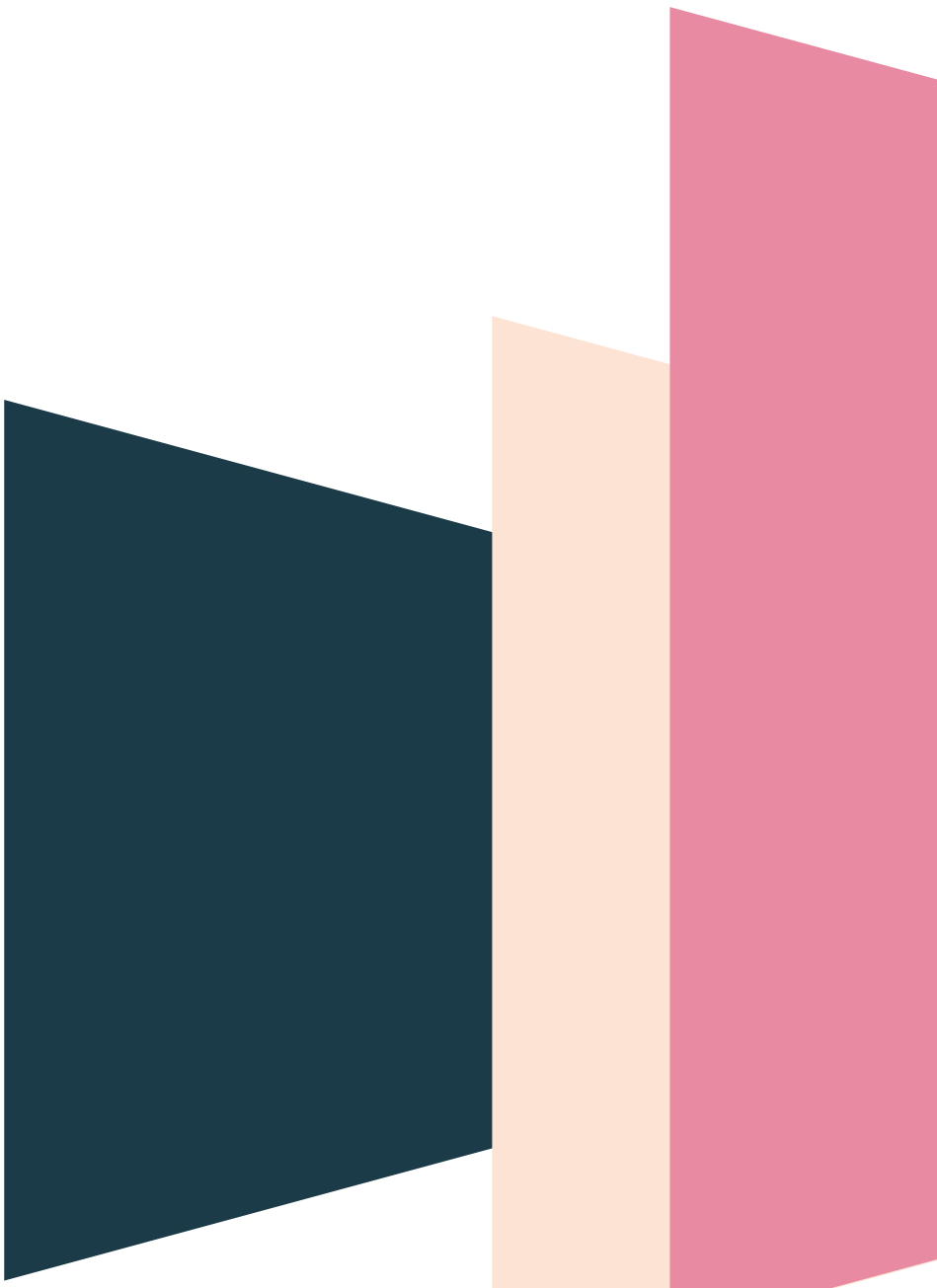
minsait

An Indra company

EDITRAN/GC 5.2

Gestión de Claves
CICS
Manual de usuario

junio de 2019



ecosystems
communications

1. INTRODUCCION

Revise el manual EP52USUC, Anexo D, Sistema Criptografía EDItran, (CICS) para entender antes que nada las posibilidades de la criptografía Editran. De esa forma podrá enlazar a continuación con este manual, para poder interpretar correctamente el funcionamiento de la gestión de claves de intercambio.

En el **modo de criptografía 3.0 y 4.0**, a diferencia del modo 2.2, tanto para DES como RSA, las entidades requieren intercambiar sus respectivas claves, es decir el **intercambio es externo** a EDItran. Este intercambio se ha venido realizando de diversas formas; aplicaciones externas a EDItran, correo y correo electrónico, teléfono, etc, con lo que se observa en muchos casos la "debilidad del intercambio". De ahí, una de las ventajas de usar Gestión de claves de intercambio

1.1. Ventajas del uso de Gestión de claves de intercambio

Las ventajas de usar gestión de claves de intercambio son:

- Que no tendremos que colocar nuevas etiquetas en las sesiones cada vez que intercambiemos claves
- Que las intercambiaremos de forma mucho más segura
- Que el sistema identificará cual es la clave activa
- Que está automatizado el envío y la recepción de esas claves a través de una aplicación ya conocida TELEGC
- Que si falla el sistema, con indicar otra clave de versión inferior activa, todas las sesiones de un determinado remoto funcionarán sin problemas
- Que una misma clave local nos servirá para múltiples remotos.
- Que nadie verá las claves en claro, a diferencia del intercambio externo.

1.2. Requerimientos.

EDItran, en su versión V5R2F00, ha incorporado una gestión fiable y segura para automatizar el proceso de intercambio, evitando la debilidad comentada, evitando la visualización de claves en claro y facilitando una incorporación e intercambio fiable en ambas entidades.

Este módulo no requiere licencia, va incorporado en las funcionalidades de la fase descrita, sin embargo, para su uso es necesario disponer de **licencia EDItran/SC RSA** (a su vez la licencia anterior requiere disponer de un entorno DES o AES, es decir de licencia **EDItran/SC DES o AES**). El motivo es que se pueden producir varios tipos de intercambios de claves con este sistema.

1.3. Tipos de intercambios de claves.

Cuando intercambiamos claves a través de la aplicación Gestión de claves de intercambio, podemos realizar 1 ó 2 tipos de intercambios:

- **Inicialmente, 2 entidades, se intercambian una clave RSA**, (parte pública), en cada sentido y en claro. Esto se hace siempre, independientemente de que lo que luego intercambien sean claves DES.
- **Posteriormente** esos 2 extremos:

  A partir del intercambio inicial, cuando se intercambien nuevas claves públicas RSA, todos los envíos irán firmados con alguna privada de la que tengamos constancia que se ha enviado al remoto la pública asociada correspondiente. Es decir, en el segundo intercambio, al menos se podrá firmar con la inicial, en el tercero con la inicial ó con la segunda y así sucesivamente.

1.4. Subsistemas. Concepto, identificación y tipos.

Toda **la gestión de claves se estructura en subsistemas.** Un subsistema es un conjunto de claves del mismo tipo. Podemos definirlo también como un **grupo de claves intercambiadas para un determinado remoto, grupo de remotos ó aplicaciones**.

El subsistema **se identifica (ó se define)**:

- Por un carácter alfanumérico (**A-Z y 0-9**)
- Por si es un subsistema **propio** (lo hemos generado nosotros) **o ajeno** (lo ha generado el remoto código yyyyyyyy).
- Por el **código de la entidad local** xxxxxxxxx (recuerde que puede tener varios códigos locales en su licencia, si trabaja con un multientorno).
- Por la **entidad remota ó ceros** si es un subsistema propio genérico
    - Si es ceros, el subsistema es RSA y además es PROPIO.
    - Si no es ceros, el subsistema puede ser propio o ajeno

Ejemplo: Supongamos que soy la entidad 4444 y quiero definir un subsistema o conjunto de MIS claves RSA en explotación, contra un determinado remoto (9999), cuya periodicidad en el cambio de claves sea anual y en base a ello decidimos llamarlo "A". En el "conjunto de claves" (ó subsistema) identificado como A-RSA-PROPIO-4444-9999, guardaremos las claves RSA PROPIAS de explotación entre mi código local 4444 y 9999. Piense que pudiera haber entre ese local y ese remoto con claves RSA PROPIAS, otros "conjuntos de claves" (ó subsistemas) B, C, 4, K, que en lugar de guardar claves de explotación, guardasen claves de un entorno de pruebas. El carácter alfanumérico que define a ese "conjunto de claves" (o subsistema) es el que podemos definirlo para pruebas, explotación, cambios quincenales de claves, aplicaciones, remotos, etc, es decir, con ese carácter debemos encontrar el "conjunto que queremos intercambiar". Habitualmente, sólo será "un conjunto de claves" el que intercambiaremos con una entidad, pero el poder hacer varios, podremos dividir aún más los intercambios que hagamos con un remoto o grupo de remotos.

Dentro de las combinaciones anteriores, encontramos **3 TIPOS DE SUBSISTEMAS ó 3 tipos de conjuntos totalmente distintos:**

1. **TIPO 1:** Subsistemas **PROPIOS RSA con código local xxxxxxxxx + codigo remoto ceros**. En estos, **se GENERAN claves RSA propias locales.** Por cada subsistema de este tipo, con código remoto a ceros, existirán tantos subsistemas propios con código local xxxxxxxxx + código remoto yyyyyyyyy, como códigos remotos queramos asociar al mismo.
2. **TIPO 2:** Subsistemas **PROPIOS con código local xxxxxxxxx + código remoto yyyyyyyyy**.

   Se **EXPORTAN claves generadas desde los anteriores**. **Las claves exportadas a estos, son ENVIADAS al remoto especificado yyyyyyyyy.**
3. **TIPO 3:** Subsistemas **AJENOS (RSA) con cód.local xxxxxxxxx + cód.rem. yyyyyyyyy. En estos se IMPORTAN las claves recibidas de esa entidad remota yyyyyyyyy**.

Dentro de cada uno de los TIPOS anteriores, evidentemente podemos diferenciar n subsistemas distintos.

Se pueden hacer las siguientes **consideraciones, respecto a los tipos** anteriores:

1) Si usted dispone de una licencia de multientidad, tendrá varios códigos locales distintos. **Para cada código local podrá tendrá los 3 tipos anteriores**. Si sólo tiene un código local, sólo podrá tener los 3 tipos anteriores.
2) **No existen subsistemas AJENOS con código remoto ceros (TIPO 1)**, puesto que en estos no generamos, ni exportamos, ni enviamos, claves remotas. Un determinado remoto, nos da sus claves (IMPORTAMOS), y por tanto ese código remoto no es ceros.
3) **Existen PROPIOS RSA con código remoto a ceros (TIPO 1)**. Esto es debido a que en los RSA exportaremos y enviaremos a los remotos sólo la clave pública, de forma que una misma clave nos servirá para enviar a distintos remotos (puesto que es pública).
4) Cuando generamos una clave en un **subsistema PROPIO RSA, con código remoto ceros (TIPO 1) y la exportamos** a varios remotos (subsistemas PROPIO RSA, código remoto (xxx, yyyy, zzzz)) **(TIPO 2.1)** en realidad **lo que hacemos es copiar de uno a otros la misma clave**.

En definitiva, se ha incluido el concepto de TIPO 1, porque sirve para EXPORTAR claves desde ese "conjunto" a los diferentes "conjuntos" de TIPO 2.1. Esto sólo ocurre con claves PUBLICAS RSA, puesto que una misma clave, se puede enviar a varios remotos, de ahí su carácter de pública.

1.4.1. Subsistemas RSA.

En el siguiente ejemplo se ven **los 3 subsistemas RSA** que se crean en cada una de las 2 entidades (A=1234 y B=6789), cuando han intercambiado claves.

Entidad A=1234, Subsistemas	**Operación**	**Red**	**Operación**	**Entidad B=6789, Subsistemas**
Subsistema X, Tipo Propio RSA Cgo local 1234, Cgo rem. 0000	**GENERA** CLAVE RSA			
Subsistema X, Tipo Propio RSA Cgo local 1234, Cgo rem. 6789	**EXPORTA**R clave desde X-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD B	→	ENTIDAD B la **IMPORTA** en su subsistema AJENO	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234
			GENERA CLAVE RSA	Subsistema Z, Tipo **Propio** RSA Cgo local 6789, **Cgo rem. 0000**
Subsistema Z, Tipo Ajeno RSA Cgo local 1234, Cgo rem. 6789	ENTIDAD A la **IMPORTA** en su subsistema AJENO	←	**EXPORTA**R clave desde Z-Propio-RSA-6789-0000 y ENVIAR a ENTIDAD A	Subsistema Z, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 1234

En el ejemplo anterior, cada entidad ha generado un subsistema PROPIO con una letra distinta al subsistema PROPIO REMOTO (X y Z). Esto **no es una limitación**, **cada entidad** del ejemplo anterior, **puede generar subsistemas PROPIOS con las mismas letras que se generan en el extremo remoto (por ejemplo SUBSISTEMA PROPIO X en ambos extremos).**

1.4.2. Varios subsistemas entre 2 entidades.

Dos entidades pueden tener varios subsistemas intercambiados dependiendo del tipo de aplicación que se vaya a usar, por ejemplo supongamos que van a funcionar con intercambios RSA, y que las aplicaciones de transmisión AAAAA1 y AAAAA2 desean intercambios de claves ANUALES (subsistemas A en ambos extremos), mientras que el resto de aplicaciones, se conforman con intercambios de claves TRIANUALES (subsistemas X y Z):

