



Manual de Usuario

Firma Avanzada Online (FAO)

Guía para el usuario: qué necesitas, cómo funciona cada modalidad de firma y validación y explica qué hacer si algo falla

Versión 1 | Documento propiedad de ecert

1. ¿Qué es la Firma Avanzada Online?

La Firma Avanzada Online (FAO) es el servicio de ecert que permite firmar documentos con validez legal, comprobando fehacientemente la identidad del firmante de forma remota antes de firmar. Ecert está acreditado por el Ministerio de Economía como Prestador de Servicios de Certificación (PSC) en Chile y emite firmas avanzadas de acuerdo con las Prácticas y Políticas de Certificación de ecert.

La firma permite certificar cualquier documento o instrumento, privado o público, acordado por medios electrónicos, otorgándole el mismo reconocimiento, protección y valor que los actos/contratos celebrados en papel.

Características principales

- Identificación única: vincula el documento directamente con el autor o firmante, de forma incuestionable.
- Integridad: si alguien altera el documento después de firmado, el sistema detecta el cambio de inmediato.
- Respaldo legal: está regulada por ley y es emitida por un Prestador de Servicios de Certificación (PSC) acreditado.

Ecert es la única PSC en Chile que ofrece diferentes mecanismos de validación de identidad para efectuar una Firma Electrónica Avanzada Online.

2. Principales requisitos para utilizar una FAO

Sin importar la modalidad de Firma Electrónica Avanzada Online (FAO) que uses, el firmante necesita cumplir con estos requisitos generales:

- Ser mayor de 18 años.
- Contar con ClaveÚnica vigente y activa.
- Tener acceso al correo electrónico registrado para el segundo factor de autenticación (2FA) de ClaveÚnica, o bien contar con la aplicación Authenticator configurada.
- Tener cédula de identidad, vigente con chip NFC en buen estado (NFC aplica solo para métodos de FAO con NFC).
- Tener acceso al correo electrónico o teléfono celular donde recibirá el código OTP/PIN dinámico de ecert.

Según la modalidad de firma establecida, se suman requisitos adicionales. Los revisamos en el capítulo 4.

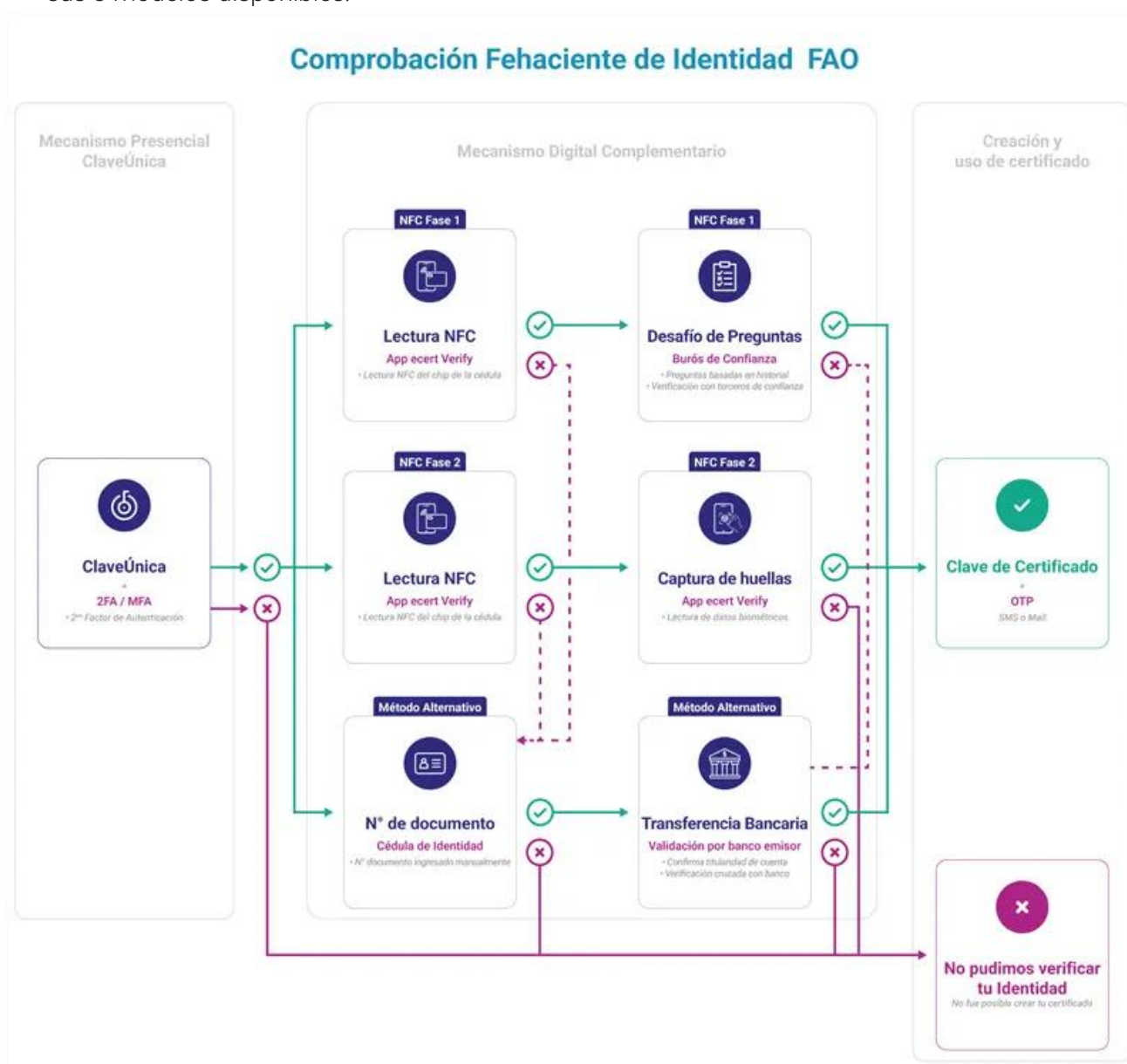
3. El proceso de FAO en términos generales

