Certificaten

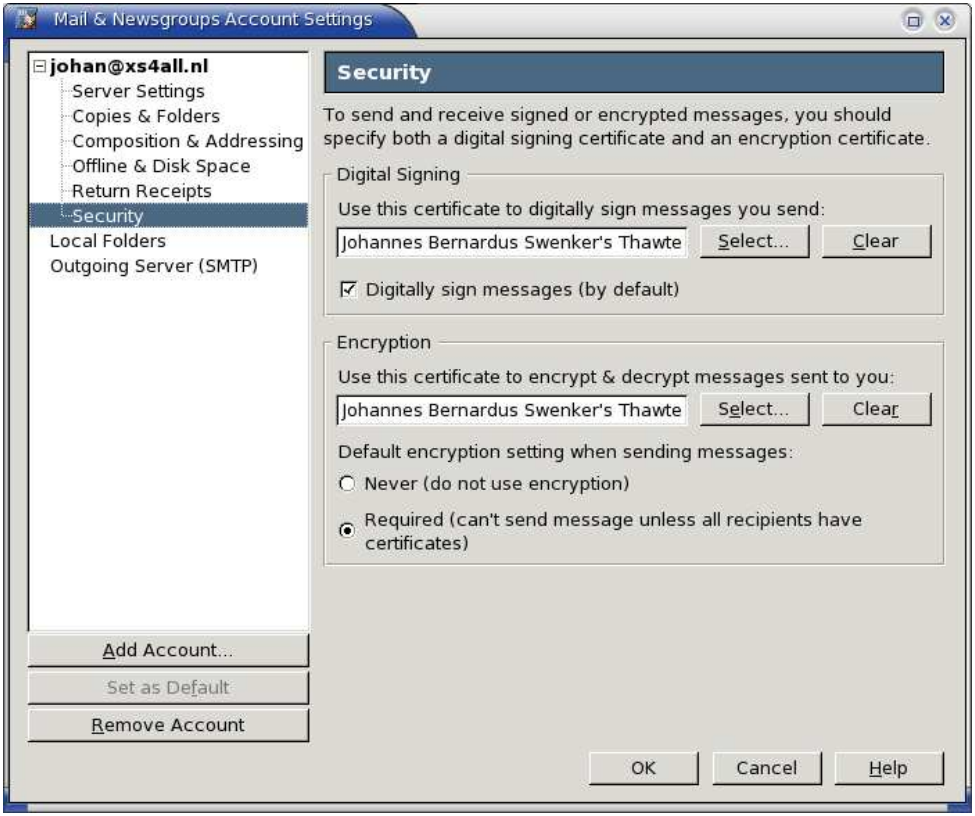
Johan Swenker, 18 mei 2005

Wat betekent certificaat

Een certificaat lijkt op een paspoort. Met beide kan ik mijn identiteit bewijzen. Met een paspoort kan ik mijn identiteit in real life aantonen. Met een certificaat kan ik mijn identiteit in de virtuele wereld van het Internet aantonen.

Certificaten bij e-mail

Ik demonstreer de certificaten met Mozilla. Mozilla is niet alleen een browser, maar ook een programma om e-mail mee te lezen en te schrijven. Andere mensen gebruiken Outlook, Netscape, Eudora of Thunderbird om hun e-mail mee te verwerken. Outlook kan met certificaten werken. Eudora heeft daar aanvullende software voor nodig.



Bij het menu-item "security" kan ik 2 zaken instellen:

- of ik digitale handtekeningen onder mijn mail wil plaatsen. En zo ja, welk certificaat ik daarvoor wil gebruiken.
- of ik e-mail wil versleutelen.

Voor de demonstratie heb ik het zo ingesteld dat ik alle berichten versleuteld wil verzenden. Ook al waarschuwt het programma me dat ik alleen berichten kan verzenden als ik de certificaten van alle ontvangers heb.

Laten we eerst mijn inbox bekijken.

Er is een mailbericht met de titel: "*demonstratie ondertekening*". Wanneer ik dat bericht kies, toont Mozilla me niet alleen het bericht, maar ook een pictogram van een pen. Die pen betekent dat het bericht ondertekend is.

Wanneer ik nu de pen selecteer, kan ik zien wie het bericht ondertekend heeft. Johannes Bernardus Swenker omdertekende het bericht; zijn e-mailadres is Johan.Swenker@xs4all.nl; de firma Thawte bevestigt dat de verzender daadwerkelijk die Johan is.

