SOLUCIÓN PARA EL MEJORAMIENTO DEL SERVICIO DE CORREO ELECTRÓNICO EN LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

Trabajo de desarrollo

DAVID FERNANDO ANDRADE SOLANO
VICTOR ANDRES CASTRO DUEÑAS

ANEXO F
CONFIGURACIÓN DE AUTENTICACIÓN (SASL) Y CIFRADO (TLS)

Director: Guefry Agredo Méndez M.Sc.

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
Grupo I+D Nuevas Tecnologías en Telecomunicaciones - GNTT
POPAYÁN, 2012

TABLA DE CONTENIDO

LISTA DE FIGURAS

ANEXO F

CONFIGURACIÓN DE AUTENTICACIÓN (SASL) Y CIFRADO (TLS)

Introducción

La autenticación se lleva acabo para realizar la confirmación del remitente en el momento que se desea enviar un mensaje y el cifrado de la información se realiza para proteger los datos de usuario con los que se ha autenticado previamente.

En este anexo se exponen las configuraciones necesarias que se realizan en los diferentes archivos para poder cumplir con las funciones de autenticación y cifrado.

1. Configuración de autenticación

Para la realizar configuración de autenticación se necesita instalar inicialmente los siguientes paquetes de SASL [1]:

- sasl2-bin
- libsasl2-modules
- libsasl2-2

Entonces a través de la consola (Terminal):

```
apt-get install sasl2-bin libsasl2-modules libsasl2-2
```

Se crea el archivo `smtpd.conf en etc/postfix/sasl`. En este se ingresa la configuración de autenticación SASL para el servidor Postfix [2]:

```
nano etc/postfix/sasl/smtpd.conf
```

La información que se guarda en este archivo es la siguiente:

```
pwcheck_method: auxprop
auxprop_plugin: ldapdb
mech_list: DIGEST-MD5 PLAIN LOGIN
ldapdb_uri:  ldap://10.200.1.111
ldapdb_id: demo4
ldapdb_pw: michaelmichael
ldapdb_mech: DIGEST-MD5
```

A continuación se hace una breve descripción acerca de esta información:

- **`pwcheck_method: auxprop`:** método utilizado para la verificación de contraseña en un servidor LDAP.

- **auxprop_plugin: ldapdb:** especifica que el plugin `ldapdb` está autorizado para leer la contraseña del cliente.
- **mech_list: DIGEST-MD5 PLAIN LOGIN:** mecanismos de autenticación manejados por sasl.
- **ldapdb_uri: ldap://10.200.1.111:** dirección del servidor LDAP.
- **ldapdb_id: demo4:** nombre de usuario con permisos para ingresar al servidor LDAP.
- **ldapdb_pw: michaelmichael:** contraseña del usuario en texto plano.
- **ldapdb_mech: DIGEST-MD5**: mecanismo de autenticación que maneja LDAP.

Se deben modificar los archivos de configuración de **Postfix** para manejar autenticación mediante SASL [3]. En el archivo `/etc/postfix/main.cf` se modifica esta línea de la siguiente manera:

```
smtpd_recipient_restrictions=permit_sasl_authenticated,permit_myne
tworks,reject_unauth_destination
```

También se ingresa en este archivo, lo siguiente:

```
smtpd_sasl_type=dovecot
smtpd_sasl_path=private/auth
smtpd_sasl_auth_enable=yes
smtpd_sasl_authenticated_header=yes
smtpd_sasl_security_options=noanonymous
smtpd_sasl_tls_security_options = $smtpd_sasl_security_options
broken_sasl_auth_clients=yes
```

En el archivo `/etc/postfix/master.cf` se descomenta la siguiente línea para que postfix trabaje con la autenticación SASL:

```
smtp      inet  n       -       -       -       -       smtpd
 #submission inet n       -       -       -       -       smtpd
 # -o smtpd_tls_security_level=encrypt
   -o smtpd_sasl_auth_enable=yes
   -o smtpd_client_restrictions=permit_sasl_authenticated,reject
 #-o milter_macro_daemon_name=ORIGINATING
```

La línea `-o smtpd_sasl_auth_enable=yes`, indica que la autenticación con SASL se encuentra activada.