Todo proceso de firma con FAO sigue la misma lógica, en 3 pasos consecutivos:

- **Mecanismo Presencial ClaveÚnica:** confirmas quién eres, con el método estándar de identidad digital del Estado de Chile.
- **Mecanismo Digital Complementario:** validación adicional con la cual confirmas tu identidad, puedes usar uno o más mecanismos dependiendo de la modalidad configurada.
- **Creación y uso de tu certificado firma:** creas e ingresas la clave de tu certificado de firma, luego validas el uso del certificado mediante la digitación de un código enviado a tu correo o celular.

Solo después de completar estos 3 pasos ejecutados correctamente, puedes continuar con la firma del documento.

A continuación, te presentamos el diagrama de Firma Electrónica Avanzada Online de ecert y sus 3 modelos disponibles:



Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

4. Modalidades de FAO disponibles

Existen 3 modalidades de Firma Avanzada Online (FAO). Todas comparten la misma lógica, pero usan distintos métodos para validar tu identidad.

A continuación, te presentamos un cuadro comparativo resumen de los 3 modelos de validación de identidad disponible para la Firma Electrónica Avanzada Online de ecert a agosto 2026:

Característica	ClaveÚnica + NFC CI + Challenge	ClaveÚnica + NFC CI + Huella	ClaveÚnica + Validación CI + Transferencia Bancaria
Métodos de validación de identidad	ClaveÚnica+2FA, NFC CI, Challenge, OTP	ClaveÚnica+2FA, NFC CI, Huella, OTP	ClaveÚnica+2FA, Validación CI, Transferencia Bancaria, OTP
Requiere app ecert Verify	Sí	Sí	No aplica
Requiere cédula de identidad vigente	Sí	Sí	Sí
Requiere cédula física con chip NFC funcionando	Sí	Sí	No aplica
Requiere cuenta bancaria propia	No aplica	No aplica	Sí
Puede usarse como respaldo de otra modalidad	No disponible por el momento	No disponible por el momento	Sí, como backup del Challenge o como método principal

4.1 Modalidad 1 – ClaveÚnica + NFC CI + Challenge

Esta modalidad será desplegada como método principal para cualquier Firma Electrónica Avanzada. Además de los requisitos generales, necesitas:

- Cédula de identidad física, vigente, con chip NFC en buen estado (no dañado).
- Un teléfono móvil compatible con tecnología NFC y con acceso a la cámara.
- Descargar la app ecert Verify en tu teléfono móvil.
- Información suficiente en fuentes públicas para generar el Challenge de preguntas.

