# Gestión de claves ERTMS Nivel 2 en Equipos Embarcados

## GAPI-2406

ER-1372/2010 GA-1999/0142 SST-0257/2010
Ver alcance en aenor.es

# ÍNDICE

## 1. INTRODUCCIÓN

El sistema de protección del tren ERTMS Nivel 2 (en adelante N2) tiene uno de sus pilares fundamentales en la transmisión vía radio a través de la red GSM-R de la información sobre la infraestructura necesaria para que el equipo embarcado pueda supervisar los movimientos del tren de forma continua.

La red GSM-R es una red abierta y por lo tanto se hace imprescindible garantizar la autenticidad e integridad de la información transmitida. Esta funcionalidad se consigue por medios criptográficos: claves simétricas. Estas claves han de manejarse de manera estrictamente confidencial y han de instalarse tanto en los equipos de vía (RBC, Radio Block Centre) como en los equipos embarcados (OBU, On Board Unit).

No es necesaria la confidencialidad de la información de N2, por lo que ésta se transmite en claro y es accesible cuando se monitoriza la red GSM-R.

El proceso de intercambio de información entre un RBC y el equipo embarcado (OBU) de un vehículo comienza con la realización de una llamada por parte de este último al RBC y tras el establecimiento de la llamada, ambas partes inician un procedimiento de autenticación en el que intervienen las claves. Para que un RBC y un OBU puedan establecer una sesión de comunicaciones es imprescindible que ambos compartan una misma clave. Si en alguna de las partes no está instalada o estando en ambas partes instalada no coincide su valor, la sesión de comunicaciones no se establecerá.

## 2. OBJETO

El presente documento tiene por objeto exponer las reglas de gestión de claves N2 de Adif/Adif AV en lo que respecta a la interfaz con las *Unidades Organizativas (UO) que gestionan Material Rodante* que necesiten circular con el sistema de protección ERTMS N2 en alguna de las líneas gestionadas por Adif/Adif AV (tanto en fase de construcción como tras la puesta en servicio).

Este documento corresponde a la parte pública del procedimiento de gestión de claves ERTMS Nivel 2 interno de Adif [Ref. 04].

## 3. ALCANCE, ÁMBITO DE APLICACIÓN

Este documento será de aplicación obligatoria para las siguientes entidades:

- Adif/Adif AV como gestor de Material Rodante dedicado a trabajos en vía y a pruebas.
- Empresas ferroviarias cuyo Material Rodante circule o pretenda circular en N2 en alguna de las líneas gestionadas por Adif/Adif AV (en fase de construcción o tras la puesta en servicio).
- Suministradores de equipos embarcados (OBU) o de Material Rodante.

Lo indicado en este documento es independiente de las características de las líneas (ancho, velocidad, tensión, etc.) en las que se encuentra instalado el RBC, así como de las características del Material Rodante (trenes convencionales, trenes de Alta Velocidad, trenes de trabajos, etc.), por lo que son de aplicación a todas las líneas gestionadas por Adif/Adif AV (en fase de construcción

o tras la puesta en servicio) y a todo el Material Rodante que circule o pretenda circular en N2 por ellas.

Toda *Unidad Organizativa (UO) que gestiona Material Rodante* que participe en el KMS de Adif/Adif AV debe gestionar las claves N2 de acuerdo con este documento.

No se considera la transmisión de claves *online*, aunque se recaba información de las entidades ETCS (RBC, OBU) que sí admiten esta interfaz para posibles mejoras futuras.

## 4. RESPONSABILIDADES

En este apartado se describen las *Unidades Organizativas (UO)* involucradas en la gestión de claves, así como las responsabilidades y funciones principales asociadas a la gestión de claves. Los detalles de cada función se encuentran descritos en el apartado 6 "Descripción del procedimiento externo".

- **Gestor de Claves:**

Es la unidad Organizativa dentro de Adif/Adif AV encargada del Sistema de Gestión de Claves (KMS).

Sus responsabilidades son:

  - Operación del KMC (Key Management Centre).
  - Gestión de la base de datos de claves, registro de RBCs, registro de OBUs y registro de Foreign KMCs.
  - Generación de los ficheros de instalación y de borrado de claves.
  - Distribución de los ficheros de instalación y de borrado de claves.
  - Servir de interfaz entre el KMS y el resto de las Unidades Organizativas.

Toda comunicación con el Gestor de Claves se realizará a través de la dirección de correo electrónico: KMC_administrator@adif.es.

La denominación dentro de este documento es: ***UO Gestor de Claves.***

- **Unidades Organizativas que gestionan los RBC:**

Son los departamentos dentro de Adif/Adif AV (o entidades colaboradoras con las que haya establecida una relación contractual que regula dicho marco a todos los efectos) que gestionan los RBC (en fase de construcción o tras la puesta en servicio).

Serán los encargados, entre otras tareas, de recibir los ficheros de instalación/borrado de claves suministrados por parte de la ***UO Gestor de Claves*** y de instalar/borrar las claves en los RBC.

Sus responsabilidades son:

  - Solicitud de alta/ modificación/ baja de usuario.
  - Solicitud de alta/ modificación/ baja de RBC en el KMS.
  - Solicitud de generación de fichero de instalación de clave KTRANS para el RBC.

- Instalación/ borrado de clave KTRANS en el RBC.
- Solicitud de Material Rodante para pruebas (en el caso de pruebas de la infraestructura).
- Instalación/ borrado de claves KMAC en el RBC.
- Solicitud de generación de ficheros de borrado de claves KMAC.
- Envío de ficheros de confirmación.

La denominación dentro de este documento es: ***UO que gestiona el RBC.***

- **Material Rodante de Adif/Adif AV:**

Son los departamentos dentro de Adif/Adif AV que gestionan el Material Rodante equipado con el sistema ERTMS N2. Este Material Rodante de Adif/Adif AV está dedicado a trabajos en vía y algunos vehículos dedicados a pruebas de diferentes tipos: geometría de vía, catenaria, etc.

Este Material Rodante pertenecerá siempre al KMC de Adif/Adif AV.

Sus responsabilidades son:

- Solicitud de alta/ modificación/ baja de usuario.
- Solicitud de alta/ modificación/ baja de OBU en el KMS.
- Solicitud de generación de fichero de instalación de clave KTRANS para el OBU.
- Instalación/ borrado de clave KTRANS en el OBU.
- Solicitud de generación de ficheros de instalación/ borrado de claves KMAC.
- Solicitud de instalación/ borrado de claves KMAC en el RBC.
- Instalación/ borrado de claves KMAC en el OBU.
- Envío de ficheros de confirmación.

La denominación dentro de este documento es: ***UO Material Rodante Adif/Adif AV.***

Podrá referirse a esta ***UO*** cuando en la descripción de las fases del proceso se indique ***UO que gestiona Material Rodante.***

- **Empresas Ferroviarias:**

Son las entidades que gestionan flotas ferroviarias con fines comerciales, tanto de viajeros como de mercancías. Son la Unidad Organizativa que típicamente inicia el proceso de petición de claves para operar comercialmente un Material Rodante en N2 en una línea determinada (aunque pueden existir otros agentes causales).

Este Material Rodante podrá pertenecer al KMC de Adif/Adif AV o tener su propio KMC (Foreign KMC).

Sus responsabilidades son:

- Solicitud de alta/ modificación/ baja de usuario.

- Solicitud de alta/ modificación/ baja del KMC de la EF (en caso de que la EF tuviera su propio KMC).
- Solicitud de generación/ intercambio de fichero de clave K-KMC (en caso de que la EF tuviera su propio KMC).
- Instalación de clave K-KMC en su propio KMC (en caso de que la EF tuviera su propio KMC).
- Solicitud de alta/ modificación/ baja de OBU en el KMS.
- Solicitud de generación de fichero de instalación de clave KTRANS para el OBU (en caso de que el Material Rodante perteneciera al KMC de Adif/Adif AV).
- Instalación/ borrado de clave KTRANS en el OBU.
- Solicitud de generación de ficheros de instalación/ borrado de claves KMAC.
- Solicitud de instalación/ borrado de claves KMAC en el RBC.
- Instalación/ borrado de claves KMAC en el OBU.
- Envío de ficheros de confirmación.

La denominación dentro de este documento es: ***UO Empresa Ferroviaria.***

Podrá referirse a esta ***UO*** cuando en la descripción de las fases del proceso se indique ***UO que gestiona Material Rodante.***

- **Suministrador de Equipos Embarcados o de Material Rodante:**

Son las empresas tecnológicas ferroviarias que, en ciertas fases del desarrollo de sus productos, necesitan realizar pruebas en N2. Dentro de este documento se refieren a los fabricantes de OBU o a los fabricantes de Material Rodante.

