E-Sign SA

Cliente

Contrato No.
RUT Cliente:

Contacto Cliente
Nombre:

Título:
Teléfono:

Fax:
Correo Electrónico:

Administrador de Programa de E-Sign
Nombre:

Título:
Teléfono:

Fax:
Correo Electrónico:

Información de Facturación del Cliente
Dirección:
Fax:
Correo Electrónico:

Fecha de Vigencia:
Período de Vigencia del Acuerdo: Tres (3) años

Anexos (marcar los que correspondan):

( ) Anexo “A”: Servicio de Certificado Managed PKI Private Label	( ) Anexo “G”: Servicios de Certificación Notarial Digital
( ) Anexo “B”: Servicio de Certificado Co-Comercializado Managed PKI	( ) Anexo “H”: Identrus Express
( ) Anexo “C”: Servicio de Gestión de Clave Managed PKI	( ) Anexo “I”: Servicios de Autenticación de Dispositivos
( ) Anexo “D”: Acuerdo de Nivel de Servicios	
( ) Anexo “E”: Tasas	
( ) Anexo “F”: Servicio de Roaming Managed PKI	

El presente Acuerdo Principal de Servicios, que se compone de esta portada, los Términos y Condiciones y los Anexos y Suplementos adjuntos pertinentes, cada uno de los cuales se incorpora y es parte del presente Acuerdo por medio de esta referencia (conjuntamente, el ”Acuerdo”), vigente a partir de la Fecha de Vigencia establecida anteriormente, se celebra por y entre (“E-Sign”), que tiene su principal centro de operaciones en el lugar ya indicado, y la parte identificada anteriormente como el Cliente (“Cliente”), que tiene su principal centro de operaciones en el lugar ya indicado.

CLIENTE:

Por:
Nombre:
Título:
Fecha:

E-Sign:

Por:
Nombre:
Título:
Fecha:

TÉRMINOS Y CONDICIONES

1. DEFINICIONES. Los términos en mayúscula que no se definan de otro modo conforme al presente documento tendrán los significados establecidos en la Sección 10 del presente Acuerdo.

2. TASAS, CONDICIONES DE PAGO, IMPUESTOS Y SEGUROS.

2.1 Tasas. Las tasas de E-Sign para los Servicios y Productos proporcionados conforme al presente documento a partir de la Fecha de Vigencia se establecen en el Anexo "E". Durante el período de vigencia del presente Acuerdo, el Cliente podrá adquirir o licenciar Productos y Servicios adicionales, sujeto a los términos del presente Acuerdo, según las tasas de E-Sign vigentes en ese momento, por medio de la presentación de una orden de compra a E-Sign que incorpore o haga referencia al presente Acuerdo.

2.2 Condiciones de Pago. Todas las tasas establecidas en el Anexo “E” serán facturadas una vez ejecutado el presente Acuerdo. Todas las tasas recurrentes serán vencidas y pagaderas por el Cliente, y serán facturadas inmediatamente por E-Sign anualmente, a menos que se especifique de otro modo en el Anexo "E". El Cliente pagará en pesos cada una de las facturas en el plazo de treinta (30) días después del acuse de recibo en la dirección de E-Sign indicada en la página 1.

2.3 Impuestos. Todos los impuestos, derechos de aduana, tasas y otros cargos gubernamentales de cualquier tipo (incluidos los impuestos de ventas, servicios y uso, pero con exclusión de los impuestos con base en los ingresos brutos o renta neta de E-Sign), que imponga la autoridad de algún gobierno o subdivisión política de éste, o bajo el control de tal, sobre las tasas para cualquiera de los Servicios o Productos será responsabilidad del Cliente, y no se considerará como parte o deducción de tales tasas, o compensación contra éstas.

2.4 Tasa de Pago Atrasado. Si el Cliente no paga una factura una vez vencida, E-Sign podrá cobrar una tasa de pago atrasado sobre los montos impagos igual a la menor cantidad de: (i) diez por ciento (10%) anual, o (ii) el porcentaje legal máximo.

2.5 Cobertura del Seguro. Cada una de las partes, a costa propia, mantendrá un seguro estándar de errores u omisiones por un monto no inferior a $130.000 US dólares (Nota: la obligación legal es de 5.000 UF que corresponde a $130.000 US, aproximadamente.)