Entidad A=1234, Subsistemas	**Operación**	**Red**	**Operación**	**Entidad B=6789, Subsistemas**
Subsistema A, Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000**	**GENERA** CLAVE RSA para aplicaciones AAAAA1 y AAAAA2			
Subsistema A, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789	**EXPORTA**R clave desde A-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD B	→	ENTIDAD B la **IMPORTA** en su subsistema AJENO	Subsistema A, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234
			GENERA CLAVE RSA para aplicaciones AAAAA1 y AAAAA2	Subsistema A, Tipo **Propio** RSA Cgo local 6789, **Cgo rem. 0000**
Subsistema A, Tipo **Ajeno** RSA Cgo local 1234, Cgo rem. 6789	ENTIDAD A la **IMPORTA** en su subsistema AJENO	←	**EXPORTA**R clave desde A-Propio-RSA-6789-0000 y ENVIAR a ENTIDAD A	Subsistema A, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 1234
Ya puede funcionar con aplicaciones AAAAA1 y AAAAA2				Ya puede funcionar con aplicaciones AAAAA1 y AAAAA2
Subsistema X, Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000**	**GENERA** CLAVE RSA **para resto aplicaciones**			
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789	**EXPORTA**R clave desde X-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD B	→	ENTIDAD B la **IMPORTA** en su subsistema AJENO	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234
			GENERA CLAVE RSA **para resto aplicaciones**	Subsistema Z, Tipo **Propio** RSA Cgo local 6789, **Cgo rem. 0000**
Subsistema Z, Tipo **Ajeno** RSA Cgo local 1234, Cgo rem. 6789	ENTIDAD A la **IMPORTA** en su subsistema AJENO	←	**EXPORTA**R clave desde Z-Propio-RSA-6789-0000 y ENVIAR a ENTIDAD A	Subsistema Z, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 1234
Ya puede funcionar con resto de aplicaciones				Ya puede funcionar con resto de aplicaciones

En cuanto a la parametrización EDItran, indicaríamos que las aplicaciones de transmisión AAAAA1 y AAAAA2 trabajan con los subsistemas A, mientras que el resto de aplicaciones trabajarían con los subsistemas X y Z:

AAAAA1 y AAAA2: PARM=*,A,A

Resto: PARM=*,X,Z

1.4.3. Compartir 1 subsistema RSA para varios remotos.

Cuando se trata de claves RSA, hemos dicho que habitualmente las claves de un subsistema RSA PROPIO (con código remoto a ceros), sirven para enviar a varios remotos. Así por ejemplo, y continuando con los ejemplos anteriores, supongamos que la entidad A (1234), genera, exporta y envía a los remotos 6789 y 9876 claves de su subsistema M, y recibe del remoto 6789 claves de subsistema N y del remoto 9876 claves del subsistema N (no tiene porqué ser igual al del remoto 6789). Tendremos:

Entidad A=1234, Subsistemas	**Operación**	**Red**	**Operación**	**Entidad B=6789 y C=9876, Subsistemas**
Subsistema M Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000**	**GENERA** CLAVE RSA			
Subsistema M, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789	**EXPORTA**R clave desde M-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD 6789	→	ENTIDAD B=6789 la **IMPORTA** en su subsistema AJENO	**ENTIDAD B=6789** Subsistema M, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234
Subsistema M, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 9876	**EXPORTA**R clave desde M-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD 9876	→	ENTIDAD C=9876 la **IMPORTA** en su subsistema AJENO	**ENTIDAD C=9876** Subsistema M, Tipo **Ajeno** RSA Cgo local 9876, Cgo rem. 1234
			GENERA CLAVE RSA	**ENTIDAD B=6789** Subsistema N, Tipo **Propio** RSA Cgo local 6789, **Cgo rem. 0000**
Subsistema N, Tipo **Ajeno** RSA Cgo local 1234, Cgo rem. 6789	ENTIDAD A la **IMPORTA** en su subsistema AJENO	←	**EXPORTA**R clave desde N-Propio-RSA-6789-0000 y ENVIAR a ENTIDAD A	**ENTIDAD B=6789** Subsistema N, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 1234
			GENERA CLAVE RSA	**ENTIDAD C=9876** Subsistema N, Tipo **Propio** RSA Cgo local 9876, **Cgo rem. 0000**
Subsistema N, Tipo **Ajeno** RSA Cgo local 1234, Cgo rem. 9876	ENTIDAD A la **IMPORTA** en su subsistema AJENO	←	**EXPORTA**R clave desde N-Propio-RSA-9876-0000 y ENVIAR a ENTIDAD A	**ENTIDAD C=9876** Subsistema N, Tipo **Propio** RSA Cgo local 9876, Cgo rem. 1234

En el ejemplo anterior, se han creado por tanto 11 subsistemas:

1. En la entidad A (1234):

1.1. Un subsistema M-RSA PROPIO código local 1234, código remoto ceros (TIPO 1).

1.2. Un subsistema M-RSA-PROPIOS código local 1234, código remoto 6789 (TIPO 2)

1.3. Un subsistema M-RSA-PROPIO código local 1234, código remoto 9876 (TIPO 2)

1.4. Un subsistema N-RSA-AJENO, código local 1234, código remoto 6789 (TIPO 3)

1.5. Un subsistema N-RSA-AJENO, código local 1234, código remoto 9876 (TIPO 3)

2. En la entidad B (6789)

2.1. Un subsistema N-RSA PROPIO código local 6789, código remoto ceros (TIPO 1).

2.2. Un subsistema N-RSA-PROPIOS código local 6789, código remoto 1234 (TIPO 2):

2.3. Un subsistema M-RSA-AJENO, código local 6789, código remoto 1234 (TIPO 3)

3. En la entidad C (9876)

3.1. Un subsistema N-RSA PROPIO código local 9876, código remoto ceros (TIPO 1).

3.2. Un subsistema N-RSA-PROPIOS código local 9876, código remoto 1234 (TIPO 2):

3.3. Un subsistema M-RSA-AJENO, código local 9876, código remoto 1234 (TIPO 3):

1.4.4. Contenido de un subsistema: Claves y versiones.

Dentro de cada uno de los subsistemas, encontramos claves (en realidad, están las etiquetas ó lábeles de las mismas) y el estado en que se encuentran las mismas. Tendremos, las siguientes claves dentro de un subsistema:

1. Parejas de claves RSA, con distinta versión (v01 a v99, dando la vuelta cuando alcanzan ese valor).
   1.1. Cuando generamos claves RSA (subsistema propio con código remoto a ceros), vamos incrementando el valor de la versión de la nueva clave contenida (V2, V3, y así sucesivamente).
   1.2. Subsistemas PROPIOS con código xxxx remoto:

   Cuando desde el anterior subsistema propio con código remoto a ceros, EXPORTAMOS la clave que queremos (pueden ser todas las anteriores ó sólo algunas) a uno ó varios subsistemas propio con código(s) remoto xxxx, yyyy, zzzz, lo que hacemos es copiar de uno a otro(s) la versión (clave), que queramos. En definitiva, generamos una clave desde el anterior, y se la exportamos a varios remotos la misma clave.

   1.3. Cuando un remoto nos envía una clave con una versión x, la IMPORTAMOS (incorporamos) en un subsistema AJENO. Si nos envía varias del mismo tipo y del mismo subsistema, tendremos por tanto varias claves de ese remoto en ese subsistema.
2. Dentro de la gestión de un subsistema, se guardan hasta las 3 últimas claves que se hayan introducido, de forma que podemos manualmente si fuera el caso, elegir entre 3 posibles claves para el funcionamiento contra una entidad remota. Si hemos introducido más de 3, se pierde el rastro de la anterior a la antepenúltima. Físicamente no se pierden (puesto que se mantienen en el fichero de claves correspondiente), al menos hasta que no se machaquen por dar vuelto, pero de cara a la gestión se han perdido.

1.4.5. Estado de las claves dentro de un subsistema.

Cada clave de un subsistema está identificada, además de por la versión, por el estado en que se encuentra. Tendremos:

- Cuando generamos clave (subsistema propio RSA con código remoto a ceros), con una determinada versión (la anterior versión generada + 1), el estado de la nueva generada pasa a **ACTIVA**. La anterior que estuviera en estado ACTIVA, pasa a estado **OPERATIVA**. Si hubiera 3 ó más claves y generamos nueva clave, se pierde el rastro de la antepenúltima que hubiera. En zos, todo esto se hace en la opción **6.2 (gestión de claves propias RSA, generación y administración).**
- Otros subsistemas propios:
    - En RSA: Ese mismo extremo, exporta al registro de remoto (subsistemas propios con código local xxxxxxxxx + código remoto yyyyyyyyy), esa clave mediante un procedimiento. Una vez exportada la clave, aparece en este último subsistema ya con la versión que le corresponde y en estado **GENERADA**. La última clave intercambiada, permanece en estado ACTIVA y se pierde el rastro de la clave que hubiera 3 versiones antes. Cuando se la enviamos al remoto, la GENERADA pasa a **ENVIADA**. Cuando el extremo remoto nos envía la confirmación de que la ha recibido, la ENVIADA pasa a **ACTIVA**. La que estuviera activa anteriormente pasa a **OPERATIVA**. En zos, esto se hace en la **opción 6.3 (asociación de claves propias RSA, administración, exportación y envío).**
- Cuando un extremo recibe una clave, accede al subsistema AJENO, código local xxxxxxxxx, código remoto yyyyyyyyy, e incorpora la clave con la versión que le viene del remoto. Esta clave se incorpora en estado **RECIBIDA**. La última clave intercambiada recibida, permanece en estado ACTIVA y se pierde el rastro de la clave que hubiera 3 versiones antes. Cuando enviamos al remoto un fichero confirmando la recepción de la recibida, la RECIBIDA pasa a **ACTIVA**. La que estuviera activa anteriormente pasa a **OPERATIVA**. En zos, esto se hace en la **opción 6.4 (asociación de claves remotas RSA, administración)** También está el estado **CANCELADO,** cuando manualmente, se coge una clave y se pasa a ese estado.
- Manualmente, podemos también pasar una clave a **ACTIVA** y por tanto la que estaba como tal pasaría a **OPERATIVA.**

1.4.6. Procesos para enviar una clave de un subsistema.

En la gestión de claves de intercambio, se puede usar una sesión Editran que es la encargada de transmitir las claves, Habitualmente se usa la sesión TELEGC.

Un **proceso de enviar una clave consta de 2 transmisiones**:

1. Envío por parte de la entidad A hacía B, de un fichero que contiene la propia clave, donde se indica también la versión generada y el subsistema PROPIO. (al llegar a B ese fichero, incorpora dicha clave con la versión indicada en el subsistema AJENO indicado (coincide con el PROPIO que le llega). En el extremo A, la clave queda en estado ENVIADA y en el extremo B, la clave queda en estado RECIBIDA.
2. Envío por parte de la entidad B hacia A, de un fichero cuyo contenido es una confirmación de haber recibido correctamente la clave. Una vez finalizada esta transmisión, la clave queda en estado ACTIVA en ambos extremos.

1.4.7. Cambios de clave en un subsistema.

Continuando con el ejemplo inicial, si 2 entidades A=1234 y B=5678, se intercambian primero una clave, pero luego la entidad A, sigue cambiando su clave 3 veces más contra ese remoto B (nótese que la V4 se generó pero no se exportó):

Entidad A=1234, Subsistemas	Operación	Red	Operación	Entidad B=6789, Subsistemas
Subsistema X, Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000** **V1=ACTIVA**	**GENERA** CLAVE RSA V1			
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V1-GENERADA, ENVIADA**	**EXPORTA**R clave V1 de X-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD B		ENTIDAD B **IMPORTA V1** en su subsistema AJENO	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V1-RECIBIDA**
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V1-ACTIVA**	Recibe file confirmación	← →	Emite file confirmación	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V1-ACTIVA**
			GENERA CLAVE RSA V1	Subsistema Z, Tipo **Propio** RSA Cgo local 6789, **Cgo rem. 0000** **V1-ACTIVA**
Subsistema Z, Tipo **Ajeno** RSA	ENTIDAD A **IMPORTA V1** en su subsistema AJENO	←	**EXPORTA**R clave V1 de Z-Propio-RSA-6789-0000 y ENVIAR	Subsistema Z, Tipo **Propio** RSA

Cgo local 1234, Cgo rem. 6789 **V1-RECIBIDA**			a ENTIDAD A	Cgo local 6789, Cgo rem. 1234 **V1-GENERADA, ENVIADA**
Subsistema Z, Tipo **Ajeno** RSA Cgo local 1234, Cgo rem. 6789 **V1-ACTIVA**	Emite file confirmación	→	Recibe file confirmación	Subsistema Z, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 1234 **V1-ACTIVA**
Subsistema X, Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000** **V1-OPERATIVA** **V2=ACTIVA**	**GENERA** CLAVE RSA V2			
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V1-ACTIVA** **V2-GENERADA, ENVIADA**	**EXPORTA**R clave V2 de X-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD B	→	ENTIDAD B **IMPORTA V2** en su subsistema AJENO	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V1-ACTIVA** **V2-RECIBIDA**
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V1-OPERATIVA** **V2-ACTIVA**	Recibe file confirmación	←	Emite file confirmación	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V1-OPERATIVA** **V2- ACTIVA**
Subsistema X, Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000** **V1-OPERATIVA** **V2-OPERATIVA** **V3=ACTIVA**	**GENERA** CLAVE RSA V3			
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V1-OPERATIVA** **V2-ACTIVA** **V3-GENERADA, ENVIADA**	**EXPORTA**R clave V3 de X-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD B	→	ENTIDAD B **IMPORTA V3** en su subsistema AJENO	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V1-OPERATIVA** **V2-ACTIVA** **V3-RECIBIDA**
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V1-OPERATIVA**	Recibe file confirmación	←	Emite file confirmación	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V1-OPERATIVA**

V2-OPEARATIVA **V3- ACTIVA**				**V2-OPERAVIVA** **V3- ACTIVA**
Subsistema X, Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000** **V1- (se pierde)** **V2-OPERATIVA** **V3-OPERATIVA** **V4=ACTIVA**	**GENERA** CLAVE RSA V4 **(OJO, NO SE EXPORTA)**			
Subsistema X, Tipo **Propio** RSA Cgo local 1234, **Cgo rem. 0000** **V2- (se pierde)** **V3-OPERATIVA** **V4-OPERATIVA** **V5=ACTIVA**	**GENERA** CLAVE RSA V5			
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V1- (se pierde)** **V2-OPERATIVA** **V3-ACTIVA** **V5-GENERADA, ENVIADA**	**EXPORTA**R clave V5 de X-Propio-RSA-1234-0000 y ENVIAR a ENTIDAD B	→	ENTIDAD B **IMPORTA V5** en su subsistema AJENO	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V1- (se pierde)** **V2-OPERATIVA** **V3-ACTIVA** **V5-RECIBIDA**
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V2-OPERATIVA** **V3-OPEARATIVA** **V5- ACTIVA**	Recibe file confirmación	←	Emite file confirmación	Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V2-OPERATIVA** **V3-OPERAVIVA** **V5- ACTIVA**

Nótese que las claves que tiene el X-PROPIO-RSA-1234-0000 no son las mismas que el X-PROPIO-RSA-1234-6789. En el primero estarían V3-V4-V5 y en el segundo V2-V3-V5

Nótese, que si hubiera existido la entidad C, podríamos haber exportado la V4 a dicha entidad C (9876), por lo que los subsistemas X-PROPIO-RSA-1234-6789 y X-PROPIO-RSA-1234-9876 no tendrían las mismas claves. En el primero estarían V2-V3-V5 y en el segundo V3-V4-V5.

