Servicio de certificación

GUÍA DEL ADMINISTRADOR

Revisión: 19/10/2018

Contenido

Copyright © Acronis International GmbH, 2002-2018

1 Acerca del servicio de certificación

El servicio de certificación es una solución basada en la tecnología de cadena de bloques que le permite hacer lo siguiente:

- Certificar archivos ante notario.
- Comprobar si un archivo certificado ante notario (o su copia) es auténtico y no se ha modificado desde su certificación.
- Enviar un archivo a varias personas para que lo firmen electrónicamente y, a continuación, validar el certificado de firma.

Este servicio está disponible a través de una interfaz web denominada "consola de certificación".

1.1 Cómo funciona la certificación

Para certificar un archivo ante notario, debe cargarlo en el almacenamiento en la nube. Después de cargar el archivo, el servicio de certificación calcula una huella digital (conocida como "código hash") de este. El código hash es único para cada archivo.

Nota *La interfaz de programación de aplicaciones (API) del servicio de certificación le permite certificar un archivo ante notario sin tener que cargarlo en el almacenamiento en la nube. En su lugar, se puede utilizar el hash del archivo que se ha generado previamente. Para obtener más información acerca del uso de la API, consulte "Gestión de claves de API" (pág. 8).*

A continuación, el servicio de certificación envía el código hash a la base de datos basada en la tecnología de cadena de bloques de Ethereum. Dicha base de datos garantiza que el código hash permanezca inalterado.

Para comprobar la autenticidad de un archivo, el servicio calcula su código hash y lo compara con el código hash almacenado en la base de datos. Si los códigos coinciden, queda garantizado que se trata del mismo archivo y que no se ha modificado.

1.2 Administradores y usuarios

Existen dos tipos de cuentas de usuario en el servicio de certificación: las cuentas de administrador y las cuentas de usuario.

Tanto los administradores como los usuarios tienen acceso a todas las funciones del servicio de certificación en la consola de certificación. No obstante, solo los administradores pueden gestionar las claves de API del servicio de certificación y utilizar la API de certificación.

Asimismo, se puede asignar a un administrador del servicio de certificación la función de administrador de empresa. Esta función da acceso al portal de gestión, donde el administrador puede gestionar cuentas de usuario, cuotas, notificaciones e informes.

Los usuarios, administradores y administradores de empresa solo tienen acceso a sus propios archivos certificados ante notario y firmados. Los administradores solo tienen acceso a sus propias claves de API.

Copyright © Acronis International GmbH, 2002-2018

1.3 Limitaciones

- Los archivos que ocupen más de 1 GB no se pueden certificar ante notario a través de la consola de certificación. Esto solo es posible a través de la API de servicios de certificación. Para ello, se envía un hash previamente calculado de un archivo al servicio de certificación.
- Los archivos que ocupen más de 1 GB no se pueden firmar a través de la consola de certificación. Esto solo es posible a través de la API del servicio de certificación. Para ello, se envía a dicho servicio un enlace al archivo.

1.4 Navegadores web compatibles

La interfaz web es compatible con los siguientes navegadores web:

- Google Chrome 29 o posterior
- Mozilla Firefox 23 o posterior
- Opera 16 o posterior
- Windows Internet Explorer 11 o posterior
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en los sistemas operativos macOS y iOS

En otros navegadores web (incluido Safari para otros sistemas operativos), es posible que la interfaz de usuario no se muestre correctamente o que algunas funciones no estén disponibles.

2 Utilización del servicio de certificación

2.1 Activación de la cuenta

Tras registrarse en el servicio, recibirá un correo electrónico con la siguiente información:

- **Un enlace de activación de cuenta**. Haga clic en el enlace y establezca la contraseña de la cuenta. Recuerde su usuario, el cual aparece en la página de activación de la cuenta.
- **Un enlace a la página de inicio de sesión a la consola de certificación**. Este enlace le permitirá acceder a la consola en el futuro. El usuario y la contraseña son los mismos que en el paso anterior.

2.2 Acceso a la interfaz web del servicio de certificación

Puede iniciar sesión en el servicio de certificación si ha activado su cuenta.

