

minsaït

An Indra company

EDITRAN/P

Interfaz Genérica de Aplicación
Windows/Unix
Manual de Usuario

mayo de 2019



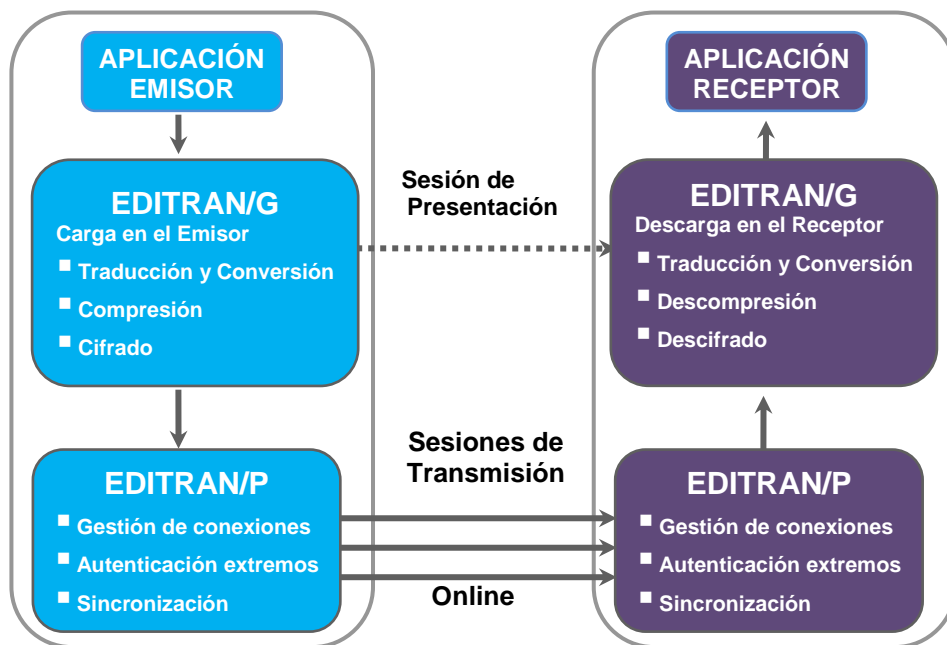
1. INTRODUCCION	1-1
2. DESCRIPCION	2-1
2.1. FUNCIONES.....	2-1
2.1.1. EDITRAN V2.0.....	2-1
2.1.2. EDITRAN V2.1.....	2-1
2.1.3. EDITRAN V2.2.....	2-2
2.1.4. EDITRAN V3.0.....	2-2
2.1.5. EDITRAN V3.1.....	2-2
2.1.6. EDITRAN V4.0.....	2-2
2.1.7. EDITRAN V4.1.....	2-2
2.1.8. EDITRAN V5.0.....	2-3
2.1.9. EDITRAN V5.1.....	2-3
2.2. TAMPONES DE EMISIÓN Y DE RECEPCIÓN	2-4
3. GESTOR DE EDITRAN/P (UNIX/LINUX).	3-1
3.1. DESCRIPCIÓN DE LA INTERFASE DE USUARIO.	3-1
3.1.1. PANTALLAS.....	3-1
3.1.2. AYUDA.....	3-2
3.1.3. TECLAS	3-2
3.2. OPERADOR DE EDITRAN/P.	3-3
3.2.1. Consulta de sesiones.....	3-3
3.2.2. Petición de conexión.....	3-4
3.2.3. Petición de liberación.....	3-4
3.2.4. Petición de emisión.....	3-4
3.2.5. Petición de recepción.....	3-4
3.2.6. Fin de emisión.....	3-4
3.2.7. Fin de recepción.....	3-4
3.2.8. Mensaje para el operador remoto.....	3-4
3.2.9. Consulta del fichero de emisión remoto.....	3-5
3.2.10. Consulta del fichero de recepción remoto.....	3-5
3.3. CONSULTA DE FICHEROS.	3-6
3.3.1. Consulta del registro de emisión / recepción.....	3-6
3.3.2. Consulta del fichero de log.....	3-7
3.3.3. Consulta genérica de sesiones.....	3-8
3.4. ADMINISTRADOR DE EDITRAN/P.	3-9
3.4.1. Entorno Local.....	3-9
3.4.2. Sesiones.....	3-10
4. ANEXOS	4-18
4.1. COMPONENTES DE EDITRAN	4-18
4.1.1. ESQUEMA ACTUAL.....	4-18
4.2. DISTRIBUCIÓN	4-19
4.2.1. Componentes.....	4-19
4.2.2. Servidores EDITRAN/P y EDITRAN/G	4-19
4.2.3. Clientes.....	4-20
4.2.4. Servidores de comunicaciones.....	4-20
4.3. COMANDOS	4-20
4.3.1. EDItran	4-20
4.3.2. editranp.....	4-20
4.3.3. editcp.....	4-20
4.3.4. makelog.....	4-20
4.3.5. menup	4-21
4.3.6. menucmd	4-21
4.3.7. copycfg	4-21
4.3.8. printcfg.....	4-22
4.3.9. resetkey	4-22
4.3.10. importkey.....	4-23
4.3.11. printlog	4-23
4.3.12. FILTRO NL	4-24
4.3.13. ediperfi	4-24
4.4. FICHEROS.....	4-25
4.4.1. Subdirectorío CFG	4-25
4.4.1.1. editranp.cfg.....	4-25

4.4.1.2.	editranp.sdx.....	4-25
4.4.2.	Subdirectorio BIN.....	4-25
4.4.2.1.	ckds.des.....	4-25
4.4.2.2.	editranp.log.....	4-25
4.4.2.3.	editranp.msg.....	4-25
4.4.2.4.	licencia.dat.....	4-25
4.4.2.5.	licencia.publick.....	4-25
4.4.3.	Subdirectorio LOG.....	4-25
4.4.3.1.	editranp.out.....	4-25
4.5.	CÓDIGOS Y MENSAJES AL OPERADOR.....	4-25
4.6.	MENSAJES DE LIBERACION EN EDITRAN.....	4-31
4.6.1.	CAUSAS Y DIAGNOSTICOS EDITRAN.....	4-31
4.6.2.	CONDICIONES DE REINTENTOS DE CONEXION.....	4-32
4.7.	SISTEMA DE CRIPTOGRAFÍA DE EDITRAN.....	4-32
4.7.1.	Introducción.....	4-32
4.7.2.	Tipos de claves.....	4-32
4.7.3.	Errores de Criptografía.....	4-33

1. INTRODUCCION.

La plataforma EDITRAN de Indra se articula en dos componentes indispensables:

- ❑ Plataforma de Comunicaciones (EDITRAN/P).
Incluye todos los servicios comunes directamente relacionados con las facilidades de la comunicación (protocolo, interfaces con los servicios de transmisión TCP, redes locales, etc.).
- ❑ Módulo Genérico de Interfaces de Aplicación (EDITRAN/G).
Aísla los servicios de comunicaciones proporcionados por EDITRAN/P de las aplicaciones usuarias, siendo el nexo de unión entre las mismas y los procesos de transmisión.



2. DESCRIPCION

EDITRAN transmite ficheros, con una estructura determinada, de un extremo local a uno remoto. Estos ficheros se denominan tampones de emisión y recepción.

Para obtener tampones de emisión a partir de ficheros convencionales de aplicación y por contra, obtener estos ficheros de aplicación a partir de tampones de recepción, se hace necesario el uso de programas de carga y descarga que, en conjunto, se pueden denominar como interfaz de aplicación.

Estas interfaces pueden variar mucho en funcionalidad y posibilidades, desde el tratamiento de un fichero concreto y determinado al de cualquier tipo de fichero. En este último caso se tendría una interfaz genérica de aplicación.

La Interfaz Genérica de Aplicación actual, en adelante EDITRAN/G, se ha desarrollado con el doble objetivo de incrementar grandemente las funcionalidades de las interfaces existentes, y al tiempo ser compatible con las anteriores, de manera que una entidad que instale la última versión de EDITRAN/G podrá:

- Prescindir de las interfaces anteriores.
- Intercambiar datos con entidades que tengan EDITRAN/G con versión anterior, en modo compatibilidad con esa versión.
- Intercambiar datos con entidades que tengan la misma versión de EDITRAN/G, tanto en modo compatible (misma funcionalidad que las interfaces anteriores con mejoras en el proceso), como en modo nativo (funcionalidades extendidas).

2.1. FUNCIONES

Se expone aquí la evolución de las funciones de presentación y de aplicación, opcionales, en las diferentes versiones de EDITRAN.

2.1.1. EDITRAN V2.0.

- Control de totales. Opción que ha sido muy poco empleada, y que consiste en que en cada bloque de emisión se pone un campo numérico (normalmente un importe) correspondiente a los registros lógicos dentro del bloque. Se incluyen registros de totales por tramos de manera que se hace un sincronismo especial y el receptor comprueba que el total corresponde a la suma de los importes de detalle del tramo.
- Compresión. Tres o más caracteres repetidos se sustituyen por 3 antes de emitir. En recepción se efectúa la operación inversa.
- CRC. Se añade un código de redundancia cíclica en el mensaje en la emisión y se comprueba en recepción.

2.1.2. EDITRAN V2.1.

- Control de totales, compresión y CRC.
- Criptografía opcional. Interfaz con varios productos de criptografía hardware y software.
- Notificación de parámetros. Se añade al perfil de sesión la versión de EDITRAN remoto. Si es V2.1, el extremo llamante notifica al remoto los parámetros de sesión, criptografía, compresión, control de totales, CRC, longitud de transmisión, etc. (en un mensaje SAP) que el remoto verifica y acepta o rechaza. Si es V1.0 o V2.0, los dos extremos se tienen que poner de acuerdo en los parámetros empleados en la transmisión.

