

CertifyID ISSUING CA ADVANCED SERVICES

Formulario de Solicitud de Certificado de Pertenencia

1. INFORMACIÓN DEL SUBSCRIPTOR	
Título	<input type="checkbox"/> Sr. <input type="checkbox"/> Sra. <input type="checkbox"/> Dr. <input type="checkbox"/> Prof. <input type="checkbox"/> Otro:
Nombre *	
Apellidos *	
Dirección de correo *	<input type="checkbox"/> Se utilizará para proteger mensajes de correo-e
Organización *	
División / Depto.	
Ciudad	
Estado o Provincia *	
País *	

2. INFORMACIÓN ADICIONAL (Sólo para fines de la inscripción – se mantendrá la confidencialidad de los datos)			
Dirección *		Código Postal *	
Ciudad *		País *	
Teléfono *	<input type="checkbox"/> Celular	Fax	
Lugar de nacimiento *		Fecha de nacimiento * (dd.mm.aaaa)	
Nacionalidad *			

* Datos obligatorios

3. DIRECCIÓN DE ENVÍO (Sólo si es diferente a la anterior)		4. DIRECCIÓN DE COBRANZA (Sólo si es diferente a la anterior)	
Nombre		Nombre	
Dirección		Dirección	
Ciudad		Ciudad	
Código Postal		Código Postal	
País		País	

La presente solicitud sólo será válida si la verificación de la identidad es exitosa, de acuerdo con las políticas de WIS@key, y el certificado digital es aceptado por el subscritor. Sírvase adjuntar copias de lo siguiente: -los adjuntos no serán devueltos-

Marque los recuadros aplicables

- Documento de Identidad (ambas caras) N° _____
 - Otro (indicar) _____ N° _____
 - Ficha RUC de Organización N° _____
 - Vigencia de Poder del RPLegal (Partida Registral N° _____)
- Firma del Solicitante:** X _____ **Fecha:** / /2018
Lea y firme también el Convenio del Subscritor del Certificado CertifyID

SOLO PARA USO INTERNO

1. DOCUMENTO DE IDENTIDAD ENTREGADO			
Prueba de la Identidad: Documento de Identidad <input type="checkbox"/> Pasaporte <input type="checkbox"/> Otro <input type="checkbox"/>			
Número:	Fecha vencimiento:	Entidad/País Emisor:	
Si fuera algún otro, especificar y brindar detalles:			
Prueba de su condición	Empleado <input type="checkbox"/>	Apoderado <input type="checkbox"/>	Profesional <input type="checkbox"/>
Cargo o número planilla (si lo hubiera):			
Documento(s) presentado(s):			
Otro:			
2. ACTIVIDADES DE VERIFICACIÓN DE IDENTIDAD (sólo para uso del registrador)			
Manipulación de documento <input type="checkbox"/>	Verificación de fotografía <input type="checkbox"/>		
Verificación por una tercera persona <input type="checkbox"/>	Verificación de la firma <input type="checkbox"/>		
Verificación Org./División Org. <input type="checkbox"/>	Comentarios (si los hay):		
3. N° DE SERIE DEL TOKEN / SMARTCARD			
4. N° DE SERIE DEL CERTIFICADO			
5. REGISTRADOR:	Fecha de Emisión: _____	ID: _____	_____

Convenio de Suscriptor de Certificado CertifyID

Al momento de recibir la solicitud de certificado, usted (“Suscriptor del Certificado”) acepta los términos y condiciones del presente Convenio y está sujeto al cumplimiento de todas sus provisiones a partir de la fecha de presentación de la solicitud.

1. **Alcance:** El presente convenio rige la entrega de servicios de certificación por parte de WIS@key a los Suscriptores del Certificado así como el uso de dichos servicios de certificación.
2. **Propósito:** Los servicios de certificación provistos por WIS@key serán otorgados de conformidad con las Prácticas y Políticas de la Fundación OISTE y las Prácticas y Políticas de Certificación de WIS@key las cuales se encuentran disponibles en www.wisekey.com/repository/, todas las cuales quedan incorporadas, por referencia, al presente Convenio.
3. **Garantía de WIS@key:** A través de la entrega de sus Servicios de Certificación, WIS@key cumplirá todas sus obligaciones de conformidad con sus Prácticas y Políticas de Certificación. Al aceptar usted un certificado, WIS@key le garantiza el cumplimiento de dichas obligaciones.
4. **Terceerización de Servicios de Certificación:** Compañías externas a WIS@key (“Proveedores Externos de Servicios”) podrían brindar parte de los servicios de certificación, como por ejemplo:
 - El procesamiento de solicitudes de emisión, suspensión y revocación de certificados;
 - La verificación de la identidad de los solicitantes de certificados;
 - El archivo de datos personales de los solicitantes cuyos certificados han sido procesados por estos proveedores, de conformidad con regulaciones locales de Protección o Privacidad de los Datos; y
 - Generación criptográfica de pares de claves.