3. CONFIDENCIALIDAD.

3.1 Información Confidencial. “Información Confidencial” se refiere a cualquier tipo de información confidencial, de secreto comercial o privilegiada revelada por una de las partes a la otra parte conforme al presente Acuerdo, incluyendo el Acuerdo de Nivel de Servicios (“SLA”), salvo la información que: (i) es de conocimiento público en el momento de la revelación, (ii) era conocida para la parte receptora antes de ser revelada por la otra parte, o se vuelve de conocimiento público o de otro modo conocida para la parte receptora después de dicha revelación, que no sea por incumplimiento de una obligación de confidencialidad o (iii) información que la parte receptora ha conocido al margen de la otra, de forma independiente.

3.2 Protección de la Información Confidencial. La parte receptora: (i) no revelará la Información Confidencial a un tercero, que no sean sus empleados, representantes o contratistas independientes, quienes están obligados por obligaciones de confidencialidad similares, (ii) no utilizará la Información Confidencial de ninguna forma salvo para cumplir lo establecido en el presente Acuerdo y (iii) tomará las prevenciones consistentes con la protección que da a su propia información confidencial y privilegiada (y en ningún caso ejercerá un cuidado menor al razonable) para evitar la revelación no autorizada de la Información Confidencial. Ambas partes reconocen que el incumplimiento de la

presente Sección 3 causará un perjuicio irreparable a la parte que revele la información, dado que la otra parte tendrá derecho a ser indemnizada por orden judicial, además de otras reparaciones.

3.3 Cooperación Mutua. Cada una de las partes notificará y cooperará con la otra parte en el cumplimiento de los derechos de la parte que hace la revelación, si dicha parte se da cuenta de una vulneración probable o real de los requisitos de confidencialidad de la presente sección. Si la parte que hace la revelación lo solicita de modo razonable, la parte receptora entregará copias de los acuerdos de confidencialidad celebrados con sus empleados, representantes o contratistas independientes.

3.4 Sin Limitación. Ninguna parte del presente Acuerdo limitará, o tendrá la intención de limitar, la capacidad de cualquiera de las partes para desarrollar o mejorar sus Productos y Servicios de ninguna manera, incluido el uso del conocimiento adquirido como resultado del cumplimiento de ambas partes de las obligaciones conforme al presente documento, siempre y cuando ninguna de las partes utilice o revele la Información Confidencial identificada como tal por ellas por escrito en el plazo de 15 días a partir de la revelación.

4. DERECHOS; LICENCIA; PRODUCTOS FINALES DE E-SIGN.

4.1 Derechos. El Cliente reconoce que E-Sign, sus vendedores y otorgantes de licencia, incluidos, entre otros, VeriSign ("Vendedores y Otorgantes de Licencia"), retienen todos los derechos de propiedad intelectual y título (incluida cualquier patente, derechos de autor, marcas registradas y otros derechos) en y para toda la Información Confidencial, secretos comerciales o demás información privilegiada, productos y las ideas, conceptos, técnicas, innovaciones, procesos, software o trabajos de autoría de E-Sign y los Vendedores y Otorgantes de Licencia desarrollados, que incluyen, contenidos en o practicados en relación con los Productos o Servicios prestados por E-Sign bajo este Acuerdo (todo lo anterior los "Trabajos"), incluyendo, entre otros, todas las modificaciones, mejoras, configuraciones, actualizaciones e interfaces hechas para el hardware y software designado por E-Sign que soporta tales Servicios, y la interfaz del sitio Web de E-Sign para el uso del Cliente (los "Componentes de Servicio"). Los Componentes de Servicio no incluyen el software de acceso a Internet o la plataforma de hardware base del Cliente. E-Sign y los Vendedores y Otorgantes de Licencia se reservan y retienen todos los derechos de propiedad intelectual y título asociados con los Trabajos creados por ellos, y los trabajos derivados de éstos, incluyendo, entre otros, todos los Trabajos o trabajos derivados desarrollados o creados por E-Sign y los Vendedores y Otorgantes de Licencia o su personal o contratistas durante el curso del cumplimiento de los Servicios para el Cliente, o la entrega de los Productos a éste. El Software, incluyendo su operación, códigos, arquitectura e implementación, junto con la apariencia y sentido de éste, son la preciada propiedad intelectual de E-Sign y los Vendedores y Otorgantes de Licencia. El Software está protegido por las leyes norteamericanas sobre derechos de autor y las disposiciones de los tratados internacionales. El presente Acuerdo no le da al Cliente ningún derecho de propiedad intelectual sobre el Software, salvo por la licencia que se otorga en la Sección 4.2.