Se necesitan configurar otros archivos como los del servidor IMAP para manejar

autenticación [4].

El archivo `/usr/local/etc/dovecot/conf.d/10-master.conf`, se configuro de la siguiente manera:

Se descomentaron los siguientes renglones:

```
unix_listener /var/spool/postfix/private/auth {
 mode = 0666
 user   =
 group =
}
```

Frente a `user` y `group` se coloca `postfix` para que **Dovecot** y **Postfix** trabajen en conjunto para manejar la autenticación. Quedando de la siguiente manera:

```
service auth {

  user = root

unix_listener auth-userdb {
   # mode = 0600
   # user = postfix
   # group = postfix
  }

  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
   mode = 0666
   user=postfix
   group=postfix
  }
```

En el archivo `/usr/local/etc/dovecot/conf.d/10-auth.conf` se configura la siguiente línea, quedando así:

```
disable_plaintext_auth = no

auth_mechanisms = plain login
```

`plain` y `login` son los algoritmos de cifrado tenidos en cuenta para la autenticación. Si no se activa la autenticación en texto plano, se coloca `disable_plaintext_auth = yes`. Para poder realizar comunicación tanto en texto plano como cifrada, debe ir `disable_plaintext_auth = no`.

Se necesita realizar las configuraciones para conectar el servidor postfix con SASL [5].

Se crea la carpeta `/var/spool/postfix/var/run/saslauthd`:

```
mkdir -p  /var/spool/postfix/var/run/saslauthd
rm –r /var/run/saslauthd/
```

Para crear un enlace entre **Postfix** y SASL se ingresan los siguientes comandos:

```
ln –s /var/spool/postfix/var/run/saslauthd /var/run
chgrp sasl /var/spool/postfix/var/run/saslauthd
```

Se adiciona el grupo y el usuario `postfix` para que trabajen con SASL.

```
adduser postfix sasl
addgroup postfix sasl
```

El archivo `etc/default/saslauthd` se modifica para que la autenticación con SASL sea activada y se ingresa el mecanismo de autenticación que se va a usar dependiendo del tipo de almacenamiento de la información de usuarios, que para este caso es LDAP.

```
START=yes
MECHANISMS="ldap"
```

Se coloca la ruta `var/spool/postfix/var/run/saslauthd` en el archivo `etc/default/saslauthd` asi:

```
#OPTIONS="-c -m /var/run/saslauthd".
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r"
```

Ahora se pasa a reiniciar todos los servicios de los cuales se modificaron sus archivos de configuración.

```
/etc/init.d/postfix restart
/etc/init.d/saslauthd restart
/etc/init.d/dovecot restart
```

2. Cifrado de la conexión SMTP por TLS

Además de la autenticación, también se emplean mecanismos como TLS para proteger los datos de usuario mediante una conexión cifrada. Generalmente la comunicación entre cliente y servidor se realiza en texto plano, esto ocasiona que la información de autenticación de usuario sea susceptible a intercepciones de terceros interesados en robar otras identidades para enviar *spam* a través de estas cuentas. Existen herramientas para implementar los protocolos SSL y TLS como **OpenSSL**. Este es un software de código abierto que ofrece cifrado de la información y autenticación basada en certificados

digitales los cuales también necesitan de una clave privada.

Para manejar la conexión cifrada TLS se hace necesario modificar algunos archivos [6], en el `/etc/postfix/main.cf` se incluyen las siguientes líneas:

```
smtpd_tls_cert_file=/etc/ssl/certif/smtp.crt
smtpd_tls_key_file=/etc/ssl/certif/smtp.key
smtp_use_tls=yes
smtpd_use_tls=yes
smtpd_tls_auth_only=no

smtp_tls_note_starttls_offer = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
```

En la línea de cifrado con TLS `smtpd_tls_cert_file=/etc/ssl/certif/smtp.crt`, la ruta `/etc/ssl/certif/`, es donde se creó el certificado digital `smtp.crt` y la llave privada `smtp.key` que se tiene en cuenta en la línea `smtpd_tls_key_file=/etc/ssl/certif/smtp.key`.

