El tacógrafo digital
Un nuevo sistema de control del tráfico pesado en carretera.

Antecedentes.

La creciente sensibilización de la sociedad ante los accidentes de tráfico en carretera provocados por el tráfico pesado colocó a los políticos europeos ante la tarea de modificar el sistema actual de control para evitar los numerosos fraudes que se producen. Después de muchos años de trabajo se llegó al acuerdo de instalar un nuevo sistema control que almacene cifrados y en formato digital los datos de la conducción, y que este sistema vaya substituyendo de forma paulatina al analógico actual.
El 13 de Junio de 2.002 la Comisión Europea aprobó el reglamento 1.360 por el que se establecieron las normas para el uso del nuevo tacógrafo digital que substituirá al tacógrafo actualmente en uso en las carreteras europeas.
La entrada en vigor de este nuevo sistema ha supuesto un reto importante para la Unión por varios motivos. Por primera vez se ha emprendido un proyecto en el que están todos los miembros y en el que de forma coordinada lo deben poner en marcha en una determinada fecha: el 5 de agosto de 2.005. También por primera vez se crea una red común de consultas, que puede servir de modelo para otros proyectos de intercambio de información.

Lanzamiento del proyecto europeo.

Por todo ello la Comisión decidió crear una serie de grupos de trabajo que ayudara a los Ministerios responsables de todos los países a implantar el nuevo proyecto del tacógrafo.
Estos grupos se concentraron en dos líneas de trabajo, que correspondieron a los dos proyectos mas interesantes que se presentaron a la Comisión para su financiación.
La primera línea de trabajo se dirigió al estudio de las normas para que, en lo posible, los controladores de todos los países tengan una interpretación común ante las mismas infracciones o problemas que surjan.
La segunda línea de trabajo fue mas técnica y se subdividió en dos: una para coordinar la instalación de la firma digital Europea en cada país y la otra para la creación de la mencionada red Europea de consulta para el registro de conductores, que se denominó Tachonet.
El trabajo de coordinación del proyecto ha sido muy importante y es una de las claves del éxito del proyecto, ya que ahora es posible decir que hay normas y procedimientos claros para que cada país pueda hacer su desarrollo y cumpla los requisitos que especifica el Reglamento.
A uno de los mencionados tres grupos de trabajo se incorporaron especialistas de la mayoría de los entonces 15 miembros, mas Suiza, Noruega e Islandia. Para poder entenderse y trabajar en esta Torre de Babel se estableció como idioma de trabajo el inglés. También se ajustó un procedimiento y calendarios diferentes para cada una de las reuniones técnicas, y se fijaron una serie de reuniones plenarias para informar de los avances en cada sector y coordinar posibles incompatibilidades entre las conclusiones de cada grupo.

Después de casi tres años de trabajo se ha dado por concluida esta fase de desarrollo para la implantación del sistema en los países de la Europa sin ampliar.

¿Que es el tacógrafo digital?

El tacógrafo digital es un computador dentro de una caja de tamaño y aspecto similares a una radio de coche.

