

EDITRAN 5.2

Descripción de pasos a seguir al descargar
CICS

Guía descarga de versión

junio de 2019

1. INTRODUCCION	1-1
2. OPERACIONES A REALIZAR AL RECIBIR EL PRODUCTO.....	1
2.1. Recepción de software	1
2.1.1. Recepción de licencia	2
2.1.2. Recepción de versión nueva	3
2.1.3. Recepción de fase nueva	3
2.2. Descarga del software	3
2.3. Adaptación de los jcls recibidos	4
2.4. Preparativos iniciales.....	5
2.5. Definiciones y recursos.....	7
2.5.1. Programas	8
2.5.2. Transacciones.....	8
2.5.3. Ficheros.....	8
2.5.4. Terminales	8
2.5.5. Otros.....	8
2.6. Criptografía.....	8
2.6.1. Programas criptografía entornos DES.....	8
2.6.2. Programas criptografía entornos RSA (es necesario disponer de DES).....	9
2.6.3. JCLS con entornos DES y RSA.....	11
2.6.4. Versiones de CRIPTOlib.....	11
2.6.5. FICHEROS en entornos DES y RSA.....	11
2.6.6. PASOS INSTALACION criptografía.....	12
2.6.7. Gestión de claves de intercambio.....	12
2.7. Migraciones.....	13

1. INTRODUCCION

Este documento pretende ser una guía abreviada que ayude a localizar los distintos puntos a tener en cuenta a la hora de instalar EDITRAN. En él mismo sólo se expondrá el modelo básico de tratamiento de la información recibida, puesto que a partir del mismo pueden establecerse múltiples variantes.

Se recomienda realizar 2 operaciones que en este manual no se van a tener en cuenta:

- ✓ Si se va a realizar una reinstalación (actualización de versión ó fase), realizar previamente un backup de los ficheros y librerías EDITRAN.
- ✓ Realizar pruebas en otro CICS antes de efectuar el paso a explotación

En EDITRAN, la mayoría de los recursos tiene una nomenclatura standard, así por ejemplo en el string ZTxyz*:

- El carácter x indica la versión. Para 4.1, 5.0 , 5.1 y 5.2, x=B (ZTB*).
- El carácter y indica el producto al que se hace referencia. Los valores de y pueden ser, entre otros: P=EDITRAN/P, G=EDITRAN/G, E=EDITRAN/E, T=EDITRAN/TR, L=Licencia, M=Migración, S=Criptografía, etc
- El carácter z indica el tipo de recurso. Los valores de z pueden ser, entre otros: F=Fichero, B=programa batch, P=Programa on-line, M=Mapa, C=Copy, I=Include, J=jcl, Q=Procedimiento, Q=TS queue, etc.

En este documento, se hace normalmente referencia a ZTB* (v5.2).

2. OPERACIONES A REALIZAR AL RECIBIR EL PRODUCTO.

Las operaciones a realizar serían:

- Recibir el producto.
- Descargar el software.
- Adaptar el software (jcls-procedimientos-etc)
- Adaptaciones iniciales
- Definir recursos necesarios.
- Migrar
- Adaptar licencia
- Pruebas
- Paso a explotación

2.1. Recepción de software

EDITRAN, puede recibirse de distintas formas:

- ✓ Vía EDITRAN (normalmente para reinstalaciones)
- ✓ Vía XMIT (instalaciones nuevas sin conectividad a INDRA)

Cuando una entidad recibe EDITRAN, normalmente, recibe varios ficheros, según los distintos productos EDI que tenga contratados y dentro de cada producto, según el software recibido (por ejemplo jcls, ejecutables, etc). También, pueden recibirse ficheros de licencia EDITRAN. Hay por tanto, tipos diferentes de ficheros en cuanto a su formato: fuentes, jcl, ejecutables y licencias. Según su contenido hay los siguientes productos, además de la caja principal de EDITRAN/P y EDITRAN/G:

1. TCP/IP. Interfaz de comunicaciones TCP/IP.
2. DES o AES. Criptografía. Algoritmo de claves DES o AES. Dentro de esta opción, se pueden presentar las siguientes subopciones:
 - 2.1. Que el cliente no disponga de ningún producto propio DES. En este caso, el software recibido se dividirá en 2 partes: CRIPTOlib/DES y APIs EDITRAN DES para CRIPTOlib/DES.
 - 2.2. Que el cliente disponga de ICSF-CMOS. En este caso, sólo se requiere recibir APIs EDITRAN DES o AES para ICSF-CMOS.
 - 2.3. Que el cliente disponga de TSS. En este caso, sólo se requiere recibir APIs EDITRAN DES para TSS.
3. RSA Criptografía. Algoritmo de claves RSA. Se recibirán 2 subproductos. CRIPTOlib/RSA y APIs EDITRAN (apis RSA para CRIPTOlib/RSA y apis RSA para producto DES). Además, el algoritmo RSA requiere funciones DES, por lo que deberá recibirse el software correspondiente de DES.
4. TDES. Criptografía Triple DES. Se entrega con el algoritmo DES.
5. AES. Criptografía Triple AES. Se entrega con el algoritmo AES.

