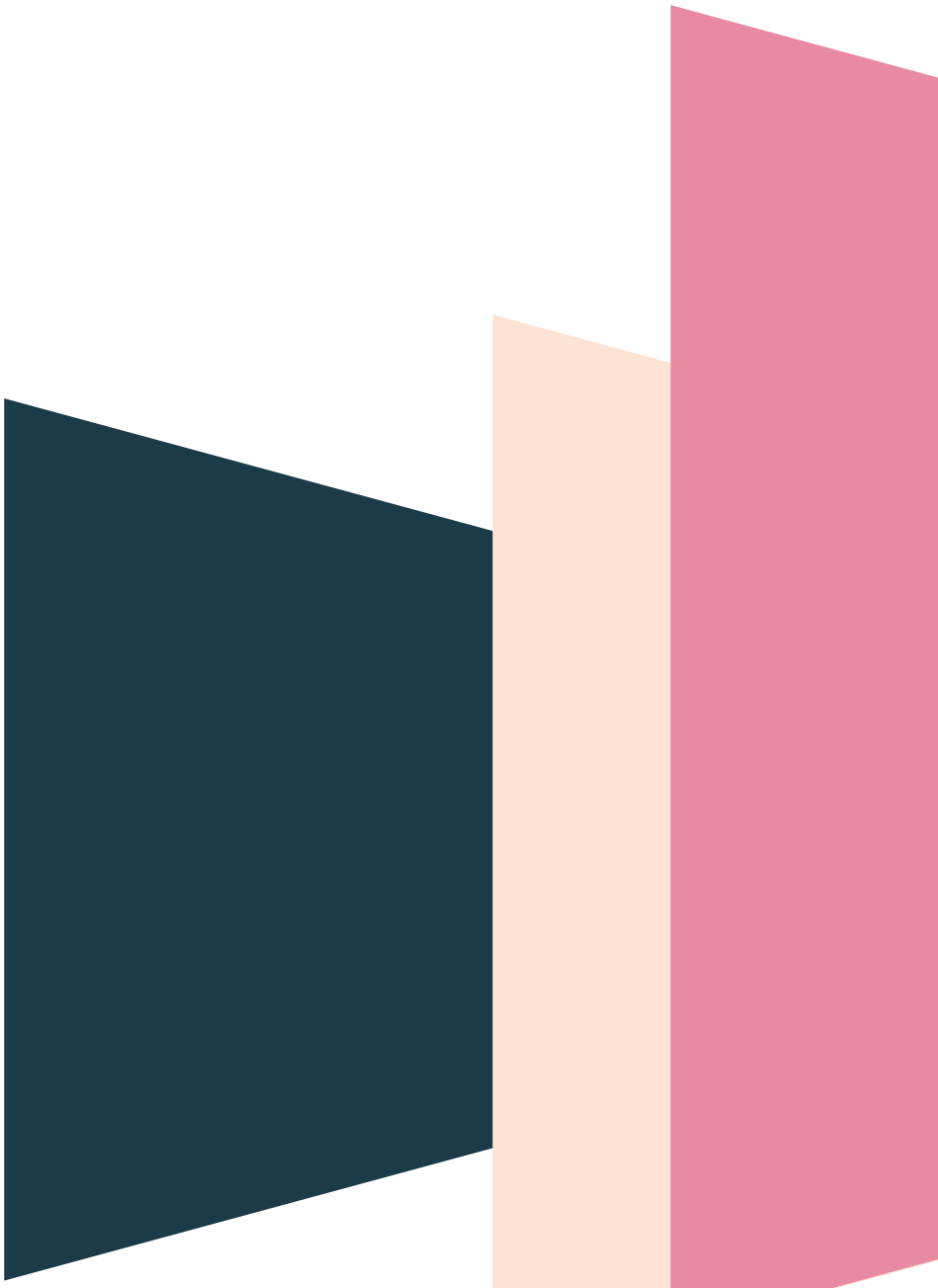
minsait

An Indra company

EDITRAN/P 5.2

EDITRAN/P Utilidades y Códigos
CICS
Manual de usuario

junio de 2019



ecosystems
communications

1. INTRODUCCION

EDITRAN/P (en adelante EDITRAN) es un producto "software" que permite la transmisión de información formateada y guardada en ficheros o bases de datos denominados TAMPONES.

La información que se desea emitir a un determinado Remoto (destino de la información) llevará la Identificación de ese destino. Esta Identificación se denomina SESION EDITRAN y está formada por el Código de Instalación de EDITRAN del Local, Remoto, y un Código de Aplicación EDITRAN (el cual permite la emisión de diversos tipos de información al mismo destino). Esta Identificación forma parte o bien del nombre del fichero TAMPON o de los registros que contiene la información.

De la misma forma la información lleva un Número de Secuencia de tal forma que permite el control de la secuencia de la información y evita pérdidas. Este Número de Secuencia unido a la Sesión es la única información que EDITRAN exige para poder emitir información a otro EDITRAN accesible por la red de comunicaciones.

Para que la Instalación Local de EDITRAN pueda comunicarse con otras Instalaciones Remotas es necesario definir un conjunto de elementos necesarios para la Comunicación. Los Elementos que es necesario definir o crear son:

- Características del "ENTORNO LOCAL GENERAL". Es un conjunto de parámetros definibles dentro del propio producto que le permiten conocer la instalación donde el producto va a estar funcionando, además de la Identificación de la Instalación de EDITRAN Local, hacia los demás.
- Características del "ENTORNO LOCAL SECUNDARIO (SUBENTORNO)". Es opcional y se podrán dar de alta tantos como se quiera. Se define el código del Subentorno Local para que la instalación pueda presentarse como dicho entorno.
- Características de "SESIONES". Son los parámetros que definen cada Instalación Remota con los Códigos de Aplicación que se vayan a utilizar con ella. Estos parámetros se definen por el Administrador de la Instalación. Se permite crear, borrar o modificarlos. Se pueden definir tantas Sesiones como se deseen.
- Ficheros TAMPONES. Son los ficheros o bases de datos que contienen la información con la SESION y el Número de Secuencia. Contiene además un registro especial (el primero) donde EDITRAN recoge y deja información referente a la transmisión (Número de Registros a Emitir o Recibir, Número de Registros Emitidos o Recibidos, Fechas y Horas de Transmisión, etc.). Estos ficheros son creados por el Usuario o por las Interfaces de Aplicación aportadas por Indra. Para más detalle de estos ficheros consulte el manual ***ED52GTAC.***

2. GENERALIDADES SOBRE EDITRAN E INTERFACES.

2.1. FUNCIONES DE APLICACION Y PRESENTACION EN EDITRAN

EDITRAN V5.2 requiere EDITRAN/G 5.2 o procedimientos de Usuario adaptados a la Identificación de SESION de EDITRAN V5.2.

Las diferencias existentes entre las versiones EDITRAN puede encontrarlas en el manual **EDFUNCV52**.

2.2. COMUNICACION ENTRE EDITRAN E INTERFACES

2.2.1. Desde una interfaz a EDITRAN.

Generalizando, cabría decir que se trata de envío de mensajes desde programas batch al CICS donde esté corriendo EDITRAN.

En la instalación de EDITRAN se suministra el jcl ZTBPJBAT y la clist ZTBG, con los que se pueden enviar A5P de tipos 1 a 4 a una sesión de transmisión determinada, cuyo significado es el siguiente:

- Tipo 1: Orden de carga de emisión y principio de emisión.
- Tipo 2: Orden de inicialización de recepción y principio de recepción.
- Tipo 3: Orden de proceso posterior a emisión.
- Tipo 4: Orden de descarga de recepción.

Estas órdenes causan que EDITRAN lance los procesos previos/posteriores a emisión/recepción, desde los cuales se informará a EDITRAN de su correcta o incorrecta finalización por medio de los mensajes AnR(+) o AnR(-), siendo n de 1 a 4 y correspondiendo a los tipos de A5P vistos antes. Concretamente

- A1R(+): Ordena a EDITRAN el comienzo de la emisión.
- A2R(+): Ordena a EDITRAN el comienzo de la recepción.
- EDP: Interrumpir emisión.
- EDR: Interrumpir recepción.

2.2.2. Desde EDITRAN a una interfaz.

En los casos que nos interesan, no se puede hablar realmente de envío de mensajes desde EDITRAN a otra región donde se esté ejecutando un proceso, sino del lanzamiento de Job's invocando procedimientos previos/posteriores a emisión/recepción con aportación de ciertos valores pasados por parámetros.

Estos procedimientos se lanzarán sólo si están especificados en el perfil de la sesión de transmisión correspondiente. En este caso, un A5P siempre determina que se lance el procedimiento correspondiente a su tipo, como hemos visto anteriormente. No obstante, también se lanzan los procedimientos en otras circunstancias:

- Se lanza el previo a emisión cuando se recibe petición de emisión del operador local ó de EDITRAN remoto y el tampón de emisión está:
  - Vacío.
  - No emitido completo pero con todos los registros confirmados por el receptor y se recibe un rechazo de éste a la emisión.
- Se lanza el previo a recepción cuando el tampón de recepción está en situaciones equivalentes a las que se acaban de ver para el de emisión.
- Se lanza el posterior a emisión al finalizar ésta.
- Se lanza el posterior a recepción al finalizar ésta.
- EDITRAN lanzará, además, los procedimientos previos a emisión o recepción, cuando el tampón correspondiente esté cerrado.
- EDITRAN lanza un procedimiento de excepción, cuando ocurra una incidencia o una interrupción de la transmisión.

3. REQUISITOS DE FUNCIONAMIENTO DE EDITRAN.

Para poder utilizar EDITRAN CICS en una instalación, es necesario realizar lo siguiente:

- θ Haber instalado correctamente el producto (consulte el manual **ED52INSC**).
- θ Mantener el fichero de Perfiles de EDITRAN, desde su Administrador. La información necesaria corresponde a:
  - Entorno Local General.
  - Entorno Local Secundario (Subentorno). Esto es opcional.
  - Sesiones. Todas las SESIONES que se vayan a utilizar (emitir, recibir, conectarse).
- θ Generar los Procedimientos de Usuario o de la Interfaz Genérica de Aplicación (EDITRAN/G) de acuerdo con los parámetros de la instalación (Nombres de Librerías, Nombre del CICS).

Una vez realizados los pasos anteriores correctamente, ya es posible utilizar el producto para realizar emisiones y recepciones de ficheros con otras Instalaciones que tengan EDITRAN compatibles.

4. INTERFAZ GRAFICA.

Consulte el manual **ED52USUC**.

5. UTILIDADES.

Se exponen en este capítulo algunas utilidades disponibles para realizar determinadas peticiones al núcleo de EDITRAN/P o para obtener listados auxiliares.

5.1. GENERACION DE MENSAJES A5P (ZTBPJBAT).

El Jcl ZTBPJBAT, se utiliza para enviar al núcleo de EDITRAN/P mensajes A5P de tipo 1, 2, 3, 4, 8 o A, ordenando el lanzamiento incondicional de los procedimientos previos/posteriores a emisión/recepción. Esta funcionalidad normalmente no se utiliza.

Se le administrarán los siguientes parámetros:

- θ Nombre CPU donde se encuentra el CICS con EDITRAN/P a utilizar.
- θ Nombre del CICS con EDITRAN/P a utilizar.
- θ Transacción de Interfase (ZTBI) especificada en el Entorno Local General de Perfiles de EDITRAN/P
- θ A5P obligatorio.
- θ Código Local.
- θ Código Remoto.
- θ Aplicación.
- θ Cualificador o tipo de petición. Se elegirá uno de los siguientes:
  - 1 - Proceso previo a emisión y petición de emisión.
  - 2 - Proceso previo a recepción y petición de recepción.
  - 3 - Proceso posterior a emisión.
  - 4 - Proceso posterior a recepción.
  - 8 - Proceso previo a emisión sin petición de emisión.
  - A - Proceso previo a recepción sin petición de recepción.
- θ 00N obligatorio.

El proceso realizado es el siguiente:

- θ El programa batch genera un Modify al CICS especificado en los parámetros para que arranque la transacción de Interfase , pasándole todos los parámetros descritos anteriormente:
  - **F cpu,CICS,FTAI A5P00009999000002098OTELECA100N**
- θ Esta transacción comprueba la existencia de la Sesión de transmisión solicitada y si existe lanzará el procedimiento solicitado siempre y cuando se haya especificado en los Perfiles de dicha Sesión.

5.2. LISTADO DE LA TRAZA (ZTBPJLTR).

El fichero de Traza se puede listar de forma selectiva con el Jcl ZTBPJLTR. Se le introducirán los parámetros y opciones necesarios, los cuales están suficientemente documentados en el propio Jcl.

Se puede observar que en el paso LISTEDI se obtiene el listado de la traza en un fichero, el cual puede enviarse a Indra, para análisis de posibles problemas e incidencias, utilizando el propio EDITRAN.

A continuación se acompaña una ejecución de ejemplo:

```
SESION    : 000000000 000000000 000000              LISTADO DE TRAZA (EDITRAN)                              PAGINA :     1
FECHA     : 11/05/1998                              ==========================                              FECHA  : 11/05/1998
E/S ORIGEN    REMOTO    APLIC.       SESION INTERNA        MEN C  NSM   T  FECHA    HORA                  MENSAJE
=== ========= ========= ====== ========================== === = ====== = ======== ====== ========== ======================================
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   XAI    I2C0    11051998 100903 TIPO= 0B CANAL= 1064 CAUSA= 00 DIAG= 00
  S 000099990 000090000 TESNCE 00000999000000900007ESNCE   XAI    I2C0    11051998 100903 TIPO= 0F CANAL= 1064 CAUSA= 7C DIAG= F0
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   XAI    I2C0    11051998 100903 TIPO= 10 CANAL= 1064 CAUSA= 00 DIAG= 40
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SAP            11051998 100907 IND. NOTIFICACION COD=00
  S 000099990 000090000 TESNCE 00000999000000900007ESNCE   SAR +          11051998 100907 RESP. NOTIFICACIONCOD=00
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SCP 0 000000   11051998 100908 PRINCIPIO RECEPCION
  S 000099990 000090000 TESNCE 00000999000000900007ESNCE   SCR 0 000000   11051998 100908 RESPUESTA PETICION DE RECEPCION
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SFP 0 000000   11051998 100913 DATOS
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SFP 0 000000   11051998 100913 DATOS
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SFP 0 000000   11051998 100913 DATOS
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SFP 0 000000   11051998 100913 DATOS
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SBP 0 000000   11051998 100925 PETICION SINCRONISMO
  S 000099990 000090000 TESNCE 00000999000000900007ESNCE   SBR 0 000000   11051998 100925 RESPUESTA SINCRONISMO
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SEP 0 000000   11051998 100925 PETICION FIN EMISION
  S 000099990 000090000 TESNCE 00000999000000900007ESNCE   SER 9 000000   11051998 100925 RECEPCION CORRECTA Y FINALIZADA
  S 000099990 000090000 TESNCE 00000999000000900007ESNCE   A4P            11051998 100925 CUALIF = N RETORNO = 00
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   SAB            11051998 100926 SOL.  LIBERACION  COD=09
  S 000099990 000090000 TESNCE 00000999000000900007ESNCE   XAI    I2C0    11051998 100926 TIPO= 13 CANAL= 1064 CAUSA= 00 DIAG= 0F
E   000000000 000000000 000000 00000000000000000000000000 XAI    I2C0    11051998 100927 TIPO= 14 CANAL= 1064 CAUSA= 00 DIAG= 40
E   000099990 000090000 TESNCE 00000999000000900007ESNCE   A4R            11051998 100955 CUALIF = N RETORNO = 00
```

5.3. LISTADO DEL LOG (ZTBPJLLO).

El fichero de Log se puede listar de forma selectiva con el Jcl ZTBPJLLO. Se le introducirán los parámetros y opciones necesarios, los cuales están suficientemente documentados en el propio Jcl.

Se puede observar que en el paso LISTEDI se obtiene el listado del Log en un fichero, el cual puede enviarse a Indra, para análisis de posibles problemas e incidencias, utilizando el propio EDITRAN.

