6105 Windows Server og datanett

Labøving: Digitale sertifikater og kryptering med EFS

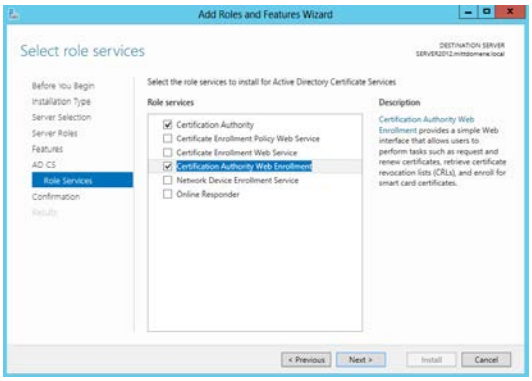
Oppgave a: Installere Active Directory Certificate Services

Bruk av kryptering i Windows forutsetter at brukerne får utstedt digitale sertifikater med krypteringsnøkler. I et Windows domene kan AD på domenekontrolleren fungere som sertifikatutsteder (CA). Dette krever at tjenerrollen *Active Directory Certificate Services* er installert på domenekontrolleren:

1. Logg på tjenermaskinen med brukeren **Administrator**.

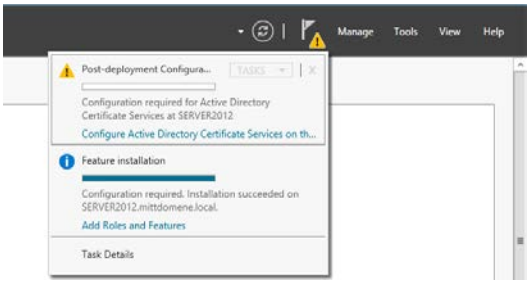
2. Bruk *Server Manager* og installer tjenerrollen **Active Directory Certificate Services** med følgende to rolletjenester (*Role Services*):

    - Certificate Authority
    - Certification Authority Web Enrollment



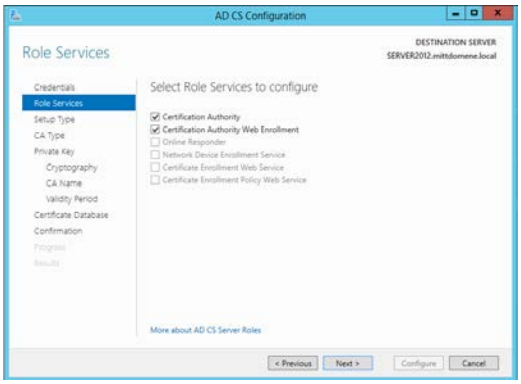
3. Installasjonen tar noen minutter.

   Etter at installasjonen er ferdig vil du få en notifikasjon om at det trengs konfigurasjon.



4. Klikk lenken *Configure Active Directory Certificate Services on the destination server* i vinduet til høyre

5. Velg rolletjenestene *Certificate Authority* og *Certification Authority Web Enrollment* på nytt under *Role Services*.



6. Velg **Enterprise CA** under *Setup Type*, slik at AD CS kan dele ut sertifikater til alle maskiner i Windows domenet.

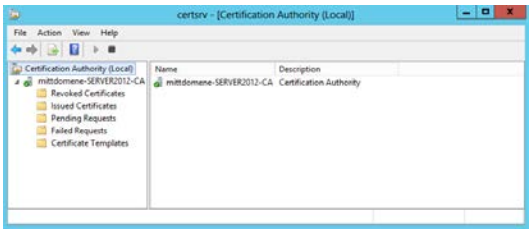
7. Siden denne CA'en er den første i domenet skal du velge **Root CA** som *CA Type*.

8. Opprett en **ny privat nøkkel** for CA'en i vinduet *Private Key*.

9. Bruk **standardverdier** som installasjons-programmet foreslår i vinduet *Cryptography for CA* og de resterende vinduene.

