Digitale Beveiliging van E-mail Communicatie

Inhoudsopgave

Onderzoek

E-mail Encryption - Het versleutelen van e-mails zorgt ervoor dat het bericht alleen leesbaar is voor de gekozen ontvanger. Om dit te doen wordt de leesbare tekst omgezet naar ciphertekst door middel van een versleutelingsalgoritme en een sleutel.

- Bij het versleutelen met asymmetrische Public Key versleuteling wordt de ontvanger zijn publieke sleutel gebruikt om het bericht te versleutelen. Omdat de publieke en private sleutel wiskundig zijn gekoppeld kan enkel de houder van de private sleutel het bericht ontsleutelen.

E-mail Signing - Door e-mails te ondertekenen kan de ontvanger zowel de afzender als de inhoud verifiëren. Op deze manier is er meer zekerheid dat er niet geknoeid is met de inhoud en de afzender legitiem is.

- Het ondertekenen van een e-mail gebruikt ook Public Key Encryption maar andersom, de verzender maakt een digitale handtekening met zijn private sleutel, de ontvanger kan deze dan verifiëren met de verzender zijn publieke sleutel.

Public Key Infrastructure - Een combinatie van hardware, software en regels die samen een robuust framework geven om confidentieel berichten uit te wisselen. Er wordt gebruikt gemaakt van een publieke sleutel, zichtbaar voor iedereen, en een private sleutel, deze moet altijd privé blijven.

Tools - **PGP:** Een programma dat men in staat stelt data te ver- en ontsleutelen. Wordt vaak gebruikt om e-mails te beveiligen.
- **GPG:** Een open-source alternatief voor PGP, wordt vaak gebruikt voor

beveiligen van data en communicatie.

- **S/MIME:** Biedt publieke sleutel encryptie als plugin voor email clients.

Opdracht

Voor deze opdracht is gebruikt gemaakt van gpg (GnuPG) versie 2.4.3 #### Aanmaken sleutel

Om een sleutel aan te maken gebruiken we het commando `gpg --gen-key` De output is dan als volgt:

```
gpg (GnuPG) 2.4.3; Copyright (C) 2023 g10 Code GmbH
GnuPG needs to construct a user ID to identify your key.

Real name: Rens Bril
Email address: 519649@student.saxion.nl
You selected this USER-ID:
    "Rens Bril <519649@student.saxion.nl>"

gpg: revocation certificate stored as '/Users/rensbril/.gnupg/openpgp-revocs.d/9C247C57F171E
public and secret key created and signed.

pub   ed25519 2023-10-06 [SC] [expires: 2026-10-05]
      9C247C57F171EE561B072D2F5E353E03ACDC134F
uid                      Rens Bril <519649@student.saxion.nl>
sub   cv25519 2023-10-06 [E] [expires: 2026-10-05]
```

Delen van de sleutel Om de sleutel te delen maken we gebruik van de keys.openpgp keyserver en het volgende commando: `gpg --send-keys --keyserver keys.openpgp.org 9C247C57F171EE561B072D2F5E353E03ACDC134F`

De laatste string getallen is mijn keyID

output:

```
> gpg --send-keys --keyserver keys.openpgp.org 9C247C57F171EE561B072D2F5E353E03ACDC134F
gpg: sending key 5E353E03ACDC134F to hkp://keys.openpgp.org
```

Ophalen sleutel klasgenoot Voor het ophalen van de sleutel van een klasgenoot gebruiken we het volgende commando: `gpg --auto-key-locate keyserver --locate-keys 518721@student.saxion.nl`

Output:

```
gpg: key BC14D1AA1E8BC4EF: public key "Sander <518721@student.saxion.nl>" imported
gpg: Total number processed: 1
gpg:               imported: 1
pub   ed25519 2023-10-06 [SC] [expires: 2026-10-05]
      361E3525B8772BDB37091BB3BC14D1AA1E8BC4EF
```

```
uid           [ unknown] Sander <518721@student.saxion.nl>
sub   cv25519 2023-10-06 [E] [expires: 2026-10-05]
```

Sleutels checken + Fingerprint Om de sleutels te checken en de fingerprint te zien gebruiken we de commando's: `gpg --list-keys` & `gpg --fingerprint <KEYID> of <email>`

Output: 1.

```
> gpg --list-keys

pub   ed25519 2023-10-06 [SC] [expires: 2026-10-05]
      361E3525B8772BDB37091BB3BC14D1AA1E8BC4EF
uid           [ unknown] Sander <518721@student.saxion.nl>
sub   cv25519 2023-10-06 [E] [expires: 2026-10-05]

pub   ed25519 2023-10-06 [SC] [expires: 2026-10-05]
      9C247C57F171EE561B072D2F5E353E03ACDC134F
uid           [ultimate] Rens Bril <519649@student.saxion.nl>
sub   cv25519 2023-10-06 [E] [expires: 2026-10-05]
```