El suministrador del OBU/Material Rodante no participará directamente en el procedimiento de gestión de claves, estando la relación con Adif/Adif AV siempre regulada dentro de un marco contractual.

Sus responsabilidades son las mismas a las indicadas anteriormente para la ***UO Empresa Ferroviaria.***

La denominación dentro de este documento es: ***UO Suministrador OBU.***

Podrá referirse a esta ***UO*** cuando en la descripción de las fases del proceso se indique ***UO que gestiona Material Rodante.***

## 5. DEFINICIONES

- **Descripción general del KMS**

Antes de establecer una sesión ERTMS N2, el equipo de vía, RBC, y el equipo embarcado, OBU, intercambian cierta información utilizando el protocolo EURORADIO [Ref. 01], con el fin de asegurar la comunicación a través del medio utilizado, que es un medio abierto y no seguro. Se comprueban las identidades del RBC y del OBU mutuamente mediante el uso de claves criptográficas.

Los protocolos utilizados en la comunicación entre el RBC y el OBU generan una clave de sesión que se utiliza para verificar la integridad de los mensajes intercambiados en dicha sesión. La clave de sesión se genera a partir de las claves KMAC correspondientes a la pareja RBC-OBU, que se encuentran almacenadas en los mismos.

El sistema KMS (Key Management System), dedicado en exclusiva a las comunicaciones ERTMS N2, genera y gestiona las claves necesarias para cumplir estos cometidos.

El KMS gestiona las siguientes claves:

- KMAC: Clave de autenticación entre entidades ETCS (RBC, OBU).
- KTRANS: Clave de encriptación utilizada en la transmisión de información relativa a las claves entre el KMC (Key Management Centre, plataforma de gestión de claves) y las entidades ETCS (RBC, OBU).
- K-KMC: Clave de encriptación utilizada en la transmisión de información relativa a las claves entre distintos KMCs, en caso de realizarse comunicación entre varias plataformas KMC (nacionales o internacionales).

Las claves KMAC tienen un período de validez determinado. Una vez superada la fecha de caducidad de una clave, si ésta no se renueva, no se logrará la comunicación entre entidades ETCS (RBC, OBU).

En virtud del Convenio de Encomienda ADIF-Alta Velocidad – ADIF, de fecha 31 de enero de 2014, queda encomendada a ADIF la realización de determinadas tareas en la red titularidad de ADIF-Alta Velocidad (en adelante, Adif AV), entre las que figuran servicios Gestión Integral del Mantenimiento, entre los que se encuentra la gestión de claves.

- **Dominio de Gestión del Claves**

Se define el concepto de "Dominio" como el conjunto formado por un KMC y las entidades ETCS (RBC, OBU) que utilizan dicho KMC como centro gestor de sus claves [Ref. 02]. En el caso particular de Adif/Adif AV, el Dominio ADIF está compuesto inicialmente por:

- El KMC de Adif.
- Los RBC de todas las líneas de la RFIG en las que se encuentra instalado el sistema ERTMS N2 y los RBC gestionados por Adif/Adif AV que estén en fase de pruebas.
- Todos los OBU de Material Rodante perteneciente a Adif/Adif AV.

Adicionalmente, y de manera opcional, podrán estar incluidos dentro del dominio de Adif/Adif AV todos los OBU cuya interfaz de carga de claves sea compatible con el definido en [Ref. 03], previo acuerdo sobre los términos de esta inclusión.

La figura 1 esquematiza un *KM Domain* con sus relaciones internas junto con las de otros *KM domain*.

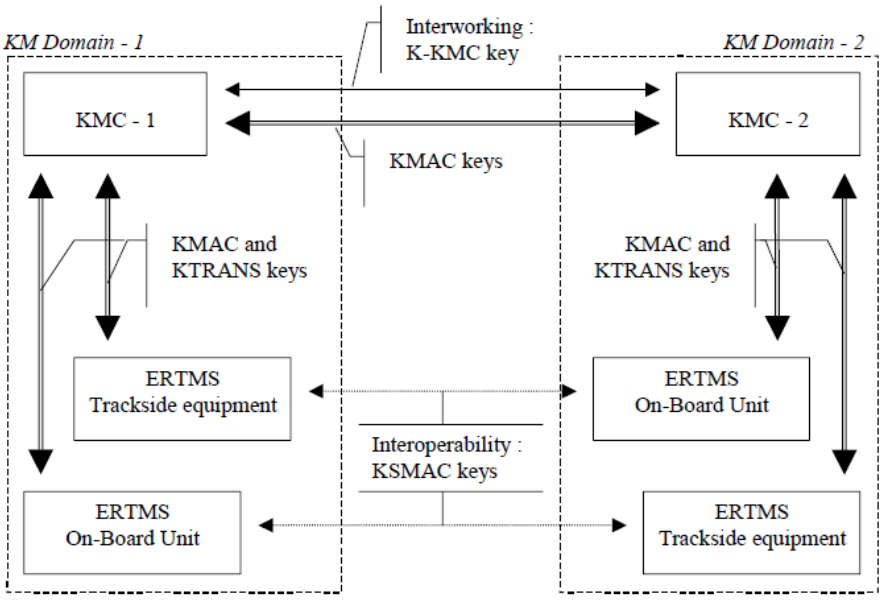



Figura 1. Relación entre diferentes dominios KM
Fuente: Subset-038 [Ref. 02].

Las siguientes entidades estarán obligatoriamente fuera del dominio Adif/Adif AV:

- Los RBC de líneas no pertenecientes a la RFIG (excepto aquéllos en fase de pruebas que en un futuro pertenecerán a la RFIG).
- Los OBU cuya interfaz de carga de claves no sea compatible con el proporcionado en el dominio Adif/Adif AV [Ref. 03].

En este caso, la transmisión de claves entre dominios se realizará utilizando una interfaz que cumpla el Subset-038 [Ref. 02].

La estructura del identificador ETCS del KMC está descrita en la tabla 24 del Subset-037 [Ref. 01]:

| ETCS ID | Range of values<br>Octet1 Octet2 Octet3<br>8765 4321 8765 4321 8765 4321 | Description |
|---|---|---|
| ETCS ID of KM entity | cccc cccc cckk kkkk kkkk kkkk | c...c Country or region ID<br>k...k Key management entity ID |

Se ha escogido para el KMC de Adif el *NID_C* 352 (el asignado a la línea L050 [Madrid-Lleida]) y el *Key Management Entity* ID = 0.

De la concatenación de estos dos valores resulta el ETCS ID del KMC de Adif:

352d = 0101 1000 00b

0d = 00 0000 0000 0000b

ETCS_ID = 0101 1000 0000 0000 0000 0000 b = 5767168d = 0x580000

Todos los valores de NID_C son asignados por la ERA a los diferentes Administradores de Infraestructuras. En el caso de que una alguna entidad (EF, fabricante de Material Rodante, suministrador de OBU, etc.) necesite operar uno o varios KMC(s) propio(s), si tiene la intención de usar un NID_C asignado a España, deberá coordinarse con Adif/Adif AV, con el fin de no duplicar identidades. El resto de las entidades podrán dirigirse al AI que consideren más conveniente.

- **Definiciones y Acrónimos**

**ADIF**: Administrador de Infraestructuras Ferroviarias.

**AESF:** Agencia Estatal de Seguridad Ferroviaria.

**AI:** Administrador de Infraestructura.

**APM:** Autorización de Puesta en el Mercado.

**CA:** Condición de Aplicación.

**CCR:** Certificado de Compatibilidad del tren con la Ruta.

**CU:** Condición de Uso.

**CVM:** Cuadro de Velocidades Máximas.

**EF:** Empresa Ferroviaria.

**ERA (European Railway Agency):** Agencia Ferroviaria Europea, actualmente EUAR (European Union Agency for Railways).

**ERTMS**: European Rail Traffic Management System.

**ETCS:** European Train Control System.

**Foreign KMC:** KMC externo.

**GSM-R**: Sistema Global de Comunicaciones Móviles ferroviario de ERTMS.

**K-KMC**: Key inter KMCs (Clave entre KMCs).

**KDC:** Key Distribution Centre: Plataforma de carga de claves en el RBC cuando ésta es un ordenador de mantenimiento o un dispositivo de acceso a red. La principal función de un KDC es distribuir datos criptográficos a las entidades ETCS e implementar una interfaz definido con el KMC. Por lo tanto, el KDC puede cumplir las funciones de interfaz con el KMC en representación de la entidad ETCS.