4.2 Licencia. A cambio del pago que hace el Cliente de la tasa de licencia pertinente, E-Sign le otorga una licencia no exclusiva e intransferible para el uso de cada una de las copias del Software que reciba de E-Sign en las CPU bajo el control del Cliente, según se especifica en el Anexo "E", siempre que dicho Software se utilice en relación con los Servicios. El Cliente puede hacer una copia del Software únicamente para fines de archivo o respaldo. El Cliente no puede utilizar el Software en varias CPU al mismo tiempo sin comprar antes una licencia (licencia de aplicación única) para cada una de las CPU que se usarán de manera simultánea, a menos que se especifique lo contrario en el Anexo "E" para las licencias de aplicación múltiple, en cuyo caso, la frase anterior quedará nula. El Cliente tiene prohibido expresamente sub-licenciar, vender, arrendar o de algún modo distribuir copias del Software. El Cliente está de acuerdo en no desarmar, descompilar, invertir la ingeniería o hacer ningún intento de ningún modo para descubrir u obtener el código fuente del Software. En el caso de hacerse alguna modificación al Software por cualquier persona que no sea E-Sign, todas las garantías respecto de éste finalizarán de inmediato. Los términos de la presente licencia sustituyen

en su totalidad los términos y disposiciones de cualquier licencia que se exija al Cliente en la forma de un acuerdo "click-on" o "click-through" con el fin de descargar u obtener dicho Software.

4.3 Servicios de Instalación. E-Sign enviará a un miembro de su personal de servicios profesionales al sitio del Cliente, durante el número de días que se especifica en el Anexo "E", para instalar el Software (conjuntamente, los "Servicios de Instalación"). E-Sign llevará a cabo los Servicios de Instalación para el Cliente según se especifica en la Declaración de Trabajo individual (la "Declaración de Trabajo"), según los términos y condiciones que se especifican en el Acuerdo. El Cliente reconoce y acepta que el Administrador de Programa de E-Sign está autorizado para formar parte de la Declaración de Trabajo en nombre de E-Sign con la condición que dicha Declaración de Trabajo no modifique los Términos y Condiciones del Acuerdo. Tal modificación deberá ser autorizada y firmada por un funcionario de E-Sign. El Cliente proporcionará espacio de trabajo y dependencias y cualquier otro tipo de servicios y materiales que pueda solicitar razonablemente E-Sign o su personal, con el fin de llevar a cabo los Servicios de Instalación. El Cliente rembolsará a E-Sign por los gastos de bolsillo o viajes en que incurra razonablemente, en relación con el hecho de prestar los servicios de instalación al Cliente (conjuntamente, los "Gastos Reembolsables"). E-Sign le entregará al Cliente las facturas por los Gastos Reembolsables en que incurra conforme al presente documento.

4.4 Derechos de Marca Registrada. E-Sign le otorga al Cliente el derecho y licencia no exclusivos para utilizar los logotipos y marcas registradas pertinentes de E-Sign, durante el período de vigencia del presente Acuerdo, únicamente en los materiales de marketing, avisos publicitarios, hojas con información básica de los productos, envolturas de productos y los sitios Web, en relación con los Productos del Cliente o los Productos y Servicios de E-Sign. E-Sign no otorga ningún derecho sobre ninguna marca registrada, nombre comercial, marca de servicio o renombre comercial propios, salvo según las licencias conforme al presente documento, o por medio de un acuerdo escrito independiente entre las partes. El Cliente acepta cumplir con todos los requisitos de uso establecidos en la versión de la Guía de Uso de Logotipos y Marcas Registradas de E-Sign vigente en ese momento, y las demás guías y procedimientos de E-Sign. Los logotipos y marcas registradas de E-Sign, junto con la Guía de Uso de Logotipos y Marcas Registradas, según se actualicen en forma periódica, se encuentran en http://www.e-sign.cl.

4.5 Marcas de Propiedad y Avisos de Derechos de Autor. El Cliente acepta no eliminar ni destruir ninguna marca o aviso de propiedad, marca registrada o derechos de autor, adherida o contenida en los Productos o los documentos. La adhesión de un aviso de derechos de autor en el Software o los documentos no constituirá una publicación, ni de otro modo afectará la naturaleza confidencial o de secreto comercial del Software o los documentos.