2.1.3. EDITRAN V2.2.

- Compresión, CRC y criptografía.
- Se sustituye el control de totales por el Sincronismo de Aplicación o Lotes, pues se entiende que las funciones de aplicación deben estar en las interfaces y no en EDITRAN, que por otra parte, cuenta con mecanismos suficientes para garantizar la integridad de la información.
- Aparece el Procedimiento de Interrupción de Transmisión, ejecutado por EDITRAN al interrumpirse una transmisión.
- La característica más reseñable de esta versión es el cambio de longitud de la identificación de la sesión que pasa de 6 a 12 caracteres.

2.1.4. EDITRAN V3.0.

- Ampliación códigos (NIF): Se incrementan los códigos de EDITRAN, que pasan de 6 dígitos numéricos a 9 dígitos, de los cuales el primero y el último son alfanuméricos y el resto numérico. Es decir formato N.I.F (Número de Identificación Fiscal).
- Multientorno, permite actuar a EDITRAN con diferentes identificaciones locales.

2.1.5. EDITRAN V3.1.

- Esta última versión tiene las mismas funcionalidades de EDITRAN 3.0, pero teniendo en cuenta el efecto 2.000. Incorporación de 4 cifras en las fechas (AÑO 2000).

2.1.6. EDITRAN V4.0.

- Incompatibilidad EDITRAN/P V2.2. Una característica importante de esta versión es que no es compatible con las versiones de EDITRAN/P inferiores a la 3.0. Las versiones de EDITRAN/G 2.1, 3.0 y 3.1 siguen siendo compatibles con EDITRAN/G 4.0.
- EDITRAN distribuido.
- Rotación de direcciones locales-remotas (x25, tcp).

2.1.7. EDITRAN V4.1.

- Indicación de la Versión de EDITRAN en el Administrador y Operador de EDITRAN.
- Incorporación del algoritmo Triple DES a la modalidad de criptografía 3.0 de EDITRAN.
- Incorporación del código origen en los datos de usuario de las conexiones por TCP/IP para posibilitar la definición de más de 10 subentornos por aplicación con un solo remoto.
- Control en el mensaje de solicitud de inicio de emisión (SCP), de la sincronización del contenido de los tampones Locales y Remotos.
- Traducción en recepción según perfil de la presentación.
- Incompatibilidad EDITRAN/G V1.0 y V2.0. Las versiones de EDITRAN/G 2.1, 3.0, 3.1 y 4.0 siguen siendo compatibles con EDITRAN/G 4.1.
- Nuevo parámetro para la validación de la dirección remota llamante.
- Incorporación de un nuevo módulo (opcional) para la gestión de las transmisiones (EDITRAN/GT, solo para Windows)
- Nueva funcionalidad en Windows para X25 con las placas EICON, que permite configurar la placa a utilizar, en caso de tener más de una, y el puerto de la placa si tuviera más de uno por placa.

2.1.8. EDITRAN V5.0.

- ❑ Ampliación en el número de líneas locales y remotas. Se ha ampliado de 3 a 6 el número de líneas ips de forma que ante caídas pueda haber más rutas alternativas.
- ❑ Actualización automática de versión. Se ha implementado un protocolo por el cual las entidades EDITRAN intercambian sus versiones. En caso de que ambos sean 5.0 o superior, actualizarán en los perfiles la versión a la mínima de ambos instalada.
- ❑ Validaciones antes de comenzar la recepción que evitan algunos problemas que se detectaban hasta ahora en la descarga posterior a la transmisión. En concreto se valida que la versión que carga es conocida y que si el fichero viene comprimido y/o cifrado hay licencia de uso.
- ❑ Incorporación de un nuevo módulo (opcional) para la transmisión de ficheros a través de la red SWIFT.
- ❑ Backup en tipos de conexión. Para cada sesión se define un protocolo de red principal, pero opcionalmente se pueden definir también otras redes que se utilizarán como backup para las conexiones que fallen.
- ❑ Se soportan ficheros de aplicación de tamaño superior a 2GBytes.

2.1.9. EDITRAN V5.1.

- ❑ El número máximo de transmisiones concurrentes es 500. El límite de sesiones concurrentes en versiones anteriores era 100. Se ha incrementado hasta 500 que será el nuevo valor por defecto para el campo "Número máximo de sesiones" del perfil local.
- ❑ Incompatibilidad con V3.1 Esta versión sólo podrá comunicar con entidades remotas que tengan instalado EDITRAN V4.0 como mínimo. Si la instalación de la versión 5.1 es una actualización de Software y se migran perfiles, siempre que aparezcan sesiones con versión inferior a 4.0 se darán de alta con la versión inferior posible (4.0).
- ❑ Control de actividad para las sesiones conectadas. El protocolo establece un nuevo Tout de inactividad que controla que si una sesión está conectada pero no hay tráfico de datos durante un tiempo dado se libera. El valor del timeout por defecto es de 600 s que el usuario puede modificar definiendo la variable de entorno EDI_TOUT_IDLE. Vencido el timeout, en el log queda registrada la liberación con el siguiente mensaje: "Liberación por Timeout de inactividad"
- ❑ Negociación de alfabeto en establecimiento de sesión. En la V5.1 se ha modificado el protocolo para que se negocie el alfabeto entre entidades siempre que sea posible quitando la responsabilidad al usuario de conocer ese dato de la instalación remota. Para mantener la compatibilidad con versiones 5.0 o inferiores se ha mantenido el campo alfabeto en el perfil de EDITRAN/P, pero hay que tener en cuenta que éste sólo se usa cuando la conexión es saliente. Si es la entidad remota la que llama, independientemente de la versión y del valor del campo, se acepta la conexión y se dialoga en su alfabeto.

2.2. TAMPONES DE EMISIÓN Y DE RECEPCIÓN

- Son los ficheros temporales utilizados por EDITRAN durante la emisión o recepción.
- Un fichero tampón contiene datos correspondientes a una única sesión de transmisión.
- La longitud del registro puede ser como máximo 9999. Cuando el extremo remoto es un HOST sólo es válido 4050.
- Los tampones están compuestos por:
 - Un primer registro de control con el nº de secuencia de la clave a ceros. Este registro contiene, entre otros, los datos siguientes y pueden afectar a una interfaz:
 - Nº de registros totales.
 - Nº de registros confirmados.
 - Indicador de emitido o recibido completo.
 - Indicador de disponibilidad para EDITRAN.
 - Nº de sesión de intercambio.
 - Varios registros de datos con número de secuencia de la clave correlativo desde 1 hasta el total de los intercambiados.

3.1.2. AYUDA

EDITRAN UNIX dispone de un sistema de ayuda sensible al contexto. De esta forma, cuando se pulsan las teclas **F1** ó **?** aparece una ventana con el texto de ayuda asociado al campo o pantalla donde se encuentre el cursor en ese momento.

3.1.3. TECLAS

En EDITRAN UNIX dentro del menú, pueden utilizarse las siguientes teclas:

F1, ?	Ayuda sensible al contexto.
F2	Introduce los valores por defecto del campo actual, siempre que sea posible.
F3	Finaliza la introducción de datos de la pantalla actual, validando todos los campos.
F4	Introduce los valores por defecto de toda la pantalla actual, siempre que sea posible.
F6	Realiza una salida al sistema operativo para ejecutar otros comandos (shell), dejando residente EDITRAN. Para volver a EDITRAN se debe ejecutar el comando de exit .
Intro	Finaliza la introducción de datos del campo presente, actualizando su valor. Si no se ha introducido ningún valor inserta el de la última petición.
Espacio	Selecciona el valor del campo dentro una lista de valores enumerados: A (o) B () C () o activa/desactiva el valor del campo de sólo dos valores posibles: D [X]
Esc	Aborta la introducción de datos y vuelve al menú anterior.
Borrar	Borra el carácter anterior al cursor
Tab	Avanza al siguiente campo sin actualizar o modificar el valor.
Flechas	Desplazan el cursor en la pantalla al siguiente/anterior campo o al siguiente/anterior valor dentro del campo.
PgUp Control-U	Retroceso de página.
PgDn Control-D	Avance de página.

3.2.2. Petición de conexión.

Para establecer manualmente la conexión física con un EDITRAN remoto y poder iniciar el proceso de transmisión, seleccionar la opción 2.- PETICION DE CONEXION del menú OPERADOR DE EDITRAN. La petición no está permitida cuando el modo de operación del EDITRAN local es Servidor.

Esta petición se genera automáticamente al solicitar una petición de emisión o recepción si se especifica el valor S en el parámetro LLAMADA AUTOMATICA del perfil de la sesión.

En el área de información aparecen indicaciones sobre el resultado de la petición (conexión realizada o no).

3.2.3. Petición de liberación.

Para poder liberar manualmente la conexión existente para una sesión seleccionar la opción 3.- PETICION DE LIBERACION del menú OPERADOR DE EDITRAN.

3.2.4. Petición de emisión.

Para iniciar la emisión local de un fichero seleccionar la opción 4.- PETICION DE EMISION del menú OPERADOR DE EDITRAN.

La petición no está permitida cuando el modo de operación de EDITRAN local es Servidor.

3.2.5. Petición de recepción.

Para iniciar la recepción de un fichero, que debe emitir el remoto, seleccionar la opción 5.- PETICION DE RECEPCION del menú OPERADOR DE EDITRAN.

No se acepta la petición cuando el modo de operación de EDITRAN local es Servidor.