**KMAC (Message Origin Authentication Key):** Clave de autenticación de origen de mensaje.

**KMC (Key Management Centre):** Centro de Gestión de Claves.

**KMS (Key Management System):** Sistema de Gestión de Claves.

**KTRANS (Transport Key):** Clave de Transporte.

**MR:** Material Rodante.

**N2:** ERTMS Nivel 2.

**OBU (On Board Unit):** Equipo ERTMS Embarcado.

**RBC (Radio Block Centre):** Centro de Control por Radio.

**RCF:** Reglamento de Circulación Ferroviaria.

**RFIG:** Red Ferroviaria de Interés General.

**RS:** Restricciones de Servicio

**RT:** Restricciones Técnicas

**UO (Unidad Organizativa):** Dirección, Subdirección, Jefatura de Área, departamento o Entidad dentro de una Organización que es responsable de una función específica.

## 6. DESCRIPCIÓN DEL PROCEDIMIENTO EXTERNO

Para la correcta interpretación de los diferentes procedimientos descritos es necesario tener en cuenta el proceso general de gestión de claves:

1. Generación de la clave de transporte (KTRANS) para el RBC.
2. Instalación de la KTRANS en el RBC.
3. Generación de la clave de transporte (KTRANS) para el OBU.
4. Instalación de la KTRANS en el OBU.
5. Generación del fichero de instalación de clave de autenticación (KMAC) [clave compartida entre RBC y OBU, fichero distinto para cada entidad ETCS].
6. Instalación de la KMAC en el RBC.
7. Instalación de la KMAC en el OBU.

A partir del paso 7 ya es posible establecer la sesión de comunicaciones en N2.

En el caso del borrado de claves KMAC, los pasos serían los siguientes:

1. Generación del fichero de borrado de clave de autenticación (KMAC) [fichero distinto para cada entidad ETCS (este fichero no contiene ninguna clave)]
2. Borrado de la KMAC en el RBC.
3. Borrado de la KMAC en el OBU.

Se ha de tener siempre en cuenta que para la instalación o borrado de una clave KMAC en cualquier entidad ETCS es condición necesaria que en dicha entidad esté instalada la clave de transporte (KTRANS).

Los procedimientos de gestión de claves se pueden dividir en **tres grupos**:

1. Procedimientos de **registro** de una entidad ETCS (RBC o OBU) y/o de **registro** de un Foreign KMC en el KMS; y los procedimientos asociados de solicitud, generación, distribución e instalación de **claves KTRANS** o de **claves K-KMC**.

2. Procedimientos de solicitud, generación, distribución e instalación de ficheros de **instalación de claves KMAC**.

3. Procedimientos de solicitud, generación, distribución e instalación de ficheros de **borrado de claves KMAC**.

Estos procedimientos presentan ligeras diferencias dependiendo del **Escenario** en el que se realicen. Se han definido 14 Escenarios desde el punto de vista de la infraestructura y 4 Escenarios desde el punto de vista del equipo embarcado.

El Escenario a aplicar es diferente dependiendo de si la línea pertenece o no a la RFIG, de si el ERTMS N2 está en servicio comercial, si el ERTMS N2 es de nueva construcción o si se trata de una modificación del ERTMS N2 en servicio, de la fase del proyecto de ERTMS N2 de vía en que se encuentre (construcción, fase de pruebas ERTMS, fase de puesta a disposición para fiabilidad, puesta en servicio, etc.), de si el OBU está o no bajo el KMS de Adif/Adif AV y de cuál es el origen de la motivación de cada solicitud de claves (pruebas de la infraestructura, pruebas del Material Rodante, entrada en servicio comercial de un Material Rodante en un tramo, etc.).

La *UO que gestiona el RBC* identificará cuál es el Escenario que le aplica para la gestión de claves (Escenario 1 a Escenario 14):

- dependiendo de si la línea pertenece o no a la RFIG,
- dependiendo de si el ERTMS N2 está en servicio comercial, si es de nueva construcción o si la actuación se trata de una modificación del ERTMS N2 en servicio y
- dependiendo de la fase del proyecto de ERTMS N2 de vía en la que se encuentre

y aplicará los procedimientos correspondientes a ese Escenario.

Los Escenarios desde el punto de vista de la infraestructura (Escenarios del 1 al 14) están recogidos en el procedimiento de gestión de claves ERTMS Nivel 2 interno de Adif [Ref. 04] y no forman parte de este documento.

La *UO que gestiona el Material Rodante* se regirá por este documento que regula su participación en relación con la gestión de claves N2. Los Escenarios que le pueden aplicar son del 15 al 18:

- dependiendo de si el OBU está bajo el KMS de Adif/Adif AV o no y
- dependiendo del origen de la motivación de la solicitud de claves.

A lo largo de todo el documento se utiliza el concepto "línea" en su acepción más general (tal y como se recoge en el RCF):

> "infraestructura ferroviaria que une dos puntos determinados"

En este sentido "línea" puede indicar tanto una línea tal y como se reflejan en el CVM o tramos de una línea.

Se hace notar que el ámbito de control de un RBC puede abarcar una línea, un tramo de línea, o varias líneas (o tramos de línea) diferentes.

En la Tabla 1 se indica la Unidad Organizativa responsable de iniciar cada actividad de cada proceso en cada uno de los Escenarios desde el punto de vista del equipo embarcado.

| | | OBU BAJO EL KMS DE ADIF/ADIF AV | | OBU PERTENECE A FOREIGN KMC (KMC EXTERNO) | |
|---|---|---|---|---|---|
| | **Motivación de la solicitud de claves** | Por interés del Material Rodante(1) | Por pruebas de la infraestructura(2) | Por interés del Material Rodante(1) | Por pruebas de la infraestructura(2) |
| | **Escenarios** | **Escenario 15** | **Escenario 16** | **Escenario 17** | **Escenario 18** |
| **REGISTRO OBU Y CLAVE KTRANS OBU Y CLAVE K-KMC** | **Solicitud alta/ modificación/baja usuario** | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR |
| | **Solicitud alta/ modificación/baja OBU** | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR |
| | **Solicitud generación clave KTRANS para OBU** | UO que gestiona MR | UO que gestiona MR | - | - |
| | **Instalación/borrado clave KTRANS en OBU** | UO que gestiona MR | UO que gestiona MR | - | - |
| | **Solicitud alta/modif./baja Foreign KMC** | - | - | UO que gestiona MR | UO que gestiona MR |
| | **Solicitud clave K-KMC** | - | - | UO que gestiona MR | UO que gestiona MR |
| | **Instalación clave K-KMC en KMC externo** | - | - | UO que gestiona MR | UO que gestiona MR |
| **INSTALACION CLAVES KMAC** | **Solicitud vehículo pruebas con claves KMAC** | - | UO que gestiona el RBC | - | UO que gestiona el RBC |
| | **Solicitud generación claves KMAC** | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR |
| | **Solicitud instalación claves KMAC en RBC** | UO que gestiona MR | - | UO que gestiona MR | - |
| | **Instalación claves KMAC en RBC** | UO que gestiona el RBC | UO que gestiona el RBC | UO que gestiona el RBC | UO que gestiona el RBC |
| | **Instalación claves KMAC en OBU** | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR |
| **BORRADO CLAVES KMAC** | **Solicitud ficheros borrado claves KMAC** | UO que gestiona MR | UO que gestiona MR o UO que gestiona el RBC | UO que gestiona MR | UO que gestiona MR o UO que gestiona el RBC |
| | **Solicitud borrado claves KMAC en RBC** | UO que gestiona MR | - | UO que gestiona MR | - |
| | **Borrado claves KMAC en RBC** | UO que gestiona el RBC | UO que gestiona el RBC | UO que gestiona el RBC | UO que gestiona el RBC |
| | **Borrado claves KMAC en OBU** | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR | UO que gestiona MR |
| | **Procedimientos de Gestión de claves** | E15.1, E15.2_EEFF y E15.3_EEFF | E16.1, E16.2 y E16.3 | E17.1, E17.2 y E17.3 | E18.1, E18.2 y E18.3 |

**Tabla 1.** Escenarios desde el punto de vista del equipo embarcado y UO responsable de cada actividad.

(1) Material Rodante: en pruebas, obtención CCR, formación maquinistas, pruebas por modificación de equipo embarcado, pruebas por ampliación área de uso, fiabilidad, entrada en servicio comercial, etc.

(2) Si bien la tabla es desde el punto de vista del equipo embarcado, se incluyen estos Escenarios, a pesar de corresponder a la infraestructura, para trazar su relación con la gestión a realizar por parte del Material Rodante.

### 6.1.- LÍNEA NO PERTENECE A LA RFIG

Los Escenarios desde el punto de vista de la infraestructura están recogidos en el procedimiento de gestión de claves ERTMS Nivel 2 interno de Adif [Ref. 04] y no forman parte de este documento.

### 6.2.- LÍNEA PERTENECE A LA RFIG

Los Escenarios desde el punto de vista de la infraestructura están recogidos en el procedimiento de gestión de claves ERTMS Nivel 2 interno de Adif [Ref. 04] y no forman parte de este documento.