Cómo iniciar sesión en el servicio de certificación

1. Vaya a la página de inicio de sesión del servicio de certificación. La dirección de la página de inicio de sesión se incluye en el correo electrónico de activación.
2. Escriba el usuario y luego haga clic en **Continuar**.
3. Escriba la contraseña y luego haga clic en **Iniciar sesión**.
4. Si tiene la función de administrador de empresa, haga clic en **Certificación**.

   Los usuarios que no tienen asignada la función de administrador de empresa inician sesión directamente en la consola de certificación.

Puede cambiar el idioma de la interfaz web si hace clic en el icono de la cuenta que hay en la esquina superior derecha.

Copyright © Acronis International GmbH, 2002-2018

Si **Certificación** no es el único servicio al que está suscrito, puede cambiar de un servicio a otro con el  icono de la esquina superior derecha. Los administradores de empresa también pueden usar este icono para pasar al portal de gestión.

2.3 Certificación de archivos

Cómo certificar archivos ante notario

1. Haga clic en **Archivos certificados ante notario**.
2. Si no hay archivos certificados ante notario, haga clic en **Examinar**. Haga clic en **Añadir archivos** y, a continuación, haga clic en **Examinar**.
3. Especifique los archivos que desee certificar ante notario.

   Cuando seleccione un archivo, el software empezará a cargarlo en el almacenamiento en la nube.
4. Cuando todos los archivos se hayan cargado, haga clic en **Certificar ante notario**.

   El software calculará un código hash para cada archivo. El estado de los archivos cambiará a **En progreso**. El uso de la cuota de **Notarizaciones** se incrementará con el número de archivos.
5. Espere hasta que el estado de cada archivo pase de **En progreso** a **Certificado ante notario**.

   El proceso de certificación puede durar hasta 70 minutos. Para reducir el coste de cada certificación, el servicio recopila los hash durante una hora, luego construye un árbol de hash basado en ellos y envía la raíz del árbol de hash a la base de datos de cadena de bloques. A continuación, el servicio de certificación espera a que la transacción se confirme en la base de datos de cadena de bloques y, después, modifica el estado de los archivos a **Certificado ante notario**.

Autenticación certificación

Una vez acabada la certificación, el servicio creará una autenticación notarial para cada archivo. Esta autenticación es una prueba irrefutable de que el archivo se ha certificado ante notario en un determinado momento. La autenticación contiene:

- Información acerca de la certificación (nombre de archivo, hash, tamaño y el número de la transacción de cadena de bloques)
- Instrucciones sobre cómo verificar el archivo manualmente sin utilizar el servicio de certificación

2.3.1 Operaciones con archivos certificados ante notario

Cómo descargar un archivo del almacenamiento en la nube

1. Haga clic en **Archivos certificados ante notario**.
2. En la lista, busque el archivo que necesite.

   Los archivos se pueden filtrar por estado y ordenar por nombre, estado, certificación y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en  o haga clic en el nombre del archivo y, a continuación, en **Descargar**.

Cómo visualizar la autenticación notarial de un archivo

1. Haga clic en **Archivos certificados ante notario**.
2. En la lista, busque el archivo que necesite. Las autenticaciones de certificación solo están disponibles en los archivos que tienen el estado **Certificado ante notario**.

   Los archivos se pueden filtrar por estado y ordenar por nombre, estado, certificación y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en el nombre del archivo.

Copyright © Acronis International GmbH, 2002-2018

4. Haga clic en **Autenticación notarial** para visualizar la autenticación en una nueva ventana.

Cómo eliminar un archivo del almacenamiento en la nube

1. Haga clic en **Archivos certificados ante notario**.
2. En la lista, busque el archivo que necesite.

   Los archivos se pueden filtrar por estado y ordenar por nombre, estado, certificación y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en  o haga clic en el nombre del archivo y, a continuación, en **Eliminar**.

   Si se trata de un archivo certificado ante notario, su estado no se alterará. Se recomienda que guarde la autenticación notarial o el enlace directo a ella antes de confirmar la eliminación.

   Importante *Si la certificación está en progreso, no se cancelará. Sin embargo, no se podrá ver ni descargar la autenticación notarial.*
4. Confirme su decisión.