6. LZW. Compresión de datos EDITRAN/G con algoritmo LZW.
7. EDITRAN/E. Estadísticas, monitorización y alarmas. Para las alarmas, requiere la recepción de software para host y software para UNIX-WINDOWS.
8. EDITRAN/TR. Módulo transaccional de consultas.
9. EDITRAN/MQ. Gestión de colas de mensajes.
10. EDITRAN/FF. Firma electrónica de ficheros.
11. EDITRAN/IC. Confirmación de datos de aplicación (sólo requiere licencia el extremo emisor de datos).
12. EDITRAN/PROXY. EDITRAN Pasarela de datos TCP/IP a TCP/IP. Requiere la recepción de software para host y software para UNIX-WINDOWS.

Cuando una entidad reciba software, normalmente, estará dividido por tanto, según los productos contratados. Un ejemplo sería el siguiente:

Por EDITRAN se han cargado versión 5.2 fase 00, que corresponde a:

- 1.- JCLS EDITRAN/P+/G (jcls y procedimientos)
- 2.- Ejecutables EDITRAN/P y G
- 3.- JCLS CRIPTO/lib DES
- 4.- Ejecutables CRIPTO/lib DES.
- 5.- JCLS API EDITRAN con CRIPTO/lib DES
- 6.- Ejecutables API EDITRAN con CRIPTO/lib DES.
- 7.- JCLS CRIPTO/lib RSA
- 8.- Ejecutables CRIPTO/lib RSA.
- 9.- Ejecutables API CRIPTO/lib RSA con CRIPTO/lib DES.
- 10.- Ejecutables API EDITRAN con CRIPTO/lib RSA.
- 11.- Fichero de licencia 5.2 para ENTIDAD XXX (9999) (EDITRAN/P, EDITRAN/G, TCP, DES, Triple DES, RSA, Interfaz X.25).

En el ejemplo anterior se ha cargado el standard EDITRAN/P y EDITRAN/G en los dos primeros ficheros. El software de DES y Triple DES va incluido en ficheros 3 a 6. El software para RSA va incluido en los ficheros 7 a 10. Por último, se incluye un fichero de licencia que permite la utilización del software anteriormente descrito”.

Estos ficheros, se dividen en 3 tipos:

- ◆ JCLS (ficheros 1, 3, 5 y 7)
- ◆ Ejecutables (ficheros 2, 4, 6, 8, 9 y 10)
- ◆ Licencia (fichero 11)

A veces, una entidad no requiere licencia, puesto que tiene la misma en vigor y sólo quiere actualizar software de una fase más moderna de la misma versión EDITRAN que tiene en producción. Otras veces, el único software recibido es la licencia, que está a punto de caducar.

2.1.1. Recepción de licencia

Si se recibe licencia, significa que se va a proceder a actualizar la misma. En este caso:

- Si se recibe versión 3.1, pasar el jcl ZTALJG00 con el fichero recibido, de forma que se incorpore al VSAM ZTALFLIC.

- Si se recibe versión 4.0 inferior a fase 7, pasar el jcl ZTBLJG00 con el fichero recibido, de forma que se incorpore al VSAM ZTBLFLIC.
- Si se recibe versión superior a 4.0 fase 6, pasar el jcl ZTBLJG02 con el fichero recibido, de forma que se incorpore al VSAM ZTBPFPE y al ZTBGFPER.

2.1.2. Recepción de versión nueva

La recepción de la nueva versión implica siempre la recepción de lo siguiente:

- JCLS EDITRAN/P y EDITRAN/G
- Ejecutables
- Licencia de la nueva versión
- Otros (jcls - ejecutables), productos contratados (si es que no fueron cargados en las anteriores).

2.1.3. Recepción de fase nueva

- En este caso, sólo debe llegar lo que se haya modificado entre la fase en explotación y la fase actualizada. Sin embargo, si ha transcurrido más de 1 fase entre una y otra, lo normal es reactualizar todo el software, de forma que se eviten errores por falta de actualización. La licencia llegará en este caso, sólo si es necesario por temas de caducidad.

2.2. Descarga del software

Una vez recibido el software, se descargará en las librerías descritas (recepción tipo standard), las cuales se crearán en el jcl de iebcopy;

θ Librería JCL's con las siguientes características :

```
//JCLS DD DSN=Puntero.JCLLIB,DISP=(NEW,CATLG), X
// DCB=(DSORG=PO,RECFM=FB,LRECL=80,BLKSIZE=6160), X
// SPACE=(CYL,(1,1,15)),UNIT=Unidad,VOL=SER=Volumen
```

θ Librería EJECUTABLES con las siguientes características :

```
//LOAD DD DSN=Puntero.LOADLIB,DISP=(NEW,CATLG), X
// DCB=(DSORG=PO,RECFM=U,LRECL=0,BLKSIZE=19069), X
// SPACE=(CYL,(25,0,100)),UNIT=Unidad,VOL=SER=Volumen
```

Se podrán descargar tantas librerías como se quiera, es decir, puede que a algún cliente le interese crear varias librerías de ejecutables. En ese caso, deberán incluirse todas ellas en los procedimientos EDITRAN y en el arranque de CICS. En este manual, se tratará como que todos los ejecutables están en la misma librería.