3.2.6. Fin de emisión.

Para solicitar la petición de fin forzado de la emisión local (interrupción de emisión) seleccionar la opción 6.- FIN DE EMISION del menú OPERADOR DE EDITRAN.

No se acepta la petición cuando el modo de operación de EDITRAN local es Servidor.

3.2.7. Fin de recepción.

Para solicitar la petición de fin forzado de la recepción local (interrupción de recepción) seleccionar la opción 7.- FIN DE RECEPCION del menú OPERADOR DE EDITRAN.

No se acepta la petición cuando el modo de operación de EDITRAN local es Servidor.

3.2.8. Mensaje para el operador remoto.

Es necesario que exista conexión con el EDITRAN remoto destinatario del mensaje de operador.

Aparecerá la siguiente pantalla donde se escribirá el texto a enviar:

3.3.3. Consulta genérica de sesiones.

Se visualizan todas las sesiones definidas en el fichero de perfiles.

Para consultar dichos registros se seleccionará la opción 3.- CONSULTA GENERICA DE SESIONES del menú CONSULTA DE FICHEROS.

```
02/10/2017 - CONSULTA DE FICHEROS - EDITRAN/P V5.2.0 x
12:07:08 - CONSULTA GENERICA DE SESIONES - TCP x
xSESION NOMBRE REMOTO NOMB APLICACION RED x
xAIX-TCP-11 TCP 172.22.249.55 x
xAIX-TCP-12 TCP 172.22.249.55 x
xAIX-TCP-13 TCP 172.22.249.55 x
xAIX-TCP-14 TCP 172.22.249.55 x
xAIX-TELEGC TCP 172.22.249.55 x
xAIX-XADES TCP 172.22.249.55 x
xAS400-10000 TCP 172.22.249.68 x
xAS400-CF TCP 172.22.249.68 x
xAS400-FF TCP 172.22.249.68 x
xAS400-GIGA TCP 172.22.249.68 x
xAS400-TCP-00 TCP 172.22.249.91 x
xAS400-TCP-01 TCP 172.22.249.68 x
xAS400-TCP-02 TCP 172.22.249.68 x
xAS400-TCP-03 TCP 172.22.249.68 x
xAS400-TCP-04 TCP 172.22.249.68 x
PgUp Ctrl-U Pagina Anterior PgDn Ctrl-D Pagina Siguiente ESC Salir x
```


SENTIDO TRAFICO (E/R/X)

E Sólo se puede emitir en esta sesión.

R Sólo se puede recibir en esta sesión.

X Se puede emitir y recibir simultáneamente.

 LLAMADA AUTOMÁTICA (S/N)

S Se establecerá automáticamente la conexión al solicitarse el comienzo de emisión o recepción.

N Se ha de establecer una conexión previa a la solicitud de emisión/recepción.

 DESCONEXION AUTOMATICA (S/N)

S Se genera la petición de desconexión de forma automática al finalizar una emisión o una recepción.

N No se genera la desconexión de forma automática.

 TIME-OUT (Segundos)

Es el intervalo de tiempo, expresado en segundos, en el que EDITRAN espera recibir desde el remoto un mensaje de respuesta a uno de control enviado previamente.

Si concluido el tiempo TIME-OUT no se ha recibido una respuesta, se volverá a enviar la misma petición, iniciándose un nuevo intervalo de espera. Equivalente también para las peticiones de conexión.

 NRO. MÁXIMO REINTENTOS

Es el número de veces que se repiten los procedimientos de TIME-OUT anteriores.

 GUARDAR ROTACIONES (S/N)

S En caso de solicitud de llamada, cuando la conexión se acaba estableciendo por direcciones ips que no están en el perfil en la primera posición, se guardan en dicha posición. El propósito es que en posteriores transmisiones, la conexión se consiga sin reintentos de llamada.

N En ningún caso se actualizan las direcciones del perfil.

Una vez configurados los valores de red, aparece la pantalla en que se especifican los parámetros de sesión que determinan las características generales de la transmisión.

```

Lqaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
x  02/10/2017      - ADMINISTRADOR DE EDITran/P -            EDITRAN/P V5.2.0
x  12:25:18      - MODIFICACION SESION -                 TCP
x
x  SESION : IMS-TCP-01
x
x  - PARAMETROS SESION -
x  SERVIDOR/CLIENTE (OPER) : C                          CRC (S/N)           : S
x  COMPRESION (S/N/L/V)   : V                          ASCII/EBCDIC (A/E) : E
x  HORA INICIO (HH:MM:SS) : 00:00:00                   HORA FIN (HH:MM:SS): 00:00:00
x  LONGITUD TAMPON       : 4050                         RAFAGA EMISION     : 010
x  TOUT SINCRONIZACION  : 030
x
x  - NOMBRE DE PROCEDIMIENTOS -
x  PROCESOS EMISION      : EDITRAN/G
x  PROCESOS RECEPCION   : EDITRAN/G
x
x
x  F1  ? Ayuda On-Line      F2  Campo por defecto     F3  Fin entrada
x  F4  Pantalla por defecto F6  Shell OS                F5C Menu previo
x
Lqaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

```

☐ SERVIDOR/CLIENTE (OPER)

Modo de operación:
S No se pueden solicitar ni emisiones ni recepciones (servidor).
C Se pueden solicitar tanto emisiones como recepciones (cliente).

☐ CRC (S/N)

S Se generará el código de redundancia cíclica para cada mensaje transmitido; se validará el CRC de cada mensaje recibido.
N No se calcula el CRC para mensajes salientes ni se valida en mensajes entrantes.

☐ COMPRESIÓN (S/N/V)

S Transmisión comprimida de los datos.
N Los datos se transmiten en el formato original de la aplicación.
V Los datos se transmiten comprimidos o en el formato original dependiendo del mejor resultado obtenido.

☐ ASCII/EBCDIC (A/E)

A El remoto utiliza alfabeto ASCII (entornos Unix y Windows).
E El remoto utiliza alfabeto EBCDIC (entornos CICS, IMS e iSeries).

☐ HORA INICIO (HH:MM:SS)

Especifica la hora del día a partir de la cual se podrá iniciar la transmisión, expresada en horas (HH), minutos (MM) y segundos (SS).

☐ HORA FIN (HH:MM:SS)

Especifica la hora del día límite hasta la cual se puede iniciar la transmisión, expresada en horas (HH), minutos (MM) y segundos (SS).

N Si no desea utilizar la Criptografía EDITRAN/P.

VERSION CRIPTOGRAFÍA

Este campo es obligatorio si la Criptografía está activada.

2.2 Para el subsistema de seguridad de la versión 2.2 de EDITRAN/P.

3.0 Criptografía compatible con CRIPTO/lib V3.0.

4.0 Cifrado AES y claves RSA de 2048 y 4096.

CAMBIO DE CLAVE V2.2 (S/N)

Selector de facilidad de cambio de clave criptográfica en el preámbulo de conexión. Solo afecta cuando la versión de criptografía es 2.2.

S Cambio de clave activada.

N Cambio de clave inhibida.

GESTION DE CLAVES V3.0

Cuando en versiones de criptografía 3.0 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 autenticar a los extremos. Es obligatorio si existe algoritmo de confidencialidad.

DES si desea autenticar los extremos con algoritmo DES (valido con versiones de criptografía 2.2 y 3.0).

RSA si desea autenticar 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 superior y hay autenticación.

