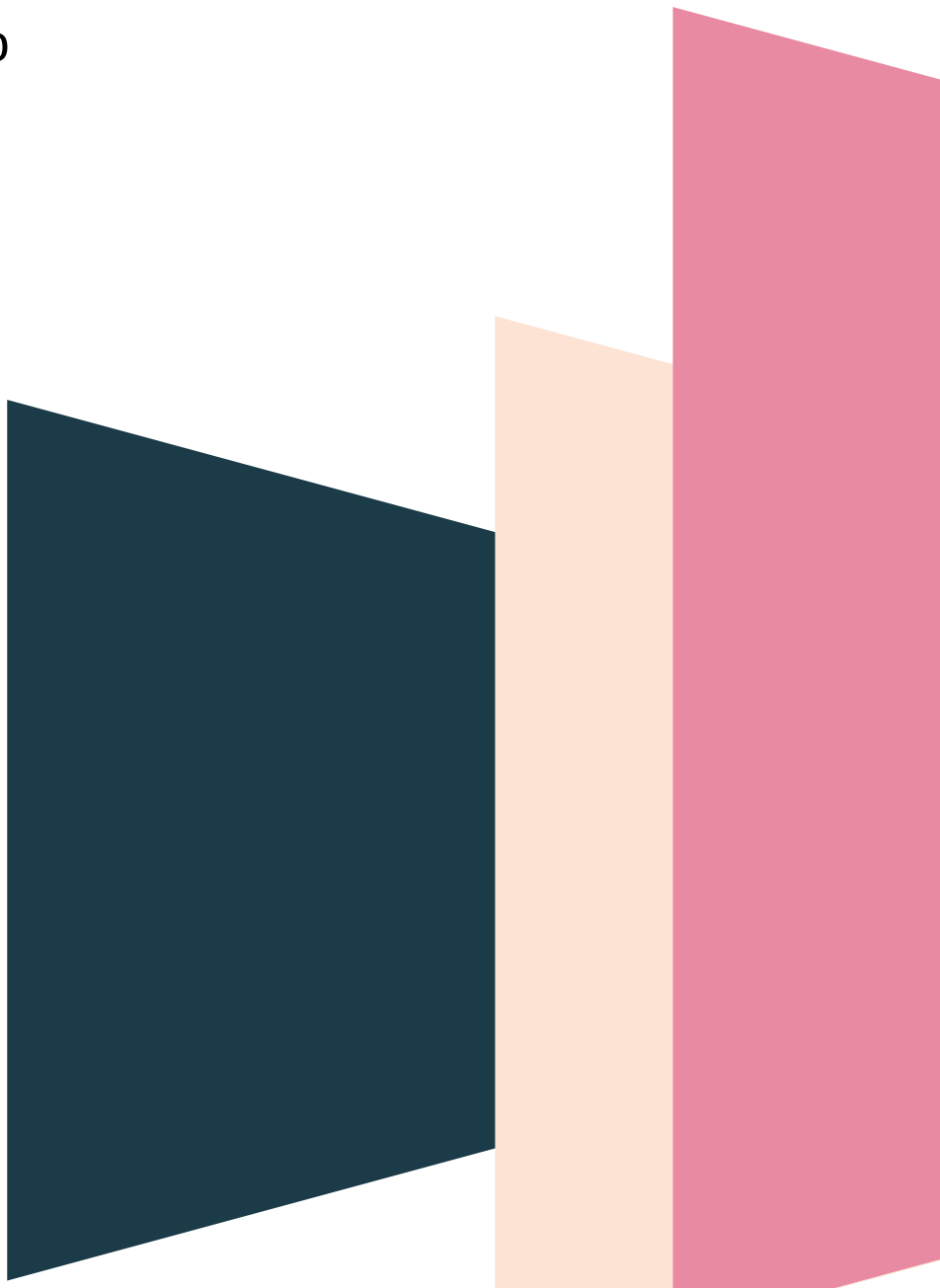
minsait

An Indra company

EDITRAN/GC

Gestión de claves
UNIX
Manual de Usuario

mayo de 2019



ecosystems
communications

1. INTRODUCCIÓN.

EDITRAN facilita al usuario la posibilidad de utilizar varias formas de intercambiar datos protegidos mediante las siguientes modalidades de criptografía:

Modalidad 2.2. Criptografía con autenticación y confidencialidad con algoritmo DES de claves simples de 8 bytes. El intercambio de claves se realiza de manera automática.

Modalidad 3.0. Criptografía de autenticación con algoritmo DES o RSA (1024 bits) y con confidencialidad DES y TDES (con claves dobles o triples).

En la modalidad 3.0 las claves para la autenticación han de intercambiarse entre los extremos antes de poder utilizarlas.

Modalidad 4.0 Criptografía con claves de autentificación RSA de 1024, 2048 o 4096 bits. Los algoritmos para el cifrado de datos son: DES, TDES (con claves dobles y triples) y AES con claves de 128, 192 y 256 bits.

Salvo en la modalidad 2.2, tanto para DES como RSA, las entidades requieren intercambiar sus respectivas claves, es decir el intercambio es externo al protocolo EDITRAN. Este intercambio se ha venido realizando de diversas formas; aplicaciones externas a EDITRAN, correo electrónico, teléfono, etc., con lo que se observa en muchos casos la "debilidad del intercambio".

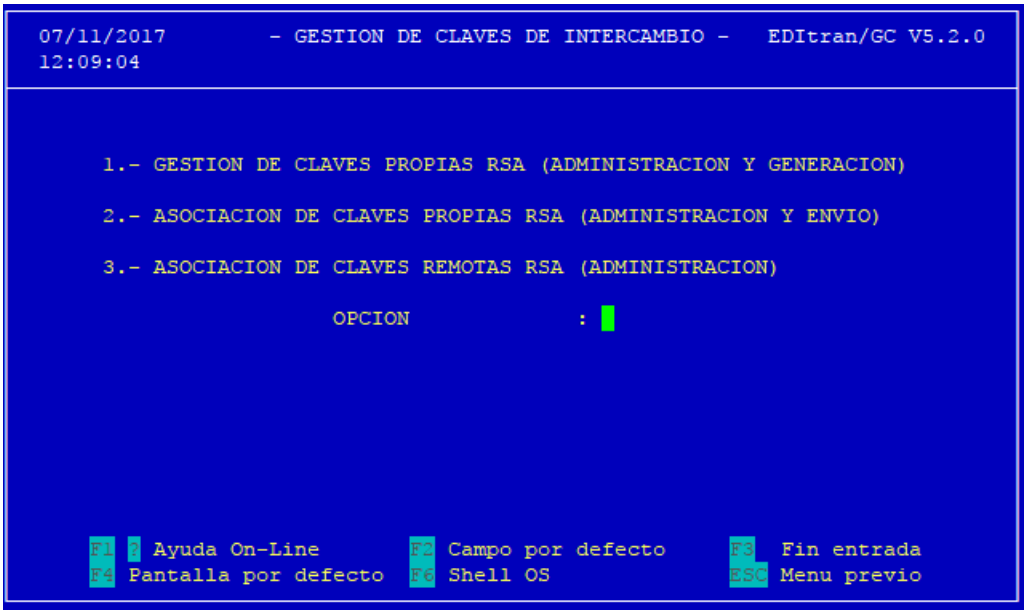
A partir de la versión 4.1.5 EDITRAN ha incorporado una gestión fiable y segura para automatizar el proceso de intercambio, evitando la debilidad comentada, evitando la visualización de claves en claro y facilitando una incorporación e intercambio fiable en ambas entidades.

Cuando se intercambien nuevas claves públicas RSA, todos los envíos (salvo el inicial) pueden ir firmados con alguna privada de la que tengamos constancia que se ha enviado al remoto la pública asociada correspondiente. Es decir, en el segundo intercambio, al menos se podrá firmar con la inicial, en el tercero con la inicial o con la segunda y así sucesivamente. Además, se ha estructurado toda la gestión en "subsistemas". Un subsistema es un grupo de claves intercambiadas para un determinado remoto, grupo de remotos o aplicaciones.

Cada subsistema admite varias claves con versión 01 a 99 (cuando llegan a esa posición dan la vuelta) conservando las 3 últimas. El intercambio con las entidades se realizará a partir de una sesión EDITRAN adaptada al efecto.

2. DEFINICIONES Y PANTALLAS

Al ejecutar **editrangc** en el directorio de EDITRAN se activará el menú principal del gestor de EDITRAN/GC que se muestra a continuación:



- **Gestión de claves propias RSA**. Las claves RSA pueden ser intercambiadas con diferentes remotos sin peligro, ya que lo que se intercambia es la clave pública. La clave privada permanece únicamente en el sistema donde se ha creado y así no hay posibilidad de que los datos puedan ser descifrados por un tercero.

  Por este motivo existen las ***Claves Propias RSA*** de EDITRAN/GC. Mediante las Claves Propias RSA se administran una serie de funcionalidades comunes a todos los remotos que utilicen esa clave como son:

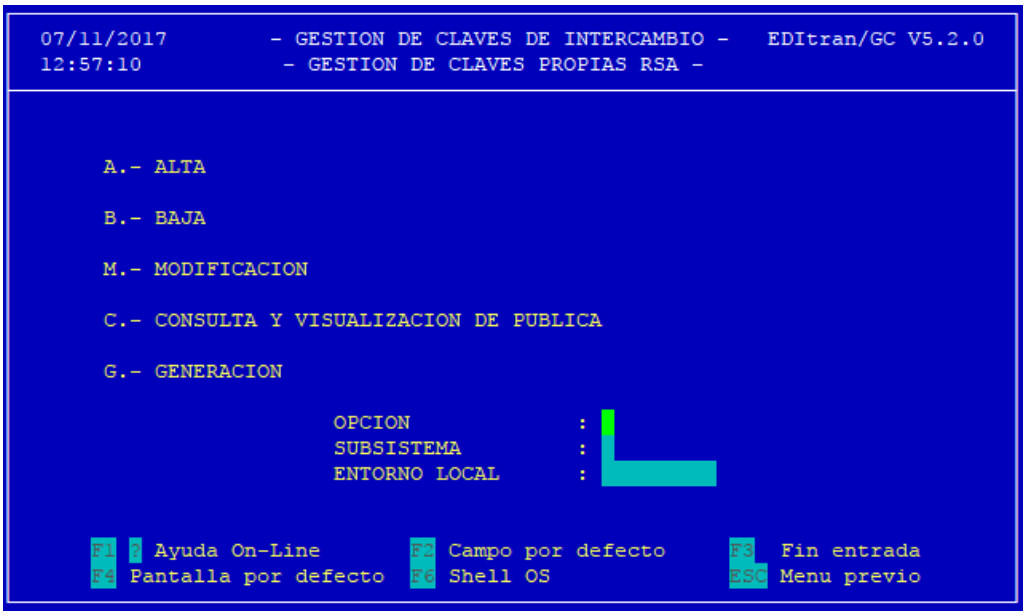
  - Generación de nuevas versiones de la clave (nuevos pares de claves pública-privada)
  - Activación de una u otra versión.

