paĝo similas ĉiajn publikajn paĝojn.

La privata paĝo estas protektata per pasvorto. La instigilo indikas ke localhost bezonas pasvorton por la sekcio: “Pasvortprotektata sekcio, (biciklo)”.

Kiam mi volas vidi alian pasvortprotektatan sekcion, mi denove devas tajpi mian nomon kaj pasvorton.

La sekreta paĝo estas protektata per atesto. Nun la instigilo indikas ke Mozilla bezonas la pasvorton por deĉifri mian privatan ŝlosilon. Tio sufiĉas, ankaŭ por la alia sekreta paĝo.

Kial uzi atestojn

Ĉiuj informoj estas pli aŭ malpli konfidenca. Kelkaj informoj estas publikaj, aliaj privataj aŭ eble eĉ sekretaj. Kutima retpoŝto similas al poŝtkarto. Ĉiu povas legi ĝin, precipe la poŝtisto. Poŝtkartoj kaj retpoŝto do ne taŭgas por forsendi konteltiron de banko aŭ sanstaton de malsanulo. Simple ĉar tio ne koncernas aliajn homojn.

En la reala mondo vi uzas koverton por tiaj aferoj. En la virtuala mondo vi uzu ateston por ĉifri la mesaĝon.

Retpoŝto ne bone identigas la sendinton. Mi povas uzi ĉiun nomon kiel sendanto. Virusoj kaj trudmesaĝoj tiel agas. Se mi volas pruvi ke estas mi kiu forsendis ion, mi devas uzi mian ateston por subskribi la mesaĝon.

Per subskribo vi do pruvas ke estas vi kiu forsendis la mesaĝon. Samtempe la tekniko iĝas la mesaĝon neŝanĝebla. Oni jes povas ŝanĝi la mesaĝon, sed tiam la subskribo ne plu taŭgas. La komputilo laŭte plendas ke la mesaĝo ŝanĝiĝis post la subskribo. En la reala mondo mi nur vidis tion kiam mi aĉetis mian domon. La oficiala kontrakto, kiun verkis la notario, havis streketojn kie alie estus blanka papero. En la virtuala mondo mi uzas tion kiam mi petas monon de kasisto. Mi ne volas ke iu ŝanĝas la ĝirkonton. Nia kastisto ankoraŭ ne tiel ricevis mian fakturon. Al la kasisto de la komputilklubo mi jam kelkfoje tiel sendis fakturojn.

Atestoj do prizorgas ke la retmesaĝoj estas kaj restas konfidencaj, aŭtentikaj kaj integraj.

Kiel akiri ateston

Por retpoŝto haveblas senpagaj atestoj de Thawte kaj CAcert. Tiuj de Thawte tuj taŭgas. Ili similas pasportojn de konata lando. Ĉiu komputila programo por retpoŝto rekonas la atestojn de Thawte kaj akceptas subskribojn per atesto de Thawte. La atestoj de CAcert similas pasportojn de ankoraŭ nekonata lando. Kiel sendanto, mi konas kaj akceptas atestojn de CAcert. Por bone funkcii ankaŭ la ricevonto devas rekoni la atestojn de CAcert.

La atestoj de CAcert validas ankaŭ por identigo cxe retejoj. CAcert estas interesa ankaŭ ĉar ĝi estas komununa afero same kiel Linukso, Mozilla kaj OpenOffice.org.

Ĉi tie mi ne havas retaliron. Mi do ne povas montri al vi kiel funkcias la retpaĝojn de www.thawte.com kaj www.cacert.org por akiri atestojn.

Reto da Fido

Ĉu vi rememoras la ateston per kio mi subskribis la retmesaĝon? Tiu atesto enhavis kaj mian nomon kaj mian retadreson. Thawte atestas ke vere estas mi. Kiel ili scias mian nomon? Aŭ pli grave, kial ili estas certa ke mia nomo estas Johannes Bernardus Swenker?

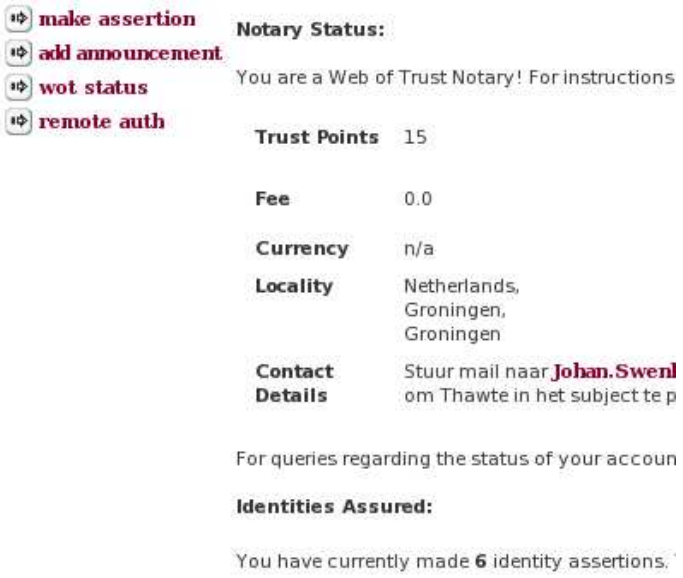
Mi unue eksplikas kiel ili kontrolas la retadreson. Mi diris al ili ke Johan.Swenker @xs4all.nl estas mia retadreso. Thawte