1.4.8. Operaciones manuales sobre las claves.

La interfaz gráfica de gestión de claves de intercambio, posibilita, acceder a cualquier subsistema y cambiar el estado de las claves que contiene. Todo ello, se puede hacer en cualquiera de las opciones del menú principal (6.2, 6.3 y 6.4,)

Si por ejemplo hemos generado en el subsistema X, 5 claves RSA contra un remoto 6789, y ese remoto sólo nos ha generado en su subsistema Z, 3 claves, tendremos:

Entidad A=1234, Subsistemas	Operación	Red	Operación	Entidad B=6789, Subsistemas
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 0000 **V3-OPERATIVA** **V4-OPEARATIVA** **V5- ACTIVA**				
Subsistema X, Tipo **Propio** RSA Cgo local 1234, Cgo rem. 6789 **V3-OPERATIVA** **V4-OPEARATIVA** **V5- ACTIVA**				Subsistema X, Tipo **Ajeno** RSA Cgo local 6789, Cgo rem. 1234 **V3-OPERATIVA** **V4-OPEARATIVA** **V5- ACTIVA**
				Subsistema Z, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 0000 **V1-OPERATIVA** **V2-OPEARATIVA** **V3- ACTIVA**
Subsistema Z, Tipo **Ajeno** RSA Cgo local 1234, Cgo rem. 6789 **V1-OPERATIVA** **V2-OPEARATIVA** **V3- ACTIVA**				Subsistema Z, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 1234 **V1-OPERATIVA** **V2-OPEARATIVA** **V3- ACTIVA**

En este momento, funcionaremos con la V5 del subsistema X, y con la V3 del Z.

Si por ejemplo, no queremos intercambiar claves, y no nos fiamos de que la clave V3 del subsistema Z sea buena, podemos activar manualmente la clave V3 del subsistema Z, en cuyo caso la última línea anterior quedaría:

Subsistema Z, Tipo **Ajeno** RSA Cgo local 1234, Cgo rem. 6789 **V1-OPERATIVA** **V2-ACTIVA** **V3- OPERATIVA**				Subsistema Z, Tipo **Propio** RSA Cgo local 6789, Cgo rem. 1234 **V1-OPERATIVA** **V2-ACTIVA** **V3- OPERATIVA**

También podíamos haber puesto la V3 en estado **CANCELADO,** en lugar de mantenerla operativa.

1.5. Codificación de las sesiones EDItran, una vez se intercambian claves.

Una vez intercambiadas claves, en las sesiones EDItran, habitualmente codificaremos:

EDItran/G

```
                    CRIPTOGRAFIA (S/N).......: S
ALGORITMO CONFIDENCIALIDAD.: AAAA       ALGORITMO AUTENTICACION ...:  BBB
INTERFAZ DE CLAVES.........: ZTBGBIGC   PARM :*,v,w
```

EDItran/P:

```
| CRIPTOGRAFIA S/N: S        VERS.CRIPTOGRAF.:3.00     CAMB.CLAVE (S/N/U): N  |
| ALG.CONFIDENC...: CCCC     ALG.AUTENTICAC..:DDD                             |
| INTERFAZ CLAVES.: ZTBPOIGC PARAMETROS......:*,x,y                           |
```

AAAA y CCCC – Es el algoritmo confidencialidad (mediante esto, indicamos la clave operacional que servirá para cifrar datos). Puede tener valores distintos en P y G. Los valores admitidos son spaces, DES, TD2C, TD3C, AES1, AES2 y AES3 (sin cifrado, DES o AES de clave simple, doble y triple). **Habitualmente colocaremos en G** uno de esos valores **por ejemplo DES** y en P no ponemos nada (para no cifrar 2 veces)

BBB y DDD – Es el algoritmo autenticación (es la clave intercambiada, que sirve para firmar y para cifrar la clave operacional). Puede tener valores distintos en P y G. Los valores admitidos son DES y RSA .El valor habitual en G y P será RSA

V,x,- Son los subsistemas PROPIOS (locales). Recuerde que para unas sesiones con ese remoto puede tener unos subsistemas locales distintos que para otra. V-x no tienen porqué tener el mismo valor, pero lo habitual es que si lo tengan, es decir que funcionemos en P y G con el mismo subsistema PROPIO

W,y,- Son los subsistemas AJENOS (remotos).. Recuerde que para unas sesiones con ese remoto puede tener unos subsistemas remotos distintos que para otra. W-y no tienen porqué tener el mismo valor, pero lo habitual es que si lo tengan, es decir que funcionemos en P y G con el mismo subsistema AJENO

Cuando cambiamos una clave dentro de un mismo subsistema NO ES NECESARIO tocar la parametrización anterior. EDItran busca dentro de los valores que le hemos dado, cual es la clave ACTIVA (sólo hay 1) que existe en ese subsistema, y opera con ella. De ahí que si alguno de los extremos realiza un nuevo intercambio, no tiene porqué avisar al otro extremo (recuerde que la TELEGC queda definida y su funcionamiento es automático desde cualquier extremo), de forma que si cambia de clave, esta pasa a activa, por lo que ambos EDItran, cogerán la nueva. En base a

lo anterior, en ninguno de los extremos habrá que tocar más veces los campos interfaz de claves y parámetros.

Interfaz de claves: Es el API EDItran, que gestiona este comportamiento. En EDItran/G indique ZTBGBIGC. En EDItran/P, indique ZTBPOIGC.

En parámetros, aparece siempre un *. Manténgalo, al igual que las comas que separan los subsistemas PROPIO y AJENO, pues sirve para identificar que estamos trabajando con ESTE sistema de gestión de claves de intercambio.

1.6. Ejemplo 1 de subsistemas.

1. Mi entidad tiene 2 códigos locales 1111 y 2222.
   1.1. El 1111, se conectará con los remotos 3333, 4444 y 5555
   1.2. El 2222 se conectará con los remotos 7777 y 8888
2. Mis subsistemas se llamarán:
   2.1. Si son PROPÌOS
      2.1.1.1. Con los remotos 3333, 4444, 5555, el subsistema propio S (semestral).
      2.1.1.2. Con los remotos 7777, 8888, el subsistema propio A (anual)
   2.2. Si son AJENOS
      2.2.1.1. Con el remoto 3333 el subsistema AJENO 3
      2.2.1.2. Con el remoto 4444 el subsistema AJENO 4
      2.2.1.3. Con el remoto 5555 el subsistema AJENO 5
      2.2.1.4. Con el remoto 7777 el subsistema AJENO 7
      2.2.1.5. Con el remoto 8888 el subsistema AJENO 8
3. Las claves enviadas - recibidas y sus versiones:
   3.1. Con los remotos del subsistema PROPIO S (ver 3.1.1.1 y 3.1.2.1) les genero y envío 45 claves
   3.2. Con los remotos del subsistema PROPIO A (ver 3.1.1.2 y 2.1.2.2), les genero y envío 65 claves.
   3.3. Cada remoto RSA me ha enviado 22 claves (ver 3.2.1).

Subs	Tipo	Local	Remoto	Claves	Clave 1 Operativa	Clave 2 Operativa	Clave 3 Activa	Comentarios	Orden	Ver puntos
S	PROPIO	1111	**0000**	RSA	43	44	45	Exporta a orden 4, 5 y 6	1	1.1, 2.2, 3.1.1.1, 4.1
S	PROPIO	2222	**0000**	RSA	43	44	45	Exporta a orden 8	2	1.2, 2.2, 3.1.1.1, 4.1
A	PROPIO	2222	**0000**	RSA	63	64	65	Exporta a orden 10, 11	3	1.2, 2.2, 3.1.1.2, 4.2
S	PROPIO	1111	3333	RSA	43	44	45	Exportado desde	4	1.1, 2.2,

								orden 1		3.1.1.1, 4.1
S	PROPIO	1111	4444	RSA	43	44	45	Exportado desde orden 1	5	1.1, 2.2, 3.1.1.1, 4.1
S	PROPIO	1111	5555	RSA	43	44	45	Exportado desde orden 1	6	1.1, 2.2, 3.1.1.1, 4.1
S	PROPIO	2222	5555	RSA	43	44	45	Exportado desde orden 2	8	1.2, 2.2, 3.1.1.1, 4.1
A	PROPIO	2222	7777	RSA	63	64	65	Exportado desde orden 3	10	1.2, 2.2, 3.1.1.2, 4.2
A	PROPIO	2222	8888	RSA	63	64	65	Exportado desde orden 3	11	1.2, 2.2, 3.1.1.2, 4.2
3	AJENO	1111	3333	RSA	20	21	22	El subsistema que el remoto nos indicó	16	1.1, 2.2, 3.2.1.1, 4.3
4	AJENO	1111	4444	RSA	20	21	22	El subsistema que el remoto nos indicó	17	1.1, 2.2, 3.2.1.2, 4.3
5	AJENO	1111	5555	RSA	20	21	22	El subsistema que el remoto nos indicó	18	1.1, 2.2, 3.2.1.3, 4.3
5	AJENO	2222	5555	RSA	20	21	22	El subsistema que el remoto nos indicó	20	1.2, 2.2, 3.2.1.3, 4.3
7	AJENO	2222	7777	RSA	20	21	22	El subsistema que el remoto nos indicó	22	1.2, 2.2, 3.2.1.5, 4.3
8	AJENO	2222	8888	RSA	20	21	22	El subsistema que el remoto nos indicó	23	1.2, 2.2, 3.2.1.6, 4.3

Ya puede observar, que por ejemplo los registros con orden 1, 4, 5 y 6 contienen las mismas claves , es decir, hemos generado unas mismas claves para varios remotos. Ocurre lo mismo con los de orden 2, 8 ó también con 3, 10 y 11

Las claves no se pierden, Una vez exportadas a un remoto, quedan en el mismo.

¿Qué ocurre si generamos claves de un subsistema local RSA propio código local xxxx + código remoto ceros, generamos una versión, no se la exportamos a todos los remotos que teníamos en ese subsistema, y a continuación generamos una nueva versión de claves en el subsistema local propio RSA código local xxxx + código remoto ceros? En principio, no pasa nada, pues esos remotos, guardan la última clave intercambiada, es decir la clave con una versión inferior. Es como si en el registro de orden 1 estuviera activa la clave de versión 45 y en los de orden 4, 5, 6 estuviera activa la V44. Sin embargo, puede ocurrir, que si hacemos esto, demos la vuelta a las 99 opciones y acabemos machacando al remoto que se encontraba en ese grupo. Ejemplo. En el registro de orden 4, hemos exportado sólo la clave 45, y en el registro de orden 1 hemos generado 99 versiones de claves a partir de la V45. Si generamos 1 más, machacaremos la etiqueta y clave de la v1, y por tanto ese remoto que no tuvo exportación dejará de funcionar.

1.7. Observaciones y consideraciones respecto a los intercambios.

Se pueden hacer las siguientes **observaciones**, unas consecuencia de otras:

1. El cifrado intercambiando claves RSA es más potente que el cifrado intercambiando claves DES (autenticación RSA)
2. La gestión de claves de intercambio, obliga a disponer de entorno RSA en ambos extremos.
3. Según las afirmaciones anteriores, **no tiene sentido hacer intercambios de claves DES por la aplicación de Gestión de claves de intercambio**. Se elimina esa funcionalidad.

Si por ejemplo generamos la V2 del subsistema S y no se la enviamos a uno de los remotos que le enviamos la V1, no ocurre nada, ese remoto sigue funcionando con la V1. Si generamos la V3, y esa si se la enviamos, el remoto (y nosotros) tendrá la V1, y la V3 activa, En esa situación ¿Qué podría ocurrir?. Imagine que a un remoto le da la V1 del subsistema S, y ya no le vuelve a exportar nuevas versiones nunca más, sin embargo, usted ha ido creando 99 versiones de parejas de claves del subsistema S y las ha ido distribuyendo a otros remotos que también asociaba a ese subsistema. Cuando se cree la versión 100, se machacará la etiqueta que contenía la V1, (y por tanto su clave asociada), con lo que el remoto que sólo se le envió la V1, dejará de funcionar.

De ahí que **es muy importante, "dimensionar correctamente los subsistemas dependiendo de las necesidades de la instalación".**

El subsistema que creamos en local no tiene porqué llamarse igual que el subsistema que ha creado la entidad remota. **Nosotros decidiremos el nombre de nuestro subsistema local y la entidad remota decidirá el nombre de su subsistema local**. Nosotros le diremos el nuestro a la entidad remota (para que ella lo cree como subsistema remoto) y la entidad remota nos dará su local para que nosotros lo creemos como subsistema remoto.