- **Asociación de claves propias RSA**. Una Clave propia RSA no puede utilizarse si no se ha intercambiado con un remoto. Para eso existe la posibilidad de asociar una Clave Propia a un Remoto, creando un ***Subsistema Local RSA***. Una vez asociado se podrá generar el fichero de intercambio y enviarlo al remoto para que éste incorpore nuestra clave pública. Además desde esta opción se realizarán otras tareas comunes de administración: modificación, consulta y eliminación del subsistema.

- **Asociación de claves remotas RSA**. Como receptores de claves públicas remotas definimos Subsistemas **Remotos RSA**. La creación de un subsistema implica conocer el identificador que le dio el remoto al definirlo puesto que debe coincidir en ambas entidades. Una vez creado, las nuevas claves se incorporan procesando los ficheros de intercambio recibidos.

2.1. Gestión de claves propias RSA (administración y generación).

Se accede al mismo con la opción 1 y presenta el siguiente menú:

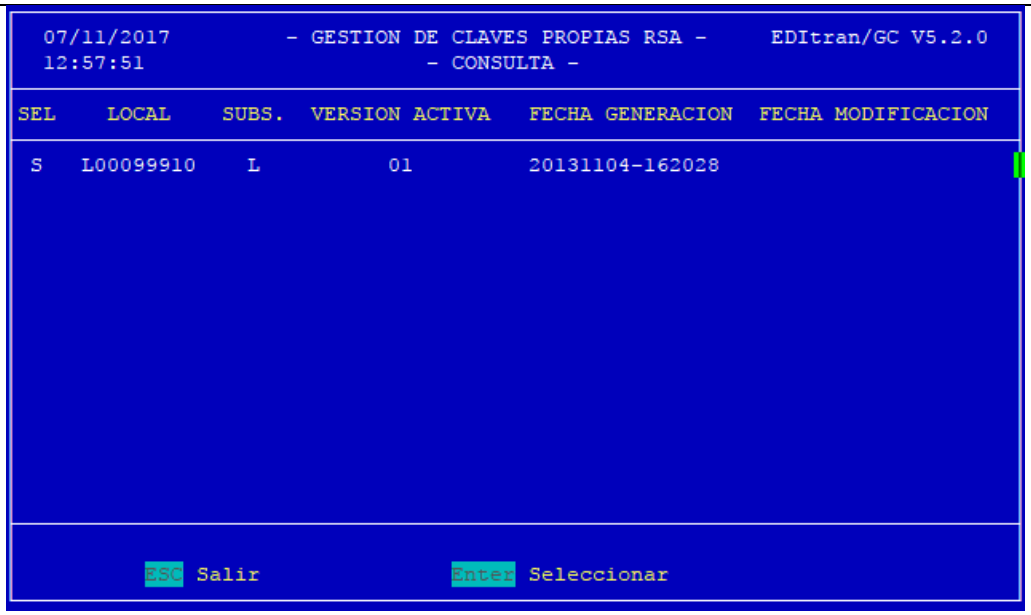


Opción. Campo obligatorio.

Subsistema. Admite valores A-Z y 0-9. Es el nombre del subsistema RSA que vamos a dar de alta. Por ejemplo, podemos tener subsistemas de pruebas o producción, subsistemas de intercambio mensual o anual, subsistemas para un grupo de entidades o para otro, etc. Es opcional salvo en la opción de alta.

Entorno local. Código EDITRAN del entorno local principal. Puede no especificarse cuando no se trate de un alta.

En caso de haber seleccionado algún campo de forma genérica aparece una pantalla en el que se listan los subsistemas que cumplen el criterio de selección planteado y donde el usuario podrá elegir el registro que busca:

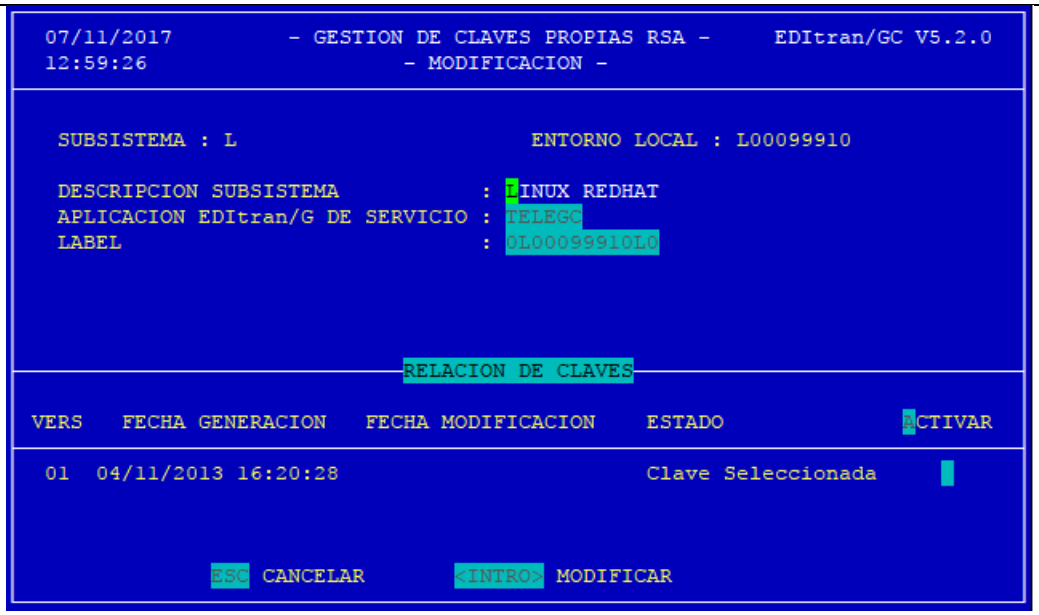


Aparecen para cada código local seleccionado, los subsistemas seleccionados. En caso de que se haya generado claves RSA (privada - pública), se muestra la versión activa, y fechas de generación y última modificación.

En caso de seleccionar algún registro o si la selección era específica desde el menú anterior, se muestra la siguiente pantalla (algunos campos pueden aparecer de forma distinta en función de la opción de acceso, alta-baja-generación, modificación o consulta):

En caso de consulta:

En el caso de modificación:



Descripción subsistema. Es un campo meramente informativo

Aplicación EDItran/G de servicio. Nombre de la aplicación EDITRAN/G que servirá para el intercambio de claves. Este valor actúa como una plantilla, que se traspasará a los registros de las entidades remotas, de forma que podrá incluirse una aplicación distinta para cada intercambio. Valor por defecto: TELEGC.

Label. Etiqueta con la que se identifica la clave pública. Se recomienda no Modificar este valor si no se conoce en profundidad los problemas que pueden aparecer. Al dar de alta el subsistema, se muestra el valor por defecto que el sistema establece para estos campos. El administrador podrá modificar en este momento su valor, asegurándose siempre de que no coincidan con los de otro subsistema

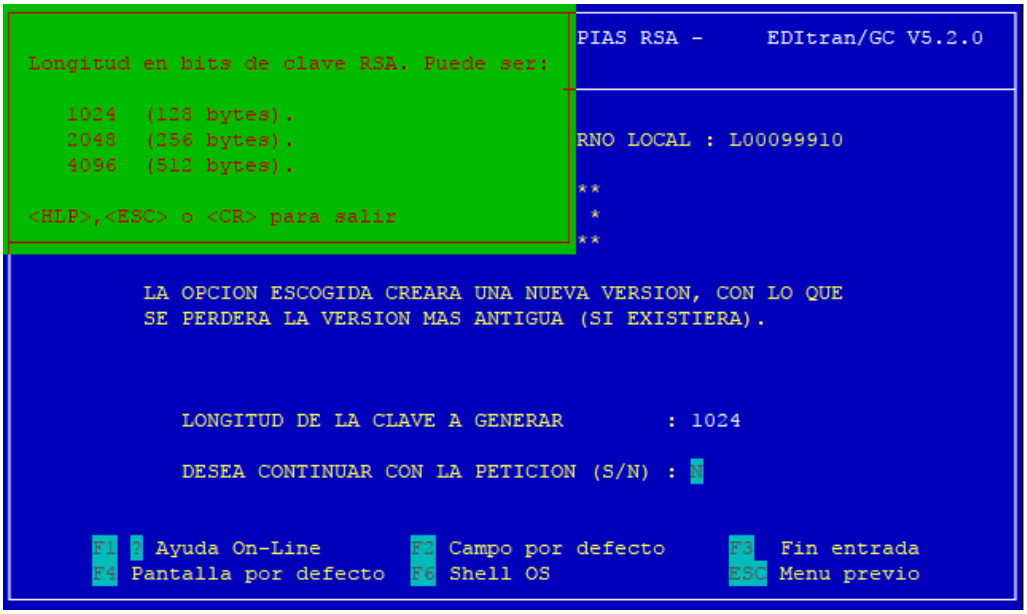
Relación de claves. A continuación se muestra información sobre las últimas tres versiones generadas. Para cada versión se detalla su número de orden, la fecha de creación y de última modificación y el estado en que está (seleccionada o no seleccionada). La versión que está seleccionada es la que actualmente está siendo enviada a los remotos. Cuando se genera una nueva versión, esta pasa a ser la clave seleccionada.

Desde la opción de modificación, el usuario además de poder cambiar otros campos, puede establecer cuál de las versiones mostradas es la que desea intercambiar. Para ello, deberá poner una **A (activar)** en la línea de la versión elegida.

