Ministerio
de Fomento

Política de la Autoridad Española

Ministerio
de Fomento

Directrices sobre gestión de claves, certificados y manejo de equipos

Para el

Sistema del tacógrafo digital

Control de versiones

Oficial Versión 1.0	noviembre 2004	Aprobada por la Autoridad Europea	Alfonso Sánchez Francisco Murillo (MFOM) Eduardo Echevarría José Luís Blanco (FNMT)

Índice

1 INTRODUCCIÓN

El presente documento establece la política de la Autoridad Española[1]. Esta política se aplicará en el funcionamiento del sistema del tacógrafo digital

La política de la Autoridad Española es un documento en el que se incluyen los requisitos para garantizar la gestión de claves, certificados y equipos relacionados.

Esta política cumple con:

- El Reglamento (CE) 2135/98 sobre el sistema del tacógrafo digital
- El Reglamento (CE) 1360/2002 sobre adaptación al proceso técnico del Reglamento (CE) 3821/85
- El sistema del tacógrafo digital: Política de Raíz Europea.

1.1 *Organizaciones responsables*

El siguiente gráfico muestra la organización del sistema del tacógrafo digital:

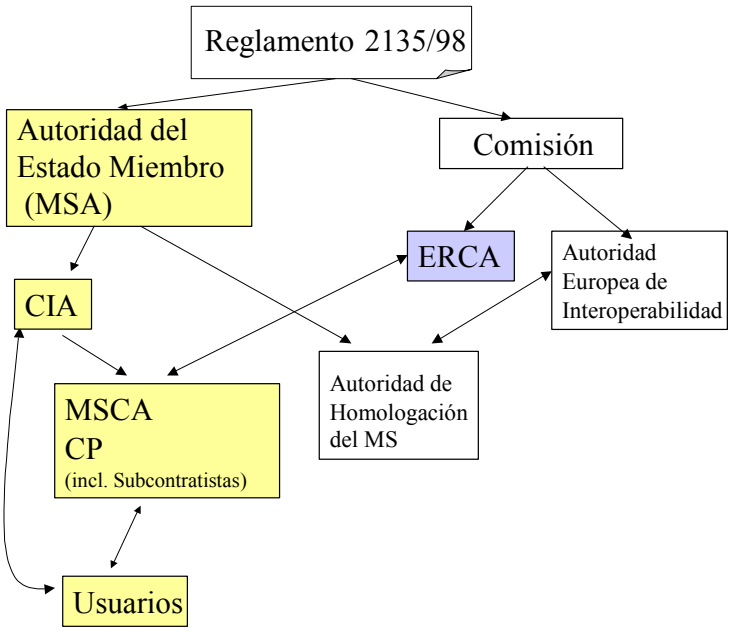

Figure 1 Organización del Sistema de tacógrafo digital.

[1] La política de la Autoridad Certificadora es una terminología común que establece los requisitos de la gestión de claves, certificados y normalmente, tarjetas para una determinada CA (Autoridad Certificadora).

La **Autoridad Española** responsable de establecer las directrices de la presente política, es el:

Ministerio de Fomento.
c) Paseo de la Castellana nº 67
E-28071 Madrid

A su vez, el **Ministerio de Fomento** ha delegado la función de **Autoridad Española** en la **Dirección General de Transportes por Carretera**, asignándole por tanto la política y la ejecución de sus tareas.

La **Dirección General de Transportes por Carretera** es también la autoridad responsable de la emisión de tarjetas. Por tanto, será la **Autoridad Española Emisora de Tarjetas** y albergará en su sede la organización, el hardware y el software para el desarrollo de esta tarea.

La entidad designada para emitir los certificados y personalizar las tarjetas, **Autoridad Española de Certificación** y **Centro Español de Personalización** es la:

Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda
c/ Jorge Juan nº 106
E-28009 Madrid

en lo sucesivo **FNMT- RCM**.

La entidad homologadora de las tarjetas en el Estado Español es la:

Subdirección General de Seguridad y Calidad Industrial
c) Paseo de la Castellana nº 160
E-28071 Madrid

1.2 *Aprobación*

La política de la Autoridad española ha sido elaborada por la **Dirección General de Transportes por Carretera.**

La Política de la Autoridad Española en su versión 1.0 ha sido aprobada por la Autoridad Europea el 23 noviembre de 2004.

1.3 *Disponibilidad y contactos*

La política de la Autoridad Española está disponible en la dirección www.mfom.es

Las preguntas relativas a la política de la Autoridad Española deberán dirigirse a la:

Dirección General de Transportes por Carretera
Ministerio de Fomento
c) Paseo de la Castellana nº 67
E-28071 Madrid

2 AMBITO Y APLICABILIDAD

[e1] La política de la Autoridad Española sólo tendrá validez para el sistema del tacógrafo digital.

[e2] Las claves y certificados emitidos por la Autoridad Española sólo se emplearán en el sistema del tacógrafo digital.

[e3] Las tarjetas emitidas por el sistema del tacógrafo digital sólo se emplearán en el sistema del tacógrafo digital.

El siguiente diagrama resume el proceso de certificación seguido por la Autoridad Española de Certificación para el sistema del tacógrafo digital.

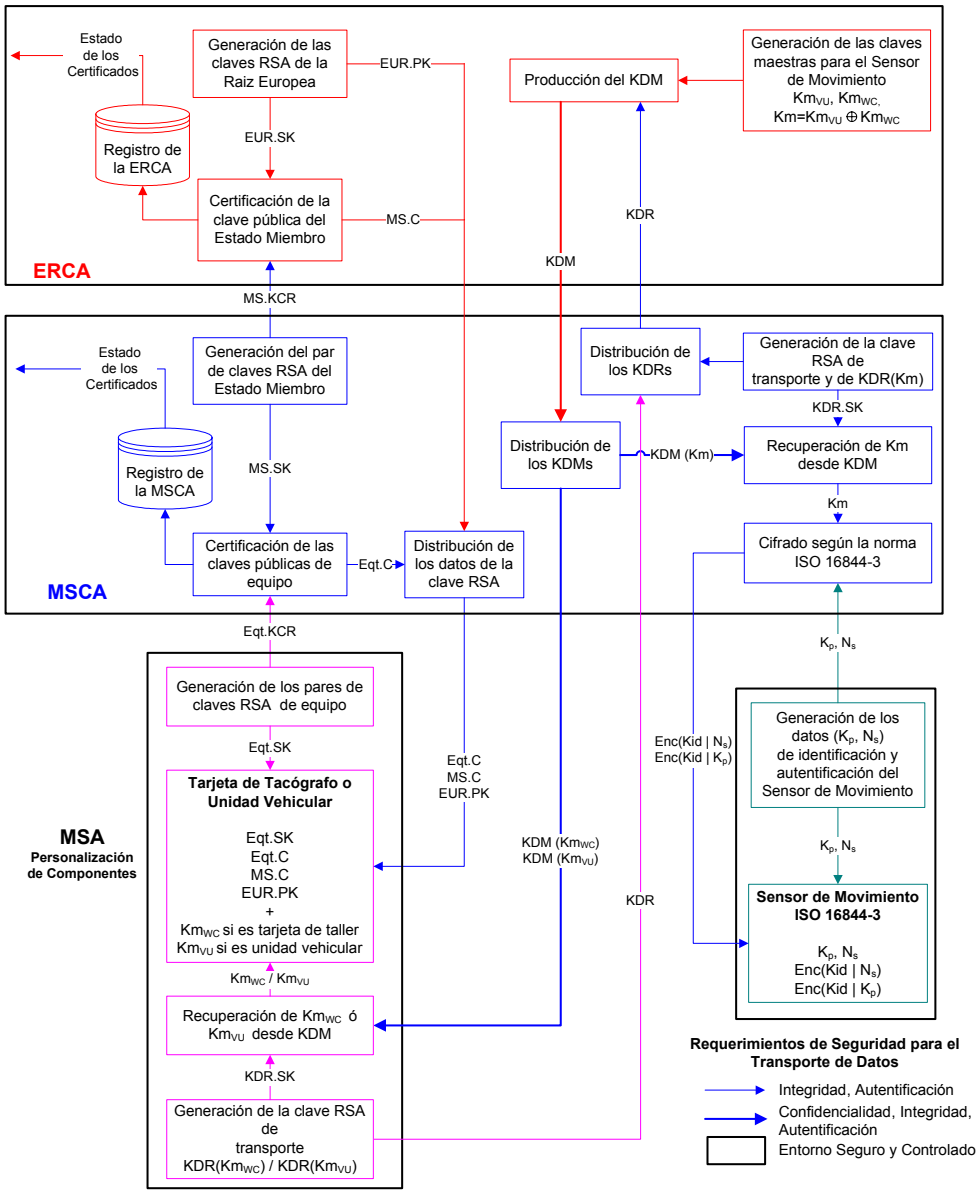

Figure 2 **Gestión de claves, certificados y equipos del sistema del tacógrafo digital**

3 CONDICIONES GENERALES

3.1 *Obligaciones*

Este apartado contiene las disposiciones relativas a las obligaciones de los siguientes organismos:

- Autoridad Española y Autoridad Española Emisora de Tarjetas.
- Autoridad Española de Certificación. Centro Español de Personalización.
- Usuarios (titulares, fabricantes de unidades para vehículos y fabricantes de Sensores de Movimiento).

3.1.1 Obligaciones de la Autoridad Española y de la Autoridad Española Emisora de Tarjetas

[e4] La Autoridad Española deberá:

a) Mantener la política de la Autoridad Española.

b) Designar a la Autoridad Española de Certificación y Centro Español de Personalización.

c) Auditar a la Autoridad Española de Certificación y al Centro Español de Personalización.

d) Aprobar los documentos de la Autoridad Española de Certificación y del Centro Español de Personalización.

e) Informar a las entidades designadas sobre la política a seguir.

f) Informar a los fabricantes de unidades para vehículos y a los fabricantes de Sensores de Movimiento sobre la política a seguir.

g) Evitar el uso no autorizado de las claves privadas generadas, almacenadas y utilizadas bajo el control de esta política.

h) Remitir esta política a la Comisión Europea para su aprobación.

