RIIGI INFOSÜSTEEMI AMET

Turvaline meilivahetus avalikus sektoris

Sisukord

Mobiilsete seadmete turvalisus 2
Veebipõhise meilikliendi turvalisus 2
Meiliserverite vahelise suhtluse turvalisus 2
  Meilinduse turvalisus lõppkasutaja vaatenurgast 3
Üldised nõuded 4
  SPF 4
  DKIM 4
  DMARC 5
  DNSSEC 5
  DANE 6
  Viirusetõrje 6
  Spämmitõrje 6
  Greylisting 6
  Väldi infra paljastamist 6
Lisamaterjaljalid 7
  Opportunistic TLSi kasutamine Postfix tarkvaraga 7
    Sissetulevate SMTP ühendustele TLSi toe lisamine 7
    Väljaminevate SMTP ühendustele TLSi toe lisamine 7
    Tulemuse kontrollimine/veaotsing 8
  Opportunistic TLSi kasutamine tarkvaraga Exchange 8

Mobiilsete seadmete turvalisus

Teemat käsitleb põhjalikult RIA varasem mobiilsete seadmete turvapoliitika loomist käsitlev juhend: https://www.ria.ee/sites/default/files/content-editors/ISKE/juhend_mobiilsete_seadmete_turvapoliitika_loomiseks.doc,

Kokkuvõtlikult tuleb silmas pidada järgmist:

- asutuse meilide, kalendri jms ressursside kasutamiseks mobiilsetes seadmetes tuleb kehtestada organisatoorsed reeglid (kas ja mida tohib teha mobiilsete seadmetega);
- soovitatav on piirata lubatud platvormid kitsamale valikule (nt iOS ja Android alates versioonist X), sellega kergendad tulevast halduskoormust;
- soovitatav on võtta kasutusele mõni MDM haldusvahend (https://en.wikipedia.org/wiki/Mobile_device_management)
    - haldusvahendi valikul otsustada, kas kasutatakse sisemist MDM lahendust oma majas või (pilve)teenusena, viimase kasutamisel on eelneva riskianalüüsi teostamine kohustuslik;
    - piisavalt toimivaks võib osutuda näiteks postiserverisse sisseehitatud MDM võimekus (tutvu oma postiserveri võimalustega);
- nõuda seadmete krüpteerimist ja turvalist ekraanilukustust (kui võimalik, siis kehtestada nõue MDM vahendusel mitte organisatoorsena);
- võimalusel suhelda oma asutuse infosüsteemidega ainult VPNi vahendusel (SSL VPN, IPsec), vältida tööks avalike WiFi võrkude kasutamist.
    - juhul kui VPNi kasutamine ei ole võimalik, siis tuleb veenduda, et asutuse pakutavad teenused kasutaksid muid krüpteeritud andmevahetuse võimalusi.

Veebipõhise meilikliendi turvalisus

Võimalusel kasutada veebipõhist meiliklienti üle asutuse VPN-ühenduse, eelistatult asutuse kontrolli all olevatest masinatest.

Igal juhul on tarvilik:

- turvata juurdepääs meilikliendile https:// kasutades TLS v1.2 ja TLS v1.3 protokolli
    - kasutada kaheastmelist autentimist (ID-kaart, mobiilid, SA SecurID jms) juhul, kui veebipõhine meiliklient on kasutusel avalikust võrgust ilma täiendava VPN-ühenduseta).
        - juhised ID-kaardi- ja mobiil-ID-põhise autentimise lisamiseks: https://eid.eesti.ee/index.php/Kasutaja_tuvastamine_veebis
- kasutada veebipõhise meilikliendi realisatsiooniks lahendusi, mis on aktiivse toega ja piisavalt levinud
    - järgida valitud lahenduse turvalise kasutamise soovitusi,
- paigata töökeskkondi korrapäraselt,
- logida töökeskkonnas asetleidvaid sündmuseid (soovitatavalt kesksesse logiserverisse).