1.8. Ejemplo 2 de subsistemas.

Nosotros somos la entidad 5555, y tenemos 2 remotos; uno con cgo 4444 y otro 6666

- Creamos el subsistema local propio RSA E (E-Propio-RSA-5555-0000) y generamos la pareja de claves versión 1 de ese subsistema (V1)
- Creamos el subsistema local especifico E para el Remoto 4444 (E-Propio-RSA-5555-4444)
- Exportamos las claves V1 del subsistema E-Propio-RSA-5555-0000-RSA a E-Propio-RSA-5555-4444
- Creamos el subsistema local especifico E para el Remoto 4444 (E-Propio-RSA-5555-6666)
- Exportamos las claves V1 del subsistema E-Propio-RSA-5555-0000-RSA a E-Propio-RSA-5555-6666
- Le decimos al remoto 4444 que cree el subsistema remoto E para nosotros. Crea E-Ajeno-RSA-4444-5555
- Le decimos al remoto 6666 que cree el subsistema remoto E para nosotros. Crea E-Ajeno-RSA-6666-5555
- Le enviamos al remoto 4444 la pública V1 de E-Propio-RSA-5555-4444. Incorpora V1 en su E-Ajeno-RSA-4444-5555 .
- Le enviamos al remoto 6666 la pública V1 de E-Propio-RSA-5555-6666. Incorpora V1 en su E-Ajeno-RSA-6666-5555.
- El remoto 4444, crea su subsistema X-Propio-4444-0000-RSA y genera pareja de claves V1 de ese subsistema
- El remoto 6666, crea su subsistema E-Propio-RSA-6666-0000 y genera pareja de claves V1 de ese subsistema
- El remoto 4444, crea el subsistema X-PROPIO-RSA-4444-5555 y le exporta las claves V1 al mismo desde su X-PROPIO-RSA-4444-0000
- El remoto 6666, crea el subsistema E-PROPIO-RSA-6666-5555 y le exporta las claves V1 al mismo desde su E-PROPIO-RSA-6666-0000
- El remoto 4444 nos indica que demos de alta el subsistema X-AJENO-RSA-5555-4444. Nos envía su clave pública V1 desde su X-PROPIO-RSA-4444-5555 la cual guardamos en el anterior.
- El remoto 6666 nos indica que demos de alta el subsistema E-AJENO-RSA-5555-6666. Nos envía su clave pública V1 desde su E-Propio-RSA-6666-5555, la cual guardamos en el anterior.
- El remoto 4444, genera otra pareja de claves V2 en su subsistema X-PROPIO-RSA-4444-0000
- El remoto 4444, exporta V2 a su subsistema X-PROPIO-RSA-4444-5555 desde su X-PROPIO-RSA-4444-0000
- El remoto 4444 nos envía su clave pública V2, que incorporaremos en X-AJENO-5555-4444-RSA. Esta clave pasará a estar activa en nuestro extremo en vez de V1.

- El remoto 4444 nos envía su clave pública V2 desde su X-PROPIO-RSA-4444-5555 la cual guardamos en X-AJENO-5555-4444-RSA. Pasa automáticamente a ACTIVA.
- A su vez, en 4444, pasará a estar activa V2 en X-PROPIO-RSA-4444-5555 en vez de V1

En esta situación, las sesiones se habrían codificado:

- Nosotros en las sesiones con 4444 tendremos PARAMETROS=*,E,X. La E quiere decir que usaremos la privada V1 del subsistema E local para descifrar datos. La X quiere decir que usaremos para cifrar la pública remota de V2 del subsistema X de ese remoto
- Nosotros en las sesiones con 6666 tendremos PARAMETROS=*,E,E. La E primera quiere decir que usaremos para descifrar la privada V1 del subsistema E local para descifrar datos. La X quiere decir que usaremos para cifrar la pública remota de V1 del subsistema E de ese remoto
- El remoto 4444 en sus sesiones con nosotros tendrá PARAMETROS=*,X,E. La X quiere decir que usará la privada V2 del subsistema X local para descifrar datos. La E quiere decir que usará para cifrar la pública remota de V1 del subsistema E nuestra
- El remoto 6666 en sus sesiones con nosotros tendrá PARAMETROS=*,E,E. La primera E quiere decir que usará la privada V1 del subsistema E local para descifrar datos. La E segunda quiere decir que usará para cifrar la pública remota de V1 del subsistema E

1.9. Ejemplo 3 de subsistemas.

En el ejemplo siguiente, se recoge un caso en que ya se han intercambiado varias claves las 2 entidades (V1, V2, V4). Además, se recoge que la clave V3 se generó pero no fue exportada en su momento a ese remoto B (6789). Se muestran en negrita los cambios de estado.

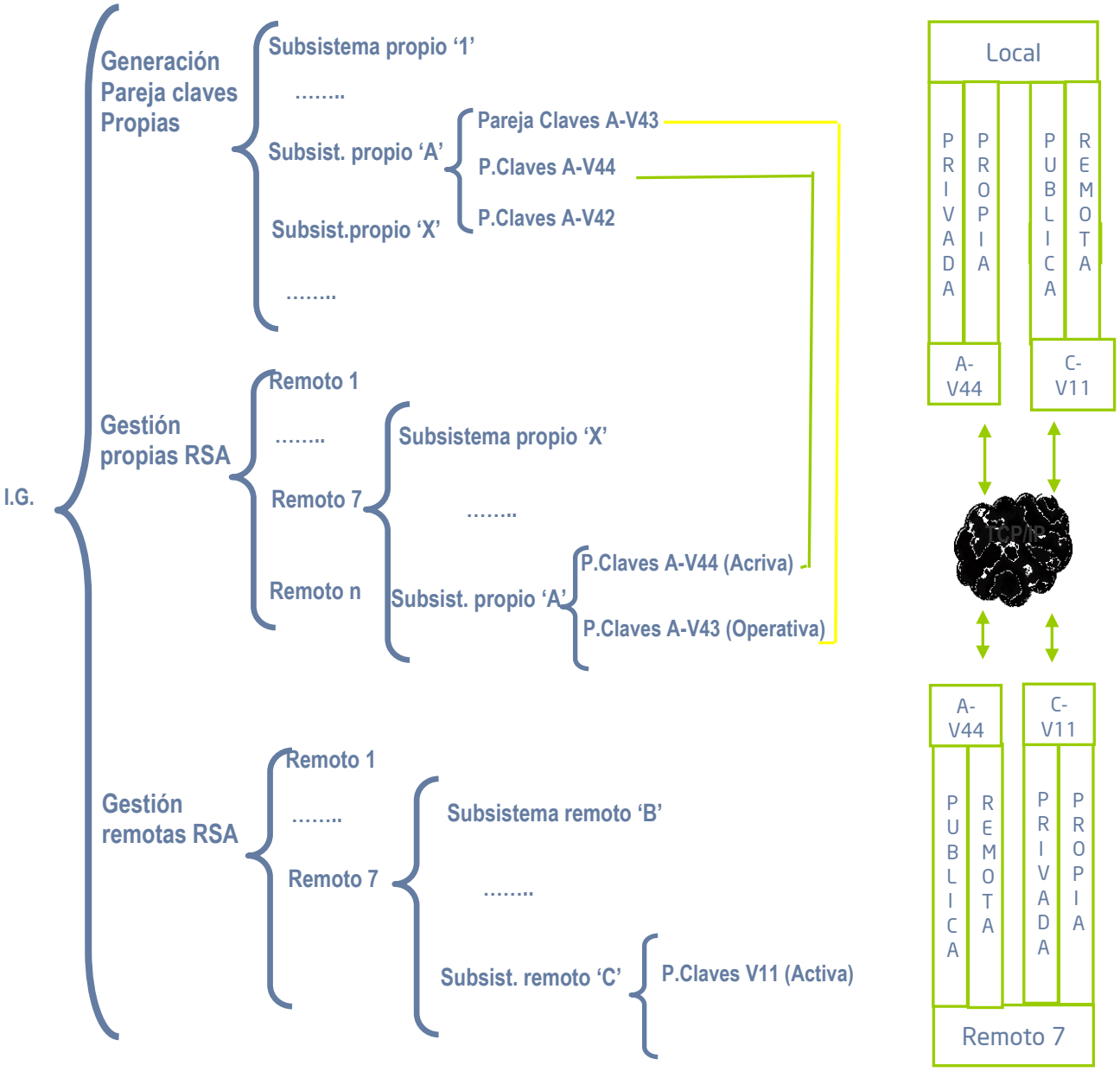
Subsistema Entidad A=1234	Estado claves	Operación	Red	Operación	Estado claves	Subsistema Entidad B 6789
Subsistema X Tipo Propio RSA Cgo local 1234 **Cgo rem. 0000**	**V2 Se pierde** V3-OPERATIVA V4-OPERATIVA **V5-ACTIVA**	Generar clave (V5)			(ya existía) V1-OPERATIVA V2-OPERATIVA V4-ACTIVA	Subsistema X Tipo Ajeno RSA Cgo local 6789 Cgo rem. 1234
Subsistema X Tipo Propio RSA Cgo local 1234 Cgo rem. 6789	**V1 Se pierde** V2-OPERATIVA V4-ACTIVA **V5-GENERADA**	Exportar clave V5 del anterior subsistema			(ya existía) V1-OPERATIVA V2-OPERATIVA V4-ACTIVA	Subsistema X Tipo Ajeno RSA Cgo local 6789 Cgo rem. 1234
Subsistema X Tipo Propio RSA Cgo local 1234 Cgo rem. 6789	V2-OPERATIVA V4-ACTIVA V5-GENERADA	Enviar clave V5 Previo a emisión	Emite A	Recibe clave		
Subsistema X Tipo Propio RSA Cgo local 1234 Cgo rem. 6789	V2-OPERATIVA V4-ACTIVA **V5-ENVIADA**	Posterior emisión		Posterior a recepción	**V1-Se pierde** V2-OPERATIVA V4-ACTIVA **V5-RECIBIDA**	Subsistema X Tipo Ajeno RSA Cgo local 6789 Cgo rem. 1234
		Recibe fichero de confirmación	Emite B	Previo a emisión Emite confirmación	V2-OPERATIVA V4-ACTIVA V5-RECIBIDA	Subsistema X Tipo Ajeno RSA Cgo local 6789 Cgo rem. 1234
Subsistema X Tipo Propio RSA Cgo local 1234	V2-OPERATIVA **V4-OPERATIVA** **V5-ACTIVA**	Posterior a recepción		Posterior a emisión	V2-OPERATIVA **V4-OPERATIVA** **V5-ACTIVA**	Subsistema X Tipo Ajeno RSA Cgo local 6789

Cgo rem. 6789						Cgo rem. 1234

Hasta el último paso, todas las sesiones EDItran entre ambos extremos en las que se indicaba subsistema X (local en A y remoto en B) , funcionaban con la clave V4. Desde el momento en que V5 está activa en ambos extremos, pasan a funcionar con ésta última.

Note que inicialmente pueden activarse manualmente en ambos extremos V1,V2,V4. Más tarde, se pierde V1 en la entidad A (ya no se puede funcionar con V1). Hasta que V5 no está activa en ambos extremos, sólo existen 2 juegos de claves y no 3, con los que poder funcionar.

1.10. Diagrama de comportamientos.



2. DEFINICIONES (Interfaz gráfica y sistemas).

2.1. Interfaz gráfica

Para más información vea manual ED52USUC , capítulo 7, (CICS) y ED52USUI (IMS).

2.1.1. CICS

Se requiere dar de alta la transacción de la gestión de claves de intercambio (ZTB2) en entorno local de EDItran/P (opción 1.3.2). Para acceder a gestión de claves de intercambio, se puede acceder directamente tecleando la transacción asociada (ZTB2) ó desde el menú principal de EDItran/P: opción 6. En CICS se puede entrar directamente a las opciones de la gestión de claves desde EDItran/P tecleando 6.x (donde x tiene los valores 1 a 6).

```
|  PLTINI TCP: ZTBZ    GEST.CLAVE: ZTB2                                    |
```

2.2. Entorno CICS

Para la gestión de claves de intercambio, se requiere definir los siguientes elementos en PCT, PPT, FCT (además debe tener también las definiciones DES y RSA correspondientes, las cuales no se indican en este manual):

```
DEFINE      TRANSACTION(ZTB2) GROUP(EDITRAN) PROGRAM(ZTBPO020)
            TWASIZE(21000) SPURGE(YES) TPURGE(YES) TASKDATALOC(ANY)

DEFINE      PROGRAM(ZTBPOIGC) GROUP(EDITRAN) LANGUAGE(COBOL) DATALOCATION(ANY)
DEFINE      PROGRAM(ZTBPO020) GROUP(EDITRAN) LANGUAGE(COBOL) DATALOCATION(ANY)
DEFINE      PROGRAM(ZTBPO021) GROUP(EDITRAN) LANGUAGE(COBOL) DATALOCATION(ANY)
DEFINE      PROGRAM(ZTBPO022) GROUP(EDITRAN) LANGUAGE(COBOL) DATALOCATION(ANY)
DEFINE      PROGRAM(ZTBPO023) GROUP(EDITRAN) LANGUAGE(COBOL) DATALOCATION(ANY)
DEFINE      MAPSET(ZTBPM20) GROUP(EDITRAN)
DEFINE      MAPSET(ZTBPM21) GROUP(EDITRAN)
DEFINE      MAPSET(ZTBPM22) GROUP(EDITRAN)
DEFINE      MAPSET(ZTBPM23) GROUP(EDITRAN)

DEFINE  FILE(ZTBPFGC) GROUP(EDITRAN)
       DSNAME(PUNTERO.INDRA.ZTBPFGC) LSRPOOLID(NONE)
       STRINGS(2) BROWSE(YES)
       RECORDFORMAT(F) ADD(YES) DELETE(YES) READ(YES) UPDATE(YES)
```

El fichero anterior, ZTBPFGC, debe inicializarse. Se requiere pasar jcl ZTBPJIGC (delete-define + llamada a programa ZTBPBIGC), para inicializar el fichero ZTBPFGC

En los procedimientos, se requieren las siguientes actuaciones en los PROCEDIMIENTOS (además debe tener también las definiciones DES y RSA correspondientes, las cuales no se indican en este manual):

- Incluir fichero ZTBPFGC en todos los procedimientos previos a emisión (ZTBGP1C y ZTBGPMC) y posteriores a recepción de la entidad (ZTBGP4C):

  ```
  //ZTBPFGC  DD   DSN=KI.EGDC.ZTBP.ZTBPFGC,DISP=SHR
  ```

- Por otra parte se han creado (y se suministran), 3 procedimientos nuevos, que sólo se utilizarán en la sesión EDItran encargada del intercambio de claves con las entidades remotas (no en las sesiones normales de intercambio de datos):
  - Previo a emisión **ZTBGP1GC.** Sólo para el extremo que emite su clave. Este procedimiento no se incluirá en perfiles, lo utiliza la propia gestión de claves.
  - Posterior a emisión **ZTBGP3GC** (en perfil de ambos extremos). Tiene un paso que sólo es utilizado por el extremo que emite una clave.
  - Posterior a recepción **ZTBGP4GC** (en perfil de ambos extremos).