Paso a paso:

- Valida tu identidad con ClaveÚnica + 2FA.
- El sistema te solicitará usar la app ecert Verify.
- Escanea el QR del reverso de tu cédula con la app.
- Posiciona la cédula sobre tu teléfono para leer el chip mediante NFC.
- Responde correctamente el Challenge de preguntas de seguridad.
- Crea e ingresa la clave de tu certificado de firma.
- Valida el código OTP enviado a tu correo electrónico, SMS o WhatsApp.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

4.2 Modalidad 2 — ClaveÚnica + NFC CI + Huella Biométrica

Esta modalidad puede desplegarse como método principal, según modelo de negocio acordado en implementación. Además de los requisitos generales, necesitas:

- Cédula de identidad física, vigente, con chip NFC en buen estado (no dañado).
- Un teléfono móvil compatible con tecnología NFC y con acceso a su cámara.
- Contar con huella dactilar legible para validarse correctamente.
- Descargar la app ecert Verify en tu teléfono móvil.

Paso a paso:

- Valida tu identidad con ClaveÚnica + 2FA.
- El sistema te solicitará usar la app ecert Verify.
- Escanea el QR del reverso de tu cédula con la app.
- Posiciona la cédula sobre tu teléfono para leer el chip mediante NFC.
- Captura tu huella dactilar con la cámara de tu teléfono.
- Posiciona la cédula sobre tu teléfono para leer el chip mediante NFC.
- Crea e ingresa la clave de tu certificado de firma.
- Valida el código OTP enviado a tu correo electrónico, SMS ó WhatsApp.

4.3 Modalidad 3 — ClaveÚnica + Validación CI + Transferencia Bancaria

Esta modalidad puede desplegarse de dos formas, y queda a elección del Cliente B2B la configuración que se realice: como método principal o como método de respaldo. Además de los requisitos generales, necesitas:

- El número de documento de tu cédula de identidad, vigente y sin bloqueo.
- Una cuenta bancaria personal a tu nombre, en un banco autorizado por la Comisión para el Mercado Financiero (CMF).
- Acceso a la banca en línea o app de tu banco.
- Saldo suficiente para realizar la transferencia solicitada.
- Completar la transferencia en menos de 10 minutos

Paso a paso:

- Valida tu identidad con ClaveÚnica + 2FA.
- Digita el número de tu cédula de identidad.
- Selecciona el banco donde tienes una cuenta a tu nombre.
- Transfiere el monto exacto indicado por el sistema, dentro del plazo establecido.
- Espera la confirmación de tu transferencia.
- Crea e ingresa la clave de dos dígitos de tu certificado de firma.
- Valida el código OTP enviado a tu correo electrónico o SMS o WhatsApp.

5. Métodos de validación de identidad

Esta sección explica en detalle cada método que puede formar parte de una modalidad de FAO. Todos se documentan con los mismos criterios, para que puedas compararlos fácilmente.