sendis provmesaĝon kun sekreta kodo al tiu adreso. Mi legis ĝin kaj respondis, uzante la sekretan kodon. Tiel Thawte scias ke mi respondecas pri tiu retadreso. Seriozaj dissendolistoj uzas la saman metodon por kontroli vian adreson.

Kiel mi certigas al Thawte ke mia nomo estas Johannes Bernardus Swenker? Mi iris al iu kiun Thawte iomete fidas. Thawte nomas tiun personon notario. La nederlandaj notarioj protestas kontraŭ tiu uzo de la vorto notario. Tial mi preferas uzi la vorton atestanto. Mi montris mian pasporton al tiu atestanto. Li kontrolis mian nomon kaj asertis al Thawte ke la retadreso Johan.Swenker@xs4all.nl vere estas de Johannes Bernardus Swenker.

Sed nun la ruzaĵo: unu sola atestanto ne sufiĉas. Thawte uzas poentsistemon. Ĉiu atestanto donas iom da poentoj. Kiam vi havas 50 poentojn, Thawte estas certa ke via nomo kaj retadreso vere apartenas al vi. Ekde tiam vi povas demandi atestojn kun via nomo en ĝi. La metodo estas eĉ pli ruza ol vi nun scias. Mi mem havas 100 poentojn. Al Thawte tio signifas ke mi estas sufiĉe serioza pri atestoj, ke ili povas fidi min kiel atestanton. Mi do estas atestanto de Thawte. Komence mi rajtis doni 10 poentojn. Mi jam kelkfoje faris tion. Neniu plendis ke mi eraris. Tiel mi kreskis kiel atestanto. Mi nun rajtas doni 15 poentojn. La plej potencaj atestantoj povas doni 35 poentojn.

CAcert uzas preskaŭ la saman metodon de atestantoj kaj poentoj. El mia vidpunkto estas nur unu diferenco: laŭ CAcert mi estas fidinda persono. Mi povas doni 35 poentojn.



Tekniko

La rezulto de subskribo estas ke Mozilla aldonas multajn kromajn liniojn. Kelkaj estas legeblaj kaj eĉ kompreneblaj. La plumulto estas sensencaĵo. La subskribo mem estas 50 linioj longa.

```
This is a cryptographically signed message in MIME format.

--------------ms070900080303080801070905
Content-Type:  text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding:  7bit

De inhoud is eigenlijk niet relevant
Johan

--------------ms070900080303080801070905
Content-Type:  application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding:  base64
Content-Disposition:  attachment; filename="smime.p7s"
Content-Description:  S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIIXzCC
AoowggHzoAMCAQICAw1OvTANBgkqhkiG9w0BAQQFADBiMQswCQYDVQQGEwJaQTElMCMGA1UE
```

kaj 50 ceteraj linioj.

La rezulto de ĉifrado estas preskaŭ 100 linioj da sensencaĵo. Rimarku ke ne ĉio estas sensencaĵo. La mesaĝo klare indikas ke ĝi estas ĉifrita. En mallibera lando la sekreta polico povas malagreble pridemandi vin pro tio. Vi povas legi ankaŭ kiuj estas la sendinto kaj la ricevanto.

```
Date:  Sat, 08 Jan 2005 17:57:07 +0100
From:  Johan Swenker <johan.swenker@xs4all.nl>
User-Agent:  Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6)
X-Accept-Language:  en-us, en
MIME-Version:  1.0
To:  Johan Swenker <johan.swenker@xs4all.nl>
Subject:  Re:  Demonstratie encryptie
References:  <41E00FDE.2020404@xs4all.nl>
In-Reply-To:  <41E00FDE.2020404@xs4all.nl>
Content-Type:  application/x-pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding:  base64
Content-Disposition:  attachment; filename="smime.p7m"
Content-Description:  S/MIME Encrypted Message
Status:  RO
X-Status:
X-Keywords:
X-UID: 2

MIAGCSqGSIb3DQEHA6CAMIACAQAxggEEMIIBAAIBADBpMGIxCzAJBgNVBAYTAlpBMSUwIwYD
VQQKExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMSwwKgYDVQQDEyNUaGF3dGUgUGVy
```

kaj preskaŭ 100 ceteraj linioj.

