**Lab 5.1 – Onderzoek een trust pad**

**Doelen:**

**Deel 1: https://www.dnb.nl**

**Achtergrond/Scenario**

Mozilla heeft in 2016 de Firefox-addon Web of Trust (WOT) van addons.mozilla.org verwijderd. WOT is een extensie die gebruikers waarschuwt of een website veilig is of niet. Uit onderzoek bleek dat WOT geanonimiseerde surfgegevens aan deze partijen zou doorverkopen. Deze gegevens zijn eenvoudig naar de originele gebruikers te herleiden. Gegevens zoals e-mailadressen, gebruikersnamen, enz.   
Voor Firefox is het probleem vastgesteld, maar andere browser gebruiken ook dergelijke add-ons. Een andere manier die wordt gezien als een van de meest veilige methoden is het gebruik van een SSL-certificaat op een website. Vanuit de AVG moet een webshop bijvoorbeeld een SSL-certificaat op hun website hebben, omdat er persoonsgegevens worden verwerkt. De URL is dan te herkennen aan https:// i.p.v. http:// (.. hoe vaak zie je die laatste variant nog?).

**Vereiste bronnen**

Device met Internet toegang

**Deel 1: https://www.dnb.nl**

1. Surf met je browser (bijvoorbeeld Firefox) naar [https://www.dnb.nl](https://www.dnb.nl/)
2. Wat is de identiteit?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Wat is de public key?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Welk algoritme?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Wie is de uitgever?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Wat is het trust pad?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Wie is de root?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Wie heeft het root certificaat gesigned?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Waarom vertrouwen we het root certificaat?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Lab 5.2 – Pretty Good Privacy**

**Doelen:**

**Deel 1: Encrypt het bericht**

**Deel 2: Decrypt het bericht**

**Deel 3: Key-signing party (optioneel)**

**Achtergrond/Scenario**

Het versturen van van berichten is de gewoonste zaak van dag. Maar wat als je vertrouwelijke gegevens/berichten wilt versturen? Dan zit er bijna niets anders op dan dat je het bericht persoonlijk langs komt brengen. Dit wordt een probleem als je vaker berichten wilt versturen en je ontvanger bevindt zich aan de andere kant van de wereld. Een manier is het versleutelen van berichten. PGP (Pretty Good Privacy) is een standaard en wordt OpenPGP genoemd (afgekort PGP). PGP wordt gebruikt voor het digitaal ondertekenen, encryptie of beiden. Veel programma’s gebruiken deze standaard en is gebaseerd op asymmetrische encryptie. Zo werkt het onderdeel GnuPG [zie hieronder] bijvoorbeeld ook in combinatie met de desktop app van Microsoft Outlook en kun je daarmee onderling veiliger mailen.

**Vereiste bronnen**

Device met Internet toegang

**Deel 1: Encrypt het bericht**

1. Download voor Windows gpg4win ([www.gpg4win.org](http://www.gpg4win.org)) GPG (GNU Privacy Guard) van <http://gnupg.org/download/index.html> (win en mac) of [www.gpgtools.org](http://www.gpgtools.org/) (osx)
2. Installeer Gpg4win. Tijdens de installatie wordt gevraagd om een aantal opties aan of uit te vinken. Laat de gekozen opties staan en klik op next en vervolgens op install

Graphical user interface, application

Description automatically generated Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated Graphical user interface, application

Description automatically generated

1. Voordat je op de button Finish klikt controleer of de optie Run Kleopatra is aangevinkt.

![Graphical user interface, application

Description automatically generated]()

1. Kleoptra is een certificate manager in Gpg4win.

![Graphical user interface, text, application, email

Description automatically generated]()

1. Kies uit het menu File voor de optie New Key Pair of klik op de button New Key Pair

![Graphical user interface, text, application, email

Description automatically generated]()

1. Klik op de optie Create a personal OpenPGP key pair

![Graphical user interface, application, Teams

Description automatically generated]()

1. Vul (eventueel) je naam en een email adres in. Klik NOG NIET op de buttin Next, maar klik op de buttin Advanced Settings