Meiliserverite vahelise suhtluse turvalisus

Meiliserverite vahelise andmevahetuse kaitsmiseks on vajalik sisse lülitada SMTP protokollil TLSi tugi (seda nii saadetavate kui vastuvõetavate e-kirjade puhul). Enamik suuremaid meiliteenuseid (nt Gmail) toetatavad seda juba aastaid.

Opportunistic TLS (STARTTLS)

Meetodi valik tähendab, et SMTP liiklust krüptitakse selle krüptomaterjaliga ja nendes tingimustes, mis parasjagu kasutada on (sertifikaate usaldatakse, šifrite kasutamine on leebe jne).

Eesmärk ei ole igakülgne kaitse MITM jms rünnete eest, vaid saada vähemalt lahtine liiklus võrgust ära.

Meetme kasutuselevõtt on riigisektoris kohustuslik tagamaks kehtivaid sõnumisaladuse- ja isikuandmetekaitse nõudeid. See kehtib ka nendele e-kirja massedastusteenustele, mida kasutatakse lepingu alusel.

Mutual TLS

Mutual TLS on meetod, mille puhul valitud domeenidega suheldakse ainult üle TLS protokolli. Suhtlusel kontrollitakse vastaspoole sertifikaatide kehtivust, seega juurutamisel peate olema kindlad, et vastaspool on võimeline korrektselt üle TLSi kommunikeeruma ja omab selleks korrektseid ja kehtivaid sertifikaate.

Opportunistic TLS meetmest turvalisema meetme kasutuselevõtt on riigisektoris vähemalt ministeeriumite ja ametite vahelises meilisuhtluses soovitatav. Sarnase tulemuse annab DANE + DMARC rakendamine, mis annab sarnase tulemuse, kuid mille mõju on laiem kui mutual TLS'il.

Meilinduse turvalisus lõppkasutaja vaatenurgast

Turvaline ühendus meilikliendi ja serveri vahel

Harjumspäraselt kasutatakse meilikliendi ühendamiseks serveriga kas POP3 või IMAP protokolli. Neid protokolle ei tohi kindlasti kasutada üle avaliku võrgu kuna kasutajatunnused ja paroolid liiguvad krüpteerimata või nõrgalt krüpteeritud kujul. Nende kasutamine näiteks halvasti konfigureeritud avalikus WiFi võrgus võib väga lihtsalt lõppeda kogu postkastis olevate andmete vargusega ja/või e-posti kuritarvitamisega.

Turvaline alternatiiv on kasutada kas POP3S või IMAPS protokolli, mis tagavad kasutajatunnuse ja parooli ning kirjade edastamise krüpteeritud kujul.

Meetme kasutuselevõtt on riigisektoris kohustuslik. Samuti on soovitatav meedet rakendada oma lepingupartneritega suhtlusel.

Tundlike andmete edastamine

Vaatamata eeltoodule tuleb lõppkasutajad treenida tundliku materjali edastamisel kasutama täiendavalt krüpteerimist.

Eestis on kõige lihtsam ja kättesaadavam meetod kasutada tundliku materjali edastamisel ID-kaardi krüptokonteinerit, mis tagab, et tundlikku infot näevad ainult selleks volitatud isikud.Siinkohal tuleb meeles pidada, et ID-kaardiga krüpteeritud materjali ei ole mõeldud pikaajaliseks säilitamiseks vaid pigem andmete kaitseks nende transpordil (ID kaardi vahetuse/kaotamise korral ei ole võimalik enam krüptokonteinerit avada).

Suhtlemisel muude organisatsioonidega on vajalik kokku leppida oma asutuses kasutatavad alternatiivsed krüpteerimismeetodid (nt paroolkaitsega zip + parooli edastamine muude kanalite kaudu, pgp jne.) ja neid läbivalt kasutada.

NB! Ära unusta lõppkasutajate väljaõpet!

Üldised nõuded

Lisaks konfidentsiaalsuse tagamise vajadusele andmete vahetamisel meiliserverite vahel või lõppkasutajate tasemel tuleb tähelepanu pöörata ka muudele asjadele, et vältida halvemal juhul asutuse mainekahju ja andmete kadu. Olulisemad märksõnad:

- asutuse meilidomeenide kaitsmine nende väärkasutamise katsete eest,
- viirusetõrje rakendamine,
- spämmitõrje.