10. Start **Tools ► Certification Authority.**

    Det er ikke så mye du kan bruke dette verktøyet til foreløpig, men senere vil du kunne administrere sertifikater her etterhvert som de blir utstedt.



Foreløpig er det bare mappen *Certificate Templates* som inneholder noe. Du ser maler som brukes for å opprette sertifikater for ulike formål der kryptering kan brukes.

Oppgave b: Kryptere en fil med EFS (Encrypted File System)

I denne øvingen skal du kryptere noen filer, og se at selv administrator ikke kan lese innholdet i disse. Deretter skal du bruke et digitalt sertifikat for å "gjenopprette" filene.

1. Bruk tjenermaskinen innlogget som **Administrator**

2. Bruk *Active Directory Users and Computers* for å lage en ny *domenekonto* **EfsUser** under mappen **Users.** Sett passord til **Password.2012** så du husker det, og bruk valget *Password Never Expires.*

3. Logg på fra **klientmaskinen** med den nye domenekontoen **EfsUser**.

4. Lag en ny mappe **C:\EfsData.** I denne mappen skal du lage en ny fil **Hemmelig.txt.** Bruk f.eks *Notepad* for å gjøre dette. Legg inn en tilfeldig tekst i denne filen, lagre og lukke *Notepad.*

   Hvilke NTFS-rettigheter har gruppen *Administrators* på denne filen? _____

   Hvilke NTFS-rettigheter har gruppen *Authenticated Users* på filen? _____

5. Gi din egen **personlige domenebruker** NTFS-rettigheten **Full Control** til denne filen.

6. Bruk *Windows Utforsker* for å kryptere filen slik:
   - Høyreklikk filen *Hemmelig.txt* og velg **Properties**
   - Bruk fanen **General** og knappen **Advanced**.
   - Sett kryss i sjekkboksen **Encrypt contents to secure data.**
   - Klikk så **OK** og deretter **Apply.**
   - I dialogboksen **Encryption Warning** velger du **Encrypt the file and its parent folder**.

   Hvilke synlige endringer skjer med filen og mappen i *Windows utforsker*? _____
   Tips: Velg **View → Large icons** hvis du ikke ser noe forskjell.

7. Sjekk at du fremdeles kan åpne og lese/endre filen *Hemmelig.txt*.

8. Logg av klientmaskinen og på igjen med din egen **personlige domenebruker** (som du ga rettigheter i pkt 5).

   Kan du lese innholdet i filen *Hemmelig.txt* nå? _____

Hvilke *effektive* NTFS-rettigheter har brukeren din på filen? _____

Hvorfor får du likevel ikke lest filen? _____

9. Logg av klientmaskinen og på igjen med domenekontoen **Administrator**.

   Kan du lese innholdet i filen *Hemmelig.txt* nå? _____

   Hvilke effektive NTFS-rettigheter har **Administrator** på filen? _____

10. Høyreklikk filen *Hemmelig.txt* og velg **Properties.**

    - Bruk fanen **General** og knappen **Advanced**.
    - Klikk knappen **Details** bak sjekkboksen *Encrypt contents to secure data.*

      Hvilken bruker har rettighet til å aksessere filen? _____

      Hvilken brukers sertifikat er definert som "*Recovery Certificate*"? _____

Forklaring: Første gang en bruker krypterer en fil/mappe vil brukeren automatisk få tildelt et digitalt sertifikat fra **CA** på domenekontrolleren. Sertifikatet inneholder bl.a. en offentlig og en privat nøkkel som brukes av EFS for kryptering/dekryptering av filene.

Samtidig blir det definert et sertifikat som kan brukes for å gjenopprette filen (recovery). Som standard defineres dette til å være Administrators sertifikat.

Administrator kan altså ikke uten videre lese filen, men kan gjenopprette (dekryptere) filen ved å bruke sitt eget digitale sertifikat.