Si se recibe fichero de licencia, lo dejaremos sin hacer IEBCOPY, pendiente de actualizar la licencia.

Se recomienda que en este paso de creación de librerías se identifique lo siguiente con el puntero creado:

- ❖ EDITRAN
- ❖ Versión recibida. Por ejemplo, V4R1. En el caso de ficheros tampones, cuando se reciban, se recomienda no poner versión. El motivo es que en EDITRAN/P se guarda el dsname de los tampones en el fichero de perfiles, de forma que si se actualiza una versión, debería seguir valiendo el mismo tampón. Si no se hace así, cuando se actualiza

la versión, debería refrescarse la fct con el nuevo nombre y todos los perfiles EDITRAN/P. Otra posibilidad es que los tampones no cambien de nombre pero tengan un puntero de una versión antigua, pero esto parece poco "limpio".

Es importante que los nombres de librerías y punteros no varíen. Los motivos son:

- Los nombres que pongamos a las librerías, o a los punteros, van a ser actualizados en todos los jcls y procedimientos.
- El nombre de librería de ejecutables estará en arranque de CICS.

2.3. Adaptación de los jcls recibidos

Los jcls, procedimientos, etc, todos ellos recibidos en librerías jcl, deben ser adaptados a los nombres de la entidad. Cuando se reciben, llevan en los nombres de librería puntero.indra, el cual debe ser sustituido por el puntero adecuado. Para ello, existirá en la entidad una clist ZTXINST que deberá ser ejecutada para que realice la conversión descrita.

Para ello, se entrará en la librería donde esté ubicada dicha clist. Una vez allí, ejecutar la Clist ZTXINST de esta forma: **TSO EX 'librería.posicionada(ZTXINST)'** y saldrá lo siguiente:

```
*****
* TECLEAR EL NOMBRE DE LA LIBRERIA DONDE SE ENCUENTRA *
*          ESTA CLIST, EL PANEL Y LA MACRO A EJECUTAR *
*****
(TECLEAR FIN PARA CANCELAR) :
```

Teclear nombre de librería posicionada

```
*****
* TECLEAR EL NOMBRE DE LA MACRO A EJECUTAR *
*****
(TECLEAR FIN PARA CANCELAR) :
```

Teclear ZTXINSM1 y saldrá el siguiente panel :

```
-----
| 01/12/97                                I N D R A                                KI0D978 |
| 13:32:00  EJECUTA UNA MACRO PARA CAMBIOS MASIVOS EN UNA LIBRERIA |
|-----|
| Libr. a cambiar : KI.PMED.CZTB.JCLS |
| Instalar Estadísticas (EDITRAN/E) (S/N) : N |
| F.Job1: //EDITRANX JOB (ACCOUNT), 'EDITRAN V4R1', CLASS=A, |
| F.Job2: //          MSGCLASS=X,MSGLEVEL=(1,1),NOTIFY={ }SYSUID |
| Prefijo Librerías CICS : CICSTS13 |
| Lib. ejecutables : EDITRAN.V4R1.LOADLIB |
|-----|
| Prefijo Fich. Perfiles : EDITRAN.V4R1 |
| Prefijo Fich. Temporales: EDITRAN.TEM |
| Clase Internal Reader : A          Nombre del Cics : CICSEDIT |
| Grupo Discos Trabajo : SYSDA      Vol. para Fich. Perfiles : SMS001 |
|-----|
| PULSAR PF3 PARA SALIR |
|-----|
|-----|
| MIEMBRO PROCESADO : |
| NUMERO DE MIEMBROS: |
|-----|
```

Se modificarán todos los datos necesarios. Esta clist modifica todos los jcl's de la librería especificada en el campo '**Libr. a cambiar**'. Si se ha contratado el módulo de estadísticas, rellene el campo adecuado. Si se equivoca en los nombres y pulsa intro, deberá restaurar la librería de jcls desde el fichero recibido, y volver a pasar la clist.

