Nota técnica para empresas desarrolladoras de software TicketBAI

Cambio de la cadena de certificación SSL/TLS de los servicios TicketBAI de Araba, Bizkaia y Gipuzkoa

Pruebas externas o preproducción	**1 de octubre de 2026**
Producción	**Previsto entre noviembre de 2026 y enero de 2027. Se comunicará con antelación en cada sede electrónica**

Importante

Aunque esta comunicación se centra en los servicios TicketBAI, las recomendaciones incluidas pueden resultar igualmente aplicables a otras integraciones máquina a máquina con servicios electrónicos de las Diputaciones Forales cuando éstos utilicen certificados asociados a la nueva infraestructura de certificación.

1. Objeto de la comunicación

Las Diputaciones Forales de Araba, Bizkaia y Gipuzkoa van a renovar los certificados SSL/TLS que protegen las comunicaciones con sus servicios TicketBAI.

Como consecuencia de esta renovación, se producirá un cambio en la cadena de certificación presentada por los servidores HTTPS de TicketBAI de los tres territorios. Los nuevos certificados estarán asociados a una nueva jerarquía de certificación de Sectigo, en sustitución de la cadena utilizada actualmente.

El cambio afecta al certificado presentado por los servidores de destino al establecer la conexión HTTPS. No afecta a los certificados de dispositivo o de firma utilizados por las aplicaciones, ni modifica el formato de los mensajes TicketBAI, los servicios funcionales o los mecanismos de identificación y firma de los ficheros.

Para preparar este cambio, deberán incorporarse al almacén de confianza las CAs indicadas en esta nota técnica, sin eliminar las CAs de confianza ya existentes que sigan siendo necesarias para validar otros servicios o cadenas de certificación.

La comunicación tiene carácter conjunto porque una misma solución de software puede operar en más de un territorio, con independencia de la diputación en la que se haya registrado inicialmente.

Este cambio también deberá ser tenido en cuenta por las empresas desarrolladoras o responsables de integraciones máquina a máquina con otros servicios de las diputaciones forales, como SII, SILICIE, Factura Electrónica u otros servicios equivalentes. Cuando estos servicios utilicen certificados asociados a la nueva jerarquía, las indicaciones relativas a la actualización de los almacenes de confianza y a la realización de pruebas resultarán igualmente aplicables.

2. Descripción del cambio

Cuando una aplicación se conecta mediante HTTPS a un servicio TicketBAI, el servidor presenta un certificado electrónico para acreditar su identidad y establecer una comunicación cifrada.

Tras la renovación, los servidores TicketBAI de Araba, Bizkaia y Gipuzkoa presentarán certificados emitidos bajo la nueva jerarquía de certificación de Sectigo.

Para validar correctamente las conexiones, las aplicaciones deberán disponer en su almacén de confianza de las CAs necesarias para construir una ruta de certificación válida.

3. Nueva cadena de certificación y actualización de los almacenes de confianza

Las tres diputaciones utilizarán una cadena de certificación cuya ruta de confianza finalizará en la CA raíz USERTrust.

De forma simplificada, la cadena será la siguiente:

Certificado SSL/TLS del servicio TicketBAI
↓
CA subordinada de Izenpe
↓
CA de la nueva jerarquía de Sectigo
↓
Certificado cruzado de Sectigo
↓
USERTrust RSA Certification Authority

La nueva jerarquía de Sectigo dispone de una ruta directa hacia su propia CA raíz. No obstante, los servidores TicketBAI de Araba, Bizkaia y Gipuzkoa presentarán la cadena que permite construir una ruta de confianza hasta USERTrust.

Esta configuración tiene como objetivo ampliar la compatibilidad con aplicaciones, dispositivos y sistemas antiguos que ya disponen de la CA raíz USERTrust en su almacén de confianza, pero que pueden no disponer todavía de la nueva CA raíz de Sectigo.

El certificado cruzado de Sectigo permite que estos sistemas construyan una ruta válida desde el certificado del servicio TicketBAI hasta la CA raíz USERTrust que ya tienen instalada. De este modo, se reduce el riesgo de interrupciones durante la transición a la nueva jerarquía de certificación.

Las empresas desarrolladoras que utilicen un almacén de confianza propio deberán verificar que dicho almacén permite validar la nueva cadena de certificación. Para ello, se deberá incorporar la CA raíz Sectigo Public Server Authentication Root R46.

La instalación de esta raíz permitirá que las aplicaciones estén preparadas para validar directamente la nueva jerarquía de certificación de Sectigo y no dependan exclusivamente de la ruta de compatibilidad hacia USERTrust. No es necesario instalar la raíz USERTrust como consecuencia de este cambio; la ruta de compatibilidad está destinada a sistemas que ya disponen de dicha raíz en su almacén de confianza.

No deberán incorporarse al almacén de confianza los certificados finales de los servidores presentados por las Diputaciones Forales. Estos certificados tienen un periodo de validez limitado y serán renovados periódicamente. Confiar directamente en ellos obligaría a actualizar de nuevo el software o su almacén con cada renovación.

Los certificados finales serán diferentes para cada servicio y entorno, puesto que estarán asociados a sus respectivos nombres DNS. Sin embargo, los servicios TicketBAI de Araba, Bizkaia y Gipuzkoa utilizarán la misma jerarquía y la misma ruta de certificación hacia USERTrust.