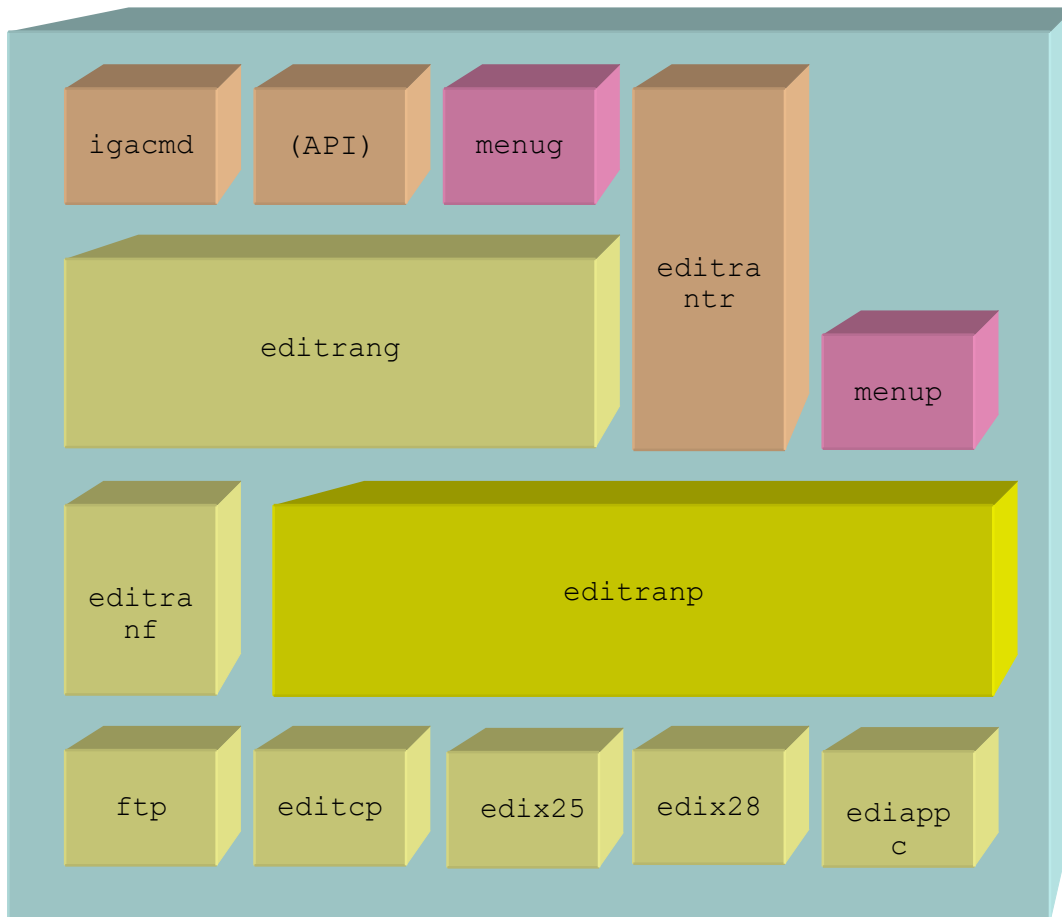
CLAVE REMOTA

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

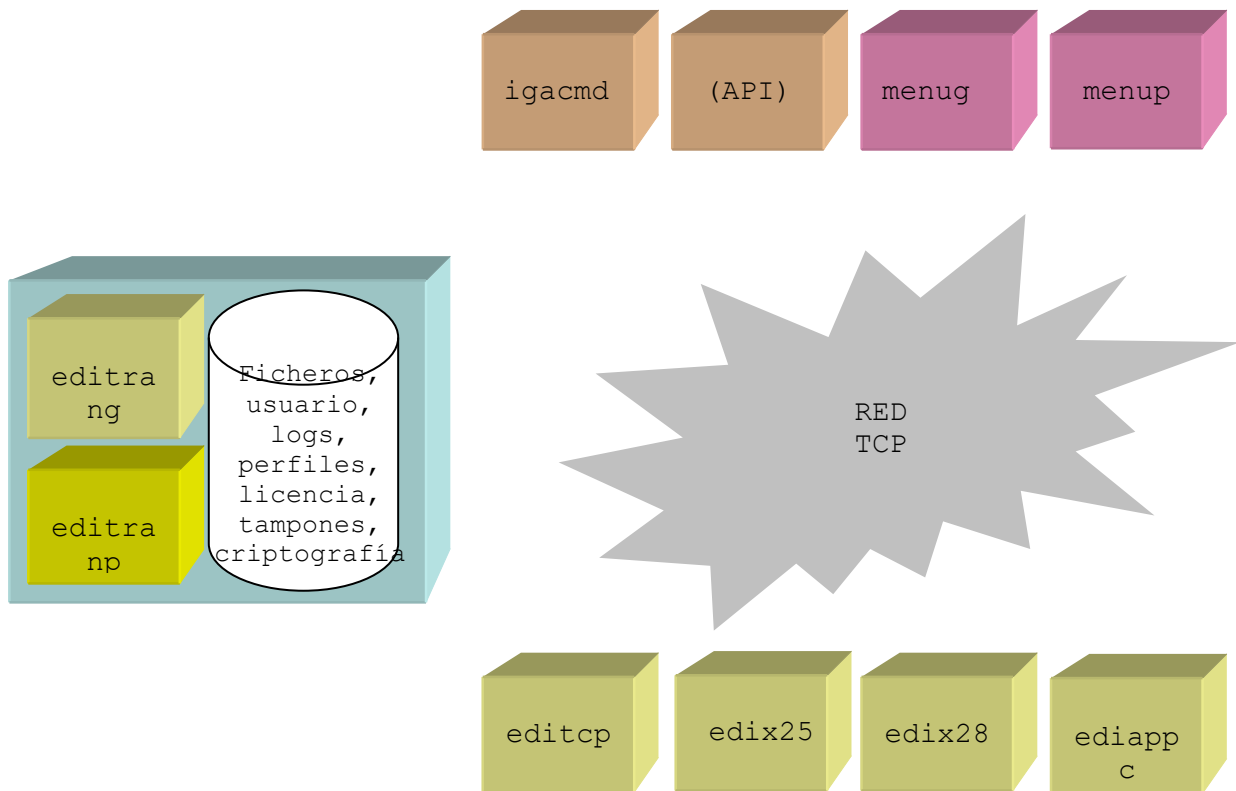
4. ANEXOS

4.1. COMPONENTES DE EDITRAN

4.1.1. ESQUEMA ACTUAL



4.2. DISTRIBUCIÓN



4.2.1. Componentes

Como se representa en la figura anterior se pueden distinguir tres tipos de componentes:

- Servidores P y G.
- Clientes
- Comunicaciones

Todos los componentes utilizan la comunicación TCP para dialogar entre sí, independientemente de si están o no en la misma máquina.

Pueden dialogar componentes independientemente de la plataforma en la que se ejecuten.

4.2.2. Servidores EDITRAN/P y EDITRAN/G

Sus funcionalidades y ficheros asociados son:

- Scripts de usuario
- Conversores + directorios origen/destino
- Perfiles de presentaciones y sesiones
- Criptografía, compresión, transformación, etc.
- Log/salida/traza/alarmas
- Ficheros de usuario, CSB y tampones

4.2.3. Clientes

- Acceso a métodos del servidor - operación.
- Acceso a los ficheros asociados a los servidores - consulta.
- Acceso a los perfiles - administración.

4.2.4. Servidores de comunicaciones

- Permiten al servidor EDITRAN/P acceder a las redes soportadas.
- Acceden a la configuración local de EDITRAN/P.

4.3. COMANDOS

4.3.1. EDItran

Es el programa que arranca y detiene el sistema EDITRAN.

Sintaxis

La sintaxis del comando es:

EDItran [-t] [-f] start | stop | status [-s]

-t Arranca EDITRAN con traza

-f Ignora otro EDITRAN arrancado

-s Sólo para Windows. Utilizar esta opción si no se desea que se muestre la ventana con el resultado del comando.

start Arranca el sistema EDITRAN

stop Detiene el sistema EDITRAN

status Obtiene el estado del sistema EDITRAN

4.3.2. editranp

Proceso principal del sistema EDITRAN. Se encarga de dialogar con los diferentes procesos de comunicaciones y con el EDITRAN/G. Se lanza en background al arrancar el sistema EDITRAN.

4.3.3. editcp

Proceso de comunicaciones cuando el protocolo a utilizar para la conexión es TCP/IP.

4.3.4. makelog

Crea un fichero de eventos llamado editran.log que contendrá un resumen de las operaciones efectuadas mediante EDITRAN.

Sintaxis

La sintaxis del comando es:

makelog -n N

donde **N** es el número máximo de entradas (número de eventos) que se desea conservar en el fichero.

Ejemplo

Se desea crear un fichero de eventos, editran.log, con una capacidad para 500 entradas distintas.

Se ha de ejecutar el comando:

```
makelog -n 500
```

4.3.5. menup

Permite acceder de forma directa al menú del gestor de EDITRAN.

4.3.6. menucmd

Establece un mecanismo de comunicación entre aplicaciones o programas de usuario y EDITRAN/P, permitiendo invocar operaciones de forma desatendida y automática.

Sintaxis

La sintaxis del comando es:

```
menucmd s sesion x
```

donde **s** es la señal enviada para solicitar una operación al EDITRAN, **sesión** es la sesión y **x** otras opciones que dependen del tipo de operación o señal solicitada al EDITRAN.

En concreto, la sintaxis exacta del comando dependiendo del valor de **s** es la siguiente:

```
menucmd {E00|E11} <sesion#>  
menucmd EOP <sesion#> <texto>
```

Las señales posibles son:

E00 solicita a EDITRAN una petición de conexión.
E11 solicita a EDITRAN una petición de liberación.
EOP solicita a EDITRAN el envío de un mensaje al operador remoto.

4.3.7. copycfg

Utilidad para copiar perfiles de EDITRAN a partir de otro utilizado como plantilla.

Sintaxis

La sintaxis del comando es:

```
Uso: copycfg -s ses_origen [-d ses_destino] [-n] [-r cod_remoto] [-p | -a]
```

Siendo:

```
-n      : numero de sesiones a crear.  
-s      : sesion origen.  
-d      : sesion destino.  
-r      : codigo remoto destino.  
-p      : solo copia sesiones EDITRAN/P  
-a      : crea aplicaciones EDITRAN/G
```

Este comando permite dar de alta perfiles de EDITRAN partiendo de una sesión tomada como plantilla. La sesión origen se da en la opción **-s**. Por defecto se crea la Sesión de EDITRAN/P y su correspondiente Presentación en EDITRAN/G, pero este comportamiento puede cambiarse mediante la opción **-p** si se quieren crear sólo los perfiles de sesión.

Los perfiles creados dependerán de la opción elegida:

Opción -n <n>: Se dan de alta <n> sesiones. Dichas sesiones se nombran igual que la original añadiendo un índice. Por ejemplo, si partimos de PRUEBA y queremos generar 5 más, se crearán desde PRUEBA-1 hasta PRUEBA-5.

Opción -d: En este caso el usuario decide el nombre que tendrá la sesión creada pero esta opción es incompatible con la anterior.

Opción -r: Por defecto las sesiones creadas se generan con el mismo código local y remoto que la original. Con esta opción se permite al usuario cambiar el código remoto del nuevo perfil.

Ejemplo

Para duplicar la sesión INDRA-TEST para otro remoto diferente nombrando la nueva como EDITRAN-TEST, ejecutar:

```
>copycfg -s INDRA-TEST -d EDITRAN-TEST -r 000001230
```

Para crear 10 sesiones partiendo de PRUEBA, ejecutar:

```
>copycfg -s PRUEBA -n 10
```

4.3.8. printcfg

Utilidad de impresión de sesiones EDITRAN.