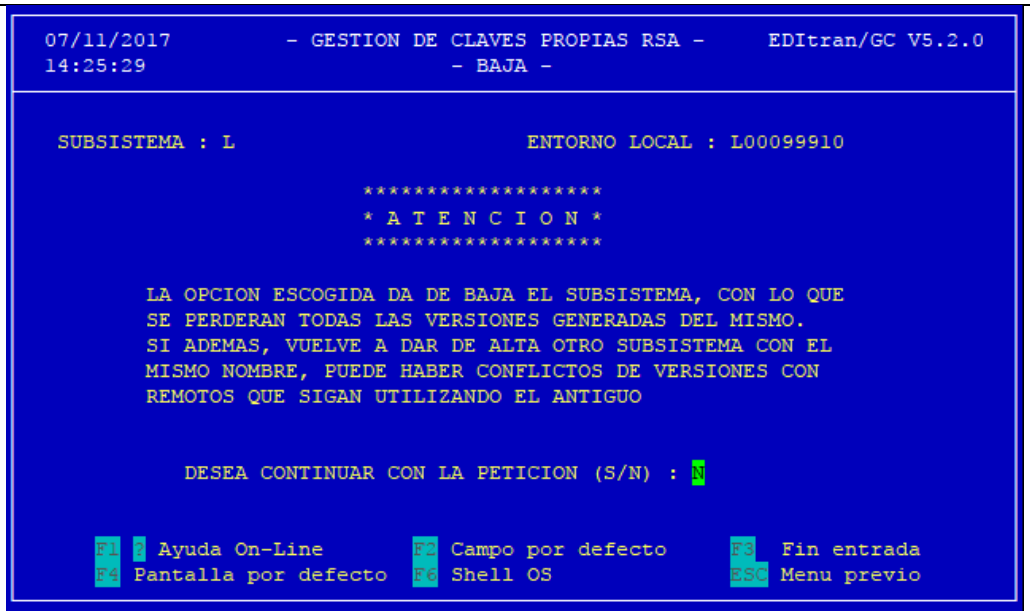
En el caso de consulta, si se ha seleccionado una versión (S), se muestra la clave pública en hexadecimal (en el label se incluye la versión seleccionada). Esta información permite al usuario comprobar de forma manual si una clave está bien intercambiada con un remoto. Para ello habrá que comprobar que el valor es idéntico al que le aparecerá al remoto al consultar la clave remota RSA tras incorporar el correspondiente fichero de intercambio.

En la opción de generación, se muestra una pantalla intermedia de confirmación. Añadiéndose la opción longitud del tamaño 1024, 2048, 4096 bits de la clave, vista en la ayuda.

Al confirmar, el menú se quedará bloqueado mientras se realiza la operación. En el caso de que pueda tardar se le advertirá al usuario con un mensaje informativo al respecto:



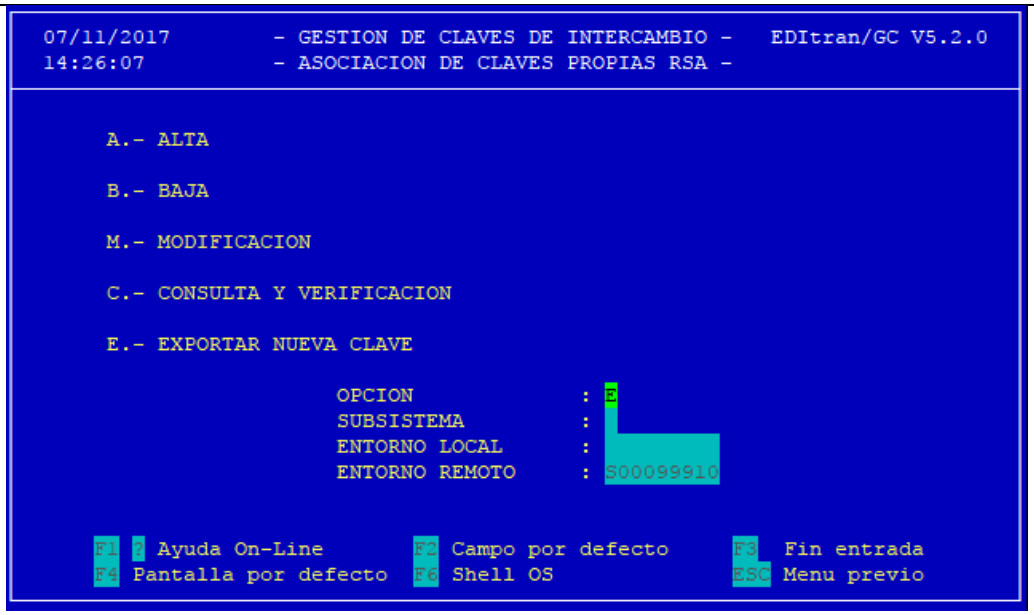
En caso de baja, se muestra una pantalla de confirmación de la misma. No se pueden dar de baja registros RSA PROPIOS si existe algún remoto asociado a los mismos.



2.2. Asociación de claves propias RSA (administración, exportación y envío).

Para acceder a esta opción, es necesario que exista un registro RSA (opción 1) de claves propias adecuado. Es decir, con el mismo código local y subsistema.

Se accede al mismo con la opción 2 y se presenta la siguiente pantalla:



Opción. Campo obligatorio.

Subsistema. Admite valores A-Z y 0-9. Es el subsistema RSA de claves propias que vamos a asociar a una determinada entidad remota. Es el nombre del subsistema RSA que notificaremos al remoto para que lo dé de alta como "subsistema remoto" y con ese nombre incorpore la clave que le enviaremos.

Entorno local. Código EDITRAN del entorno local principal. Si no se rellena se mostrará la lista de los posibles códigos locales (licencias multientorno).

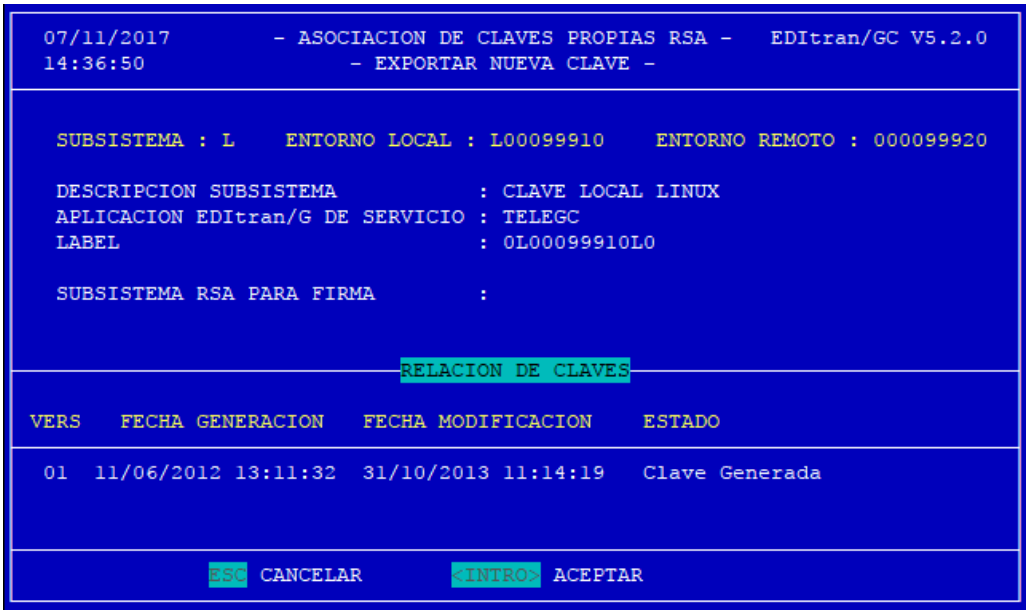
Entorno remoto. Código EDITRAN de la entidad remota. Si no se rellena se mostrará la lista de los códigos remotos existentes.

En caso de no haber especificado todos los campos (campos genéricos) aparecerá una pantalla que muestra la lista de los subsistemas encontrados que se ajustan al criterio de búsqueda dado. El usuario podrá seleccionar uno tecleando **S** en la columna **SEL**:

En la pantalla de selección se muestra, solo en el caso de que el subsistema tenga una clave activa con el remoto, el número de versión y fechas de generación y última modificación.

Al seleccionar algún registro o si la selección era específica desde el menú anterior, se muestra la siguiente pantalla (algunos campos pueden aparecer de forma distinta en función de la opción de acceso, alta-baja-exportación, modificación o consulta):

En el caso de modificación:



Descripción Subsistema. Es un campo meramente informativo

Aplicación EDItran/G, por la que vamos a enviar al remoto nuestra clave pública.

Label. Están protegidos. Son los del registro RSA propias del subsistema que coincide.

Subsistema RSA para firma. Puede ser el mismo (si se han intercambiado claves por él) o distinto (si se han intercambiado claves por otro). Si no se han intercambiado claves con la entidad remota, no se tiene que rellenar dicho campo.

Relación de claves. A continuación, vienen las versiones que se han intercambiado con ese remoto y el estado en que están (activa, cancelada, operativa, etc.).

Sólo puede existir una clave "activa". Una clave enviada a un remoto, pasa a estado activo cuando se recibe del remoto la confirmación de su correcta incorporación; Si existía alguna activa, ésta pasa a estado operativa. De forma excepcional, las claves pueden ser activadas y canceladas manualmente por el usuario desde el menú de modificación.

El funcionamiento de las opciones de consulta y baja es el mismo que el comentado en el apartado anterior. Un subsistema local RSA solo podrá eliminarse cuando no esté siendo usado para firmar los intercambios de clave de otros subsistemas.

La opción *EXPORTAR NUEVA CLAVE*, "asocia" la clave actualmente *seleccionada* del registro de claves propias RSA del subsistema a la entidad remota y crea un fichero con la clave pública local correspondiente (irá obligatoriamente firmada si ha habido algún intercambio satisfactorio de claves RSA con ese remoto). Este fichero será enviado por EDITRAN de forma automática si así se indica. Al seleccionar esta opción se muestra la siguiente pantalla intermedia de confirmación.