[e5] La Autoridad Española Emisora de Tarjetas deberá:

a) Garantizar la introducción en la Autoridad Española de Certificación y en el Centro Español de Personalización de los datos correctos y relevantes del usuario generados durante el proceso de solicitud de tarjeta.

b) Informar a los usuarios, por ejemplo, titulares, fabricantes de unidades para vehículos y fabricantes de Sensores de Movimiento, de los requisitos de esta política relacionados con el uso del sistema.

3.1.2 Obligaciones de la Autoridad Española de Certificación

[e6] Dichas obligaciones serán:

a) Seguir las directrices de la política de la Autoridad Española.

b) Publicar el documento de Disposiciones Prácticas de la Autoridad Española de Certificación, con referencia a presente política , para su aprobación por parte de la Autoridad Española.

c) Mantener los recursos financieros y organizativos para actuar de conformidad con los requerimientos expresados en esta política, en concreto para evitar perjuicios y daños de responsabilidad civil.

[e7] La Autoridad Española de Certificación deberá cerciorarse de que se cumplan todos los requisitos especificados en esta política.

[e8] La Autoridad Española de Certificación será responsable de que la práctica se ajuste a los procedimientos recomendados en esta política.

3.1.3 Obligaciones del Centro Español de Personalización

[e9] El Centro Español de Personalización ha de:

a) Seguir las directrices de la política de la Autoridad Española.

b) Elaborar el documento de Disposiciones Prácticas del Centro Español de Personalización incluyendo las referencias a esta política y remitirla para su aprobación a la Autoridad Española.

c) Mantener suficientes recursos financieros y organizativos para actuar de conformidad con los requerimientos expresados en esta política de la Autoridad Española, en concreto para evitar perjuicios o daños de responsabilidad civil.

[e10] El Centro Español de Personalización deberá cerciorarse de implementar todos los requisitos expresados en esta política.

[e11] El Centro Español de Personalización es responsable de ajustarse a los procedimientos expresados en esta política.

3.1.4 Obligaciones de las Empresas Colaboradoras

[e12] Las empresas colaboradoras asumirán las obligaciones expresadas en esta política, por medio de acuerdos contractuales establecidos con la Autoridad Española de Certificación o el Centro Español de Personalización y los usuarios.

3.1.5 Obligaciones de los titulares de las tarjetas

[e13] La Autoridad Española Emisora de Tarjetas requerirá, mediante un formulario firmado, a los titulares (u organizaciones de titulares) el cumplimiento de las siguientes obligaciones:

a) Proporcionar información verdadera en los formularios de solicitud,

b) Asegurarse que la tarjeta se usa de forma apropiada, únicamente para aquello para lo que ha sido emitida y evitar su mal uso especialmente por terceros,

c) Los titulares de tarjetas de conductor solo podrán estar en posesión de una única tarjeta válida de conductor,

d) No emplear tarjetas dañadas o caducadas,

e) Informar a la autoridad responsable de su pérdida, robo, daño o mal uso de la tarjeta o su clave privada.

3.1.6 Obligaciones de los fabricantes de unidades para vehículos

[e14] La Autoridad Española exigirá a los fabricantes de unidades para vehículos, mediante acuerdo firmado, el cumplimiento de las siguientes obligaciones:

a) proporcionar información completa y precisa a la Autoridad Española según lo especificado en esta política, en concreto en lo relativo a los datos de registro;

b) usar las claves y certificados solamente en el sistema del tacógrafo digital;

c) emplear exclusivamente la clave privada del equipo en la unidad para vehículos;

d) evitar el uso no autorizado de la clave privada del equipo;

e) notificar inmediatamente a la Autoridad Española Emisora de Tarjetas, dentro del período de validez que figura en el certificado, si la clave privada del equipo se ha perdido, ha sido vulnerada o está en situación comprometida.

[e15] La Autoridad de Certificación podrá suspender, reactivar o revocar el permiso de uso del certificado e informar posteriormente a la Autoridad Española.

3.1.7 Obligaciones de los fabricantes de sensores de movimiento

[e16] La Autoridad Española exigirá a los fabricantes de Sensores de Movimiento, mediante acuerdo firmado, el cumplimiento de las siguientes obligaciones:

a) proporcionar información completa y precisa a la Autoridad Española según lo especificado en esta política, en concreto en lo relativo a los datos de registro;

b) usar las claves solamente en el sensor de movimiento;

c) notificar a la Autoridad Española inmediatamente si la clave del equipo se ha perdido, ha sido vulnerada o está en situación comprometida.

[e17] La Autoridad de Certificación podrá suspender, reactivar o revocar el permiso de uso del certificado e informar posteriormente a la Autoridad Española.

3.2 *Responsabilidad*

La Autoridad Española de Certificación y el Centro Español de Personalización no serán responsables frente a los usuarios finales, sólo lo serán frente a la Autoridad Española y la Autoridad Española Emisora de Tarjetas.

Cualquier asunto sobre responsabilidad frente a los usuarios finales será competencia de la Autoridad Española o de la Autoridad Española Emisora de Tarjetas.

[e18] Las tarjetas de tacógrafo, claves y certificados sólo serán válidos dentro del sistema del tacógrafo digital. El uso de cualquier otro tipo de certificado constituirá una violación de esta política, y por tanto ni la Autoridad Española, ni la Autoridad Española Emisora de Tarjetas, ni la Autoridad Española de Certificación ni el Centro Español de Personalización se hacen responsables de dicho uso.

3.2.1 Responsabilidad de la Autoridad Española y de la Autoridad Española Emisora de Tarjetas frente a los titulares y organismos relacionados

[e19] La Autoridad Española y la Autoridad Española Emisora de Tarjetas serán responsables de los daños ocasionados al cumplir con sus obligaciones sólo en el caso de que hayan actuado con negligencia. Si la Autoridad Española o la Autoridad Española Emisora de Tarjetas han actuado según esta política y cualquier otro documento pertinente, dicha actuación no se considerará negligente.

3.2.2 Responsabilidad de la Autoridad Española de Certificación y el Centro Español de Personalización frente a la Autoridad Española y la Autoridad Española Emisora de Tarjetas

[e20] El Centro Español de Personalización o la Autoridad Española de Certificación serán responsables de los daños ocasionados al cumplir con sus obligaciones sólo en el caso de que hayan actuado con negligencia. Si la organización ha actuado según esta política y las de su correspondiente documento de Disposiciones Prácticas, dicha actuación no se considerará negligente.

3.3 *Interpretación y aplicación*

3.3.1 Jurisdicción competente

[e21] Los conflictos que pudieran surgir de la interpretación o ejecución de esta política, se resolverán ante los juzgados y tribunales del orden jurisdiccional competente de Madrid capital.

3.4 *Confidencialidad*

La confidencialidad está restringida según la directiva 95/46/EC y la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999 de 13 de diciembre sobre protección de datos personales y su procesado y manejo.

3.4.1 Información considerada confidencial

[e22] Cualquier información personal o corporativa de la que disponga la Autoridad Española de Certificación, el Centro Español de Personalización o las entidades colaboradoras, y que no aparezca en las tarjetas o certificados se considerará confidencial y no se revelará sin el consentimiento previo del titular, ni (donde sea aplicable) sin consentimiento del empresario responsable o su represente, a menos que la legislación especifique en contrario.

[e23] Todas las claves secretas y privadas utilizadas y manejadas por la Autoridad Española de Certificación y el Centro Español de Personalización, bajo el ámbito de la presente política, serán confidenciales.

[e24] Todas las claves secretas y privadas utilizadas y manejadas por los fabricantes de unidades para vehículos, bajo el ámbito de la presente política, serán confidenciales.

[e25] Las claves secretas utilizadas y manejadas por los fabricantes de sensores de movimiento, bajo el ámbito de la presente política, serán confidenciales.

[e26] Los archivos de auditoría y grabaciones no se podrán consultar, salvo que así sea requerido por ley.

3.4.2 Información considerada no confidencial

[e27] Los Certificados se consideran no confidenciales

[e28] La información sobre identificación u otra información personal o corporativa que aparezca en las tarjetas y en los certificados se considera no confidencial, salvo que disposiciones o acuerdos especiales así lo dispongan.

4 DISPOSICIONES PRÁCTICAS

[e29] La Autoridad Española y el Centro Español de Personalización tendrán un conjunto de disposiciones de prácticas y procedimientos a seguir para alcanzar los requisitos establecidos en esta política, en adelante, documento de Disposiciones Prácticas. La Autoridad Española será la encargada de aprobar dicho documento.

En concreto:

a) El documento de Disposiciones Prácticas reflejará las obligaciones de todas las organizaciones externas que den apoyo a las Autoridades Españolas de Certificación y de Personalización, incluyendo las políticas y prácticas aplicables.

b) El documento de Disposiciones Prácticas será tratado como información confidencial y estará a disposición de la Autoridad Española. Su consulta por parte de los usuarios del sistema del tacógrafo digital, y de las demás entidades implicadas (por ejemplo los organismos de control) deberá justificarse convenientemente.

   En cualquier caso, no será necesario que las Autoridades Españolas de Certificación y de Personalización pongan a disposición de los usuarios todos los detalles de sus prácticas.

c) Los órganos gestores de las Autoridades Españolas de Certificación y de Personalización deben garantizar que el cumplimiento del documento de Disposiciones Prácticas se realiza correctamente.

d) Las Autoridades Españolas de Certificación y de Personalización definirán un proceso de revisión del documento de Disposiciones Prácticas.

e) Las Autoridades Españolas de Certificación y de Personalización notificarán los cambios proyectados en sus documentos de Disposiciones Prácticas y, una vez que dichos cambios estén aprobados, el nuevo documento de prácticas estará inmediatamente disponible.