SPF

Kõige lihtsam on vältida oma domeeni meilidega seotud väärkasutamise katseid, võttes korrektselt kasutusele SPFi. SPFi rakendamise puhul on oluline teada, millistest serveritest ametlikud e-kirjad väljuvad. SPF kirjeldatakse TXT kirjena ning oluline on kirjeldada SPF iga domeeni ja iga alamdomeeni kohta eraldi: SPF alamdomeenidele automaatselt ei laiene. Oluline on tähele panna, et SPF kirjete puhul on piirang: 10 DNS päringut SPF kirje kohta.

NB! SPF kirje valideerimine ei pruugi töötada automaatse e-posti edastuse puhul, sest vastuvõtja jaoks saadetakse e-kiri automaatset edastust teinud serverist, mitte esialgsest.

SPF kirje peaks olema ka nendel domeenidel, mida ei kasutata e-kirjade väljasaatmiseks. Sel juhul peaks olema märgitud üheselt, et antud domeenilt kirju ei saadeta. Seda saab teha järgmiselt:

v=spf1 -all

Juhul, kui on vaja kasutada mõne e-kirja mass-saatja teenust (nt. Smaily, MailChimp jt.) tuleks teenusepakkuja käest küsida nende SPF ning lisada see sarnaselt enda andmetele oma domeeni SPF kirjesse.

Meetme kasutuselevõtt on riigisektoris kohustuslik. Samuti on soovitatav meedet rakendada oma lepingupartneritega suhtlusel.

Alusta tutvumist siit: https://en.wikipedia.org/wiki/Sender_Policy_Framework.

SPF syntaxi kohta saab lugeda lähemalt siit: http://www.openspf.org/SPF_Record_Syntax.

DKIM

DKIM on PKI põhine meetod allkirjastamaks väljuvaid e-kirju tagamaks nende usaldusväärsust. Iga domeeni või alamdomeeni puhul tuleb kirjeldada selle domeeni avalik võti ning lisada see domeeni DNS kirjesse. DKIM on disainitud selliselt, et automaatse e-posti edastuse puhul (nt. e-posti list) säilib esialgne allkiri ja vaatamata automaatsele edastusele, saab

vastuvõtja veenduda, et e-kirja saatis lubatud saatja. DKIM kirjeldatakse TXT kirjena ning oluline on kirjeldada DKIM iga domeeni ja iga alamdomeeni kohta eraldi.

DKIM HOST kirje näide: mail._domainkey.cert.ee
DKIM TXT kirje näide: v=DKIM1; h=sha256; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtFC1vh/QJEKpVEzbNjwm7xjBXdffgKm3JuigoiHZn+uhc4d6iL4oZFOCXNEdANZGBK8cnWNeW8yQDCDtqYRekrSNHtKUYCqBlRkZnKDDk8+WmlSxXscexxUt2Fd3op0JLSEMQnAbEMZTi9oBBVGuS19eqGcsqb6bollktlaRRAGkABweFPfiWXHPmBR9sTAU8r+2MdCH4PKLlrIg1epEE+4ljNWW2SXZuSVUUsYp3PdeiQH0eHIdIZFAqvixKq2z/MqQlpcO9YvwvYMRech1ESxuA4omG4hMl4GstioSxzNdETukhIRhiT0QCKJEt6Dx5tDTTzSTsL2Vi4Tq3Ty6EQIDAQAB

Juhul, kui on vaja kasutada mõne e-kirja mass-saatja teenust (nt. sendsmaily või mailchimp) tuleks teenusepakkuja käest küsida nende spetsiifiline DKIM ning lisada see sarnaselt enda avaliku võtme kirjega oma domeeni DKIM kirjesse.

DKIM on vajalik, et tagada DMARCi korrektne töö juhul, kui DMARCi *policy* p=quarantine või p=reject.

Alusta tutvumist siit: http://www.dkim.org/

DMARC

DMARC on SPFi edasiarendus tagamaks e-kirjade usaldusväärsust.