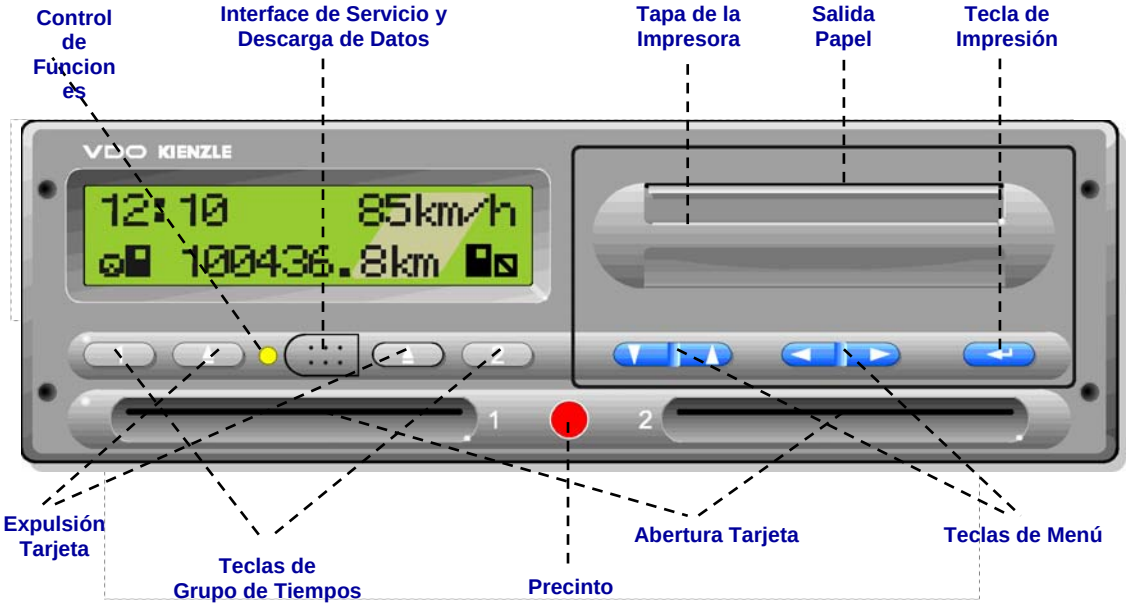

Ilustración 1. Tacógrafo digital.

Este computador recibe el número de revoluciones del motor mediante un sensor acoplado a la caja de cambios y, mediante un reloj interno, genera los datos de conducción: tiempos de marcha y descanso y velocidad del vehículo.

Ilustración 2. Sensor de movimiento.

Estos datos se personalizan cuando se introduce una de las varias tarjetas inteligentes que de una u otra forma controlan al tacógrafo. Todos los datos que circulan por el sistema: tacógrafo, sensor y tarjetas inteligentes, están cifrados mediante claves.
Existen cuatro tipos de tarjetas:

Ilustración 3. Anverso de las tarjetas

- de conductor, que contiene los datos personales del conductor y almacena los parámetros de su conducción durante un período de un mes,
- de empresa, que controla los datos de sus conductores y permite el control de flotas y conductores,
- de control, para revisar los datos contenidos en los dos tipos anteriores de tarjetas y los de los tacógrafos, y
- de centro de ensayo (coloquialmente de taller), que permiten activar y calibrar el sistema tacógrafo – sensor de movimiento.

Como puede observarse, cada tarjeta tiene un color predominante para facilitar su rápida diferenciación.
El acceso al sistema y a las diferentes funciones de este computador está controlado mediante el uso de claves de cifrado RSA, de forma que solo aquellos que poseen la llave adecuada pueden generar datos y acceder a la información mencionada anteriormente.

Ilustración 4. Reverso de las tarjetas.

Sistema de claves y cifrado de datos del tacógrafo.

La Comisión Europea, máxima autoridad sobre la que descansa toda la cadena de confianza, genera una clave privada y una clave pública de las características especificadas en el Anexo 1B del mencionado reglamento 1.360.
A su vez, cada uno de los países miembros que cumplen las normas definidas en el Anexo 1B y aquellos otros criterios acordados en los anteriormente mencionados grupos técnicos, generan sus propias claves privadas y públicas.
Sus claves públicas se envían a la Comisión para su certificación, o firma por la clave privada de la comisión. De esta forma, cada país se constituye en entidad certificadora de los equipos que se producirán en su país: tarjetas, tacógrafos y/o sensores de movimiento.
El formato de esta firma digital es similar al estándar 509X que se emplea en los certificados digitales de la mayoría de las autoridades de certificación, pero no es compatible con el.
Todos los equipos fabricados bajo esta norma llevan una clave privada y la firma digital de todas las autoridades a las que pertenecen: En el caso de una tarjeta fabricada en España, llevará las firmas europea y la de la autoridad española de certificación; el Ministerio de Fomento.
El sistema de reconocimiento mutuo entre las tarjetas el tacógrafo y el sensor y el cifrado de datos se basa en la generación de claves tipo RSA y firmas digitales. Cada vez que un sensor o una tarjeta inteligente se ponen en comunicación con un tacógrafo deben establecer una sesión de trabajo. Para ello deben reconocerse como pertenecientes al sistema del tacógrafo digital de la Comisión. Para ello generan un número aleatorio y lo cifran con la clave pública europea para que el otro equipo lo descifre con la suya privada. Una vez que se comprueba que ese número aleatorio es el emitido por el otro equipo se establece la comunicación. El tacógrafo almacena en su propia memoria los