A continuación, se deben seguir los siguientes pasos:

- θ Si se reciben procedimientos:
 - θ EDITRAN proporciona procedimientos standard. En algunas entidades, se crean procedimientos específicos. Copiar o no (dependiendo de la versión del MVS) los 6 procedimientos a la librería PROCLIB. Esto no es necesario con versión 4.2 o superior del MVS, ya que existe una ficha Jcl donde se especifica la librería de donde ejecutar los procedimientos, por lo tanto los procedimientos pueden ser ejecutados desde la librería de JCL's del producto, especificando en perfiles EDITRAN/P la siguiente ficha :

```
//Libproc JCLLIB ORDER=Puntero.JCLLIB
```

- θ Si la entidad dispone de procedimientos específicos, adaptarlos si fuera necesario a los nuevos cambios recibidos, etc. Siempre debe compararse los procedimientos standard recibidos con los antiguos standard o con los antiguos específicos, para tener claro si ha habido cambios y cuales son. Los procedimientos standard son, entre otros (la nomenclatura standard es ZTBGP*):

- ZTBGPMC** Procedimiento previo a emisión de Macroficheros.
- ZTBGP1C** Procedimiento previo a emisión.
- ZTBGP2C** Procedimiento previo a recepción.
- ZTBGP3C** Procedimiento posterior a emisión.
- ZTBGP4C** Procedimiento posterior a recepción.
- ZTBGP5C** Procedimiento de excepción.
- ZTBGP6C** Procedimiento de modificación Estados EDITRAN/G.

Existen otros procedimientos, para otro tipo de situaciones:

ZTBGP1EA Procedimiento para enviar alarma sms a los servicios UNIX.

ZTBGP1CF Procedimiento previo a emisión, para firma electrónica de ficheros.

ZTBGP1GC Procedimiento previo a emisión para la aplicación TELEGC, gestión de claves de intercambio.

ZTBGP3GC Procedimiento posterior a emisión para la aplicación TELEGC, gestión de claves de intercambio.

ZTBGP4GC Procedimiento posterior a recepción para la aplicación TELEGC, gestión de claves de intercambio.

2.4. Preparativos iniciales.

- θ Si se creó librería de ejecutables, apfautorizarla en APF e incluirla en arranque de CICS.
- θ Si se recibe una versión nueva que requiera la creación de ficheros nuevos, ó si se trata de una instalación inicial, pasar los jcls descritos a continuación (sólo los que se necesiten):

Producto	Fichero	Jcl inic.	Descripción	Tipo	Incluir en procedimientos
EDITRAN/EA Alarmas	ZTBEFAL	ZTBEJIAL	Log alarmas	Relativo	Todos.
EDITRAN/EA Alarmas	ZTBEFPE	ZTBEJIPE	Perfil alarmas	KSDS	Todos.
EDITRAN/EA Estadísticas	ZTBEFMT	ZTBEJIMT	Estadísticas ses. transmisión	KSDS	Todos.
EDITRAN/EA Estadísticas	ZTBEFMP	ZTBEJIMP	Estadísticas ses. presentación	KSDS	Todos.

EDITRAN/EA Estadísticas	ZTBEFMH	ZTBEJIMH	Estadísticas histórico	Relativo	Todos.
EDITRAN/FF Firma	ZTBFFLO	ZTBFJILO	Log Firma USS	Relativo	Previo emisión y posterior recepción
EDITRAN/FF Firma	ZTBFFPE	ZTBFJIPE	Perfil Firma USS	KSDS	Previo emisión y posterior recepción
EDITRAN/G	ZTBGFES	ZTBGJIES	Estados G	KSDS	Todos.
EDITRAN/G	ZTBGFLO	ZTBGJILO	LOG G	Relativo	Todos.
EDITRAN/G	ZTBGFPE	ZTBGJIPE	Perfiles G	KSDS	Todos.
EDITRAN/G	ZTBGFQF	ZTBGJIQF	Colas de ficheros	KSDS	Previo a emisión y posterior a emisión
EDITRAN/G	ZTBGFTCO	ZTBGJITC	Tablas de conversión	Plano	Previos a emisión y posteriores a recepción. No definido a CICS
EDITRAN/GC	ZTBPFGC	ZTBPJIGC	Gestión de claves	KSDS	Requiere RSA y DES. Previo emisión y posterior recepción. Tiene proc. especiales para TELEGC
EDITRAN/P	ZTBPFLO	ZTBPJILO	LOG P	Relativo	NO
EDITRAN/P	ZTBPFPE	ZTBPJIPE	Perfiles P	KSDS	Todos
EDITRAN/P	ZTBPFTR	ZTBPJITR	TRAZA P	Relativo	NO
EDITRAN	TAMPON	ZTBPJITD	Tampón Excii ó desatendido	KSDS	NO (alocación dinámica)
EDITRAN	TAMPON	ZTBPJITE	Tampón Específico	KSDS	NO (alocación dinámica)
EDITRAN	TAMPON	ZTBPJITM	Tampón Matrcial	KSDS	NO (alocación dinámica)
Criptolib/DES	FICHKDES	JGENFICH	Claves DES	KSDS	Previos a emisión y posterior a recepción.
Criptolib/RSA	FICKRSA	XSCRFIL	Claves RSA	KSDS	Previos a emisión y posterior a recepción.