DMARCi üks peamine eelis SPFi ees on see, et üldine *policy* laieneb vaikimisi ka kõikidele alamdomeenidele. DMARCi kirje on sarnaselt SPFiga vaja lisada DNS kirjesse.

DMARCi teine peamine eelis on see, et see kontrollib saatja e-posti aadressis kasutatava domeeni puhul nii selle domeeni SPFi kui DKIM väärtust ning sõltuvalt *policy* seadistusest käitub kirjaga vastavalt juhisele (nt. tõstab kirja SPÄM kataloogi).

Kolmanda eelisena annab DMARCi rakendamine tagasisidet domeeni omanikule, kui palju ja kust tema nimel kirjutatakse (see võimaldab tuvastada domeeni väärkasutust). DMARC parameetrid defineeritakse DNS serveril rakendatava domeeni osas TXT tüüpi kirjetena.

DMARC HOST kirje näide: _dmarc.cert.ee
DKIM TXT kirje näide: v=DMARC1; p=reject; sp=reject; pct=100; fo=1; rua=mailto:dmarc@cert.ee; ruf=mailto:dmarc@cert.ee

DMARCi rakendamise puhul on oluline e-kirja vastuvõtmisel täiel määral lähtuda RFCst.

Meetme kasutuselevõtt on riigisektoris kohustuslik. Samuti on soovitatav meedet rakendada oma lepingupartneritega suhtlusel.

Alusta tutvumist siit: https://dmarc.org/

DNSSEC

Soovitame rakendada oma domeenidel DNSSECi kaitsmaks neid paremini võltsimisrünnete vastu. DNSSEC on oluline eeldus DANEil põhineva krüpteeritud e-kirja edastamiseks.

DNSSECi kasutuselevõtuks pöördu oma avaliku DNSi haldaja poole. Riigivõrgus pakub DNSSEC teenust oma klientidele soovi korral RIA (https://www.ria.ee/et/riigi-infosusteem/riigiasutuste-andmesidevork.html#vorguteenused). DNSSEC'iga tuleb katta nii *forward* kui ka *reverse* kirjed.

Meetme kasutuselevõtt on tugevalt soovitatav. Samuti on soovitav meedet rakendada oma lepingupartneritega suhtlusel.

Ülevaade DNSSECi omadustest: https://www.internet.ee/dnssec

DANE

DANE (DNS-based Authentication of Named Entities) on protokoll, mis kasutab DNSSECi taristut, lisaks DNS kirjete digiallkirjastamisele, ka kõikvõimalike teiste domeenidega seotud sertifikaatide jagamiseks, allkirjastamiseks ning kontrolliks. DANE on hea võimalus kommunikeerida usaldusväärselt oma meiliserverites kasutatavate sertifikaatide avalik võti, mille vastu saab saatja kogu ühenduse kohe krüpteerida.

DANE koostoimes DMARCiga tagab, et MITM tüüpi rünnakuid ei ole võimalik edukalt läbi viia ning kõik kohale jõudnud e-kirjad on tulnud korrektsetest allikatest. Selle kombinatsiooni rakendamine on lihtsam kui Mutual TLSi ning on korratavam.

Alusta tutvumist siit: https://www.internet.ee/dnssec/mis-on-dane

Meetme kasutuselevõtt on riigisektoris vähemalt ministeeriumite ja ametite vahelises meilisuhtluses soovitatav.

Viirusetõrje

Viirusetõrje rakendamine meiliserveri juures ja organisatsioonis laiemalt on ISKE kohuslastele kohustuslik.

Spämmitõrje

Meiliserverite puhul on soovitatav kasutusele võtta elementaarne spämmitõrjevõimekus. Spämmitõrjeks on võimalik kasutada nii kommertsvahendeid kui ka vabavaralisi lahendusi. Kommertslahendustes on tihtipeale viirusetõrje ja spämmitõrje omavahel funktsioonidena ühendatud.