### 6.3.- EQUIPOS EMBARCADOS

#### 6.3.1.- OBU BAJO KMS DE ADIF/ADIF AV

Estos Escenarios (15 y 16) aplican en el caso de que el equipo embarcado del tren se encuentre dentro del dominio de gestión de claves de Adif/Adif AV (ver apartado 5).

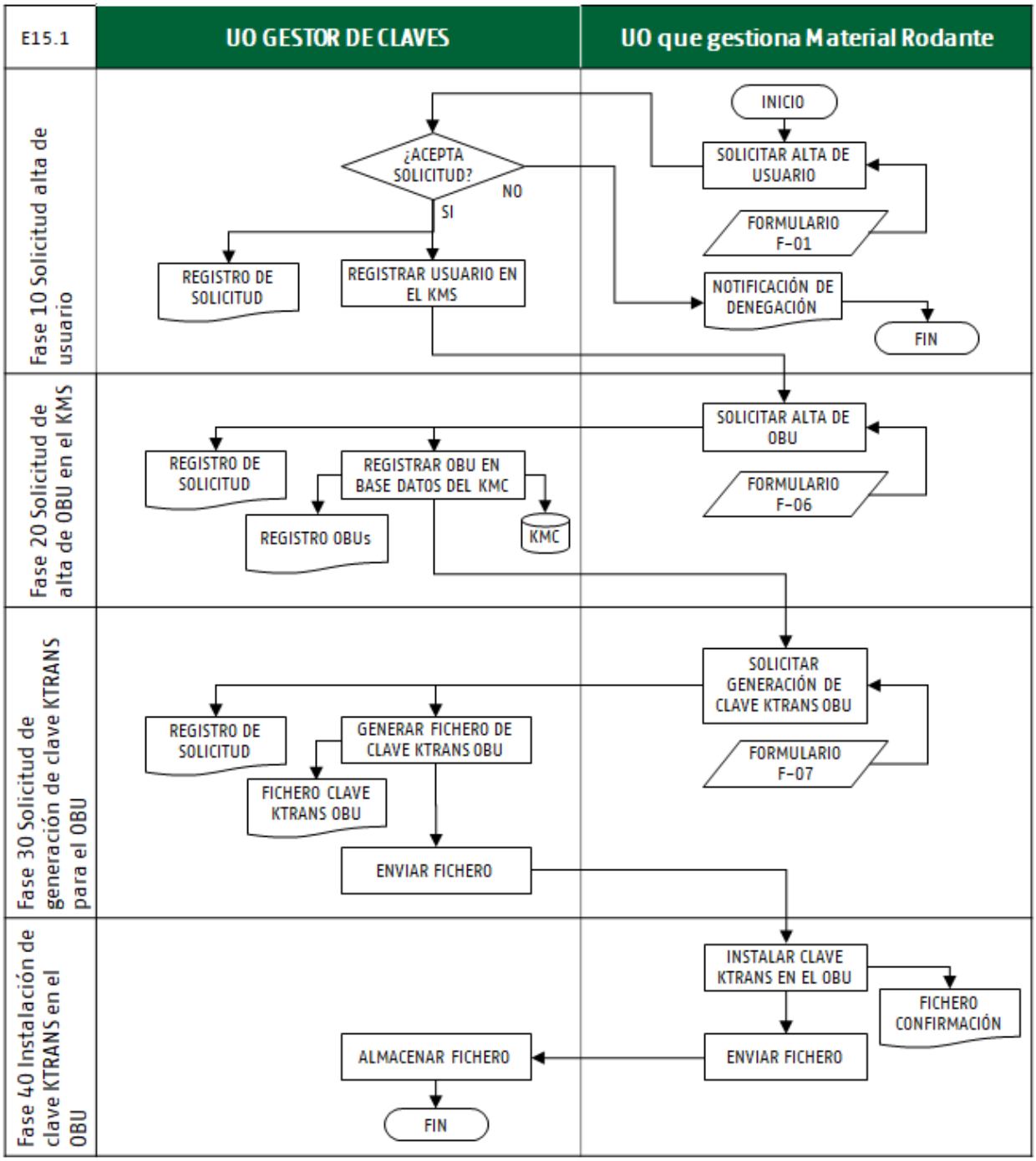
En estos Escenarios, la ***UO que gestiona el Material Rodante***, para poder obtener las claves que permiten el establecimiento de la sesión de comunicación entre el OBU y el/los RBCs en ERTMS N2, debe solicitar, previamente, el alta de un usuario en el KMS, solicitar el alta del OBU en el KMS y solicitar la generación de la clave KTRANS para el OBU, así como instalarla en el OBU.

### 6.3.1.1.- ESCENARIO 15: Pruebas de Material Rodante, CCR, Formación, Servicio Comercial

La *UO que gestiona el Material Rodante* deberá solicitar tanto la generación de ficheros de instalación/borrado de claves KMAC como solicitar su instalación/borrado efectivos en el RBC.

#### 6.3.1.1.1.- PROCEDIMIENTO E15.1: Solicitud de generación e instalación de KTRANS para OBU

##### *6.3.1.1.1.1.- Diagrama de flujo*



### *6.3.1.1.1.2.- Descripción de las fases del procedimiento*

**FASE 10 Solicitud de alta de usuario**

Toda persona física asociada a una ***UO que gestiona Material Rodante*** que desee formar parte del KMS, deberá de darse de alta suministrando la información según el formato *ADIF-PE-301-001-IS-05-F-01* para establecer con ella un canal de comunicación apropiado.

El solicitante remitirá toda la información a la ***UO Gestor de Claves.***

La ***UO Gestor de Claves*** responderá a la solicitud de inclusión en el KMS en el plazo de 30 días hábiles.

En caso de denegarse la solicitud, se argumentará convenientemente al solicitante las razones de dicha denegación.

La solicitud de alta se realizará una única vez por cada usuario del KMS.

En el resto de este procedimiento se entenderá que las comunicaciones con la ***UO que gestiona el Material Rodante*** se realizan con un usuario debidamente acreditado dentro del KMS.

**FASE 20 Solicitud de alta de OBU en el KMS**

La ***UO que gestiona el Material Rodante***, a través de un usuario debidamente acreditado dentro del KMS, solicitará la inclusión del OBU dentro del KMS.

El solicitante recopilará la información contenida en el formato *ADIF-PE-301-001-IS-05-F-06* y la enviará a la ***UO Gestor de Claves***.

Adicionalmente, el solicitante deberá enviar a la ***UO Gestor de Claves*** toda la información relativa a las herramientas de carga de claves utilizadas por el OBU para su estudio y evaluación de posibles problemas de compatibilidad.

La ***UO Gestor de Claves*** introducirá la información de un nuevo OBU en el KMS y actualizará el registro de OBUs.

**FASE 30 Solicitud de generación de clave KTRANS para el OBU**

La ***UO que gestiona el Material Rodante***, a través de un usuario debidamente acreditado dentro del KMS, solicitará la generación de la clave KTRANS para un OBU enviando a la ***UO Gestor de Claves*** la información contenida en el formato *ADIF-PE-301-001-IS-05-F-07*.

La ***UO Gestor de Claves*** enviará la clave KTRANS a la ***UO que gestiona el Material Rodante.***

La clave KTRANS se considera provisional en el caso de que el Material Rodante no cuente aún con la autorización de puesta en el mercado (APM) para circular en ERTMS N2 en algún tramo de la RFIG. En el momento en el que el Material Rodante cuente con la APM para circular con ERTMS N2 en algún tramo de la RFIG la ***UO*** que lo gestiona debe solicitar la generación de la clave KTRANS definitiva a la ***UO Gestor de Claves***.