Om jullie te tonen dat een certificaat daadwerkelijk op een paspoort lijkt, toon ik jullie nu het certificaat.

- het gaat over mij, net zoals mijn paspoort;
- paspoorten worden uitgegeven door de burgemeester, certificaten worden uitgegeven door Thawte en andere bedrijven en organisatie's;
- het is slechts gedurende een beperkte tijd geldig, zodat je na enige tijd opnieuw een pasfoto moet geven en opnieuw moet betalen;
- er zit geen pasfoto op, maar een zogenaamde vingerafdruk.

Een ander interessant bericht is het antwoord. In eerste instantie weigert Mozilla het bericht te laten zien. Sterker nog, Mozilla kan het bericht niet laten zien. Het bericht is versleuteld. Alleen

met mijn privé sleutel kan het bericht ontsleuteld worden. Als ik die sleutel verlies, kan ik het bericht nooit meer lezen. De sleutel zelf is ook weer versleuteld. Mozilla heeft de code nodig om de sleutel te ontcijferen. Als ik die code zou vergeten, zou ik feitelijk de sleutel kwijt zijn en het bericht dus nooit meer kunnen lezen.

Wanneer ik nu het pictogram van pen met sleutel selecteer, dan legt Mozilla me uit dat andere mensen het bericht niet kunnen lezen omdat het bericht versleuteld was.

Mozilla kent nu mijn privé sleutel. Ik wil dat Mozilla er opnieuw om vraagt. Daarom start ik Mozilla opnieuw op.

Zoals ik al verteld heb, onderteken en versleutel ik alle berichten. Ik zal nu laten zien hoe dat werkt.

Ik ga een bericht verzenden naar Johan.Swenker@xs4all.nl. Met de knop "*security*" kan ik zien dat alles in orde is. Mozilla heeft een geldig certificaat voor de ontvanger. Versleutelen is daarmee mogelijk. Ik ga het bericht ook verzenden naar een Esperanto-kennis van mij. Als ik nu aan Mozilla vraag of alles in orde is, dan krijg ik te horen dat Mozilla geen certificaat heeft voor wvganswk. Het

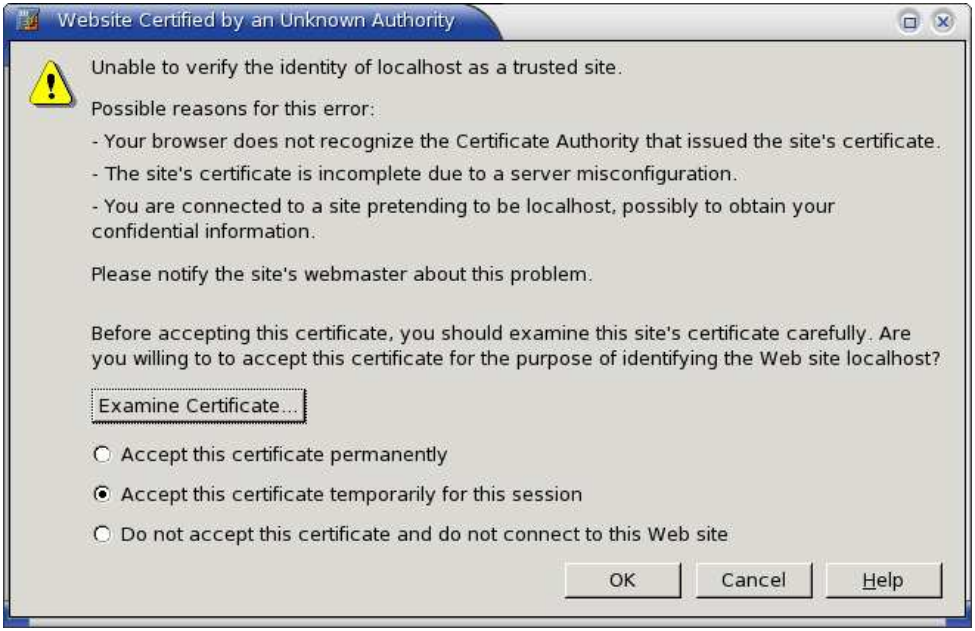
versleutelen is daarmee niet mogelijk. Wanneer ik nu toch probeer om het bericht te verzenden, dan protesteert Mozilla luidkeels. Ik kan het bericht niet eens opslaan. Net als bij de demonstratie voor de Esperantoclub, krijgt die wvganswk het bericht niet. Wanneer ik opnieuw probeer het bericht te verzenden, dan vraagt Mozilla de code om mijn privé sleutel te kunnen lezen. Mozilla heeft die privé sleutel nodig om het bericht te kunnen ondertekenen. Nu alles in orde is, kan Mozilla het bericht verzenden.