En CICS, (SIN INCLUIR TAMPONES) :

```

Fil (ZTBEFAL ) Vsa Clo Ena Rea Upd Add Bro Del Sha
      Dsn( KI.EGDC.ZTBE.ZTBEFAL )
Fil (ZTBEFMH ) Vsa Ope Ena Rea Bro Sha
      Dsn( KI.EGDC.ZTBE.ZTBEFMH )
Fil (ZTBEFMP ) Vsa Ope Ena Rea Bro Sha
      Dsn( KI.EGDC.ZTBE.ZTBEFMP )
Fil (ZTBEFMT ) Vsa Ope Ena Rea Upd Add Bro Del Sha
      Dsn( KI.EGDC.ZTBE.ZTBEFMT )
Fil (ZTBEFPE ) Vsa Clo Ena Rea Upd Add Bro Del Sha
      Dsn( KI.EGDC.ZTBE.ZTBEFPE )
Fil (ZTBFFLO ) Vsa Clo Ena Rea Bro Sha
      Dsn( KI.EIDC.ZTBG.ZTBFFLOG )
Fil (ZTBFFPE ) Vsa Clo Ena Rea Upd Add Bro Del Sha
      Dsn( KI.EIDC.ZTBG.ZTBFFPER )
Fil (ZTBGFES ) Vsa Ope Ena Rea Bro Sha
      Dsn( KI.EIDC.ZTBG.ZTBGFEST )
Fil (ZTBGFLO ) Vsa Ope Ena Rea Bro Sha
      Dsn( KI.EIDC.ZTBG.ZTBGFLOG )
Fil (ZTBGFPE ) Vsa Ope Ena Rea Upd Add Bro Del Sha
      Dsn( KI.EIDC.ZTBG.ZTBGFPER )
Fil (ZTBGFQF ) Vsa Ope Ena Rea Upd Add Bro Del Sha
      Dsn( KI.EIDC.ZTBG.ZTBGFQF )
Fil (ZTBPFLO ) Vsa Ope Ena Rea Upd Add Bro Del Sha
  
```

```

    Dsn( KI.EGDC.ZTBP.ZTBPFLO )
Fil(ZTBPFPE ) Vsa Ope Ena Rea Upd Add Bro Del Sha
    Dsn( KI.EGDC.ZTBP.ZTBPFPE )
Fil(ZTBPFTR ) Vsa Ope Ena Rea Upd Add Bro Del Sha
    Dsn( KI.EGDC.ZTBP.ZTBPFTR )
Fil(FCHKDES) Vsa Ope Ena Rea Upd Add Bro Del Sha
    Dsn( KI.GCDA.CIFRADO.FCHKDES )
Fil(FCHKRSA) Vsa Clo Ena Rea Upd Add Bro Del Sha
    Dsn( KI.GCDA.CIFRADO.FCHKRSA )
  
```

- Archivos de **EDITRAN/G**, jcls **ZTBGJlxx**, donde:
 - XX=**ES**, fichero de Estados (indexado).
 - XX=**PE**, fichero de Perfiles (indexado).
 - XX=**LO**, fichero de Log (relativo).
 - XX=**QF**, fichero de colas de ficheros (indexado).
- Archivos de **EDITRAN/P**, jcls **ZTBPJlxx**, donde:
 - XX=**GC**, fichero de Gestión de claves de intercambio (indexado).
 - XX=**PE**, fichero de Perfiles (indexado).
 - XX=**LO**, fichero de Log (relativo).
 - XX=**TR**, fichero de Traza (relativo).
 - XX=**TE, TM, TD**, ficheros tampones: específicos, matriciales, desatendidos-excii, etc. (indexados).
- Archivos de **EDITRAN/FF**, Firma electrónica, jcls **ZTBFJlxx**, donde:
 - XX=**PE**, fichero de perfiles (indexado).
 - XX=**LO**, fichero log (relativo).
- Archivos de **EDITRAN/EA**, en éste caso, sólo si tiene contratado el producto Estadísticas, monitorización y alarmas, jcls **ZTBEJlxx**, donde:
 - XX=**PE**, fichero de Perfiles de alarmas (e-mail, sms, externas) (indexado).
 - XX=**AL**, fichero de Log de alarmas (e-mail, sms, externas) (relativo).
 - XX=**MT**, fichero de Monitorización-Estadísticas transmisiones (indexado).
 - XX=**MP**, fichero de Monitorización-Estadísticas presentaciones (indexado).
 - XX=**MH**, fichero de Monitorización-Estadísticas Histórico (relativo).
- Archivos de **CRIPTOlib**, jcls:
 - FCHKRSA, fichero de rsa (indexado).
 - FCHKDES, fichero de DES (indexado).
 -

θ Si se ha recibido el fichero de licencia, incorporar la misma.