2.4 Verificación de la autenticidad de los archivos

Se puede verificar la autenticidad de un archivo cargándolo al almacenamiento en la nube o utilizando el recibo de cadena de bloques de la autenticación notarial del archivo.

Los archivos que se cargan para su verificación no utilizan la cuota de **almacenamiento de Notary**, sino que se eliminan del almacenamiento en la nube una vez completado el proceso de verificación.

Cómo verificar la autenticidad de un archivo cargándolo al almacenamiento en la nube

1. Haga clic en **Verificación**.
2. Haga clic en **Examinar** y, a continuación, seleccione el archivo cuya autenticidad desee verificar. Puede seleccionar varios archivos.

   Cuando seleccione un archivo, el software empezará a cargarlo en el almacenamiento en la nube.
3. Haga clic en **Verificar**.
4. El software muestra los informes de verificación de los archivos seleccionados.
   - Si el archivo es auténtico, su estado es **Certificado ante notario**.
   - Si, por el contrario, el archivo no es auténtico, su estado es **Sin certificar ante notario**.
   - Si el archivo aún está en proceso de certificación, su estado es **En progreso**.

Cómo verificar un archivo mediante un recibo de cadena de bloques

1. Acceda a la autenticación notarial tal y como se describe en el apartado "Cómo visualizar la autenticación notarial de un archivo" (pág. 5).
2. Busque la sección **recibo de cadena de bloques** y copie lo siguiente, incluidos los corchetes:

```
{
 "key": "filename.pdf",
 "eTag": "52bf7a18744b384afba39f3646d8e245...",
 "size": 1267387,
 "sequencer": "B56C3FE5ED984F5337"
}
```

   Estas cadenas presentan el nombre del archivo, el hash SHA-256, el tamaño en bytes y el número de transacción de cadena de bloques.
3. En la consola de certificación, haga clic en **Verificación**.
4. Haga clic en **Verificar mediante el uso del recibo de cadena de bloques**.
5. Pegue los contenidos que copió de la sección **Recibo de cadena de bloques** en el campo en blanco.

Copyright © Acronis International GmbH, 2002-2018

6. Haga clic en **Verificar**.
7. El software muestra el informe de verificación.
   - Si el archivo es auténtico, su estado es **Certificado ante notario**.
   - Si, por el contrario, el archivo no es auténtico o no se ha certificado, su estado es **Sin certificar ante notario**.
   - Si el archivo aún está en proceso de certificación, su estado es **En progreso**.

2.5 Firmado de archivos

El servicio de certificación le permite enviar un archivo a varias personas para que lo firmen electrónicamente.

Para que se firme un archivo, debe cargarlo en el almacenamiento en la nube. Una vez que se haya firmado el archivo, el servicio de certificación generará un certificado de firma que contenga una recopilación de las firmas. A continuación, el certificado quedará autentificado por parte del servicio de certificación ante notario. Los archivos firmados no están certificados ante notario.

Por ejemplo, puede firmar electrónicamente los siguientes archivos:

- Contratos de concesión o de alquiler
- Contratos de ventas
- Contratos de adquisición de activos
- Contratos de préstamos
- Formularios de permisos
- Documentos financieros
- Documentos del seguro
- Exenciones de responsabilidad
- Documentos de salud
- Documentos de investigación
- Certificados de autenticidad del producto
- Acuerdos de confidencialidad
- Cartas de oferta
- Acuerdos de confidencialidad
- Acuerdos de contratista independiente

Cómo firmar un archivo

1. Haga clic en **Archivos firmados**.
2. Si no hay archivos firmados, haga clic en **Examinar**. Como alternativa, puede hacer clic en **Añadir archivo** y, a continuación, en **Examinar**.
3. Especifique el archivo que desea firmar.

   Cuando seleccione un archivo, el software empezará a cargarlo en el almacenamiento en la nube.
4. Haga clic en **Añadir firmantes** y, a continuación, agregue los firmantes escribiendo sus direcciones de correo electrónico.

   Para eliminar un firmante, haga clic en el icono del cubo de basura.

   Importante *No es posible añadir ni eliminar firmantes una vez enviadas las invitaciones, así que asegúrese de que la lista incluya a todos aquellos cuyas firmas se requieran.*
5. Haga clic en **Enviar a firma** para enviar las invitaciones a los firmantes.