A continuación se acompaña una ejecución de ejemplo:

```
SESION    : 000000000 000000000 000000               LISTADO DE LOG (EDITRAN)                                PAGINA :        1
FECHA     : 11/05/1998                               ============================                            FECHA  : 11/05/1998
  ORIGEN   DESTINO  APLIC.       SESION INTERNA          FECHA    HORA                          MENSAJE
========= ========= ====== ========================== ======== ====== ============================================================
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100140 ZTP0627 : NOTIFICACION BATCH: TAMPON RECEP. PREPARADO
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100903 ZTP0520 : LLAMADA REMOTA ACEPTADA
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100903 ZTP0055 : CONEXION REALIZADA
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100907 ZTP0895 : SESION ESTABLECIDA
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100908 ZTP0390 : INICIO DE RECEPCION
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100925 ZTP0780 : RECEPCION CORRECTA Y FINALIZADA
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100925 ZTP0855 : SE HA LANZADO BATCH POSTERIOR A RECEPCION
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100926 ZTP0490 : LIBERACION TRANSMISION            C:00 D:0F
000099990 000090000 TESNCE 00000999000000900007ESNCE    11051998 100955 ZTP0740 : POSTERIOR RECEPCION FINALIZADO CORRECTAMENTE
```

5.4. LISTADO DE SESIONES (ZTBPJLSE).

Las sesiones contenidas en el Fichero de Perfiles de EDITRAN/P se pueden listar de forma selectiva con el Jcl ZTBPJLSE. Se le introducirán los parámetros y opciones necesarios, los cuales están suficientemente documentados en el propio Jcl. Se sacan varios tipos de listados: identificadores de acceso, identificadores de transporte y nris-ip remotas (se muestra a continuación el de identificador de acceso). El programa ZTBPBLSE saca los identificadores de acceso, el programa ZTBPBLDT los id transporte y el programa ZTBPBLNR los nris-ip remotas (si algún paso no le interesa, puede eliminarlo, ajustando las características de los 3 ficheros intermedios (disp) de los que tiran los pasos no eliminados.

```
CODIGO REMOTO : 000000000                LISTADO DE SESIONES (EDITRAN)                      PAGINA :        1
APLICACION    : TELECA                   ==============================                     FECHA  : 11/05/1998
SESIONES PERTENECIENTES AL ENTORNO :  000099990
  CODIGO  APLIC.      NOMBRE  REMOTO       NOMBRE APLICACION           SESION INTERNA            IDENTIFICADOR ACCESO
========= ======  ====================  ====================  ================================   ====================
A00099980 TELECA  ARGENTINA             TELECARGA             ARGENTINA-TELECA                          0
000000080 TELECA  BANCO ATLANTICO       TELECARGA             0000999900000000080TELECA                 0
000000130 TELECA  NATWEST                PRUEBAS               0000999900000000130TELECA                 0
000000150 TELECA  BCA.CATALANA          TELECARGA             0000999900000000150TELECA                 0
000000190 TELECA  DEUTSCHE BANK         OBJETOS               0000999900000000190TELECA                 0
000000260 TELECA  ELECTRA DE VIESGO     TELECARGA             0000999900000000260TELECA                 0
000000300 TELECA  BANESTO               PRUEBAS               0000999900000000300TELECA                 0
000000420 TELECA  B. GUIPUZCOANO        TELECA                0000999900000000420TELECA                 0
000000490 TELECA  BCH                   PRUEBAS               0000999900000000490TELECA                 0
```

5.5. ALTA-BAJA DE PERFILES EDITRAN/P.

Consulte el manual **EP52GPEC**. En la interfaz gráfica tiene una opción más simple

5.6. MODIFICACION DE PERFILES EDITRAN/P.

Consulte el manual **EP52GPEC**. En la interfaz gráfica tiene una opción más simple

6. ANEXO A. MENSAJES DE EDITRAN AL OPERADOR Y LOG.

Estos mensajes aparecen en TERMINAL OPERADOR (y siempre se graban en el fichero de Log) de cada Sesión EDITRAN, como consecuencia de eventos en las transmisiones.

A continuación se detallan dichos mensajes, en orden numérico, con su explicación o la acción aconsejada a seguir.

ZTP0005 ERROR DE PROCESO EN EL PROGRAMA: XXXXXXXX

ZTP0010 ACEPTACION DE LLAMADA RECHAZADA
La interfaz rechaza paquete de aceptación de llamada remota.

ZTP0020 ARRANQUE NO CONTEMPLADO EN NUCLEO
Arranque de transacción fuera de protocolo.

ZTP0025 CAIDA DE RED
Llega mensaje de caída de red.

ZTP0030 CANAL NO ENCONTRADO. NO REALIZA LLAMADA
Se ha recibido un information report (NPSI-DATE) con diagnóstico para reintentar llamada, pero esta no se puede realizar por no encontrar canal.

ZTP0035 CAUSA DE INFORMATION REPORT NO CONTROLADA
Ha entrado un information report (NPSI-DATE) con código-diagnóstico desconocidos.

ZTP0040 COMIENZO DE LA TRANSMISION
Se inicia la emisión al remoto.

ZTP0045 CONEXION NO REALIZADA
En NPSI-PCNE o conexiones punto a punto no se consigue activar el terminal.

ZTP0047 TIPO DE CONEXION INVALIDO
Llamada entrante rechazada porque la sesión tiene un tipo de conexión en perfiles que no se corresponde con la interfaz de la llamada entrante.

ZTP0055 CONEXION REALIZADA
Se ha aceptado una petición de conexión tanto local como remota.

ZTP0080 CONSULTA DE ESTADO
Mensaje en desuso.

ZTP0085 CONSULTA DEL FICHERO EMISOR REMOTO.
Se ha consultado el registro de control del tampón de emisión remoto (opción 1 de Consulta de ficheros). Se exige estar en sesión con el remoto y tener un terminal puesto en TERM. OPER. En el Perfil de la Sesión.

ZTP0090 CONSULTA DEL FICHERO RECEPTOR REMOTO
Lo mismo que el anterior para el tampón receptor remoto.

ZTP0092 DESCUADRE TOTALES EN PROCESO EMISOR
Mensaje en desuso.

ZTP0095 DESCUADRE TOTALES EN PROCESO RECEPTOR
Mensaje en desuso.

ZTP0097 CORREGIR CTCP
Ha entrado un mensaje error-information report (NPSI-DATE). Es posible que EDITRAN subsane el problema. En caso contrario, remitirse al mensaje.

ZTP0098 CORREGIR CTCP O GENERACION X25
Ha entrado un mensaje error-information report (NPSI-DATE). Es posible que EDITRAN subsane el problema. En caso contrario, remitirse al mensaje.

ZTP0100 DETECTADA CONEXION REMOTA PUNTO A PUNTO
En tipos de conexión Punto a Punto o LU 6.2, igual que en NPSI/PCNE, se detecta conexión ante un mensaje entrante del remoto.

ZTP0103 EXISTE PASSWORD PARA DESCIFRAR.PARA BORRARLA PULSE ESPACIOS.
El certificado incluido en perfiles tiene password y si quieres quitarla tienes que dejar el campo a espacios.

ZTP0105 DETECTADA LIBERACION DE TRANSMISION
El terminal real se ha desactivado en medio de una transmisión. EDITRAN intentará conectar a la sesión afectada y restablecer la transmisión.

ZTP0110 EMISION CORRECTA Y FINALIZADA
Se ha completado la emisión. El local ha enviado al remoto el mensaje de fin de emisión y éste ha contestado afirmativamente. Se da por terminada una emisión de forma correcta.

ZTP0115 ENVIADO CLEAR POR INFORMATION REPORT
Ha entrado un mensaje error-information report (NPSI-DATE) y como consecuencia de ello se ha generado una liberación.

ZTP0120 ENVIADO RESTART POR INFORMATION REPORT
Ha entrado un mensaje error-information report (NPSI-DATE) y se ha generado un restart.

ZTP0125 ERROR A5P CON CUALIFICADOR INCORRECTO
Corregir tipo de petición A5P.

ZTP0128 CERTIF.CON PASSW. PARA FIRMAR. PARA BORRARLA PULSE ESPACIOS.
El certificado incluido en perfiles tiene password y si quieres quitarla tienes que dejar el campo a espacios.

ZTP0130 ERROR AL ABRIR EL FICHERO XXXXXXXX
El fichero no puede abrirse en CICS. Posiblemente no se definió a VSAM. Comprobar en el Log del Cics el error que está dando.

ZTP0135 ERROR AL CERRAR EL FICHERO XXXXXXXX
El fichero no puede cerrarse en CICS. Comprobar en el Log del Cics el error que está dando.

ZTP0140 ERROR CLAVES INCOMPATIBLES. (ERRX)
Error en autenticación de claves. No coincide la clave operacional local con la remota. Véase anexo D.

ZTP0145 ERROR ALLOCATE DEL FICHERO XXXXXXXX
El fichero no puede liberarse para ceder su control a CICS. Comprobar que no esté cedido a otro Job, o que haya sido bien definido a VSAM.

ZTP0150 ERROR EN CALCULO DE CRC EN PROCESO EMISOR
Antes de emitir un mensaje al remoto, hay un error local en el cálculo de su crc. Se ignora el mensaje.

ZTP0153 LONGITUD DE DATOS A ENVIAR EXCEDEN DE 4096 BYTES.

ZTP0155 ERROR EN CALCULO CRC EN MENSAJE RECIBIDO
Al recibir un mensaje del remoto, hay un error local en el cálculo de su CRC.

ZTP0160 ERROR RESID (LLAMADA ACEPTADA) XXXX
Cuando se realiza una llamada (NPSI/DATE o GATE) y entra el paquete de aceptación de llamada, se detecta que el cvc por el que entra no está comprendido en el rango de cvc's en perfiles.

ZTP0161 ERROR RESID (LLAMADA REMOTA) XXXX
Cuando entra una llamada (NPSI/DATE o GATE) el circuito por el que entra no está comprendido en el rango de cvc's en perfiles.

ZTP0162 ERROR TERMID (LLAMADA ACEPTADA) XXXX
Cuando se realiza una llamada (NPSI/DATE o GATE) y entra el paquete de aceptación de llamada el terminal que se calcula no está definido.

ZTP0163 ERROR TERMID (LLAMADA REMOTA) XXXX
Cuando entra una llamada (NPSI/DATE o GATE) el terminal que se calcula no está definido.

ZTP0165 ERROR EN DESALOCATION DEL FICHERO XXXXXXXX
El fichero no puede liberarse del CICS para ceder su control a trabajos batch. Comprobar que no este cedido a otro Job , o que haya sido bien definido a VSAM.

ZTP0167 ERROR EN EJECUCION DEL PROC. BATCH XXXXXXXX
El procedimiento ha terminado anormalmente, mirar la salida de la ejecución.

ZTP0170 ERROR EN PROCESO BATCH REMOTO
Se ha producido en algún proceso batch automático del remoto, con la consiguiente liberación.

ZTP0180 ERROR EN RANGO DE TERMID XXXX
Revisar el primer terminal definido en la sesión así como la definición de los terminales (netnames) (NPSI-DATE o GATE).

ZTP0185 ERROR EN TRANSPARENCIA EN MENSAJE RECIBIDO
Al recibir un mensaje en tipo de conexión PAD Público o Privado, se produce un error local en el cálculo de su transparencia.

ZTP0190 ERROR INFORMATION REPORT C:XX D:XX
Se ha recibido un mensaje error information report (NPSI-DATE o GATE).

ZTP0192 ERROR EN INTERFASE APLICACION : CODIGO RET=??
Se recibe un return-code desde la interfaz de comunicaciones con código no traducido.

ZTP0194 DATOS APL. INCOMPATIBLES CON COMPRESION RISTRAS
Se ha realizado una compresión batch (compresor LZW) y se intenta hacer una compresión por ristras (compresión on-line), esta opción no es compatible.

ZTP0195 ERROR LOCAL EN COMPRESION/DESCOMPRESION : X
Se produce un error local de compresión-descompresión.

ZTP0197 ERROR LOCAL CRIPTOGRAFIA:XXXX - XXXX (ERRX)
Se ha producido un error en proceso de cifrado, comprobar códigos resultado en Anexo D.

ZTP0200 ERROR REMOTO DE CRIPTOGRAFIA (ERRx)
Se ha detectado un error remoto de criptografía. Véase ERRx en Anexo D.

ZTP0205 ERROR REMOTO EN COMPRESION/DESCOMPRESION
El remoto tuvo un error al comprimir/descomprimir datos, con la consiguiente liberación del circuito.

ZTP0210 ERROR SIN JOB O FICHERO EN PERFILES
Revise última pantalla del perfil de la sesión de EDITRAN/P.

ZTP0215 EXCESO DE REINTENTOS DE BLOQUE EMISION
El emisor, después de enviar el número de registros especificado en NUM.REG. SINCRONISMO del perfil de la Sesión, envía un mensaje de sincronismo al receptor y al no recibir respuesta, reintenta tantas veces y con la periodicidad que se especifica en el perfil de la sesión, asimismo sin recibir respuesta. Una posible causa sería tener el emisor un número de registros de sincronismo muy elevado en función de la velocidad de la línea, en cuyo caso habría que poner valores coherentes en NUM.REG. SINCRONISMO, TIME-OUT y MAX. REINTENTOS del Perfil de la Sesión.

ZTP0220 EXCESO DE REINTENTOS DE CONEXION
Se han cumplido todos los reintentos de conexión, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN, y por cada combinación de NRI Local - NRI Remoto sin lograr la conexión. Consulte las posibles liberaciones producidas en Anexo C.

ZTP0225 EXCESO DE REINTENTOS DE FIN DE RAFAGA
Se han cumplido todos los reintentos de sincronismo, atendiendo al número de reintentos en los perfiles de la sesión EDITRAN.

ZTP0230 EXCESO DE REINTENTOS EN EL PROCESO EMISOR

Se han cumplido todos los reintentos con duplicados en el proceso emisor de mensajes que requieren respuesta.

ZTP0235 EXCESO DE REINTENTOS EN EL PROCESO RECEPTOR
Se han cumplido todos los reintentos con duplicados en el proceso receptor de mensajes que requieren respuesta.

ZTP0245 EXCESO DE REINTENTOS PARA ESTABLECER SESION
Se han cumplido todos los reintentos de notificación de parámetros para el establecimiento de sesión sin recibir respuesta del remoto.

ZTP0246 EXCESO DE REINTENTOS DE ESPERA DE SAP.
Se han cumplido todos los reintentos de espera de SAP sin que el remoto haya enviado dicho mensaje y se haya podido establecer sesión. Se libera para evitar que quede el cvc - socket conectado.

ZTP0250 EXCESO DE REINTENTOS PARA FIN DE EMISION
Cuando a una petición de fin de emisión, se dan por finalizados los reintentos para esperar respuesta.

ZTP0260 EXTREMO LLAMANTE INVALIDO PERFIL C:XX D:XX
Incompatibilidad en los valores de dicho campo en el registro de perfiles.

ZTP0265 FICHERO DE EMISION 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. El fichero de emisión / recepción no está cargado, o no está disponible para EDITRAN (se desencadena el proceso batch que se especifique en perfiles).

ZTP0270 FICHERO CERRADO XXXXXXXX
Mensaje en desuso.

ZTP0272 FICHERO SIN ESPACIO XXXXXXXX
Recibiendo datos del remoto, el fichero tampón se ha llenado. Definir nuevamente el fichero VSAM con mayor número de registros y realizar la petición nuevamente.

ZTP0275 FICHERO NO CREADO XXXXXXXX
Mensaje en desuso.

ZTP0280 FICHERO DE RECEPCION 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.
El fichero de emisión / recepción no está cargado, o no está disponible para EDITRAN (se desencadena el proceso batch que se especifique en perfiles).

ZTP0282 FICH.RECEP.INCOMP.(REG.TOTALES-FECHA CREACION)

Número de registros totales del fichero tampón de recepción local distintos que del fichero emisión remoto. También se puede dar con igual número de registros. En todos los casos, se debe a que el receptor, ya tenía parte de fichero recibida, se liberó la transmisión y el emisor cargó de nuevo (el mismo o distinto contenido), de forma que el receptor lo detecta a través de la fecha de creación de su tampón receptor. Como el receptor no sabe si ha variado entre una carga y otra el contenido, rechaza. La forma de salir es inicializar la recepción y volver a comenzar desde el principio. La fecha de creación del tampón receptor se actualiza con la del tampón emisor, sólo en el primer comienzo de la primera transmisión (cuando todavía no tiene ningún registro confirmado).

ZTP0283 FICH.RECEPCION NO PREPARADO (ID.CONFIR.APL)
Identificador de aplicación del fichero tampón de recepción no coincide con el del mensaje de inicio de recepción y se ha especificado en perfiles sincronismo de aplicación 'Q'.

ZTP0285 FICHERO INCORRECTO XXXXXXXX
Mensaje en desuso.

ZTP0290 TAMPON EMISOR REMOTO EN SIT. NO COMPATIBLE
Se intenta recibir un tampón con un número total de registros inferior al que tiene registrado el tampón. Posiblemente hubo una emisión anterior incompleta y el emisor volvió a cargar un fichero mas reducido y el receptor no inicializó la recepción. El receptor debe inicializar su tampón receptor.

ZTP0293 TAMPON RECEPTOR REMOTO EN SIT. INCOMPATIBLE
Mensaje similar al anterior.

ZTP0295 FICHERO TAMPON DE EMISION CERRADO
Este mensaje no sale en el Log, pero lo puede recibir el remoto al hacer la consulta del tampón emisor del local si no está cargado..

ZTP0300 FICHERO TAMPON DE RECEPCION SIN ESPACIO
Recibiendo datos del remoto, el fichero tampón se ha llenado. Definir nuevamente el fichero VSAM con mayor número de registros y realizar la petición nuevamente.

ZTP0310 FICHERO TAMPON DE RECEPCION CERRADO
Similar al mensaje **ZTP0295**.

ZTP0320 FIN DE EMISION PEDIDO POR OPERADOR REMOTO
El remoto ha solicitado el fin de la transmisión sin que ésta se haya completado.

ZTP0325 FIN EMISION PEDIDO POR INTERFASE APL. LOCAL
Cuando la interfaz Local solicita fin de emisión forzada.

ZTP0330 FIN DE EMISION PEDIDO POR OPERADOR LOCAL
El local ha solicitado el fin de la transmisión sin que ésta se haya completado.

ZTP0335 FIN DE RECEPCION PEDIDO POR OPERADOR REMOTO
Similar al anterior..

ZTP0340 FIN RECEPCION PEDIDO POR INTERFAZ AP. LOCAL
Cuando la interfaz Local solicita fin de recepción forzada.

ZTP0345 FIN DE RECEPCION PEDIDO POR OPERADOR LOCAL
similar al mensaje **ZTP0330**.

ZTP0350 INDICACION CONFIRMACION INTERRUPCION
Contestación a una petición interrupción solicitada por EDITRAN (NPSI-DATE o GATE).

ZTP0355 INDICACION CONFIRMACION RESET
Contestación a una petición Reset solicitada por EDITRAN (NPSI-DATE o GATE).

ZTP0360 INDICACION CONFIRMACION REARRANQUE
Contestación a una petición Rearranque solicitada por EDITRAN (NPSI-DATE).