datos proporcionados por el sensor y actúa según lo que le indica la tarjeta que está introducida en el mismo. Si es de conductor almacena también los datos en la memoria del chip de la tarjeta, si es de control los envía a la impresora del tacógrafo o al puerto de comunicaciones RS232 del tacógrafo para su almacenamiento externo, o si es de taller para el calibrado del sistema.

El proyecto europeo.

Con la información contenida en el Reglamento cada uno de los países miembros es responsable de implantar un sistema que identifique y entregue las tarjetas a sus usuarios nacionales. El reto que se lanzó es importante. En primer lugar, el sistema que se describía en el Reglamento solo existía sobre papel, y su realización dependía de que cada parte se responsabilizara de cumplir unos hitos y plazos para que el sistema se hiciera realidad al confluir todos ellos en agosto de 2.004. La Comisión debía generar sus claves a tiempo para que las tarjetas y tacógrafos se sirvieran de ellas. Los fabricantes de tacógrafos deberían tener equipos homologados un año antes de la fecha de lanzamiento para que los fabricantes de camiones y autobuses pudieran probar el sistema en todas las condiciones reales. Y, por último, quince países debían instalar sus sistemas de registro, control y fabricación a tiempo además de coordinarse para cambiar mensajes por una red inexistente.
Por muy diversas causas el proyecto se retrasó y la Comisión aplazó la fecha de puesta en marcha dando un respiro de un año a la fecha de implantación original. En este momento hay cinco países que están en disposición de emitir tarjetas y tacógrafos, y uno de ellos es Francia, llave por la que pasa la mayoría del tráfico que circula por Europa, por lo que la fecha del 5 de Agosto de 2.005 es ya un hecho.

El sistema de registro en España.

Cada miembro de la UE es libre de diseñar su propio sistema para registrar a usuarios de tarjetas, fabricarlas y hacer las entregas siempre que se cumplan los plazos y normas obligadas por el Reglamento. En consecuencia, España ha optado por el diseño de un sistema descentralizado para el registro y entrega de tarjetas a los usuarios, y centralizado en la fabricación.
Otros países han optado por esquemas muy diferentes, Francia por un sistema centralizado en el que se envían en un formulario los datos por correo, Alemania por un sistema similar al español, e Italia por sistema descentralizado tanto en la captura como en la fabricación y personalización.
El sistema descentralizado para la captura de los datos de registro tiene la ventaja de acercar al solicitante la administración y reducir los tiempos de espera. La fabricación centralizada para un sistema complejo como el que se está describiendo, disminuye mucho los costes de inversión, aunque presenta la desventaja de alargar el período de entrega de las tarjetas. Como botón de muestra: Italia tiene estimado en este momento el precio de venta de las tarjetas más alto entre los países de la UE.
Dado que es obligatoria la identificación del usuario por la autoridad de emisión, es necesario que el solicitante pase al menos una vez por una oficina de registro.