En el campo *Archivo Exportación* el sistema muestra el nombre del fichero que se creará para enviar la nueva clave al remoto. Si el subsistema contiene una *Aplicación de Servicio de EDItran/G* (Aplicación de EDITRAN/G que se utilizará para enviar el fichero de intercambio) el nombre del fichero que aparece por defecto será el que esté dado de alta en EDITRAN/G, así se asegura que el fichero generado se enviará correctamente.

Si el subsistema no contiene una Aplicación *de Servicio de EDITRAN/G* o bien esa aplicación no existe en EDITRAN, se muestra un nombre de fichero por defecto, que puede ser modificado, y que no podrá ser enviado automáticamente por EDITRAN.

La clave exportada al fichero de intercambio será la que esté en estado "*seleccionada"* de las tres claves RSA propias. No se permitirá generar un nuevo fichero de intercambio si hay otro intercambio de clave en proceso de finalización. Una vez generado el fichero de intercambio y si el usuario así lo pide con el campo *Desea enviar ahora*, se intentará enviar el fichero por EDITRAN.

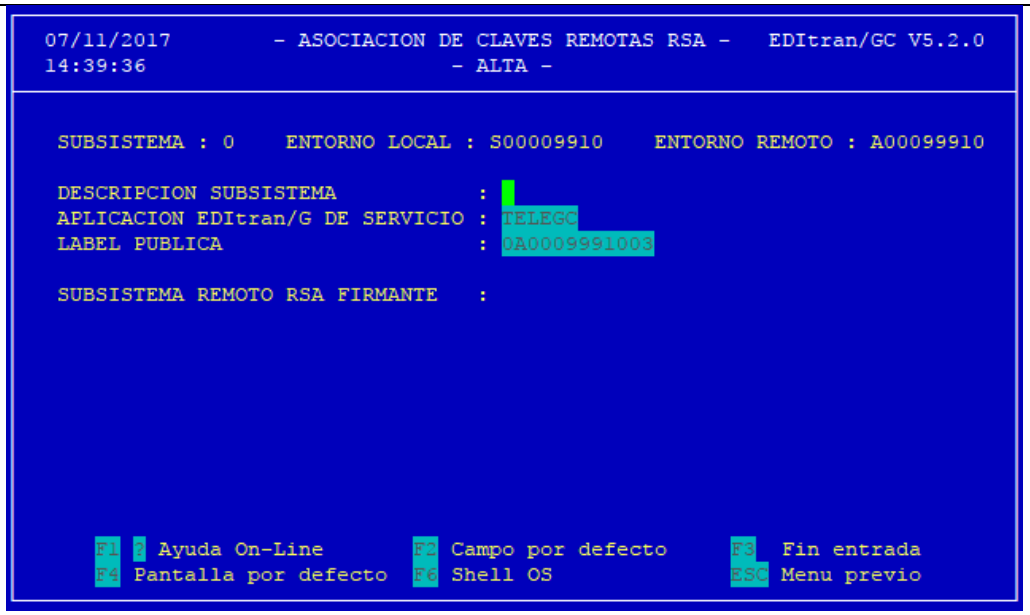
2.3. Asociación de claves remotas RSA (administración).

Se puede generar un subsistema remoto de dos formas:

Automáticamente utilizando el programa de usuario de EDITRAN/G posterior a recepción (mirar sección 4.2). Manualmente a través de la interfaz gráfica como se muestra a continuación.

Para generar un subsistema Remoto RSA desde la interfaz, seleccionar la opción 4 del menú principal y en el menú de asociación de claves remotas RSA seleccionar la opción **ALTA**. Para esta opción es obligatorio especificar código local, código remoto y subsistema.

Una vez seleccionado el subsistema que se quiere crear y siempre que no exista ya otro con los mismos datos, se muestra la siguiente pantalla:



En esta el usuario rellenará opcionalmente la descripción y podrá modificar las etiquetas que por defecto el sistema asigna, aunque se aconseja no modificarlas ya que trabajar con los valores por defecto asegura que no haya "labeles" repetidas.

La aplicación de servicio de EDITRAN/G se utiliza si se quiere enviar las confirmaciones por EDITRAN. Se recomienda utilizar la Aplicación de EDITRAN/G TELEG.

En el campo *Subsistema Remoto RSA firmante* se muestra al usuario el subsistema con que el remoto firmó el último fichero de intercambio incorporado. Es meramente informativo y no puede modificarse.

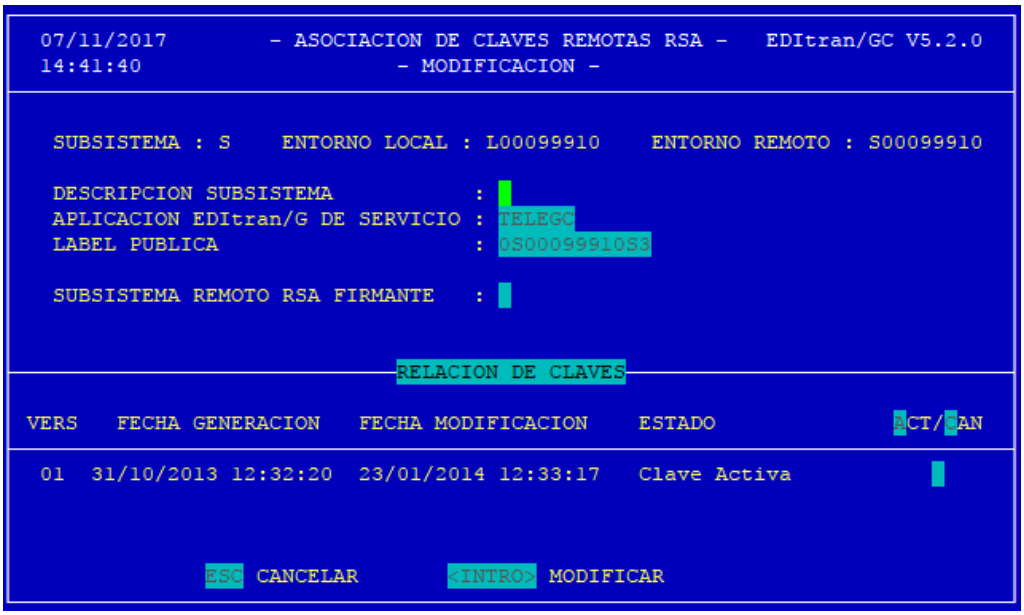
Pulsando F3, se generará el nuevo subsistema remoto RSA. Sin embargo aún no se tiene la clave pública necesaria. Está se tendrá que añadir automáticamente mediante los automatismos de EDITRAN/G o manualmente desde la opción **IMPORTAR NUEVA CLAVE**.

Como se ha visto en los apartados anteriores, para el resto de opciones de administración (baja, consulta, modificación) aparece una misma pantalla en la que además de la información relativa al subsistema se muestran los datos de las tres últimas claves recibidas (versión, estado y fechas de creación y modificación).

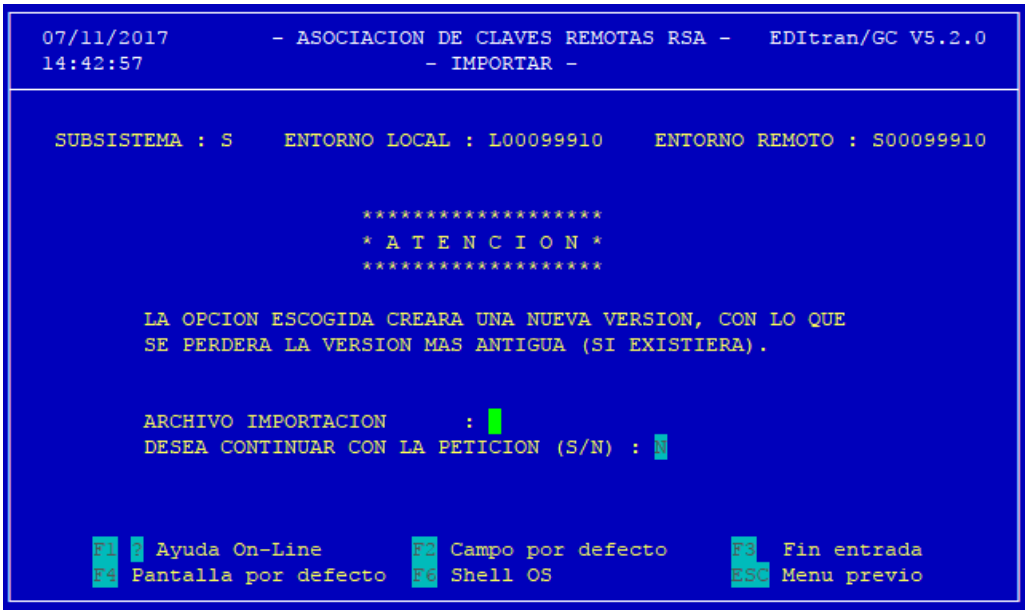
En **BAJA**, tras pedir la confirmación del usuario, al pulsar INTRO se borrará el subsistema mostrado. No se permite eliminar los subsistemas remotos RSA que se estén utilizando para cifrar el envío de algún otro subsistema.

En **CONSULTA**, con las teclas de cursor el usuario puede seleccionar la versión para la que desea ver la clave pública.

En **MODIFICACION**, con la tecla tabulador el usuario va recorriendo los campos del subsistema que son modificables. Además, en la lista de versiones puede modificar el estado de la clave, poniendo **A** (activar) o **C** (cancelar) en la línea correspondiente.



En **IMPORTAR NUEVA CLAVE**, se debe seleccionar el fichero de intercambio recibido del remoto y confirmar la operación.



EDITRAN/GC primero comprueba la firma del fichero de intercambio, luego, se comprueba que el subsistema que viene en el fichero coincide con el subsistema que aparece en la pantalla. Si coincide se incorpora la clave pública, sino el mensaje de error mostrado es *Subsistema no encontrado*.

3. EJEMPLO DE FUNCIONAMIENTO.

En este apartado se resumen los pasos que debe seguir el usuario para intercambiar claves RSA mediante EDITRAN/GC.

Supongamos que las 2 entidades se identifican con los códigos: 100099910 (local) y 200099940 (remoto).