Copyright © Acronis International GmbH, 2002-2018

Cada firmante recibe un mensaje de correo electrónico con la solicitud de la firma. Recibirá una notificación cuando cada firmante firme el archivo y cuando todo el proceso se haya completado.

6. Cuando el proceso haya terminado, seleccione el archivo firmado y haga clic en **Certificado de firma** para descargar un documento .pdf que contiene:
   - La sección Certificado de firma con una recopilación de todas las firmas.
   - La sección Seguimiento de control con un historial de actividades: cuándo se envió la invitación a los firmantes, cuándo firmó el archivo cada firmante y otros datos.

Una vez que el proceso se haya completado, cada firmante recibirá una notificación que contiene:

- Un enlace al archivo firmado.
- Un enlace al certificado de firma.
- Un enlace a la autenticación notarial del certificado de firma. Una vez terminado el proceso de firma, la autenticación notarial estará disponible en un plazo de 70 minutos.

2.5.1 Operaciones con archivos firmados

Cómo descargar un archivo firmado del almacenamiento en la nube

1. Haga clic en **Archivos firmados**.
2. En la lista, busque el archivo que necesite.
   Los archivos se pueden filtrar por estado y ordenar por nombre, estado, firma y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en  o haga clic en el nombre del archivo y, a continuación, en **Descargar**.

Cómo eliminar un archivo firmado del almacenamiento en la nube

1. Al eliminar un archivo firmado del almacenamiento en la nube, también se borrará su certificado de firma. Si es posible que vaya a necesitar el certificado de firma, asegúrese de que haya guardado una copia local del mismo, tal y como se describe en el paso 6 del apartado "Cómo firmar un archivo" (pág. 7).

   El certificado de firma se mantendrá certificado ante notario.
2. Haga clic en **Archivos firmados**.
3. En la lista, busque el archivo que necesite.
   Los archivos se pueden filtrar por estado y ordenar por nombre, estado, firma y fechas de carga. También puede hacer una búsqueda.
4. Haga clic en  o haga clic en el nombre del archivo y, a continuación, en **Eliminar**.
5. Confirme su decisión.

   Se recomienda descargar la autenticación notarial del certificado de firma o guardar el enlace directo a ella antes de confirmar la eliminación.

3 Administración del servicio de certificación

En este apartado se describe la funcionalidad que solo está disponible para los administradores del servicio de certificación.

3.1 Gestión de claves de API

El servicio de certificación puede integrarse con sistemas de terceros mediante la interfaz de programación de aplicaciones (API) del servicio de certificación. Para obtener más información

Copyright © Acronis International GmbH, 2002-2018

acerca del uso de la API, consulte la guía del desarrollador en https://dl.managed-protection.com/u/baas/api/NotaryDeveloperGuide.

Un administrador del servicio de certificación puede crear y gestionar claves de la API para las integraciones.

Cómo crear una clave de la API

1. Haga clic en **Claves de la API** > **Crear clave de la API**.
2. Cree e introduzca un nombre único para la clave de API.
3. Haga clic en **Crear**.
4. De forma predeterminada, la clave de API se crea con el estado **Habilitada**.

Importante *Copie y guarde la clave. Por motivos de seguridad, la clave solo se muestra una vez. No hay ninguna forma de recuperar la clave si la pierde.*

Cómo deshabilitar una clave de API

1. Haga clic en **Claves de API**.
2. En la lista, busque la clave que necesite.

   Puede filtrar las claves por estado y ordenarlas por nombre, estado y fecha de creación.
3. Haga clic en  y, a continuación, haga clic en **Deshabilitar**.
4. Confirme su decisión.

   Todas las integraciones que usen esta clave dejarán de funcionar. La clave se podrá volver a habilitar en cualquier momento.

Cómo habilitar una clave de API deshabilitada

1. Haga clic en **Claves de API**.
2. En la lista, busque la clave que necesite.

   Puede filtrar las claves por estado y ordenarlas por nombre, estado y fecha de creación.
3. Haga clic en  y, a continuación, haga clic en **Habilitar**.