2.3. Obtención de las librerías

Se obtendrán, siempre que sea posible, ficheros formato IEBCOPY vía EDItran, que se volcarán en la librerías correspondientes verificando que su contenido coincide con la lista de módulos indicada anteriormente.

2.4. Compilación MFSs

Se ensamblarán los formatos adaptándolos a los dispositivos (DEV) de la instalación.

3. EJEMPLO DE FUNCIONAMIENTO.

Supongamos 2 entidades con NIF : 100099940 (local) y otra 200099940 (remota).

El administrador de la entidad 100099940 es Pepe Pérez Gonzalez (telef.111111111).

El administrador de la entidad 200099940 es Luis Díaz Lopez (telef.22222222).

Acuerdan: El subsistema de la entidad 100099940 es '1' y el subsistema de la entidad 200099940 es '2'. Intercambiar sus claves RSA por la aplicación TELEGC. El envío de la primera clave se iniciará desde 100099940 (un proceso de intercambio lleva 2 emisiones, envío de la clave y fich. Confirmación por lo que no conviene mezclar dos procesos de intercambio a la vez).

En el siguiente cuadro, se muestran las operaciones y la descripción a las mismas:

Subsistema (S) Entidad A	Estado claves	Operación	Red	Operación	Estado claves	Subsistema (S) Entidad B
(S)1 Propio RSA Local 100099940 Rem. 000000000	**V1-ACTIVA**	Da de alta el subsistema propio genérico. Generar clave (V1) Ver capítulo 3.3		Da de alta el subsistema propio genérico. Generar clave (V1) Ver capítulo 3.4	**V1-ACTIVA**	(S)2 Propio RSA Local 200099940 Rem. 000000000
(S)1 Propio RSA Local 100099940 Rem. 20009940		Da de alta el subsistema contra ese remoto. Ver capítulo 3.3		Da de alta el subsistema contra ese remoto. Ver capítulo 3.4		(S)2 Propio RSA Local 200099940 Rem. 10009940
(S)2 Ajeno RSA Local 100099940 Rem. 20009940		Da de alta el subsistema que le indica ese remoto. Ver capítulo 3.3		Da de alta el subsistema que le indica ese remoto. Ver capítulo 3.4		(S)1 Ajeno RSA Local 200099940 Rem. 10009940
				Exportar clave V1 del subsistema genérico Ver capítulo 3.4	V1-GENERADA	(S)2 Propio RSA Local 200099940 Rem. 10009940
			Emite File B Telegc	Envía la clave Ver capítulo 3.5	V1-GENERADA	(S)2 Propio RSA Local 200099940 Rem. 10009940
(S)2 Ajeno RSA Local 100099940	V1-RECIBIDA	Fin de recepción Posterior a recepción	Fin Telegc	Fin de emisión Posterior a emisión	V1-ENVIADA	(S)2 Propio RSA Local 200099940

Rem. 20009940		Incorpora la clave Ver capítulo 3.5		Actualiza estado Ver capítulo 3.5		Rem. 10009940
(S)2 Ajeno RSA Local 100099940 Rem. 20009940	V1-RECIBIDA		Emite Conf. A Telegc			
(S)2 Ajeno RSA Local 100099940 Rem. 20009940	**V1-ACTIVA**	Fin de emisión Posterior a emisión Actualiza estado Ver capítulo 3.5	Fin Telegc	Fin de recepción Posterior a recepción Actualiza estado Ver capítulo 3.5	**V1-ACTIVA**	(S)2 Propio RSA Local 200099940 Rem. 10009940
(S)1 Propio RSA Local 100099940 Rem. 20009940	V1-GENERADA	Exportar clave V1 del subsistema genérico Ver capítulo 3.6				
(S)1 Propio RSA Local 100099940 Rem. 20009940	V1-GENERADA	Envía la clave Ver capítulo 3.6	Emite File A Telegc			
(S)1 Propio RSA Local 100099940 Rem. 20009940	V1-ENVIADA	Fin de emisión Posterior a emisión Actualiza estado Ver capítulo 3.6	Fin Telegc	Fin de recepción Posterior a recepción Incorpora la clave Ver capítulo 3.6	V1-RECIBIDA	(S)1 Ajeno RSA Local 200099940 Rem. 10009940
			Emite Conf. B Telegc		V1-RECIBIDA	(S)1 Ajeno RSA Local 200099940 Rem. 10009940
(S)1 Propio RSA Local 100099940 Rem. 20009940	**V1-ACTIVA**	Fin de recepción Posterior a recepción Actualiza estado Ver capítulo 3.6	Fin Telegc	Fin de emisión Posterior a emisión Actualiza estado Ver capítulo 3.6	**V1-ACTIVA**	(S)1 Ajeno RSA Local 200099940 Rem. 10009940
(S)1 Propio RSA **Local 100099940**	**V1-ACTIVA** **V1-ACTIVA**	**OPERATIVO** **Para funcionar criptografía en todas las sesiones contra remoto**	**Emisión** **Recepc.** **Otras** **Ses.**	**OPERATIVO** **Para funcionar criptografíaen todas las sesiones contra**	**V1-ACTIVA** **V1-ACTIVA**	**(S)2 Propio RSA** **Local 200099940**

Rem. 20009940 **(S)2 Ajeno RSA** **Local 100099940** **Rem. 20009940**		**200099940** **PARM=*,1,2** AUT=RSA		**remoto 200099940** **PARM=*,1,2** AUT=RSA		**Rem. 10009940** **(S)1 Ajeno RSA** **Local 200099940** **Rem. 10009940**
(S)1 Propio RSA Local 100099940 Rem. 000000000	**V1-OPEATIVA** **V2-ACTIVA**	Ver 3.7		Se generan 2 claves V2 y V3, Ver 3.7	**V1-OPEATIVA** **V2-OPERATIVA** **V3-ACTIVA**	(S)2 Propio RSA Local 200099940 Rem. 000000000
(S)1 Propio RSA Local 100099940 Rem. 20009940	**V1-ACTIVA** **V2-GENERADA** **V2-ENVIADA**	Ver 3.7 Se hace el envío de V2(generada) y en post emi pasa a enviada	Telegc Emite File A Emite Conf B	Ver 3.7 Se hace recepción de v2 y en post rec pasa a recibida	**V1-ACTIVA** **V2-** **V2-RECIBIDA**	(S)1 Ajeno RSA Local 200099940 Rem. 10009940
(S)1 Propio RSA Local 100099940 Rem. 20009940	**V1-OPERATIVA** **V2-ACTIVA**	Ver 3.7 Post.rec.	Fin	Ver 3.7 Post emi	**V1-OPERATIVA** **V2-ACTIVA**	(S)1 Ajeno RSA Local 200099940 Rem. 10009940
(S)1 Propio RSA **Local 100099940** **Rem. 20009940** **(S)2 Ajeno RSA** **Local 100099940** **Rem. 20009940**	**V1-OPERATIVA** **V2-ACTIVA** **V1-ACTIVA**	OPERATIVO Con la V2 se descifran PARM=*,1,2 AUT=RSA	Emisión Recepc. Otras Ses.	OPERATIVO Con la V1 se cifran PARM=*2,1 AUT=RSA	**V1-ACTIVA** **V1-OPERATIVA** **V2-ACTIVA**	**(S)2 Propio RSA** **Local 200099940** **Rem. 10009940** **(S)1 Ajeno RSA** **Local 200099940** **Rem. 10009940**
(S)2 Ajeno RSA Local 100099940 Rem. 20009940	**V1-ACTIVA** **V3-RECIBIDA**	Ver 3.7 Se hace recepción de v3 y en post rec pasa a recibida	Telegc Emite File B Emite Conf A	Ver 3.7 Se hace el envío de V3(generada) y en post emi pasa a enviada	**V1-ACTIVA** **V3-ENVIADA**	(S)2 Propio RSA Local 200099940 Rem. **10009940**
(S)2 Ajeno RSA Local 100099940	**V1-OPERATIVA** **V3-ACTIVA**	Ver 3.7 Post.rec.	Fin	Ver 3.7 Post emi	**V1-OPERATIVA** **V3-ACTIVA**	(S)2 Propio RSA Local

Rem. 20009940						200099940 Rem. **10009940**
(S)1 Propio RSA **Local 100099940** **Rem. 20009940** **(S)2 Ajeno RSA** **Local 100099940** **Rem. 20009940**	**V1-OPERATIVA** **V2-ACTIVA** **V1-OPERATIVA** **V3-ACTIVA** **v2 no se recibió**	OPERATIVO Con la V2 se descifran PARM=*,1,2 AUT=RSA	Emisión Recepc. Otras Ses.	OPERATIVO Con la V1 se cifran PARM=*,2,1 AUT=RSA	**V1-OPERATIVA** **V3-ACTIVA** **v2 no exportó** **V1-OPERATIVA** **V2-ACTIVA**	**(S)2 Propio RSA** **Local 200099940** **Rem. 10009940** **(S)1 Ajeno RSA** **Local 200099940** **Rem. 10009940**

3.1. Definición del perfil de entorno

En ambas entidades, si no existiera, los administradores, dan de alta su respectivo registro de entorno local, opción 6.1 en CICS:

```
|    REQUIERE EDITRAN PARA GESTION (S/N): S                                    |
|    PREFIJO DE INSTALACION DE FICHEROS.: KI.EGDC                              |
|    APLICACION EDITRAN/P DE SERVICIO...: TELEGC                               |
|    PREFIJO LABEL.....................: LABEL.PRODUCTOS.EDI                   |
|    NOMBRE PROC. PARA GENERACION CLAVES: ZTBGP1GC                             |
|                                                                              |
|   FICHAS DE JCL                                                              |
|   =============                                                              |
|        ===> //KI0F6AEX JOB (EGDC,KIT,,99),EDITRAN,MSGCLASS=H,CLASS=A,       |
|        ===> //             MSGLEVEL=1                                        |
|        ===> //*                                                              |
|        ===> //*JOBLIB   DD DSN=KI.EIDC.ZTBG.LOAD,DISP=SHR                   |
|        ===> //*                                                              |
```

3.2. Definición de la sesión TELEGC

En ambas entidades, los administradores, dan de alta una sesión TELEGC (por donde intercambiarán claves). Se recomienda no usar criptografía ni compresión.

En esa sesión, no se ponen ficheros de aplicación de emisión. En CICS, en los procedimientos, se indica:

- Sin previo a emisión.
- En posterior a emisión, ZTBGP3GC, que se suministra al efecto
- En posterior a recepción, ZTBGP4GC, que se suministra al efecto
- El resto, los estándar

En cuanto a **traducción**:

- Lenguaje original de datos EBCDIC,
- Traducir en emisión No, y traducir en recepción **E**BCDIC

Antes de proseguir, realice una prueba de conexión en ambos sentidos.

3.3. Definición del perfil de propias RSA y remotas RSA en 100099940.

El administrador de la entidad 100099940 (Pepe Pérez González), da de alta el subsistema '1' PROPIO RSA opción 6.2. Si ya existiera algún subsistema, podría aprovecharlo para exportar y enviar claves que tuviera ese subsistema a la entidad 200099940, pero supongamos que la entidad 100099940 está comenzando con la gestión de claves.

Al dar de alta, puede cambiar las etiquetas, pero no se recomienda

Nótese que al dar de alta este registro, no indica en ningún sitio que las claves que incluirá son para la entidad 200099940.

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   15:57:45             GESTION DE CLAVES PROPIAS RSA                        |
|------------------------------------------------------------------------------|
|                                                                              |
|      SUBSISTEMA.....: 1                      ENTORNO LOCAL..: 100099940      |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                 |
|      NOMBRE DEL ADMINISTRADOR...........:                            LOCAL   |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
|                                                                              |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.1.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD DE GENERACION DE CLAVE: 2048 (1024/2048/4096)                       |
|                                                                              |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

A continuación, genera pareja de claves en la misma opción 6.2. Esto ocasiona que se lanza el procedimiento indicado en el perfil de entorno, ZTBGP1GC, que genera la pareja de claves RSA privada-pública con Versión 01, y en dicho registro, una vez acaba el procedimiento, aparece en dicha pantalla:

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   15:57:45             GESTION DE CLAVES PROPIAS RSA                        |
|------------------------------------------------------------------------------|
|                                                                              |
|      SUBSISTEMA.....: 1                      ENTORNO LOCAL..: 100099940      |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                 |
|      NOMBRE DEL ADMINISTRADOR...........:                            LOCAL   |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
|                                                                              |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.1.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD DE GENERACION DE CLAVE: 2048 (1024/2048/4096)                       |
|                                                                              |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  01  20160609-162740 20160609-162740 4-ACTIVO         (S)ELEC. VER PUBLICA   |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

A continuación, como es la primera vez, que va a intercambiar claves con la entidad 2000999940, entra en la opción 6.3 y da de alta el registro de claves propias RSA, subsistema 1, local 100099940, remoto 200099940

Nota: En subsistema RSA para Firmar, no se indica nada, puesto que es el primer intercambio de claves con ese remoto.