2.5. Definiciones y recursos.

Se recomienda seguir el manual de instalación y el de reinstalación, así como los manuales específicos de cada producto contratado. Cuando se reciba una fase o una nueva versión, debe verificarse si hay "nuevos recursos", los cuales hay que definir:

- ✓ Programas
- ✓ Transacciones
- ✓ Ficheros
- ✓ Terminales

- ✓ Le/370 (parámetros batch y on-line).
- ✓ Tabla de inicialización de CICS
- ✓ Otros (TCP/IP, vtam, ncp, etc)

2.5.1. Programas.

Los necesarios para ser dados de alta en el monitor de teleproceso, aparecen descritos en los distintos manuales (instalación de EDITRAN/P+G, EDITRAN/E, EDITRAN/TR, EDITRAN/MQ, Criptografía, TCP/IP, etc). Para algunos de ellos, se proporciona una tabla (ver PPT* de la librería de jcls).

2.5.2. Transacciones.

Las necesarias para ser dadas de alta en el monitor de teleproceso, aparecen descritos en los distintos manuales (instalación de EDITRAN/P, EDITRAN/E, TCP/IP, etc). Para algunos de ellos, se proporciona una tabla (ver PCT* de la librería de jcls).

2.5.3. Ficheros

Los necesarios para ser dados de alta en el monitor de teleproceso, aparecen descritos en los distintos manuales (instalación de EDITRAN/P+G, EDITRAN/E, Criptografía, TCP/IP, etc). Para algunos de ellos, se proporciona una tabla (ver FCT* de la librería de jcls).

2.5.4. Terminales.

Los necesarios para ser dados de alta en el monitor de teleproceso, aparecen descritos en los distintos manuales (instalación de EDITRAN/P, etc). Para algunos de ellos, se proporciona una tabla (ver TCT* de la librería de jcls).

2.5.5. Otros.

Se describen en los distintos manuales de productos y en el manual de instalación - reinstalación. Si cambia de versión y aprovecha líneas de comunicaciones, etc, debe cambiar las definiciones de terminales lu ficticia y lu real (transacción arrancada), así como transid listener tcp/ip, etc, de forma que apunten a las nuevas transacciones.

2.6. Criptografía.

A continuación, se muestran todos los recursos de criptografía.

2.6.1. Programas criptografía entornos DES.

En negrita están marcados los que deben de darse de alta en el monitor de teleproceso.

	EDITRAN 3.1	EDITRAN 4.0	EDITRAN 4.1- 5.2
CRIPTO/lib DES		CRIPDBKS CRIPDB01 CRIPDB02 CRIPDB03 CRIPDOKS Cobol CRIPDOK1 C CRIPDO01 C CRIPDO02 C CRIPDO03 C PGINDES PINSTDES	SCDALBAO C SCDALTA SCDALTAO Cobol SCDALTAX SCDBAJA SCDBAJAO Cobol SCDBAJAX SCDCIFR SCDCIFRO C SCDDESC SCDDESCO C SCDGMAC

			SCDGNAP SCDGNAPO C SCDHMD5 SCDHSHA1 SCDIHMK SCDOPER SCDOPERO C SCDRAND SCDRAPL SCDRAPLO C SCDDROPE SCDDROPEO C
APIS CRIPTO/lib DES	ZTAGB051 ZTAGB052 ZTAGB053 ZTAPBCRL ZTAPOC1 C ZTAPOC2 C ZTAPOC3 C	ZTBSBCRL ZTBSBD01 ZTBSBD02 ZTBSBD03 ZTBSOD01 C ZTBSOD02 C ZTBSOD03 C	ZTBSBCRL ZTBSBD01 ZTBSBD02 ZTBSBD03 ZTBSOD01 Cobol ZTBSOD02 Cobol ZTBSOD03 Cobol
APIS DES ICSF	ZTAGB051 ZTAGB052 ZTAGB053 ZTAPBICS ZTAPOC1 Cobol ZTAPOC2 Cobol ZTAPOC3 Cobol		ZTBSBD01 ZTBSBD02 ZTBSBD03 ZTBSBICS ZTBSOD01 Cobol ZTBSOD02 Cobol ZTBSOD03 Cobol
APIS DES TSS (Relinkar programas)	ZTAGB051 ZTAGB052 ZTAGB053 ZTAPBTSS ZTAPOC1 Cobol ZTAPOC2 Cobol ZTAPOC3 Cobol		ZTBSBD01 ZTBSBD02 ZTBSBD03 ZTBSBTSS ZTBSOD01 Cobol ZTBSOD02 Cobol ZTBSOD03 Cobol

2.6.2. Programas criptografía entornos RSA (es necesario disponer de DES).

En negrita están marcados los que deben de darse de alta en el monitor de teleproceso.