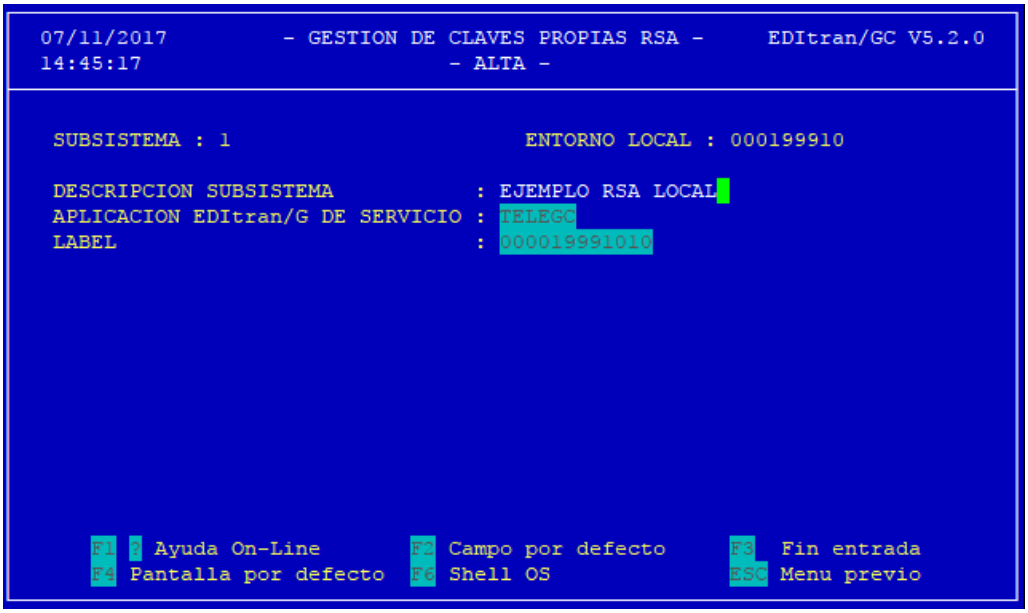
Asumiendo que ambos acuerdan intercambiar sus claves por la aplicación de servicio TELEGC, deberán tener una presentación en EDITRAN/G definida para esos códigos y esa aplicación.

3.1. Intercambio de claves RSA

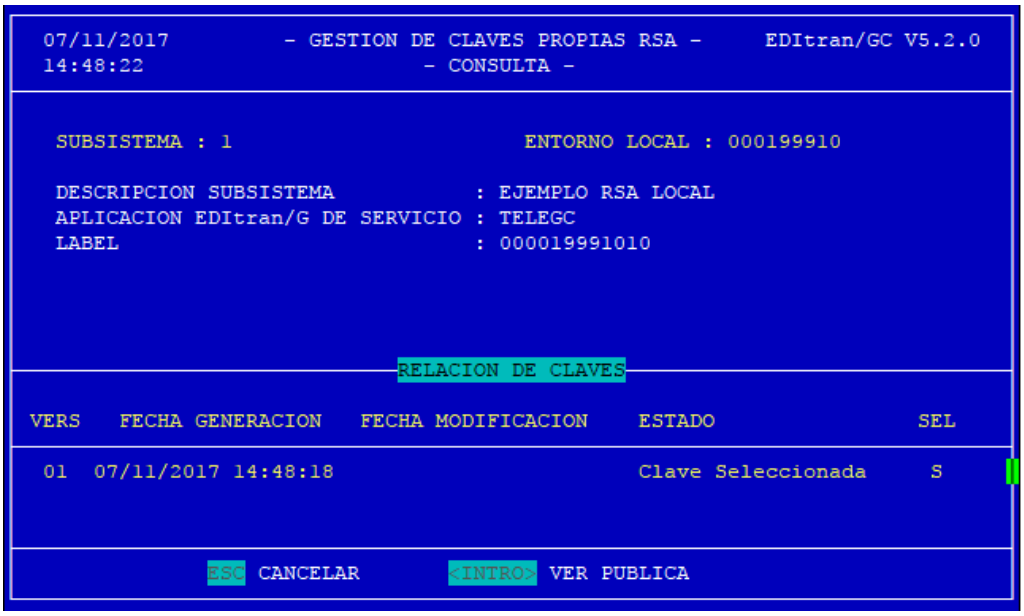
3.1.1. Generación y envío de una clave local RSA

- ❑ Generar una pareja de claves RSA:

- Seleccionar opción **1**: Gestión de claves Propias RSA
- Seleccionar **A**: ALTA poniendo en SUBSISTEMA **1** (o el identificador que se desee) y en ENTORNO LOCAL **000199910**.
- Completar el resto de campos de la pantalla siguiente que incluye el tamaño de la clave a generar y pulsar Intro para generar la versión 1 de la clave.

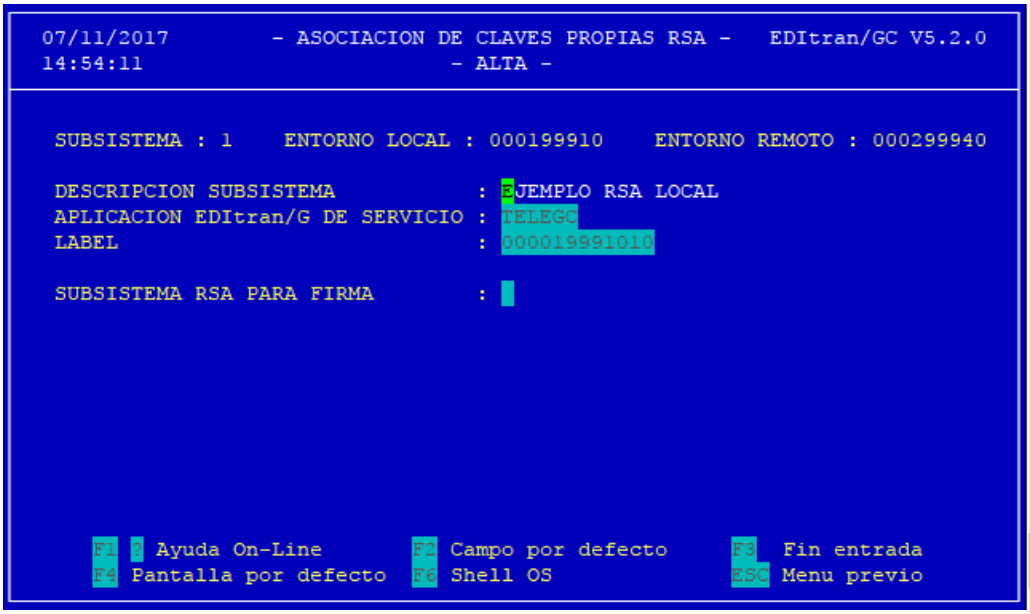


- Comprobar seleccionando **C**: CONSULTA que la clave generada es la que queda como *seleccionada*.

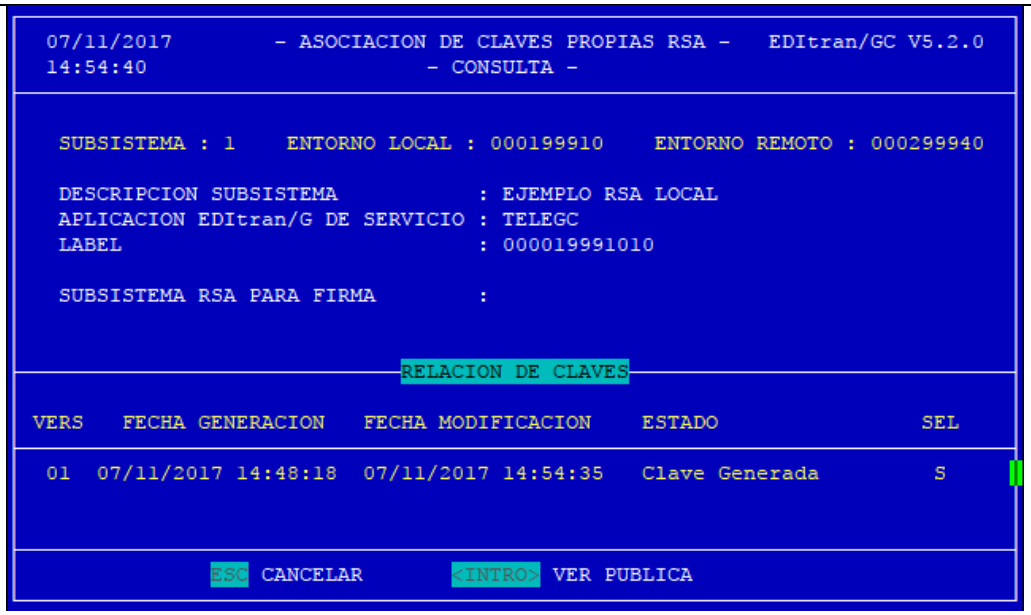


❑ Asociar y enviar claves locales al remoto

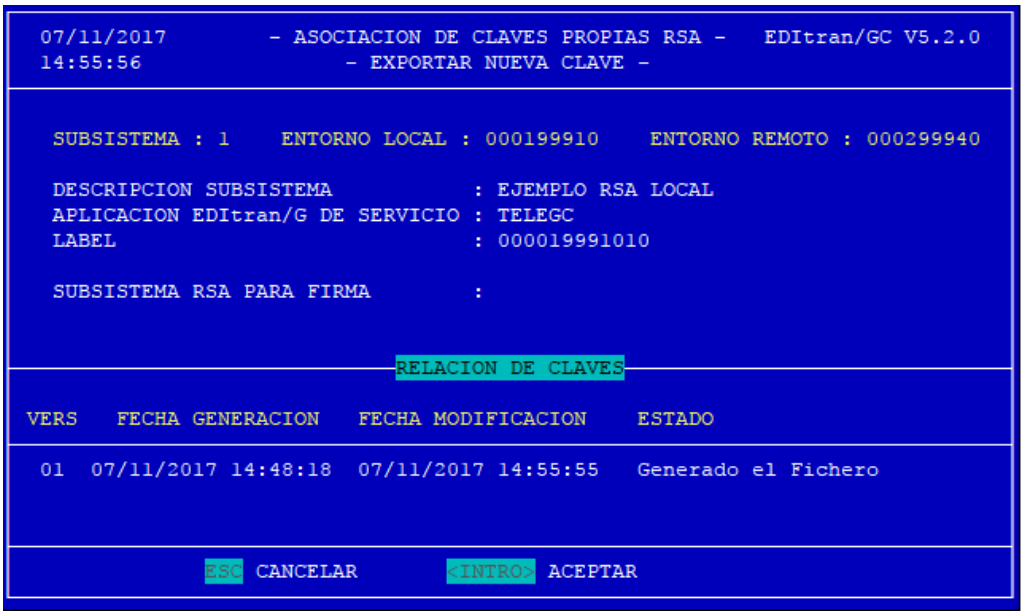
- Seleccionar opción **2** del menú principal: Asociación de claves propias RSA.
- Seleccionar **A** (ALTA) poniendo en SUBSISTEMA **1**, ENTORNO LOCAL **100099910** y ENTORNO REMOTO **200099940** para establecer que queremos intercambiar con ese remoto la clave generada previamente.
- Observar que en la pantalla que aparece, la "label" no puede ser modificada ya que debe coincidir con la dada en la generación. Si ya hubiéramos intercambiado alguna clave RSA con este remoto podríamos firmar el envío de las siguientes claves.