5 ADMINISTRACIÓN DE LOS EQUIPOS: TARJETAS Y TACÓGRAFOS.

[e30] La Autoridad Española se asegurará en sus instrucciones a la Autoridad Española de Certificación que los certificados producidos y las claves secretas corresponden a su propósito y únicamente se emplean en las tarjetas y tacógrafos que cumplen el Reglamento (EC) 2135/98.

[e31] La Autoridad Española de Certificación rechazará la emisión de claves y certificados si existe riesgo de su mal uso.

[e32] La Autoridad Española de Emisión y el Centro de Personalización garantizarán el cumplimiento de los procedimientos e instrucciones del Reglamento (EC) 2135/98.

[e33] La Autoridad Española de Emisión y el Centro de Personalización garantizarán los periodos de canje y renovación de tarjetas mencionados en el Reglamento (EC) 2135/98.

[e34] El Centro de Personalización garantizará que la personalización de las tarjetas se lleva a cabo según las instrucciones del Reglamento (EC) 2135/98. La integridad de los datos deberá ser especialmente respetada.

[e35] La Autoridad Española de Certificación y el Centro de Personalización garantizarán que las claves secretas se almacenarán en un entorno seguro.

[e36] La Autoridad Española de Emisión dispondrá de datos suficientes para asociar cada tarjeta a un usuario o portador.

[e37] La Autoridad Española de Emisión garantizará que las tarjetas se entregarán de acuerdo a lo mencionado en el Reglamento (EC) 2135/98 y que el usuario sea identificado personalmente en cualquier momento del proceso de solicitud de la tarjeta o en la entrega de la misma.

[e38] El Centro de Personalización garantizará que las tarjetas de Centro de Ensayo llevarán asignado un PIN que cumpla las instrucciones del Reglamento (EC) 2135/98.

[e39] El PIN se generará en un sistema seguro, de acceso controlado, que garantice su asignación a una única tarjeta de Centro de Ensayo. Una vez generado será impreso y enviado a su destinatario por vía segura y diferente a la de su tarjeta correspondiente.

[e40] La reconstrucción del PIN debe ser imposible.

6 GESTIÓN DE LAS CLAVES

Esta sección contiene las disposiciones para el manejo de:

- la clave raíz europea, clave pública de la Autoridad de Certificación Raíz Europea;
- las claves de estado españolas, es decir, el par de claves Españolas firmado;
- las claves de Sensor de Movimiento;
- las claves de transporte (entre la Autoridad de Certificación Raíz Europea y la Autoridad Española de Certificación).

La **clave pública de la Autoridad de Certificación Raíz Europea** se usa para verificar los certificados españoles.

Las **claves del Estado español** son las claves firmadas de España y también pueden denominarse claves raíz españolas.

Las **claves del sensor de movimiento** son las claves simétricas que se colocan en la tarjeta de centro de ensayo, la unidad para vehículos y en el sensor de movimiento para su reconocimiento mutuo. La Autoridad Española de Certificación recibe las claves del sensor de movimiento de la Autoridad de Certificación Raíz Europea, las almacena y las distribuye a los fabricantes homologados.

Las **claves de transporte** son pares de claves asimétricas empleadas para el intercambio seguro de información entre la Autoridad de Certificación Raíz Europea y la Autoridad Española de Certificación.

Si la Autoridad Española de Certificación necesitara otras claves criptográficas distintas a las mencionadas anteriormente, éstas no se considerarán parte del sistema del tacógrafo digital y no serán objeto de esta política.

6.1 *Clave Pública de la Autoridad de Certificación Raíz Europea*

[e41] La Autoridad Española de Certificación conservará la clave pública de la Autoridad de Certificación Raíz Europea (EUR.PK) de tal forma que se mantenga su integridad y disponibilidad en todo momento.

[e42] La Autoridad Española deberá reconocer el formato de distribución de certificados mencionado en el Anexo B de la política de la Autoridad Europea.

[e43] El Centro Español de Personalización y los fabricantes de equipos se asegurarán que la EUR.PK se inserte en todas las tarjetas de tacógrafo y unidades para vehículos que estén bajo su responsabilidad.

6.2 *Par de claves de la Autoridad Española*

Las claves españolas se usan para firmar todos los certificados generados para los equipos.

El par de claves consiste en una clave pública (ES.PK) y una clave privada o secreta (ES.SK)

[e44] La clave pública de la autoridad española será certificada por la Autoridad de Certificación Raíz Europea, pero será la misma Autoridad Española de Certificación quien la genere.

[e45] La Autoridad Española deberá tener en cuenta el plazo para la firma de las claves requerido por la Autoridad Europea de Certificación.

[e46] La Autoridad Española deberá tener en cuenta el formato de solicitud de certificados mencionado en el Anexo A de la política de la Autoridad Europea.

[e47] La Autoridad Española se asegurará de que las claves se usan exclusivamente para:

- firmas digitales de los equipos del sistema del tacógrafo digital,
- generación de la solicitud de certificación para la Autoridad Europea,
- emisión de Listas de Revocación de Certificados.

6.2.1 Generación del par de claves de la Autoridad Española de Certificación

[e48] El par de claves de la Autoridad Española de Certificación se generará dentro de un dispositivo que:

- cumpla con los requisitos especificados en el nivel 3 de FIPS 140-2 (ó FIPS 140-1) o superior ; o
- cumpla con los requisitos especificados en el Acuerdo CEN de talleres 14167-2 ; o
- sea un sistema de confianza que asegure que cumpla con la EAL 4 o superior según la ISO 15408, con la E3 o superior de la ITSEC, o criterios de seguridad equivalentes.

[e49] La Autoridad Española de Certificación firmará los certificados de equipo en el mismo dispositivo en el que se almacenan las claves privadas de la Autoridad Española.

[e50] Este dispositivo y sus requisitos se recogerán en el documento de Disposiciones Prácticas de la Autoridad Española de Certificación.

[e51] La generación del par de claves de la Autoridad Española requerirá la participación activa de **dos (2)** personas diferentes. Al menos una de ellas tendrá permisos de Administrador de la Autoridad de Certificación ó administrador del Sistema de Personalización.

[e52] La Autoridad Española de Certificación contará al menos con un **mínimo de dos (2)** y un **máximo de cinco (5)** pares de claves españolas, con sus correspondientes certificados firmados para asegurar la continuidad.

6.2.2 Periodo de validez de las claves

[e53] La clave privada española se usará durante un máximo de **dos (2)** años desde la certificación de su correspondiente clave pública, y será destruida por la Autoridad Española de Certificación para evitar posibles futuros malos usos de la misma.

6.2.3 Almacenamiento de la clave privada de la Autoridad Española de Certificación

[e54] Las claves privadas estarán contenidas y serán gestionadas desde un dispositivo anti-manipulación que:

- cumpla con los requisitos especificados en el nivel 3 de FIPS 140-2 (ó FIPS 140-1) o superior; o
- sea un sistema de confianza que asegure que cumpla con la EAL 4 o superior según la ISO 15408, con la E3 o superior de la ITSEC, o criterios de seguridad equivalentes.

[e55] Ninguna persona de forma individual dispondrá de los medios necesarios para acceder al entorno en el que se guardan las claves privadas.

6.2.4 Copia de seguridad de la clave privada de la Autoridad Española de Certificación

[e56] Se podrá disponer de una copia de seguridad de las claves privadas firmadas de la Autoridad Española de Certificación, mediante un proceso de recuperación de claves que requiera al menos doble control. El procedimiento se especificará en el documento de Disposiciones Prácticas de la Autoridad Española de Certificación. Sin embargo, si se usan los pares de claves según lo especificado en el punto [e52] no será necesario hacer copia de seguridad.

6.2.5 Fideicomiso de la clave privada española

[e57] Las claves privadas españolas no se darán en fideicomiso.

6.2.6 Situación de compromiso de las claves españolas

[e58] Existirán instrucciones escritas, incluidas en el documento de Disposiciones Prácticas de la Autoridad Española de Certificación, con las medidas a tomar por parte de los usuarios y los responsables de la seguridad en la Autoridad Española de Certificación y/o de las empresas colaboradoras, en caso de que las claves privadas españolas hayan sido expuestas o cuando se considere o sospeche que ello ha ocurrido.

[e59] En este caso, la Autoridad Española de Certificación informará inmediatamente, a la Autoridad Española, a la Autoridad de Certificación Raíz Europea y al resto de Autoridades de certificación de los Estados Miembros.

6.2.7 Fin de validez de las claves españolas

[e60] La Autoridad Española de Certificación dispondrá de rutinas que aseguren siempre la existencia de un par de claves españolas certificadas.

[e61] Una vez finalizado el uso del par de claves firmadas españolas, la clave pública se guardará y la privada se destruirá de modo que no pueda ser recuperada.

6.3 *Claves del Sensor de Movimiento*

[e62] La Autoridad Española de Certificación podrá solicitar, si le son necesarias, a la Autoridad de Certificación Raíz Europea las claves del sensor de movimiento Km, Km_{VU}, Km_{WC}, (Anexo 1B del Reglamento, apartado 11:3.1.3).

[e63] La Autoridad Española solicitará las claves simétricas para el sensor de movimiento usando el protocolo de petición de distribución de claves (KDR) descrito en el Anexo D de la política de la Autoridad Europea.

[e64] La Autoridad Española de Certificación, cuando lo solicite el fabricante, cifrará los datos de los Sensores de Movimiento (la clave de emparejado K_P y el número de serie extendido N_S) con Km (Anexo 1B del Reglamento, apartado 11:3.1.3). La Autoridad Española de Certificación se asegurará de que la clave del sensor de movimiento (Km) se usa exclusivamente para este propósito

[e65] La Autoridad Española de Certificación enviará la clave de la Unidad para vehículos, Km_{VU} a los fabricantes de unidades para vehículos para su inserción en éstas (Anexo 1B del Reglamento, apartado 11:3.1.3)

[e66] La Autoridad Española de Certificación enviará la clave de centro de ensayo al Centro Español de Personalización para su inserción en las tarjetas de centro de ensayo.