Sintaxis

```
Uso : printcfg [ -lgrapsv ]
Siendo :
  -l : Local EDITRAN/G.
  -g : Presentaciones EDITRAN/G.
  -r : Remotos EDITRAN/G.
  -a : Aplicaciones EDITRAN/G.
  -p : Local EDITRAN/P.
  -s : Sesiones EDITRAN/P. (Defecto)
  -v : Imprime cabeceras.
```

Ejemplo

SESION	LOCAL	REMOTO	APLIC	DIR LOCAL	DIR REMOTA
INDRA-TEST	W00005100	000099990	PRUEBA	TCP	editran.indra.es

4.3.9. resetkey

Reinicia las claves de intercambio cifradas de una sesión determinada.

Ha de ser utilizado con mucha precaución, puesto que deja las claves en un estado diferente al original. Es imprescindible realizar la misma operación en el extremo remoto para que sea posible una sincronización en el intercambio de claves.

Sólo debe ejecutarse si es la primera vez que se hace uso de las claves, o si se han perdido las claves del último intercambio en el fichero de perfiles.

Sintaxis

La sintaxis del comando es:

resetkey [sesión]

donde sesión es la sesión de EDITRAN/P. Se debe escribir en mayúsculas, y si tiene algún espacio, entre comillas dobles: "

Ejemplo

En una instalación se desea poner a un valor inicial la clave de la sesión TEST-INDRA.

Se ha de ejecutar el comando:

```
resetkey TEST-INDRA
```

4.3.10. importkey

El fichero *ckds.des* mantiene la clave maestra y claves auxiliares DES en el sistema EDITRAN. En la versión 5.02 el formato ha cambiado para poder almacenar claves simples y dobles. Por ello, en algunos casos puede ser necesario importar claves que procedan de versiones anteriores.

Por seguridad, para exportar las claves el usuario debe conocer el valor de la HMK que guarda y debe proporcionar los dos primeros octetos en hexadecimal como password de acceso al fichero. Se puede dar como argumento del comando, pero si no se pone se le pedirá al usuario.

Sintaxis

La sintaxis del comando es:

```
Uso: importkey [ -s ] [-k<k>] -f<f> [--] [etiquetas]
-- : Fin de opciones. El resto de argumentos son etiquetas
-s : El fichero origen contiene claves simples
-k<k> : Clave de acceso al fichero (HMK)
-f<f> : Fichero que almacena las claves a exportar
etiquetas: Etiquetas de las claves a importar
```

Si no se da ninguna etiqueta, el comando incorpora todas las claves del fichero origen cuya etiqueta no sea SI0000000000XX.

Si la etiqueta de la clave a importar ya existe en el fichero destino, la clave se actualizará con el valor de la antigua.

Ejemplo

Para incorporar la clave auxiliar usada por EDITRAN para sesiones con criptografía 2.2 ha de ejecutar el comando:

```
> importkey -s -fckds.des.v510 SI000000000016
```

Para incorporar las claves auxiliares de usuario dando la password de acceso como argumento, ejecutar:

```
> importkey -s -fckds.des.v510 -kA1A3
```

4.3.11. printlog

Utilidad de impresión del log de EDITRAN.

Sintaxis

printlog

Opciones del comando:

```
-P Log de EDITRAN/P
-G Log de EDITRAN/G
-s sesion
-f fecha DDMMAAAA
-h hora HHMMSS
Todos los parametros son opcionales
```

4.3.12.FILTRO nl

El filtro **nl** se utiliza para convertir líneas de un sistema a otro. Dicho filtro se limita a leer y escribir líneas. La utilidad del filtro radica en la diferencia física entre unos sistemas y otros al representar líneas de texto.

En general, un fichero conteniendo líneas se estructura de una de dos formas:

Con registros de longitud fija (se guardan siempre un número fijo de caracteres por cada línea; por ejemplo, 100 caracteres para cada línea).

Con registros de longitud variable (se utilizan delimitadores de fin de línea para separar las líneas). Estos a su vez tienen separadores distintos en cada sistema. El filtro conoce los de UNIX.

Para utilizar el filtro basta decirle cual es la estructura de partida (por ej. registros fijos de 50 caracteres, o registros variables con delimitador tipo UNIX) y la estructura que deseamos obtener. El filtro cambiará la estructura del fichero para obtener la estructura deseada con el mismo contenido en cada línea.

Sintáxis

```
Uso: nl [ -<#> | -v ] -i<f> -o<f> [--] [ficheros]
  -- : Fin de opciones. El resto de argumentos son ficheros
  -<#>: Registros de longitud # (fija) sin contar delimitadores (Ej.: -80)
  -v : Registros de longitud variable (por defecto)
  -i<f>: Formato de entrada (Ej.: -id)
  -o<f>: Formato de salida (Ej.: -on)
       <f> puede ser: u (UNIX), d (MSDOS), n (ningun delimitador)
ficheros: Ficheros a traducir (stdin->stdout por defecto)
```

Para indicarle el tipo de registro que vamos a utilizar (fijos o variables) utilizamos las siguientes opciones:

opcion -N (donde N es un número, ej. 80): registros fijos de N caracteres.

opcion -v: registros variables.

Para indicar el delimitador de fin de línea utilizado en el fichero de entrada se utiliza la **opcion -iX** (donde X es 'n', 'u' o 'd').

Si X es n el filtro espera que no haya delimitador de fin de línea en el fichero de entrada (en este caso deberá haberse utilizado -N para indicar la longitud del registro puesto que ha de ser de registros de longitud fija).

Si X es u el filtro espera que haya un '\n' delimitando cada registro. (tipo unix).

Si X es d el filtro espera que haya un '\r\n' delimitando cada registro. (tipo MSDOS).

Para indicar el delimitador de fin de línea a utilizar en el fichero de salida se utiliza la **opcion -oX** (donde X es 'n', 'u' o 'd').

Si X es n el filtro no escribe ningun delimitador tras cada línea.

Si X es u el filtro escribe un '\n' tras cada registro.

Si X es d el filtro escribe un '\r\n' tras cada registro.

4.3.13. ediperfi

Es el comando para la administración de los perfiles de EDITRAN/P.

Puede consultar el manual de usuario *EDITRAN/GP Gestión de Perfiles* para ampliar información sobre esta utilidad.

4.4. FICHEROS

4.4.1. Subdirectorío CFG

4.4.1.1. editranp.cfg

Fichero de configuración de EDITRAN. Almacena el perfil local y los perfiles de las sesiones para entidades remotas. Utilizado exclusivamente por EDITRAN.

4.4.1.2. editranp.sdx

Fichero de índice de configuraciones de EDITRAN. Utilizado exclusivamente por EDITRAN.

4.4.2. Subdirectorío BIN

4.4.2.1. ckds.des

Fichero donde se encuentran las claves Auxiliares de intercambio de las sesiones EDITRAN cifradas.

4.4.2.2. editranp.log

Fichero creado por el comando **makelog**. Almacena de forma cíclica el resumen de las operaciones realizadas por EDITRAN, por lo que una vez alcanzado el número máximo de entradas sobre escribe la más antigua.

Puede consultarse desde los menús de EDITRAN y mediante el comando **printlog**.

4.4.2.3. editranp.msg

Fichero donde están almacenados los mensajes que EDITRAN presenta al operador de EDITRAN. Utilizado exclusivamente por EDITRAN.

4.4.2.4. licencia.dat

Fichero de licencia de EDITRAN. Se verifica siempre antes de iniciar los procesos de comunicaciones de EDITRAN. Si no existe este fichero o su contenido es alterado, no se podrán ejecutar los procesos de EDITRAN.

4.4.2.5. licencia.publick

Fichero con la clave pública entregada por Indra para la verificación de la licencia. Al igual que el fichero licencia.dat no debe ser manipulado.

4.4.3. Subdirectorío LOG

4.4.3.1. editranp.out

Fichero donde se registran todas las salidas producidas por el proceso **editranp** y los procedimientos y comandos que este proceso lanza. Es generado por la redirección de la salida estándar del proceso **editranp**.

4.5. CÓDIGOS Y MENSAJES AL OPERADOR

Estos códigos son los que quedan reflejados en el fichero **editranp.log** para indicar los distintos estados por los que pasa una sesión. En la pantalla del operador de EDITRAN/P, aparecen en forma de mensajes.