4.6 Utilización de la Información de Estado de Certificado. El Cliente reconoce y acepta que el acceso que el haga, el uso que le de y la confianza que tenga en la Información de Estado de Certificado a que accede por medio de, o que incluye las CRL y/o cualquier Servicio de Validación Premium, están sujetas a y regidas por el Acuerdo de Confianza de E-Sign (el "Acuerdo de Confianza"), que se publica en el Depósito de E-Sign en línea ubicado en la URL HYPERLINK "http://www.e-sign.cl/repository" http://www.e-sign.cl/repositorio, según E-Sign la actualice ocasionalmente. El Acuerdo de Confianza se incorpora al presente Acuerdo con respecto a dicho acceso, uso o confianza.

5. VIOLACIÓN DE LOS DERECHOS DE PROPIEDAD POR E-SIGN.

5.1 Obligación de Defender. Sujeto a la presente Sección 5.1, E-Sign, a costa propia: (i) defenderá o, a opción propia, resolverá cualquier reclamación, juicio o procedimiento contra el Cliente en razón a la violación de alguna patente, derecho de autor o secreto comercial chileno por parte de los Productos o Servicios no modificados que entregue E-Sign, o cualquier reclamación que indique que E-Sign no tiene derecho a proporcionar los Productos o Servicios conforme al presente documento, y (ii) pagará los gastos de cualquier juicio final entablado o resolución en contra del Cliente sobre

dicho tema en tal juicio o procedimiento defendido por E-Sign. E-Sign no tendrá ninguna obligación con el Cliente conforme a la Sección 5.1, a menos que: (A) el Cliente le entregue a E-Sign una notificación por escrito oportunamente de tal reclamación, (B) se le otorgue a E-Sign el derecho a controlar o dirigir la investigación, preparación, defensa o solución de la reclamación y (C) el Cliente le brinde a E-Sign la asistencia e información razonables.

5.2 Opciones de E-Sign. Si E-Sign recibe la notificación de una supuesta violación por parte de los Productos y Servicios, éste tendrá derecho, únicamente a opción propia, a obtener el derecho a continuar la utilización de los Productos o Servicios afectados, o a reemplazar o modificar los Productos o Servicios afectados de tal forma que cese tal violación. Si ninguna de las opciones anteriores está disponible razonablemente para E-Sign, entonces la utilización de los Productos o Servicios afectados deberá finalizar a opción de E-Sign, después de lo cual las partes no tendrán ninguna obligación o responsabilidad adicional, salvo según lo previsto en las Secciones 5.1, 8.5 y 8.6.

5.3 Solución Exclusiva. LOS DERECHOS Y SOLUCIONES QUE SE ESTABLECEN EN LAS SECCIONES 5.1 Y 5.2 CONSTITUYEN LA TOTALIDAD DE LAS OBLIGACIONES DE E-SIGN, Y LAS SOLUCIONES EXCLUSIVAS DEL CLIENTE CON RESPECTO A LA VIOLACIÓN DE LOS DERECHOS DE PROPIEDAD QUE EN RELACIÓN CON LOS PRODUCTOS Y SERVICIOS DE E-SIGN.

6. GARANTÍAS LIMITADAS Y MANTENIMIENTO.

6.1 Garantía Limitada del Cliente. Durante el período de vigencia del presente Acuerdo, y siempre que el Cliente continúe emitiendo Certificados, éste último garantiza a E-Sign que: (i) toda la información fundamental para la emisión de un Certificado y validada por el Cliente es verdadera y correcta en todos sus aspectos esenciales y (ii) sin limitar la generalidad de lo anterior, la aprobación del Cliente de las Solicitudes de Certificado no resultará en una Emisión Errónea, incluyendo, entre otros, la Emisión Errónea que resulta de la Suplantación de Identidad.

6.2 Garantías Limitadas de E-Sign. Durante el período de vigencia del presente Acuerdo, E-Sign garantiza que la Clave Privada del Cliente no ha sido comprometida, siempre que E-Sign no haya entregado una notificación al Cliente indicando lo contrario. E-Sign le garantiza al Cliente que al momento que emite un Certificado en virtud del presente documento: (i) E-Sign no originó ninguna falsa declaración fundamental de hecho en tal Certificado, (ii) E-Sign no introdujo ningún error en la información de tal Certificado, (iii) dicho Certificado cumple con todos los requisitos fundamentales de la normativa CPS, para cualquier certificado emitido dentro del subdominio de E-Sign de la red VTN, y (iv) E-Sign ha cumplido de modo substancial con la normativa CPS, para cualquier certificado emitido dentro del subdominio de E-Sign de la red VTN, al emitir el Certificado. E-Sign garantiza además que los Servicios se proporcionarán de acuerdo con el SLA según se establece en el Anexo “D”.