ZTP0365 INDICACION DIAGNOSTICO C:XX D:XX
Mensaje de diagnóstico entrante a EDITRAN (NPSI-DATE o GATE).

ZTP0370 INDICACION DE INTERRUPCION
Mensaje de interrupción entrante a EDITRAN (NPSI-DATE o GATE).

ZTP0375 INDICACION DE RESET C:XX D:XX
Mensaje de Reset entrante a EDITRAN (NPSI-DATE o GATE).

ZTP0380 INDICACION LIBERACION C:XX D:XX
Mensaje de liberación de un circuito.

ZTP0385 INDICACION REARRANQUE C:XX D:XX
Mensaje de Rearranque entrante a EDITRAN (NPSI-DATE).

ZTP0390 INICIO DE RECEPCION
Cuando comienza la recepción del fichero remoto.

ZTP0392 INTERFAZ APLICACION DENIEGA PETICION BATCH
EDITRAN/G rechaza la petición realizada por encontrarse en situación incompatible con la petición.

ZTP0395 INTERFASE DE COMUNICACIONES NO CONTEMPLADA
Se recibe un mensaje no acorde con la interfaz de comunicaciones dada de alta en el entorno local.

ZTP0400 INTERFASE NO PRECISA REARRANQUE
Se recibe un mensaje de petición de Rearranque por parte del operador, no necesario para entornos con interfaz de comunicaciones determinadas.

ZTP0405 IMPOSIBILIDAD DE EMISION: PERFIL DEL REMOTO
No se permite la emisión debido a SENTIDO TRAFICO del perfil de la sesión.

ZTP0410 IMPOSIBILIDAD DE RECEPCION: PERFIL DEL REMOTO
Similar al anterior.

ZTP0413 IMPOSIBILIDAD TRANSMISION: FUERA DE HORARIO
Se intenta realizar una transmisión teniendo una ventana horaria en perfiles y estando fuera de ese horario.

ZTP0420 LA LU FICTICIA REMOTA ESTA EN REL C:XX D:XX
Se recibe una liberación **C:00 D:43** que puede ser del ISARD X.25 remoto por tener la LU ficticia en Rel. Se puede recibir de otros entornos en cuyo caso la interpretación que se hace de la liberación no tiene sentido. Suele ser un problema del sistema remoto, no de EDITRAN/P, relacionado con alguna dificultad de redireccionar la llamada a la aplicación.

ZTP0425 LIBERACION DE CNID. C:XX D:=XX
Se ha liberado una llamada que no llegó a conectarse (NPSI-DATE o GATE).

ZTP0435 LIBERACION DEL OPERADOR REMOTO
El operador remoto ha solicitado la liberación.

ZTP0440 LIBERACION POR CRUCE DE LLAMADAS C:XX D:XX
Cuando se produce un cruce de llamadas entre el local y el remoto, el EDITRAN/P con código local menos libera con **C:00 D:04**. En este caso es el local quien ha liberado. Es de suponer que la llamada del remoto prospera.

ZTP0445 LIBERACION POR EL OPERADOR C:XX D:XX
Se ha recibido una liberación **C:00 D:08** con posible procedencia de un EDITRAN/P remoto debido a una petición del operador correspondiente.

ZTP0450 NO UTILIZADO.
No utilizado. En versiones previas (EDITRAN < 2.1) significaba liberación por error compresión.

ZTP0455 LIBERACION POR EXISTIR YA CANAL C:XX D:XX
Se libera una llamada con **C:00 D:05** por ya existir circuito establecido para la sesión. La causa más probable es que EDITRAN/P local tiene registrada la sesión como conectada sin que al remoto le conste.

ZTP0460 LIBERACION FACILIDADES INVALIDAS C:XX D:XX
Se ha producido una liberación con **C:00 D:0A** por facilidades no válidas en el paquete de llamada. Analice el paquete de llamada.

ZTP0465 LIBERACION POR HORARIO INCORRECTO C:XX D:XX
Se ha producido una liberación con **C:00 D:0C** por haber llamado fuera del intervalo horario especificado en l perfil de la sesión..

ZTP0470 LIB. NO ACEPTADO COBRO REVERTIDO C:XX D:XX
Se ha producido una liberación con **C:00 D:06** por venir con facilidad de cobro revertido y tener la sesión COBRO REVERTIDO = N.

ZTP0475 LIB. AL NO EXISTIR CANALES LIBRES C:XX D:XX

Limitación de circuitos, se podrá establecer la conexión una vez libere otra sesión establecida, o bien modificar número máximo de cvc en entorno local.

ZTP0480 LIBERACION POR REARRANQUE DE RED C:XX D:XX
Liberación local o remota **C:00 D:09** por rearranque de la red.

ZTP0485 LIB. FORMA-PAGO INVALIDO PERFILES C:XX D:XX
Se produce una liberación con **C:00 D:07** por no coincidir el TIPO DE PAGO del perfil de la sesión con lo indicado en el paquete de llamada. En concreto, se produce cuando Tipo de Pago = L y la llamada remota no viene a cobro revertido, o cuando Tipo de Pago = R y la llamada viene a cobro revertido.

ZTP0490 LIBERACION TRANSMISION C:XX D:XX
Se ha producido una liberación del circuito que no se traduce en un mensaje determinado. Debe venir acompañado de la Causa y Diagnóstico de la liberación. Para más información ver el Anexo C.

ZTP0495 LOCAL NO PUEDE EMITIR (PERFILES)
Petición de emisión rechazada por no especificarse parámetro 'sentido-tráfico ' con valor 'E' o 'X'.

ZTP0500 LOCAL NO PUEDE LLAMAR (PERFILES)
Petición de conexión rechazada por especificar en parámetro 'extremo-llamante = R', de modo que solo puede llamar el remoto.

ZTP0501 LOCAL NO PUEDE LLAMAR (SESION NO HABILITADA)
Petición de conexión rechazada por especificar en parámetro SESION HABILITADA = 'N' en el perfil de la sesión.

ZTP0505 LOCAL NO PUEDE RECIBIR (PERFILES)
Revisar el parámetro 'sentido de tráfico' .

ZTP0507 LLAMADA CON FACILIDADES NO CONTEMPLADAS
Se recibe una llamada con facilidades no contempladas por el protocolo de transporte.

ZTP0510 LLAMADA REMOTA RECHAZADA (FUERA DE HORARIO)
Petición de conexión fuera de horario. Revisar perfiles.

ZTP0513 CON VERSION 5.2 LA LONGITUD DE TRANSMISION DEBE SER 4050.
Solo se permite longitud de transmisión 4050 a partir de la versión EDITRAN 5.2.

ZTP0515 LLAMADA REM.RECHAZADA (NRI LOC-REM,LUS FICT,TC)
La llamada entrante remota se rechaza con **C:00 D.0D** por no coincidir los siguientes parámetros entre el paquete de llamada entrante y los perfiles de la sesión: las longitudes de los nris (llamado-llamante), los nris (llamado-llamante), la lu ficticia ó el terminal code. Compruebe con el remoto y en la sesión los parámetros descritos.

ZTP0517 LLAMADA REMOTA RECHAZADA (NRIS INVALIDOS)
Similar al mensaje anterior.

ZTP0520 LLAMADA REMOTA ACEPTADA
La llamada remota ha pasado todos los controles de existencia de perfil de la sesión, Nri's locales y remotos y demás parámetros de conexión. Se envía una confirmación al remoto.

ZTP0521 ALGORITMO CONFIDENCIALIDAD EN 2.2 DEBE SER ESPACIOS O DES
En versión criptográfica 2.2 el algoritmo de confidencialidad solo puede tomar los valores DES o Espacios.

ZTP0525 LLAMADA REMOTA ACEPTADA (CRUCE)
Ambos extremos han pedido el establecimiento de conexión y se ha gestionado primero la remota.

ZTP0530 LLAMADA REMOTA ANTERIOR
Ambos extremos han pedido el establecimiento de conexión y se ha gestionado primero la remota.
ZTP0540 LLAMADA REMOTA RECHAZADA (COBRO-REVERTIDO)
La llamada remota se rechaza con **C:00 D.06** por venir con facilidad de cobro revertido y tener la sesión COBRO REVERTIDO = N.
ZTP0541 ALG.CONFIDEN. PUEDE SER DES TD2C TD3C AES AES2 AES3 O ESPACIOS

ZTP0542 ALG.AUTENTIC. PUEDE SER DES O RSA PARA V3.0 Y RSA PARA V4.0

ZTP0543 CON FIRMA SEPARADA (D), DEBE PONER UN DIRECTORIO
Para el tipo de firma DETTACHED el campo nombre o directorio de los ficheros de firma debe estar informado.

ZTP0545 LLAMADA REMOTA RECHAZADA (CRUCE)
Cuando se produce un cruce de llamadas entre el local y el remoto, el EDITRAN/P con código local menor libera con **C:00 D:04**. En este caso es el local quien ha liberado. Es de suponer que la llamada del remoto prospera.

ZTP0550 LLAMADA REMOTA RECHAZADA (EXTREMO-LLAMANTE)
La llamada remota se rechaza con **C:00 D:0E** por tener EXTREMO LLAMANTE = L (Local) en el perfil de la sesión.

ZTP0551 LLAMADA REMOTA RECHAZADA (SESION NO HABILITADA)
La llamada remota se rechaza con **C:00 D:0D** por tener SESION HABILITADA = 'N' en el perfil de la sesión.

ZTP0555 LLAMADA REM.RECHAZADA (SESION/PARM DESCONOCIDOS)
Se rechaza la llamada entrante del remoto por no estar dada de alta la sesión en el local. También puede ser debido a que no coincide la versión de EDITRAN/P, el tipo de conexión o el identificador de acceso en los perfiles de sesión local y remota. El remoto recibe una liberación con Causa **00** y Diagnóstico **0D**.

ZTP0560 LLAMADA REMOTA RECHAZADA (SIN CANAL)
Se rechaza la llamada remota por sobrepasar el nº máximo de cvc reflejado en entorno local.

ZTP0565 LLAMADA REMOTA RECHAZADA (FORMA DE PAGO)

La llamada remota se rechaza con **C:00 D:07** por no coincidir la FORMA DE PAGO del perfil de la sesión con lo indicado en el paquete de llamada. En concreto, se produce cuando Forma de Pago = L (local) y la llamada remota no viene a cobro revertido, o cuando Forma de Pago = R (Remoto) y la llamada viene a cobro revertido.

ZTP0570 LLAMADA REMOTA RECHAZADA (YA HAY CVC)
Se libera una llamada del remoto con **C:00 D:05** por ya existir circuito establecido para la sesión. La causa más probable es que EDITRAN/P local tiene registrada la sesión como conectada sin que al remoto le conste. El local debe de solicitar la liberación con la opción 3 del Operador de EDITRAN/P.

ZTP0575 MENSAJE NPSI/DATE INCORRECTO
Se ha recibido un mensaje (NPSI-DATE) desconocido.

ZTP0580 MENSAJE DE NOTIFICACION INCORRECTO
Se ha recibido un mensaje de notificación fuera de especificaciones.

ZTP0585 MENSAJE RECIBIDO CON CRC INVALIDA
Se ha recibido un mensaje del remoto y calculando su CRC no coincide con el que viene en el propio mensaje. Problema de integridad del mensaje recibido. Debe ser muy poco frecuente ya que en caso contrario puede darse un mal funcionamiento en alguno de los equipos de comunicaciones, configuración de líneas inadecuadas a sus características, etc. Puede exigir trazas de línea en los dos extremos para su diagnóstico.

ZTP0590 NO EXISTE CONEXION
Se ha hecho una petición que requería previamente el establecimiento de conexión.

ZTP0595 NO EXISTE PROCEDIMIENTO EN PERFILES
Se ha solicitado desde una aplicación el lanzamiento por EDITRAN/P de un proceso previo/posterior a emisión/recepción y no existe el procedimiento correspondiente en el perfil de la sesión.

ZTP0605 NO EXISTE SESION EN PERFILES
Se ha hecho una petición a EDITRAN/P de una sesión y no está dada de alta en perfiles.

ZTP0607 NO REALIZA LLAMADA. LU FICTICIA XXXX EN REL
Se intenta hacer una llamada y la LU ficticia está en REL, se intenta activar y agotados los reintentos sigue sin estar activada. Comprobar la línea X.25

ZTP0610 NO SE ESTA EMITIENDO
Estando en conectado, se recibe una petición local desde la interfaz de fin de emisión.

ZTP0612 NO SE ESTA RECIBIENDO
Estando en conectado, se recibe una petición local desde la interfaz de fin de recepción.

ZTP0620 NO HAY CANALES LIBRES (AGOTADO NRO. CVCS)
Ya existen tantas sesiones gestionadas por EDITRAN/P como las especificadas en NRO. CVC MAXIMO en el perfil del Entorno Local Principal, por lo que no se acepta otra solicitud de conexión.

ZTP0625 NOTIFICACION BATCH: TAMPON EMISOR PREPARADO
La interfaz de aplicación notifica al núcleo que se ha realizado una carga de datos en el fichero tampón de emisión y queda disponible para EDITRAN/P local o remoto.

ZTP0627 NOTIFICACION BATCH: TAMPON RECEP. PREPARADO
La interfaz de aplicación notifica al núcleo que se ha realizado una inicialización del fichero tampón de recepción y queda disponible para EDITRAN/P.

ZTP0630 NUMERO SESION DE INTERCAMBIO INCOMPATIBLE
El Número de Sesión de Intercambio del fichero tampón receptor y emisor de la parte Local y Remota no coinciden. Es necesario que coincidan en ambos extremos. Inicializar los estados de EDITRAN/G, poniendo el número de sesión de intercambio correcto. Normalmente lo tiene que hacer el receptor, ya que si lo hace el emisor obliga a que se cargue nuevamente el fichero. Pedir nuevamente la recepción.

ZTP0635 OPERADOR DEBE CHEQUEAR MCH
Ha entrado un mensaje error-information report (NPSI-DATE). Es posible que EDITRAN subsane el problema. En caso contrario remitirse al mensaje.

ZTP0645 PERDIDA SECUENCIA EN PROCESO EMISOR
Se ha detectado salto en número de secuencia del mensaje. Posible problema de CRC inválido.

ZTP0650 PERDIDA SECUENCIA EN PROCESO RECEPTOR
Se ha detectado salto en número de secuencia del mensaje. Posible problema de CRC inválido.

ZTP0655 PERFILES INCOMPATIBLES (COMPRESION)
La petición de emisión del remoto se rechaza por tener distinto parámetro COMPRESION en los perfiles de la sesión. No debería producirse este mensaje ya que este parámetro se comprueba previamente en el establecimiento de la sesión. Proviene de versiones anteriores de EDITRAN/P.

ZTP0660 PERFILES INCOMPATIBLES (SENTIDO TRAFICO)
Se rechaza la petición de emisión del remoto por no permitirlo el SENTIDO TRAFICO del perfil de la sesión.

ZTP0670 PERFILES SIN CARACTERISTICAS LOCALES
Dar de alta registro de entorno.

ZTP0675 PETICION BATCH DE DESCARGA DE EMISION
Se ha recibido una petición desde batch de lanzamiento del posterior a emisión especificado en perfiles.

ZTP0680 PETICION BATCH DE DESCARGA DE RECEPCION
Se ha recibido una petición desde batch de lanzamiento del posterior a recepción especificado en perfiles.

ZTP0685 PETICION BATCH DE INICIO DE EMISION
Se ha recibido una petición batch de comienzo de emisión local.

ZTP0690 PETICION BATCH DE INICIO DE RECEPCION
Se ha recibido una petición batch de comienzo de recepción local.

ZTP0700 PETICION BATCH DE CARGA E INICIO DE EMISION
Se ha recibido una petición desde batch de lanzamiento de un trabajo especificado en perfiles.

ZTP0705 PETICION BATCH DE CARGA DE EMISION
Se ha recibido una petición desde batch de lanzamiento de un trabajo especificado en perfiles.

ZTP0710 PETICION BATCH DE PREP. E INICIO DE EMISION
Se ha recibido una petición desde batch de lanzamiento de un trabajo especificado en perfiles.

ZTP0715 PETICION BATCH DE PREPARACION DE RECEPCION
Se ha recibido una petición desde batch de lanzamiento de un trabajo especificado en perfiles.

ZTP0720 PETICION DE RECEPCION AL REMOTO
Se ha recibido una petición local para el comienzo de la emisión remota.

ZTP0735 POSTERIOR EMISION FINALIZADO CORRECTAMENTE
La interfaz comunica que ha finalizado el proceso posterior a emisión que se solicitó desde EDITRAN/P.

ZTP0740 POSTERIOR RECEPCION FINALIZADO CORRECTAMENTE
Similar al anterior relativo al proceso posterior a recepción.

ZTP0745 PREVIO A EMISION FINALIZADO CORRECTAMENTE
Similar al anterior relativo al proceso previo a emisión.

ZTP0750 PREVIO A RECEPCION FINALIZADO CORRECTAMENTE
Similar al anterior relativo al proceso previo a recepción.

ZTP0752 PROCEDIMIENTO PREVIO EN POSIBLE EJECUCION
Sin haber recibido respuesta del proceso lanzado por EDITRAN/P, se realiza una nueva petición.

ZTP0755 PRINCIPIO DE SESION. EMISION LOCAL
Se ha enviado la primera ráfaga de la transmisión.

ZTP0760 REALIZA LA LLAMADA
EDITRAN/P local realiza una llamada al remoto como consecuencia de una petición de conexión del operador (opción 2) o de una petición de emisión o recepción del operador o Interfaz cuando no existe conexión y CONEXIÓN AUTOMATICA = S en el perfil de la sesión.