5.1 ClaveÚnica + 2FA

¿Qué es?	Mecanismo Presencial ClaveÚnica es una verificación obligatoria para todos los firmantes de Firma Avanzada Online en Chile. ClaveÚnica es la identidad digital del Estado de Chile. Ecert está autorizado para usarla como uno de los métodos que confirman la identidad del firmante al iniciar un proceso de Firma Electrónica Avanzada Online.
¿Para qué sirve?	Confirma que la persona que inicia el proceso es efectivamente el firmante, combinando RUT, ClaveÚnica y un segundo factor de seguridad (2FA).
Requisitos previos	Contar con ClaveÚnica vigente y activa. Tener acceso al correo registrado para el 2FA, o la app Authenticator configurada.
¿Cómo funciona?	Debes ingresar ClaveÚnica y luego confirmar el segundo factor de autenticación.
Paso a paso	1) Ingresa RUT y ClaveÚnica. 2) Confirma el segundo factor de autenticación (2FA).
Requisitos técnicos	Tener registrada ClaveÚnica en sistema de Gobierno Digital.
Intentos permitidos	5 intentos para ClaveÚnica 5 intentos para 2FA
Time out	ClaveÚnica 20 minutos 2FA 5 minutos
¿Se puede reintentar?	Sí, hasta agotar los 5 intentos, luego el usuario queda bloqueado.
Criterio de aprobación	Se comprueba la identidad del firmante: - Ingresa correctamente ClaveÚnica y el 2FA.
Criterio de rechazo	No se logra comprobar la identidad del firmante: - ClaveÚnica o el 2FA no coinciden. - No se completa la validación dentro de los 5 intentos.
Qué ocurre si falla / se agotan los intentos	Si se agotan los intentos de comprobación de identidad, el usuario queda bloqueado temporalmente y tendrá que solicitar el desbloqueo en Portal Ciudadano.
Restricciones	Personas chilenas y extranjeros residentes en Chile que cumplan con ser mayor de 18 años y cuenten con cédula de identidad vigente para obtención de su ClaveÚnica. Ecert requiere de disponibilidad de servicios de Gobierno Digital para validar ClaveÚnica.
Consideraciones	El certificado de firma avanzada online se emite con el nombre del usuario registrado en ClaveÚnica. Si el usuario no tiene acceso al correo de 2FA, puede cambiarlo en el Portal Ciudadano de ClaveÚnica, agendar una videollamada, o acudir presencialmente a una oficina del Registro Civil o ChileAtiende.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

5.2 NFC CI (lectura de cédula)

¿Qué es?	NFC es un mecanismo digital complementario de verificación de identidad para Firma Avanzada Online en Chile. Verificación de identidad que se basa en lectura del chip NFC de la cédula de identidad física, mediante la app ecert Verify.
¿Para qué sirve?	Confirma que el usuario cuenta con la cédula física en su poder.
Requisitos previos	Contar con cédula de identidad física, vigente, con chip NFC funcionando (no dañado). Teléfono compatible con NFC y acceso a cámara. App ecert Verify descargada.
¿Cómo funciona?	Desde la app ecert verify, se debe escanear el QR del reverso de la cédula y luego posicionarla sobre el teléfono para que lea el chip NFC.
Paso a paso	1) Escanea el QR del reverso de la cédula. 2) Posiciona la cédula sobre el teléfono hasta que el chip sea leído.
Requisitos técnicos	Teléfono compatible con NFC y acceso a cámara. App ecert Verify (Android o iOS).
Intentos permitidos	Intentos en cada paso realizado en la App: - 3 intentos para escanear QR de cédula. - 3 intentos para verificar NFC de cédula.
Time out	10 minutos.
¿Se puede reintentar?	Sí, hasta agotar los 3 intentos.
Criterio de aprobación	Se comprueba la identidad del firmante: - Coincidencia exitosa entre QR y chip NFC de la cédula del firmante.
Criterio de rechazo	No se logra comprobar la identidad del firmante: - Cedula no vigente o con chip NFC dañado. - No se logra comprobar la consistencia de datos entre la cédula y el firmante. - No completar la validación dentro de los 3 intentos o de los 10 minutos.
Qué ocurre si falla / se agotan los intentos	Si agotas los intentos, o expira el ID de la transacción debes reiniciar el flujo con la app o bien seleccionar vía alternativa por transferencia bancaria. Si no cuentas con cedula con las condiciones necesarias no podrás avanzar en el flujo, puedes seleccionar la vía alternativa por transferencia bancaria.
Restricciones	Usuario debe contar con requisitos previos para completar el proceso de firma avanzada online.
Consideraciones	La App ecert Verify está disponible en Google Play (Android) y App Store (iOS). Todos los iPhone desde el modelo 6 en adelante tienen NFC integrado. Si el teléfono no es compatible con NFC, puedes validar la identidad por el método alternativo Transferencia Bancaria.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