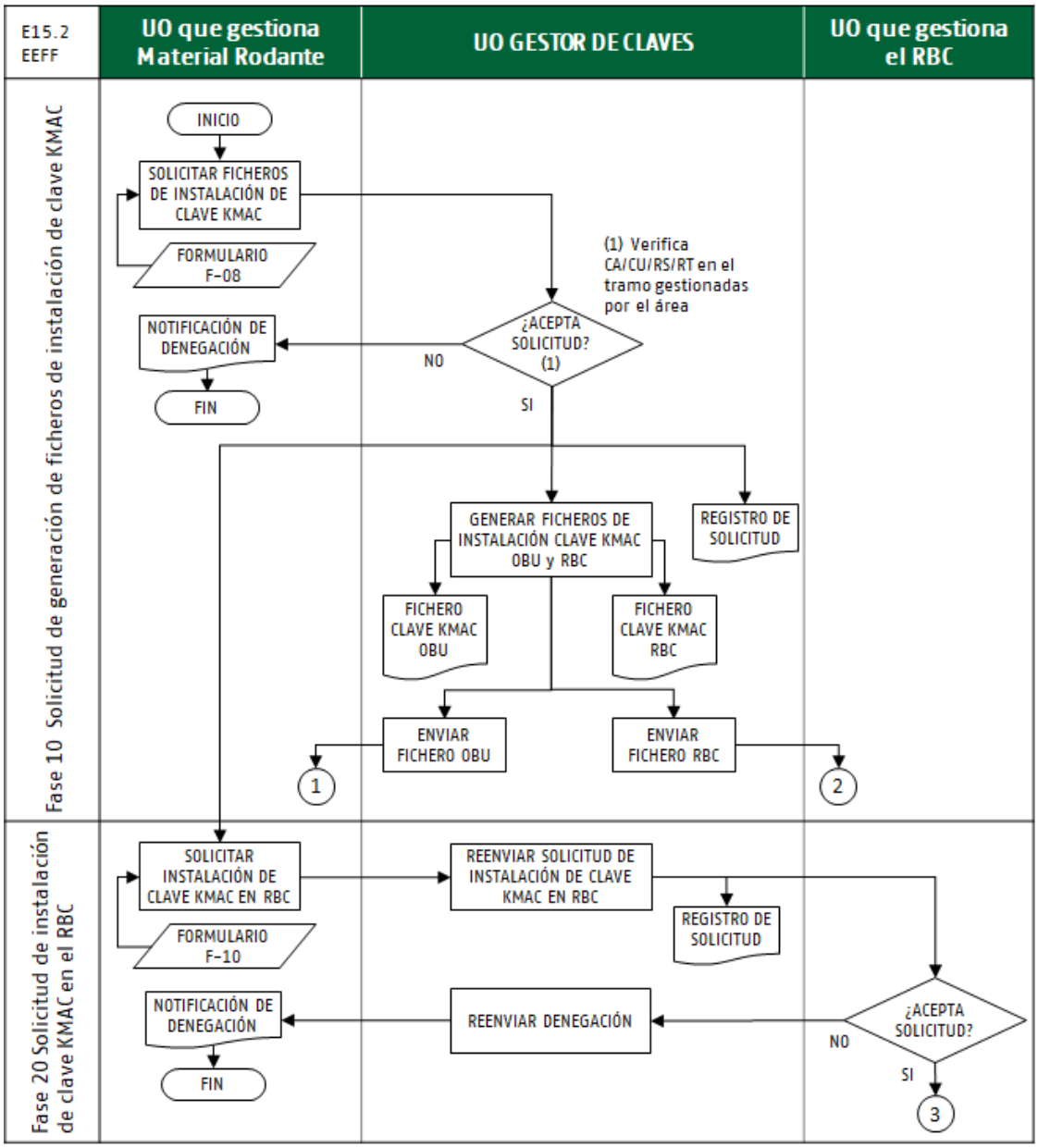
**FASE 40 Instalación de clave KTRANS en el OBU**

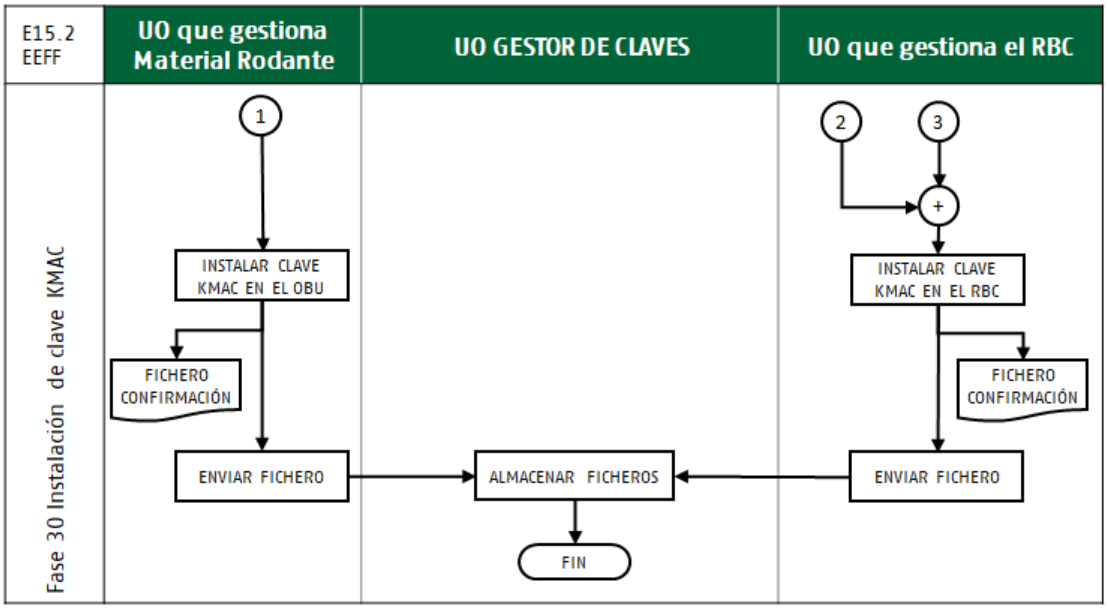
La mera posesión del fichero de instalación de KTRANS es condición suficiente para que la ***UO que gestiona el Material Rodante*** realice u ordene la instalación de clave según la Guía de Carga de Claves del tecnólogo del OBU correspondiente en el momento que estime más oportuno.

La ***UO que gestiona el Material Rodante*** enviará el fichero de confirmación de la instalación de la clave KTRANS en el OBU a la ***UO Gestor de claves*** y/o notificará la fecha de la instalación efectiva de la clave.

### 6.3.1.1.2.- PROCEDIMIENTO E15.2_EEFF: Solicitud de generación e instalación de clave KMAC

#### *6.3.1.1.2.1.- Diagrama de flujo*






### *6.3.1.1.2.2.- Descripción de las fases del procedimiento*

**FASE 10 Solicitud de generación de ficheros de instalación de clave KMAC**

La ***UO que gestiona el Material Rodante*** solicitará la generación de la clave KMAC suministrando a la ***UO Gestor de Claves*** la información según el formato *ADIF-PE-301-001-IS-05-F-08* con una antelación de al menos 30 días.

La ***UO Gestor de claves*** podrá denegar la solicitud informando de ello al solicitante.

La ***UO Gestor de Claves*** se encargará de generar, custodiar y distribuir los ficheros de instalación de clave KMAC tanto a la ***UO que gestiona el RBC*** como a la ***UO que gestiona el Material Rodante*** (para el OBU).

**FASE 20 Solicitud de instalación de clave KMAC en el RBC**

La ***UO que gestiona el Material Rodante*** solicitará la instalación de la clave KMAC en el RBC suministrando a la ***UO Gestor de Claves*** la información según el formato *ADIF-PE-301-001-IS-05-F-10.*

La ***UO Gestor de Claves*** reenviará a la ***UO que gestiona el RBC*** la solicitud de instalación de clave KMAC en el RBC.

La ***UO que gestiona el RBC*** revisará la solicitud de instalación y en el caso de que no pueda llevarla a cabo por alguna circunstancia, denegará la solicitud informando de ello a la ***UO Gestor de claves*** y éste a su vez al solicitante.