ZTP0765 REALIZA LLAMADA POR INF. REPORT
Se ha recibido un mensaje error-information report en NPSI-DATE, con diagnóstico de reintentar llamada.

ZTP0770 REARRANQUE DE RED DE OPERADOR REMOTO
Se recibe del remoto una solicitud de liberación por rearranque de su red.

ZTP0780 RECEPCION CORRECTA Y FINALIZADA
Cuando se da por terminada una transmisión recepción.

ZTP0790 RECIBIDO MENSAJE INCORRECTO DESDE BATCH
Petición batch fuera de protocolo.

ZTP0800 RECIBIDO MENSAJE INCORRECTO EN EMISION
Mensaje fuera de protocolo.

ZTP0805 RECIBIDO MENSAJE INCORRECTO EN RECEPCION
Mensaje fuera de protocolo.

ZTP0810 RECUPERACION DE CIRCUITOS
En ISARD X.25 se ha recibido un mensaje FB de rearranque de red que puede estar originado por una petición del operador de EDITRAN/P con la opción 9, o puede ser debido a que una LU ficticia asociada a una línea local se ha "adquirido" (ACQ) por el CICS donde se ejecuta el EDITRAN/P. También puede ser provocado por la primera petición de conexión local por una LU ficticia determinada.

ZTP0815 REINTENTO PARA ESTABLECER SESION
Se detecta time-out para establecer sesión y se solicita al remoto la misma.

ZTP0816 REINTENTO DE ESPERA DE SAP
Se detecta time-out para que el remoto nos envíe SAP. Se relanza hasta fin de reintentos.

ZTP0820 SES/PARAMETROS ERRONEOS EN REMOTO C:XX D:XX
Se recibe una liberación **C:00 D:0D** siendo el caso más probable que EDITRAN/P remoto rechaza la llamada del local por no identificar la Sesión o por comprobación de Nri's (consulte los diagnósticos de liberación).

ZTP0825 SBP RECIBIDO EN ESTADO INCORRECTO
Mensaje fuera de protocolo.

ZTP0835 SE RECIBE DESCUADRE DE TOTALES REMOTO
Mensaje en desuso. En una transmisión de una aplicación con control de totales (valor T en perfiles), el remoto tiene un descuadre en la suma de los importes de dicha aplicación.

ZTP0840 SE ESTA EMITIENDO. SE IGNORA PETICION BATCH
Se ha recibido una petición batch de emisión, que no será procesada, por estar emitiendo.

ZTP0845 SE ESTA RECIBIENDO. IGNORADA PETICION BATCH
Se ha recibido una petición batch de recepción, que no será procesada, por estar recibiendo.

ZTP0847 SE LANZA BATCH DE EXCEPCION. REF: XXXX
Se ha lanzado proceso de excepción según perfiles con un código de referencia.

ZTP0850 SE HA LANZADO BATCH POSTERIOR A EMISION
Se ha lanzado proceso batch según perfiles.

ZTP0855 SE HA LANZADO BATCH POSTERIOR A RECEPCION
Se ha lanzado proceso batch según perfiles.

ZTP0860 SE HA LANZADO BATCH PREVIO A EMISION
Se ha lanzado proceso batch según perfiles.

ZTP0865 SE HA LANZADO BATCH PREVIO A RECEPCION
Se ha lanzado proceso batch según perfiles.

ZTP0870 ERROR EXIT DE USUARIO. CGO.RESULTADO
Error de proceso en la exit de usuario codificada en perfiles.

ZTP0871 ERROR EXIT DE USUARIO. PGMIDERR. EXIT:XXXXXXXX
No existe la exit de usuario especificada en perfiles.

ZTP0872 PROCESO INTERFERIDO POR EXIT DE USUARIO. XXXXXXXX
La exit de usuario interfiere un proceso y no permite la realización de alguna acción a EDITRAN.

ZTP0885 SEP RECIBIDO EN ESTADO INCORRECTO
Mensaje fuera de protocolo.

ZTP0895 SESION ESTABLECIDA
Se han intercambiado mensajes de notificación y ambos extremos están en sesión.

ZTP0900 SESION NO ESTABLECIDA
Se ha recibido una petición del remoto o del operador local sin estar establecida la sesión.

ZTP0905 SESION RECHAZADA PERFILES (ASCII/EBCDIC)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0910 SESION RECHAZADA POR PERFILES (CALCULO CRC)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0915 SESION RECHAZADA PERFILES (CALIDAD SERVICIO)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0920 SESION RECHAZADA PERFILES (CONTROL TOTALES)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0925 SESION RECHAZADA POR PERFILES (COMPRESION)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0930 SESION RECHAZADA PERFILES (CRIPTOGRAFIA)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0935 SESION RECHAZADA PERFILES (LONGITUD REG.)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0940 SESION RECHAZADA PERFILES (TIPO APLICACION)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0945 SESION RECHAZADA POR PERFILES (TIPO CONEX.)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0950 SESION RECHAZADA POR PERFILES (VERSION)
Ambos extremos no están de acuerdo en dicho parámetro.

ZTP0951 VERSION EDI REMOTA DISTINTA. SIGUE PROCESO
Ambos extremos no están de acuerdo en dicho parámetro, pero continua el proceso como si no hubiera ocurrido nada.

ZTP0955 SE SOLICITA CAMBIO DE CLAVE LOCAL
En el establecimiento de sesión el extremo local pide cambiar su clave al remoto.

ZTP0960 SE SOLICITA CAMBIO DE CLAVE REMOTA
En el establecimiento de sesión el extremo remoto pide cambiar su clave al local.

ZTP0965 SOLICITADA LIBERACION POR OPERADOR LOCAL
El operador local ha pedido la liberación de la sesión.

ZTP0966 SOLICITADA LIBERACION POR EXCESO DE TIEMPO
La sesión estaba parada. Ha transcurrido más de 1 hora desde el último evento. Se libera y si estaba en transmisión, se reconecta.

ZTP0970 SOLICITUD REARRANQUE C:XX D:XX
Solicitud Rearranque por operador (ISA/X.25 y NPSI-DATE o GATE).

ZTP0975 START A TRANSACCION ERRONEA XXXX
Revisar transacciones especificadas en entorno o en petición de consultas de aplicación (buzón erróneo).

ZTP0980 START A TRANSACCION NO AUTORIZADA
Transacción protegida por el sistema.

ZTP0985 FICHERO TAMPON EMISOR REMOTO INACCESIBLE
Respuesta a consulta de fichero emisión remoto.

ZTP0990 FICHERO TAMPON RECEPTOR REMOTO INACCESIBLE
Respuesta a consulta de fichero recepción remoto.

ZTP0992 FICHERO REMOTO NO PREPARADO (LANZA PREVIO)
El remoto rechaza petición local por no tener su fichero tampón preparado. Se ha lanzado su automatismo previo correspondiente a la petición. Si el remoto lo tiene permitido en el perfil de la sesión, su EDITRAN/P tomará la iniciativa cuando se haya preparado su tampón emisor, en caso contrario el local debe solicitar de nuevo la recepción.

ZTP0993 FICH.REMOTO NO PREPARADO (NO EXISTE PREVIO)

El remoto no tiene el fichero preparado y no tiene especificados los automatismos (procedimiento previo en perfiles)

ZTP0994 FICHERO REMOTO NO PREPARADO (NO DISPONIBLE)
El fichero tampón remoto está en un estado no disponible para EDITRAN, lo tiene la interfaz.

ZTP0995 FICHERO REMOTO INCOMPATIBLE (NUMERO SESION)
Se rechaza la transmisión por no coincidir el número de sesión de intercambio de los dos tampones. Dicho número deberá coordinarse con el remoto. La operatoria a seguir depende de la interfaz usada. Si es EDITRAN/G, la más frecuente, el local deberá inicializar el estado de recepción con el número indicado por el remoto e inicializar el tampón receptor.

ZTP0996 FICH.REMOTO INCOMP.(REG.TOTALES-FECHA CREACION)
Número de registros totales del fichero tampón de recepción remoto distintos que del fichero emisión local. También se puede dar con igual número de registros. En todos los casos, se debe a que el receptor, ya tenía parte de fichero recibida, se liberó la transmisión y el emisor cargó de nuevo (el mismo o distinto contenido), de forma que el receptor lo detecta a través de la fecha de creación de su tampón receptor. Como el receptor no sabe si ha variado entre una carga y otra el contenido, rechaza. La forma de salir es avisar al receptor para que inicialice la la recepción y volver a comenzar desde el prinicipio. La fecha de creación del tampón receptor se actualiza con la del tampón emisor, sólo en el primer comienzo de la primera transmisión (cuando todavía no tiene ningún registro confirmado).

ZTP0997 FICHERO REMOTO INCOMPATIBLE (ID.CONFIR.APL)
El fichero tampón receptor remoto espera recibir el mismo identificador de aplicación que se 25imul en el SCP, pero no coincide y el extremo remoto tiene sincronismo aplicación 'Q'.

ZTP1000 TERMINAL DE RED INVALIDO XXXX
Revisar terminal e idnum dado de alta en perfiles.

ZTP1003 TERMINAL NO ADQUIRIDO XXXX
Al ir a enviar un mensaje al remoto, se detecta que la LU real no está adquirida por el CICS. Habrá que comprobar la situación de dicha LU. En ISARD X.25 el TERMINAL LOCAL e IDNUM deberán ser correctos y corresponderse. En NPSI las lu's del nodo mayor conmutado deben especificar IDNUM'S correctos de acuerdo con la generación de la línea y los parámetros de la línea local en el perfil de la sesión deber ser correctos.

ZTP1005 TIPO DE CONEXION PAD PRIVADO NO PUEDE LLAMAR
Se recibe una petición local de conexión para un remoto definido con tipo de conexión PAD PRIVADO.

ZTP1007 TIPO DE CONEXION PAD PUBLICO NO PUEDE LLAMAR
Se recibe una petición local de conexión para un remoto definido con tipo de conexión PAD PUBLICO.

ZTP1008 TIPO DE CONEXION EDTX POR PAD NO PUEDE LLAMAR
Se recibe una petición local de conexión para un remoto definido con tipo de conexión EDI/TX con PAD PUBLICO.

ZTP1010 TODAVIA SE ESTA TRANSMITIENDO
Petición no procesada por encontrarse en transmisión.

ZTP1020 YA EXISTE CONEXION DE TRANSPORTE
Se ha solicitado la conexión de una sesión por el operador de EDITRAN/P o por una interfaz y ya está conectada dicha sesión.

ZTP1025 YA SE ESTA RECIBIENDO
Se recibe petición duplicada por parte del operador.

ZTP1030 YA SE ESTA EMITIENDO
Se recibe petición duplicada por parte del operador.

ZTP1035 YA SE HABIA LLAMADO ANTES
Se ha recibido una petición de conexión cuando ya se procesaba una anterior a la misma sesión.

ZTP1040 TAMPON CARGADO CON LONG. XXXX (<> PERFILES)
El fichero tampón ha sido cargado con una longitud diferente a la especificada en perfiles. Vuelva a cargar el tampón o modifique la longitud de transmisión en el perfil de la sesión.

ZTP1045 TAMPON CON COMPRESION (INCOMPATIB.PERFILES)
El fichero tampón de emisión ya ha sido cargado mediante batch con compresión (compresor LZW) y en perfiles está especificado compresión por ristras. No son compatibles las dos compresiones.

ZTP1050 TAMPON CIFRADO INCOMPATIBLE CON PERFIL: XXXXXXXX

ZTP1055 NO EXISTE LA CLAVE QUE CIFRO TAMPON EMISION
Mientras se está realizando una carga de datos batch con cifrado, se realiza un cambio de clave.

ZTP1060 CAMBIO CLAVE INCOMPATIB. CON TAMPON CIFRADO
Se ha realizado una carga batch de datos y se ha cifrado. No se permite un cambio de clave cuando se ha cifrado batch.

ZTP1065 LONG.TRANS.INCOMPATIBLE CON TAMPON RECEPTOR
Se intenta realizar una transmisión con una long. De datos y el receptor espera otra.

ZTP1070 LU REAL CAIDA. MENSAJE X25 GATE NO ENVIADO
No se puede liberar por tener la LU real fuera de servicio.

ZTP1075 LU REAL CAIDA. MENSAJE DE DATOS GATE NO ENVIADO
La LU real no ha entrado en tráfico de datos. Revisar con CEMT.

ZTP1080 ERROR CVC NO ENCONTRADO EN COLA DE ESTADOS
Mensaje ignorado por no encontrar CVC.

ZTP1085 CIRCUITO CONECTADO. IMPOSIBILIDAD DE LIBERACION
No ha entrado un paquete de liberación y el local no puede liberar por no estar la LU real en ACQ.

ZTP1090 LLAMADA RECHAZADA. TAMAÑO PAQUETE ERRONEO
El tamaño de paquete no es correcto.

ZTP2005 ERROR CICS FN:XXXX RES: XX/XX TRN: XXXX R: XXXXXXXX
Esto ocurre cuando se produce un ABEND en el CICS. FN: es el comando CICS que se estaba ejecutando en ese momento. RES: es el código de respuesta EIBRESP. TRN: es la transacción que produce el ABEND. R: es el recurso utilizado.

ZTP2010 SESION RECHAZADA POR PARAMETROS VARIABLES
Error interno.

ZTP2015 SESION RECH. POR TIPO REPRESENTACION.
Error interno.

ZTP2020 SESION RECH. POR LONG. PARM. VBLES.
Error interno.

ZTP2025 ERROR VARIABLE XXXXXXXXXXXXXXX CGO.: XXXX
Dicha variable corresponde a los parámetros de sesión que tienen que estar codificados de igual forma en los dos extremos. Si en alguno de los extremos no coincide, saldrá este error indicando la variable.

ZTP2026 RDO. VARIABLE XXXXXXXXXXXXXXX CGO.: XXXX
Dicha variable corresponde a los parámetros de sesión que NO tienen que estar codificados de igual forma en los dos extremos. Si en alguno de los extremos no coincide, saldrá este error indicando la variable, aunque continua el proceso normalmente.

ZTP2030 SAR IGNORADO POR IDENTIFICADOR DE SESION.
Se intenta establecer sesión, y queda un mensaje SAP encolado para enviar al remoto ó para recibir desde el remoto. En una transmisión posterior, sale dicho mensaje, además del SAP correspondiente a la transmisión en curso. Al remoto, en primer lugar, le llega el de la primera transmisión (el encolado), de forma que lo contesta con un SAR. Cuando llega el SAR al extremo que inició el SAP de la segunda transmisión se da cuenta de que no corresponde a la misma, por lo que lo rechaza. Esto evita que si se han modificado los perfiles entre ambas transmisiones, se acepte algo que más tarde va a fallar. Normalmente, se sale automáticamente de dicha situación, si no es así reintente la transmisión.

ZTP2035 ESTADO INCONGRUENTE EN FICHERO DE MONITORIZACION

ZTP2040 INICIALIZACION EMISION PEDIDA POR INTERFAZ APL.

ZTP2045 INICIALIZACION RECEPCION PEDIDA POR INTERFAZ AP.

ZTP2050 INICIO TRANSMISION SIN FINAL PROCESO POSTERIOR.

ZTP2060 ERR. TCP MACRO XXXXXXXXXXXXXX XX-XX.ERRNO=XXXXX

Se ha producido un error en la macro especificada para TCP/IP. Revise documentación específica de IBM. Para causa y diagnóstico XX-XX puede consultar en menú ZTBM la opción "CAUSA Y CODIGOS DE ERROR TCP/IP".

ZTP2061 ERR. TCP MACRO XXXXXXXXXXXXXX XX-XX. RTCD=XXXXX
Se ha producido un error en la macro especificada para TCP/IP. Revise documentación específica de IBM. Para causa y diagnóstico XX-XX puede consultar en menú ZTBM la opción "CAUSA Y CODIGOS DE ERROR TCP/IP".

ZTP2062 ERR. TCP PROG. XXXXXXXXXXXXXX XX-XX. RTCD=XXXXX
Se ha producido un error en los programas de IBM especificados para TCP/IP. Revise documentación específica de IBM. Para causa y diagnóstico XX-XX puede consultar en menú ZTBM la opción "CAUSA Y CODIGOS DE ERROR TCP/IP".

ZTP2063 ERROR TCP/IP. XXXXXXXXXXXXXX XX-XX.
Se ha producido un error en procesos TCP/IP. Para causa y diagnóstico XX-XX puede consultar en menú ZTBM la opción "CAUSA Y CODIGOS DE ERROR TCP/IP".

ZTP2161 TIPO CONEX. TCP/IP ERR. TRAN. CLIENTE EN ENTORNO
Se intenta pedir una solicitud de conexión TCP/IP y no se ha incluido en el entorno la transid CLIENTE TCP (TRANSID API TCP). Modifique entorno incluyendo dicho parámetro.

ZTP2162 TIPO CONEX. TCP/IP ERR. TRAN. SERVIDOR EN ENTORNO.
Mensaje en desuso.

ZTP2163 TIPO CONEXION TCP/IP SIN TCPNAME EN ENTORNO
Se intenta pedir una solicitud de conexión TCP/IP y no se ha incluido en el entorno el address space del stack TCP (TCPNAME). Modifique entorno incluyendo dicho parámetro.

ZTP2164 ERROR SERVER (API-CONEX) : XXXX- XXXXX
Error al establecer la conexión con el servidor EDITRAN/CD. Las causas-diagnósticos del error se especifican en el anexo F.

ZTP2165 SE SOLICITA CANAL CERTIFICADO LOCAL
Se solicita un canal certificado local, a través de llamada al EDITRAN/CD.

ZTP2166 SE SOLICITA CANAL CERTIFICADO REMOTO
El extremo remoto ha solicitado un canal certificado, a través de llamada al EDITRAN/CD.