Seguidamente, se listan los mensajes dando una breve explicación o acción recomendada, según corresponda:

MENSAJE	EXPLICACIÓN/ACCIÓN RECOMENDADA
Asociación establecida	Petición de asociación local aceptada por extremo remoto.
Asociación remota aceptada	Asociación entre aplicaciones aceptada por el extremo local.
Comienzo de la transmisión	Se inicia la emisión al remoto.
Conexión realizada	Se ha establecido un circuito con el remoto.
Conexión remota rechazada (Perfiles)	Discrepancia en los perfiles del remoto y el local.
Consulta de estado	Respuesta a una consulta de la situación de una sesión.
Consulta del fichero emisor remoto	Se ha pedido la consulta del registro de control del fichero tampón de emisión remoto.
Consulta del fichero receptor remoto	Se ha pedido la consulta del registro de control del fichero tampón de recepción remoto.
Descuadre totales en proceso emisor	En aplicaciones con control de totales no coinciden los totales confirmados intercambiados (sincronismo).
Descuadre totales en proceso receptor	En aplicaciones con control de totales no coinciden los totales confirmados intercambiados (sincronismo).
Emisión abortada	Se ha abortado la emisión de un fichero al remoto.
Emisión correcta y finalizada	Ha finalizado una emisión correctamente.
Emisión local	Inicio de la emisión local de un fichero.
Error al abrir fichero	Se ha producido un error al abrir un fichero.
Error al cerrar fichero	Se ha producido un error al cerrar un fichero.
Error al escribir fichero	Se ha producido un error al escribir en un fichero.
Error al leer fichero	Se ha producido un error al leer de un fichero.
Error en la ejecución del <i>SCRIPT</i>	Se ha producido un error en la ejecución de un shell script.
Error en proceso batch remoto	Se ha producido un error en la ejecución de un shell script remoto.
Error general en la interfase	Se ha producido un error en la ejecución de un shell script.
Error remoto de criptografía (ERR##)	Se ha producido un error de criptografía. Consultar apartado 4.7.3 Errores de Criptografía..
Error remoto en compresión/descompresión	Se ha producido un error de compresión/descompresión en el extremo remoto.
Agotados reintentos de conexión	Se han agotado los reintentos de conexión, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN.
Agotados reintentos de sincronismo	Se han agotado los reintentos de sincronismo, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN.
Agotados reintentos en proceso emisor	Se han agotado los reintentos en el proceso emisor de mensajes que requieren respuesta.
Agotados reintentos en proceso receptor	Se han agotado los reintentos en el proceso receptor de mensajes que requieren respuesta.
Agotados reintentos para emitir	Se han agotado los reintentos de inicio de emisión, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN.
Agotados reintentos para establecer sesión	Se han agotado los reintentos de establecimiento de sesión, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN.
Agotados reintentos para fin de emisión	Se han agotado los reintentos de fin de emisión, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN.
Agotados reintentos para recibir	Se han agotado los reintentos de inicio de emisión, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN.
Existe conexión. Se ignora petición batch	Se ha solicitado una petición de conexión y está ya existe.
Extremo llamante inválido (perfiles)	Incompatibilidad en los valores de dicho campo en el registro de perfiles.
Fichero de perfiles vacío o no existe	Se ha producido un error al acceder al fichero de perfiles de EDITRAN.
Fichero de recepción no preparado	La información del registro de control intercambiada entre los dos extremos, en el mensaje de petición/respuesta de inicio de transmisión, no permite iniciar el intercambio de datos. No coincide el número de sesión de intercambio contenida en los registros de control. El fichero de emisión/recepción no está cargado, o no está disponible para EDITRAN (se desencadena el proceso batch que se especifique en perfiles).
Fichero tampón de emisión no preparado	Respuesta a consulta de fichero remoto.
Ficheros tampones en situación no compatible	El remoto rechaza la petición local por no tener su fichero tampón preparado. Posiblemente ha lanzado su automatismo previo correspondiente a la petición.
Fin de emisión pedida por operador	Cuando el operador solicita fin de emisión forzada.
Fin de emisión pedida por operador remoto	Cuando el operador remoto solicita fin de emisión forzada.
Fin de recepción pedida por operador	Cuando el operador solicita fin de recepción forzada.
Fin de recepción pedida por operador remoto	Fin de la transmisión solicitada por el operador remoto.
Fin de transmisión local pedido por el remoto	Cuando remoto solicita fin de recepción (fin de transmisión local).

Imposibilidad de emisión remota debido a perfiles	Revisar procesos definidos en perfil de sesión.
Imposibilidad de recepción remota debido a perfiles	Revisar procesos definidos en perfil de sesión.
Inicio de recepción	Cuando comienza la recepción del fichero remoto.
Liberación de aplicación remota	Se ha liberado la conexión por la aplicación remota.
Liberación de la transmisión XX XX	Mensaje de liberación de un circuito.
Liberación del operador remoto	Se produce como consecuencia de una petición de liberación por el operador remoto.
Liberación por cruce de llamadas	Hay un cruce de llamadas entre el remoto y el local y solo acepta una.
Liberación por el operador	Se produce como consecuencia de una petición de liberación por el operador.
Liberación por error de compresión	Se solicita liberación al producirse un error en la compresión/descompresión de algún mensaje.
Liberación por existir otro canal establecido	Se libera un circuito por existir otro conectado para una sesión determinada.
Liberación por facilidades invalidas	Se comprobará que tipo de facilidades se utilizan al solicitar la conexión. EDITRAN sólo gestionará la utilización de cobro revertido.
Liberación por horario incorrecto	Comprobar en perfil de sesión el horario dado de alta y modificarlo.
Liberación por no aceptar cobro revertido	Comprobar en perfil de sesión el campo COBRO REVERTIDO .
Liberación por no existir canales libres	Limitación de circuitos. Se podrá establecer la conexión cuando libere otra sesión establecida.
Liberación por rearranque de red	Se ha producido una liberación de circuito por rearranque de red.
Liberación por tipo pago invalido (perfiles)	Comprobar FORMA DE PAGO de sesión en previsión de conflictos. Algún extremo deberá soportar coste.
Llamada rechazada (hora invalida)	Petición de conexión fuera de horario. Revisar perfiles.
Llamada rechazada dirección remota invalida (perfiles)	Comprobar NRI/IP del remoto de la sesión en perfiles.
Llamada remota aceptada	Petición de conexión del remoto ha sido aceptada. Se establece la conexión.
Llamada remota aceptada (cruce)	Ambos extremos han pedido el establecimiento de conexión y se ha gestionado primero la local.
Llamada remota rechazada (cobro revertido)	No coincide la especificación para dicho parámetro en ambos extremos.
Llamada remota rechazada (cruce)	Se rechaza la llamada entrante del remoto.
Llamada remota rechazada (extremo llamante)	No coincide la especificación para dicho parámetro en ambos extremos.
Llamada remota rechazada (tipo pago)	No coincide la especificación para dicho parámetro en ambos extremos.
Local no puede emitir (perfiles)	Petición de emisión rechazada por no especificarse parámetro SENTIDO TRAFICO con valor E o X o por no tener la licencia adecuada.
Local no puede llamar (perfiles)	Petición de conexión rechazada por especificar en parámetro EXTREMO LLAMANTE R , de modo que sólo puede llamar el remoto.
Local no puede recibir (perfiles)	Revisar el parámetro SENTIDO DE TRAFICO y licencia para sentido.
Mensaje de notificación incorrecto	Se ha producido un error en el establecimiento de la sesión debido al formato del mensaje de notificación.
No existe conexión	Se ha hecho una petición que requería previamente el establecimiento de conexión.
No existe sesión en perfiles	Dar de alta la sesión en perfiles.
No hay recursos disponibles	Se podrá establecer la conexión una vez que se haya liberado otra ya establecida. Esto es debido, a la limitación de circuitos físicos de entorno local.
No hay servicio de red	El extremo local no tiene servicio X.25.
No hay sesión	La petición requiere la existencia de una conexión entre aplicaciones.
No se lanza batch posterior a emisión	Se ha recibido una petición batch de emisión, que no será procesada, por estar emitiendo.
No se lanza batch posterior a recepción	Se ha recibido una petición batch de recepción, que no será procesada, por estar recibiendo.
No se lanza batch previo a emisión	Se ha recibido una petición batch de recepción, que no será procesada, por estar recibiendo.
No se lanza batch previo a recepción	Se ha recibido una petición batch de recepción, que no será procesada, por estar recibiendo.
Pendiente conexión	La petición requiere la existencia de una conexión entre aplicaciones. La conexión no se ha completado todavía.
Perdida secuencia en proceso emisor	Se ha detectado salto en número de secuencia del mensaje.

Perdida secuencia en proceso receptor	Se ha detectado salto en número de secuencia del mensaje.
Perfiles incompatibles (compresión)	No coincide el valor especificado en ambos extremos para el parámetro de compresión.
Recepción rechazada por perfiles (sentido transmisión)	No coincide el valor especificado en ambos extremos para el parámetro de sentido de transmisión.
Petición batch de descarga de emisión	Se ha recibido una petición batch de descarga de emisión.
Petición batch de inicio de emisión	Se ha recibido una petición batch de comienzo de transmisión local.
Petición batch de inicio de recepción	Se ha recibido una petición batch de comienzo de recepción local.
Petición batch de preparación e inicio de emisión	Se ha recibido una petición desde batch de lanzamiento de un trabajo especificado en perfiles.
Petición batch de preparación e inicio de recepción	Se ha recibido una petición desde batch de lanzamiento de un trabajo especificado en perfiles.
Petición batch posterior a emisión	Se ha recibido una petición desde batch de lanzamiento de un trabajo especificado en perfiles.
Petición batch posterior a recepción	Se ha recibido una petición desde batch de lanzamiento de un trabajo que había sido especificado en perfiles.
Petición de asociación	Se ha solicitado una petición de conexión entre aplicaciones.
Petición de recepción	Se ha solicitado una petición de recepción desde el operador local o remoto.
Petición no aceptada. Modo de operación servidor	Se ha solicitado una petición no permitida en modo de operación servidor.
Posterior a emisión finalizado correctamente	Se recibe respuesta desde batch de finalización correcta de un proceso.
Posterior a recepción finalizado correctamente	Se recibe respuesta desde batch de finalización correcta de un proceso.
Previo a emisión finalizado correctamente	Se recibe respuesta desde batch de finalización correcta de un proceso.
Previo a recepción finalizado correctamente	Se recibe respuesta desde batch de finalización correcta de un proceso.
Principio de sesión. Emisión local	Se ha enviado la primera ráfaga de la transmisión.
Rearranque de red de operador remoto	Se ha producido un re arranque de red solicitado por el operador remoto.
Recepción abortada	Se ha abortado la recepción de un fichero.
Recepción correcta y finalizada	Se ha realizado correctamente la recepción de un fichero.
Recibido mensaje con CRC invalida	Se ha recibido un mensaje del remoto en una sesión definida en perfiles con validación de CRC, siendo incorrecto su CRC.
Recibido mensaje incorrecto desde batch	Corregir tipo de petición ASP.
Recibido mensaje incorrecto en proceso emisor	Mensaje fuera de protocolo.
Recibido mensaje incorrecto en proceso receptor	Mensaje fuera de protocolo.
Remoto sin sesión / NRI de alta (perfiles)	El NRI de una llamada entrante no coincide con el de la sesión dada de alta en los perfiles.
SBP recibido en estado incorrecto	Mensaje fuera de protocolo.
SBR con descuadre de totales	Respuesta negativa a un sincronismo de totales por no coincidir los totales en el proceso receptor.
SCP recibido en estado incorrecto	Mensaje fuera de protocolo.
SEP recibido en estado incorrecto	Mensaje fuera de protocolo.
Se ha lanzado batch posterior a emisión	Se ha lanzado proceso batch según perfiles.
Se ha lanzado batch posterior a recepción	Se ha lanzado proceso batch según perfiles.
Se ha lanzado batch previo a emisión	Se ha lanzado proceso batch según perfiles.
Se ha lanzado batch previo a recepción	Se ha lanzado proceso batch según perfiles.
Se ha llamado antes	Se ha recibido una petición de conexión cuando ya se procesaba una anterior a la misma sesión.
Se realiza la llamada	Se intenta conectar con el sistema EDITRAN remoto.
Se solicita cambio de clave local	El extremo local ha solicitado un cambio de clave en la fase de establecimiento de una asociación entre aplicaciones.
Se solicita cambio de clave remota	El extremo remoto ha solicitado un cambio de clave en la fase de establecimiento de una asociación entre aplicaciones.
Sesión rechazada por perfiles (Ascii/Ebdcic)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Calculo CRC)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Calidad servicio)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Compresión)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Control totales)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Criptografía)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Longitud registro)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Tipo aplicación)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Tipo conexión)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Versión)	Corregir el parámetro en el perfil de la sesión.