4. Preparación para futuros certificados basados en curvas elípticas

El cambio previsto para 2026 utilizará certificados y cadenas de certificación basados en RSA. No está previsto que en este cambio se utilicen certificados SSL/TLS basados en criptografía de curvas elípticas.

No obstante, con el objetivo de reforzar la seguridad criptográfica, en el futuro podría ser necesario utilizar certificados SSL/TLS basados en curvas elípticas o ECC.

Sectigo dispone de una jerarquía específica para este tipo de certificados. La CA raíz correspondiente es Sectigo Public Server Authentication Root E46.

Por este motivo, se recomienda incorporar también de forma preventiva al almacén de confianza la CA raíz Sectigo Public Server Authentication Root E46.

Esta incorporación permitirá preparar las aplicaciones para una futura transición a certificados SSL/TLS basados en curvas elípticas y reducir la necesidad de actualizar nuevamente los almacenes de confianza.

La instalación de esta CA raíz no significa que los servicios TicketBAI vayan a utilizar inmediatamente certificados de curvas elípticas. Cualquier cambio futuro de este tipo se comunicará previamente.

La incorporación de la raíz E46 al almacén de confianza tampoco garantiza, por sí sola, la compatibilidad con certificados de curvas elípticas. La aplicación, el sistema operativo y las bibliotecas TLS utilizadas deberán ser compatibles con los algoritmos y curvas criptográficas correspondientes.

5. Calendario del cambio

5.1. Entornos de pruebas externas o preproducción

Está previsto que los nuevos certificados SSL/TLS se instalen en los entornos de pruebas externas o preproducción de TicketBAI de Araba, Bizkaia y Gipuzkoa el 1 de octubre de 2026.

A partir de esa fecha, las empresas desarrolladoras deberán probar la correcta conexión de sus aplicaciones con los entornos correspondientes y realizar los envíos de prueba que consideren necesarios.

La actualización deberá realizarse mediante la incorporación de los certificados de CA requeridos, sin eliminar del almacén de confianza otros certificados de CA que continúen siendo necesarios.

Una conexión HTTPS establecida correctamente con los entornos de preproducción, sin errores de validación de certificados, constituirá evidencia suficiente de que la aplicación está preparada para la nueva jerarquía de certificación.

5.2. Entornos de producción

La fecha de instalación de los nuevos certificados en el entorno de producción de cada Diputación Foral es probable que sea diferente, y se prevé que se sitúe entre noviembre de 2026 y enero de 2027. No obstante, se comunicará con antelación en cada una de las sedes electrónicas de las Diputaciones Forales.

6. Descarga de los certificados de CA

6.1. Certificado necesario para el cambio previsto

- **CA raíz Sectigo Public Server Authentication Root R46:**
  https://www.izenpe.eus/contenidos/informacion/descargas_tecnica/es_def/adjuntos/SECTIGO/SectigoPublicServerAuthenticationRootR46_ROOT.crt.cer

Las aplicaciones deberán confiar en la CA raíz Sectigo Public Server Authentication Root R46. Los certificados subordinados, intermedios y cruzados serán presentados por los servicios para construir la ruta de certificación correspondiente.

6.2. Certificado recomendado para una futura transición a curvas elípticas

- **CA raíz Sectigo Public Server Authentication Root E46:**
  https://www.izenpe.eus/contenidos/informacion/descargas_tecnica/es_def/adjuntos/SECTIGO/SectigoPublicServerAuthenticationRootE46_ROOT.crt.cer

La instalación de esta CA raíz es una medida preventiva y no forma parte de la cadena RSA que presentarán inicialmente los servicios TicketBAI.

7. Soporte y comunicación de incidencias

Las dudas o incidencias deberán comunicarse a la diputación correspondiente al servicio con el que se esté realizando la prueba o el envío.

Una misma empresa puede operar con más de un territorio. En ese caso, deberá dirigirse al contacto del territorio en cuyo servicio se produzca la incidencia.

	Araba	Bizkaia	Gipuzkoa
	945 18 15 30	946 083 566	943 113 000
	egoitza.sede@araba.eus	programak@bizkaia.eus	ticketbaikontsultak@gipuzkoa.eus

Información que deberá aportarse en las incidencias: licencia de software y versión, entorno afectado, URL del servicio, fecha y hora de la prueba y mensaje de error completo.

8. Recomendación general de mantenimiento

Como buena práctica general de seguridad, se recomienda mantener actualizados los almacenes o contenedores de confianza utilizados por las aplicaciones. Cuando se utilicen almacenes propios, deberá revisarse periódicamente la incorporación de las CAs de confianza necesarias, tomando como referencia los almacenes mantenidos por los principales sistemas operativos y plataformas.

Asimismo, se recomienda mantener actualizadas las bibliotecas criptográficas y componentes TLS utilizados para el establecimiento y validación de conexiones seguras.

Estas medidas facilitan la incorporación de nuevas autoridades de certificación de confianza y reducen el riesgo de incidencias derivadas de futuros cambios en las jerarquías de certificación utilizadas por los servicios electrónicos.