[e67] El Centro Español de Personalización asumirá la tarea de la Autoridad Española de Certificación para asegurar que la clave de centro de ensayo Km_{WC} se inserta en todas las tarjetas de centro de ensayo emitidas (Anexo 1B del Reglamento, apartado 11:3.1.3).

[e68] La Autoridad Española de Certificación y/o el Centro Español de Personalización impedirán el uso no autorizado de las claves del sensor de movimiento y las protegerán durante su almacenamiento, uso y distribución con controles de seguridad físicos y lógicos. Las claves han de estar contenidas y ser gestionadas dentro de un dispositivo criptográfico que no pueda ser manipulado y que:

- cumpla con los requisitos especificados en el nivel 3 de FIPS 140-2 (ó FIPS 140-1) o superior; o
- sea un sistema de confianza que asegure que cumpla con la EAL 4 o superior según la ISO 15408, con la E3 o superior de la ITSEC, o criterios de seguridad equivalentes.

6.4 *Claves de transporte*

[e69] Para garantizar las comunicaciones de datos seguras, la Autoridad Española de Certificación emitirá claves asimétricas especiales de transporte. La Autoridad Española de Certificación, durante el almacenamiento, uso y distribución, protegerá la parte privada de estas claves con controles que garanticen la seguridad física y lógica. Las claves han de estar contenidas y ser gestionadas dentro de un dispositivo criptográfico que no pueda ser manipulado y que:

- cumpla con los requisitos especificados en el nivel 3 de FIPS 140-2 (ó FIPS 140-1) o superior; o
- sea un sistema de confianza que asegure que cumpla con la EAL 4 o superior según la ISO 15408, con la E3 o superior de la ITSEC, o criterios de seguridad equivalentes.

[e70] La Autoridad Española se asegurará de que el identificador de clave (KID) y el módulo de las claves de transporte remitidas a la Autoridad Europea para la certificación y para distribución de las claves del sensor de movimiento son únicos dentro del dominio de la Autoridad Española de Certificación.

[e71] La Autoridad Española se asegurará de que los medios físicos empleados en el transporte de la solicitud de certificación de claves de la Autoridad Española de Certificación, de los certificados de la Autoridad Española de Certificación, de la clave pública de la Autoridad de Certificación Raíz Europea, y de las claves del sensor de movimiento, son los descritos en el Anexo C de la política de la Autoridad Europea.

7 CLAVES DE EQUIPO (ASIMÉTRICAS)

Las claves de equipo son claves asimétricas generadas en algún punto del proceso de emisión/fabricación y certificadas por la Autoridad Española de Certificación para su empleo en el sistema del tacógrafo digital en las:

- tarjetas de tacógrafo
- unidades para vehículos

7.1 *Generalidades sobre las Autoridades Españolas de Certificación y de Personalización y fabricantes de unidades para vehículos*

[e72] En la inicialización del equipo (tarjetas y unidad para vehículos), la introducción de la clave y la personalización se llevará a cabo en un entorno físicamente seguro y vigilado. El acceso a esta área, quedará estrictamente controlado y se requerirá al menos la presencia de dos personas para operar en el sistema. Se guardará registro de las entradas y operaciones efectuadas en el sistema.

[e73] Ninguna información confidencial contenida en los sistemas de generación de claves saldrá del sistema infringiendo la política establecida en este documento.

[e74] Ninguna información confidencial contenida en los sistemas de personalización de los equipos saldrá de los mismos infringiendo la política de este documento.

7.2 *Generación de claves de equipo*

[e75] La entidad que lleva a cabo la generación de claves, se asegurará de que las claves de equipo se generen de forma segura y de que la clave privada del equipo se mantenga en secreto.

[e76] La generación de claves se llevará a cabo en un dispositivo que cumpla:

- cumpla con los requisitos especificados en el nivel 3 de FIPS 140-2 (ó FIPS 140-1) o superior; o
- cumpla con los requisitos especificados en el Acuerdo CEN de talleres 14167-2; o
- sea un sistema de confianza que asegure que cumpla con la EAL 4 o superior según la ISO 15408, con la E3 o superior de la ITSEC, o criterios de seguridad equivalentes; o
- demuestre un sistema de seguridad equivalente a los anteriores.

[e77] El procedimiento de creación y almacenamiento de las claves privadas impedirá su exposición fuera del sistema que las generó. Además, la clave privada será eliminada inmediatamente del sistema después de haber sido insertada en el dispositivo.

[e78] La solicitud de certificación que conlleve el transporte de la clave privada no está permitido.

[e79] Es responsabilidad de la entidad que genera las claves, la toma de medidas adecuadas para asegurar la unicidad de la clave pública en su dominio, antes del proceso de asignación.

7.2.1 Validez de las claves de equipo

[e80] El uso de una clave privada relacionada con los certificados emitidos para los equipos según esta política no excederá nunca el fin de validez del certificado emitido para los mismos.

7.2.2 Protección y almacenamiento de la clave privada de equipo – tarjetas

[e81] El Centro Español de Personalización se asegurará de que la clave privada está protegida por, y restringida a, una tarjeta que ha sido entregada al titular según los procedimientos detallados en esta política.

[e82] Las copias de la clave privada sólo se almacenarán en la tarjeta de tacógrafo. Si durante el proceso de personalización es necesario su uso, las claves se mantendrán cifradas.

7.2.3 Protección y almacenamiento de la clave privada de equipo – unidad para vehículos

[e83] El fabricante de la unidad para vehículos se asegurará de que la clave privada de ésta, así como que sus formas de empleo, estén protegidas por, y restringidas a, dicha unidad para vehículos.

[e84] Las copias de la clave privada sólo se almacenarán en la unidad para vehículos. Si durante el proceso de personalización es necesario su uso, las claves se mantendrán cifradas.

7.2.4 Fideicomiso y archivo de las claves privadas de equipo

[e85] Las claves privadas del equipo no se darán en fideicomiso ni serán archivadas.

7.2.5 Archivo de las claves públicas de equipo

[e86] Todas las claves públicas certificadas por la Autoridad Española de Certificación serán archivadas por la misma.

8 GESTIÓN DEL CERTIFICADO DE EQUIPO

Esta sección describe el ciclo vital del certificado que incluye su función de registro, la emisión del certificado, distribución, uso, renovación y fin de periodo de validez.

8.1 *Entrada de datos*

[e87] En la emisión de los certificados de equipos la Autoridad Española de Certificación verificará la unicidad del número de referencia del titular del equipo (CHR).

8.2 *Certificados de tarjeta de tacógrafo*

8.2.1 Certificados de conductor

[e88] Los certificados de conductor se emiten sólo a aquellas solicitudes correctas de tarjeta de conductor.

1.1.1 Certificados de centro de ensayo

[e89] Los certificados de centro de ensayo se emiten sólo a aquellas solicitudes correctas de tarjeta de centro de ensayo.

8.2.2 Certificados de organismos de control

[e90] Los certificados de organismo de control se emiten sólo a aquellas solicitudes correctas de tarjeta de organismo de control.

8.2.3 Certificados de empresa

[e91] Los certificados de empresa de transporte se emiten sólo a aquellas solicitudes correctas de tarjeta de empresa de transporte.

8.3 *Certificados de unidades para vehículos*

[e92] La Autoridad Española de Certificación emitirá los certificados sólo a fabricantes de unidades para vehículos y a unidades para vehículos homologadas en España.

[e93] Para obtener los certificados de las unidades para vehículos los fabricantes deberán facilitar, al menos:

- los datos identificativos del dispositivo (p.e. homologación y número de serie), o un CRI (Certificate Request Identifier, identificador de petición de certificado) en caso de que el dispositivo no esté aún identificado;
- el nombre completo del fabricante;
- un número de identidad español u otros datos que distingan al fabricante de otros con el mismo nombre.

8.4 *Validez temporal del certificado de equipo*

[e94] Los certificados no tendrán un periodo de validez superior a la validez del correspondiente equipo.

- Los certificados de conductor tendrán un periodo de validez no superior a **cinco (5)** años (Reglamento14.4a)
- Los certificados de centro de ensayo tendrán un periodo de validez no superior a **un (1)** año (Reglamento 12.1)
- Los certificados de organismo de control tendrán un periodo de validez no superior a **cinco (5)** años.
- Los certificados de empresa de transporte tendrán un periodo de validez no superior a **cinco (5)** años.
- Los certificados de unidades para vehículos tendrán un periodo de validez no superior a **treinta (30)** años.

8.5 *Emisión de certificados de equipo*

[e95] La Autoridad Española de Certificación se asegurará de emitir los certificados de modo que preserve su autenticidad e integridad. El contenido del certificado viene definido en el Anexo 1B del Reglamento, apéndice 11.

8.6 *Renovación y modificación del certificado de equipo*

Dado que los certificados y las tarjetas tienen el mismo tiempo de validez, se gestionan juntos. Se asume que el tiempo de vida del equipo es más corto que el del certificado.

8.7 *Tareas informativas de la Autoridad Española de Certificación.*

[e96] La Autoridad Española de Certificación será la responsable de transferir todos los datos existentes sobre certificados, tanto al Centro de Personalización como a los fabricantes. Tanto los certificados como las tarjetas y sus portadores estarán relacionados inequívocamente.

[e97] En el caso de que algunas autoridades estén interesadas en información sobre el funcionamiento de la Autoridad Española de Certificación o de sus contratistas externos, y no exista ninguna norma o consideración de seguridad que impida proporcionar esta información, la Autoridad Española de Certificación facilitará dicha información tan pronto como le sea posible en coordinación con la Autoridad Española.

[e98] El funcionamiento de la Autoridad Española de Certificación se considerará confidencial. La información contenida en dicho centro sólo podrá consultarse en las instalaciones de la Autoridad Española de Certificación, previo acuerdo con la Autoridad Española, siempre y cuando exista un interés legítimo contrastado y el receptor de dicha información se comprometa a mantenerla en secreto.

[e99] La Autoridad Española de Certificación mantendrá disponible información sobre el estado de los certificados.