En el archivo `/usr/local/etc/dovecot/conf.d/10-ssl.conf` se configuran las rutas de los certificados de Dovecot:

```
ssl_cert= </etc/ssl/certif/certs/dovecot.pem
ssl_key= </etc/ssl/certif/private/dovecot.pem
```

La creación del certificado digital se realiza con el fin autenticar el dominio del cual se esta enviando el mensaje y sirve para negociar entre el cliente y el servidor, las claves que se necesitan para cifrar la ruta. A continuación se explica como se llevo a cabo la creación del certificado [6]:

El certificado fue creado en `etc/ssl/.` Primero se creó el directorio `certif`:

```
root@anker:/etc/ssl# mkdir certif
```

Se ingresa al directorio creado:

```
root@anker:/etc/ssl# cd certif
```

Se utiliza el siguiente comando para crear un archivo de parámetros DSA, luego este archivo se utiliza para crear la llave privada con algoritmo DSA y el certificado.

```
root@anker:/etc/ssl/certif# openssl dsaparam 1024 -out dsa1024.pem
```

En la ventana del Terminal que muestra la Figura 1, se observa la creación de este archivo:

Figura 1. Creación de archivo DSA.

Con el siguiente comando se crea el certificado `smtp.crt` y la llave privada `smtp.key`:

```
root@anker:/etc/ssl/certif# openssl req -x509 -nodes -newkey dsa:dsa1024.pem -days 1095 -out smtp.crt -keyout smtp.key
```

A continuación aparece lo siguiente, solicitando ingresar la información para el certificado. Se ingreso la información que aparece en la Figura 2:

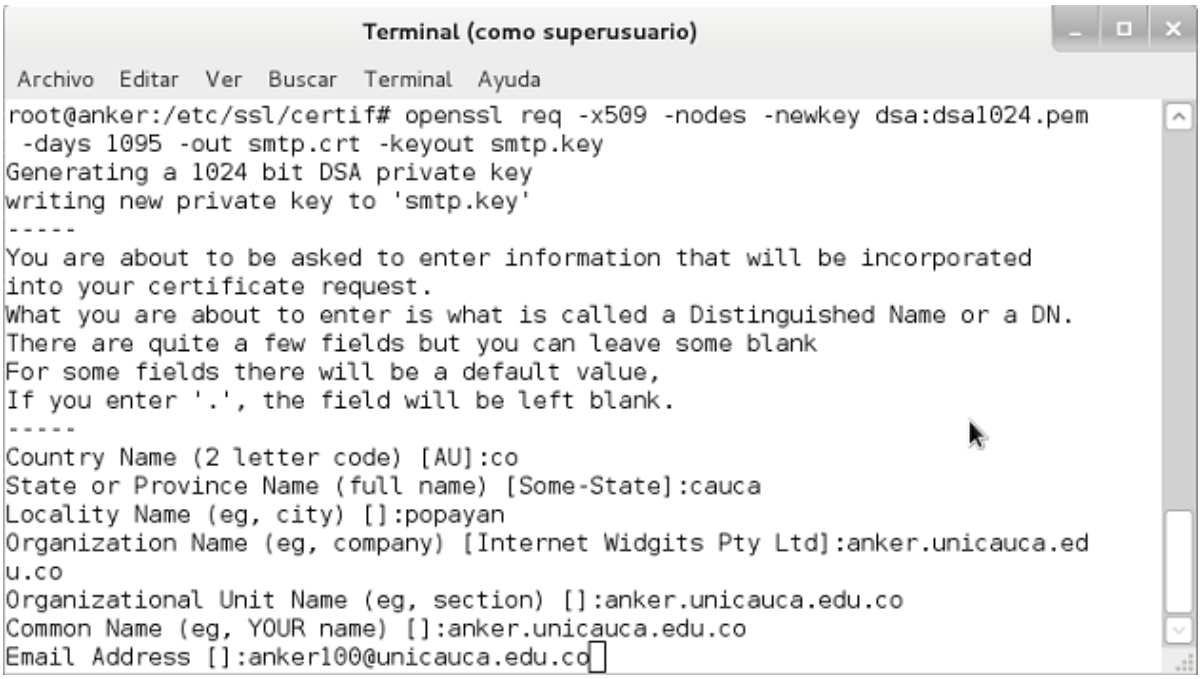

Figura 2. Creación de certificado y llave privada

Se observa que se creo el certificado smtp.crt con su llave privada `smtp.key`, también esta el archivo `dsa1024.pem`, este se puede eliminar ya que no es necesario tenerlo, solo se necesita para poder crear el certificado y la llave privada.

```
root@anker:/etc/ssl/certif# ls
dsa1024.pem smtp.crt smtp.key
root@anker:/etc/ssl/certif# rm -f dsa1024.pem
```