Greylisting

Definitsioon ja selgitus: https://en.wikipedia.org/wiki/Greylisting

Väldi infra paljastamist

Võimalusel puhasta perimeetril oma meilide päised ebavajalikust, et vältida sisemise meilisüsteemi infra ülesehituse eksponeerimist avalikku võrku (nt. sisevõrgu IP aadressid).

Lisamaterjaljalid

Opportunistic TLSi kasutamine Postfix tarkvaraga

Sissetulevate SMTP ühendustele TLSi toe lisamine

Vajalikud tegevused:

- privaatse võtme ja sertifikaadi soetamine,
- Postfixi seadistuse muutmine (vajadusel).

Nt Ubuntu puhul tegelevad seadistusfailis /etc/postfix/main.cf sissepöördumistele TLSi rakendamisega vaikimisi read

```
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
```

Need sobib asendada ridadega

```
smtpd_tls_cert_file=/etc/postfix/mx.domeeninimi.ee.crt
smtpd_tls_key_file=/etc/postfix/mx.domeeninimi.ee.key
smtpd_tls_CAfile = /etc/postfix/CA-teenusepakkuja.crt
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtpd_tls_loglevel = 1
smtpd_tls_security_level = may
smtpd_tls_received_header = yes
```

kus

- esimesed kolm rida defineerivad kasutatava sertifikaadi, salajase võtme ja sertifitseerimisteenuse pakkuja poolse juursertifikaadi,
- smtpd_use_tls – lülitatakse sissepöördumiste jaoks TLS sisse,
- smtpd_tls_loglevel – logitakse lühidalt info TLSi kohta,
- smtpd_tls_security_level – kasutatakse *oportunistic encryption*'it,
- smtpd_tls_received_header – kirjale lisatakse Received päisega info TLSi kohta.

Väljaminevate SMTP ühendustele TLSi toe lisamine

Vajalikud tegevused on lisaks eeltoodule:

- CA teenusepakkujate sertifikaadiahela lisamine,
- Postfix seadistuste muutmine (vajadusel).

Nt Ubuntu puhul vaikimisi seadistusfailis /etc/postfix/main.cf väljapöördumistele TLSi rakendamiseks sobib asendada rida

```
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

ridadega

```
smtp_use_tls = yes
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

```
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtp_tls_loglevel = 1
smtp_tls_security_level = may
smtp_tls_note_starttls_offer = yes
```

kus

- smtp_use_tls – lülitab väljapöördumiste jaoks TLSi sisse,
- smtp_tls_CAfile – milliseid CA teenusepakkujate sertifikaatide kasutatakse,
- smtp_tls_loglevel -– logitakse lühidalt info TLSi kohta,
- smtp_tls_security_level – kasutatakse *oportunistic encryption*'it,
- smtp_tls_note_starttls_offer– logitakse lühidalt info TLSi kohta.

Tulemuse kontrollimine/veaotsing

- saata läbi kõnealuse postimasina kirju välja ja sisse,
- saata kiri http://checktls.com/ abil,
- jälgida logi,
- vajadusel analüüsi veaotsinguks oma võrguliiklust.

Opportunistic TLSi kasutamine tarkvaraga Exchange

Eeldus: Exchange'i jaoks on soetatud SSL-sertifikaadid ja serveris on sertifikaadid olemas.

Sertifikaatide lisamiseks ja uuendamiseks on väga hea juhendmaterjal: https://www.digicert.com/csr-creation-microsoft-exchange-2010.htm