Certificaten bij websites

Bij verschillende websites kun je certificaten gebruiken in plaats van wachtwoorden. Veel websites gebruiken een certificaat om hun eigen identiteit aan te tonen. Met name internetbanken, maar ook internetwinkels moeten bewijzen dat ze daadwerkelijk mijn bank zijn of die goede winkel.

Ik ga certificaten bij websites demonstreren met de website localhost. Localhost is een gewone normale website, net zoals hccnet.nl. Localhost staat echter op mijn eigen computer. Ik hoef dus niet op zoek te gaan op Internet naar de juiste voorbeelden. Op localhost staan een aantal voorbeelden met certificaten.

Localhost gebruikt een certificaat om zijn eigen identiteit te bewijzen. Mozilla kan dat echter niet controleren.



Daar zijn 3 mogelijke redenen voor:

- de browser herkent de uitgever van het certificaat niet;
- de webserver maakt fouten;
- een andere website doet zich voor als de enige echte localhost.

Wanneer ik nu het certificaat van localhost laat zien, zien jullie dat de uitgever van het certificaat niet bekend is, tenminste, niet bij Mozilla. Ik accepteer het certificaat en laat de communicatie met localhost verder gaan.

Het slotje rechts onder in het venster van Mozilla is nu gesloten.

Dit gesloten slotje betekent dat de identiteit van de website gecontroleerd is en dat de communicatie versleuteld zal plaatsvinden. Je kunt nu op een veilige wijze vertrouwelijke informatie, zoals je creditcardnummer, uitwisselen met de website. Het slotje zegt overigens niets over de kwaliteit van de website, over hun privacy regels en over de beveiliging. Bij een slechte beveiliging kunnen de creditcardnummers toch in handen van derden vallen.

De publieke pagina lijkt op alle andere publieke pagina's.

De privé pagina is afgeschermd met een wachtwoord. De prompt geeft aan dat de website localhost een wachtwoord vraagt voor de sektie: "Pasvortprotektata sekcio, (biciklo)". What's in a name?

Wanneer ik nu een andere sektie wil bekijken die met een wachtwoord beveiligd is, dan moet ik opnieuw mijn wachtwoord intypen.

De geheime pagina is afgeschermd met een certificaat. De prompt geeft nu aan dat Mozilla de code nodig heeft om mijn privé sleutel te ontcijferen. Dat is voldoende, ook voor alle andere websites die een certificaat accepteren.

Waarom certificaten?

Alle informatie is in meer of mindere mate vertrouwelijk. Sommige informatie is publieke informatie, andere is privé of zelfs geheim. Internet e-mail lijkt enigszins op een briefkaart. Iedereen en in het bijzonder de postbode, kan lezen wat er op staat. Een briefkaart is niet geschikt voor het versturen van een dagafschrift van de bank en ook niet voor de uitslag van een medisch onderzoek. Heel eenvoudig omdat het niemand anders iets aangaat.

In real life worden enveloppen gebruikt om dergelijke zaken te verzenden. Bij e-mail moet je de berichten versleutelen om de gewenste privacy te krijgen.

Met e-mail wordt de afzender niet goed geïdentificeerd. Ik kan elke naam gebruiken als naam van de afzender. Virussen en spam doen precies dat. Zij verzenden mail uit naam van anderen. Als ik wil bewijzen dat ík het ben die iets verstuurd heeft, dan moet ik mijn certificaat gebruiken om een bericht te ondertekenen.

Met de ondertekening bewijs je dus dat jij het was die het bericht verzond. Gelijktijdig voorkom je daarmee dat het bericht ongemerkt veranderd kan worden. Als het bericht veranderd wordt, dan klopt de ondertekening niet meer. De computer zal dan luidkeels klagen dat het bericht gewijzigd is sinds de ondertekening.

In real life heb ik dat alleen gezien toen ik mijn huis kocht. In het officiële contract wat de notaris opstelde, stonden streepjes waar anders wit papier zou zijn. Op het internet gebruik ik dat om geld te vragen aan de penningmeester. Ik zou niet graag willen dat iemand het gironummer verandert. Ale en inmiddels ook Henk, hebben zo declaraties van mij ontvangen.