ZTP2167 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Texto del error indicado por el EDITRAN/CD. También sirve para dar errores de detalle.

ZTP2170 NO EXISTE REGISTRO DE CONTROL XXXXXX
Edltran/P intenta acceder al tampón y no existe el registro de control. En ocasiones puede ser una situación correcta. En la mayoría de los casos se trata de un mensaje informativo.

ZTP2175 SE PLANIFICA REINT. VENT. HORARIA- XXXXXXXX
Edltran/P al llegarle una petición local de emisión ó recepción, verifica que el parámetro reintentar ventanta horaria está activo, por lo que planifica dicha petición a la hora de inicio indicada en la sesión (ya sea de ese día o del siguiente).

ZTP2180 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Texto del error indicado por el control de licencias. Contacte con INDRA para actualizar su licencia.

ZTP2185 VERSION EDI IGNORADA POR CONTROL DE FECHAS.
EdItran/P al llegarle una petición de establecimiento de sesión detecta que la diferencia de fechas del sistema local y remoto es superior a 48 horas. Notifiquelo al remoto para que este inroduzca la fecha correcta.

ZTP2190 TIPO CONEXION PROXY SIN IP-PROXY EN ENTORNO
Se intenta pedir una solicitud de conexión PROXY y no se ha incluido en el entorno la dirección ip del proxy. Modifique entorno incluyendo dicho parámetro.

ZTP2191 TIPO CONEXION PROXY CON VERSION-REMOTA < 41.
Con tipo-conexión proxy, sólo se permite versión-EDITRAN-p-remota 4.1. Modifique versión y comunique al remoto que haga lo mismo.

ZTP2195 RECIBIDO MSG SWIFT. PERFIL NO ADECUADO EN SESION.
Se recibe una indicación de swr (del servidor EDITRAN swift), pero la sesión no tiene el parámetro swift activo.

ZTP2196 POSTERIOR A EMISION NO LANZADO. DATOS EN SWIFT.
En la sesión definida con parámetro swift activo, no se lanza el posterior a emisión, hasta no recibir confirmación del servidor swift.

ZTP2197 RECIBIDO MSG SWIFT. TIPO DE MENSAJE DESCONOCIDO.
Error interno.

ZTP2198 RECIBIDO MSG SWIFT. IDENTIFICADOR DESCONOCIDO.
En la sesión definida con parámetro swift activo, se recibe una confirmación del servidor, que no corresponde a la última transmisión conocida.

ZTP2199 RECIBIDO MSG SWIFT. TAMPON ESTADO INCOMPATIBLE.
En la sesión definida con parámetro swift activo, se recibe una confirmación del servidor, pero el tampón emisor ya no se encuentra en estado adecuado.

ZTP2200 RECIBIDO MSG SWIFT. EMISION NO PROCESADA TODAVIA.
En la sesión definida con parámetro swift activo, se recibe una confirmación del servidor, indicando que no conoce aún el resultado del proceso de la emisión SWIFT.

7. ANEXO B. PROCEDIMIENTO DE EXCEPCION .

El procedimiento de excepción, es ejecutado por EDITRAN con un mensaje A7I cuando ocurre una incidencia que impide realizar una emisión o recepción completa. Para que se genere es necesario que se estuviera emitiendo – recibiendo ó que se tuviera intención de ello. El procedimiento de excepción se arranca con un parm Xzzz, donde X indica si el problema es de ®misión ó ®ecepción, y zzz indica el código de referencia de l problema. Si se estuviera emitiendo-recibiendo 30simultáneamente, en algunas ocasiones se generan 2 A7I (uno Exxx y otro Rxxx). Una vez recibido el código A7I, se debe hacer lo siguiente:

- θ Informar al Operador de la Instalación, de la Incidencia con el comentario correspondiente. En los no reintentables, es probable que tenga que contactar con el operador remoto para solventar la situación.
- θ Dependiendo del Código de Referencia del mensaje A7I puede reintentar la emisión o la recepción de la Sesión implicada. Existe un subconjunto de Códigos de Referencia ante los cuales no se debe reintentar si no se repara el error (para evitar el riesgo de bucle). Los demás Códigos es posible reintentar para finalizar la transmisión completa, aunque se debe reintentar un número finito de veces, pues siempre es posible que debido a un error inesperado se llegue a una situación de bucle.

7.1. TABLA DE CODIGOS DE INCIDENCIAS A7I.

Estos Códigos son los que aparecen a continuación con su correspondiente comentario explicativo:

	EMISION
E010	FIN DE EMISION POR PETICION DE LIBERACION DE OPERADOR (E11).
E020	FIN DE EMISION POR TAMPON RECEPTOR REMOTO INCORRECTO. LANZA PREVIO.
E021	FIN DE EMISION POR TAMPON RECEPT. REMOTO INCORRECTO.NO EXISTE PREVIO
E022	FIN EMISION POR TAMPON RECEPT. REM. INCORRECTO.PREVIO EN EJECUCION.
E023	FIN DE EMISION POR TAMPON RECEPTOR REMOTO INCORRECTO. NUMERO SESION NO COINCIDE
E024	FIN DE EMISION POR TAMPON RECEPTOR REMOTO INCORRECTO. NUM.REGISTROS TOTALES DE EMISION MENOR A RECEPCION.
E025	**NO UTILIZADO.**
E026	FIN DE EMISION POR ERRORES AL COLOCAR EL TAMPON EMISOR EN LA RED SWIFT.
E027	FIN DE EMISION POR TOTALES INCOMPATIBLES EN FICHERO TAMPON REMOTO
E030	FIN DE EMISION DEBIDO A PETICION DE LIBERACION REMOTA.
E040	FIN DE EMISION POR EXCESO REINTENTOS DE INICIO DE SESION (STR).
E050	FIN DE EMISION POR ERROR PROTOCOLO PETICION INICIO DE SESION (SCR). **NO UTILIZADO**
E060	FIN DE EMISION POR ERROR PROTOCOLO CONFIRMACION SINCRONISMO (SBR).
E070	FIN DE EMISION POR EXCESO DE REINTENTOS SINCRONISMO (STR/SBP).
E080	FIN DE EMISION POR ERROR PROTOCOLO CONFIRMACION FIN FICHERO (SER). **NO UTILIZADO**
E090	FIN DE EMISION POR EXCESO REINTENTOS FIN TRANSMISION (STR).
E100	FIN DE EMISION POR ERROR ASOCIACION POR PARAMETROS INCOMPAT(SAP/SAR)
E110	FIN DE EMISION POR ERROR ASOCIACION POR CRIPTOGRAFIA (SAP/SAR).
E120	FIN DE EMISION POR EXCESO DE REINTENTOS DE ASOCIACION (STN).
E130	FIN DE EMISION POR EXCESO DE REINTENTOS CONEXION (STC).
E140	IMPOSIBILIDAD DE EMISION POR PERFILES DE SESION (ECP).
E150	IMPOSIBILIDAD DE EMISION POR FICH. TAMPON EMISOR NO DISPONIBLE (ECP)
E200	IMPOSIBILIDAD DE EMISION POR ERROR PREVIO EMISION (A1R).
E210	IMPOSIBILIDAD DE EMISION POR ERROR DE LINEA.
E220	IMPOSIBILIDAD DE EMISION POR ERROR DE COMPRESION O CRIPTOGRAFIA.

E230	IMPOSIBILIDAD DE EMISION POR HORARIO LOCAL NO PERMITIDO.

	RECEPCION
R010	FIN RECEPCION POR PETICION DE LIBERACION DE OPERADOR (E11).
R020	FIN RECEPCION POR TAMPON EMISOR REMOTO INCORRECTO. LANZA PREVIO.
R021	FIN RECEPCION POR TAMPON EMISOR REM. INCORRECTO. NO EXISTE PREVIO.
R022	FIN RECEPCION POR TAMPON EMISOR REM. INCORRECTO. PREVIO EN EJECUCION
R027	FIN DE RECEPCION POR TOTALES INCOMPATIBLES EN FICHERO TAMPON REMOTO
R030	FIN RECEPCION DEBIDO A PETICION DE LIBERACION REMOTA
R040	FIN RECEPCION POR EXCESO REINTENTOS DE INICIO DE RECEPCION (STP).
R050	FIN RECEPCION POR ERROR PROTOCOLO PETICION INICIO DE RECEPCION (SCP). **NO UTILIZADO**
R060	FIN RECEPCION POR ERROR PROTOCOLO EN PETICION SINCRONISMO (SBP).
R080	FIN RECEPCION POR ERROR PROTOCOLO PETICION FIN FICHERO (SEP). **NO UTILIZADO**
R100	FIN DE RECEPCION POR ERROR ASOCIACION POR PARAMET. INCOMPAT(SAP/SAR)
R110	FIN DE RECEPCION POR ERROR ASOCIACION POR CRIPTOGRAFIA (SAP/SAR).
R120	FIN DE RECEPCION POR EXCESO DE REINTENTOS DE ASOCIACION (STN).
R130	FIN DE RECEPCION POR EXCESO REINTENTOS CONEXION (STC)
R140	IMPOSIBILIDAD DE RECEPCION POR PERFILES DE SESION (ECP).
R150	IMPOSIBILIDAD DE RECEPCION POR FICH.TAMPON DE REC.NO DISPONIBLE(ECP)
R155	IMPOSIBILIDAD DE RECEPCION POR FICH.TAMPON DE RECEP. SIN ESPACIO.
R200	IMPOSIBILIDAD DE RECEPCION POR ERROR PREVIO RECEPCION (A2R).
R210	IMPOSIBILIDAD DE RECEPCION POR ERROR DE LINEA
R220	IMPOSIBILIDAD DE RECEPCION POR ERROR DE COMPRESION O CRIPTOGRAFIA.
R230	IMPOSIBILIDAD DE RECEPC. POR HORARIO LOCAL NO PERMITIDO.

7.2. TABLA DE CODIGOS A7I (REINTENTABLES - NO REINTENTABLES).

Se enumeran los códigos A7I en función de reintentables o no por la aplicación.

- θ Los Códigos no reintentables son:

E: 010, 020, 022, 023, 024, 100, 110, 140, -----, 200, 230
R: 010, 020, 022, -----, -----, 100, 110, 140, 155, 200, 230
(Nota: 020 y 022 sólo si EXTREMO-LLAMANTE="X" o "R" de la Sesión implicada).

- θ Los Códigos en los que **se puede reintentar un número de veces finito** (en otro caso puede haber situación de bucle) son:

E: 020, 022, 025, 030, 040, 050, 060, 070, 080, 090, 120, 130, 150, 210
R: 020, 022, 025, 030, 040, 050, 060, -----, 080, ----, 120, 130, 150, 210
(Nota: 020 y 022 sólo si EXTREMO-LLAMANTE="L" de la Sesión implicada).

7.3. TABLA DE CODIGOS A7I (GENERACION DE ALARMAS).

Cuando se ejecuta el procedimiento de excepción, si se tienen contratadas estadísticas, se genera alarma (externa, sms ó e-mail en función del código A7I):

- θ Los Códigos que generan alarma son:

E: 010, 021, 022, 023, 024, 025, 030, 040, 050, 060, 070, 080, 090,100, 110, 120, 130, 140, 150, -----, 210, 220, 230
R: 010, 021, 022, ----, -----, -----, 030, 040, 050, 060, -----, 080, ----, 100, 110, 120, 130, 140, 150, 155, 210, 220, 230

- θ Los Códigos que no generan alarma son:

E: 020, 200
R: 020, 200

7.4. TABLA DE CODIGOS A7I (CAMBIO DE ESTADO DEL TAMPON).

En función del código A7I, se cambia el estado del tampón a no disponible (es necesario en este caso que se ejecute un nuevo procedimiento antes de volver a emitir-recibir) ó se deja

como estuviera. Por ello es conveniente que cuando ocurra esta circunstancia los Procedimientos de Usuario o Interfaz de Aplicación obren en consecuencia si desean que EDITRAN vuelva a emitir (ponga ESTADO-TAMPON a "C").

- Los Códigos que dejan el tampón no disponible (ESTADO-TAMPON a valor "I") son:

E: 010, 021, 023, 024, 025, 026, 027, 100, 110, 200, 210
R: 010, 021, -----, -----, -----, ---, --- , 100, 110, 200, 210

- Los Códigos que no tocan el estado del tampón son:

E: 020, 022, 030, 040, 050, 060, 070, 080, 090,120, 130, 140, 150, -----, 220, 230
R: 020, 022, 030, 040, 050, 060, -----, 080, ----, 120, 130, 140, 150, 155, 220, 230

8. ANEXO C. CAUSAS Y DIAGNOSTICOS DE LIBERACION.

Las liberaciones son mensajes que en cualquier caso suponen el no establecimiento o el corte de una conexión. Estos mensajes vienen identificados por dos códigos de dos dígitos hexadecimales (causa y diagnóstico respectivamente).

Es prácticamente imposible documentar todas las posibles causas y diagnósticos que EDITRAN/P puede recibir, ya que el origen de una liberación puede ser muy variado, a saber entre otros:

- EDITRAN/P Local.
- EDITRAN/P Remoto.

Por lo dicho, solo se contemplan en esta documentación las liberaciones que están originadas por EDITRAN/P.

También se incluyen en este capítulo las condiciones de reintento de conexión ya que se actúa, en la mayoría de los casos, en función de las liberaciones recibidas.

8.1. CAUSAS Y DIAGNOSTICOS EDITRAN

A continuación se especifican los códigos de causa y diagnóstico de liberación o rechazo de llamada dados por EDITRAN. En caso de liberaciones EDITRAN para conexiones TCP/IP consulte el manual **IP52USIC**.

- 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 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 - No utilizado (en versiones EDITRAN < 2.1, 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 por:
- Sesión no dada de alta.
- No coincide el nri local o el remoto (o sus longitudes) del paquete de llamada entrante con los especificados en la sesión.
- No coincide la versión.
- No coincide el terminal code por el que entra la llamada con el definido en perfiles.
- No coincide la lu ficticia por la que entra la llamada con la definida en perfiles.
- No coincide el tipo de conexión.
- No coinciden los identificadores de acceso.
- Coincidencia de un diagnóstico X25 con diagnóstico EDITRAN.

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.).

10 - NPSI-DATE pide que se libere un canal determinado.

11 - Error en rango de resid (NPSI-DATE o GATE). Se produce cuando el definido para una Sesión no está dentro del rango que da NPSI.

12 - Error en rango de termid (NPSI-DATE o GATE).Se produce cuando el resid que da NPSI calcula el terminal que tiene que activar y éste no existe o no se puede conectar. En estos casos debe revisarse el registro de Sesión y en concreto el campo primer terminal.

8.2. CONDICIONES DE REINTENTOS DE CONEXION

Las condiciones en las que EDITRAN realiza REINTENTO de CONEXION con las mismas características (NRI, facilidades y datos de usuario), son las siguientes.

θ Cuando se cumple todas las condiciones siguientes:

- EXTREMO LLAMANTE = "L" (Local) o "X" (cualquiera).
- TIPO DE CONEXION = "I", "Y". (TCP, EDITRAN/PR)
- Diagnóstico de Liberación distinto de:
  - 04 : Se ha producido un cruce de llamadas.
  - 05 : Ya hay CVC para esa Sesión.
  - 06 : Error en cobro revertido.
  - 07 : Error en tipo de pago.
  - 08 : Liberación por Operador.

- 09 : Liberación por Rearranque.
- 0A : Facilidades inválidas.
- 0C : Hora de transmisión incorrecta.
- 0E : Extremo Llamante inválido.
- 11 : Error de resid devuelto por NPSI.
- 12 : Error de termid devuelto por NPSI.
- 5D : Lacb no disponible.
- 7F : Error de nodo. Desconexión a petición del Host.

- Causa = 00 u 80 y Diagnóstico distinto de:
  - 0F : Liberación genérica de EDITRAN.
  - 58 : Terminal erróneo.
- Causa = 00 u 80, sesión pendiente de conexión y Diagnóstico distinto de:
  - 00 : Nivel de transporte remoto caído. Sin embargo se Reintento si se está transmitiendo.

Las condiciones en las que EDITRAN realiza REINTENTO de CONEXION con otro NRI remoto o local (ó dir-ip) son las siguientes:

θ Cuando se cumplen todas las condiciones siguientes si es un mensaje de Liberación, REPORT NPSI V3R8 o rechazo a solicitud de llamada..

- EXTREMO-LLAMANTE = "L" o "X".
- TIPO-CONEXION = "I","Y". (TCP, EDITRAN/PR)
- Diagnósticos no comprendidos en los anteriores de EDITRAN.
- La secuencia de reintentos de Backup es la siguiente (:
  - IP-REMOTA(1)
  - IP-REMOTA(2)

  Y así sucesivamente....

9. ANEXO D. SISTEMA DE CRIPTOGRAFIA EN EDITRAN.

9.1. Conceptos iniciales.

Una clave, se guarda siempre asociada a una etiqueta. En los perfiles EDITRAN, se especifican las etiquetas que contienen esas claves (ó al menos, una referencia que permita encontrar etiqueta y clave, si se usa gestión de claves de intercambio).

Hay 3 tipos de criptografía: DES, RSA y AES. Para usar cualquiera de ellas, se requieren distintos módulos EDITRAN (y que el remoto con el que nos conectemos, también disponga de ellos.

Se requiere disponer de licencias según se use uno u otro sistema:

- En DES:
    - CRIPTOlib/DES (producto comercializado por Indra, válido para todos los entornos) ó tarjeta criptográfica ICSF-CMOS (sólo en los entornos zos)
    - API de criptografía DES (para CRIPTOlib/DES ó para ICSF-CMOS), comercializado por Indra.
- En RSA:
    - Disponer de entorno DES, con las licencias descritas anteriormente
    - CRIPTOlib/RSA (producto comercializado por Indra, válido para todos los entornos)
    - API de criptografía RSA para enlace con entorno DES utilizado, comercializado por Indra.
- En AES
    - Disponer de entorno RSA, con las licencias descritas anteriormente
    - API de criptografía RSA para enlace con entorno AES utilizado, comercializado por Indra.
    - API de criptografía AES.