Se necesitan dar permisos de acceso a los certificados y claves para que sean de solo lectura:

```
root@anker:/etc/ssl/certif# chmod 400 smtp.crt smtp.key
```

Luego se crea el certificado para **Dovecot**, este requiere de una clave con algoritmo RSA. Primero se crean los directorios `certs` y `private` dentro del directorio `certif` para almacenar el certificado de **Dovecot** y la clave privada.

```
root@anker:/etc/ssl/certif# mkdir certs private
```

El certificado se crea con el siguiente comando:

```
root@anker:/etc/ssl/certif# openssl req -x509 -nodes -newkey
rsa:1024 -days 1095 -out certs/dovecot.pem -keyout
private/dovecot.pem
```

Se genera lo siguiente solicitando la información para este certificado, en la Figura 3 se muestra la información ingresada:

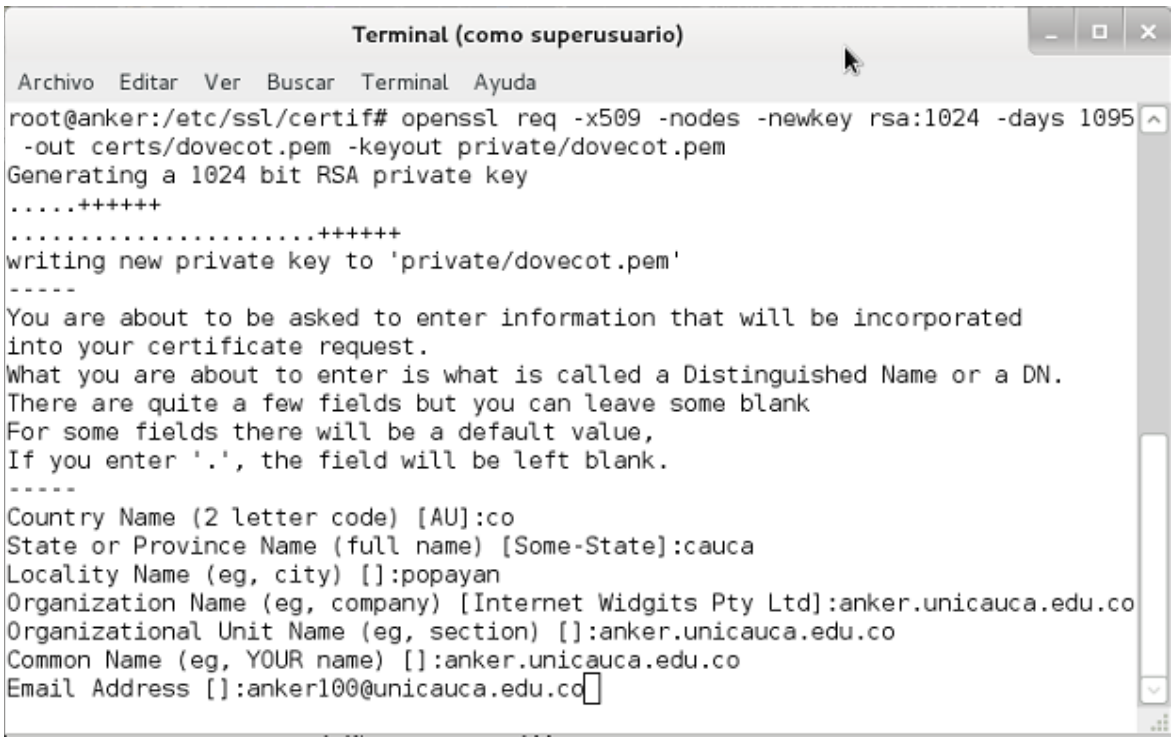

Figura 3. Certificado para Dovecot

Se escribe el siguiente comando para verificar la información del certificado:

```
root@anker:/etc/ssl/certif# openssl x509 -subject -fingerprint -
noout -in certs/dovecot.pem
```