![Graphical user interface, text, application, email

Description automatically generated]()

1. De settings voor RSA is waarschijnlijk op 3.072 bits ingesteld. Op zich is dat niet nodig en volstaat 2.048 bits. Wijzig indien nog en klik op de OK, vervolgens op de button Next

![Graphical user interface

Description automatically generated]() ![Graphical user interface

Description automatically generated]()

1. Vink eventueel de optie Show all details aan en klik op de button Create

Graphical user interface, text, application, email

Description automatically generated

1. Creating Key Pair……

![Graphical user interface, text, application, Word

Description automatically generated]()

1. Versleutel de private key met een wachtwoord, zodat niemand hem kan stelen.

![Graphical user interface

Description automatically generated]()

1. Het is aan te bevelen om een back-up te maken van je key pair (om welke keys gaat het trouwens?). Klik op de button Make a Backup Of Your Key Pair

![Graphical user interface, text, application, email

Description automatically generated]()

1. Geef een naam aan de backup bijvoorbeeld backup.pgp

Graphical user interface, text, application

Description automatically generated

1. Gebruik voor de backup een wachtwoord.

Graphical user interface

Description automatically generated ![Graphical user interface, application

Description automatically generated]()

1. Wissel public keys uit door de public key te exporteren en te mailen naar je partner. Bekijk de inhoud van de sleutels. Importeer vervolgens je partners public key in GPA. Daarvoor kan je de optie Send Public Key by Email. Heb je geen mailclient geïnstalleerd, dan zal je handmatig de public key moeten exporteren.

![Graphical user interface, text, application, email

Description automatically generated]()

1. Het certificaat is te zien in de Kleopatra manager.

Graphical user interface, text, application, email

Description automatically generated

1. De volgende stap is het encrypten van een bericht. Maak een tekstbericht voordat je het bericht gaat Signen/Encrypten.



1. Klik in de ribbon op de optie Sign/Encrypt. Er zal worden gevraagd wat je wilt Signen/Encrypted. Kies het eerder gemaakte bericht.

Graphical user interface, text, application, email

Description automatically generated

1. Eventueel kan je encrypted met nogmaals een wachtwoord. Dat is voor nu niet nodig. Laat de settings zo staan, tenzij je later een foutmelding krijgt in de trant van ‘no secret’.

Graphical user interface, text, application, email

Description automatically generated

1. Toch wordt er wederom om een wachtwoord gevraagd. Hoeveel wachtwoorden heb je tot nu gemaakt en waar dienen deze wachtwoorden dan precies voor?

**Nu zal je het password op een of andere manier veilig bij een groepsgenoot moeten krijgen…………**

Graphical user interface, application

Description automatically generated

1. Klik op Finish nadat het bericht is gesigned/encrypted

![Graphical user interface, application

Description automatically generated]()

1. Je vindt nu naast je tekstbericht hetzelfde tekstbericht maar nu geencrypted

![Graphical user interface, text, application

Description automatically generated]()

1. Open beide bestanden

![Graphical user interface, text, application, email

Description automatically generated]()

1. Mail nu het geencrypte bestand naar een groepsgenoot.

**Deel 2: Decrypt het bericht**

1. Van je groepsgenoot heb je een wachtwoord (op een beveiligde manier….) en een geencrypt bericht gekregen. Klik op de ribbon op de optie Decrypt en kies het geencrypte bericht van je groepsgenoot. Hoe controleer je vervolgens de authenticiteit?

Graphical user interface, text, application, email

Description automatically generated

1. Het bericht zal vervolgens worden gedecrypt. Wordt er om een wachtwoord gevraagd? Waarom wel of waarom niet? Klik op de button Save All nadat het bericht is gedecrypt.

Graphical user interface, text, application, email

Description automatically generated

1. Open het gedecrypte bestand

![Graphical user interface, text, application, email

Description automatically generated]()

1. AIVD/google/facebook/twitter/dropbox: eat your heart out!

**Deel 3: Key-signing party public keys (optioneel)**

Organiseer een [digitale] key-signing party om public keys met al je vrienden en bekenden uit te wisselen.