Tampón emisor remoto inaccesible	Se ha producido un error al acceder al fichero tampón de emisión remoto.
Tampón receptor remoto inaccesible	Se ha producido un error al acceder al fichero tampón de recepción remoto.
Todavía se está transmitiendo	Petición no procesada por encontrarse en transmisión.
Ya existe conexión	Se ha hecho una petición de conexión a una sesión que ya estaba conectada.
Ya se está recibiendo	Se recibe petición duplicada por parte del operador.
Ya se está transmitiendo	Se recibe petición duplicada por parte del operador.
Fichero receptor remoto incorrecto (lanza previo)	El remoto está preparando su tampón de recepción.
Fichero receptor remoto incorrecto (no existe previo)	El remoto no tiene preparado su tampón de recepción porque no tiene previo.
Fichero receptor remoto incorrecto (previo en posible ejecución)	El fichero remoto de recepción está posiblemente siendo preparado.
Fichero receptor remoto incorrecto (núm. sesión)	El número de sesión del fichero receptor remoto no coincide con el local.
Fichero receptor remoto incorrecto (n. reg. totales)	El número de registros totales del fichero receptor remoto no coincide con el local.
Fichero emisor remoto incorrecto (lanza previo)	El remoto está preparando su tampón de emisión.
Fichero emisor remoto incorrecto (no existe previo)	El remoto no tiene preparado su tampón de emisión porque no tiene previo.
Fichero emisor remoto incorrecto (previo en posible ejecución)	El fichero remoto de emisión esta posiblemente siendo preparado.
EDITRAN/G local deniega petición batch	EDITRAN/G no ejecuta la petición solicitada.
Fichero tampón cargado	EDITRAN/G notifica la carga del tampón de emisión.
Error. tampón emisor cifrado y perfil sin Criptografía	Perfil de IGA con criptografía y perfil de EDITRAN sin criptografía.
Error. tampón emisor cifrado y perfil con cambio clave	No se permite el cifrado de IGA y cambio de clave en EDITRAN.
Error. Clave tampón emisor y clave de emisión difieren	La clave utilizada por la IGA para Criptografiar el tampón no coincide con la clave actual de EDITRAN.
Error. Longitud tampón emisor y perfil diferentes	La longitud del tampón cargado por EDITRAN/G no coincide con la longitud actual de EDITRAN/P.
Error. tampón emisor comprimido y perfil con compresión	Se han comprimido los datos en EDITRAN/G y se solicita compresión en EDITRAN/P.
Error. Longitud tampón recepción y perfil diferentes	
Error. tampón emisor cifrado y perfil con compresión	Se han cifrado los datos en EDITRAN/G y perfil de EDITRAN/P con compresión.
RTC - Puerto en uso por otra conexión	Puerto serie está siendo utilizado por otra conexión de EDITRAN.
RTC - Puerto fuera de rango	El puerto especificado en el perfil no existe.
Adaptador de red no instalado o no operativo	El adaptador de red (módem, tarjeta X.25, etc.) no funciona.
RTC - El módem no responde	El módem no responde.
RTC - No se detecta portadora o se ha perdido	
Error al inicializar el adaptador de red	
RTC - No hay tono de marcación	
RTC - Remoto ocupado	La red identifica el ETD llamado como ocupado con otras comunicaciones y por lo tanto como imposibilitado para aceptar la llamada entrante.
RTC - No hay respuesta de remoto	
RTC - Respuesta del módem no reconocida	
RTC - Numero de RTC en blanco	
X.28 - Liberación por el ETD(P)	El equipo terminal distante ha liberado la comunicación.
X.28 - Error de procedimiento local	El DEP detecta un error de procedimiento causado por el ETD.
X.28 - Congestion de Red	Condición producida dentro de la red: Por congestión temporal. Por fallo temporal.
X.28 - Fuera de servicio	El número llamado está fuera de servicio.
X.28 - Error de procedimiento remoto	La red detecta en el extremo distante ETD/ETCD un error de procedimiento causado por el ETD.
X.28 - Numero ocupado	La red identifica el ETD llamado como ocupado con otras comunicaciones y por lo tanto como imposibilitado para aceptar la llamada entrante.
X.28 - Petición de facilidad invalida	Facilidad no válida pedida por el ETD llamante.
X.28 - Acceso prohibido	El equipo terminal llamante no está autorizado para obtener la comunicación con el ETD llamado.
X.28 - Inobtenible	La dirección del ETD llamado no está en el plan de numeración o no se ha asignado a ningún ETD.
X.28 - Liberación por el PAD	La comunicación ha sido liberada por el DEP local como respuesta a

	una invitación de liberación procedente del ETD distante.
X.28 - Numero sin cobro revertido	El equipo terminal llamado no está abonado a la aceptación de cobro revertido.
X.28 - IUR erróneo	El identificativo usuario de red es erróneo.
X.28 - Sin información adicional	Liberación con diagnostico 000 procedente de la red.
X.28 - Comando inválido	Liberación con diagnostico 016 procedente de la red.
X.28 - Comando no permitido	Liberación con diagnostico 032 procedente de la red.
X.28 - Vencimiento temporizador	Liberación con diagnostico 048 procedente de la red.
X.28 - Error al conectar con el PAD	
Sesión rechazada por perfiles (Confidencialidad)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Autenticación)	Corregir el parámetro en el perfil de la sesión.
Sesión rechazada por perfiles (Desconexión automática)	Corregir el parámetro en el perfil de la sesión.
Sesión interrumpida	Verificar el código interrupción
Certificado remoto aceptado	Se acepta el certificado remoto correctamente
TCP - Reset de la conexión	
TCP - Dirección destino requerida	Se debe especificar la dirección IP remota
TCP - Dirección no disponible	La dirección a la cual se llama no está disponible
TCP - Red inalcanzable	La dirección a la cual se llama no está disponible
TCP - Conexión rechazada	
TCP - Host caído	Verificar el estado del equipo remoto
TCP - No hay ruta para el host	
TCP - Host no encontrado	
TCP - Error irrecuperable	
Fichero receptor local incorrecto (n. reg. totales)	No coincide la cantidad de registros totales del extremo emisor con la cantidad del registros esperados recibir.
Fichero receptor local incorrecto (fecha creación)	No coincide la fecha del fichero receptor local, con la fecha de creación del extremo remoto.
Versión ignorada por control de fechas	
Agotado Timeout de asociación	
Recibido mensaje con cabecera desconocida	Mensaje de protocolo inválido.
Llamada remota rechazada (licencia red)	La sesión no tiene licencia para el tipo de llamada entrante.
SWIFT - Petición GetFile realizada	Informativo.
SWIFT - Petición GetFile recibida	Informativo.
SWIFT - Petición PutFile realizada	Informativo.
SWIFT - Petición PutFile recibida	Informativo.
SWIFT - Petición aceptada	Informativo.
SWIFT - Petición rechazada	Informativo.
SWIFT - Estado incorrecto	Informativo.
Opción no disponible para sesiones SWIFT	Informativo.
No se lanza batch posterior a emisión. Datos en SWIFT	Informativo en funcionamiento pasarela Swift.
SWIFT. Tampón en estado incompatible	Informativo en funcionamiento pasarela Swift.
SWIFT. Mensaje con identificador desconocido	Informativo en funcionamiento pasarela Swift.
Respuesta SWIFT.	Informativo.
Recepción rechazada por perfiles	
Llamada remota rechazada (datos sesión)	Revisar que existe la sesión para el Id. recibido: local-remoto-aplicación.
Llamada procedente de PAD rechazada	Revisar el campo correspondiente de los parámetros X25 del perfil de la sesión.
Liberación por número máximo de sesiones (perfil)	Revisar el campo correspondiente en el perfil local.
Liberada sesión en curso	Informativo.
Versión EDITRAN remota diferente (admitida)	Revisar el campo del perfil de la sesión.
Liberación por Timeout de inactividad	
Agotado Timeout de confirmación de descarga remota	
Consulta de recepción remota	
Descarga remota en curso	

Notas:

- ETD - Equipo terminal de datos.
- ETCD - Equipo conversor de señales (módem)
- I.U.R. - Identificativo usuario de red.