9 SEGURIDAD DE LA INFORMACIÓN

9.1 *Gestión de la información de la Autoridad Española de Certificación y del Centro Español de Personalización*

[e100] La Autoridad Española de Certificación y el Centro Español de Personalización serán los responsables de todos los servicios de certificación de claves incluso aunque algunas tareas se subcontraten.

[e101] Cualquier cambio que repercuta en el nivel de seguridad deberá ser aprobado por la Autoridad Española.

[e102] La Autoridad Española de Certificación y el Centro Español de Personalización adoptarán un sistema de gestión de seguridad equivalente a la ISO 17799. No se requiere certificación formal de este aspecto.

9.2 *Clasificación y gestión de los recursos de la Autoridad Española de Certificación y el Centro Español de Personalización*

[e103] La Autoridad Española de Certificación y el Centro Español de Personalización se asegurarán de que sus recursos e información están protegidos en un nivel adecuado.

En concreto:

a) La Autoridad Española de Certificación y el Centro Español de Personalización llevarán a cabo un análisis de riesgos para evaluar y determinar las medidas de seguridad necesarias y los procedimientos operativos.

b) La Autoridad Española de Certificación y el Centro Español de Personalización llevarán un inventario con toda la información de sus recursos y asignarán una clasificación para los requisitos de protección de éstos conforme al análisis de riesgos.

9.3 *Controles de seguridad del personal de la Autoridad Española de Certificación y el Centro Español de Personalización*

9.3.1 Perfiles de confianza

[e104] La Autoridad Española de Certificación y el Centro Español de Personalización, de acuerdo a esta política, establecerán **cuatro** perfiles diferentes de usuarios, que se describen a continuación.

[e105] Para garantizar que ninguna persona pueda burlar la salvaguarda, las responsabilidades en los sistemas de la Autoridad Española de Certificación y el Centro Español de Personalización serán desempeñadas por múltiples perfiles e individuos. Cada cuenta del sistema tendrá limitadas sus capacidades de acuerdo con el perfil del propietario de la cuenta.

[e106] Los perfiles son:

a) Controlador de seguridad del sistema de información (ISSO): responsable de la administración del software para el control y la producción de certificados o de los pares de claves RSA.

b) Administrador del Sistema (SA): responsable de la administración del hardware y el sistema operativo. Autorizado para instalar, configurar y mantener el sistema. Responsable de las copias y recuperaciones del sistema

c) Administrador de la Autoridad de Certificación (CAA) o Administrador del Sistema de Personalización (PA): responsables de la operación de los sistemas de la Autoridad de Certificación y el Centro de Personalización respectivamente.

d) Auditor (AU): Autorizado para revisar, mantener y consolidar los archivos y los archivos de auditorias.

9.3.2 Identificación y autentificación para cada perfil

[e107] La identificación y autentificación de los Administradores de la Autoridad de Certificación o del sistema de Personalización de Tarjetas, Administradores del Sistema, Auditores y Controladores de Seguridad del Sistema de Información serán las apropiadas y determinadas en las prácticas, procedimientos y condiciones de esta política.

9.3.3 Requisitos de formación, cualificación, experiencia y autorización

[e108] Todo el personal de la Autoridad Española de Certificación y del Centro Español de Personalización que ostente cargos comprometidos, incluyendo al menos todas las posiciones de Administrador de la Autoridad de Certificación o del Sistema de Personalización de Tarjetas y Controladores de Seguridad del Sistema de Información deberán acreditar:

a) no estar asignados a otras tareas que puedan entrar en conflicto con las responsabilidades derivadas de los perfiles de Administrador de la Autoridad de Certificación o del Sistema de Personalización de Tarjetas y Controlador de Seguridad del Sistema de Información;

b) no haber sido relevados en el pasado de otros puestos por motivos de negligencia o abandono de sus tareas;

c) haber recibido una formación adecuada para el desarrollo de sus responsabilidades.

[e109] La Autoridad Española de Certificación y el Centro Español de Personalización podrán también elaborar unos requisitos específicos, tales como requisitos de ciudadanía, rango, cualificación, comprobación de cuentas bancarias y ausencia de antecedentes criminales. Tales requisitos deberán quedar detallados en el correspondiente documento de Disposiciones Prácticas.

9.3.4 Requisitos de formación

[e110] El personal tendrá una formación adecuada al perfil y trabajo que va a desempeñar.

9.4 *Controles de seguridad del sistema de la Autoridad de Certificación y del Centro de Personalización*

[e111] La Autoridad Española de Certificación y el Centro Español de Personalización se asegurarán de que los sistemas sean seguros y funcionan correctamente con riesgo mínimo de fallo.

En concreto:

- La integridad de los sistemas y de la información se protegerá frente a virus o software dañino o no autorizado.
- Los daños causados por fallos en la seguridad o mal funcionamiento se minimizarán mediante el uso de mecanismos de respuesta e informes de incidentes.

[e112] El Sistema Español de la Autoridad de Certificación así como el Sistema de Personalización proporcionarán los adecuados controles de seguridad para hacer cumplir la separación de perfiles descrita en esta política o en el correspondiente documento de Disposiciones Prácticas.

9.4.1 Requisitos técnicos de seguridad en determinados equipos informáticos

[e113] La inicialización del sistema que trabaja con las claves de certificación privadas de la Autoridad Española de Certificación requerirá la cooperación de **al menos dos personas**, ambas autorizadas por el sistema.

9.4.2 Clasificación de la seguridad en los equipos informáticos

[e114] Los sistemas de certificación y personalización no requerirán una clasificación formal siempre y cuando cumplan todos los requisitos especificados en esta sección.

9.4.3 Controles de desarrollo del sistema

[e115] Se llevará a cabo un análisis de los requisitos de seguridad en cuanto al diseño y a la especificación de requisitos concretos de cualquier proyecto de desarrollo de sistemas llevado a cabo por la Autoridad Española de Certificación o el Centro Español de Personalización o en nombre de las mismas para garantizar que dicha seguridad se lleva a cabo dentro de sistemas de Tecnología de la Información.

[e116] Los procedimientos de cambio de control se emplearán en caso de nuevas versiones y modificaciones para cualquier software operativo.

9.4.4 Controles de gestión de seguridad

[e117] Los perfiles del sistema habrán de ser implementados y de obligado cumplimiento.

9.5 *Procedimientos de auditoría de seguridad*

Los procedimientos de auditoría de seguridad de esta sección serán válidos para todos los equipos informáticos y componentes de sistemas relacionados con la creación de claves, certificados y procesos de emisión de equipos reflejados en esta política.

9.5.1 Tipos de eventos registrados

[e118] Las funciones de auditoría de seguridad relacionadas con los sistemas informáticos o sistemas de la Autoridad Española de Certificación y del Centro Español de Personalización archivarán, a efectos de auditoría:

a) la creación de cuentas (privilegiadas o no);

b) peticiones de transacción junto con el registro de la cuenta peticionaria, tipo de petición e indicación de si la transacción se completó o no y la causa eventual de la transacción incompleta;

c) instalación de software nuevo o de actualizaciones;

d) fecha y hora y otra información relevante sobre las copias de seguridad;

e) apagados y reinicios del sistema;

f) fecha y hora de todas las mejoras de hardware;

g) fecha y hora del volcado de los archivos de auditoría;

h) fecha y hora del volcado de los registros de transacciones.

9.5.2 Frecuencia del proceso del archivo de auditoría

[e119] El archivo de auditoría se procesará con regularidad y se analizará para evitar actuaciones fraudulentas. Los procedimientos de archivo estarán descritos en los correspondientes documentos de Disposiciones Prácticas.

9.5.3 Periodo de conservación del archivo de auditoría

[e120] El archivo de auditoría se conservará al menos durante **2 (dos)** años.

9.5.4 Protección del archivo de auditoría

[e121] Se protegerá convenientemente la integridad de los archivos de auditoría. Todas las entradas tendrán un sello de tiempo (será suficiente con la fecha y hora del sistema).

[e122] Los archivos de auditoría serán verificados y consolidados al menos mensualmente. La verificación la realizará una persona con el perfil de Administrador y la consolidación una con el de Auditor.

9.5.5 Procedimientos de copia de seguridad del archivo de auditoría

[e123] El archivo de auditoría estará protegido frente a accesos no autorizados.

9.5.6 Sistema de ejecución de auditorías (internas frente a externas)

[e124] Sólo se requiere sistema de ejecución de auditorías internas.

9.6 *Archivo de registros*

9.6.1 Tipos de eventos almacenados por la Autoridad Española Emisora de Tarjetas

[e125] Los registros incluirán los hechos relevantes que obren en posesión de la Autoridad Española Emisora de Tarjetas:

a) solicitud de certificados y mensajes relacionados intercambiados con la Autoridad Española de Certificación y el Centro Español de Personalización, usuarios y el directorio;

b) los acuerdos de registro firmados desde la solicitud del usuario para solicitar los certificados y las tarjetas, incluyendo la identidad de la persona responsable de aceptar la aplicación;

c) aceptación firmada de la entrega de tarjetas;

d) acuerdos contractuales relativos a los certificados y tarjetas asociadas;

e) renovación de certificados y todos los mensajes intercambiados con el usuario;

f) mensajes intercambiados con el peticionario y/o usuario.

g) documentos referentes a la política actual y a las implantadas previamente.

9.6.2 Tipos de eventos guardados por la Autoridad Española de Certificación y el Centro Español de Personalización

[e126] Los registros incluirán los hechos relevantes que obren en posesión de la Autoridad Española de Certificación y del Centro Español de Personalización:

a) contenidos de los certificados emitidos;

b) informes de auditoría que incluyan registros de auditorías anuales de la Autoridad Española de Certificación y el Centro Español de Personalización según lo establecido en sus Disposiciones Prácticas;

c) documentos referentes a la política de la Autoridad Española vigente y a las implantadas previamente y sus respectivos documentos de Disposiciones Prácticas;

[e127] Los registros de todas las peticiones electrónicas firmadas digitalmente hechas por la Autoridad Española de Certificación y el Centro Español de Personalización o por el personal (Administrador de la Autoridad de Certificación o del sistema de Personalización de Tarjetas) incluirán los datos del administrador responsable de cada petición junto con toda la información requerida para el no repudio de la petición mientras el registro esté custodiado.