En aquellos casos en que los Proveedores Externos de Servicios presten dichos servicios, el formulario de solicitud de certificado contará con los detalles necesarios sobre la provisión de sus servicios, los cuales, en todos los casos, deberán garantizar el cumplimiento de las prácticas y políticas de WIS@key mencionadas en la cláusula 2 del presente convenio.
5. **Reconocimiento por parte del Suscriptor del Certificado:** Al momento de la firma del presente convenio, usted reconoce que:
 - Conoce las Políticas y Prácticas de WIS@key;
 - Ha recibido manuales de instrucciones sobre el uso, precauciones de seguridad y funcionalidades de los certificados, claves criptográficas, y servicios de certificación provistos por WIS@key y cualquier Proveedor Externo de Servicios;
 - Comprende la naturaleza de los servicios provistos por WIS@key y los Proveedores Externos de Servicios;
 - Entiende las garantías y comprende que existen limitaciones de responsabilidad y daños, tal como está indicado en las Políticas y Prácticas de WIS@key;
 - WIS@key y/o el Proveedor Externo de Servicios pertinente pueden, a su única y absoluta discreción, optar por no procesar o emitir un certificado a su nombre;
 - WIS@key o el Proveedor Externo de Servicios que procesó su certificado podrá requerir la suspensión o revocación de su certificado si así usted lo solicitara o si WIS@key o dicho Proveedor Externo de Servicios recibieran alguno o cualquiera de los siguientes:
 - La clave privada correspondiente a la clave pública en el certificado se ha, potencialmente o efectivamente, perdido, ha sido revelada sin autorización, ha sido robada o se ha visto comprometida de alguna manera;
 - Se ha perdido el control sobre su clave privada debido al compromiso de los datos de activación (por ejemplo, frase de contraseña o código PIN) o debido a cualquier otro motivo;
 - Inexactitud o cambios al contenido del certificado, tal como se le notifica a usted;
 - Usted no cumple materialmente con las obligaciones adquiridas con WIS@key o el Proveedor Externo de Servicios para procesar su solicitud de certificación;
 - Se ha presentado una emisión incorrecta o defectuosa del certificado debido a:
 - Un pre-requisito materialmente crítico para la emisión del certificado no ha sido satisfecho;
 - Se sabe, o se cree razonablemente, que un dato materialmente crítico en el certificado es falso.
 - Cualquiera otra circunstancia que se cree podría afectar la confiabilidad, seguridad o integridad del certificado o del par de clave criptográfico asociado al mismo.
 - En caso usted desee convertirse en una “Parte que Confía”, usted deberá aceptar y firmar el Convenio de la Parte que Confía (disponible en <http://www.wisekey.com/repository/>).
 - Que el certificado será tratado como información pública y será puesto a disposición de otras partes.
6. **Vuestras Obligaciones y Garantías:** Al momento de solicitar la emisión de un certificado, usted acepta:
 - Proporcionar información precisa y completa para permitir el procesamiento de la solicitud de emisión de certificado;
 - Generar o haber generado vuestras claves criptográficas de manera tal que cumplan con los requerimientos de la política aplicable;
 - Revisar el certificado que se le ha emitido para establecer la precisión de los datos ahí contenidos y aceptar el certificado o comunicar a WIS@key o al Proveedor Externo de Servicios que procesó la solicitud del certificado sobre la necesidad de realizar modificaciones al mismo;

Al aceptar el certificado que se le ha emitido, usted garantiza que:

 - Los datos contenidos en el certificado son correctos;
 - La clave criptográfica privada asociada a la clave pública contenida en el certificado no se ha visto comprometida;
 - Usted empleará el par de clave criptográfica y los certificados únicamente de conformidad con la Política de Certificación aplicable;
 - Usted ejercerá razonablemente el cuidado necesario para mantener la seguridad de la clave criptográfica privada asociada a la clave pública contenida en el certificado así como impedir su uso no autorizado;
 - Usted procederá sin demora alguna a notificar a WIS@key o al Proveedor Externo de Servicios que procesó su solicitud de certificado para la suspensión o revocación de su certificado si usted sospecha o sabe que su clave privada, el dispositivo en el cual está guardado o el PIN/contraseña se han visto comprometidos, se han perdido o su seguridad se ha visto en alguna otra manera afectada materialmente.
 - Usted seguirá los procedimientos necesarios para la suspensión o revocación de los certificados de conformidad con las prácticas y políticas aplicables.
 - Usted pagará las tarifas de los servicios de certificación provistos de conformidad con la lista de precios aplicable.
7. **Aceptación del Certificado:** La aceptación del certificado por parte de su persona se producirá cuando ocurra alguno de los siguientes eventos:
 - A la firma del formulario de aceptación del certificado y su presentación ante la entidad que procesó la solicitud del certificado;
 - Al momento del pago de los servicios de emisión del certificado; o
 - Al primer uso del certificado con propósitos distintos a la verificación del contenido del certificado y prueba de su funcionalidad (como parte de la evaluación realizada por el Suscriptor del Certificado para decidir si lo acepta o no).
8. **Período de Validez del Certificado y Tarifas:** El período inicial de validez del certificado emitido a su nombre será de un (1) año, sujeto al pago de las tarifas correspondientes, de conformidad con el cronograma previsto en la lista de precios aplicable.
9. **Límites de la Responsabilidad:** Las cláusulas de descarga de responsabilidad y de responsabilidad contenidas en la Prácticas y Políticas mencionadas en la Cláusula 2 del presente convenio rigen con respecto a los reclamos que podrían producirse en relación con los certificados y los servicios de certificación provistos por WIS@key, los Proveedores Externos de Servicios, incluyendo el tope acumulativo de daños.
10. Todas dichas limitaciones se extenderán a todo y cada uno de los reclamos contra WIS@key y otras entidades dentro de WIS@key PKI que brindan servicios de certificación. La limitación será aplicable por certificado, independientemente del número de transacciones, firmas digitales o causas de acción que se produzcan por o en relación con dicho certificado o cualquier servicio provisto con respecto a dicho certificado.
11. Las limitaciones antes indicadas se aplicarán a cualquier responsabilidad sea por motivo contractual, agravio (incluyendo negligencia) o cualquiera otra teoría de la responsabilidad, incluyendo daños directos, indirectos, especiales, punitivos, ejemplares, consecuentes, de confianza o incidentales.
12. **Protección y Privacidad de los Datos:** Por el presente usted acepta la Política de Privacidad de WIS@key y por lo tanto autoriza la publicación de los datos que proporcionó para incorporación en el certificado que ha solicitado así como la información pertinente de estado del certificado. Dicha publicación se llevará a cabo por Internet y por cualquier otro medio que WIS@key estime necesario para la provisión de los servicios de certificación. Además, usted autoriza a WIS@key o al Proveedor Externo de Servicios que procesó su solicitud de certificado a revelar cualquier información relevante que sea requerida para cualquier proceso judicial o pesquisa relativa a la confiabilidad y/o validez legal del certificado o cualquier firma digital respaldada por el certificado emitido, independientemente de si dicho certificado se encuentra válido, vencido, revocado o suspendido.
13. **Indemnización:** Usted indemnizará y mantendrá indemne de cualquier y toda responsabilidad a WIS@key, el Proveedor Externo de Servicios correspondiente así como sus directores, ejecutivos, empleados, agentes y afiliadas, que se produzca como consecuencia de cualquier uso de los Certificados WIS@key fuera de los objetivos previstos o por cualquier motivo que viole materialmente vuestras obligaciones en virtud del presente convenio.
14. **Contratación Electrónica:** Al aceptar el presente convenio, usted también acepta la formación y conclusión de contratos, entrega de notificaciones y comunicaciones en general a través de medios electrónicos (incluyendo la firma del presente contrato y los avisos de cancelación) con WIS@key para los fines de los servicios de certificación digital. Usted reconoce que está preparado y tiene la capacidad y el equipo para hacerlo.
15. **Terminación/Cancelación:** El presente convenio podrá ser rescindido por cualquiera de las partes en cualquier momento. En caso usted rescinda el contrato sin motivo aparente, no se le reembolsarán las tarifas pagadas hasta la fecha. En caso el convenio sea rescindido sin motivo aparente por parte de WIS@key, esta última le hará el reembolso correspondiente de conformidad con su política de devoluciones vigente. Cuando la cancelación del convenio por parte de WIS@key cuente con motivo aparente (debido al incumplimiento o cualquier otro motivo material), usted no recibirá reembolso alguno. En todos los casos, el presente contrato culminará al momento de su vencimiento o a la revocación del certificado que le fuera emitido a usted.
16. **Divisibilidad:** Si alguna de las secciones, oraciones, cláusulas o frases contenidas en el presente convenio son consideradas inválidas o inconstitucionales por un tribunal con competencia jurisdiccional, dicha invalidez o inconstitucionalidad no afectará la validez o constitucionalidad de cualquiera otra sección, oración, cláusula o frase del presente convenio.
17. **Ley Aplicable:** El presente convenio se regirá y será interpretado de acuerdo con las leyes de Suiza, y las partes aceptan someterse a la exclusiva jurisdicción de los tribunales suizos.

FIRMADO por y a nombre de: **X**
Usuario Final

Nombre: _____

Fecha: _____