6.3 Virus. E-Sign ha hecho y hará todos los esfuerzos comercialmente razonables para asegurar que cada uno de los Productos entregados conforme al presente Acuerdo esté libre de cualquier “virus” informático, “gusano” y otros códigos ilícitos, y acepta notificar oportunamente al Cliente sobre cualquiera de ellos una vez descubierto en alguno de los Productos.

6.4 Limitaciones Adicionales sobre las Garantías de E-Sign. Las garantías limitadas de E-Sign en las Secciones 6.2 y 6.3 no serán aplicables a ningún incumplimiento que resulte de (i) las adaptaciones, mejoras o modificaciones que haga el Cliente a los Productos o Servicios, (ii) el uso de los Productos o Servicios con software, hardware o firmware de terceros no proporcionado por E-Sign o (iii) datos de fecha y otras entradas de datos, o salidas, según corresponda, incorrectos, del Cliente, un tercero o software, hardware o firmware de terceros no proporcionado por E-Sign.

6.5 “TAL CUAL". SALVO POR LAS GARANTÍAS LIMITADAS EXPRESAS CONTENIDAS EN LA PRESENTE SECCIÓN, Y EN LOS ANEXOS PERTINENTES, SI LOS HAY, E-SIGN NO ELABORA NINGUNA OTRA

GARANTÍA EN ABSOLUTO. E-SIGN RENUNCIA POR MEDIO DEL PRESENTE DOCUMENTO A TODA GARANTÍA DE CUALQUIER TIPO, EXPRESA, IMPLÍCITA O POR DISPOSICIÓN LEGAL, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO, CUMPLIMIENTO DE LOS REQUISITOS DEL CLIENTE O, SALVO SEGÚN SE ESTABLECE EN LA SECCIÓN 5.1, LA NO CONTRAVENCIÓN DE LOS DERECHOS DE TERCEROS. VERISIGN RENUNCIA POR MEDIO DEL PRESENTE DOCUMENTO A TODAS LAS GARANTÍAS, EXPRESAS, IMPLÍCITAS O POR DISPOSICIÓN LEGAL, INCLUYENDO, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO O LA NO CONTRAVENCIÓN DE LOS DERECHOS DE TERCEROS.

6.6 Responsabilidad del Cliente en Relación con la Validación. EL CLIENTE SERÁ EL ÚNICO RESPONSABLE, ANTE CUALQUIERA Y TODAS LAS PERSONAS, POR LA VALIDACIÓN DE TODAS LAS SOLICITUDES DE CERTIFICADO QUE APRUEBE Y POR LA CONDUCTA DE LOS ADMINISTRADORES DEL CLIENTE Y/O RAA. E-SIGN RENUNCIA A TODA RESPONSABILIDAD. EL CLIENTE SE RECONOCE COMO EL ÚNICO RESPONSABLE DE LA IDONEIDAD DE LOS PRODUCTOS Y SERVICIOS PARA SU APLICACIÓN Y USO DESEADOS. E-SIGN NO GARANTIZA QUE LOS PRODUCTOS Y/O SERVICIOS PROPORCIONADOS CONFORME AL PRESENTE DOCUMENTO CUMPLAN CON LOS REQUISITOS DEL CLIENTE.