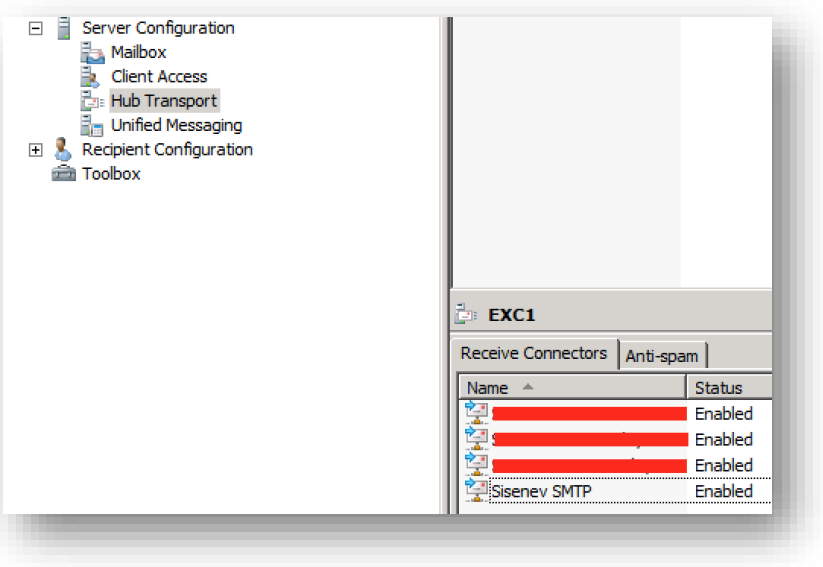
NB! Sertifikaadi CN kirje peab olema sama, mis meiliserveri avalikus võrgus oleva MX kirje, see välistab hulga hilisemaid probleeme.

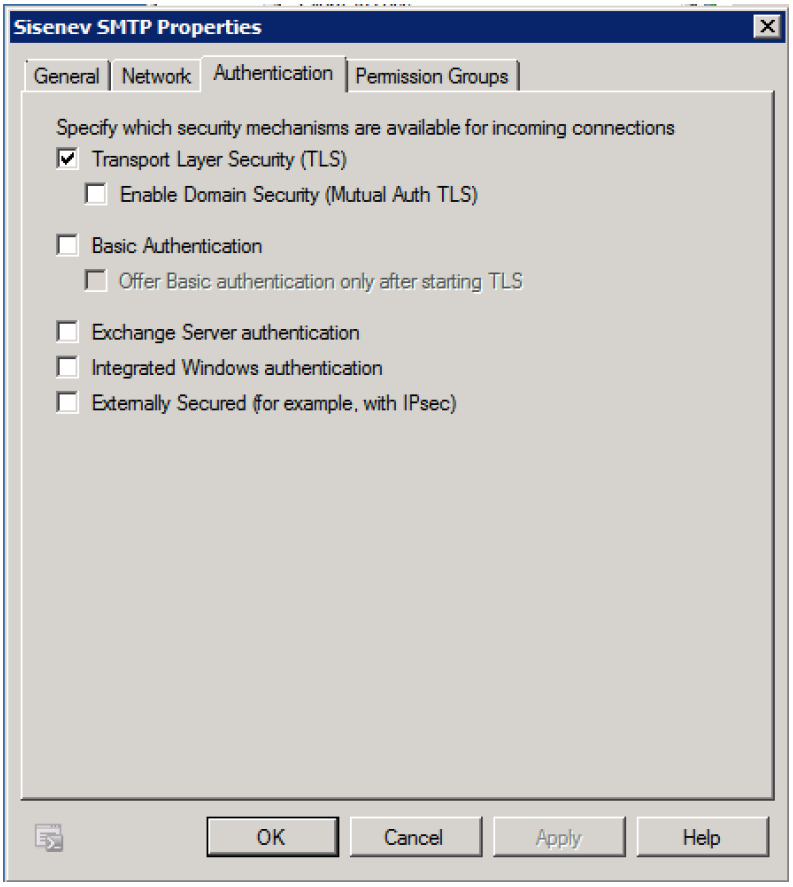
Soovitame kulude kokkuhoiuks kasutada sertifitseerimisteenuse osutajatelt SSL-sertifikaadi ostmisel SAN nimede lisamise võimalust.

Opportunistic TLSi lubamine EMC (Exchange Management Console) vahendusel:

- Ava Exchange Management Console.
- Vali Server Configuration > Hub Transport > Sisenev SMTP (*näites kasutatud Connector*).
- Vali jaotis Authentication.
- Märgi ära valik Transport Layer Security.
- Vajuta OK.