**FASE 30 Instalación de clave KMAC**

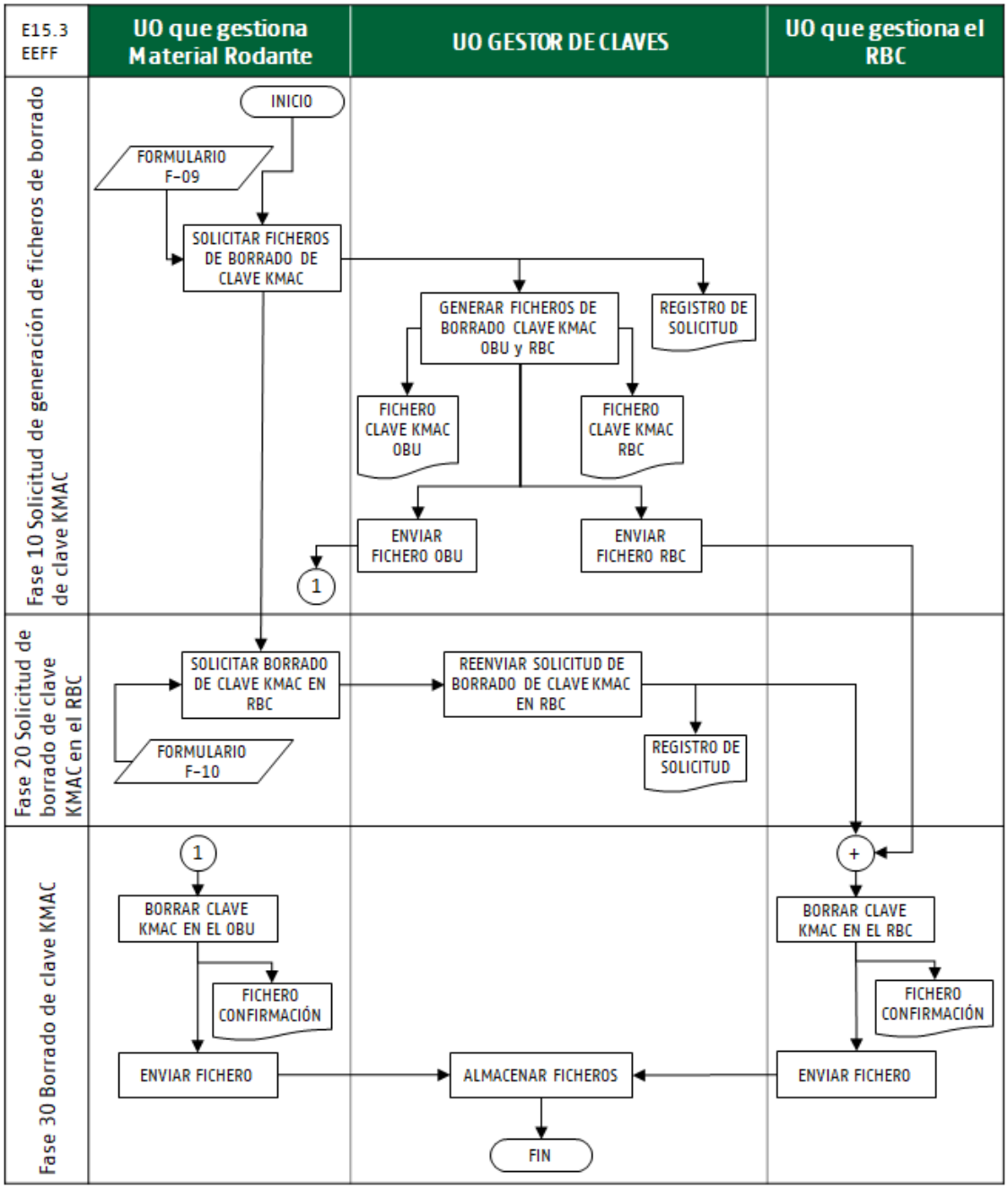
La ***UO que gestiona el RBC***, tras aceptar la solicitud de instalación de la clave KMAC y comprobar que dispone del fichero de instalación, se encargará de instalar el fichero de clave KMAC en el RBC

(a partir de la fecha indicada en la solicitud) y de enviar el fichero de confirmación a la *UO Gestor de Claves*.

La *UO que gestiona el Material Rodante* se encargará de instalar el fichero de clave KMAC en el OBU y de enviar el fichero de confirmación a la *UO Gestor de Claves.*

### 6.3.1.1.3.- PROCEDIMIENTO E15.3_EEFF: Solicitud de generación de ficheros de borrado y borrado de clave KMAC

#### *6.3.1.1.3.1.- Diagrama de flujo*



### *6.3.1.1.3.2.- Descripción de las fases del procedimiento*

**FASE 10 Solicitud de generación de ficheros de borrado de clave KMAC**

La ***UO que gestiona el Material Rodante*** podrá solicitar a la ***UO Gestor de Claves*** la generación de los ficheros de borrado de clave KMAC suministrando la información según el formato *ADIF-PE-301-001-IS-05-F-09*.

La ***UO Gestor de Claves*** se encargará de generar, custodiar y distribuir los ficheros de borrado de clave KMAC tanto a la ***UO que gestiona el RBC*** como a la ***UO que gestiona el Material Rodante*** (para el OBU).

**FASE 20 Solicitud de borrado de clave KMAC en el RBC**

La ***UO que gestiona el Material Rodante*** solicitará el borrado efectivo de la clave KMAC en el RBC suministrando a la ***UO Gestor de Claves*** la información según el formato *ADIF-PE-301-001-IS-05-F-10* indicando la razón por la que solicita el borrado (finalización de pruebas, finalización de servicio comercial, etc.).

La ***UO Gestor de Claves*** reenviará a la ***UO que gestiona el RBC*** que corresponda la solicitud de borrado de clave KMAC en el RBC.

**FASE 30 Borrado de clave KMAC**

La ***UO que gestiona el RBC*** se encargará de borrar la clave KMAC en el RBC y de enviar el fichero de confirmación a la ***UO Gestor de Claves***.

La ***UO que gestiona el Material Rodante*** se encargará de borrar la clave KMAC en el OBU y de enviar el fichero de confirmación a la ***UO Gestor de Claves***.

La ***UO Gestor de Claves*** se encargará de informar a la ***UO que gestiona el Material Rodante*** de que la clave KMAC ha sido borrada del RBC.

### 6.3.1.2.- ESCENARIO 16: Pruebas de infraestructura

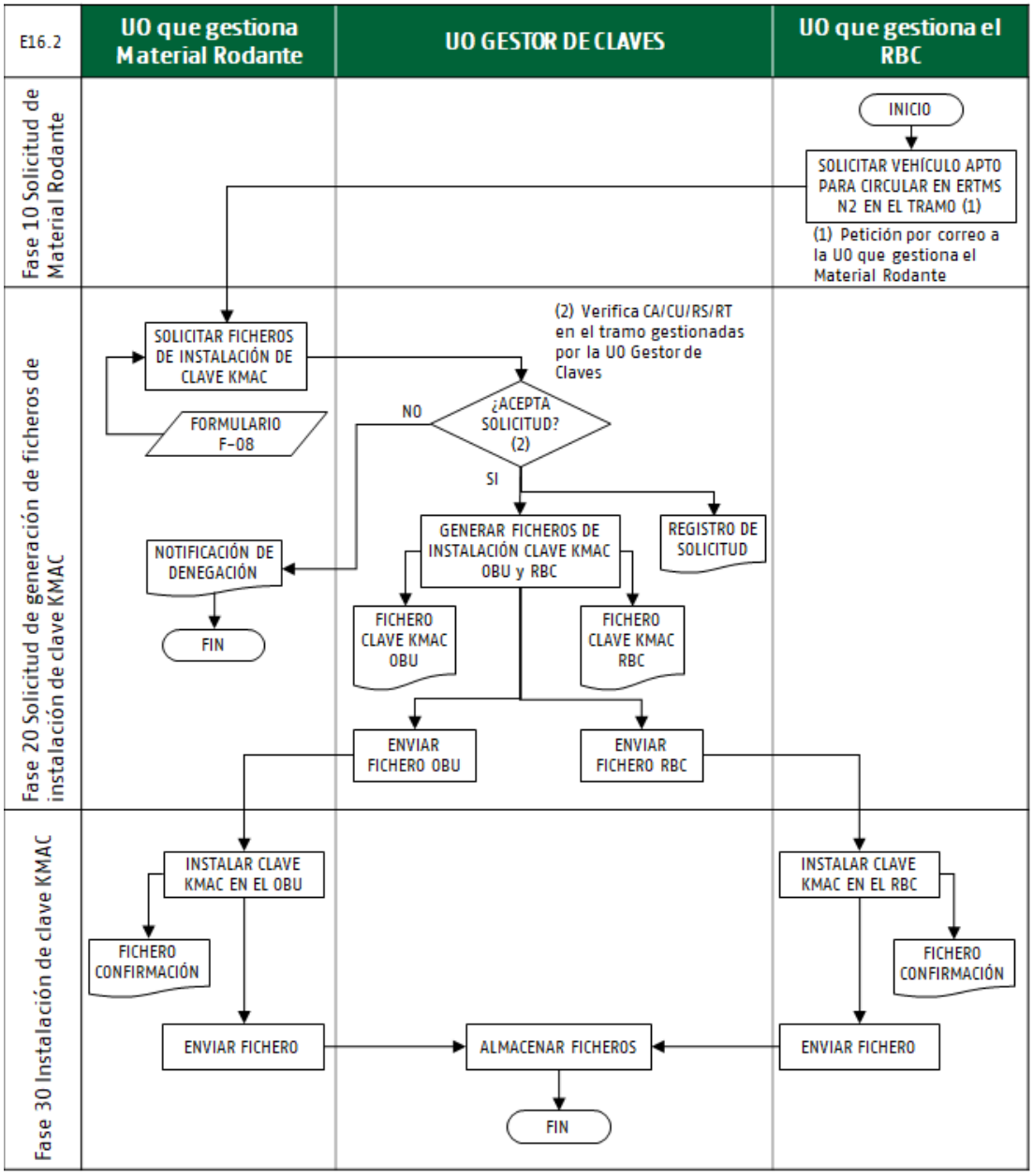
#### 6.3.1.2.1.- PROCEDIMIENTO E16.1: Solicitud de generación e instalación de KTRANS para OBU

Este procedimiento es idéntico al Procedimiento E15.1.