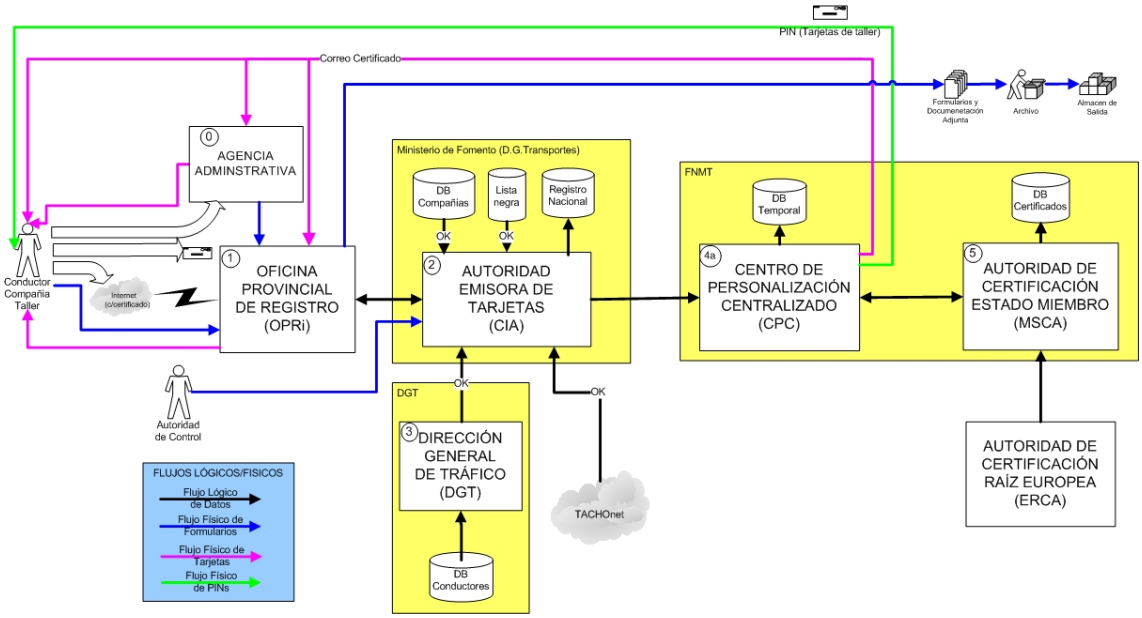

Ilustración 5. Proceso de emisión de tarjetas.

Se ha diseñado un sistema informático por el que todas las oficinas provinciales de registro, unas 80, se conectan por Internet a un servidor central.

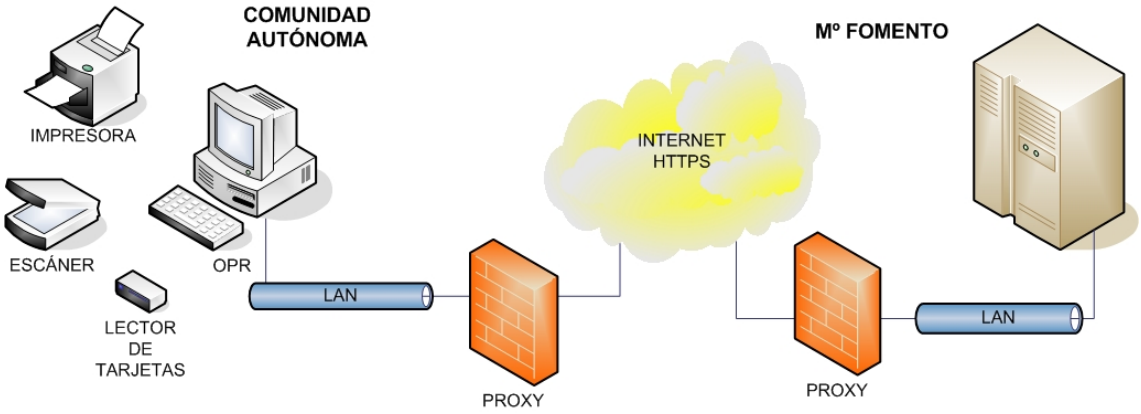

Ilustración 6. Esquema de conexión entre oficinas de Registro y Fomento.

Todos los clientes de este servidor en la primera conexión reciben el software que permite el registro de los usuarios. De esta forma las sesiones son rápidas y solo se actualiza el software de forma automática cuando hay una nueva versión y el servidor así se lo hace saber al cliente. Todos los datos están cifrados y firmados por certificados digitales.
El solicitante se presenta en la oficina de registro con el mínimo número de justificantes, en el caso de un conductor solo es necesario el número de su licencia de conducir y una fotografía. Como mediante ese terminal se tiene acceso a las bases de datos de la DGT y de Transportes, la mayoría de los datos necesarios para el alta se transfieren a la solicitud de forma automática y el solicitante solo debe corroborarlos.