Certificaten zorgen er dus voor dat e-mail vertrouwelijk blijft, met een onweerlegbare afzender en zonder wijzigingen door derden.

Het verkrijgen van certificaten

Voor e-mail kun je gratis certificaten krijgen bij Thawte en CAcert. Die van Thawte zijn meteen te gebruiken. Zij lijken op paspoorten van een bekend land. Elk computer programma voor e-mail herkent de certificaten van Thawte en accepteert handtekeningen die daarmee gezet zijn. De certificaten van CAcert lijken op paspoorten van nog onbekende landen. Als afzender, accepteer ik de certificaten van CAcert. Om ze goed te laten werken, moeten ook de ontvangers de certificaten van CAcert accepteren.

De certificaten van CAcert zijn ook geldig om je bij een website te identificeren. Verder is CAcert interessant omdat het een samenwerkingsverband is, net als Linux, Mozilla en OpenOffice.org.

Web of Trust

net van vertrouwen

Herinner je je het certificaat waarmee ik mijn e-mail ondertekende? Dat certificaat bevatte mijn naam en mijn e-mail adres, Thawte bevestigt dat het werkelijk mijn adres is. Maar, . . . , hoe kennen zij mijn naam? En belangrijker nog, hoe weten zij zeker dat mijn naam Johannes Bernardus Swenker is?

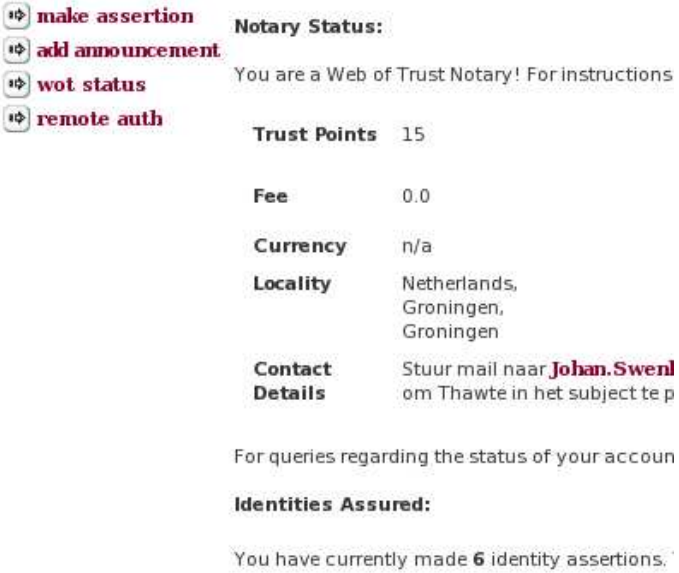
Ik zal eerst uitleggen hoe ze het e-mail adres controleren. Ik vertelde hen dat Johan.Swenker@xs4all.nl mijn e-mail adres is. Thawte stuurde toen een testbericht met een geheime code naar dat adres. Ik las het bericht en antwoorde met de geheime code. Zo wist Thawte dat ik verantwoordelijk was voor dat e-mail adres. Serieuze verzendlijsten gebruiken dezelfde methode om jouw aanmeldadres te controleren.

Hoe heb ik aan Thawte bevestigd dat ik Johannes Bernardus Swenker ben? Ik ben daarvoor gegaan naar iemand die door Thawte enigszins vertrouwd wordt. Thawte noemt die mensen “notary”. De nederlandse notarissen protesteerden echter tegen dat gebruik van het woord notaris. We gebruiken daarom in het nederlands het begrip waarmerker. Ik heb mijn paspoort aan die waarmerker laten zien. Hij controleerde mijn naam en bevestigde aan Thawte dat het e-mail adres Johan.Swenker@xs4all.nl aan Johannes Bernardus Swenker toebehoort.

En nu de slimmigheid: een enkele waarmerker is niet voldoende. Thawte gebruikt een puntensysteem. Elke waarmerker geeft een bepaald aantal punten. Zodra je er 50 hebt, weet Thawte zeker dat naam en e-mail adres bij elkaar horen. Vanaf dat moment kun je certificaten aanvragen waar je naam in staat. Deze methode is nog veel slimmer dan je nu weet. Ik heb zelf 100 punten. Voor Thawte betekent dat, dat ik zo serieus ben met certificaten, dat ze mij kunnen vertrouwen als waarmerker. Ik ben inderdaad waarmerker voor Thawte. In het begin mocht ik slechts 10 punten uitdelen. Ik heb dat nu een paar keer gedaan en niemand heeft geklaagd. Ik ben daardoor als waarmerker in achting gestegen. Ik mag nu 15 punten uitdelen. Ik kan nog uitgroeien tot een waarmerker

die 35 punten mag uitdelen. Dat is het maximum.