- Comprobar seleccionando **C** (Consulta) que se ha actualizado la clave para ese remoto con la propia asociada.



- Seleccionar **E** (Exportar nueva clave) para generar y/o enviar el fichero de intercambio para el remoto (ver apartado 2.2). Si todo va bien y dependiendo de si el usuario encadenó o no el envío por EDITRAN el estado de la clave quedará:



En este momento, si intentamos volver a exportar una nueva clave, el sistema dará un mensaje de error (*estado incompatible*) por haber una clave pendiente de ser confirmada. Si se quisiera anular la clave pendiente sería necesario cancelarla manualmente desde la opción de **Modificación**.

❑ Recepción del fichero de confirmación

Una vez que el remoto haya insertado nuestra clave pública nos enviará un fichero de confirmación. Este fichero nos indica que el remoto incorporó la clave correctamente y que puede ser utilizada con ese remoto.

Si estamos utilizando EDITRAN y tenemos el automatismo posterior a recepción de EDITRAN/GC, entonces al recibir la confirmación, automáticamente se activará la clave.

❑ **Generar y enviar una nueva versión de la clave**

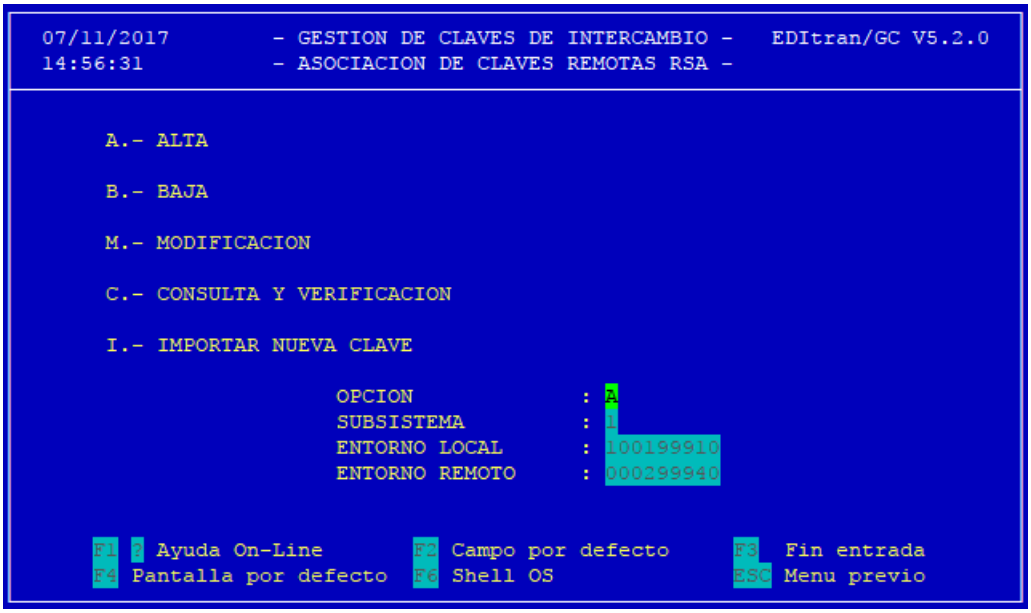
- Para generar una nueva pareja de claves para este subsistema, entrar en el menú ***Gestión de claves propias RSA*** y seleccionar la opción **G** (Generación). Una vez confirmada la operación entrar en consulta y comprobar que en la relación de claves aparece la nueva versión como la clave actualmente seleccionada.

- Para enviar esta nueva versión, entrar en el menú ***Asociación de claves propias RSA*** y seleccionar la opción **E** (Exportar), rellenando o eligiendo el subsistema deseado. En este caso, antes de generar el fichero de intercambio se actualizará automáticamente la clave del subsistema con la versión activa de la clave propia asociada.

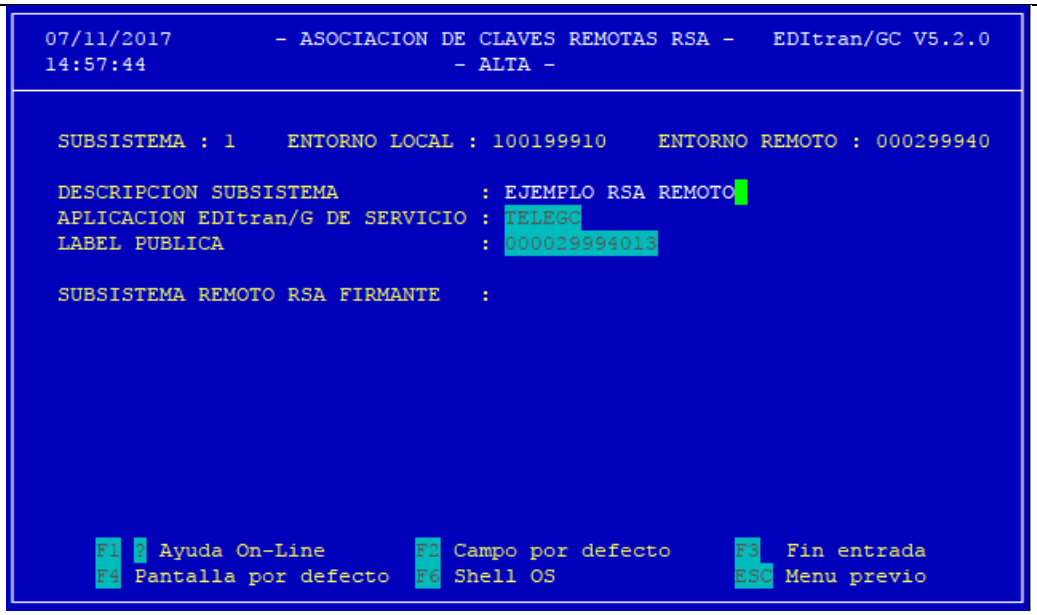
3.1.2. Incorporar y confirmar claves remotas RSA

❑ **Generar subsistema RSA remoto.**

- Seleccionar la opción **4** del menú principal: Asociación de claves remotas RSA.
- Seleccionar **A** (Alta). Los datos que identifican este subsistema los decide el remoto por lo que antes de darlo de alta debemos conocer esta información. Si suponemos que el remoto nos comunica que ha definido el subsistema 2, en los campos del alta pondremos:



- Completar los campos editables de la siguiente pantalla y pulsar F3 para generar el nuevo subsistema.



- **Incorporar nueva clave.**

  Para ello hay que procesar el fichero de claves recibido. Como se ha comentado antes, esto se puede hacer de dos formas: mediante un programa de usuario o desde la interfaz gráfica.

  - El programa de usuario se explica en el apartado 4.2.1. Hay que tener en cuenta, que a diferencia con la interfaz gráfica, al procesar el fichero si no existiera el subsistema que viene en el fichero se generaría automáticamente.
  - Desde la interfaz gráfica, una vez dado de alta el subsistema para el que se quiere incorporar la clave, seleccionar la opción **I** (Importar) para ese subsistema y poner el path del fichero a procesar en la pantalla de confirmación. En este caso se validará que los datos del subsistema que van en el fichero coinciden con los especificados por el usuario.
  - Si todo va bien, entrar en **C** (Consulta) para visualizar la lista de claves una vez incorporada.

- **Confirmar la incorporación de la clave**

  Tras incorporar la clave pública RSA remota, se debe generar un fichero de confirmación que se enviará al remoto para que éste pueda comprobar que el proceso de incorporación se ha efectuado correctamente y así pasar la clave a estado *"Activa"* para que pueda ser utilizada por EDITRAN.

  La generación y envío del fichero de confirmación se hará mediante el programa de usuario que se detalla en el apartado XXXX. El usuario podrá automatizar el proceso adaptando el procedimiento posterior a recepción de EDITRAN/G.

4. UTILIZACION DE EDITRAN JUNTO A EDITRAN/GC

La utilización de EDITRAN como medio de transmisión del fichero de intercambio facilita enormemente la operativa necesaria de EDITRAN/GC. Por tanto aunque no es obligatorio, es sumamente recomendable que EDITRAN/GC y EDITRAN estén instalados.

Fundamentalmente existen dos ventajas claves a la hora de tener instalado EDITRAN:

- ❑ Posibilidad de envío y recepción automática desde la interfaz de EDITRAN/GC de los ficheros de confirmación y claves.
- ❑ Posibilidad de incorporación automática desde EDITRAN, mediante un procedimiento de usuario posterior a recepción, del fichero de intercambio o del fichero de confirmación recibido.

A continuación se explicará cómo aprovechar cada una de las ventajas mencionadas.

4.1. Envío y recepción automática utilizando EDITRAN

4.1.1. Subsistema Local

Para que un fichero de intercambio que contenga una clave (ya sea RSA o DES), es decir un fichero generado por EDITRAN/GC al crear una nueva versión de una clave en un subsistema local, sea enviado automáticamente simplemente hay que añadir el parámetro de Aplicación Servicio EDITRAN/G.