5.3 Challenge (Desafío de preguntas)

¿Qué es?	Challenge de preguntas es un mecanismo digital complementario de verificación de identidad para Firma Avanzada Online en Chile. Es un cuestionario de seguridad con preguntas que solo el firmante podría responder correctamente.
¿Para qué sirve?	Confirma la identidad del firmante mediante información que solo él conoce.
Requisitos previos	Contar con información suficiente en fuentes públicas (registro civil, registros societarios, de vehículos motorizados, de educación, de propiedades, entre otros) para que el sistema genere 4 preguntas de seguridad.
¿Cómo funciona?	El sistema genera preguntas de seguridad a partir de información pública que el usuario debe responder correctamente.
Paso a paso	1) El sistema presenta 4 preguntas. 2) Responder cada pregunta correctamente.
Requisitos técnicos	No aplica.
Intentos permitidos	3 intentos diarios.
Time out	10 minutos.
¿Se puede reintentar?	Sí, hasta agotar los 3 intentos, luego el usuario se bloquea por 24hrs.
Criterio de aprobación	Se comprueba la identidad del firmante: - Responde correctamente al menos 3 de 4 preguntas dentro de los intentos permitidos.
Criterio de rechazo	No se logra comprobar la identidad del firmante: - No alcanzar el mínimo de respuestas correctas requeridas dentro de los intentos permitidos.
Qué ocurre si falla / se agotan los intentos	Si falla la comprobación de la identidad, se agotan los intentos o expira el ID de la transacción el usuario queda bloqueado por 24 horas. El sistema puede ofrecer validación vía Transferencia Bancaria como método alternativo.
Restricciones	El modelo antifraude de ecert considera bloqueos adicionales. Por motivos de seguridad, las reglas y criterios específicos que activan estos bloqueos no pueden ser declarados ni compartidos. Personas sin información pública suficiente para generar el mínimo de 4 preguntas, no podrán validarse. Ecert requiere de disponibilidad de servicios de terceros para consultas en registros públicos. Burós de información puede generar mantenciones o intermitencias que impidan la validación de ecert
Consideraciones	Si el usuario no responde correctamente las preguntas, no cuenta con información pública suficiente para generar preguntas o está bloqueado, el sistema ofrece validación vía Transferencia Bancaria como método alternativo.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

5.4 Validación Cédula de Identidad (CI)

¿Qué es?	Validación de cédula es un mecanismo digital complementario de verificación de identidad para Firma Avanzada Online en Chile. Es una verificación del estado de la cédula de identidad de los firmantes consultada en registros oficiales de Chile.
¿Para qué sirve?	Principalmente busca confirmar que RUT y número de documento coincidan. Adicionalmente, confirma que la cédula está vigente, que no existen bloqueos y que el firmante no está difunto.
Requisitos previos	Contar con el número de documento de la cédula de identidad, vigente y sin bloqueo.
¿Cómo funciona?	El sistema concilia el número de documento con tu RUT y revisa su estado.
Paso a paso	1) Ingresa el número de documento de la cédula de identidad. 2) El sistema valida automáticamente su estado.
Requisitos técnicos	No aplica.
Intentos permitidos	No aplica.
Time out	No aplica.
¿Se puede reintentar?	Sí
Criterio de aprobación	Se comprueba la identidad del firmante: - Número de documento coincide con RUT. - La cédula está vigente, no bloqueada, y no pertenece a una persona fallecida.
Criterio de rechazo	No se logra comprobar la identidad del firmante: - Número de documento no coincide con RUT. - La cédula está vencida, bloqueada, o pertenece a una persona fallecida.
Qué ocurre si falla / se agotan los intentos	Si falla no puede validarse la identidad, debe reintentar con información correcta o utilizar otro método de validación para firma.
Restricciones	Registro Civil puede generar mantenciones o intermitencias que impidan la validación de ecert.
Consideraciones	No existen bloqueos por reintentos.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