Tegevust illustreerivad ekraanikuvad:



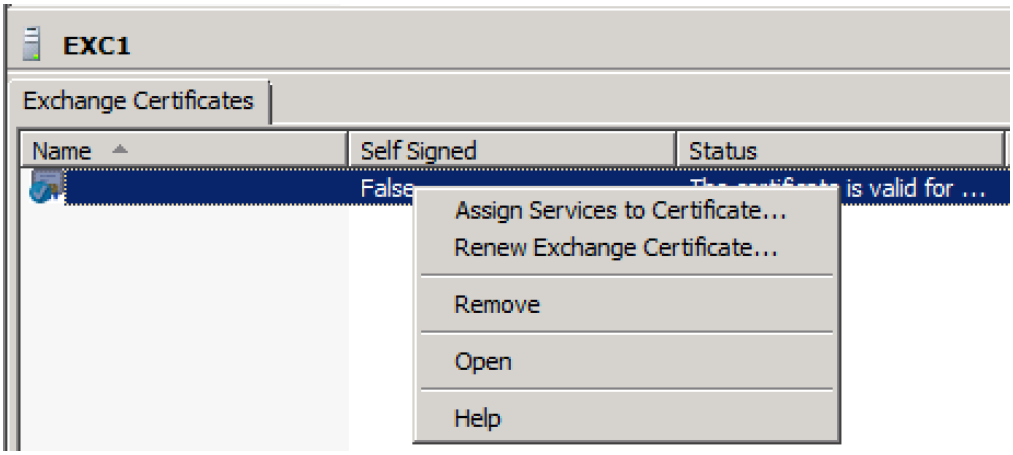


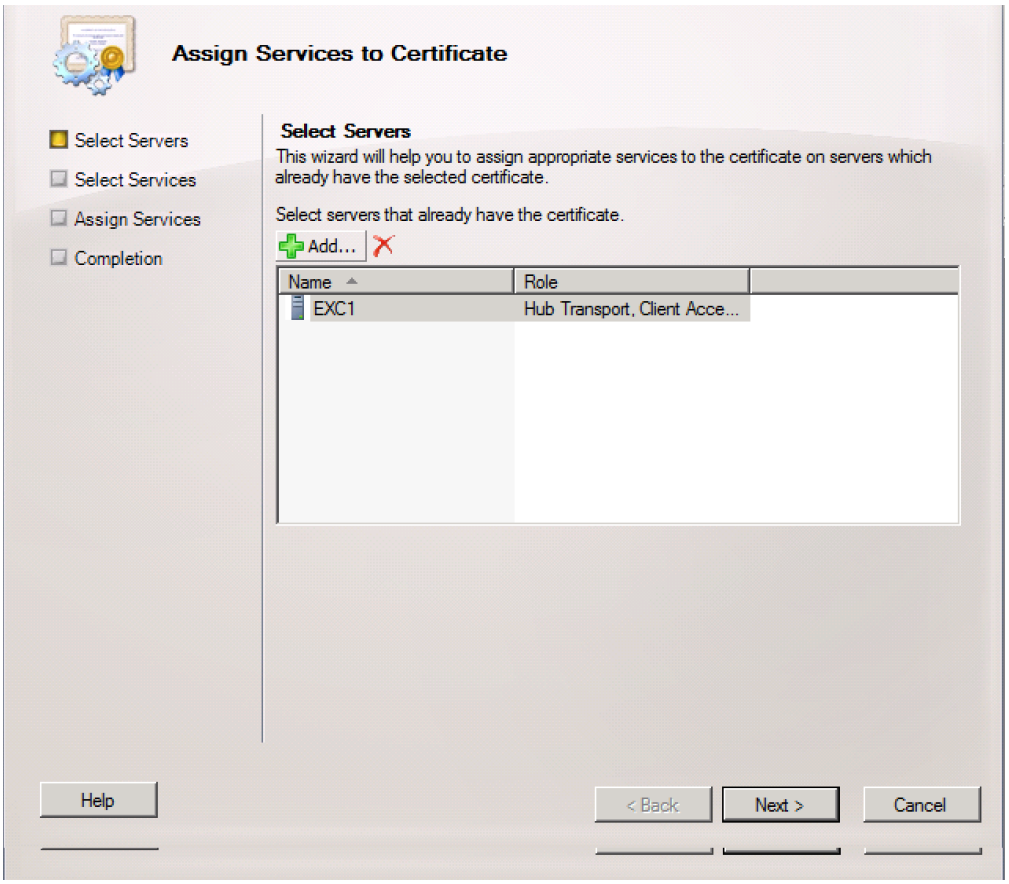
SMTP protokollile kehtiva sertifikaadi omistamine:

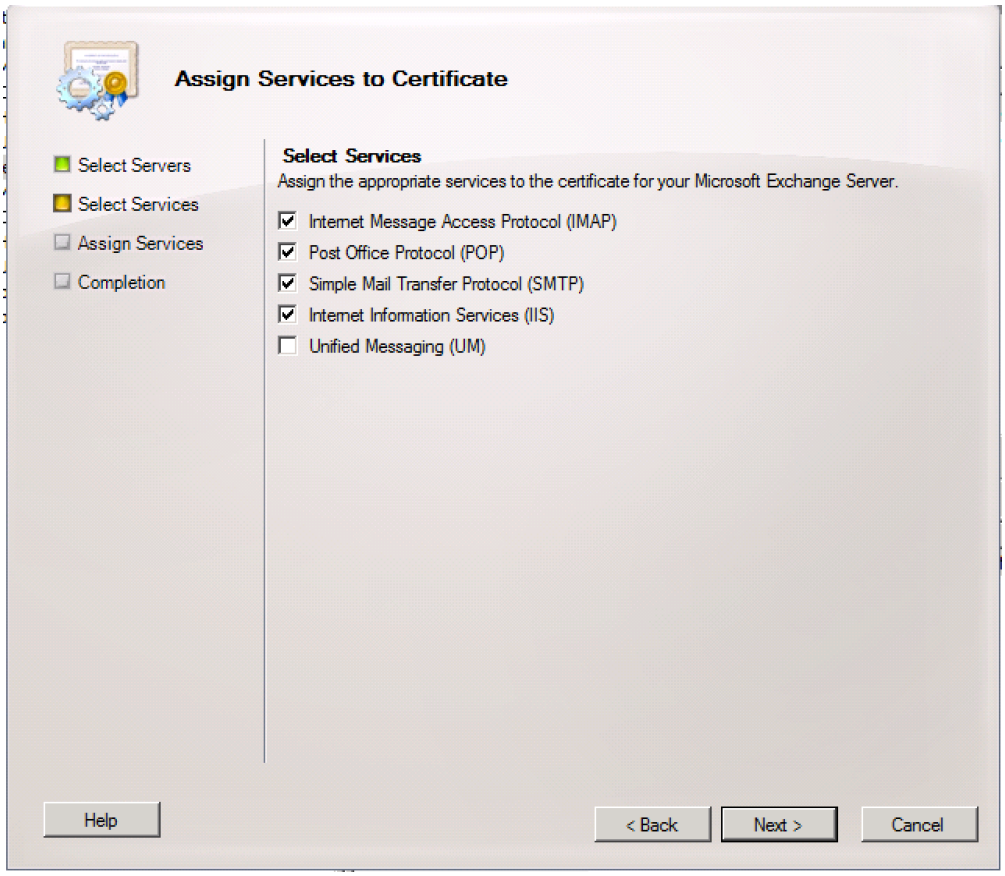
- Ava Exchange Management Console.
- Vali Server Configuration.
- Tee parem hiireklikk olemasoleval kehtival sertifikaadil, mida soovid kasutada SMTP jaoks ja vali Assign Services to Certificate (alternatiivina kasuta halduskonsooli parempoolset abimenüüd või EMS konsooli).

- Märgi sertifikaati kasutavaks teenuseks vähemalt SMTP (vajadusel ka muud teenused).
- Lõpeta häälestamine.

Tegevust illustreerivad ekraanikuvad:







Sellega on Opportunistic TLSi meetodi kasutamine Exhcange'i tarkvaral häälestatud.