4.6. MENSAJES DE LIBERACION EN EDITRAN

Cuando en EDITRAN no se puede establecer la conexión o se produce un corte durante la transmisión, se generan mensajes de liberación que identifican mediante dos códigos (causa y diagnóstico) el motivo que las produjo.

Es difícil documentar todas las posibles causas y diagnósticos que EDITRAN/P puede recibir, ya que en muchos casos depende del protocolo de red utilizado y del suministrador del driver, por eso en esta documentación nos centraremos sólo en las liberaciones que están originadas por el propio protocolo EDITRAN.

También se incluyen en este capítulo las condiciones de reintento de conexión ya que se actúa en función de las liberaciones recibidas.

4.6.1. CAUSAS Y DIAGNOSTICOS EDITRAN

A continuación se especifican los códigos de causa y diagnóstico de liberación o rechazo de llamada dados por EDITRAN.

Causa = x'00'.

Diagnostico = x'XX'. Donde "XX" vale lo siguiente:

03	El número máximo de sesiones definido en Entorno Local (Número Máximo de Circuitos) ha llegado al límite y por tanto no existe canal disponible.
04	Se ha producido un cruce de llamadas en vuelo. Se libera la que tiene Código de Instalación EDITRAN menor.
05	Se ha producido una liberación por existir ya un canal establecido para esa Sesión.
06	No se admite en la llamada entrante la facilidad de cobro revertido según los parámetros de la Sesión en Perfiles.
07	Llamada rechazada por Tipo de Pago. En los parámetros de Perfiles de Sesión se define el tipo de pago como "R" (Remoto), mientras que la llamada entrante viene con cobro revertido.
08	Liberación de EDITRAN por parte del Operador.
09	Se ha producido un Rearranque de red por el Operador.
0A	Se rechaza la llamada entrante por utilizar facilidades inválidas.
0B	Se libera circuito por error de Compactación-Compresión.
0C	Se rechaza una llamada entrante porque la hora de entrada es incorrecta según especificaciones de la Sesión (HORA INICIO y HORA FIN).
0D	Se rechaza la llamada porque la Sesión no ha sido dada de Alta en Perfiles o porque el NRI remoto no corresponde con ninguno de los definidos en la Sesión.
0E	Se rechaza la llamada porque el Extremo Llamante definido en la Sesión no corresponde con el que realiza la llamada.
0F	Liberación genérica de EDITRAN (ficheros no preparados, arranque de automatismos, etc.).

4.6.2. CONDICIONES DE REINTENTOS DE CONEXION

El protocolo EDITRAN tiene un mecanismo de recuperación ante fallos temporales de la red basado en reintentar la conexión. Los únicos casos es los que no se intenta de nuevo es:

- Si el campo EXTREMO LLAMANTE es Remoto
- Si el código de liberación es Causa = 0 y Diagnóstico:

04	Se ha producido un cruce de llamadas.
05	Ya había conexión para esa Sesión.
08	Liberación por Operador.
0F	Liberación genérica EDITRAN.
00	Sin información adicional. Sólo se reintentará si se está estableciendo conexión, no en caídas durante la transmisión.

En todos los casos al reintentar la conexión se rotará al siguiente remoto siempre que en el perfil se hayan especificado varios.

4.7. SISTEMA DE CRIPTOGRAFÍA DE EDITRAN

4.7.1. Introducción.

El sistema de criptografía empleado en EDITRAN se basa en el algoritmo DES.

En cada entorno de ejecución de EDITRAN UNIX existe un fichero **ckds.des** donde reside la Host Master Key (HMK) de la instalación y las claves que cifran claves. EDITRAN utiliza una clave local y una remota.

No es necesaria ninguna acción por parte del usuario de EDITRAN sobre dicho fichero.

La criptografía de EDITRAN contempla un cifrado on-line bidireccional, es decir, tanto para emisión como para recepción. Los datos de salida se cifrarán con una clave y los de entrada se descifrarán con otra. Así, ambos extremos disponen de dos claves de datos homónimas.

4.7.2. Tipos de claves.

HMK - Host Master Key

Su función es cifrar las claves de la entidad usuaria local y reside de forma enmascarada en el fichero **ckds.des**.

AK - Auxiliary Key

Su función es cifrar la clave maestra de EDITRAN.

Se genera aleatoriamente y se incorpora al fichero **ckds.des** bajo una etiqueta.

EMK - Clave Maestra de EDITRAN

Su función es cifrar las claves de emisión y recepción de una sesión. Se almacena en el fichero de perfiles de EDITRAN editranp.cfg cifrada bajo la clave AK local.

TKE - Clave de Transporte de Emisión

Su función es cifrar los datos de aplicaciones usuarias de EDITRAN que se envían al remoto.

Se almacena cifrada bajo la clave EMK en el fichero de perfiles.

TKR - Clave de Transporte de Recepción

Su función es descifrar los datos recibidos de una aplicación usuaria remota.

Se almacena cifrada bajo la clave EMK en el fichero de perfiles.

En el establecimiento de una conexión se resuelve la autenticación de las claves TKE y TKR de ambos extremos, con independencia de que se realice o no un cambio de claves, es decir, se valida que TKE local = TKR remota y que TKR local = TKE remota.

4.7.3. Errores de Criptografía.

Cualquier error de criptografía generará una información para el operador local y una desconexión.

Los errores que se pueden producir son:

Errores de Criptografía v2.2.

ERR1	El extremo que solicita una Petición de Conexión no ha podido hacer el Recifrado de las Claves de su fichero.
ERR2	El extremo que solicita autenticar su clave TKE no ha podido cifrar el Código de Autenticación, aunque sí hizo el recifrado.
ERR3	El extremo que solicita una Petición de Conexión con Cambio de Clave no ha podido generar una clave de emisión TKE-nueva.
ERR4	El extremo que recibe la Indicación de Notificación del Remoto tuvo un error al hacer Recifrado de la clave TKR de su fichero.
ERR5	El extremo que recibe la Indicación de Notificación no ha podido descifrar el Código de Autenticación que le envía el Remoto, aunque sí hizo el Recifrado.
ERR6	El extremo que recibe una Indicación de Notificación con Cambio de Clave, tuvo un error al hacer el Recifrado de la nueva clave de Recepción que viene del remoto (TKR-nueva).
ERR7	El extremo que va a enviar un dato de usuario o Mensaje de Operador, ha tenido un error en el cifrado "on-line".
ERR8	El extremo que recibe un dato de usuario o Mensaje de Operador del Remoto ha tenido un error en el descifrado "on-line".
ERR9	El extremo que recibe una Notificación del Remoto (con o sin Cambio de Clave) ha descifrado el Código de Autenticación, pero es incorrecto (a pesar de guardar la clave antigua de recepción). Posiblemente algún extremo dio de Baja y Alta la Sesión EDITRAN de Perfiles. Es el error más grave. Sólo se sale de esta situación dando de Baja y Alta la Sesión en Perfiles en ambos extremos.

Errores de Criptografía v3.0 RSA o DES.

ERR1	Se produjo un error al obtener la clave local, bien porque no se suministró en Perfiles o bien por un error en la Interfaz de Claves Externa.
ERR2	Al intentar enviar una petición de asociación o una respuesta se produce un error al generar la incertidumbre o la firma. Si el algoritmo empleado es DES el error se encuentra en la clave local. Si es RSA el error es de la clave local cuando se genera firma, o de la clave remota cuando se genera incertidumbre.
ERR3	Error al intentar generar clave de la sesión. Si el algoritmo empleado es DES el error concierne a la clave local. Si es RSA la clave errónea es la remota.
ERR4	Se produjo un error al obtener la clave remota, bien porque no se suministró en Perfiles o bien porque se produjo un error en la Interfaz de Claves Externa.
ERR5	Al procesar una petición o una respuesta del remoto se produce error al intentar descifrar la incertidumbre o la firma. Si se utiliza algoritmo DES la clave errónea es la clave remota. Si se emplea RSA el error es de la clave remota al descifrar firma, o de la clave local al descifrar incertidumbre.
ERR6	Al procesar una petición o una respuesta del remoto se produce un error al descifrar la clave de sesión. Si el algoritmo es DES el error es de la clave remota. Si es RSA la clave en error es la local.
ERR7	El extremo que va a enviar un dato de usuario o Mensaje de Operador, ha tenido un error en el cifrado "on-line".
ERR8	El extremo que recibe un dato de usuario o Mensaje de Operador del Remoto ha tenido un error en el descifrado "on-line".
ERR9	Al procesar un petición o una respuesta se consigue descifrar la clave de la sesión y la firma pero o bien no coincide la incertidumbre o bien no coincide la firma (este caso sólo en RSA). El error se produce porque las claves de intercambio no coinciden en ambos extremos. Si se utilizó una Interfaz de Claves Externa, el mensaje debe acompañar los 8 últimos bytes del label empleado. Si el algoritmo utilizado es DES la clave errónea es la clave local del extremo que genera el mensaje. Si es RSA la clave errónea es la clave local (si se produce error al validar la incertidumbre) o la remota (si se produce error al verificar la firma).

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