9.6.3 Periodo de custodia de los archivos

[e128] Los archivos se custodiarán y protegerán frente a modificación o destrucción durante el período especificado en el documento de Disposiciones Prácticas.

9.6.4 Procedimientos para obtener y verificar la información archivada

[e129] La Autoridad Española de Certificación y el Centro Español de Personalización actuarán según lo especificado en la sección 3.4 sobre confidencialidad.

[e130] Los registros de transacciones individuales podrán consultarse a petición de cualquiera de las entidades implicadas en la transacción o de sus representantes acreditados.

[e131] La Autoridad Española de Certificación y el Centro Español de Personalización mostrarán, previa petición justificada, su documentación según el correspondiente documento de Disposiciones Prácticas de acuerdo con el apartado 11.5.

[e132] De manera reglada, podría cargarse una tasa razonable para cubrir los gastos ocasionados por las gestiones efectuadas para la recuperación de los archivos.

[e133] Tanto la Autoridad Española de Certificación como el Centro Español de Personalización garantizarán la disponibilidad del archivo y de la información almacenada en un formato legible durante su custodia, incluso en el caso de que las operaciones de la Autoridad Española de Certificación o del Centro Español de Personalización se interrumpan, suspendan o finalicen.

[e134] En el supuesto de que los servicios de la Autoridad Española de Certificación o el Centro Español de Personalización deban interrumpirse, suspenderse o finalizarse; dichos organismos enviarán una notificación a todas las organizaciones clientes para garantizar la disponibilidad ininterrumpida del archivo. Todas las solicitudes de acceso a la información almacenada se enviarán a la Autoridad Española de Certificación y al Centro Español de Personalización o entidad señalada por la Autoridad Española de Certificación y el Centro Español de Personalización antes de la finalización del servicio

9.7 *Plan de continuidad*

[e135] La Autoridad Española de Certificación y el Centro Español de Personalización tendrán un plan de continuidad de negocio (BCP). Esto incluye, pero no está limitado a, eventos tales como:

- compromiso de clave;
- pérdida catastrófica de datos causada por ejemplo por robo, por incendio, fallo del software o hardware;
- otro tipo de fallos del sistema.

9.7.1 Situación de compromiso de las claves españolas

El compromiso de las claves españolas se trata en el apartado 6.2.6.

9.7.2 Recuperación de datos

[e136] La Autoridad Española de Certificación, el Centro Español de Personalización y las empresas colaboradoras dispondrán de rutinas establecidas para prevenir y minimizar los efectos de desastres en el sistema. Dichas rutinas incluirán copias de seguridad de los datos almacenados que sean fiables y se puedan realizar remotamente, procesos de recuperación de datos, etc. que han de detallarse en el BCP.

9.8 *Control de seguridad física*

[e137] Los controles de seguridad física se implantarán para controlar el acceso al hardware y software de la Autoridad Española de Certificación y del Centro Español de Personalización. Se guardará un registro de todas las entradas físicas a esta(s) área(s).

[e138] Las claves españolas para la firma de certificados se guardarán en un entorno protegido física y lógicamente, tal y como se describe en el documento de Disposiciones Prácticas.

[e139] Las instalaciones de la Autoridad Española de Certificación y del Centro Español de Personalización dispondrán de un lugar para almacenar las copias de seguridad y medios de almacenamiento, de forma que se evite la pérdida o manipulación de la información almacenada. Los soportes físicos de las copias de seguridad se guardarán en lugares diferentes a donde se encuentren los sistemas de la Autoridad Española de Certificación y el Centro Español de Personalización para facilitar la recuperación en caso de desastre en las instalaciones de dichos organismos.

[e140] Las comprobaciones de seguridad de los equipos principales de las instalaciones de la Autoridad Española de Certificación y del Centro Español de Personalización, se realizarán semanalmente.

9.8.1 Acceso físico

[e141] El acceso debe ser controlado por el uso de un listado de control a las instalaciones que alojen el sistema. Una persona autorizada escoltará a cualquiera que no aparezca en la lista de control. Si la lista de control no está disponible para alguna instalación en particular, el material sensible de la Autoridad Española de Certificación y el Centro Español de Personalización deberá guardarse en un entorno seguro bajo llave cuando no se utilice.

10 CESE DE ACTIVIDADES

10.1 *Finalización de los servicios*

La finalización de los servicios de la Autoridad Española de Certificación o el Centro Español de Personalización se refiere al cese de la actividad. Este no es el caso en que el servicio sea transferido de una organización a otra o cuando se sustituya el par de claves españolas por otro nuevo o se sustituya la clave de la Autoridad de Certificación Raíz Europea.

[e142] La Autoridad Española garantizará que las tareas enumeradas a continuación se lleven a cabo.

[e143] Antes de que la Autoridad Española de Certificación o el Centro Español de Personalización acaben de prestar sus servicios, habrán de completar al menos los siguientes procedimientos:

a) informar a todos los usuarios y partes relacionadas con los que la Autoridad Española de Certificación y el Centro Español de Personalización mantenga acuerdos u otro tipo de relaciones;

b) poner a disposición pública la información relativa a su disolución con al menos 3 meses de antelación a la misma;

c) la Autoridad Española de Certificación y el Centro Español de Personalización pondrán fin a todas las autorizaciones facilitadas a empresas colaboradoras que actúen en nombre de la Autoridad Española de Certificación y el Centro Español de Personalización en el proceso de emisión de certificados;

d) la Autoridad Española de Certificación y el Centro Español de Personalización facilitarán obligatoriamente los medios para el mantenimiento y el acceso continuo a los archivos al transferirlos a la Autoridad de Certificación Raíz Europea.

10.2 *Traspaso de responsabilidades*

El traspaso de responsabilidades de la Autoridad Española de Certificación y del Centro Español de Personalización tendrá lugar cuando la Autoridad Española decida designar a una nueva Autoridad Española de Certificación o un nuevo Centro Español de Personalización para remplazar a las anteriores.

[e144] La Autoridad Española se asegurará de que el traspaso de responsabilidades y activos pertinentes se lleve a cabo.

[e145] La antigua Autoridad Española de Certificación destruirá todas las claves raíz que estén en su poder.

11 AUDITORÍA

[e146] La Autoridad Española será la responsable de garantizar que la Autoridad Española de Certificación y el Centro Español de Personalización sean auditadas.

11.1 *Frecuencia de la auditoría de conformidad de la entidad*

[e147] Una Autoridad Española de Certificación o el Centro Español de Personalización que actúen según lo especificado en esta política, serán auditadas al menos anualmente. Cuando se audite el funcionamiento de la Autoridad Española de Certificación o el Centro Español de Personalización, se verificará especialmente su coincidencia con los requerimientos de la Autoridad de Certificación Raíz Europea.

11.2 *Temas cubiertos por la auditoría*

[e148] La auditoría abarcará las prácticas de la Autoridad Española de Certificación y del Centro Español de Personalización.

[e149] La auditoría cubrirá también la conformidad de la Autoridad Española de Certificación y del Centro Español de Personalización con la presente política.

11.3 *Quien debe realizar la auditoría*

[e150] La Autoridad Española podrá encargar a una organización de certificación o acreditación externa la aprobación de los documentos de Disposiciones Prácticas de la Autoridad Española de Certificación y del Centro Español de Personalización. También podrá ser la propia Autoridad Española la encargada de llevar a cabo la auditoría.

11.4 *Medidas a tomar en caso de deficiencias*

[e151] En el caso de que existan irregularidades en la auditoría, la Autoridad Española tomará las medidas adecuadas según su gravedad.

11.5 *Comunicación de resultados*

[e152] La Autoridad Española incluirá los resultados de la auditoría en un informe en el que se definan las acciones correctivas y incluyendo una planificación para su implementación, tal como se requiere en las obligaciones de la Autoridad Española. El informe se entregará, en idioma inglés, a la Autoridad de Certificación Raíz Europea.

[e153] Los resultados de las auditorías de un determinado nivel de seguridad podrán consultarse previa petición. Los informes detallados de la auditoría no podrán consultarse salvo que sea necesario el conocimiento detallado de la información que contienen.

12 CAMBIOS DE LOS PROCEDIMIENTOS DE LA POLÍTICA DE LA AUTORIDAD ESPAÑOLA

12.1 *Asuntos que podrían cambiarse sin notificación*

[e154] Los únicos cambios que pueden efectuarse en esta política sin notificar son:

a) correcciones tipográficas o editoriales;

b) cambios en los datos de contacto o denominaciones de organismos.

12.2 *Cambios con notificación*

12.2.1 Aviso

[e155] Cualquier asunto contenido en esta política puede modificarse si se comunica con **noventa (90)** días de antelación.

[e156] Los cambios sobre asuntos que, a juicio de la organización responsable de la política, (la Autoridad Española) no afecten sustancialmente a la mayoría de los usuarios o a terceras partes, podrán modificarse con un plazo de **treinta (30)** días de antelación.

12.2.2 Periodo de alegaciones

[e157] Los usuarios afectados podrán presentar sus alegaciones sobre cambios en la organización de la administración de la política con al menos **quince (15)** días de antelación.

12.2.3 Destinatarios de la información

[e158] La información sobre los cambios en esta política se notificará a:

- ERCA
- E-CP
- fabricantes de unidades para vehículos y sensores de movimiento afectados.

[e159] Si el cambio propuesto en la política viene determinado por comentarios, dicho cambio se notificará con al menos **treinta** (**30)** días de anterioridad a la fecha de su entrada en vigor.

12.3 *Cambios que requieren la aprobación de una nueva política de la Autoridad Española*

[e160] Si la Autoridad Española decide algún cambio en la política, deberá remitirla previamente a la Autoridad Europea de Certificación para su aprobación.