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 1    LOCAL......: 100099940     REMOTO.....: 200099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA...........: SUBS.PRINCIPAL RSA               |
|      NOMBRE DEL ADMINISTRADOR............:                          REMOTO   |
|      TELEFONO DEL ADMINISTRADOR..........:                                   |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.1.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                         |
|  10  20160609-162740 20161019-164235 1-GENERADO       (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

Fíjese que las etiquetas, no llevan el código remoto, porque serán las claves exportadas desde la opción 6.2 (todavía no se han exportado).

Una vez realizado esto, el administrador de la entidad 100099940, da de alta el subsistema ajeno (que le indicó el administrador de la entidad 200099940). Este subsistema lo da de alta en la opción 6.4.

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:01:34           ASOCIACION DE CLAVES AJENAS RSA                        |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 100099940     REMOTO.....: 200099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA...........: SUBS. SECUNDARIO RSA              |
|      NOMBRE DEL ADMINISTRADOR............:                          REMOTO   |
|      TELEFONO DEL ADMINISTRADOR..........:                                   |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.2.200099940.RSA.AJENA.PUBLICA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:     0                            |
|                                                                              |
| SUBSISTEMA RSA FIRMADO.......:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                         |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> SALIR                                             |
```

Nótese que en este caso, si aparece en las etiquetas el código remoto

Nota: En subsistema RSA Firmado, no se indica nada, puesto que es el primer intercambio de claves con ese remoto.

En este punto, el administrador de 100099940, está preparado para recibir la clave de 200099940

Ahora entramos en la definición del perfil de propias RSA y remotas RSA en el otro extremo 200099940.

El administrador de la entidad 200099940 (Luis Díaz López), ya ha trabajado con gestión de claves, y ya tenía creado el subsistema propio 2 (opción 6.2), de forma que no le hace falta crearlo. En este momento en esa opción tiene:

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:04:14           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 200099940     REMOTO.....: 100099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                |
|      NOMBRE DEL ADMINISTRADOR...........:                            REMOTO  |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.2.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...: 0                                             |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  01  20050830-105719 20160511-133714 4-ACTIVO         (S)ELEC.VER PUBL.LOC.  |
|  02  20080704-122959 20130211-142214 4-ACTIVO         (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

En concreto ya tiene definidas 2 claves en ese subsistema, V1 y V2, que exportó a otros remotos, de forma que va a exportar V3 al remoto 100099940.

A continuación, como es la primera vez, que va a intercambiar claves con la entidad 1000999940, entra en la opción 6.3 y da de alta el registro de claves propias RSA, subsistema 2, local 200099940, remoto 100099940

Nota: En subsistema RSA para Firmar, no se indica nada, puesto que es el primer intercambio de claves con ese remoto.

```
--------------------------------------------------------------------------------
|   14/02/2011         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:58:47           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 200099940     REMOTO.....: 100099940        |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                |
|      NOMBRE DEL ADMINISTRADOR...........:                            REMOTO  |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.2.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> ALTA                                              |
--------------------------------------------------------------------------------
```

Fíjese que las etiquetas, no llevan el código remoto, porque serán las claves exportadas desde la opción 6.2 (todavía no se han exportado).

Una vez realizado esto, el administrador de la entidad 200099940, da de alta el subsistema ajeno (que le indicó el administrador de la entidad 100099940). Este subsistema lo da de alta en la opción 6.4.

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:01:34           ASOCIACION DE CLAVES AJENAS RSA                        |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 1    LOCAL......: 200099940     REMOTO.....: 100099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA...........: SUBS. SECUNDARIO RSA              |
|      NOMBRE DEL ADMINISTRADOR............:                            REMOTO   |
|      TELEFONO DEL ADMINISTRADOR..........:                                   |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.1.100099940.RSA.AJENA.PUBLICA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:     0                            |
|                                                                              |
| SUBSISTEMA RSA FIRMADO........:                                              |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                         |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> SALIR                                             |
```

Nótese que en este caso, si aparece en las etiquetas el código remoto

Nota: En subsistema RSA Firmado, no se indica nada, puesto que es el primer intercambio de claves con ese remoto.

En este punto, el administrador de 100099940, está preparado para recibir la clave de 200099940, pero como acordaron que el administrador de 200099940, enviase primero, Luis, entra de nuevo en la opción 6.3, generación y exportación de claves de forma que le acaba quedando:

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 200099940     REMOTO.....: 100099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA...........: SUBS.PRINCIPAL RSA                |
|      NOMBRE DEL ADMINISTRADOR............:                            REMOTO   |
|      TELEFONO DEL ADMINISTRADOR..........:                                   |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.2.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                         |
|  10  20160609-162740 20161019-164235 1-GENERADO       (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

3.4. Emisión de la clave RSA desde la entidad 200099940.

Automáticamente se ha lanzado un previo a emisión que ha cargado la clave V3 y la está enviando al remoto 100099940.

Una vez se lanza el posterior a emisión, el administrador de la entidad 200099940, en la opción 6.3 verá

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 200099940     REMOTO.....: 100099940       |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                |
|      NOMBRE DEL ADMINISTRADOR...........:                            REMOTO  |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.2.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  03  20160609-162740 20161019-164235 2-ENVIADA        (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

En la entidad 100099940, el administrador, en su opción 6.4, una vez finalizado el posterior a recepción verá:

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:01:34           ASOCIACION DE CLAVES AJENAS RSA                        |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 100099940     REMOTO.....: 200099940       |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS. SECUNDARIO RSA               |
|      NOMBRE DEL ADMINISTRADOR...........:                            REMOTO  |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.2.200099940.RSA.AJENA.PUBLICA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:     0                            |
|                                                                              |
| SUBSISTEMA RSA FIRMADO.......:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  03  20100210-174527 20050210-174527 2-RECIBIDA                              |
|                                                                              |
|  <PF3> SALIR, <INTRO> MODIFICAR                                              |
--------------------------------------------------------------------------------
```

Sin embargo, en la entidad 100099940, se ha generado un fichero de confirmación, que comienza a emitirse de forma automática a la entidad 200099940.

Una vez acaba este envío, y tras su posterior a emisión, en la entidad 100099940, el administrador, accede a la opción 6.4 y encontrará que el estado de la clave ha cambiado a ACTIVO. Debe entrar por modificación e incluir el subsistema RSA firmado, de forma que si recibe nuevas claves vendrán firmadas por una clave anteriormente intercambiada

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES AJENAS RSA                        |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 100099940     REMOTO.....: 200099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                 |
|      NOMBRE DEL ADMINISTRADOR...........:                          REMOTO    |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.2.200099940.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  10  20160609-162740 20161019-164235 4-ACTIVA         (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

Una vez acaba este envío, y tras su posterior a recepción, en la entidad 200099940, el administrador, accede a la opción 6.3 y encontrará que el estado de la clave ha cambiado a ACTIVO. Debe entrar por modificación e incluir el subsistema RSA para firmar, de forma que si emite nuevas claves irán firmadas por una clave anteriormente intercambiada

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 2    LOCAL......: 200099940     REMOTO.....: 100099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                 |
|      NOMBRE DEL ADMINISTRADOR...........:                          REMOTO    |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.2.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  03  20160609-162740 20161019-164235 4-ACTIVA         (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

3.5. Emisión de la clave RSA desde la entidad 100099940.

El administrador de la entidad 100099940, debe

Exportar la clave de su subsistema 1 propio RSA

Enviarla al remoto.

Para ello, accede a la opción 6.3, y exporta y envía, quedándole:

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 1    LOCAL......: 100099940     REMOTO.....: 200099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA...........: SUBS.PRINCIPAL RSA               |
|      NOMBRE DEL ADMINISTRADOR............:                          REMOTO   |
|      TELEFONO DEL ADMINISTRADOR..........:                                   |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.1.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  01  20160609-162740 20161019-164235 1-GENERADO       (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

Automáticamente se ha lanzado un previo a emisión que ha cargado la clave V1 y la está enviando al remoto 200099940.

Una vez se lanza el posterior a emisión, el administrador de la entidad 100099940, en la opción 6.3 verá

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 1    LOCAL......: 100099940     REMOTO.....: 200099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA...........: SUBS.PRINCIPAL RSA               |
|      NOMBRE DEL ADMINISTRADOR............:                          REMOTO   |
|      TELEFONO DEL ADMINISTRADOR..........:                                   |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.1.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  01  20160609-162740 20161019-164235 2-ENVIADA        (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

En la entidad 200099940, el administrador, en su opción 6.4, una vez finalizado el posterior a recepción verá:

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:01:34           ASOCIACION DE CLAVES AJENAS RSA                        |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 1    LOCAL......: 200099940     REMOTO.....: 100099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS. SECUNDARIO RSA               |
|      NOMBRE DEL ADMINISTRADOR...........:                              REMOTO  |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.1.100099940.RSA.AJENA.PUBLICA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:     0                            |
|                                                                              |
| SUBSISTEMA RSA FIRMADO.......:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  03  20100210-174527 20050210-174527 2-RECIBIDA                              |
|                                                                              |
|  <PF3> SALIR, <INTRO> MODIFICAR                                              |
--------------------------------------------------------------------------------
```

Después, en la entidad 200099940, se ha generado un fichero de confirmación, que comienza a emitirse de forma automática a la entidad 100099940.

Una vez acaba este envío, y tras su posterior a emisión, en la entidad 20099940, el administrador, accede a la opción 6.4 y encontrará que el estado de la clave ha cambiado a ACTIVO.

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:01:34           ASOCIACION DE CLAVES AJENAS RSA                        |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 1    LOCAL......: 200099940     REMOTO.....: 100099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS. SECUNDARIO RSA               |
|      NOMBRE DEL ADMINISTRADOR...........:                              REMOTO  |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.200099940.1.100099940.RSA.AJENA.PUBLICA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:     0                            |
|                                                                              |
| SUBSISTEMA RSA FIRMADO.......:                                               |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  03  20100210-174527 20050210-174527 4-ACTIVA                                |
|                                                                              |
|  <PF3> SALIR, <INTRO> MODIFICAR                                              |
--------------------------------------------------------------------------------
```

Una vez acaba este envío, y tras su posterior a recepción, en la entidad 100099940, el administrador, accede a la opción 6.3 y encontrará que el estado de la clave ha cambiado a ACTIVO. Debe entrar por modificación e incluir el subsistema RSA para firmar, de forma que si emite nuevas claves irán firmadas por una clave anteriormente intercambiada.