2.

```
> gpg --fingerprint 518721@student.saxion.nl
pub   ed25519 2023-10-06 [SC] [expires: 2026-10-05]
      361E 3525 B877 2BDB 3709  1BB3 BC14 D1AA 1E8B C4EF
uid           [ unknown] Sander <518721@student.saxion.nl>
sub   cv25519 2023-10-06 [E] [expires: 2026-10-05]
```

Bericht versleutelen en ondertekenen Eerst maken we een message.txt en schrijven een leuk bericht:

```
touch message.txt
nano message.txt
```

Originele bericht:

```
Beste klasgenoot,

Dit bericht mag echt niemand lezen, ik wil je iets speciaals vertellen.
Het weer vandaag:
Het KNMI meldt dat er in het noorden af en toe regen valt, terwijl het elders meestal droog
Vanochtend is het overwegend bewolkt. In de middag zijn er perioden met zon, hoewel er in he
De temperatuur in de middag varieert van 20°C op de Wadden tot 26°C in Zuid-Limburg
```

Versleutelen en ondertekenen Het commando encrypten en signen is vrij simpel: `gpg --encrypt --sign --armor -r 518721@student.saxion.nl message.txt`

– armor: armor converteert de binaire data naar ascii format. Daarmee is het wat vriendelijker om mee te werken en makkelijker te versturen.

Output `message.txt.asc`:

```
-----BEGIN PGP MESSAGE-----

hF4DPs2BX6f0POoSAQdADb71NN5xDc7fdtbP6Opx6Pz5zmAMM6odBZanCxmpbV0w
1/nr+UFtvWhdonMiBOhT3oMxXbq6v+5pnUp3jKxCFByuanTJGmeYzdweQX8arZtj
1OkBCQIQQ5C6YNr5MCjOJEqu7xAdON3STQd4SUELL+lwS2c7Orecd/jbo1lYy/bO
wMC7OrEJxnXDGOCq92ipPHh1tzqXVvT1vh3Xe0E3AW7KCSEZTiREeT5yzmxs6zBW
0NuDU0l6Zy9+8cYyqg4pjcw6ne1OsWbhTphq56Zt+6VZb/4Den5KVWZkY4eq2VM2
fQjVihV7BnUtNn1Ei/iMOYwIprEGA1ZQR8icqNkqQXWjsUYGzvrgjVZ79x7UDaAX
BKOOFc3C6lN0U60XO6OI+EDJHPSO/99UpbGYlt/lieGQbCB75uGK+lqRf1sr9FIj
R/QwO9GJNN8fd1dl11j8fdgBUQg6hxBxTl24gg/SJRUBO8z9j9BMEs0xV2Qxr3C/
7OJkWJOrOFR4f18Wi5q98bjvvhix5tzQf5leQ11tvNm5//qdepMP/SMOZrSjYl+d
0VjuuKmKVgM3idfWQ7mq5IruetxKw75gRjmNzRc5AXs8ZwfpAGyMPcbbFhOfaHyX
rmDMKYa0a+oOktZBy+LsFnRDy9wWawETr5CiH68Jgt6ejs4BShkcgCDa9npRcl0u
M12mmR53uPVdvdNJDomGvOpPIGc4a6oAC8jwbRCrzX5RvunML7WcBNcllT0J+Q8V
FEXV8tYoUC81WO5URCqa4yE1TTYAmuvqnIzqJOgf/UiIFBFTjGDB/VUaHkyhMqnb
PTIdnA==
=dm7T
-----END PGP MESSAGE-----
```

Ontsleutelen bericht Het ontsleutelen is nog makkelijker dan het versleutelen:
`gpg --decrypt message.txt.asc`

Resultaat:

```
> gpg --decrypt message.txt.asc

gpg: encrypted with cv25519 key, ID 3ECD815FA7F43CEA, created 2023-10-06
      "Rens Bril <519649@student.saxion.nl>"

Beste klasgenoot,

Dit bericht mag echt niemand lezen, ik wil je iets speciaals vertellen.
Het weer vandaag:
Het KNMI meldt dat er in het noorden af en toe regen valt, terwijl het elders meestal droog
Vanochtend is het overwegend bewolkt. In de middag zijn er perioden met zon, hoewel er in he
De temperatuur in de middag varieert van 20°C op de Wadden tot 26°C in Zuid-Limburg

gpg: Signature made vr  6 okt 16:03:11 2023 CEST
gpg:                using EDDSA key 730CC0E870CE3BF2ADE6BEA764DCE817AD7AF715
gpg: Good signature from "Rens <519649@student.saxion.nl>" [ultimate]
```

Onderin wordt de handtekening gevalideerd.

Bronnen

https://support.microsoft.com/en-us/office/encrypt-messages-by-using-s-mime-in-outlook-on-the-web-878c79fc-7088-4b39-966f-14512658f480
https://keys.openpgp.org/
https://gnupg.org/
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
https://www.digitalocean.com/community/tutorials/how-to-use-gpg-to-encrypt-and-sign-messages
https://unix.stackexchange.com/questions/656205/sks-keyservers-gone-what-to-use-instead
https://unix.stackexchange.com/questions/49497/how-do-i-specify-the-keyserver-with-gpg