13 CONFORMIDAD CON LA POLÍTICA DE LA AUTORIDAD DE CERTIFICACIÓN RAÍZ EUROPEA

La siguiente tabla muestra la relación de cumplimientos requeridos por la Política de la Autoridad de Certificación Raíz Europea en su párrafo 5.2.3.

Ítem	Referencia de la política de la ERCA	Requerimiento	Referencia de la política E-MSA
1.	5.3.1	La política de cada autoridad deberá identificar las entidades encargadas de cada operación.	1.1 Organizaciones responsables.
2.	5.3.2	Los pares de claves de equipos y del sensor deberán generarse y almacenarse en equipos que bien: a) estén certificados para cumplir las normas FIPS 140-2 (o FIPS 140-1) nivel 3 o superior; b) cumplan las normas CEN Workshop Agreement 14167-2; c) sea un sistema de confianza según EAL4 o superior de acuerdo con ISO 15408; nivel E3 o superior con ITSEC, d) se demuestre que cumple un criterio equivalente de seguridad.	6.2.1 Generación del par de claves de la Autoridad Española de Certificación. [e48] 6.3 Claves del Sensor de Movimiento. [e68]
3.	5.3.3	Los pares de claves de equipos y del sensor deberán generarse en un lugar seguro con personal con adecuado perfil de confianza y, al menos, doble control.	6.2.1 Generación del par de claves de la Autoridad Española de Certificación. [e51] 9.3.1 Perfiles de confianza. [e104] a [e106] 9.4 Controles de seguridad del sistema de la Autoridad de Certificación y del Centro de Personalización. [e111] y [e112] 9.8 Control de seguridad física. [e137] a [e140] 9.8.1 Acceso físico. [e141]
4.	5.3.4	Los pares de claves de equipos deberán utilizarse durante un periodo máximo de dos años a partir de la fecha del certificado de la ERCA.	6.2.2 Periodo de validez de las claves. [e53]

Ítem	Referencia de la política de la	Requerimiento	Referencia de la política E-MSA
5.	5.3.5	Para la generación de nuevas claves para la E-MSA se tendrá en cuenta el mes de plazo requerido por la ERCA.	6.2 Par de claves de la Autoridad Española. [e45]
6.	5.3.6	La E-MSA suministrará a la ERCA las claves públicas para certificar de acuerdo con el protocolo (KCR) descrito en el Anexo A de la política de la ERCA.	6.2 Par de claves de la Autoridad Española. [e46]
7.	5.3.7	La E-MSA solicitará a la ERCA las claves del sensor de movimiento de acuerdo al protocolo (KCR) descrito en el Anexo D de la política de la ERCA.	6.3 Claves del Sensor de Movimiento. [e63]
8.	5.3.8	La E-MSA reconocerá la clave pública de la ERCA con el formato descrito en el Anexo B de la política de la ERCA.	6.1 Clave Pública de la Autoridad de Certificación Raíz Europea. [e42]
9.	5.3.9	La E-MSA empleará el medio físico descrito en el Anexo C para el transporte de claves y certificados.	6.4 Claves de transporte. [e71]
10.	5.3.10	La E-MSA se asegurará que la clave de identificación (KID) y el módulo *(n)* de las claves enviadas a la ERCA son únicos en su ámbito de aplicación.	6.4 Claves de transporte. [e70]
11.	5.3.11	La E-MSA se asegurará de que las claves caducadas no se empleen para ningún otro propósito. Dicha clave privada será destruida o guardada de forma que se impida su uso.	6.2.2 Periodo de validez de las claves. [e53]

Ítem	Referencia de la política de la	Requerimiento	Referencia de la política E-MSA
12.	5.3.12	La E-MSA se asegurará que las claves RSA para equipos se generan, transportan e insertan en el equipo de forma que se preserve su confidencialidad e integridad. Para ello, la E-MSA deberá: • cerciorarse de que se cumplen cualesquiera recomendaciones pertinentes del certificado de seguridad del equipo. • asegurarse que tanto la generación como la inserción (si no es en la placa) se realiza en un lugar controlado; • a menos que la generación de la clave se haga con equipo certificado de seguridad, emplear algoritmos criptográficos de cálculo apropiados; Estos dos últimos requisitos para la generación deberán cumplirse por un aparato que bien: a) esté certificado para cumplir las normas FIPS 140-2 (o FIPS 140-1) nivel 3 o superior; b) cumpla las normas CEN Workshop Agreement 14167-2; c) sea un sistema de confianza según EAL4 o superior de acuerdo con ISO 15408; nivel E3 o superior con ITSEC, d) o se demuestre que cumple un criterio equivalente de seguridad.	5 Administración de los equipos: Tarjetas y tacógrafos. [e35] 7.1 Generalidades sobre las Autoridades Españolas de Certificación y de Personalización y fabricantes de unidades para vehículos. [e72] 7.2 Generación de claves de equipo. [e75] y [e76] .

Ítem	Referencia de la política de la	Requerimiento	Referencia de la política E-MSA
13.	5.3.13	La E-MSA asegurará confidencialidad, integridad y disponibilidad de las claves privadas generadas, almacenadas y empleadas bajo control de la política de la E-MSA.	3.4.1 Información considerada confidencial. [e23] a [e25] 5 Administración de los equipos: Tarjetas y tacógrafos. [e34] 6.2.1 Generación del par de claves de la Autoridad Española de Certificación. [e49] a [e52] 6.2.3 Almacenamiento de la clave privada de la Autoridad Española de Certificación. [e54] y [e55] 6.4 Claves de transporte. [e69] 7.1 Generalidades sobre las Autoridades Españolas de Certificación y de Personalización y fabricantes de unidades para vehículos [e73] y [e74] 7.2 Generación de claves de equipo. [e75] a [e78] . 7.2.2 Protección y almacenamiento de la clave privada de equipo – tarjetas. [e81] y [e82] 7.2.3 Protección y almacenamiento de la clave privada de equipo – unidad para vehículos. [e83] y [e84]
14.	5.3.14	La E-MSA evitará el uso inadecuado de las claves privadas generadas, almacenadas y empleadas en su proceso.	3.1.1 Obligaciones de la Autoridad Española y de la Autoridad Española Emisora de Tarjetas. [e4] g).
15.	5.3.15	Las claves de la E-MSA podrán ser recuperadas mediante un procedimiento de recuperación que requiera como mínimo un control doble.	6.2.4 Copia de seguridad de la clave privada de la Autoridad Española de Certificación. [e56]

Ítem	Referencia de la política de la	Requerimiento	Referencia de la política E-MSA
16.	5.3.16	No se permitirán solicitudes de certificación que requieran transporte de claves privadas.	7.2 Generación de claves de equipo. [e78]
17.	5.3.17	El fideicomiso de claves está prohibido.	6.2.5 Fideicomiso de la clave privada española. [e57] 7.2.4 Fideicomiso y archivo de las claves privadas de equipo. [e85]
18.	5.3.18	La E-MSA deberá impedir el uso no autorizado de sus claves de transporte.	3.4.1 Información considerada confidencial. [e25] 6.3 Claves del Sensor de Movimiento. [e68]
19.	5.3.19	La E-MSA se asegurará que la clave maestra del sensor (Km) se empleará únicamente para cifrar datos procedentes del sensor. Los datos a cifrar se definen en norma la ISO / IEC 16844-3.	6.3 Claves del Sensor de Movimiento. [e64]
20.	5.3.20	La clave maestra (Km) del sensor de movimiento no deberá nunca salir de la zona de seguridad controlada de la E-MSA.	6.3 Claves del Sensor de Movimiento. [e64] y [e68]
21.	5.3.21	La E-MSA transmitirá la clave de transporte del sensor (Km_{WC}) al personalizador de forma segura y para el único propósito de su inserción en las tarjetas de Centro de Ensayo.	6.3 Claves del Sensor de Movimiento. [e66]
22.	5.3.22	La E-MSA transmitirá la clave de transporte del sensor (Km_{VU}) al personalizador de forma segura y para el único propósito de su inserción en las unidades vehiculares.	6.3 Claves del Sensor de Movimiento. [e65]
23.	5.2.23	La E-MSA mantendrá la confidencialidad, integridad y disponibilidad de todas las copias de las claves del sensor.	6.3 Claves del Sensor de Movimiento. [e68]

Ítem	Referencia de la política de la	Requerimiento	Referencia de la política E-MSA
24.	5.3.24	La E-MSA se asegurará que sus copias de las claves del sensor están almacenadas en un dispositivo que bien cumpla: a) esté certificado para cumplir las normas FIPS 140-2 (o FIPS 140-1) nivel 3 o superior; b) sea un sistema de confianza según EAL4 o superior de acuerdo con ISO 15408; nivel E3 o superior con ITSEC, o criterios de seguridad equivalentes. Estas evaluaciones se aplicarán a perfiles de protección o de seguridad.	6.3 Claves del Sensor de Movimiento. [e68]
25.	5.3.25	La E-MSA deberá tener varios pares de claves para la producción de tarjetas y unidades vehiculares.	No aplicable. No se incluyen fabricantes de Unidades para Vehículos en el sistema español del tacógrafo digital.
26.	5.3.26	La E-MSA deberá asegurarse de la disponibilidad de su servicio de certificación de claves públicas.	6.2.1 Generación del par de claves de la Autoridad Española de Certificación. [e52]
27.	5.3.27	La E-MSA empleará sus claves privadas de Estado únicamente para: a) la producción de certificados para equipos empleando el algoritmo ISO / IEC 9796-2 descrito en apéndice 11 *Common Security Mechanisms* del Anexo 1 B b) solicitud de certificados de la ERCA según se describe en el Anexo A. c) emisión de listas de revocación si se emplea ese método para dar información de certificados (ver 5.3.30 de la Política de la ERCA).	6.2 Par de claves de la Autoridad Española. [e47]
28.	5.3.28	La E-MSA firmará los certificados de equipo en el mismo dispositivo que almacene sus claves privadas (ver 5.3.2 de la Política de la ERCA).	6.2.1 Generación del par de claves de la Autoridad Española de Certificación. [e49]
29.	5.3.29	Dentro de su ámbito, la E-MSA se asegurará que sus claves públicas para los equipos se identifican de forma única según lo dispuesto en el Anexo 1 B.	8.1 Entrada de datos. [e87]