La criptografía DES, puede realizarse de 2 formas:

- Criptografía hardware (sólo entornos Zos con tarjeta criptográfica). Se usa ICSF-CMOS. Para su uso con EDITRAN, se requiere el módulo EDITRAN API DES para ICSF. El fichero de claves DES se llama CKDS ó MKDS.
- Criptografía software. Para su uso con EDITRAN, se requieren 2 módulos propiedad de Indra: CRIPTOlib/DES y API DES para CRIPTOlib/DES. El fichero de claves DES, se llama FICHKDES (entornos zos) ó ckds.des (entornos abiertos)

El fichero de claves de **criptografía DES,** contiene una clave maestra de la entidad, llamada HMK (Host Master Key) ó clave maestra de la instalación. El producto proporciona herramientas para incorporar esa primera clave a dicho fichero (en el caso de criptografía software). En el caso de zos con CRIPTOlib/DES, se proporciona el **jcl JGENFICH**, donde se inicializa el FICHKDES y se incorpora una clave que se introduce 2 veces en la sysin del jcl, para evitar errores. Si usted lista el fichero, ya no verá el valor que indicó en claro. Una vez

introducida la HMK, en zos, se deben introducir 2 claves, llamadas AUXILIARES. Cuando en el entorno local EDITRAN indicamos:

```
|  LABEL LOCAL.....: xxxxxxxx          LABEL REMOTO....: yyyyyyyy          |
```

estamos señalando esas claves auxiliares (mediante 2 etiquetas que contienen las claves), que serán importantes en la instalación, pues servirán para cifrar, generar, recifrar, otras claves, de forma que queden ocultas en los distintos sitios donde se guarden éstas últimas. Estas 2 etiquetas guardan claves DES SIMPLES, de 8 octetos), cuyo valor debe ser idéntico en ambas. Se proporcionan herramientas EDITRAN que sirven para incorporar dichas claves auxiliares al FICHKDES: **jcl ZTBSJCR (CRIPTOlib/DES) ó ZTBSJICS (ICSF-CMOS)**. En este último, hay paneles donde se indica el label escogido y la clave escogida. El label local contiene una clave de tipo EXPORTER y el label remoto contiene una clave de tipo IMPORTER. Las claves que se generan son aleatorias, no se especifican en el jcl, las crea el propio programa llamado. Una vez están ambas claves incorporadas al entorno DES correspondiente y en el entorno local, se podrá empezar a funcionar con la criptografía.

En entornos abiertos, habitualmente, los pasos anteriores de criptografía DES, vienen "preinstalados". Al instalar el producto, se genera automáticamente el fichero ckds.des con las claves anteriores. Si usted quiere empezar de cero, creando sus propias claves (sólo se puede hacer este proceso cuando no hay sesiones EDITRAN creadas), renombre el ckds.des antiguo y ejecute en una ventana MSDOS sobre el directorio EDITRAN instalado el comando **pinsdes xxxxxxxxxxxxxxxx yyyyyyyyyyyyyyyy** (x e y son los mismos valores, de confirmación de la HMK, que es de 16 caracteres hexadecimales, 8 octetos finales), de forma que se creará la HMK, A continuación, para la AUXILIAR, introduzca el comando **introsec SI000000000016 yyyyyyyyyyyyyyyy** (SI000000000016 es la etiqueta. El resto es el valor de esa clave, que debe tener paridad impar

Cuando se usa **criptografía RSA**, además de disponer de un entorno DES, se requieren 2 módulos: CRIPTOlib/RSA + API RSA (para ICSF-CMOS ó para CRIPTOlib/DES). Es un cifrado software, propiedad de Indra, que simula las funciones de la criptografía RSA. Cuando se usa RSA, se crea en zos un fichero llamado FICHKRSA (en entornos abiertos se llama ckds.rsa). Es necesario incorporar en el entorno DES que tengamos, una etiqueta asociada a una clave DES, que servirá para cifrar todas las claves RSA que incorporemos en el FICHKRSA. En zos se proporciona un **jcl XSCRFILE**, que inicializa el FICHKRSA, y a través de 2 sysin se incorporan 2 etiquetas (de hasta 64 octetos en este caso), de forma que el programa inicializa el registro de control de dicho fichero con las 2 claves DES que protegen al mismo (claves en forma aplicativa junto con los lábeles). A continuación, el programa en un paso posterior, genera una clave aleatoria de paridad impar (la que cifra a las 2 anteriores), y la incorpora 2 veces en el fichero DES de la entidad (ICSF ó CRIPTOlib), una con el primer laber (local o de tipo exporter) y otra con el segundo label (remota o importer)

En entornos abiertos, habitualmente los pasos anteriores de criptografía RSA, se consiguen ejecutando en una ventana MSDOS sobre el directorio EDITRAN instalado el comando **inst_rsa xxxxxxxxxxxxxx** (x es un label de 14 caracteres)

La criptografía RSA, se basa en lo siguiente:

- Una clave tiene 2 partes, parte privada y parte pública, cada una se guarda con una etiqueta distinta.
- La parte pública la puede conocer cualquiera sin riesgo de integridad

- Ambos extremos se intercambian la parte pública de sus respectivas claves. La parte privada, no se intercambia nunca. Es propiedad de la entidad que generó la clave RSA. Ni siquiera esta, puede verla en claro.
- Con la parte pública remota, se cifran claves DES, (que servirán luego para cifrar los datos). El único capaz de descifrar esta clave DES (para luego descifrar los datos), es la entidad que dispone de la parte privada de la clave RSA asociada.
- Con la parte privada, se firman textos. El que tenga la parte pública de la anterior privada, puede reconocer al que firmó, (pues sólo lo pudo firmar el que tenía la privada)

9.2. Tipos de claves. Versión criptográfica y cambio de clave.

La única diferencia en cuanto a parámetros de criptografía, de estar en EDITRAN/P ó en EDITRAN/G, son los parámetros VERSION CRIPTOGRAFICA y CAMBIO DE CLAVE (ambos valores no existen en EDITRAN/G, por lo que éste último tira de EDITRAN/P para conocer dichos campos). Los valores del campo VERSION CRIPTOGRAFICA son:

1) Versión 2.20 (también llamada 2.2). Es el modo de funcionamiento con un intercambio automático de claves. Los operadores de las 2 entidades implicadas, no se envían claves unos a otros, el producto lo hace de forma automática. Las 2 entidades, al dar de alta la sesión, generan una primera clave a partir de una semilla común, idéntica a todas las sesiones y entornos de EDITRAN. De ahí que surja el parámetro CAMBIO DE CLAVE. Lo habitual es que cuando se use criptografía 2.20, ambos extremos indiquen CAMBIO DE CLAVE S, y hagan una petición de conexión en cada sentido (primero un extremo pide la conexión, libera y luego el otro hace lo mismo). De esta forma, el producto y cualquier elemento externo, pierde el rastro de la semilla común, y resulta aún más complicado "descifrar" la clave con la que se cifrarán los datos. En ese momento, lo habitual es indicar CAMBIO DE CLAVE N y el producto está listo para funcionar normalmente en el envío de ficheros (se habrá cambiado la clave generada de la semilla común y además se ha probado que funciona el cifrado). Cuando se indica Versión 2.20, el único valor posible en CONFIDENCIALIDAD es DES (ó espacios), es decir, generar una DES simple ó no cifrar. El único valor posible en autenticación es DES. En resumen, el cifrado sólo puede hacerse con claves DES simples (de 8 octetos). Respecto a las claves hay las siguientes:
   - θ HMK (Host Master Key): Su función es cifrar claves de la Entidad usuaria local. Reside en el MKDS.
   - θ AK (Auxiliary Key):
     - En versión Criptográfica V-2.2, sirve para cifrar la Clave Maestra de EDITRAN. Se genera con valor aleatorio, incorporándose en el CKDS (KS) con dos "lábeles", que pueden ser consultados en el Entorno Local de Perfiles de EDITRAN.
     - En versión criptográfica V-3.0 y 40, sirve para intercambiar los extremos utilizados para cifrar la clave de sesión.
   - θ EMK (Clave Maestra de EDITRAN): Su función es cifrar datos relevantes de Perfiles. Se guarda en Perfiles cifrada bajo la clave AK local.
   - θ TKE (Clave Transporte Emisión): En "on-line", su función es cifrar los datos de las aplicaciones usuarias de EDITRAN que se envían al remoto y los Mensajes de Operador para el Remoto. Sin embargo, en "batch" su función es cifrar a la clave de presentación que cifra los datos. Se guarda en Perfiles cifrada bajo la EMK.
   - θ TKR (Clave Transporte Recepción): En "on-line", su función es descifrar los datos y Mensajes de Operador que se reciben cifrados del Remoto. En "batch", su función es recifrar la clave de presentación que viene cifrada con la TKE del remoto. Se guarda cifrada bajo la clave EMK en Perfiles.
   - θ TKE-nueva (Clave Transporte Emisión Nueva): Esta clave pasa a ser la TKE tras una petición de Cambio de Clave al Remoto. Se guarda cifrada bajo la EMK de forma temporal en el establecimiento de Sesión. Es generada aleatoriamente por EDITRAN Local.

- θ TKR-nueva (Clave Transporte Recepción Nueva): Pasa a ser la TKR tras una indicación de Cambio de Clave del Remoto. Su almacenamiento es temporal, cifrada bajo la EMK. Es generada aleatoriamente por EDITRAN Remoto.
- θ Clave de Sesión: Esta clave, diferente en cada sesión de transmisión -EDITRAN/P- y sesión de presentación -EDITRAN/G-, se genera con valor aleatorio y es la que cifra/descifra en "batch" a los datos de la "presentación". Se intercambia con el remoto cifrada con la TKE del emisor (igual a la TKR del receptor). Su almacenamiento es temporal, cifrada bajo la HMK, en el transcurso de la carga/descarga y durante el establecimiento de sesión (proceso de autenticación).

a) En el establecimiento de Sesión se resuelve la Autenticación de las claves TK de ambos extremos, con independencia de que haya o no Cambio de Clave en uno o ambos extremos. Se valida que TKE local = TKR remota y TKE remota = TKR local.
b) En definitiva, **en 2.20** la clave común es la de sesión (TKE-TKR), **no hay una clave común para intercambiar la de sesión**. Las claves auxiliares (EMK-AK) sirven para que cada entidad se guarde su clave de sesión de forma segura, siendo propias de cada entidad. Cuando se genera nueva clave de sesión (TKE-TKR nueva) , se entrega al remoto cifrada con la anterior clave de sesión (que es en ese momento común), de forma que en ambos extremos pasan a ser desde ese momento claves de sesión (TKE-TKR)
c) El proceso de cambio de clave no es necesario , pero proporciona más seguridad.

2) Versión 3.00 y 4.00 con autenticación DES ó RSA. El intercambio no es de forma automática como la criptografía 2.20 Esta modalidad utiliza claves Criptográficas que los usuarios deben haber intercambiado previamente por el método que estimen conveniente: correo, mail, teléfono, EDITRAN, ó como crean conveniente las 2 entidades implicadas (con el módulo Gestión de claves de intercambio, se puede realizar este intercambio de manera segura, sin que ninguno de los intervinientes conozca el valor real de la clave intercambiada). Cuando se usa criptografía 3.00 o 4.00 , existen 2 tipos de claves:

- Claves de intercambio ó de transporte (las que se intercambian las 2 entidades). Estas claves pueden ser DES, RSA. Con ellas, se hace referencia al algoritmo de autenticación con los valores posibles: DES, RSA
  a) Si son DES (algoritmo autenticación DES), las entidades pueden intercambiar:
     i) Claves DES simples (8 bytes). Cualquier máquina EDITRAN puede intercambiar estas claves
     ii) Claves DES dobles (16 bytes). Dependiendo del sistema operativo y de la versión EDITRAN instalada, es o no posible (entorno abiertos v.EDITRAN > 5.0, entornos zos, todas las versiones, entorno i-series no disponible aún). Si alguno de los 2 entornos no es compatible, pero quiere funcionar con claves dobles, los 8 primeros bytes de la clave deben tener el mismo valor que los 8 últimos. Si por ejemplo un UNIX genera una clave de transporte DES SIMPLE y se la envía a un zos, éste podría incluirla como una clave de transporte IMPORTER DES DOBLE (16 bytes), simplemente repitiendo los 8 bytes que le han enviado con la CLAVE DES SIMPLE (8 BYTES) A su vez, si un zos genera una clave de transporte EXPORTER DES DOBLE y el valor de sus 8 primeros bytes es idéntico al valor de sus últimos 8 bytes, el UNIX puede incluirla como CLAVE DES SIMPLE metiendo los 8 primeros bytes que le llegan. En ambos casos, el proceso funciona bien. Sin embargo, en claves

dobles lo que se realiza son procesos de cifrado (con 8 primeros), descifrado (con 8 segundos) y recifrado (con 8 primeros), por lo que repetir los 8 primeros y los 8 segundos bytes en una clave doble, es triplicar las operacionales a realizar (comparando con claves simples), obteniendo al final el mismo resultado. Por ello, se recomienda no usar dobles iguales.

iii) Claves DES tiples (24 octetos). Ningún extremo las genera.

b) Si son RSA, (algoritmo autenticación RSA) las entidades intercambian la parte pública de la clave, como se explicó anteriormente.

- Claves operacionales. Estas claves son siempre DES (simples, dobles o triples). Con ellas, se hace referencia al algoritmo de confidencialidad con los valores posibles: DES (8 bytes ó DES simple), TD2C (16 bytes, ó doble DES) y TD3C (24 bytes ó triple DES). Son las claves que cifrarán los datos EDITRAN (como se expuso anteriormente). No confunda con las claves de intercambio. Todos los entornos EDITRAN pueden generar claves operacionales DES triples, y sin embargo, ninguno genera claves de intercambio triples.

En criptografía 3.0 o 4.0: Así por **ejemplo**, **si intercambiamos una clave RSA (**clave de intercambio o transporte, autenticación RSA), enviamos al remoto la parte pública de nuestra clave y el remoto nos envía la suya. Al comienzo de cada transmisión, se genera una clave operacional des, (por ejemplo triple, de 24 octetos. si hemos indicado confidencialidad TD3C). Por un lado, esa clave operacional DES, se guarda cifrada bajo la pública RSA que nos dio ese remoto. Por otro lado, EDITRAN cifra los datos con la operacional (cifrado-descifrado-cifrado). Por último, EDITRAN envía la operacional DES cifrada y los datos cifrados. Ese remoto, dispone de la privada, por lo que descifra con la misma la clave operacional cifrada y le da como resultado la clave operacional en claro (con la que ciframos los datos nosotros). A continuación descifra los datos con esa operacional (descifrado-cifrado-descifrado). En el ejemplo anterior, cuando se indica cifrado-descifrado-cifrado ó descifrado-cifrado-descifrado, lo que quiere decir en realidad es que la clave operacional es triple, de 24 bytes. Los datos se cifran con los 8 primeros bytes de la operacional. El resultado se descifra con los 8 segundos. El resultado se cifra con los 8 últimos. El resultado se envía al remoto. Este, descifra la operacional (como se expuso antes) y a continuación, descifra el dato que le llega con los 8 últimos de la operacional. El resultado lo cifra con los 8 intermedios y el resultado lo descifra con los 8 primeros de la operacional. El resultado final es el dato en claro.

En criptografía 3.0: Así por **ejemplo**, **si intercambiamos una clave DES** (simple contra cualquier entorno ó doble entre 2 zos) (clave de intercambio o transporte, autenticación DES), enviamos al remoto la misma. Al comienzo de cada transmisión, se genera una clave operacional DES, (por ejemplo triple, si hemos indicado confidencialidad TD3C). El proceso es igual al ejemplo anterior. Por un lado, se cifra la operacional generada bajo la DES remota intercambiada y por otro los datos se cifran bajo la operacional generada.

Como se ha visto, el cifrado 3.00 de la operacional, es DES o RSA. Es más seguro RSA.

Ejemplo de un intercambio de claves DES y uso de TDES para cifrar datos

Entidad A	Acción	Entidad B
1.- Genera una clave DES x'AAA...' (proceso externo a EDITRAN)	2.- A comunica a B clave DES x'AAA...' (proceso externo a EDITRAN)	3.- Incorpora clave DES x'AAA...' (proceso externo a EDITRAN)
6.- Incorpora clave DES x'BBB...' (proceso externo a EDITRAN)	5.- B comunica a A clave DES x'AAA...' (proceso externo a EDITRAN)	4.- Genera una clave DES x'BBB...' (proceso externo a EDITRAN)
7.- EDITRAN A, en cada transmisión genera una clave OPERACIONAL TRIPLE DES x'CCC...'	8.- EDITRAN A envía a EDITRAN B la clave x'CCC..' cifrada bajo x'BBB..'	9.- EDITRAN B, descifra x'CCC...' bajo x'BBB..' y saca en claro x'CCC..'

	Además, firma bajo x'AAA..'	
10.- EDITRAN A, cifra DATOS bajo x'CCC'	10.- EDITRAN de A, envía a EDITRAN B, DATOS cifrados bajo x'CCC'	11.- EDITRAN B, descifra datos bajo x'CCC..' y los saca en claro Verifica la firma de x'AAA..'