Oppgave c: Se innholdet i, og eksportere, et digitalt sertifikat

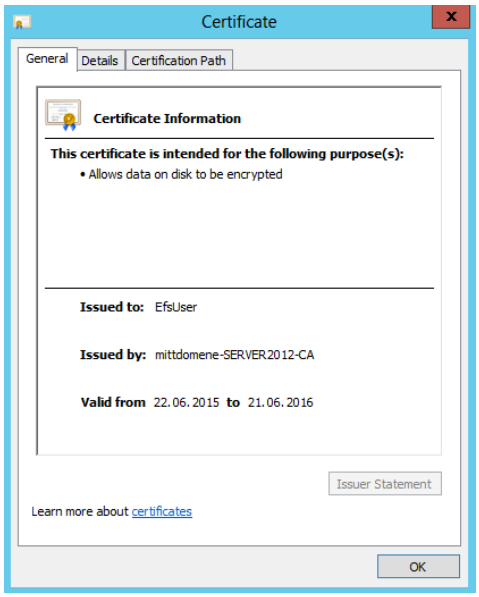
I Windows er digitale sertifikater knyttet til en bruker (eller en datamaskin) i domenet. Sertifikatene lagres i et sentralt sertifikatlager (*Certificate store)*. Sertifikatene er derfor tilgjengelige fra alle applikasjoner som har behov for kryptering.

1. Vær pålogget **tjenermaskinen** som **Administrator**.

2. Start **Tools ► Certification Authority** fra *Server Manger*

3. Åpne mappen **Issued Certificates**.

4. Dobbeltklikk sertifikatet for **EfsUser** slik at innholdet vises.



Vinduet viser hvilken bruker sertifikatet er utstedt til, hvilken CA som har utstedt det og hvilken periode det er gyldig for.

5. Velg fanen **Details** og svar på følgende:

   Hva er navnet på krypteringsalgoritmen som brukes for signatur? _____

   Når utløper sertifikatet? _____

   Hvor lang er den offentlige nøkkelen som benyttes i sertifikatet (antall bits)? _____

   Hva brukes den offentlige nøkkelen til i EFS?

   _____

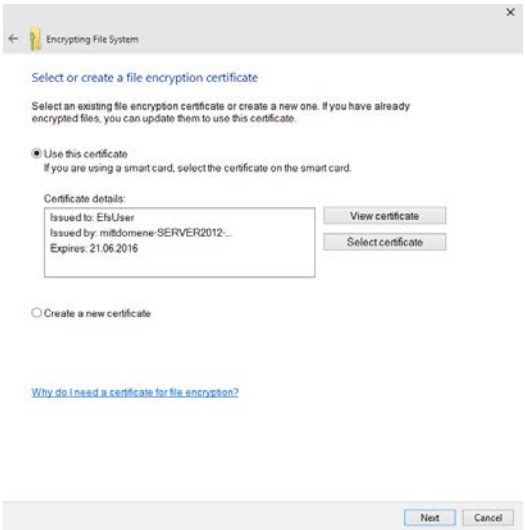
6. Klikk på linjen *Public key*. Nedre del av vinduet vil nå vise den offentlige nøkkelen (i hexadesimal form).

7. Hvorfor er den offentlige nøkkelen åpent lesbar? _____

<u>Se ditt eget sertifikat fra klientmaskin</u>

8. Logg på **klientmaskinen** med domenebrukeren **EfsUser**.

9. Start **Control Panel ► User Accounts ► User Accounts** og klikk linken **Manage your file encryption certificates** i venstre kolonne:



10. Klikk knappen **View certificate**. Du får opp samme informasjon som administrator så i **Certification Authority.** I tillegg skal du nederst se informasjon om at du har en **privat nøkkel** som hører sammen med sertifikatet.