Muestra lo siguiente en la Figura 4:

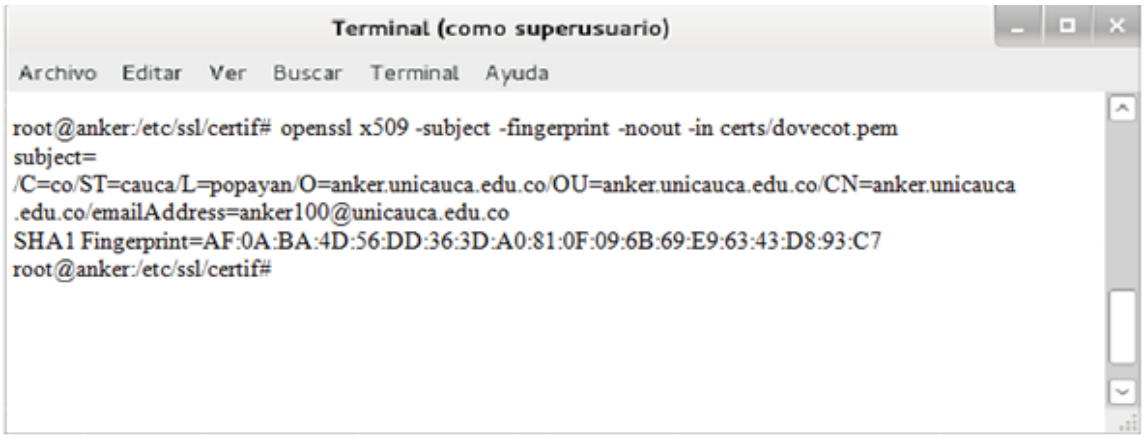

Figura 4. Verificacion de certificado

En el archivo **/etc/postfix/master.cf** se descomentan las siguientes líneas, quedando de la siguiente manera:

```
smtp      inet  n       -       -       -       -       smtpd
#submission inet n       -       -       -       -       smtpd
 -o smtpd_tls_security_level=encrypt
 -o smtpd_sasl_auth_enable=yes
 -o smtpd_client_restrictions=permit_sasl_authenticated,reject
 -o milter_macro_daemon_name=ORIGINATING
#smtps     inet  n       -       -       -       -       smtpd
 #-o smtpd_tls_wrappermode=yes
 #-o smtpd_sasl_auth_enable=yes
 #-o smtpd_client_restrictions=permit_sasl_authenticated,reject
 #-o milter_macro_daemon_name=ORIGINATING
```

En este caso se descomentan las líneas de SMTP para que la comunicación se realice por el puerto 25, la otra opción es SMTPS y la comunicación se realiza por el puerto seguro de SMTP 465.

Cuando el parámetro `-o smtpd_tls_security_level=encrypt` se encuentra activado, quiere decir que la comunicación solamente se puede llevar a cabo cifrada mediante TLS, mientras que si este no esta activado, además de TLS, también se puede realizar en texto plano.

REFERENCIAS BIBLIOGRÁFICAS

[1] «www.taringa.net,» [En línea]. Available: http://www.taringa.net/posts/linux/1889932/Postfix-autenticado.html.

[2] 2009. [En línea]. Available: http://th3d0ctor.blogspot.com/2010/05/autenticacion-smtp-postfix.html.

[3] «GNU/Linux, Sistema estable,» 2010. [En línea]. Available: http://jpertuz.wordpress.com/postfix-smtp-autenticado-con-sasl/.

[4] «www.linuxmail.info,» [En línea]. Available: http://www.linuxmail.info/postfix-smtp-auth-dovecot-sasl/.

[5] R. Cores. [En línea]. Available: http://www.slideshare.net/judas3107/postfix-internet-site-sasl-2577352.

[6] J. Barrios, «www.alcancelibre.org,» 2011. [En línea]. Available: http://www.alcancelibre.org/staticpages/index.php/como-postfix-tls-y-auth.