Ejemplo de un intercambio de claves RSA y uso de TDES para cifrar datos

Entidad A	Acción	Entidad B
1.- Genera una clave RSA, con 2 partes: privada x'AAA...' y pública x'YYY' (proceso externo ó automatizado con GC)	2.- A comunica a B clave RSA pública x'YYY...' (proceso externo ó automatizado con GC)	3.- Incorpora clave RSA x'YYY...' (proceso externo ó automatizado con GC)
6.- Incorpora clave RSA x'ZZZ...' (proceso externo ó automatizado con GC)	5.- B comunica a A clave RSA pública x'ZZZ...' (proceso externo ó automatizado con GC)	4.- Genera una clave RSA, con 2 partes: privada x'BBB...' y pública x'ZZZ' (proceso externo ó automatizado con GC)
7.- EDITRAN A, en cada transmisión genera una clave OPERACIONAL TRIPLE DES x'CCC...'	8.- EDITRAN A envía a EDITRAN B la clave x'CCC..' cifrada bajo x'ZZZ..' Además, firma bajo x'AAA..'	9.- EDITRAN B, descifra x'CCC...' bajo x'ZZZ..' (e x'YYY) y saca en claro x'CCC..'
10.- EDITRAN A, cifra DATOS bajo x'CCC'	10.- EDITRAN de A, envía a EDITRAN B, DATOS cifrados bajo x'CCC'	11.- EDITRAN B, descifra datos bajo x'CCC..' y los saca en claro Verifica la firma de x'AAA..' (porque dispone de x'YYY..')

No confunda TRIPLE DES – DES - RSA

TRIPLE DES ó DES es la forma de cifrar los datos, es la forma de generar CLAVE OPERACIONAL.

DES ó RSA es la forma de intercambiar la clave, es la forma de intercambiar la CLAVE DE INTERCAMBIO.

9.3. Conclusiones y aplicación en la parametrización EDITRAN

Cuando en una sesión EDITRAN indicamos:

- Algoritmo de confidencialidad (DES, TD2C, TD3C) estamos indicando el algoritmo para cifrar los datos (DES = DES de clave simple 8 octetos, TD2C = DES de clave doble 16 octetos y TD3C= DES de clave triple 24 octetos).
- Algoritmo de autenticación (DES, RSA) estamos indicando el algoritmo para autenticar los datos (y para cifrar las operacionales)

El cifrado de datos (algoritmo de confidencialidad), se puede hacer:

- En EDITRAN/G, cogiendo el fichero de aplicación y cifrándolo para que quede así guardado cifrado en el fichero tampón
- En EDITRAN/P, en cuyo caso en tiempo de transmisión, se coge el mensaje contenido en el tampón (en claro) y se cifra.

De ahí, que se muestren 2 pantallas de cifrado (en P y en G). Lo más práctico, seguro y cómodo es cifrar-descifrar y autenticar en EDITRAN/G, y autenticar en EDITRAN/P. **No tiene sentido que cifremos en EDITRAN/G y luego otra vez en EDITRAN/P**

De ese modo, **se recomienda (algunos de los valores dependen de V 2.20, 3.00 o 4.00):**

- **En EDITRAN/G, indicar CRIPTOGRAFIA = S, CONFIDENCIALIDAD = XXXX (DES, TD2C, TD3C, AES1, AES2, AES3), AUTENTICACION = XXXX (DES, RSA). El resto de parámetros; INTERFAZ CLAVES, PARM, CLAVE LOCAL, CLAVE REMOTA, dependerán de otros factores, que se explican más adelante,**
- **En EDITRAN/P, indicar CRIPTOGRAFIA = S, CONFIDENCIALIDAD = spaces, AUTENTICACION = XXXX (DES, RSA). El resto de parámetros; VERSION, CAMBIO DE CLAVE (ya explicado), INTERFAZ CLAVES, PARM, CLAVE LOCAL, CLAVE REMOTA, dependerán de otros factores, que se explican más adelante.**

Otras recomendaciones:

1. Cuando usamos criptografía 2.20 (parámetro VERSION CRIPTOGRAF: 2.20), sólo intervienen los parámetros CRIPTOGRAFIA, CONFIDENCIALIDAD, AUTENTICACION y CAMBIO DE CLAVE.

En EDITRAN/P, (se debe haber indicado VERSION CRIPTOGRAF: 2.20). Si indica CRIPTOGRAFIA S, le obligará a poner el campo ALGORITMO AUTENTICACION = DES. Además, intervendrá lo que ponga en algoritmo confidencialidad. Los valores posibles son: DES (cifra los datos del tampón **en tiempo de transmisión**) y spaces (no los cifra).. También interviene el campo CAMBIO DE CLAVE. Si indica S, no le permitirá poner CRIPTOGRAFIA S en EDITRAN/G.

En EDITRAN/G (se debe haber indicado VERSION CRIPTOGRAF: 2.20 en EDITRAN/P). Si indica CRIPTOGRAFIA S, le obligará a poner el campo ALGORITMO AUTENTICACION = DES. Además, intervendrá lo que ponga en algoritmo confidencialidad. Los valores posibles son: DES (cifra los datos del tampón **en tiempo de carga**) y espacios (no los cifra).

Recomendación:

En EDITRAN/P (inicialmente Cambio Clave S, pero tras un par de conexiones se cambia a N)

```
| CRIPTOGRAFIA S/N: S        VERS.CRIPTOGRAF.: 2.20     CAMB.CLAVE (S/N/U): N |
| ALG.CONFIDENC...:          ALG.AUTENTICAC..: DES                            |
```

En EDITRAN/G

```
                    CRIPTOGRAFIA (S/N).......: S
ALGORITMO CONFIDENCIALIDAD.:  DES       ALGORITMO AUTENTICACION ...: DES
```

Recuerde que no es recomendable alg. Confidencialidad DES en P y G (porque cifraría 2 veces los datos). Es recomendable colocar autenticación DES en P y G, para autenticar la transmisión y el tampón.

2. Cuando usamos criptografía 3.0 o 4.0 (parámetro VERSION CRIPTOGRAF: 3.00 o 4.0), según hemos visto, entran **al menos** los parámetros CRIPTOGRAFIA, CONFIDENCIALIDAD Y, AUTENTICACION.

En EDITRAN/P, (se debe haber indicado VERSION CRIPTOGRAF: 3.00 o 4.00). Si indica CRIPTOGRAFIA S, intervendrá lo que ponga en algoritmo confidencialidad. Los posibles valores son TD3C (cifra los datos del tampón **en tiempo de transmisión** con clave des triple), TD2C (con clave des doble), DES (con clave des simple), AES3 (cifra los datos del tampón **en tiempo de transmisión** con clave aes triple), AES2 (con clave aes doble), AES1 (con clave aes simple) y espacios (no los cifra). También interviene lo que indique en algoritmo de autenticación. Los valores posibles son DES ó RSA, y lógicamente debe poner un valor acorde a las claves que se han intercambiado.

En EDITRAN/G, (se debe haber indicado VERSION CRIPTOGRAF: 3.00 o 4.00 en EDITRAN/P). Si indica CRIPTOGRAFIA S, intervendrá lo que ponga en algoritmo confidencialidad. Los posibles valores son TD3C (cifra los datos del tampón **en tiempo de carga** con clave des triple), TD2C (con clave des doble), DES (con clave des simple)), AES3 (cifra los datos del tampón **en tiempo de carga** con clave aes triple), AES2 (con clave aes doble), AES1 (con clave aes simple) y espacios (no los cifra). También interviene lo que indique en algoritmo de autenticación. Los valores posibles son DES ó RSA, y lógicamente debe poner un valor acorde a las claves que se han intercambiado.

Recomendación:

En EDITRAN/P (inicialmente Cambio Clave S, pero tras un par de conexiones se cambia a N)

```
| CRIPTOGRAFIA S/N: S        VERS.CRIPTOGRAF.: 2.20     CAMB.CLAVE (S/N/U): N |
| ALG.CONFIDENC...:          ALG.AUTENTICAC..: DES                            |
```

En EDITRAN/G

```
                    CRIPTOGRAFIA (S/N).......: S
ALGORITMO CONFIDENCIALIDAD.:  DES       ALGORITMO AUTENTICACION ...: DES
```

Recuerde que no es recomendable alg. Confidencialidad XXXX en P y G (porque cifraría 2 veces los datos). Es recomendable colocar autenticación XXX en P y G, para autenticar la transmisión y el tampón.

3. En criptografía 3.0 y 4.0, si hemos indicado CRIPTOGRAFIA S y VERSION CRIPTOGRAF: 3.00 o 4.00, **además,** intervienen también otros valores, dependiendo del algoritmo de autenticación y del modo en que hemos intercambiado la clave (de transporte o intercambio):

   3.1. **Si hacemos un intercambio de claves externo DES o RSA**, **sin gestión de claves de intercambio**, intervienen también los valores CLAVE LOCAL y CLAVE REMOTA. En esos valores, se indicará:

      3.1.1. Si autenticación es DES,

3.1.1.1. En clave local se indica la etiqueta de la clave local DES generada y enviada al remoto. (el remoto insertará en su sistema de claves esa clave con la etiqueta que le venga en gana y codificará esa etiqueta en su clave remota).

3.1.1.2. En clave remota, se indica la etiqueta con la que hemos incorporado en nuestro sistema de claves la clave DES que nos envió el extremo remoto (y que el remoto habrá colocado con su etiqueta en su parámetro clave local)

3.1.2. Si autenticación es RSA,

3.1.2.1. En clave local se indica la etiqueta de la clave privada RSA generada y no enviada al remoto. El remoto incorporará en su sistema de claves la parte pública de esa clave (que le enviamos), con la etiqueta que le venga en gana en el campo clave remota).

3.1.2.2. En clave remota, se indica la etiqueta con la que hemos incorporado en nuestro sistema de claves la clave RSA pública que nos envió el extremo remoto (y que el remoto habrá colocado la etiqueta que contiene la parte privada de esa pública que nos envió en su su parámetro clave local)

3.2. **Si hacemos un intercambio de claves externo RSA, con gestión de claves de intercambio**, sólo Intervienen los campos INTERFAZ DE CLAVES y PARAMETROS. En esos valores, se indicará:

3.2.1. En EDITRAN/G. INTERFAZ DE CLAVES ZTBGBIGC (programa que se encarga de averiguar en EDITRAN/G cual es la clave activa de los subsistemas intercambiados

3.2.2. En EDITRAN/P INTERFAZ DE CLAVES ZTBPOIGC (programa que se encarga de averiguar en EDITRAN/G cual es la clave activa de los subsistemas intercambiados)

3.2.3. PARAMETROS, (ya sea P ó G donde hayamos decidido cifrar los datos), se indicará *,A,B, siendo A el subsistema local intercambiado y siendo B el subsistema remoto intercambiado.

9.4. Intercambios de claves sin gestión de claves de intercambio.

En versión de criptografía 3.00 ya se indicó que los intercambios se podrían hacer con gestión de claves ó sin ella.

Cuando se **hacen sin gestión de claves de intercambio**, un extremo A, genera una clave y otro extremo B, genera otra. En este caso, la clave generada (de intercambio), puede ser:

- DES. En este caso, ya se indicó que las claves intercambiadas eran simples ó dobles (con limitaciones). Dependiendo de la interfaz:
    - CRIPTOlib/DES
        - Si va a generar y enviar una clave, crea la misma con una etiqueta (de hasta 64 octetos) y asocia a la misma una clave que le venga en gana. Para generarla, se facilita el **jcl XSCDALTA**. Por último, incorpora la etiqueta en los perfiles EDITRAN como clave local. Le envía al remoto la clave en claro.
        - Si recibe una clave de la entidad remota, (en claro), la asocia con una etiqueta que quiera y la mete en su FICHKDES a través del **jcl XSCDALTA**. Por último, incorpora la etiqueta en los perfiles EDITRAN como clave remota. La etiqueta puede ser de hasta 64 octetos.
    - Entorno ICSF: Se hace a través de los paneles del propio ICSF.
        - Si va a generar y enviar una clave, crea la misma con una etiqueta (que meterá en los perfiles EDITRAN como clave local y que puede ser de hasta 64 octetos) y asocia a la misma una clave que le venga en gana. Esa clave es de tipo exporter y debe dársela al remoto en claro. Por último, incorpora la etiqueta en los perfiles EDITRAN como clave local.
        - Si recibe una clave de la entidad remota, (en claro), la asocia con una etiqueta que quiera (de hasta 64 octetos) y la mete en ICSF como de tipo importer. Por último, incorpora la etiqueta en los perfiles EDITRAN como clave remota.
- RSA
    - Si va a generar y enviar una clave. Se proporciona el **jcl XSCRKGEN**, En el mismo se incluyen 2 DD (de hasta 64 octetos cada una), en las cuales se introduce la etiqueta de la clave privada local y la etiqueta de la clave pública local. El sistema, genera una clave aleatoriamente y asociada cada parte a cada etiqueta concreta. A través del **jcl XSCRKEXP**, indicando la etiqueta de la clave pública local, exporta la misma a un fichero, que remite al remoto. Por último, incorpora la etiqueta de la pública en los perfiles EDITRAN como clave local
    - Si recibe una clave pública de la entidad remota, (en claro), la mete en un fichero. Se le proporciona un **jcl XSCRKIMP**, que tira de ese fichero. Se incluye una DD (de hasta 64 octetos) donde incluye el nombre de la etiqueta que le dará a la clave pública remota que ha recibido. Por último, incorpora la etiqueta en los perfiles EDITRAN como clave remota.

Ejemplo1.

La entidad A, genera una clave DES x'AA..AA' asociada a la etiqueta CLAVE-A-LOCAL-DES envía la clave x'AA..AA' a la entidad B. La entidad B, genera una clave DES x'BB..BB' asociada a la etiqueta CLAVE-B-LOCAL-DES y envía la clave x'BB..BB' a la entidad A. La entidad A, incorpora en su fichero de claves DES, la clave x'BB..BB' con la etiqueta CLAVE-B-REMOTA-DES. La entidad B, incorpora en su fichero de claves DES, la clave x'AA..AA' con la etiqueta CLAVE-A-REMOTA-DES.

En los perfiles de A

```
| CLAVE LOC: CLAVE-A-LOCAL-DES                    |
| CLAVE REM: CLAVE-B-REMOTA-DES                   |
```

En los perfiles de B:

```
| CLAVE LOC: CLAVE-B-LOCAL-DES                    |
| CLAVE REM: CLAVE-A-REMOTA-DES                   |
```

Nota: Tanto CLAVE-A-LOCAL-DES como CLAVE-A-REMOTA-DES, aunque son etiquetas distintas, contienen la misma clave. Tanto CLAVE-B-REMOTA-DES como CLAVE-B-LOCAL-DES, aunque son etiquetas distintas, contienen la misma clave.

Ejemplo2.

La entidad A, genera una clave RSA con 2 etiquetas CLAVE-A-LOCAL-RSA-PRIVADA y CLAVE-A-LOCAL-RSA-PUBLICA, esta última etiqueta asociada a la clave x'AA..AA', la cual remita a la entidad B. La entidad B, genera una clave RSA con 2 etiquetas CLAVE-B-LOCAL-RSA-PRIVADA y CLAVE-B-LOCAL-RSA-PUBLICA, esta última etiqueta asociada a la clave x'BB..BB', la cual remita a la entidad A. La entidad A, incorpora en su fichero FICHKRSA, la clave x'BB..BB' con la etiqueta CLAVE-B-REMOTA-RSA-PUBLICA. La entidad B, incorpora en su fichero de claves RSA, la clave x'AA..AA' con la etiqueta CLAVE-A-REMOTA-RSA-PUBLICA.

En los perfiles de A

```
| CLAVE LOC: CLAVE-A-LOCAL-RSA-PRIVADA            |
| CLAVE REM: CLAVE-B-REMOTA-RSA-PUBLICA           |
```

En los perfiles de B:

```
| CLAVE LOC: CLAVE-B-LOCAL-RSA-PRIVADA            |
| CLAVE REM: CLAVE-A-REMOTA-RSA-PUBLICA           |
```

. Nota: Tanto CLAVE-A-LOCAL-RSA-PUBLICA (no aparece en el perfil) como CLAVE-A-REMOTA-RSA-PUBLICA, aunque son etiquetas distintas, contienen la misma clave. Tanto CLAVE-B-REMOTA-RSA-PUBLICA como CLAVE-B-LOCAL-RSA-PUBLICA (no aparece en el perfil), aunque son etiquetas distintas, contienen la misma clave.

9.5. Intercambios con Gestión de claves de intercambio.

Se ha creado una aplicación, gratuita que permite automatizar el intercambio de claves de intercambio ó de transporte, ya sean DES o RSA (requiere disponer criptografía DES y RSA ambos extremos). Mediante este sistema, los intercambios de claves, se hacen seguros (nadie ve claves en claro), fiables y automatizados. Además, se permite el poder cambiar de clave, sin necesidad de cambiar los perfiles EDITRAN. Para más información revise el manual **EGC52USUC**.