Matematiko

Mi jam kelkfoje uzis la esprimon "privata ŝlosilo". Ligita al la privata ŝlosilo estas publika ŝlosilo. Ĉiu rajtas vidi tiun publikan ŝlosilon. Vi eĉ devas publikigi ĝin. Pere de la atesto vi publikigas ĝin. Ĝi estas parto de la atesto. Privata kaj publika ŝlosiloj laboras kune. Tion kion vi ĉifras per unu vi povas deĉifri nur per la alia. Tamen ne eblas diveni la privatan ŝlosilon kiam vi konas la publikan.

Tiu ideo pri privata kaj publika ŝlosiloj ekzistas ekde 1976. En 1978 Rivest, Shamir kaj Adleman eltrovis metodon por vere kalkuli tiajn ŝlosilojn.

La bazo de la RSA-algoritmo estas primoj. Primoj estas numeroj kiuj estas divideblaj nur per 1 kaj si mem. La unuaj primoj estas $1, 2, 3, 5, 7, 11$. La publika ŝlosilo estas la produto de 2 primoj, ekzemple $1633 = 23 * 71$. Kiam la nombroj estas malgrandaj, kiel en la ekzemplo, vi simple povas retrovi la primoj el la produto. Kiam la nombroj estas grandegaj –ekzemple ambaŭ primoj havas 100 ciferojn– tiam ne vere eblas malkomponi la produto el la 2 primoj. La produto ja havas 200 ciferojn.

Tial vi nuntempe ofte aŭdas pri primoj, precipe kiam iu malkomponis grandegan nombron.

Komputi la privatan ŝlosilon el la 2 primoj estas altnivela matematiko. Ankaŭ ĉifrado kaj deĉifrado estas altnivelaj matematikaj aferoj. Mi do ne eksplikos. Ĉu mi tamen montros?

Ekzemplo
Ĉiu mesaĝo estas nombro inter 0 kaj 1632. La publika ŝlosilo estas trifoje multipliki kaj la nombro 1633. Kiam la mesaĝo estas 144, tiam la kodo kalkuliĝas jene:

$$\underbrace{144 * 144 * 144}_{\text{trifoje}} = 2.985.984 =$$
$$= 1828 * 1633 + \mathbf{860}$$

La nombro 1828 tute ne gravas. La kodo estas 860.

La sekreta ŝlosilo estas 1027-foje multipliki kaj la sama nombro 1633. Por retrovi la mesaĝon, la kalkulado estas preskaŭ la sama.

$$\underbrace{860 * 860 * \cdots * 860}_{\text{1027-foje}} = X * 1633 + \mathbf{144}$$

X estas tri mil cifera nombro, kies valoro tute ne gravas.

Vortlisto

alĝustigi	instellen
atestanto	waarmerker
atesto	certificaat
ĉifri, kriptigi	versleutelen, vercijferen
foliumilo	webbrowser
instigilo	prompt
konteltiro	dagafschrift
pasvorto	wachtwoord
piktogramo	icoon
retadreso	e-mailadres
retejo	webstek, website
retpoŝta mesaĝo	e-mailbericht
trudmesaĝo	spam

Atesto

Subskribanto	*Thawte Consulting (Pty) Ltd.*
atestas ke	*Johannes Bernardus Swenker*
	havas
retadreson	*Johan.Swenker@xs4all.nl*
kaj publikan ŝlosilon	00:e5:eb:96:7e:63:46:a6:e8:0c:8c:24:4b:73:93: 64:92:41:44:ab:42:c5:1a:72:12:6b:20:0d:d6:8d: c3:f1:b3:7b:83:96:da:f0:56:85:4c:4b:b3:62:99: a6:47:20:a3:c6:cc:27:c5:8c:ef:7f:46:0f:d8:e2: 7c:70:83:73:49:2f:d1:e0:b7:8b:48:a7:a9:5c:61: c5:49:6f:0a:0a:42:ae:62:3c:3d:17:27:2c:a0:a2: 6f:65:a4:6d:bb:65:a4:5a:22:56:89:da:02:a9:df: 33:52:f3:33:c1:f9:eb:d1:f9:f6:f8:ba:66:00:f4: 0e:4d:f0:6a:23:2a:be:a7:83
Subskribo	71:12:3a:96:c9:a9:10:8e:f6:1c:a5:d1:2b:57:30:fe:f4:13: 33:50:3e:9d:6f:c4:71:09:95:49:22:e0:3d:91:d8:ac:6f:ad: 29:62:bd:b5:3c:69:28:e7:78:e2:66:a3:80:40:29:10:56:ae: a4:c5:5b:60:46:81:91:b8:71:6d:5d:e3:aa:64:04:8b:64:a3: 4b:fa:0b:63:1c:05:32:7c:3a:20:43:de:5d:92:27:ab:25:dd: 7c:59:52:f3:50:90:4a:39:47:0d:76:ae:b0:83:5b:db:a2:c1: 52:fd:f1:0e:42:2f:5c:12:33:7f:9e:a8:0b:f1:1c:48:ec:a9: 8a:df
Dato	*La dudeksesan de oktobro du mil kvar*