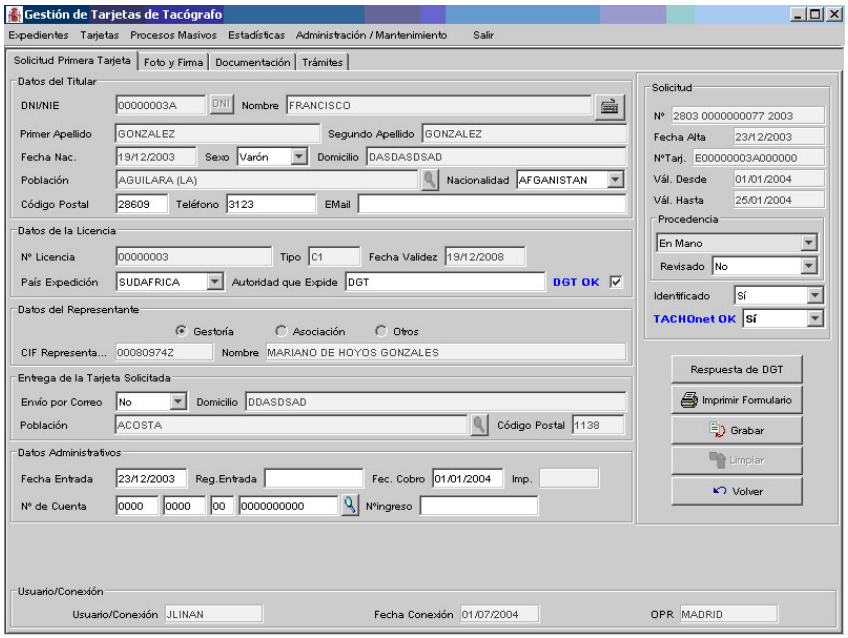

Ilustración 7. Ejemplo de solicitud.

Por último, se escanea la fotografía que, a voluntad del operador, puede ser corregida si algunos de sus parámetros, brillo, contraste, color predominante, etc., no están bien balanceados. Igualmente se modifica el eje de la foto si ésta está torcida.

Ilustración 8. Tratamiento de imágenes.

Una vez concluido el registro, se actualizan las bases de datos, en las que se incluye el estado en el que se encuentra el proceso para su consulta por los operadores o por el solicitante, y se hace una consulta a todos los países de la UE para verificar que ese conductor no tiene otra tarjeta válida.
La consulta por Tachonet tiene una espera máxima de 24 horas para que el resto de los países emisores consulten en sus bases de datos y formulen la correspondiente

respuesta. Pasado ese plazo, si la respuesta es negativa; ese conductor no está dado de alta en otro país, el sistema envía una nota autorizando la fabricación de la tarjeta en la FNMT.
Existen otras dos formas de acceso al sistema de Registro mediante Internet. La primera con una firma digital de una autoridad española reconocida. La segunda sin firma digital.
En el primer caso y dado que los datos provienen de una fuente conocida, sea aceptan como válidos todos los datos de la solicitud, incluidos el pago de las tasas, fotografía, etc. Todas estas solicitudes llegan electrónicamente al funcionario de la Comunidad correspondiente, que los valida de forma automática. En el caso de una solicitud sin firma digital, el sistema genera un código de acceso que entrega al usuario. Con este código el solicitante acude a la oficina tramitadora más cercana, desde donde el funcionario puede recuperar los datos de una base de datos intermedia. De esta forma se facilita y acorta el trámite de solicitud tanto para el solicitante como para el operador de la oficina.

La red europea Tachonet.