Normalmente las pruebas de la infraestructura se realizan con un vehículo que ya dispone de APM en algún tramo con ERTMS N2, por lo que en ese caso, solo aplicaría la Fase 10 Solicitud de alta de usuario del procedimiento.

#### 6.3.1.2.2.- PROCEDIMIENTO E16.2: Solicitud de generación e instalación de clave KMAC

##### *6.3.1.2.2.1.- Diagrama de flujo*



#### *6.3.1.2.2.2.- Descripción de las fases del procedimiento*

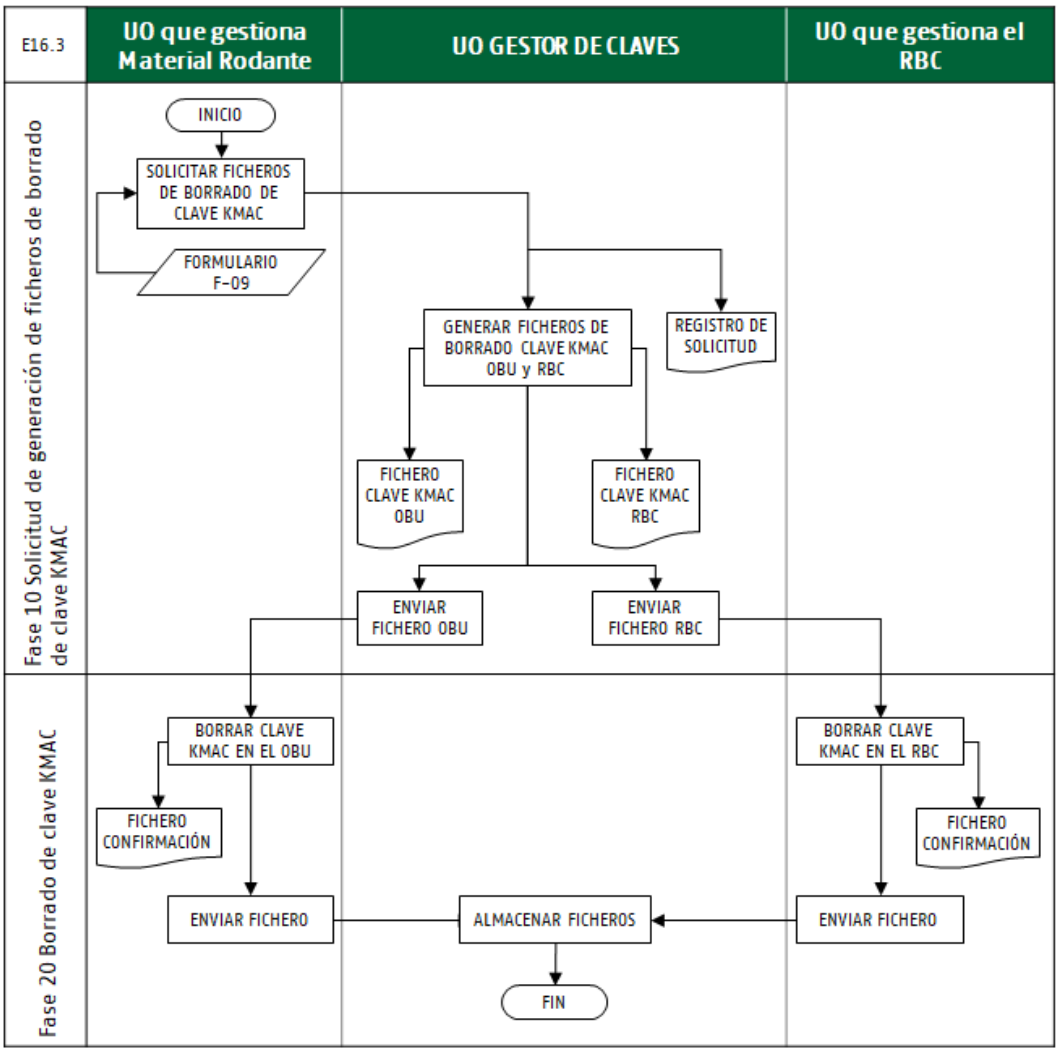
Una vez que la ***UO que gestiona el Material Rodante*** recibe la solicitud por parte de la infraestructura de un vehículo apto para circular en ERTMS N2 en el tramo que disponga de claves KMAC, la ***UO que gestiona el Material Rodante*** deberá solicitar la generación de ficheros de instalación de claves KMAC.

Este procedimiento, desde el punto de vista del OBU, es idéntico al Procedimiento E15.2_EEFF excepto que la FASE 20 **Solicitud de instalación de clave KMAC en el RBC,** por parte de la ***UO que gestiona el Material Rodante***, no aplica.

Al tratarse de pruebas de infraestructura, no es necesario que la ***UO que gestiona el Material Rodante*** solicite la instalación de la clave KMAC en el RBC.

### 6.3.1.2.3.- PROCEDIMIENTO E16.3: Solicitud de generación de ficheros de borrado y borrado de clave KMAC

#### *6.3.1.2.3.1.- Diagrama de flujo*



### *6.3.1.2.3.2.- Descripción de las fases del procedimiento*

Este procedimiento, desde el punto de vista del OBU, es idéntico al Procedimiento E15.3_EEFF excepto que la FASE 20 **Solicitud de borrado de clave KMAC en el RBC,** por parte de la ***UO que gestiona el Material Rodante***, no aplica.

Al tratarse de pruebas de infraestructura, no es necesario que la ***UO que gestiona el Material Rodante*** solicite el borrado de la clave KMAC en el RBC.

### 6.3.2.- OBU PERTENECE A FOREIGN KMC

Estos escenarios (17 y 18) aplican en el caso de que el equipo embarcado del Material Rodante se encuentre fuera del dominio de gestión de claves de Adif/Adif AV (ver apartado 5) y por lo tanto opera bajo su propio KMC (denominado Foreign KMC).

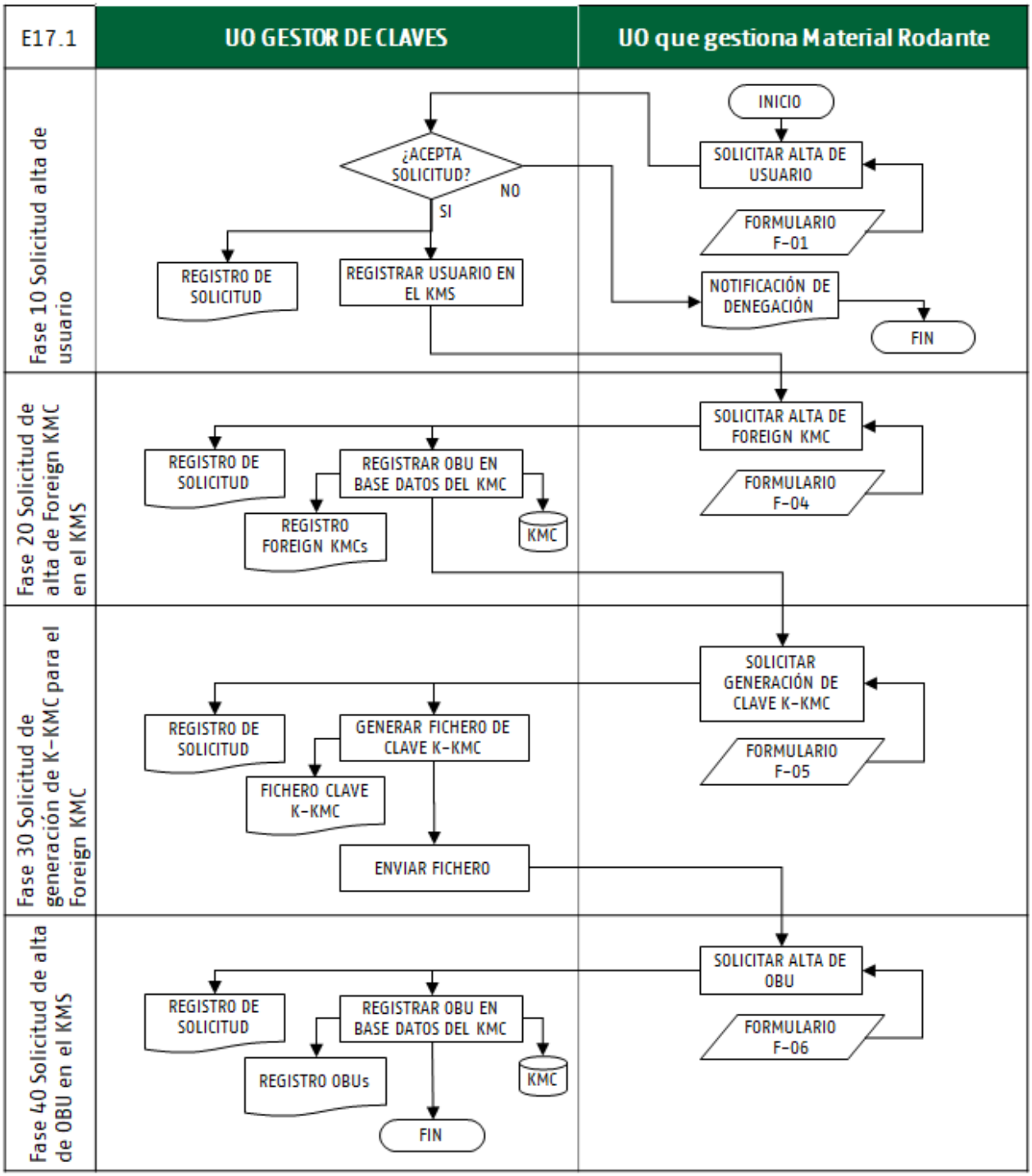
Para el intercambio de claves KMAC con un Foreign KMC es necesario el intercambio de una clave denominada K-KMC.