```
--------------------------------------------------------------------------------
|   23/05/2017         GESTION DE CLAVES DE INTERCAMBIO         EDITRAN 5.2   |
|   16:00:28           ASOCIACION DE CLAVES PROPIAS RSA                       |
|------------------------------------------------------------------------------|
|  SUBSISTEMA.: 1    LOCAL......: 100099940     REMOTO.....: 200099940        |
|                                                                              |
|      DESCRIPCION DE SUBSISTEMA..........: SUBS.PRINCIPAL RSA                |
|      NOMBRE DEL ADMINISTRADOR...........:                            REMOTO  |
|      TELEFONO DEL ADMINISTRADOR.........:                                    |
|      APLICACION EDITRAN/P DE SERVICIO...: TELEGC                             |
| LABEL PAREJA: LABEL.PRODUCTOS.EDI.100099940.1.000000000.RSA.LOCAL.PRIVADA    |
| LONGITUD CLAVE ACTIVA EN EL SUSBSISTEMA...:                                  |
|                                                                              |
| SUBSISTEMA RSA PARA FIRMAR...:  1                                            |
|          RELACION DE CLAVES PRIVADAS Y PUBLICAS (LABEL + VERSION)            |
| VERS F-HORA GENERAC. F-HORA MODIFIC.    ESTADO   SEL                         |
| ---- --------------- --------------- ----------- ---                        |
|  01  20160609-162740 20161019-164235 4-ACTIVA         (S)ELEC.VER PUBL.LOC.  |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|       <PF3> SALIR, <INTRO> VISUALIZACION DE PUBLICA                          |
--------------------------------------------------------------------------------
```

3.6. Nuevos intercambios RSA.

Una vez que se han intercambiado claves las 2 entidades, pueden intercambiarse nuevas claves del mismo subsistema ó intercambiarse claves de otro subsistema.

El proceso de intercambio, es el mismo que el intercambio inicial

3.7. Exportación masiva de claves RSA. Actualización del subs.rsa firma.

En la opción 6.2, si existe una clave en estado ACTIVA, se exporta a todos los remotos de ese subsistema que no tuvieran claves en vuelo.

Por otra parte, anteriormente, al dar de alta un subsistema y enviar por primera vez claves a un remoto, éstas se envían en claro y se activan de forma automática. Posteriormente, si una entidad genera nuevas claves, para poder exportarlas a ese remoto de un determinado subsistema, lo primero que debe hacer es entrar en la opción 3 (propias), y modificar el campo SUBSISTEMA RSA PARA FIRMAR, incluyendo en el mismo un subsistema que tiene claves activas, anteriormente intercambiadas, para así enviar las nuevas claves firmadas bajo esas. Esto, en la última versión, se hace de forma automática, evitando así al usuario el tener que acceder por modificación.

Ejemplo. Si tenemos el siguiente fichero::

Tipo	Prop	Local	Subs.	Rem	Sub.firm	Vers(1)-Est	Vers(1)-Est	Vers(3)-Est	Apl.serv
R	**L**	**xxxx**	**D**	**----**		**V11-E04**			**xxxx**
R	L	xxxx	D	0001					**spaces**
R	L	xxxx	D	0002		V01-E01			xxxx
R	L	xxxx	D	0003		V01-E02			xxxx
R	L	xxxx	D	0004		V11-E01			xxxx
R	L	xxxx	D	0005		V11-E02			xxxx
R	L	xxxx	D	0006		V11-E03			xxxx
R	L	xxxx	D	0007		V11-E04			xxxx
R	L	xxxx	D	0008	E	V01-E03	V11-E05		xxxx
R	L	xxxx	E	....		V01-E04			xxxx
R	L	xxxx	E	0008		V01-E01			xxxx
R	L	xxxx	D	0009	F	V01-E04	V11-E05		xxxx
R	L	xxxx	F	....		V01-E02			Xxxx
R	L	xxxx	F	0009		V01-E02			xxxx
R	L	xxxx	D	0010					xxxx
R	L	xxxx	E	0010		V01-E04			xxxx
R	L	xxxx	D	0011					xxxx
R	L	xxxx	E	0011		V01-E04			xxxx
R	L	xxxx	D	0012		V01-E04	V11-E05	V03-E03	xxxx

R	L	xxxx	D	0013	D	V11-E05			xxxx
R	L	xxxx	E	0013		V01-E03			xxxx
R	L	xxxx	D	0014	E	V10-E05			xxxx
R	L	xxxx	D	0015	J	V11-E05			xxxx
R	L	xxxx	J	....					xxxx
R	L	xxxx	K	....		V01-E05			xxxx
R	L	xxxx	K	0015		V11-E03			xxxx
R	L	xxxx	D	0016	D	V11-E05			xxxx
R	L	xxxx	E	0016		V01-E03			xxxx
R	L	xxxx	F	0016		V01-E04			xxxx
R	L	xxxx	D	0017					xxxx
R	L	xxxx	E	0017		V01-E03			xxxx
R	L	xxxx	D	0018					xxxx
R	L	xxxx	E	0018		V01-E04			xxxx
R	L	xxxx	L	....		V01-E03			xxxx
R	L	xxxx	L	0018		V01-E04			xxxx
R	L	xxxx	D	0019					xxxx
R	L	xxxx	H	0019		V01-E03			xxxx

Si queremos hacer exportaciones masivas (desde opción 6.2). Exportamos RSA del subsistema D (registro 1).

a. No exportamos el remoto 0001 porque no tiene aplicación de servicio. Registro R-L-nif local-D-000000010

b. No exportamos el remoto 0002 porque tiene una clave V01 en estado 01. Registro R-L-nif local-D-000000020

c. No exportamos el remoto 0003 porque tiene una clave V01 en estado 02. Registro R-L-nif local-D-000000030

d. No exportamos el remoto 0004 porque tiene la clave a exportar V11 en estado 01. Registro R-L-nif local-D-000000040

e. No exportamos el remoto 0005 porque tiene la clave a exportar V11 en estado 02. Registro R-L-nif local-D-000000050

f. No exportamos el remoto 0006 porque tiene la clave a exportar V11 en estado 03. Registro R-L-nif local-D-000000060

g. No exportamos el remoto 0007 porque tiene la clave a exportar V11 en estado 04. Registro R-L-nif local-D-000000070

h. No exportamos el remoto 0008 (Registro R-L-nif local-D-000000080) porque el registro R-L-nif local-E-000000080 tiene una clave V01 en estado 01.

i. No exportamos el remoto 0009 (Registro R-L-nif local-D-000000090) porque el registro R-L-nif local-E-000000090 tiene una clave V01 en estado 02.

j. Exportamos el remoto 0012. Cambiará el subsistema para firmar (D) y el orden de las claves, V1-V3-V11. No existía subsistema para firmar, pero en el registro, existían claves en E03-E04, luego se habían intercambiado claves por el subsistema D, y por tanto, esta nueva se firma con ese subsistema.

k. Exportamos el remoto 0013. Cambiará el subsistema para firmar (E) y el estado de la clave V11. Existía subsistema para firmar, pero se detecta que estaba en estado cancelada. Como existe el Registro R-L-nif local-E-0000000130, con una clave activa (V1 en estado 03), significa e habían intercambiado claves por el subsistema H, y por tanto, esta nueva se firma con ese subsistema.

l. Exportamos el remoto 0014. Cambiará el subsistema para firmar (espacios) y aparecerá la nueva clave V11 en estado 01. No existía ningún registro intercambiado con ese remoto con otro subsistema. Como además la clave que tiene es la V10 y está cancelada, significa que no se ha intercambiado nada con el remoto, y por ello, se cambia el subsistema a firmar a espacios.

m. Exportamos el remoto 0015. Cambiará el subsistema para firmar (E) y cambiará el estado de la clave V11, a estado 01. Tenía subsistema firma D, pero no había claves activas, por lo que ha encontrado el registro R-L-nif local-E-0000000150 con una clave en estado 3, por lo que actualiza el subistema para firmar.

n. Exportamos el remoto 0016. Cambiará el subsistema para firmar (F) y cambiará el estado de la clave V11, a estado 01. Existían los registros R-L-nif local-E-0000000160 y -L-nif local-F-0000000160, el primero con una clave en estado 03 y el segundo en 04, con lo que nos quedamos con el F porque es de estado 04. No cogemos el subsistema de firma que había porque sólo había una clave cancelada.

o. Exportamos el remoto 0017. Cambiará el subsistema para firmar (E) y aparece la nueva clave V11 en estado 01. Existía el registro R-L-nif local-E-0000000170 con calves activas, estado 03, por eso cambiamos el subsistema para firmar.

p. Exportamos el remoto 0018. Cambiará el subsistema para firmar (E) y aparece la nueva clave V11 en estado 01. Existía el registro R-L-nif local-E-0000000180 con claves activas, estado 04, por eso cambiamos el subsistema para firmar.

q. Exportamos el remoto 0019. Cambiará el subsistema para firmar (E) y aparece la nueva clave V11 en estado 01. Existía el registro R-L-nif local-E-0000000190 con claves activas, estado 04, por eso cambiamos el subsistema para firmar.

Al finalizar el proceso, dará un mensaje **"Exportación correcta (0008 exportados de 0019 tratados)". Deben haberse lanzado 8 cargas.** En negrita los cambios en algunos registros:

Tipo	Prop	Local	Subs.	Rem	Sub.firm	Vers(1)-Est	Vers(1)-Est	Vers(3)-Est	Apl.serv
R	L	xxxx	D	0012	D	V01-E04	V03-E03	V11-E01	xxxx
R	L	xxxx	D	0013	**E**	**V11-E01**			xxxx
R	L	xxxx	D	0014	**nada**	V10-E05	**V11-E01**		xxxx
R	L	xxxx	D	0015	**E**	**V11-E01**			xxxx
R	L	xxxx	D	0016	**F**	**V11-E01**			xxxx
R	L	xxxx	D	0017	**E**	**V11-E01**			xxxx
R	L	xxxx	D	0018	**E**	**V11-E01**			xxxx
R	L	xxxx	D	0019	**E**	**V11-E01**			xxxx

4. Anexo.

4.1. Aplicación de intercambio de claves.

Se propone la aplicación TELEGC para intercambiar claves (no es obligatorio, incluso puede ser una aplicación para un sentido y otra para el otro).

En caso de utilizar TELEGC, se define la sesión de presentación y la de transmisión asociada en ambos extremos.

En esta aplicación, se puede utilizar cifrado, pero las claves enviadas-recibidas ya van cifradas, con lo que no es muy útil su uso.

En caso de utilizar TELEGC en ambos sentidos, se van a dar procesos distintos:

a) PROCESO 1- El extremo local emite una clave local (previo a emisión y posterior a emisión). El extremo remoto la recibe (posterior a recepción+previo a emisión de la confirmación).

b) PROCESO 2- El extremo remoto emite la confirmación de que la ha procesado (posterior a emisión). El extremo local la recibe (posterior a recepción)

c) PROCESO 3- El extremo remoto emite una clave remota (previo a emisión y posterior a emisión). El extremo local la recibe (posterior a recepción+previo a emisión de la confirmación).

d) PROCESO 4- El extremo local emite la confirmación de que la ha procesado (posterior a emisión). El extremo local la recibe (posterior a recepción).

e) PROCESO 5- Adicionalmente, cada vez que se generan claves rsa (privada y pública), aunque no se transmiten al remoto, entra el procedimiento especificado en el perfil de Gestión de Claves.

El perfil de la sesión EDItran/P y EDItran/G sería el siguiente:

- No poner fichero de aplicación en la sesión de presentación.
- Procedimiento previo a emisión, previo a recepción, modificación de estados y excepción. Colocar los standard de EDItran (ZTBGP1C, ZTBGP2C, ZTBGP6C, ZTBGP5C). **Nota:** Desde la gestión de claves de intercambio, en caso de emitir claves, se lanzará un previo a emisión distinto (ZTBGP1GC). El motivo, se explica un poco más adelante.
- Procedimiento posterior a emisión: ZTBGP3GC.
- Procedimiento posterior a recepción: ZTBGP4GC.

Los procedimientos proporcionados funcionan de la siguiente forma:

1) Previo a emisión. **ZTBGP1GC**. Este procedimiento tiene 2 pasos PASO001 y A1P (previo a emisión). Se utiliza para varias cosas:

   a) Para generar pareja de claves propias RSA (PROCESO 5). En este caso **PASO001** acaba con **rc=00** y el **paso A1P no se ejecuta.**

b) Para emitir claves: PROCESO 1 de extremo local ó PROCESO 3 en extremo remoto. En ambos casos, el operador correspondiente, desde la opción 6.3 ó 6.4, asociará (RSA), generará (DES) y cargará el tampón y emitirá en ese momento ó no, en función de lo que quiera. Por ello, el **PASO001 acaba con rc=01** (para diferenciarlo de la situación de generar pareja de claves propias) y el paso A1P se ejecuta y debe acabar con rc=00 (con función 01 carga y con función 03 emite). Nota: El motivo de que en los perfiles de EDItran/P y G, tenga el procedimiento standard previo a emisión ZTBGP1C, en vez de ZTBGP1GC, es porque en caso de no querer emitir, si más tarde desde EDItran/G se emite, se lanzará ZTBGP1C, que encontrará tampón cargado y emitirá normalmente.

2) Posterior a emisión. **ZTBGP3GC.** Este procedimiento tiene varios pasos: el propio posterior a emisión, el de listado de ficheros y el PASO003. Este **PASO003** puede acabar con los siguientes valores:

   a) En caso de PROCESO1 (entra en extremo local al emitir una clave local) ó PROCESO 3 (entra en extremo remoto al emitir su clave local), acaba **con rc=304**, El motivo es que no se actualizará el estado de la clave enviada hasta recibir confirmación a la misma (ZTBGP4GC, posterior a recepción del extremo que recibe la confirmación ó posterior a emisión de extremo que emite la confirmación).

   b) En caso de PROCESO 2 (entra en extremo remoto al emitir confirmación de una clave recibida desde local) ó PROCESO 4 (entra en extremo local al emitir confirmación de una clave recibida desde remoto) acaba **con rc=00**, actualizando el estado de la clave desde RECIBIDA a ACTIVA.

3) Posterior a recepción. **ZTBGP4GC.** Este procedimiento tiene varios pasos: el propio posterior a recepción, el de listado de ficheros, el PASO003 y a continuación un mandato de PREVIO A EMISION (A1P), para emitir la confirmación automática en algún caso. Este PASO003 ó el paso A1P, pueden acabar con los siguientes valores:

   a) El **PASO003** en caso de PROCESO 2 (extremo local recibe la confirmación) ó PROCESO 4 (extermo remoto recibe la confirmación) acaba con **rc=00.** En ambos casos, **el paso A1P NO SE EJECUTA.**

   b) El **PASO003** en caso de PROCESO 1 (extremo remoto recibe clave local) ó PROCESO 3 (extremo local recibe clave remota) acaba con **rc=01**. En ambos casos, **el paso A1P** que se ejecuta a continuación para emitir la confirmación, debe acabar con **rc=00.**

En ambos extremos no se pone fichero de aplicación de emisión:

- Cuando se va a emitir la clave (PROCESO 1 ó 3), el PASO001 (rc=01) crea una lista de ficheros cuyo contenido es el nombre del fichero a cargar el el paso siguiente A1P (parámetro LF=S, Lista de ficheros = 'S').
- Cuando se carga la confirmación PROCESO 1 ó 3) el PASO003 hace lo mismo.

En resumen:

Procedimientos que entran según el extremo que emite / recibe.			
Extremo	**Procedimiento**		
	Previo a emisión (ZTBGP1GC) PASO001 + A1P	Posterior a emisión (ZTBGP3GC) A3P +PASO003	Posterior a recepción + Previo a emisión (ZTBGP4C) A4P +PASO003+A1P
Emisor de la clave y Receptor confirmac.	**Caso 1:** Generar claves propias RSA: **PASO001 rc=00** **A1P FLUSH**	A3P **rc=00** PASO3 **rc=304**	**A4P rc=00** **PASO003 rc =00** **A1P = FLUSH**
	Caso 2: Enviar clave **PASO001 rc= 01** **A1P (LF=S) rc=00**		
Receptor de la clave y Emisor confirmac.	No entra.	A3P **rc=00** PASO3 **rc=00**	**A4P rc=00** **PASO003 rc =01** **A1P (LF=S) rc = 00**

Cambios de estado de las claves enviadas recibidas según el extremo que emite / recibe.			
Extremo	**Procedimiento**		
	Previo a emisión (ZTBGP1GC) PASO001 + A1P	Posterior a emisión (ZTBGP3GC) A3P +PASO003	Posterior a recepción + Previo a emisión (ZTBGP4C) A4P +PASO003+A1P
Emisor de la clave y Receptor confirmac.	**Caso 1:** Generar claves propias RSA: **PASO001 ACTIVA**		**PASO003 ACTIVA**
	Caso 2: Enviar clave **PASO001 ENVIADA**		
Receptor de la clave y Emisor confirmac.	No entra.	PASO3 **ACTIVA**	**PASO003 RECIBIDA**

4.2. Verificacion de claves intercambiadas..

Cuando 2 entidades han utilizado el intercambio de claves, pueden validar de la siguiente forma, en caso de que falle la criptografía:

- E**n EDItran/P y en EDItran/G, deben tener puestos los mismos valore**s: cifrado = 's', versión = 3.0 o 4.0, algoritmos adecuados e interfaz de claves (ZTBGBIGC para batch y ZTBPOIGC para on-line).
- Si un extremo tiene puesto **en parm** de una sesión con cifrado el valor *,a,b, en la entidad remota, deben haber puesto **el valor inverso**, es decir, *,b,a (la entidad remota puede utilizar los campos clave local y clave remota, pero no tiene mucho sentido actuar así).
- Una vez que se está de acuerdo en los valores anteriores:
    - **Consulta de la versión y clave enviada en un sentido**.
        - **El extremo local, consulta el subsitema que tiene con la entidad remota**, por ejemplo el subsistema 0 (opción 6.3 para RSA y 6.4 para DES).
        - **El extremo remoto consulta el MISMO** subsistema (opción 6.4 para RSA).
        - En ambos extremos **DEBE DE APARECER la misma VERSION ACTIVA.** Si no es así, activar manualmente alguna, poniéndose de acuerdo en ambos extremos para que en ambos quede activa la misma versión.
        - Seleccionar el label de versión (cálculo de módulo-exponente para RSA y cifrado para DES). Ambos extremos **deben "visualizar" lo mismo**.
    - **Consulta de la versión y clave enviada en el otro sentido**.
        - **El extremo remoto, consulta el subsitema que tiene con nuestra entidad,** por ejemplo el subsistema 0 (opción 6.3)
        - **El extremo local consulta el MISMO subsistema** (opción 6.4).
        - En ambos extremos **DEBE DE APARECER la misma VERSION ACTIVA**. Si no es así, activar manualmente alguna, poniéndose de acuerdo en ambos extremos para que en ambos quede activa la misma versión.
        - Seleccionar el label de versión (cálculo de módulo-exponente para RSA y cifrado para DES). Ambos extremos **deben "visualizar" lo mismo**.

4.3. Lábeles (por defecto) creados por EDItran.

Los punteros de label, van separados por puntos, acaban siempre con el string VXX, donde xx es la versión.

Nivel	Nombre	Long.	Tipo	Descripción
1	Prefijo	11	Alfn.	Prefijo label especificado en entorno local
1	Punto	01	Alfn.	Valor '.'
1	Nif local	09	Alfn.	Nif local de la entidad
1	Punto	01	Alfn.	Valor '.'
1	Subsistema	01	Alfn.	Subsistema Subsistema local para el que emite claves Subsistema remoto para el que recibe claves
1	Punto	01	Alfn.	Valor '.'
1	Nif remoto	09	Alfn.	Ceros para RSA locales Nif remoto para resto.
1	Punto	01	Alfn.	Valor '.'
1	Tipo-clave	03	Alfn.	Tipo. RSA
1	Punto	01	Alfn.	Valor '.'
1	Propia-ajena	Xx	Alfn.	Para RSA a enviar valor 'LOCAL' Para RSA pública recibida, valor AJENA
1	Punto	01	Alfn.	Valor '.'
1	STRING TIPO-RSA	07	Alfan.	Valores 'PRIVADA' ó 'PUBLICA'
1	Punto	01	Alfn.	Valor '.'
3	Versión	03	ALFN.	Valor Vxx, donde xx es versión 01-99

- Para RSA locales:

Prefijo-label+Nif-local+Subsistema+ceros(9)+RSA+LOCAL+PRIVADA+Vxx

Prefijo-label+Nif-local+Subsistema+ceros(9)+RSA+LOCAL+PUBLICA+Vxx

- Para RSA remotas (pública):

Prefijo-label+Nif-local+Subsistema+Nif-remoto+RSA+AJENA+PUBLICA+Vxx

4.4. Parámetros para llamar a la interfaz de cifrado

El nombre de la interfaz es en CICS ZTBPOIGC (on-line) - ZTBGBIGC (batch), y en IMS ZTBPBIGC.

Nivel	Nombre	Long.	Tipo	Descripción
1	Asterisco	01	Alfn.	Valor '*'. Indica que se trata de la interfaz de gestión de claves de EDItran.
1	Coma	01	Alfn.	Valor ','.
1	Subsistema local	01	Alfn.	Subsistema local del que se extrae el label activo.
1	Coma	01	Alfn.	Valor ','.
1	Subsistema remoto	01	Alfn.	Subsistema remoto del que se extrae el label activo .

Ejemplo para EDItran/P:

```
                    -----  CRIPTOGRAFIA (S/N) ..:  S -----
VERSION CRIPTOGRAFICA.........: 3 . 00   CAMBIO DE CLAVE V2.2 (S/N/U).: N
ALGORITMO CONFIDENCIALIDAD ..: DES      ALGORITMO AUTENTICACION .....: RSA
INTERFAZ DE CLAVES: ZTBPOIGC            PARM : *,1,2
```

Ejemplo para EDItran/G:

```
|                -----  CRIPTOGRAFIA (S/N)...:  S  -----                      |
| ALGORITMO CONFIDENCIALIDAD ..:  DES   ALGORITMO AUTENTICACION ..:  RSA      |
| INTERFAZ DE CLAVES :  ZTBGBIGC   PARAMETROS: *,1,2                          |
```

4.5. Códigos de retorno devueltos por la interfaz de cifrado

Códigos de retorno y motivos de la gestión de claves EDItran			
Código Retorno		**Motivo (razón)**	
01	Error en parámetros de entrada. (Revise parámetros de paso a la interfaz de claves, en EDItran/P y/o EDItran/G)	01	Código local incorrecto
		02	Código remoto incorrecto
		03	Tipo algoritmo distinto de R (RSA)
		04	No hay asterisco "*" en posición 1 de parámetro
		05	No hay coma "," en posición 2 de parámetro (revise parámetros área de entrada).
		06	No hay subentorno local en posición 3 de parámetro.
		07	No hay coma "," en posición 4 del parámetro
		08	No hay subsistema remoto en posición 5 de parámetro
02	Error de acceso a fichero ZTBPFGC.	Xx	File status en batch Eibresp en CICS.
03	No existe algún registro en fichero ZTBPFGC (propias o ajenas). Nota: (además de que no exista el registro se verifica el contrario para ver si tiene activas).	01	No existe registro de propias. Si existe registro de ajenas activas.
		02	No existe registro de propias. Si existe registro de ajenas, pero están inactivas.
		03	No existe registro de ajenas. Si existe registro de propias activas.
		04	No existe registro de ajenas. Si existe registro de propias, pero están inactivas.
		05	No existe registro de propias. No existe registro de ajenas.
04	Existen los registros en fichero ZTBPFGC (propias o ajenas), pero alguno de ellos (o ambos) no tienen label activa.	01	No existe label activa propia
		02	No existe label activa ajena
		03	No existen label activas ni propias, ni ajenas
99	Errores CICS	97	Error ZTBGB020 en DSNAME ENQ.
		98	Error en ENQ ZTBGB020.
		99	Error al llamar al módulo ZTBP0062

Una vez extraído el label "activo", se consulta su clave asociada (FICHKRSA, FICHKDES ó CKDS) y en caso de error se producen otros códigos-motivos.

Por ejemplo, si en la interfaz **batch** cuando carga, no existe el label (label+versión activa, indicados en fichero ZTBPFGC, de gestión de claves), en el fichero FICHKRSA ó en CKDS se dará un error en carga ó descarga, y displays, por ejemplo:

LOG EDItran/G : ZTG0175: ZTBGBG10: ERROR AL CIFRAR EL FICHERO DE APLICACION
Display en job para DES : ZTBSBD02 : Error en generacion de clave. (retorno 97, razon 59)

Display en job para RSA : ZTBSBR04 : Error en generacion de firma. (retorno 103, razon 16)

Si el mismo caso se produce **en CICS,** ó en la gestión de claves RSA, salen mensajes como los que siguen (motivo 13 = eibresp2 = notfnd):

LOG de EDItran/G :ZTP0197 : ERROR XXXXXX CRIPTOGRAFIA: 97 - **13** (ERRX)
Display de EDItran/GC:PROGRAM:XXXXXXXX ,RETORNO=xxxxxxxx,**RAZON=00000013**

En CICS, PUEDE OCURRIR, que el label proporcionado por la gestión de claves, no sea encontrado en FICHKRSA ó FICHKDES-CKDS, Y REALMENTE EXISTA en dichos ficheros.

El motivo es que en ocasiones, sobre todo cuando hay numerosas grabaciones en los vsam (procesos batch), estos ficheros no son "REFRESCADOS AUTOMATICAMENTE EN CICS", con lo que se puede dar el caso de que el programa no encuentre el label y unos minutos más tarde si.

Se recomienda por tanto para REFRESCAR EL FICHERO en MONITOR DE TELEPROCESO CICS, que cuando se actúe incluyendo claves en dichos ficheros, a continuación, e cierren - abran a CICS.

4.6. Nombre de los ficheros creados por EDItran para el intercambio de claves.

Se forman ficheros con el siguiente nombre:

Nivel	Nombre	Long.	Tipo	Descripción
1	Prefijo	11	Alfn.	Prefijo ficheros especificado en entorno local
1	Punto	01	Alfn.	Valor '.'
1	Tipo-extremo	02	Alfn.	RL (rsa local), para extremo emisor de pública. RR (rsa remota), para extremo emisor de confirm.
1	Punto	01	Alfn.	Valor '.'
1	Nif local-1	08	Alfn.	L + 7 primeros caracteres de nif local.
1	Punto	01	Alfn.	Valor '.'
1	Nif-local-2	03	Alfn.	L + 2 últimos caracteres de nif local.
1	Punto	01	Alfn.	Valor '.'
1	Subsistema	01	Alfn.	Subsistema local para extremo que emite clave Subsistema remoto para extremo que emite confirmación
1	Punto	01	Alfn.	Valor '.'
1	Nif-remoto-1	03	Alfn.	R + 7 primeros caracteres de nif remoto.
1	Punto	01	Alfn.	Valor '.'
1	Nif-remoto-2	03	Alfn.	R + 2 últimos caracteres de nif remoto.
1	Punto	01	Alfn.	Valor '.'
1	Tipo-extremo	02	Alfn.	RL (rsa local), para extremo emisor de pública. RR (rsa remota), para extremo emisor de confirm. .
1	Subsistema	01	Alfn.	Subsistema local para extremo que emite clave Subsistema remoto para extremo que emite confirmación
1	Versión	03	ALFN.	Valor Vxx, donde xx es versión 01-99 Es la versión activa del extremo emisor de la clave

Para RSA, para el extremo que envía su pública al remoto.

Prefijo-ficheros.L-nif-loc-1.L-nif-loc-2.R-nif-rem-1.R-nif-rem-2.RLSubsVxx

Para RSA, para el extremo que confirma haber recibido la pública del remoto.

Prefijo-ficheros.L-nif-loc-1.L-nif-loc-2.R-nif-rem-1.R-nif-rem-2.RRSubsVxx

4.7. Formato del fichero ZTBPFGC.

Contiene los datos necesarios para el control de las claves locales y remotas.

Nivel	Nombre	Long.	Tipo	Descripción
1	Clave acceso	30		Clave de acceso al fichero de claves
2	Tipo Clave	1	Alf.	Indica si la clave es RSA (R) **Indica si es registro de entorno (A), en cuyo caso resto de clave es low-values**
2	Propietario	1	Alf	Indica si la clave es propia o ajena (L/R)
2	Código Local	9	Alf	Código del entorno local de EDItran propietario de las claves locales
2	Subsistema	1	Alf.	Determina la aplicación o aplicaciones en las que se van a utilizar dichas claves en el extremo propietario de las claves.

2	Código Remoto	9	Alf	Código del entorno remoto al cual se le han enviado las claves locales y del cual se han recibido las claves remotas. Low-values para el registro que contiene las claves propias RSA
2	Filler	9	Alfn.	Area reserva
1	**Resto**	482		
1	Area para entorno local redefines **RESTO**	482		
2	EDI requerido	1	Alfn.	S/N Indica si se dispone de EDItran.
2	Prefijo instal fich	11	Alfn.	Siempre es necesario.
2	Filler	8	Alfn.	Area reserva
2	Aplic. Servicio	6	Alfn.	Aplicación EDItran/P de intercambio, si dispone de EDItran.
2	Prefijo label	19	Alfn.	Prefijo para meter labeles, puesto por usuario.
2	Nombre proc	8	Alfn.	Nombre del proc para generar.
2	Filler	8	Alf.	Area reserva
2	Fichas JCL	295	Alfn.	5 fichas jcl de 59.
2	Filler	126	Alf.	Resto registro entorno local
1	Area para reg.propios rsa (sin remoto). redefines **RESTO**	482		
2	Descripción	20	Alf.	Descripción del subsistema.
2	Aplicación servicio	6	Alf.	Aplicación servicio.
2	Nombre administr.	20	Alfn.	Nombre administrador
2	Telef administr.	11	Alfn.	Teléfono administrador
2	Nombre label privada	60/12		Label privada rsa/des sin .VXX. En registros DES ya sean propios como ajenos.
2	Nombre label pública	60/12	Alfn.	Label pública rsa sin .VXX
2		1	Alfn.	FILLER
2	Subsistema loc-rsa	1	Alfn.	Subsistema local rsa
2	Subsistema rem-rsa	1	Alfn.	Subsistema remoto
2	Tabla	93		Datos de las tres últimas claves generadas / recibidas
3	Estado	1	Num.	Indica el estado de la clave 1- Generada 2- Enviada/recibida 3- Operativa 4- Activa 5- Cancelada
3	Versión	2	Num.	Versión de la clave
3	Fecha-Hora Creación	14	Num.	SSAAMMDD-HHMMSS del momento de generación
3	Fecha-Hora ULTIMA MODIFICACION	14	Num.	SSAAMMDD-HHMMSS de la última modificación.
2	Filler	201/ 249	alfn	Area reserva

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