Dado que las bases de datos que contienen los registros de conductores son propiedad de organismos nacionales muy diferentes y las leyes de protección de datos de cada país son muy restrictivas, se optó por no aunar los datos. En su lugar, las autoridades emisoras de cada país se hacen preguntas y respuestas de una serie de contenido y formato previamente definidos. La red por donde circula esta información es privada, pertenece a la Comisión, y une organismos oficiales de cada miembro de la UE. La información que circula va cifrada mediante certificado digital. La organización está centralizada en Bruselas que recibe las peticiones de información y/o respuestas, y las bombea a los organismos emisores del país/países receptores.
El nodo español de Tachonet está situado en la DGTrans.
Mediante este nodo, también se comunicarán las fuerzas de seguridad que controlan el transporte por carretera y los controladores con el resto de emisores. De esta forma se podrá tener información instantánea en carretera sobre las tarjetas y los conductores de cualquier país, y aquellos otros datos pertinentes que requiera el agente.

Fabricación de tarjetas.

Una vez aceptada la solicitud, el sistema genera un fichero conteniendo los datos necesarios para la fabricación de las tarjetas en la FNMT. Esta conexión se realiza mediante una red privada virtual entre la DGTrans y la FNMT. Una vez fabricadas las tarjetas, la FNMT genera un fichero con datos de control de la fabricación, claves públicas y números de serie de cada tarjeta con el fin de mantener la base de datos de la entidad emisora.

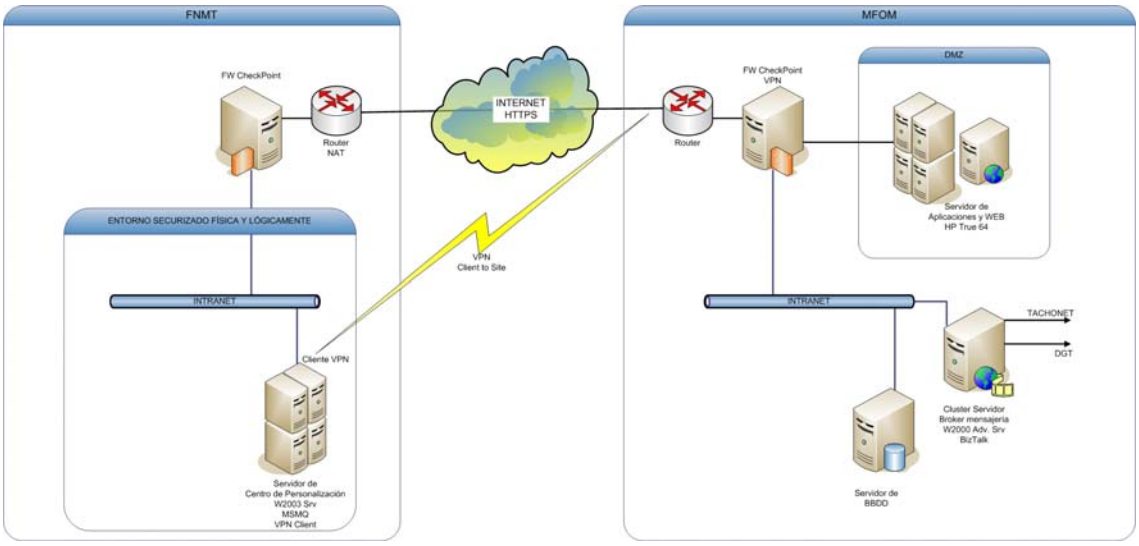

Ilustración 9. Esquema de conexión entre la DGTrans y la FNMT.

Con los datos recibidos de la entidad de emisión, se procede a la generación de todos los campos necesarios para imprimir la tarjeta y personalizar su chip:

- Generación de las claves RSA pública, PK, y privada de cada tarjeta,
- Cifrado de cada clave privada, SK, mediante una clave de sesión TDES,
- Firmado de la clave pública por la autoridad europea, ERCA,
- Generación de diversos parámetros, tales como el CHR (Certificate Holder Referente) identificador único para cada tarjeta que relaciona las PK y SK, un identificador único de tarjeta CHA (Certificate Holder Authoritation),
- PIN para las tarjetas de taller (Centro de ensayo),
- adecuación de datos identificativos a sus respectivos campos: nombres, direcciones, etc.,
- generación de los datos administrativos y de gestión: facturación, envío, control de situación de la tarjeta, etc.

