verslag labo certificaten

Opgave 1. Ising configureren als CA

op Ising:

-start

-administrative tools

-server manager

-add role > Active directory certficate services

-role services > certification authority & web enrollment

-> nieuwe private key creëren

op zowel Ising als Huygens:

-IIS installeren

op Huygens:

- naar site gaan (http://ising/certsrv)

-Ising-CA toevoegen als trusted root authority

het certificaat bevat de publieke sleutel van de CA, de

naam van de CA en andere zaken

Opgave deel 2: configureren van IIS voor SSL

--------------------------------------------

Via de snapin Server Certificates :

create certificate request + alles opgeven

Naar ising/srvcert surfen

->request a certificate

-> advanced

-> Submit a certificate request by using a base-64-encoded

CMC or PKCS #10 file, or submit a renewal request by using

a base-64-encoded PKCS #7 file.

common name moet gelijk zijn aan de nama van de web site.

Hierna het request goedkeuren op ising-ca.

Downloaden certificaat & chain,

->complete certificate request en

opgeven van de locatie van het gedownloade certificate

en geven een 'Friendly Name' in.

De bindings wijzigen:

http binding verwijderen en we voegen een https binding toe

en selecteren het aangemaakte certificaat.

Als we nu vanop ising naar http://huygens surfen dan zien

we error, surfen we naar http://huygens dan wordt gevraagd

om het certificaat toe te voegen en zien we de default iis

pagina.

Opgave deel 3: gebruik van S/MIME

--------------------------------

Deel 1

------

een certificaat request uitvoeren, gegevens invullen en

submitten.

-> exporteren in firefox:

edit - preferences - advanced - encryption

- certificaten bekijken - in juiste tabblad

certificaat aanduiden en klikken op export

Firefox vraagt om een wachtwoord bij dit proces.

-> importeren in thunderbird : op dezelfde manier:

advanced - certificates - authorities - import

hier bij vraagt thunderbird om het wachtwoord in te geven

Waarom wordt naar een wachtwoord gevraagd?

Dit wordt gebruikt om het document te encrypteren.

Deel 2

------

Na instellen van de default encryptie:

Versturen naar een andere gebruiker lukt niet want we

hebben zijn public key niet. Naar jezelf lukt wel, want

iedereen beschikt over zijn eigen public key.

Deel 3

------

Bij verzenden in thunderbird: security-sign optie

selecteren, de boodschap wordt normaal getoond, een icoon-

tje met een enveloppe en een rode stempel komt tevoor-

schijn.

Bij het aanpassen van dit bericht in mail map: een rood

kruisje komt door de enveloppe: 'signature is not valid'.

aanpassen emailadres: mail blijft signed: waarschijnlijk

is enkel het bericht geencrypteerd

Dit bericht is clear signed, dit is te zien aan de content

type.

verschil signed vs clear-signed:

signed: op basis van inhoud wordt een handtekening gevormd,

het geheel wordt vervolgens in base64 gecodeerd.

clear signed: enkel handtekening gecodeerd in base 64

met anders emailadres het bericht versturen:

signed by correct adres, bericht mail komt toe

Deel 4

------

encrypted versturen naar andere persoon:

certificaat van die persoon importeren

verzenden lukt dan wel, anders niet.

een slotje is zichtbaar

(boodschap in mail bestand is niet leesbaar)

bericht in mail bestand wijzigen -> slotje met kruis door

Thunderbird kan het bericht niet decrypteren.

Deel 5

------

beide symbolen zijn zichtbaar

formaat: zeer lang, onleesbaar, leesbare header

onderwerp wijzigen: thunderbird merkt niets

vooraan iets aanpassen: foutief geencrypteerd

einde: wel geencypteerd (na AAA), voor AA: fout

Deel 6

------

backup certificaat

-> paswoord ingeven

-certificaat verwijderen

import

mail verzenden lukt

certificaat aanpassen: importeren lukt niet,

het certificaat kan niet gedecodeerd worden, en kan dus

niet toegevoegd worden.

7.

firefox:

bij submit: wordt m.b.v. javascript gegenereerd a.d.h.v.

de ingevulde informatie + extra informatie zoals de huidige

tijd, browser.

beide sleutels zitten in het certificaat bij het ophalen.

Bij het signen van bestanden mag nooit de pricate key mee-

geleverd worden. deze dient om zaken te decrypteren.

Opgave deel 4: configureren van Apache voor SSL

-----------------------------------------------

Deel 1

------

commando:

openssl genrsa -des3 -rand /boot/intitramfs.. -out

ising.key 1024

vanaf de key een certificaat maken:

openssl req -new -key ising.key -out ising.csr

Hierbij moeten we extra info meegeven i.v.m. de key