Además habrá que dar de alta en EDITRAN/G la presentación, teniendo en cuenta que el código local y el código remoto de EDITRAN/G deben coincidir con el código local y el código remoto del subsistema de EDITRAN/GC.

4.1.2. Subsistema Remoto

Para que un fichero de confirmación (ya sea de un subsistema RSA o DES), es decir un fichero generado por EDITRAN/GC al insertar una nueva versión de una clave en un subsistema remoto, sea enviado automáticamente simplemente hay que añadir el parámetro de Aplicación Servicio EDITRAN/G en el subsistema Remoto.

Además habrá que dar de alta en EDITRAN/G la presentación, teniendo en cuenta que el código local y el código remoto de EDITRAN/G deben coincidir con el código local y el código remoto del subsistema de EDITRAN/GC.

4.1.3. Perfiles de EDITRAN/G

Los ficheros de intercambio a trasmitir, tanto el fichero de claves RSA como el fichero de claves DES como el fichero confirmación tienen el mismo formato que habrá que dar de alta en las Presentaciones de EDITRAN/G. A continuación se añade una tabla donde aparecen los parámetros de configuración de la Presentación:

Sentido	Concepto	Valor
Emisión	Compresión	Si
Emisión	Alfabeto	ASCII
Emisión	Formato de Ficheros de Aplicación	Fijo
Emisión	Traducción ASCII/EBCDIC	No

Emisión	Longitud de registros de Aplicación	00823
Emisión	Delimitador	Ninguno
Recepción	Traducir en recepción	ASCII

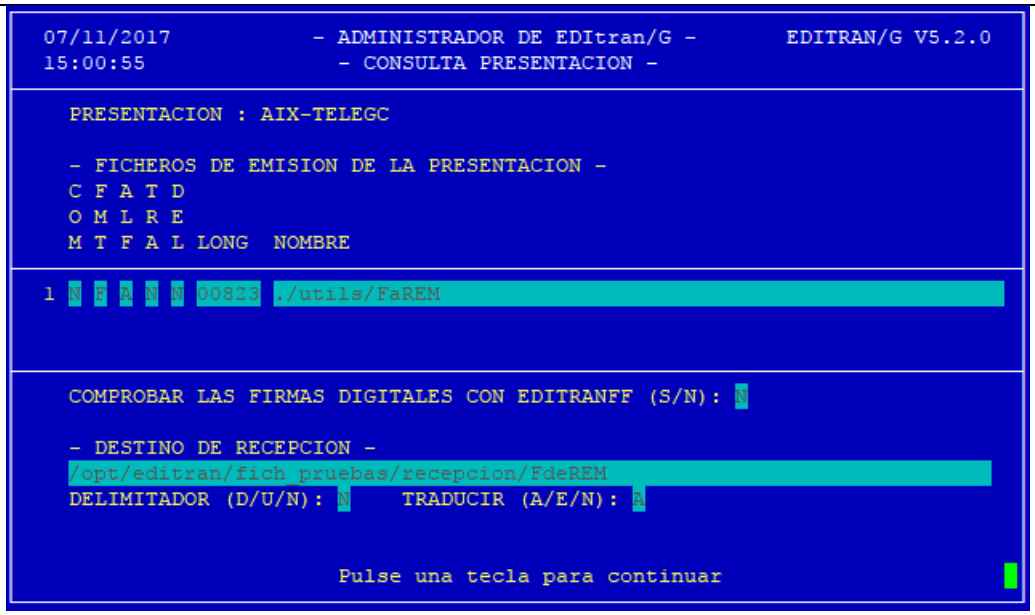
4.2. Procedimiento Automático para EDITRAN

La segunda ventaja es la incorporación automática de los ficheros de intercambio de claves y de confirmación que el remoto nos envíe.

EDITRAN tiene la posibilidad de añadir programas de usuario que se ejecutan antes y después de las transmisiones. Si se quiere utilizar la incorporación automática de los ficheros, se deberá modificar el programa de usuario "Posterior a recepción" y poner el posterior a recepción de Editran/GC.

Por tanto, de la Presentación de EDITRAN/G, con código local y código remoto igual que la dada de alta en EDITRAN/GC, y con la Aplicación de EDITRAN/G igual que la de EDITRAN/GC se deberá modificar el programa posterior a recepción por PSTRECGC.

Además, es conveniente poner como destino de recepción un nombre de un fichero en vez de un directorio. De esta manera nos aseguramos que el fichero que se recibe se llama siempre de la misma manera e igual a como se le ha dado de alta:



4.2.1. PSTRECGC

Es un procedimiento especial que incorpora automáticamente la clave RSA recién recibida del extremo remoto, la asocia al subsistema correspondiente y confirma su recepción al extremo remoto para que pueda ser utilizada en la siguiente transmisión.

```
#Argumentos:
# $1 - Presentacion
# $2 - Sentido
# $3 - Codigo local
# $4 - Codigo remoto
# $5 - Aplicacion
# $6 - Path del fichero con la lista de ficheros transmitidos

EXIT_STATUS=""
echo "################################################################################
######"
echo "SCRIPT DE USUARIO INTEGRACION EDITRAN/GC : $0."
echo "`date`"
echo "PRESENTACION : $2-$1 ($3-$4-$5)"
echo "FICHEROS : [$6]"
sleep 5
while read fclave
do
  if [ "$fclave" != "" ]; then
    echo "insertgc $fclave"
    insertgc -f "$fclave" -c
  fi
done < $6

EXIT_STATUS="$?"
echo "EXIT CODE : ${EXIT_STATUS}"
echo "################################################################################
```

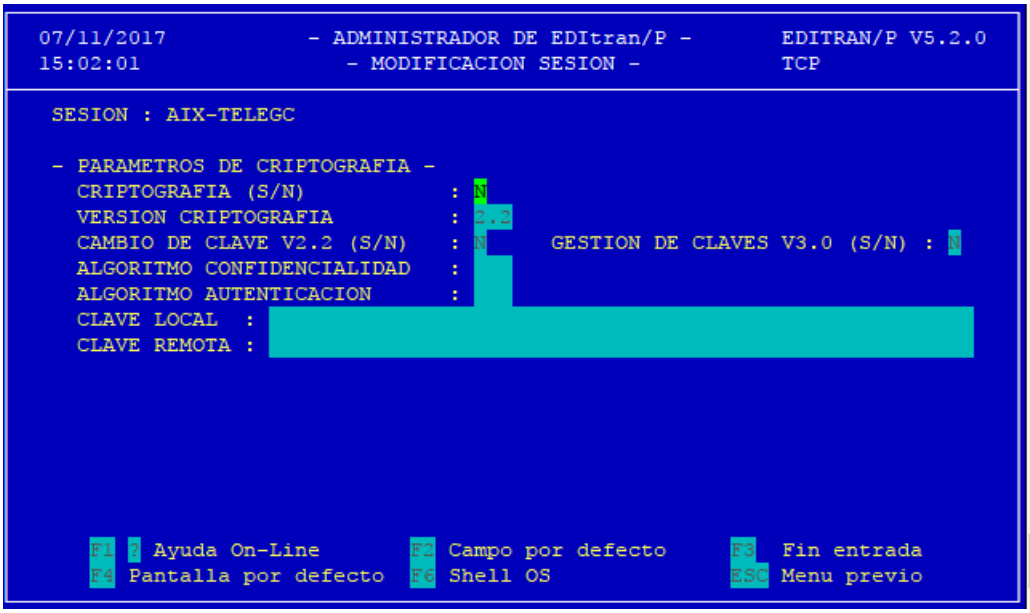
```
######"
exit ${EXIT_STATUS}
```

En el posterior a recepción está la llamada al comando **insertgc** de EDITRAN/GC. El segundo parámetro que se le pasa es el fichero que se ha recibido.

Debe ser definido en el apartado PROGRAMAS DE USUARIO \ POSTERIOR RECEPCION de la presentación del **menú EDITRAN/G**.

4.3. Parámetros de cifrado en EDITRAN

Las claves intercambiadas mediante EDITRAN/GC son usadas en EDITRAN para la transmisión de datos protegidos. Los parámetros de criptografía en este caso serán:



Los parámetros que aparecen en la pantalla son:

- **CRIPTOGRAFÍA (S/N)**

  S Si desea Criptografía EDITRAN/P.
  N Si no desea utilizar la Criptografía EDITRAN/P.

- **VERSION CRIPTOGRAFÍA**

  Este campo es obligatorio si la Criptografía está activada.

  3.0 Criptografía compatible con CRIPTO/lib V3.0.

  4.0 Cifrado AES y claves RSA de 1024, 2048 y 4096.

- **GESTION DE CLAVES V3.0 o V4.0**

  Cuando en versiones de criptografía 3.0 o 4.0 se selecciona esta facilidad, el módulo EDITRAN/GC será el encargado de facilitar las etiquetas correspondientes a las claves activas para los subsistemas indicados en los parámetros CLAVE LOCAL y CLAVE REMOTA.
  S Etiquetas proporcionadas por EDITRAN/GC.

N Etiquetas proporcionadas por el usuario.

- **ALGORITMO CONFIDENCIALIDAD**

  Algoritmo a utilizar para cifrar los datos. Dejar vacío para emitir sin cifrado.
  DES cifrado DES con clave simple.
  TD2 cifrado DES con clave doble.
  TD3 cifrado DES con clave triple.
  AES cifrado AES-128.
  AE2 cifrado AES-192.
  AE3 cifrado AES-256.

- **ALGORITMO AUTENTICACION**

  Algoritmo a utilizar para proteger la clave de sesión y los datos intercambiados para autentificar a los extremos. Es obligatorio siempre que haya cifrado.
  DES si desea autentificar los extremos con algoritmo DES (valido con versiones de criptografía 2.2 y 3.0).
  RSA si desea autentificar los extremos con algoritmo RSA (valido solo para versión 3.0 y 4.0).

- **CLAVE LOCAL**

  Etiqueta de la clave auxiliar DES o la clave privada RSA. Obligatoria cuando la versión de criptografía es 3.0 o 4.0 y hay autenticación.

- **CLAVE REMOTA**

  Etiqueta de la clave auxiliar DES o la clave pública RSA del remoto. Obligatoria cuando la versión de criptografía es 3.0 o 4.0 y hay autenticación.