	EDITRAN 3.1	EDITRAN 4.0	EDITRAN 4.1-5.0, 5.1 y 5.2
CRIPTO/lib RSA		RSBENQD RSBVVSAM RSBX0DEL RSBX0INI RSBX1GEN RSBX2EMI RSBX3REC RSBX4FIR RSBX5VER RSBX6EDK RSBX7RDK RSOXR002 Cobol RSOXR003 Cobol RSOXR004 Cobol	SCRBNQD SCRVSAM SCRFILE0 SCRFILE1 SCRGDESB SCRGDESO Cobol SCRGDESX SCRGDE1B SCRGDE10 C SCRGFIRB SCRGFIRO Cobol SCRGFIRX

	RSOXR005 Cobol RSOXR006 Cobol RSOXR007 Cobol RSOXR008 Cobol RSOXR009 Cobol RSOXR041 C RSOXR051 C RSOXR081 C RSOXR091 C RSRXR001 RSRXR002 RSRXR003 RSRXR004 RSRXR005 RSRXR006 RSRXR007 RSRXR008 RSRXR009 RSRXR011 RSRXR041 RSRXR051 RSRXR081 RSRXR091	SCRGF11B SCRGF110 C SCRKDELB SCRKEXPB SCRKEXPO Cobol SCRKEXPX SCRKGENB SCRKGENX SCRKGE1B SCRKIMPB SCRKIMPO Cobol SCRKIMPX SCRDES SCRDESO Cobol SCRDESX SCRDE1B SCRDE10 C SCRVFIRB SCRVFIRO Cobol SCRVFIRX SCRVF11B SCRVFI10 C SCRSET Cobol
APIS RSA	CRIPTO/lib ZTAGBR04 ZTAGBR05 ZTAGBR08 ZTAGBR09 ZTAPOR04 Cobol ZTAPOR05 Cobol ZTAPOR08 Cobol ZTAPOR09 Cobol	ZTBSBR04 ZTBSBR05 ZTBSBR08 ZTBSBR09 ZTBSOR04 Cobol ZTBSOR05 Cobol ZTBSOR08 Cobol ZTBSOR09 Cobol
APIS RSA para CRIPTOLib/DES, ICSF y TSS (distinto software en cada caso) Si es TSS, debe relinkar progr.	RSBOCRLD (sólo si es Criptolib/DES) RSBOICSF (sólo si es ICSF) RSBOTSS (sólo si es TSS) RSOXDKS0 Cobol RSOXD001 Cobol (C en Criptolib/des) RSOXD002 Cobol (C en Criptolib/des) RSOXD003 Cobol (C en Criptolib/des) RSRXDKS0 RSRXD001 RSRXD002 RSRXD003	SCRDES0B SCRDES00 Cobol SCRDES1B SCRDES10 Cobol SCRDES2B SCRDES20 Cobol SCRDES3B SCRDES30 Cobol

2.6.3. JCLS con entornos DES y RSA.

	EDITRAN 3.1	EDITRAN 4.0	EDITRAN 4.1-5.0 5.1 y 5.2	Observaciones
CRIPTO/lib DES		JCAMBHMK JINSTDES JINCFICH	JCAMBHMK JGENFICH XSCDALTA XSCDBAJA	Cambio de clave maestra de FICHKDES Generación inicial e instalación de clave maestra FICHKDES Incorporación de clave de transporte Borrado de clave de transporte
APIS CRYPTO/lib DES	ZTAPJCRL		ZTBSJCRL	Incorpora 2 labels de entorno local EDITRAN a FICHKDES
APIS DES ICSF	ZTAPJICS		ZTBSJICS	Incorpora 2 labels de entorno local EDITRAN a CKDS
APIS DES TSS	ZTAPJTSS ZTAPJLOT		ZTBSJTSS ZTBSJLOT	Incorpora 2 labels de entorno local EDITRAN a KS Relink para resolver verbos TSS
CRIPTO/lib RSA		JORSADEL JORSAINI J1RSAGEN J2RSAEMI J3RSAREC J4RSAFIR J5RSAVER J6RSAEDK J7RSARDK	XSCRKDEL XSCRKGEN XSCRKEXP XSCRKIMP XSCRGFIR XSCRVFIR XSCRFILE XSCRGDES XSCRDES	Borrado de registro en FICHKRSA Instalación FICHKRSA Generación de pareja privada y pública Exportación de la pública local Importación de la pública remota Generación de firma digital Verificación de firma digital Envío de clave des cifrada con pública e incorporación DES Recepción clave des cifrada pública e incorporación DES Instalación FICHKRSA y generación de pública-privada Genera clave DES y la cifra bajo clave pública Extrae clave DES de un bloque cifrado con clave pública
APIS RSA para CRYPTO/lib DES		JRSOICRLD		Incorpora claves auxiliares en FICHKDES
APIS RSA para ICSF		JRSOICSF		Incorpora claves auxiliares en CKDS
APIS RSA para TSS		JRSLKEOT JRSOTSS	JRELINKO	Relink para resolver verbos TSS Incorpora claves auxiliares en KS
EDITRAN	ZTAPJMIG		ZTBPMIG	Incorpora 2 labels de entorno local EDITRAN

2.6.4. Versiones de CRIPTOLib.

A continuación se muestra el software de CRIPTOLib que debe recibirse en función de la versión EDITRAN.