9.6. Recomendaciones finales a la criptografía.

Por todo ello, se recomienda usar para los intercambios la aplicación gestión de claves de intercambio (interfaz y parámetros) y además usar TRIPLE DES en la clave DES operacional (confidencialidad) y clave RSA en la clave de intercambio (autenticación), pues claramente es el sistema criptográfico más seguro expuesto :

- **En EDITRAN/P, indicar (X e Y son los subsistemas que se definan)**

```
| CRIPTOGRAFIA S/N: S        VERS.CRIPTOGRAF.:3.00     CAMB.CLAVE (S/N/U): N  |
| ALG.CONFIDENC...:          ALG.AUTENTICAC..:RSA                             |
| INTERFAZ CLAVES.: ZTBPOIGC PARAMETROS......:*,X,Y                           |
| CLAVE LOC:                                                                  |
| CLAVE REM:                                                                  |
| ALIAS PSS:                                                                  |
| PIN......:                                                                  |
| DN REMOTO:                                                                  |
```

- **En EDITRAN/G, indicar (X e Y son los subsistemas que se definan)**

```
                      CRIPTOGRAFIA (S/N)........: S
ALGORITMO CONFIDENCIALIDAD.:TD3C        ALGORITMO AUTENTICACION ...:RSA
INTERFAZ DE CLAVES.........:ZTBGBIGC    PARM :*,X,Y
CLAVE LOCAL:
CLAVE REMOT:
ALIAS PSS  :
PIN DEL PSS:
DN DESTINO :
```

Si hubiera que elaborar una tabla en función de la seguridad del sistema criptográfico empleado, de menor a mayor, en la que se indican las necesidades:

Tipo de criptografía	Requiere DES	Requiere RSA	Claves intercambiadas sin Gestión de claves de intercambio	Claves intercambiadas con Gestión de claves de intercambio	Inconvenientes
Versión 2.20 sin cambio de clave	X				Semilla común conocida
Versión 2.20 con al menos 1 cambio de clave	X				Cifrado menos seguro que 3.00
Versión 3.00, autentif DES, confidencialidad DES	X		X		Clave de intercambio DES en claro
Versión 3.00, autentif DES, confidencialidad TD2C	X		X		Clave de intercambio DES en claro
Versión 3.00, autentif DES, confidencialidad TD3C	X		X		Clave de intercambio DES en claro
Versión 3.00, autentif DES, confidencialidad DES	X	X		X	Es mejor intercambiar claves RSA
Versión 3.00, autentif DES, confidencialidad TD2C	X	X		X	Es mejor intercambiar claves RSA
Versión 3.00, autentif DES, confidencialidad TD3C	X	X		X	Es mejor intercambiar claves RSA
Versión 3.00, autentif RSA, confidencialidad DES	X	X	X		Mejor usar Gestión claves intercamb.
Versión 3.00, autentif RSA, confidencialidad DES	X	X		X	Mejor usar confidencialidad TD3C
Versión 3.00, autentif RSA, confidencialidad TD2C	X	X	X		Mejor usar Gestión claves intercamb.
Versión 3.00, autentif RSA, confidencialidad TD2C	X	X		X	Mejor usar confidencialidad TD3C
Versión 3.00, autentif RSA, confidencialidad TD3C	X	X	X		Mejor usar Gestión claves intercamb.
Versión 3.00, autentif RSA, confidencialidad TD3C	X	X		X	
Versión 4.00, autentif RSA, confidencialidad AES1	X	X	X		Mejor usar Gestión claves intercamb.
Versión 4.00, autentif RSA, confidencialidad AES1	X	X		X	Mejor usar confidencialidad TD3C
Versión 4.00, autentif RSA, confidencialidad AES2	X	X	X		Mejor usar Gestión claves intercamb.
Versión 4.00, autentif RSA, confidencialidad AES2	X	X		X	Mejor usar confidencialidad TD3C
Versión 4.00, autentif RSA, confidencialidad AES3	X	X	X		Mejor usar Gestión claves intercamb.
Versión 4.00, autentif RSA, confidencialidad AES3	X	X		X	

9.7. Backups y centros BRS.

Si dispone de una licencia de backuo ó de una licencia para un centro BRS, debe considerar lo siguiente:

- El fichero de perfiles de EDITRAN/P, ZTBPFPE, debe ser idéntico al de producción
- El fichero de perfiles de EDITRAN/G, ZTBGFPE, debe ser idéntico al de producción
- Si utiliza CRIPTOlib/DES (cifrado software), ya sea con DES o RSA, el fichero FICHKDES, debe ser idéntico al de producción
- Si utiliza tarjeta criptográfica ICSF-CMOS en entornos zos, ya sea con DES o RSA, debe disponer de una tarjeta criptográfica copia idéntica de la tarjeta de producción (el fichero CKDS debe ser idéntico al de producción).
- Si utiliza CRIPTOlib/RSA, el fichero FICHKRSA, debe ser idéntico al de producción.
- Si utiliza Gestión de claves de intercambio, el fichero ZTBPFGC, debe ser idéntico al de producción.

9.8. PARAMETRIZACION DEL SISTEMA CRIPTOGRAFICO.

Como se puede apreciar en la tabla siguiente, el modo de criptografía V2.2 requiere una relación entre los parámetros de EDITRAN/G y EDITRAN/P, siendo totalmente independientes para el modo V3.0 y 4.00.

El parámetro versión de criptografía está contenido en los perfiles de EDITRAN/P pero afecta tanto a EDITRAN/P como a EDITRAN/G.

- Si se desea cifrar datos en tiempo de transmisión y con el Sistema de Intercambio de Claves propio de EDITRAN (opción no recomendada), los parámetros a codificar serían los siguientes:

	EDITRAN/P	EDITRAN/G
CRIPTOGRAFÍA	**S**	**N**
VERSIÓN CRIPTOGRÁFICA	**2.2**	
CAMBIO DE CLAVE	**S, U o N**	
ALGORITMO DE CONFIDENCIALIDAD	**DES**	
ALGORITMO DE AUTENTICACIÓN	**DES**	
INTERFAZ DE CLAVES		
PARÁMETROS		
CLAVE LOC.		
CLAVE REM.		

- Si se desea cifrar datos en tiempo de carga (Batch) y con el Sistema de Intercambio de Claves propio de EDITRAN (opción poco recomendada), los parámetros a codificar serían los siguientes:

	EDITRAN/P	EDITRAN/G
CRIPTOGRAFÍA	**S**	**S**
VERSIÓN CRIPTOGRÁFICA	**2.2**	
CAMBIO DE CLAVE	**N**	
ALGORITMO DE CONFIDENCIALIDAD		**DES**
ALGORITMO DE AUTENTICACIÓN	**DES**	**DES**
INTERFAZ DE CLAVES		
PARÁMETROS		
CLAVE LOC.		
CLAVE REM.		

A continuación se muestra la configuración en caso de usar la Criptografía basada en claves intercambiadas de forma externa a EDITRAN. Los lábeles o etiquetas son proporcionados por una Interfaz de Claves o bien se referencian directamente en el Perfil de la sesión. El algoritmo de autenticación puede ser DES o RSA.

- Si se desea cifrar datos en tiempo de carga (Batch) con Claves de Intercambio obtenidas de forma externa a EDITRAN y con algoritmo de cifrado DES (o Triple DES), los parámetros a codificar serían los siguientes:

	EDITRAN/P	EDITRAN/G
CRIPTOGRAFÍA	**S**	**S**
VERSIÓN CRIPTOGRÁFICA	**3.0**	
CAMBIO DE CLAVE	**N**	
ALGORITMO DE CONFIDENCIALIDAD		**DES ó TD2C ó TD3C (1)**
ALGORITMO DE AUTENTICACIÓN	**DES**	**DES**
INTERFAZ DE CLAVES		
PARÁMETROS		
CLAVE LOC.	**Etiqueta de la clave local**	**Etiqueta l de la clave local**
CLAVE REM.	**Label de la clave remota**	**Label de la clave remota**

- Si se desea cifrar datos en tiempo de carga (Batch) con Claves RSA, que proporciona la interfaz de EDITRAN, y con algoritmo de cifrado DES, los parámetros a codificar serían los siguientes:

	EDITRAN/P	EDITRAN/G
CRIPTOGRAFÍA	**S**	**S**
VERSIÓN CRIPTOGRÁFICA	**3.0/4.0**	
CAMBIO DE CLAVE	**N**	
ALGORITMO DE CONFIDENCIALIDAD		**DES / TD2C / TD3C**
ALGORITMO DE AUTENTICACIÓN	**RSA**	**RSA**
INTERFAZ DE CLAVES	**Nombre del programa que proporciona las claves: ZTBPBIGC**	**Nombre del programa que proporciona las claves: ZTBPBIGC**
PARÁMETROS	**Parámetros de paso a la Interfaz de claves Por Ejemplo : *,P,K**	**Parámetros de paso a la Interfaz de claves Por Ejemplo : *,P,K**
CLAVE LOC.		
CLAVE REM.		

- Si se desea cifrar datos en tiempo de carga (Batch) con algoritmo de cifrado AES y claves RSA, que proporciona la interfaz de EDITRAN, los parámetros a codificar serían los siguientes:

	EDITRAN/P	EDITRAN/G
CRIPTOGRAFÍA	**S**	**S**
VERSIÓN CRIPTOGRÁFICA	**3.0/4.0**	
CAMBIO DE CLAVE	**N**	
ALGORITMO DE CONFIDENCIALIDAD		**AES1 / AES / AES3**
ALGORITMO DE AUTENTICACIÓN	**RSA**	**RSA**
INTERFAZ DE CLAVES	**Nombre del programa que proporciona las claves: ZTBPBIGC**	**Nombre del programa que proporciona las claves: ZTBPBIGC**
PARÁMETROS	**Parámetros de paso a la Interfaz de claves Por Ejemplo : *,P,K**	**Parámetros de paso a la Interfaz de claves Por Ejemplo : *,P,K**
CLAVE LOC.		
CLAVE REM.		

9.9. ERRORES DE CIFRADO

Cuando se produce un Error Criptográfico, EDITRAN da una información local del error producido y envía al remoto una petición de liberación con el Motivo del error, liberando posteriormente la conexión.

En el extremo donde se produce el error se informa del Código de Retorno devuelto por el producto que proporciona los servicios criptográficos (CRIPTOlib/DES 3.0, BDKDES, PCF, CUSP, TSS, ICSF, ...), por lo que, de producirse, habría que consultar las referencias que del return-code y/o Reason-Code se dan en el correspondiente manual de cada producto, como:

- CRIPTOlib/DES : "Criptolib/DES 3.0 versión MVS. Sistema de Seguridad DES. Manual de Usuario e Instalación"

- CUSP/3848 : "Cryptographic Unit Support: Installation Reference Manual"
- TSS/4753 : "Transaction Security System. Programming Guide and Reference"
- ICSF/ICRF : "Integrated Cryptographic Service Facility/MVS. Aplication Programmer's Guide".

Los Motivos EDITRAN de los Errores Criptográficos que pueden ocurrir son:

(ERR1): El extremo que solicita una Petición de Conexión no ha podido hacer el Recifrado de las Claves de su fichero (si no hay Interfaz claves externas) o bien, error al obtener el Label en el extremo que inicia la sesión.

(ERR2): El extremo que solicita autentificar su clave TKE o su Clave de Intercambio externa (con Interfaz) no ha podido cifrar el Código de Autenticación, aunque sí hizo el Recifrado.
Si AUTENTICACION es DES : Probable error en clave local.
Si AUTENTICACION es RSA : Si el error se produce en la firma, el problema puede ser en la clave local (Privada).
Si el error es en la incertidumbre, el problema puede ser en la clave remota (pública).

(ERR3): El extremo que solicita una Petición de Conexión con Cambio de Clave no ha podido generar una clave de emisión.

(ERR4): El extremo que recibe la Indicación de Notificación del Remoto tuvo un error al hacer Recifrado de la clave TKR de su fichero, o en la obtención del Label de la clave auxiliar.

(ERR5): El extremo que recibe la Indicación de Notificación no ha podido descifrar el Código de Autenticación que le envía el Remoto, aunque si hizo el Recifrado.
Si AUTENTICACION es DES : Probable error en clave remota.
Si AUTENTICACION es RSA : Si el error se produce en la firma, el problema puede ser en la clave remota(Pública).
Si el error es en la incertidumbre, el problema puede ser en la clave local (privada).

(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): Claves incompatibles.

- Si en versión CRIPTOGRAFICA tiene 2.2, un (ERR9) significa que 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.

- Si en versión CRIPTOGRAFICA tiene 3.0 o 4.0 un (ERR9) significa que las claves de Intercambio externas utilizadas en el proceso de autenticación no coinciden en ambos extremos. Aún así, el mensaje EDITRAN que describe este error vendrá acompañado de otro que informa en cada extremo del "Label" de la clave de intercambio utilizada (8 últimos octetos diferentes de "blancos", de los 64 octetos de la etiqueta que identifica a una clave). De esta forma, ambos extremos pueden verificar que la Interfaz de claves externas identifica de forma correcta a la clave de intercambio externa que realmente se pretende utilizar.

```
|   ERR01 - EL EXTREMO LLAMANTE NO HA PODIDO HACER RECIFRADO DE CLAVES (SI NO |
|           HAY INTERFAZ DE CLAVES EXTERNAS) (CIFRADO V2.2).                  |
|         - ERROR AL OBTENER EL LABEL (CLAVE LOCAL) EN EL EXTREMO QUE INICIA  |
|           LA SESION (CIFRADO V3.0)                                          |
|                                                                             |
|   ERR02 - EL EXTREMO QUE SOLICITA AUTENTICAR SU TKE O SU CLAVE EXTERNA (SI  |
|           HAY INTERFAZ), NO PUDO CIFRAR CGO AUTENTICACION (CIFRADO V2.2).   |
|         - ERROR AL GENERAR LA INCERTIDUMBRE O LA FIRMA (CIFRADO V.30).      |
|           - SI AUTENT. DES, PROBABLE ERROR EN CLAVE LOCAL                   |
|           - SI AUTENT. RSA, SI EL ERROR SE PRODUCE EN LA FIRMA, CLAVE LOCAL |
|             ERRONEA.                                                        |
|           - SI AUTENT. RSA, SI EL ERROR SE PRODUCE EN LA INCERTIDUMBRE,     |
|             CLAVE REMOTA ERRONEA.                                           |
|   ERR03 - EL EXTREMO QUE SOLICITA ASOCIACION CON CAMBIO DECLAVE, NO PUDO    |
|           GENERAR CLAVE DE EMISION TKE NUEVA (CIFRADO V2.2).                |
|         - ERROR AL INTENTAR GENERAR CLAVE DE SESION (CIFRADO V3.0).         |
|           - SI AUTENTICACION ES DES, ERROR EN LA CLAVE LOCAL.               |
|           - SI AUTENTICACION ES RSA, ERROR EN LA CLAVE REMOTA.              |
|   ERR04 - EL EXTREMO QUE RECIBE SAP (INDICACION DE ASOCIACION), TUVO ERROR  |
|           AL RECIFRAR CLAVE TKR DE SU FICHERO (CIFRADO V2.2).               |
|         - ERROR AL OBTENER CLAVE REMOTA (CIFRADO V3.0).                     |
|   ERR05 - EL EXTREMO QUE RECIBE SAP (INDICACION DE ASOCIACION), NO PUDO     |
|           DESCIFRAR CODIGO DE AUTENTICACION DEL REMOTO (CIFRADO V2.2).      |
|         - ERROR AL INTENTAR DESCIFRAR LA INCERTIDUMBRE O FIRMA (CIFR. V3.0) |
|           - SI AUTENT. DES, PROBABLE ERROR EN CLAVE REMOTA                  |
|           - SI AUTENT. RSA, SI EL ERROR SE PRODUCE EN LA FIRMA PUEDE SER UN |
|             PROBLEMA EN LA CLAVE REMOTA (PUBLICA).                          |
|           - SI AUTENT. RSA, SI EL ERROR SE PRODUCE EN LA INCERTIDUMBRE, ES  |
|             UN PROBLEMA EN LA CLAVE LOCAL (PRIVADA).                        |
|   ERR06 - EL EXTREMO QUE RECIBE SAP (INDICACION DE ASOCIACION) CON CAMBIO   |
|           DE CLAVE, TUVO ERROR AL RECIFRAR LA CLAVE DE RECEPCION DEL REMOTO |
|           (TKR NUEVA) (CIFRADO V2.2).                                       |
|         - ERROR AL DESCIFRAR LA CLAVE DE SESION (CIFRADO V3.0).             |
|           - SI AUTENTICACION ES DES, ERROR EN LA CLAVE REMOTA.              |
|           - SI AUTENTICACION ES RSA, ERROR EN LA CLAVE LOCAL.               |
|   ERR07 - ERROR AL CIFRAR DATO (SESION ESTABLECIDA).                        |
|   ERR08 - ERROR AL DESCIFRAR DATO (SESION ESTABLECIDA).                     |
|   ERR09 - EL EXTREMO QUE RECIBE ASOCIACION, HA DESCIFRADO CGO.AUTENTICACION |
|           PERO ES INCORRECTO. LAS CLAVES SE HAN PERDIDO. DEBE DAR DE ALTA Y |
|           BAJA LA SESION EN AMBOS EXTREMOS (CIFRADO V2.2).                  |
|         - LA INCERTIDUMBRE O LA FIRMA DESCIFRADAS, NO COINCIDEN. LAS CLAVES |
|           EMPLEADAS SON DISTINTAS EN AMBOS EXTREMOS (CIFRADO V3.0).         |
|           - SI AUTENTICACION DES, ERROR EN LA CLAVE LOCAL.                  |
|           - SI AUTENTICACION RSA Y NO COINCIDE INCERTIDUMBRE, ERROR EN LA   |
|             CLAVE LOCAL.                                                    |
|           - SI AUTENTICACION RSA Y NO COINCIDE FIRMA, ERROR EN CLAVE REMOTA |
```

10. ANEXO E. FICHEROS TAMPONES

Son ficheros que pueden contener los datos correspondientes a una o varias Sesiones de Transmisión. Cada Sesión de Transmisión está compuesta por un registro de control, con los parámetros necesarios para la transmisión (número de registros a emitir o recibir, número de registros emitidos o recibidos, fecha y horas de transmisión, etc...), y N registros de datos.

Existen varios tipos de ficheros Tampones (específico, matricial compartido, público, matricial exci, etc). Para más información sobre los cambios, consulte el manual **ED52GTAC**.

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