5. APENDICES

5.1. Estados de los subsistemas

A continuación aparece una lista con todos los estados posibles de las claves de los subsistemas:

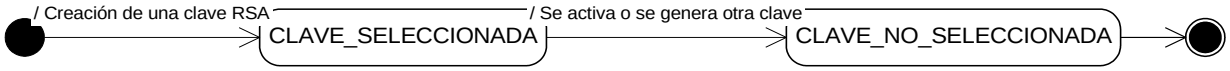
Id	Estado	Texto
1	CLAVE_GENERADA	Clave Generada
2	CLAVE_OPERATIVA	Clave Operativa
3	CLAVE_ACTIVA	Clave Activa
4	GENERADO_FICHERO_ENVIO_CLAVE	Generado el Fichero de Envió de Clave
5	ENVIANDO_FICHERO_CLAVE	Enviando el Fichero de Clave
6	ERROR_ENVIO_FICHERO_CLAVE	Error al Enviar el Fichero de Clave
7	FICHERO_CLAVE_ENVIADO	Fichero de Clave Enviado
8	RECIBIDA_CONFIRMACION	Confirmación Recibida
9	CONFIRMACION_INVALIDA	Recibido un Fichero de Confirmación Inválido
10	CLAVE_REMOTA_INSERTADA	Clave Remota Insertada
11	GENERADO_FICHERO_CONFIRMACION	Generado Fichero de Confirmación
12	ENVIANDO_FICHERO_CONFIRMACION	Enviando del Fichero de Confirmación
13	ERROR_ENVIO_FICHERO_CONFIRMACION	Error al Enviar el Fichero de Confirmación
14	FICHERO_CONFIRMACION_ENVIADO	Fichero de Confirmación Enviado
15	CLAVE_CANCELADA	Clave Cancelada
16	CLAVE_NO_SELECCIONADA	Clave NO Seleccionada
17	CLAVE_SELECCIONADA	Clave Seleccionada

La tabla será útil para localizar por el identificador cada uno de los estados del siguiente diagrama.

5.2. Diagrama de Estados

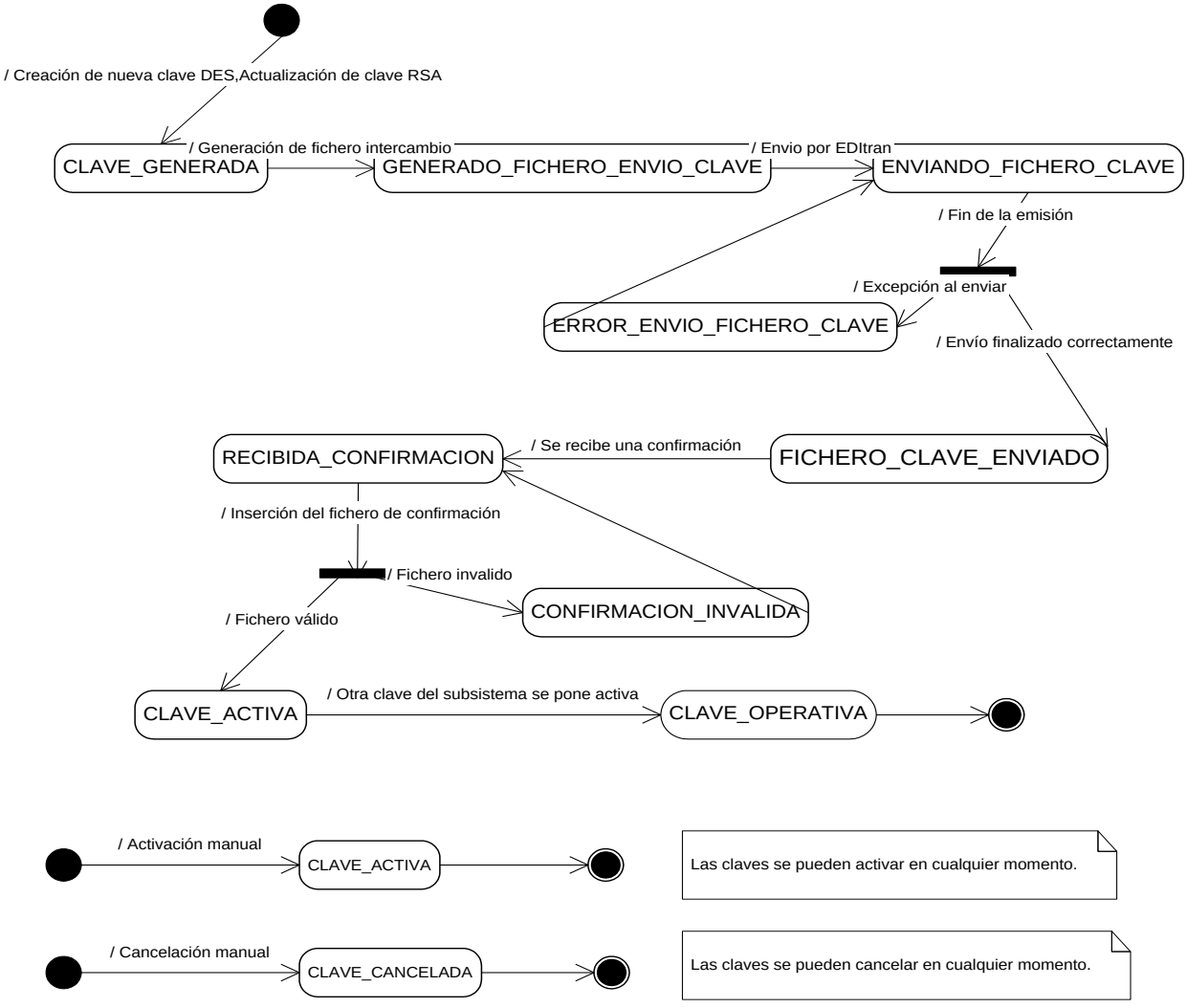
5.2.1. Clave Propia RSA

Diagrama de secuencia de estados para una clave de un Subsistema propio RSA:



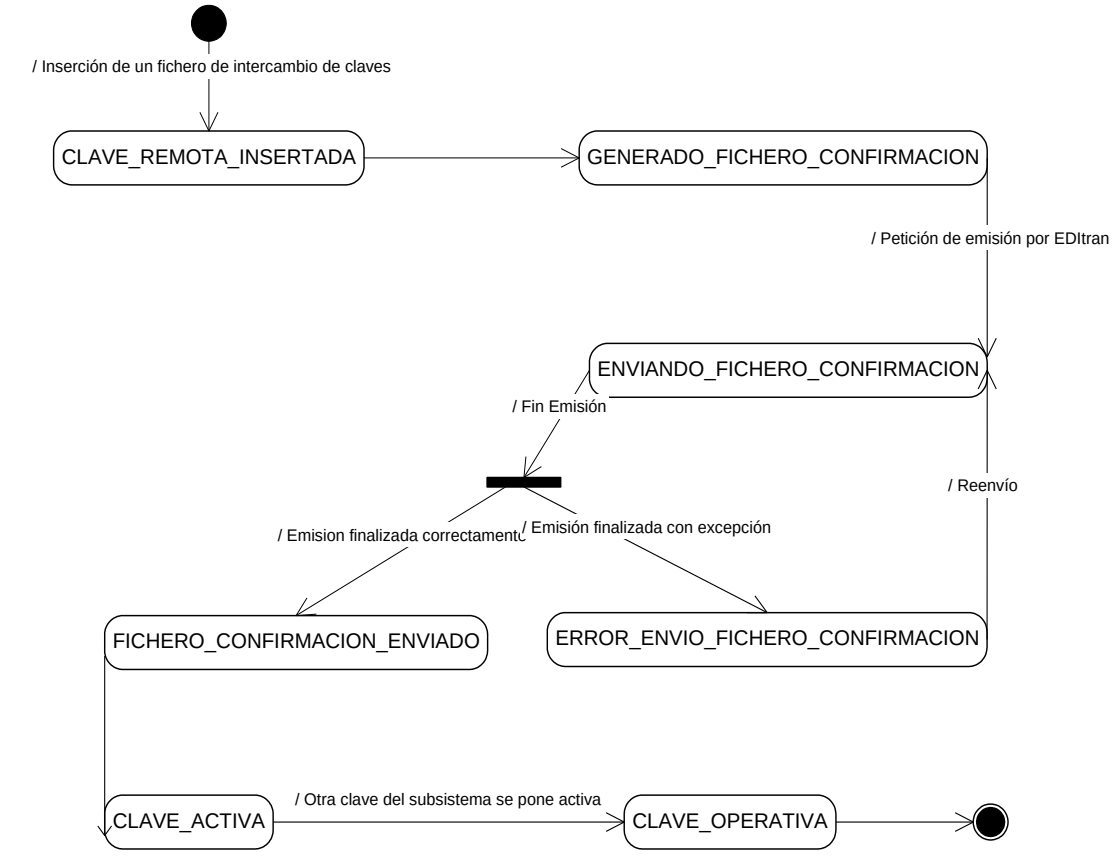
5.2.2. Clave Local

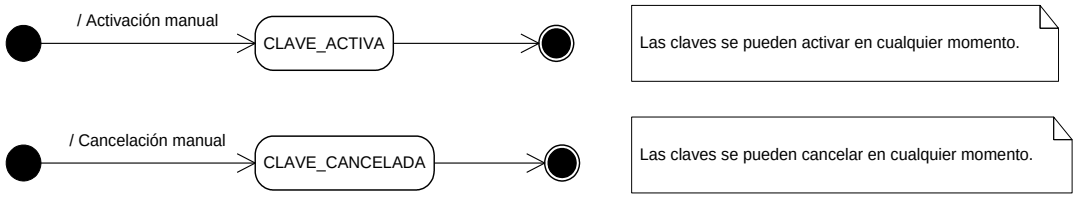
Diagrama de secuencia de estados para una clave Local RSA:



5.2.3. Clave Remota

Diagrama de secuencia de estados para una clave Remota RSA:





minsait

An Indra company

Contacto
editran@indra.es
T +34 91 480 80 80

Avda. de Bruselas 35
28108 Alcobendas,
Madrid, España
T +34 91 480 50 00
F +34 91 480 50 80

www.minsait.com