Cómo eliminar una clave de API

1. Haga clic en **Claves de API**.
2. En la lista, busque la clave que necesite.

   Puede filtrar las claves por estado y ordenarlas por nombre, estado y fecha de creación.
3. Haga clic en  y, a continuación, haga clic en **Eliminar**.
4. Confirme su decisión.

   Todas las integraciones que usen esta clave dejarán de funcionar. No hay manera de recuperar una clave de API eliminada.

3.2 Administración de cuentas de usuario y cuotas

La administración de cuentas de usuario y de cuotas de uso del servicio está disponible en el portal de gestión. Para acceder al portal de gestión, haga clic en **Portal de gestión** cuando inicie sesión en el servicio de certificación, o bien haga clic  en el icono de puntos suspensivos vertical de la esquina superior derecha y, a continuación, en **Portal de gestión**. Solo aquellos usuarios a los que se les ha asignado la función de administrador de empresa pueden acceder a este portal.

Copyright © Acronis International GmbH, 2002-2018

Para obtener información sobre la administración de cuentas de usuario y sus cuotas, consulte la Guía del administrador del portal de gestión. Para acceder a este documento, haga clic en el icono del signo de interrogación en el portal de gestión.

En este apartado se proporciona información adicional relacionada con la gestión del servicio de certificación.

Cuotas

Las cuotas le permiten limitar la capacidad de los usuarios de utilizar el servicio. Para establecer las cuotas, seleccione el usuario en la pestaña **Usuarios** y haga clic en el icono del lápiz en la sección **Cuotas**.

Cuando se supera una cuota, se envía una notificación a la dirección de correo electrónico del usuario. Si no establece un uso por encima del límite de cuota, la cuota se considera "blanda". Esto significa que no se aplican restricciones para usar el servicio de certificación.

También puede especificar usos por encima del límite de la cuota. Un uso por encima del límite permite al usuario sobrepasar la cuota en un valor especificado. Cuando se exceda el límite, se aplicarán restricciones en el uso del servicio de certificación.

Los proveedores de servicios gestionados también pueden especificar cuotas para las empresas de sus clientes de una forma similar.

Están disponibles las cuotas siguientes:

- **Almacenamiento de Notary**

  El almacenamiento de Notary es el almacenamiento en la nube donde se guardan los archivos certificados ante notario, los firmados y aquellos cuya certificación está en progreso. Esta cuota define el espacio máximo que pueden ocupar estos archivos.

  Para reducir el uso de esta cuota, puede eliminar los archivos ya certificados ante notario o firmados del almacenamiento de Notary.
- **Notarizaciones**

  Esta cuota define el número máximo de archivos que se pueden certificar ante notario con el servicio de certificación. Un archivo se considera certificado ante notario en el momento en el que se carga al almacenamiento de Notary y su estado de certificación cambia a **En progreso**.

  Si el mismo archivo se certifica varias veces, cada certificación cuenta como una nueva.
- **Firmas electrónicas**

  Esta cuota define el número máximo de archivos que se pueden firmar con el servicio de certificación. Un archivo se considera firmado desde el momento en el que se envía para su firma.

Notificaciones

Para cambiar los ajustes de notificaciones para un usuario, seleccione el usuario en la pestaña **Usuarios** y haga clic en el icono del lápiz en la sección **Configuración**. Están disponibles los siguientes ajustes de notificaciones:

- **Notificaciones de uso excesivo de las cuotas** (habilitado de forma predeterminada)

  Las notificaciones sobre cuotas superadas.
- **Informes de uso planificados**

  Informes de uso descritos a continuación que se envían el primer día de cada mes.

Todas las notificaciones se envían a la dirección de correo electrónico del usuario.

Copyright © Acronis International GmbH, 2002-2018

Informes de uso

El informe sobre el uso del servicio de certificación incluye los datos siguientes sobre una empresa o unidad:

- Tamaño de los archivos guardados en el almacenamiento de Notary (salvo aquellos que se están verificando) por unidad y por usuario.
- Número de notarizaciones por unidad y por usuario.
- Número de archivos firmados por unidad y por usuario.
- Tamaño total de los archivos guardados en el almacenamiento de Notary (salvo aquellos que se están verificando).
- El número total de notarizaciones.
- El número total de archivos firmados.

Copyright © Acronis International GmbH, 2002-2018