En estos escenarios la ***UO que gestiona el Material Rodante,*** para poder obtener las claves que permiten el establecimiento de la sesión de comunicación entre el OBU y el/los RBCs en ERTMS N2, debe solicitar, previamente, el alta de un usuario en el KMS, solicitar el alta de Foreign KMC en el KMS y solicitar la generación de la clave K-KMC. Además, deberá solicitar el alta del OBU en el KMS.

### 6.3.2.1.- ESCENARIO 17: Pruebas de Material Rodante, CCR, Formación, Servicio Comercial

#### 6.3.2.1.1.- PROCEDIMIENTO E17.1: Solicitud de generación e instalación de clave inter KMC (K-KMC)

##### *6.3.2.1.1.1.- Diagrama de flujo*



### *6.3.2.1.1.2.- Descripción de las fases del procedimiento*

**FASE 10 Solicitud de alta de usuario**

Toda persona física asociada a una ***UO que gestiona Material Rodante*** *que opera bajo un Foreign KMC*, deberá de darse de alta suministrando la información según el formato *ADIF-PE-301-001-IS-05-F-01* para establecer con ella un canal de comunicación apropiado.

El solicitante remitirá toda la información a la ***UO Gestor de Claves.***

La ***UO Gestor de Claves*** responderá a la solicitud de inclusión en el KMS en el plazo de 30 días hábiles.

En caso de denegarse la solicitud, se argumentará convenientemente al solicitante las razones de dicha denegación.

La solicitud de alta se realizará una única vez por cada usuario del KMS.

En el resto de este procedimiento se entenderá que las comunicaciones con la ***UO que gestiona el Material Rodante*** se realizan con un usuario debidamente acreditado dentro del KMS.

**FASE 20 Solicitud de alta de Foreign KMC en el KMS**

La ***UO Empresa Ferroviaria*** o la ***UO Suministrador de equipos embarcados*** a través de un usuario debidamente acreditado dentro del KMS debe solicitar la inclusión del Foreign KMC dentro del KMS. El solicitante recopilará la información contenida en el formato *ADIF-PE-301-001-IS-05-F-04* y la enviará a la ***UO Gestor de Claves***.

Nota: podría ser necesario por parte de la ***UO Empresa Ferroviaria*** el solicitar previamente un NID_KMC al AI que corresponda, de acuerdo con el apartado 5.

Adicionalmente, el solicitante deberá enviar al gestor de claves toda la información relativa a los procedimientos de intercambio de la clave K-KMC para su estudio y evaluación de posibles problemas de compatibilidad.

La ***UO Gestor de Claves*** introducirá la información de un nuevo Foreign KMC en el KMS y actualizará el registro de Foreign KMCs.

La solicitud de alta de Foreign KMC se realizará una única vez para cada ***UO Empresa Ferroviaria*** o la ***UO Suministrador OBU***.

Nota: es posible que una **UO** cuente con más de un Foreign KMC (por ejemplo, uno por cada tecnólogo de OBU) en cuyo caso será necesario dar de alta a cada uno de ellos.

**FASE 30 Solicitud de generación de K-KMC para el Foreign KMC**

La ***UO Empresa Ferroviaria*** o la ***UO Suministrador OBU***, a través de un usuario debidamente acreditado dentro del KMS, solicitará la generación de la clave K-KMC para un Foreign KMC enviando a la ***UO Gestor de Claves*** la información contenida en el formato *ADIF-PE-301-001-IS-05-F-05* y la enviará a la ***UO Gestor de Claves.***

El solicitante enviará toda la información a la ***UO Gestor de Claves***.

La *UO Gestor de Claves* enviará la clave K-KMC a la *UO* solicitante.

La clave K-KMC se considera definitiva.

**FASE 40 Solicitud de alta de OBU en el KMS**

La *UO Empresa Ferroviaria* o la *UO Suministrador de equipos embarcados*, a través de un usuario debidamente acreditado dentro del KMS debe solicitar la inclusión del OBU dentro del KMS.

El solicitante recopilará la información contenida en el formato *ADIF-PE-301-001-IS-05-F-06* y la enviará a la *UO Gestor de Claves*.

La *UO Gestor de Claves* introducirá la información de un nuevo OBU en el KMS y actualizará el registro de los OBUs.

### 6.3.2.1.2.- PROCEDIMIENTO E17.2: Solicitud de generación e instalación de clave KMAC

Este procedimiento es idéntico al Procedimiento E15.2_EEFF.

### 6.3.2.1.3.- PROCEDIMIENTO E17.3: Solicitud de generación de ficheros de borrado y borrado de clave KMAC

Este procedimiento es idéntico al Procedimiento E15.3_EEFF.

#### 6.3.2.2.- ESCENARIO 18: Pruebas de infraestructura

##### 6.3.2.2.1.- PROCEDIMIENTO E18.1: Solicitud de generación e instalación de clave inter KMC (K-KMC)

Este procedimiento es idéntico al Procedimiento E17.1.

##### 6.3.2.2.2.- PROCEDIMIENTO E18.2: Solicitud de generación e instalación de clave KMAC

Este procedimiento es idéntico al Procedimiento E16.2.

##### 6.3.2.2.3.- PROCEDIMIENTO E18.3: Solicitud de generación de ficheros de borrado y borrado de clave KMAC

Este procedimiento es idéntico al Procedimiento E16.3.

## 7. DOCUMENTACIÓN DE REFERENCIA

[Ref. 01] Subset-037 Euroradio FIS. Issue 2.3.0. Date: 14.10.2005.

[Ref. 02] Sutset-038 Off-line Key Management FIS. Issue 2.3.0. Date: 11.11.2010.

[Ref. 03] NAS 841. Requisitos de Interfaz de Gestión de claves.

[Ref. 04] ADIF-PE-301-001-IS-05-Procedimiento Gestión Claves ERTMS Nivel 2.

## 8. REGISTROS

Esa apartado no aplica.

## 9. ANEXOS Y FORMATOS

**Anexos:**

No aplica

**Formatos:**

- ADIF-PE-301-001-IS-05-F-01: Solicitud de Alta/ Modificación/ Baja de usuario en el KMS
- ADIF-PE-301-001-IS-05-F-02: Solicitud de Alta/ Modificación/ Baja de RBC en el KMS, este formato no aplica en este documento
- ADIF-PE-301-001-IS-05-F-03: Solicitud de Generación de clave KTRANS para RBC, este formato no aplica en este documento
- ADIF-PE-301-001-IS-05-F-04: Solicitud de Alta/ Modificación/ Baja de Foreign KMC
- ADIF-PE-301-001-IS-05-F-05: Solicitud de Generación de clave K-KMC para Foreign KMC
- ADIF-PE-301-001-IS-05-F-06: Solicitud de Alta/ Modificación/ Baja de OBU en el KMS
- ADIF-PE-301-001-IS-05-F-07: Solicitud de Generación de clave KTRANS para OBU
- ADIF-PE-301-001-IS-05-F-08: Solicitud de Generación de clave KMAC
- ADIF-PE-301-001-IS-05-F-09: Solicitud de Ficheros de borrado de clave KMAC
- ADIF-PE-301-001-IS-05-F-10: Solicitud de Instalación/ Borrado de clave KMAC en el RBC

## 10. CONTROL DE MODIFICACIONES

| Revisión | | Modificaciones | Hojas Revisadas |
|---|---|---|---|
| N.º | Fecha | | |
| 0 | Diciembre 2024 | Edición Inicial | Todas |