    Hva blir denne private nøkkelen brukt til i EFS? _____

Eksportere et sertifikat med privat nøkkel

11. Velg fanen **Details**, og knappen **Copy to File**. Dette starter en veiviser for eksport av sertifikatet til fil.

    - På siden *Export Private Key* velger du **Yes, export the private key.**
    - På siden *Export File Format* velger du **Personal Information Exchange – PKCS (.PFX)**
    - På siden *Security* velger du **Password** og skriver inn et nytt passord, f.eks. **password** (i begge felt). Dette passordet beskytter den private nøkkelen.
    - På siden *File to export* lagrer du sertifikatet som **C:\temp\EfsUserCert.pfx** (lag om nødvendig mappen temp)
    - Til slutt klikker du **Finish** i oppsummeringsbildet.

Sertifikatet er nå lagret på filen **C:\temp\EfsUserCert.pfx.** Husk at alle som får tilgang til denne filen, også har tilgang til brukerens private nøkkel!

I en virkelig driftssituasjon ville man selvsagt være forsiktige med å lage sertifikater med kopier av brukernes private nøkler. Slike filer bør lagres på et medium som er innelåst og som kun utvalgte administratorer har tilgang til hvis behovet oppstår.

Oppgave d: Lese krypterte filer med en annen brukers sertifikat

Krypterte filer kan bare dekrypteres dersom man har et sertifikat som inneholder den private nøkkelen til brukeren som krypterte filen. Som du har sett ble sertifikatet til **Administrator** lagt inn som *Recovery Certificate* for brukeren **EfsUsers** sertifikat.

Du har nå eksportert en kopi av brukerens sertifikat som inneholder brukerens private nøkkel. En annen bruker kan da importere dette sertifikatet og bruke den private nøkkelen for å gjenopprette (dekryptere) filen.

Scenario: Bruker av kontoen **EfsUser** har forlatt firmaet, og kontoen er slettet. Det viser seg at brukeren har kryptert noen filer som firmaet trenger. Disse filene må derfor dekrypteres / gjenopprettes slik at de blir lesbare for andre. Dette kan gjøres hvis du har en kopi av brukerens sertifikat med privat nøkkel.

1. Logg på **klientmaskinen** med din egen private **domenebruker**.

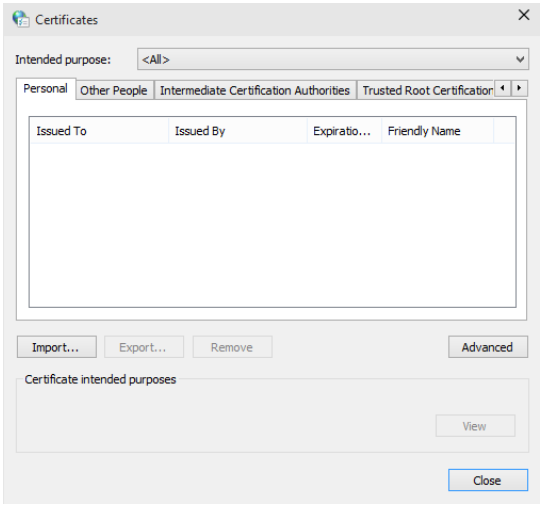
2. Start **Control Panel ► Network and Internet ► Internet Options**.

3. Velg fanen **Content** og knappen **Certificates**

   Finnes det noen sertifikater tilknyttet din bruker her? _____

4. Bruk knappen **Import…** og importer sertifikatet fra filen **C:\temp\EfsUserCert.pfx** som du laget i forrige oppgave. (Bruk **Browse** knappen og søk etter ***.pfx** filer.)

5. Du må nå oppgi passordet du laget når du eksporterte sertifikatet til fil.



6. På siden *Certificate Store* sørger du for at sertifikatet havner i lageret *Personal.*

7. Kontroller at sertifikatet til brukeren **EfsUser** har kommer inn i listen over dine sertifikater.

8. Lukk kontrollpanelet

9. Forsøk å åpne filen *C:\EfsData\Hemmelig.txt* i Windows Utforsker nå.

   Nå bør du kunne lese innholdet i filen. Hvorfor? _____

10. Lukk filen i *Notepad.*

Slutt på øvingen