Una vez fabricada la tarjeta/s se envía a su destinatario final: el solicitante si ya se ha identificado previamente o la oficina de registro si no lo ha hecho anteriormente por haber solicitado la tarjeta por Internet o una agencia.

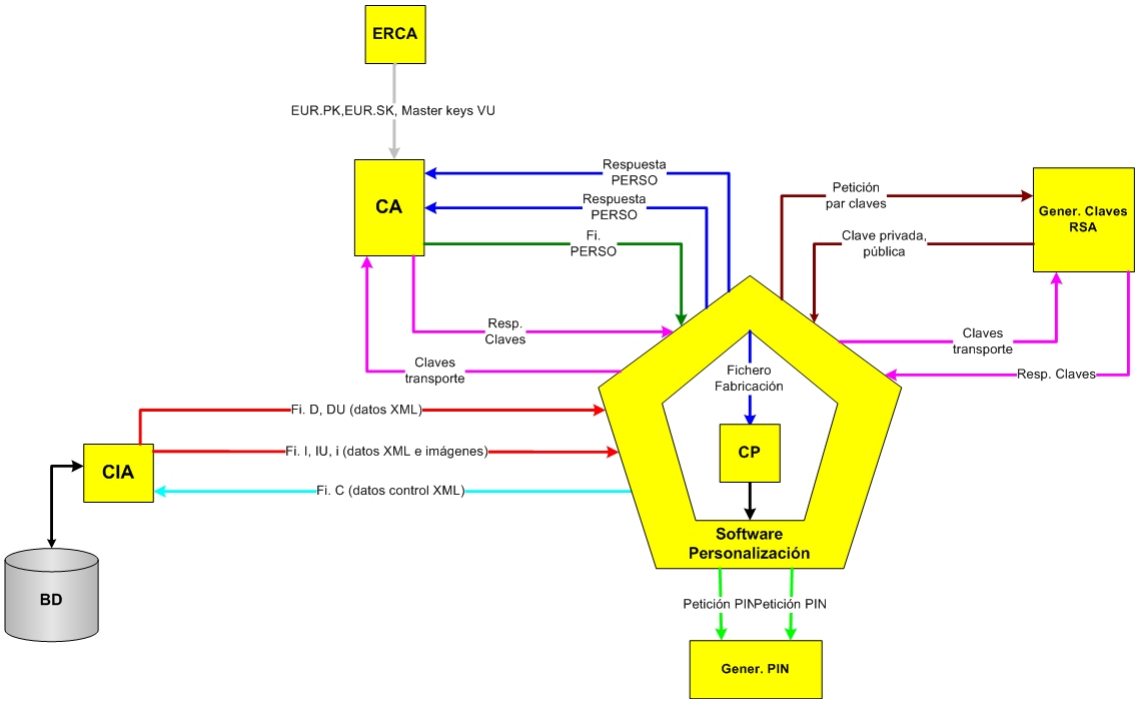

Ilustración 10. Esquema de fabricación de tarjetas.

Nomenclatura empleada.

TACHOnet	Sistema informático europeo de preguntas y respuestas, que se implantará sobre la red TESTA.
CA	(Certification Authority) Autoridad de certificados; se usará en algunas ocasiones en lugar de MSCA
CIA	(Card Issuing Authority). Autoridad emisora de tarjetas. En el caso español, la Dirección General de Transportes del Ministerio de Fomento
CDAD	Centro de descarga y análisis de datos
CP	Centro de personalización. FNMT
DGTrans	Dirección General de Transportes por carretera
DGT	Dirección General de Tráfico
ERCA	(European Root Certification Authority). Autoridad de certificación de raíz europea
MSCA	(Member State Certification Authority). Autoridad de certificación de estado miembro
OPR	Oficina provincial de registro