5.5 Transferencia Bancaria

¿Qué es?	Validación Transferencia Bancaria es un mecanismo digital complementario de verificación de identidad para Firma Avanzada Online en Chile. Es un método que valida la identidad del firmante mediante una transferencia bancaria desde tu cuenta personal.
¿Para qué sirve?	Confirma que eres el titular de una cuenta bancaria, ya que solo tú tienes acceso a tu banca en línea. Puede usarse como respaldo o como método principal, según cómo lo configure ecert. Método de respaldo se activa si el usuario: - No dispone de los requisitos necesarios para utilizar el método NFC CI. - No dispone de los requisitos necesarios para utilizar el método Challenge de preguntas.
Requisitos previos	Tenar cuenta bancario personal a nombre del firmante, en un banco autorizado por la CMF. Acceso a la banca en línea o app del banco registrado al inicio del flujo. Saldo suficiente para transferir el monto solicitado.
¿Cómo funciona?	Seleccionas tu banco y transfieres el monto exacto que el sistema te indica, dentro de un plazo de 10 minutos. El sistema concilia 4 datos: que banco coincida con el declarado inicialmente, que seas el titular de la cuenta, que el monto transferido coincida, y que lo hagas en el tiempo definido.
Paso a paso	1) Selecciona el banco donde tienes cuenta. 2) Transfiere el monto exacto indicado. 3) Espera la confirmación de la transferencia.
Requisitos técnicos	Acceso a la banca en línea o app del banco registrado al inicio del flujo.
Intentos permitidos	6 intentos.
Time out	10 minutos.
¿Se puede reintentar?	Sí, hasta agotar los 6 intentos.
Criterio de aprobación	Se comprueba la identidad del firmante: - Transferir desde el banco previamente indicado el monto exacto solicitado, desde una cuenta a nombre del firmante, dentro de los 10 minutos.
Criterio de rechazo	No se logra comprobar la identidad del firmante: - Banco o monto de transferencia incorrectos, cuenta bancaria no está a nombre del firmante o no completa transferencia dentro del plazo de 10 minutos.
Qué ocurre si falla / se agotan los intentos	Si falla la comprobación de la identidad o expira el ID de la transacción debes reiniciar el flujo. Si agotas los 6 intentos, usuario queda bloqueado por 24 horas.
Restricciones	Primer contacto creado para una transferencia restringe un segundo intento en 12 o 24hrs (según cada banco) por motivos de seguridad.
Consideraciones	El dinero se devuelve en un máximo de 24 horas hábiles, incluso si la transferencia fue errónea Es sin costo para ti. Nunca se te pedirá tu clave bancaria ni tus credenciales. La mayoría de los bancos usa un rango de \$90 a \$300; excepciones: Santander (\$1.000 a \$1.100) y Consorcio (\$2.000 a \$2.100). El proceso usa a Khipu como proveedor de pagos, un método que no almacena credenciales bancarias.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

5.6 Huella Biométrica

¿Qué es?	Validación de huella biométrica es un mecanismo digital complementario de verificación de identidad para Firma Avanzada Online en Chile. Es una validación de huella dactilar, que captura datos biométricos de la huella y la compara contra la almacenada en el chip de la cédula.
¿Para qué sirve?	Es una comprobación robusta de identidad: compara la minucia de la huella directamente contra la información almacenada en la cédula de identidad (Match on Card), sin almacenar datos ni enviar información a servidores externos.
Requisitos previos	Cédula de identidad física, vigente, con chip NFC funcionando (no dañado). Teléfono compatible con NFC y con acceso a cámara. Al menos una huella dactilar legible para validarse correctamente. App ecert Verify descargada.
¿Cómo funciona?	Capturas la huella con la cámara del teléfono y el sistema la compara localmente contra la información almacenada en el chip de la cédula.
Paso a paso	1) Abre la cámara desde la app ecert Verify. 2) Captura QR de la cédula 3) Posiciona la cédula para lectura NFC. 4) Captura tu huella dactilar. 5) Posiciona la cédula para lectura NFC. 6) Espera la validación.
Requisitos técnicos	Teléfono compatible con NFC y con cámara. App ecert Verify.
Intentos permitidos	Sin límite de intentos en escaneo de huella dactilar. 3 intentos para hacer la lectura NFC.
Time out	10 minutos.
¿Se puede reintentar?	Sí, sin límite de intentos para lectura de huella dentro de los 10 minutos.
Criterio de aprobación	Se comprueba la identidad del firmante: - La huella capturada coincide con la almacenada en el chip de la cédula, y corresponde a quien está realizando el flujo de firma.
Criterio de rechazo	No se logra comprobar la identidad del firmante: - La huella no coincide con la información de la cédula de identidad del firmante, o no se logra capturar dentro de los 10 minutos.
Qué ocurre si falla / se agotan los intentos	Si agotas los reintentos de validación con la app o expira el ID de la transacción debes reiniciar el flujo con la app o bien seleccionar flujo alternativo por transferencia bancaria.
Restricciones	Usuario debe contar con requisitos previos para completar el proceso de firma avanzada online.
Consideraciones	La validación ocurre localmente en el chip de tu cédula, sin enviar tu huella a servidores externos. Ecerc no almacena datos biométricos. Para la correcta lectura de las huellas biométricas, considera limpiar la cámara de tu dispositivo móvil, limpiar tu dedo con alcohol gel.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