Ítem	Referencia de la política de la	Requerimiento	Referencia de la política E-MSA
30.	5.3.30	A menos que la generación de claves y la certificación se lleven a cabo en la misma zona de seguridad, la petición de claves se hará con verificación de origen e integridad y sin revelar la calve privada.	7.2 Generación de claves de equipo. [e75] a [e78] 7.2.2 Protección y almacenamiento de la clave privada de equipo – tarjetas. [e81] y [e82] 7.2.3 Protección y almacenamiento de la clave privada de equipo – unidad para vehículos. [e83] y [e84]
31.	5.3.31	La E-MSA mantendrá disponible la información sobre el estado de sus certificados.	8.7 Tareas informativas de la Autoridad Española de Certificación. [e99]
32.	5.3.32	La validez del certificado de las tarjetas equivaldrá al de la tarjeta.	8.4 Validez temporal del certificado de equipo. [e94]
33.	5.3.33	La E-MSA evitará la inserción de certificados de validez indefinida.	8.4 Validez temporal del certificado de equipo. [e94]
34.	5.3.34	La E-MSA permitirá la inserción de certificados de validez indefinida en las unidades vehiculares.	8.4 Validez temporal del certificado de equipo. [e94]
35.	5.3.35	La E-MSA The MSA shall ensure that users of cards are identified al some stage of the card issuing process.	5 Administración de los equipos: Tarjetas y tacógrafos. [e37]
36.	5.3.36	La E-MSA notificará inmediatamente a la ERCA la perdida, robo o compromiso de sus claves.	6.2.6 Situación de compromiso de las claves españolas. [e59]
37.	5.3.37	La E-MSA implantará mecanismos apropiados de recuperación ante desastres que no dependan del tiempo de respuesta de la ERCA.	6.2.1 Generación del par de claves de la Autoridad Española de Certificación. [e52] 9.7 Plan de continuidad. [e135]
38.	5.3.38	La E-MSA establecerá un Sistema de Información de Seguridad basado en un estudio de riesgos para todas las operaciones afectadas..	9.1 Gestión de la información de la Autoridad Española de Certificación y del Centro Español de Personalización. [e102]

Ítem	Referencia de la política de la	Requerimiento	Referencia de la política E-MSA
39.	5.3.39	La E-MSA asegurará una adecuada política de formación al personal, asignación de tareas y autorizaciones.	9.3 Controles de seguridad del personal de la Autoridad Española de Certificación y el Centro Español de Personalización. [e104] a [e110]
40.	5.3.40	La E-MSA mantendrá registros de las operaciones de certificación.	9.6.2 Tipos de eventos guardados por la Autoridad Española de Certificación y el Centro Español de Personalización. [e126] y [e127]
41.	5.3.41	La E-MSA incluirá en su política previsiones en caso de cese.	10.1 Finalización de los servicios. [e142] y [e143]
42.	5.3.42	La E-MSA incluirá un procedimiento de cambios.	12 Cambios de los procedimientos de la Política de la Autoridad Española. [e155] a [e160]
43.	5.3.43	La E-MSA auditará que los requisitos establecidos en esta sección son operativos.	11.1 Frecuencia de la auditoría de conformidad de la entidad. [e147]
44.	5.3.44	La E-MSA auditará las operaciones establecidas en su política en periodos no superiores a 12 meses.	11.1 Frecuencia de la auditoría de conformidad de la entidad. [e147]
45.	5.3.45	La E-MSA remitirá a la ERCA en ingles los resultados de la auditoria mencionada en 5.3.43.	11.5 Comunicación de resultados. [e152]
46.	5.3.46	La auditoria definirá aquellas acciones correctivas, incluyendo un calendario de implantación, requeridas para cumplir las obligaciones de la E-MSA.	11.5 Comunicación de resultados. [e152]

14 REFERENCIAS

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Gru de Trabajo de Emisión de Tarjetas, 16 de noviembre 2001(provisional), propiedad de la Comisión.

[CC] Criterios comunes ISO/IEC 15408 (1999): "Informati technology-Security techniques-Evaluation criteria for security (partes de la 1 a la 3)".

[CEN] CEN Workshop Agreement 14167-2: Módulo Criptográfi para Operaciones Firmadas CSP – Perfil de Protecci (MCSO-PP)

[ETSI 102 042] ETSI TS 102 042. Requerimientos de la Política para emisi de certificados de clave pública para autoridades certificación.

[FIPS] FIPS PUB 140-2 (25 de mayo de 2001): "Secur Requirements for Cryptographic Modules". Informati Technology Laboratory, National Institute of Standards a Technology (NIST).

[ISO 17799] BS ISO/IEC 17799: 2000. Information Technology -- Code practice for information security management.

[CSG] Guía de Seguridad Común, Proyecto de Emisión de Tarjeta (provisional), propiedad de la Comisión

[ERCA POLICY] Política de la Autoridad de Certificación Raíz Europea para Sistema del Tacógrafo Digital. Borrador versión 2.0

15 GLOSARIO DE TÉRMINOS Y ABREVIATURAS

15.1 *Glosario/Definiciones*

Política de la Autoridad Española: Conjunto de normas que indican la aplicabilidad de las claves, certificados y equipo respecto a un colectivo concreto y/o clase de aplicación con requisitos comunes de seguridad.

Tarjeta/Tarjetas de tacógrafo: Tarjeta dotada de un circuito integrado; en esta política equivale a los términos "**tarjeta IC"** y **"Tarjeta Inteligente**"

Usuario de Tarjeta Persona u organización que es titular y usuario de la tarjeta de tacógrafo. Incluye a los conductores, representantes de las compañías de transporte, mecánicos y personal de cuerpos de control.

Certificado: en un contexto general, el certificado es una estructura de mensaje que contiene una firma introducida por el emisor, certificando que la información contenida en el certificado es correcta y que el titular de la clave pública certificada puede probar que posee la clave privada asociada.

Sistema de la Autoridad de Certificación (CAS): El sistema informático en el que se emiten los certificados para los datos de un usuario firmándolos con la clave privada firmada de la CA.

Equipos: En el sistema del tacógrafo digital figuran los siguientes equipos: Tarjetas de tacógrafo, unidades para vehículos y Sensores de Movimiento.

Fabricante/fabricante de equipos: Fabricantes de equipos de tacógrafo. En esta política se alude a ellos como fabricantes de unidades para vehículos y fabricantes de Sensores de Movimiento, dado que cada uno desempeña un papel diferente dentro del sistema.

Clave de sensor de movimiento: Clave simétrica empleada para que los sensores de movimiento y las unidades para vehículos se reconozcan entre sí.

Disposiciones practices (PS): Disposiciones sobre las medidas de seguridad a tomar en los procesos del tacógrafo. El documento de Disposiciones Prácticas es equivalente al documento estándar de PKI, Disposiciones Prácticas de certificación.

Clave privada: La parte privada de un par de claves asimétrico utilizada en las técnicas de cifrado de la clave pública. La clave privada se suele utilizar para firmar digitalmente o descifrar mensajes. También se la conoce como clave secreta.

Clave pública: La parte pública de un par de claves asimétrico utilizada en las técnicas de cifrar para claves públicas. La clave pública se suele utilizar para verificar firmas digitales o para cifrar mensajes dirigidos al titular de la clave privada.

Claves RSA: RSA es un algoritmo criptográfico utilizado para claves asimétricas (PKI) en el sistema del tacógrafo digital.

Empresas colaboradoras: Una entidad, subcontratista, que asume las tareas en nombre de la Autoridad Española de Certificación, o del Centro Español de Personalización.

Tarjetas de tacógrafo/tarjetas: Existen cuatro tipos de tarjetas inteligentes usadas en el sistema del tacógrafo digital: de conductor, de empresa, de centro de ensayo y de control.

Usuario: Son los usuarios del equipo, tanto los **titulares** de tarjetas como los **fabricantes** de unidades para vehículos o de Sensores de Movimiento. Todos los usuarios serán entidades identificables individualmente.

En este documento:

Firmado: cuando esta política requiera una firma, esta será una firma digital segura y verificable que cumpla las especificaciones.

Escrito: cuando esta política requiera que la información esté por escrito, se hará mediante un mensaje de datos si la información contenida es accesible para ser empleada por las partes implicadas.

15.2 *Lista de abreviaturas*

CA	Autoridad de Certificación
CAA/PA	Administrador de la Autoridad de Certificación/Administrador del sistema de Personalización de Tarjetas.
CAS	Sistema de la Autoridad de Certificación
CIA	Autoridad Emisora de Tarjetas
CC	Criterios comunes
CP	Centro de Personalización de Tarjetas
CPS	Disposiciones Prácticas de Certificación
E-CIA	Autoridad Española Emisora de Tarjetas
E-CP	Centro Español de Personalización
E-MSA	Autoridad del Estado Español
E-MSCA	Autoridad Española de Certificación
ERCA	Autoridad de Certificación Raíz Europea
ISSO	Responsable de la seguridad del sistema de información
ITSEC	Criterios de Evaluación de la Seguridad en Tecnología de la Información
KG	Generación de claves
KCR	Petición de certificación de clave
KDR	Petición de distribución de clave (para el Sensor de Movimiento)
KDM	Mensaje de distribución de clave (clave cifrada del Sensor de Movimiento)
MS	Estado Miembro
MSA	Autoridad del Estado Miembro
MSCA	Autoridad de Certificación del Estado Miembro
PIN	Número de Identificación Personal
PKI	Infraestructura de Clave Pública
RSA	Un algoritmo específico de clave pública
SA	Administrador del Sistema
PS	Disposiciones Prácticas
VU	Unidad para vehículos
VUP	Organización de Personalización de las unidades para vehículos