CAcert gebruikt vrijwel dezelfde methode van waarmerkers en punten. Vanuit mijn gezichtpunt is er slechts één verschil: volgens CAcert ben ik te vertrouwen. Ik mag 35 punten uitdelen.



Techniek

Het resultaat van een ondertekening is dat Mozilla vele regels toevoegt aan een bericht. Sommige zijn leesbaar en zelfs begrijpelijk. De meeste zijn binaire bagger.

```
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
```

en nog 50 vergelijkbare regels.

Het resultaat van de versleuteling zijn bijna 100 regels binaire bagger. Merk echter op dat niet alles onleesbaar is. Het bericht zelf geeft duidelijk aan dat het versleuteld is. In onvrije landen kan de geheime politie je alleen al daarover heel onaangenaam ondervragen. Je kunt ook duidelijk zien wie de afzender is, wie de ontvanger is en wat het onderwerp is.

```
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
```

en nog 100 vergelijkbare regels.

Wiskunde

Ik heb al een paar keer de uitdrukking "privé sleutel" gebruikt. Verbonden met de privé sleutel is een publieke sleutel. Iedereen mag de publieke sleutel zien. Je moet die zelfs publiceren. Met het certificaat wordt de publieke sleutel gepubliceerd. De publieke sleutel is onderdeel van het certificaat. De privé sleutel en de publieke sleutel werken samen. Dat wat met de ene versleuteld wordt, kan alleen met de ander ontsleuteld worden. En toch kun je uit de publieke sleutel niet afleiden wat de privé sleutel is.

De engelse termen zijn private key respectievelijk public key. Deze manier van versleutelen heet public key encryption. Er bestaat ook secret key encryption. Hierbij wordt dezelfde sleutel gebruikt om te versleutelen en om te ontsleutelen.

Het idee van public key cryptography bestaat sinds 1976. In 1978 hebben Rivest, Shamir en Adleman een methode bedacht om daadwerkelijke zo'n sleutelpaar te genereren.

Aan de basis van het RSA-algorithme staan priemgetallen. Priemgetallen zijn getallen die alleen deelbaar zijn door 1 en zichzelf. De eerste priemgetallen zijn $1, 2, 3, 5, 7,$ en 11. De publieke sleutel is het product van 2 priemgetallen, bijvoorbeeld $1633 = 23 * 71$. Kleine getallen, zoals in het voorbeeld, kun je makkelijk ontbinden in factoren en zo achterhalen uit welke priemgetallen het product bestaat. Als de getallen zeer groot zijn –als ze allebei bestaan uit bijvoorbeeld 100 cijfers– dan is het practisch niet mogelijk om de beide getallen uit het product af te leiden. Het product is dan immers een getal van 200 cijfers.

Dit is de reden waarom men tegenwoordig geïnteresseerd is in priemgetallen en met name in het ontbinden in factoren.

Het berekenen van de privé sleutel uit de 2 priemgetallen is hogeschool wiskunde. Dat gaan we hier dus niet doen. Ook bij het versleutelen en ontsleutelen wordt hogeschool wiskunde gebruikt. Ik ga het niet uitleggen, maar zal ik het wel tonen?

Voorbeeld
Elk bericht is een getal tussen 0 en 1632. De publieke sleutel is driemaal met zichzelf vermenigvuldigen en het getal 1633. Als het bericht 144 is, dan bereken je het versleutelde bericht als volgt:

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

Het getal 1828 is niet meer relevant, die moet je vergeten. Het versleutelde bericht is 860.

De privé sleutel is 1027-keer met zichzelf vermenigvuldigen en weer het getal 1633. Om het oorspronkelijke bericht terug te krijgen, moet je de volgende berekening maken:

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

X is een getal van 3000 cijfers, waarvan de waarde niet relevant is.

Certificaat

Ondergetekende	*Thawte Consulting (Pty) Ltd.*
certificeert dat	*Johannes Bernardus Swenker*
e-mail adres	*Johan.Swenker@xs4all.nl*

heeft

en publieke sleutel

```
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
```

handtekening

```
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
```

Datum	*De zesentwintigste oktober tweeduizend en vier*