Configurazione TLS

1. Il primo passo è creare il CSR e la coppia di chiavi per il server email.
   Si consiglia di utilizzare il seguente comando creando una directory per i certificati
   mkdir tls in /etc/postfix:

   /etc/postfix/tls da qui lanciare poi il comando openssl:

   ```
   openssl req -out CSR.csr -new -newkey rsa:2048 -nodes
   -keyout privateKey.key
   ```

   Se non già installato fare → apt-get install openssl

   I dati che openssl ci chiederà per generare il nostro CSR saranno:

   Common Name: l'hostname a cui dovrà appoggiarsi il certificato (esempio http://www.cecchi.biz)
   Organization: Il nome dell'organizzazione o dell'azienda (Cecchi Business Solutions)
   Organization Unit: L'unità organizzativa dell'azienda (Area CED cecchi.biz)
   City or Locality: La città dove l'organizzazione ha sede (esempio Prato)
   State or Province: Lo stato o la provincia dove ha sede l'organizzazione (esempio Prato)
   Country: Il paese dove ha sede l'organizzazione (esempio IT)

   NB: quando verranno richiesti ulteriori informazioni lasciare i campi vuoti, come riportato

   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []: LASCIARE VUOTO
   An optional company name []: LASCIARE VUOTO

2. Per l'utilizzo del TLS, il server deve avere un certificato ed è possibile utilizzare sia certificati self-signed che certificati rilasciati da una Certification Authority. Nel nostro caso possiamo far rilasciare il certificato da EJBCA che è già riconosciuta come affidabile dato che è nel trustore java del Bizlayer (per l'utilizzo dei WS di EJBCA).

3. Per generare il certificato è necessario seguire, da webui di EJBCA, gli step riportati:

   - *Administrator -> CERTIFICATE PROFILES -> ADD PROFILES* -> Scrivere il nome del profilo. Premere Add e verrà aggiunto.

Una volta aggiunto selezionarlo e con edit settare la durata (es da 730d a 3650d), e soprattutto in Extended Key Usage inpostare Server e Client Authentication ed email protection (con CTRL). Salvare le impostazioni con Save.

- *Administrator -> End Entity Profiles* -> Add profile con same name.inserire username e psw e impostare i campi corretti in Main certificate data. Mettere il profile creato precedentemente. E salvare.
- *Administrator -> Add End Entity* -> Nel campo End Entity Profile, selezionare il profile end entity appena creato sopra.Compila la entity ggiungendo il CN.

4. A questo punto nella pagina *public web* recarsi su *Certificate enrollment from a CSR(o Create Certificate from CSR)*, inserire username, password(Enrollment code) (precedentemente scelti) e caricare il CSR creato allo step 1.
   E' ora possibile generare il certificato.

5. Importare il certificato e la chiave creata al punto 1 nel server email ed aggiornare i riferimenti del TLS (impostando quindi il certificato e la chiave creati in questa guida)
6. Configurare opportunamente Postfix per il TLS nel seguente /etc/postfix/main.cf file:

```
#TLS parameters
#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:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

#enable major logging TLS
smtp_tls_note_starttls_offer = yes
#TLS - SMTP AUTH
disable_vrfy_command = yes

#smtpd_tls_auth_only = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_cert_file = /etc/postfix/tls/Infrastructure.pem  //APPENA GENERATO DAL SITO EJBCA
smtpd_tls_key_file = /etc/postfix/tls/privateKey.key  //GENERATO CON STEP DEL CSR
```

7. I parametri java da settare per utilizzare TLS sono :

```
mail.transport.protocol = smtp
mail.smtp.auth = true
mail.smtp.port = 80
mail.smtp.starttls.enable = true
mail.smtp.ssl.trust=mail.mydomain.it
mail.debug = true
```

Dello specifico file *mailaas.mailer.properties*

8. In assenza di TLS oltre a settare su false mail.smtp.starttls.enable bisogna utilizzare mail.smtp.host invece di mail.smtp.ssl.trust.