5.7 OTP o PIN dinámico (código de un solo uso)

¿Qué es?	OTP/PIN dinámico es una verificación obligatoria para confirmar el uso de un certificado digital Firma Avanzada Online en Chile. Un código de verificación de un solo uso, enviado al usuario vía correo electrónico, SMS o WhatsApp.
¿Para qué sirve?	Confirma que tienes acceso al correo o teléfono registrado al momento de iniciar el flujo y permite dar uso al certificado de firma avanzada online.
Requisitos previos	Tener acceso al correo electrónico o teléfono celular donde recibirás el código.
¿Cómo funciona?	Ingresas el código que el sistema te envía.
Paso a paso	1) Recibe el código. 2) Ingresa el código en el sistema. 3) Si no llega, puedes solicitar el reenvío del código o seleccionar un nuevo método de envío, luego de 60 segundos desde el primer envío.
Requisitos técnicos	Tener acceso al teléfono y /o correo electrónico registrado previamente.
Intentos permitidos	6 intentos.
Time out	5 minutos.
¿Se puede reintentar?	Sí. Puedes cambiar el método de envío del código 60 segundos después del primer envío.
Criterio de aprobación	Ingresa correctamente el código OTP.
Criterio de rechazo	No ingresar el código o falla en el ingreso del código dentro de los 6 intentos.
Qué ocurre si falla / se agotan los intentos	Rut de usuario queda bloqueado por 24 horas.
Restricciones	Cada intento fallido descuenta 1 intento del total disponible para tu RUT, indistintamente.
Consideraciones	A nivel de integración en la preinscripción se debe declarar el correo electrónico y número telefónico del firmante o bien al momento de ingresar el contacto al portal empresas. Actualmente el correo es un campo obligatorio, mientras que el número telefónico es opcional, es importante tener en consideración que si no cuenta este último no será posible desplegar las alternativas de envío OTP/ PIN dinámico vía SMS o WhatsApp, es decir solo lo recibirá al correo electrónico.

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.

6. Tabla comparativa de métodos

Compara y resume las condiciones de cada método de validación.

Criterio	ClaveÚnica + 2FA	NFC CI	Challenge	Validación CI	Transferencia Bancaria	Huella Biométrica	OTP
Intentos permitidos	ClaveÚnica: 5 intentos 2FA: 5 intentos	Escanear QR: 3 intentos Verificar NFC: 3 intentos	3 intentos diarios	Sin límite (No aplica)	6 intentos	Huella: sin límite Verificar NFC: 3 intentos	6 intentos
Time out	ClaveÚnica: 20 min 2FA: 5 min	10 minutos	10 minutos	No aplica	10 minutos	10 minutos	5 minutos
Qué pasa al agotar intentos/tiempo	Bloqueo temporal (requiere desbloqueo en el Portal Ciudadano)	Expira la transacción; puede optarse por Transferencia Bancaria como alternativa	Bloqueo por 24 horas; el sistema puede ofrecer Transferencia Bancaria como alternativa	No aplica (no bloquea; se reintentará con información correcta)	Expira la transacción (por tiempo) o bloqueo por 24 horas (al agotar los 6 intentos)	Expira la transacción; puede optarse por Transferencia Bancaria como alternativa	Bloqueo por 24 horas, por RUT
¿Se puede reintentar?	Sí, hasta agotar los 5 intentos de cada paso	Sí, hasta agotar los 3 intentos de cada paso	Sí, hasta agotar los 3 intentos	Sí, sin límite	Sí, hasta agotar los 6 intentos	Sí — huella sin límite; Verificar NFC hasta 3 intentos	Sí, hasta agotar los 6 intentos
Requiere app ecert Verify	No aplica	Sí	No aplica	No aplica	No aplica	Sí	No aplica

Nota: Las modalidades mencionadas, describe el proceso de FAO disponibles y vigentes hasta el 01 de diciembre de 2026, las cuales están sujetas a modificaciones por posibles cambios normativos en Chile.