	EDITRAN 3.1	EDITRAN 4.0	EDITRAN 4.1-5.0, 5.1 y 5.2
CRIPTOlib DES	V 2.0		V 3.0
CRIPTOlib RSA	V 2.0		V 3.0

2.6.5. FICHEROS en entornos DES y RSA.

ENTORNO CRIPTOGRAFICO	Tipo	Fichero
DES	CRIPTO/lib DES	FICHKDES
	ICSF	CKDS
	TSS	KS
RSA (NECESARIO DISPONER DES)	CRIPTO/lib RSA	FICHKRSA

```

DEFINE FILE (FICHKDES) GROUP (EDITRAN) Fichero con claves CRIPTOLib/DES
DSNAME (Puntero. FICHKDES)
LSRPOOLID (NONE) RECORDFORMAT (F)
ADD (NO) BROWSE (YES) DELETE (NO) READ (YES) UPDATE (NO)

DEFINE FILE (FICHKRSA) GROUP (EDITRAN) Fichero con claves CRIPTOLib/RSA
DSNAME (Puntero. FICHKRSA)
LSRPOOLID (NONE) RECORDFORMAT (F)
ADD (NO) BROWSE (YES) DELETE (NO) READ (YES) UPDATE (NO)

```

2.6.6. PASOS INSTALACION criptografía.

1. Relinkar programas (sólo en caso de entorno DES con TSS)
2. En los procedimientos previos a emisión y posterior a emisión, incluir:
 - 2.1. Si entorno DES, el fichero FICHKDES (DD FICHKDES DSN=xxx,DISP= SHR)
 - 2.2. Si entorno RSA, el fichero FICHKRSA (DD FICHKRSA DSN=xxx,DISP= SHR)
 - 2.3. Librerías añadir en STEPLIB las librerías de RUN-TIME de LE/370 (SCEERUN), y las del entorno DES correspondiente, teniendo en cuenta que deben estar todas apfautorizadas
3. En arranque de monitor de teleproceso añadir las librerías necesarias LE/370, entorno DES, ejecutables EDI, etc

```
//DFHRPL DD DSN=CEE.SCEECICS,DISP=SHR
//          DD DSN=CEE.SCEERUN,DISP=SHR
```
4. Dar de alta los recursos en el monitor de teleproceso (programas y ficheros)
5. Inicializar fichero DES (FICHKDES, CKDS o KS) y/o FICHKRSA e incorporar clave maestra, etc.

	EDITRAN 3.1	EDITRAN 4.0	EDITRAN 4.1-5.0 5.1 y 5.2	Observaciones
CRIPTO/lib DES		JINSTDES	JGENFICH	Generación inicial e instalación de clave maestra FICHKDES
CRIPTO/lib RSA		JORSAINI J1RSAGEN	XSCRKGEN XSCRFILE	Instalación FICHKRSA Generación de pareja privada y pública Instalación FICHKRSA y generación de pública-privada

6. Incorporar 2 lábeles de 8 octetos en entorno local de EDITRAN/P, por ejemplo LEDITRAN Y REDITRAN:

	EDITRAN 3.1	EDITRAN 4.0	EDITRAN 4.1.5.0 5.1 y 5.2	Observaciones
EDITRAN	ZTAPJMIG		ZTBPJMIG	Incorpora 2 lábeles de entorno local EDITRAN

7. Incorporar en entorno DES los lábeles que se incorporaron en el entorno local de EDITRAN

	EDITRAN 3.1	EDITRAN 4.0	EDITRAN 4.1.5.0 5.1 y 5.2	Observaciones
APIS CRIPTO/lib DES	ZTAPJCRL		ZTBSJCRL	Incorpora 2 lábeles de entorno local EDITRAN a FICHKDES
APIS DES ICSF	ZTAPJICS		ZTBSJICS	Incorpora 2 lábeles de entorno local EDITRAN a CKDS
APIS DES TSS	ZTAPJTSS		ZTBSJTSS	Incorpora 2 lábeles de entorno local EDITRAN a KS

2.6.7. Gestión de claves de intercambio.

Consulte el manual **EGC52USUA**.

2.7. Migraciones.

Probablemente, una vez definido todo haya que proceder a la migración de los perfiles a la nueva versión-fase. Para migraciones consulte el manual **ED52RINC**. Debido a los cambios y mejoras que se van produciendo, en cada fase aparecen nuevas funcionalidades que hacen que deban inicializarse nuevos campos o reposicionar campos antiguos. En el caso de migración de 3.1 a 4.x, hay un paso inicial que deja un fichero con los parámetros que van a ser traspasados en la migración. Verifique parámetros de salida.

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