7. LIMITACIÓN DE RESPONSABILIDAD.

SALVO POR EL INCUMPLIMIENTO DE LA SECCIÓN 3, NINGUNA DE LAS PARTES SERÁ RESPONSABLE ANTE LA OTRA PARTE O ANTE UN SUSCRIPTOR, O ANTE OTRA PARTE, POR NINGÚN DAÑO CONSECUENCIAL, INDIRECTO, ESPECIAL, INCIDENTAL O EJEMPLAR, YA SEA PREVISIBLE O IMPREVISIBLE (INCLUYENDO, ENTRE OTROS, DAÑOS POR LA PÉRDIDA DE DATOS, RENOMBRE COMERCIAL, UTILIDADES, INVERSIONES, USO DE DINERO O USO DE DEPENDENCIAS, INTERRUPCIÓN EN EL USO O DISPONIBILIDAD DE LOS DATOS, SUSPENSIÓN DE OTROS TRABAJOS O DETERIORO DE OTROS VALORES, AUN CUANDO DICHA PARTE HAYA SIDO ADVERTIDA DE LA POSIBILIDAD DE TALES DAÑOS), QUE SURJA DEL PRESENTE ACUERDO, LOS PRODUCTOS O SERVICIOS, INCUMPLIMIENTO DE CONTRATO O CUALQUIER GARANTÍA, YA SEA EXPRESA O IMPLÍCITA, O INDEMNIZACIÓN CONFORME AL PRESENTE ACUERDO, O DE OTRO MODO, FALSA DECLARACIÓN, NEGLIGENCIA, RESPONSABILIDAD ESTRICTA U OTRA RESPONSABILIDAD CIVIL. SALVO POR EL INCUMPLIMIENTO DE LA SECCIÓN 3, BAJO NINGUNA CIRCUNSTANCIA LA RESPONSABILIDAD DE NINGUNA DE LAS PARTES ANTE LA OTRA PARTE O ANTE UN SUSCRIPTOR O CUALQUIER OTRA PARTE, QUE SURJA DE O RELACIONADA CON EL PRESENTE ACUERDO, LOS PRODUCTOS O SERVICIOS, EXCEDERÁ DOS (2) VECES LOS MONTOS PAGADOS POR EL CLIENTE CONFORME AL PRESENTE ACUERDO PARA UN MÁXIMO DE CIENTO TREINTA MIL DÓLARES ($130.000 US.) (Nota: la obligación legal es de 5.000 UF que corresponde a $130.000 US, aproximadamente.) SIN IMPORTAR SI ALGUNA DE LAS ACCIONES O RECLAMACIONES SE BASA EN DICHO CONTRATO, GARANTÍA, INDEMNIZACIÓN, NEGLIGENCIA, RESPONSABILIDAD ESTRICTA U OTRA RESPONSABILIDAD CIVIL U OTRO. EL CLIENTE TOMARÁ LAS PRECAUCIONES RAZONABLES PARA ASEGURAR QUE LOS TÉRMINOS Y CONDICIONES ESTABLECIDAS EN LA PRESENTE SECCIÓN SE INCORPOREN EN CUALQUIER ACUERDO ENTRE EL CLIENTE Y UN SUSCRIPTOR. LA PRESENTE SECCIÓN SUSTITUYE CUALQUIER OTRA SECCIÓN DEL PRESENTE ACUERDO QUE NO SEA CONSISTENTE CON ÉSTA. VERISIGN RENUNCIA A TODA RESPONSABILIDAD CON EL CLIENTE CONFORME AL PRESENTE ACUERDO.

8. TÉRMINO Y FINALIZACIÓN.

8.1 Término. El presente Acuerdo se hará efectivo a partir de la Fecha de Vigencia establecida en la primera página del presente documento, y seguirá vigente durante el término inicial que se establece en la primera página del mismo. Después de la expiración del término inicial, el presente Acuerdo podrá ser renovado por un término adicional con el acuerdo mutuo de E-Sign y el Cliente.

8.2 Finalización por Incumplimiento. Ambas partes tendrán derecho a finalizar el presente Acuerdo en el caso de un incumplimiento por la otra parte de sus obligaciones fundamentales conforme a

éste, si dicho incumplimiento no se repara en el plazo de sesenta (60) días una vez recibida la notificación de la misma de la parte no causante del incumplimiento, o en el plazo de diez (10) días una vez recibida tal notificación, si ésta se relaciona con el pago de tasas u otros montos adeudados conforme al presente documento, o un incumplimiento por parte del Cliente que comprometa de algún modo la seguridad de los Servicios.

8.3 Cesión. Ambas partes tendrán derecho a finalizar el presente Acuerdo si llegare a ocurrir una supuesta Cesión del mismo como contravención de la Sección 9.2.

8.4 Insolvencia. El presente Acuerdo finalizará con la elección y la notificación de una parte ante la otra, si ésta es declarada insolvente o en quiebra, o el establecimiento de cualquier procedimiento por o en contra de la otra parte que busca redención, la reorganización o disposición conforme a cualquier ley que tenga relación con la insolvencia, o cualquier cesión para el beneficio de los acreedores, o el nombramiento de un receptor, liquidador o consignatario de cualquiera de las propiedades o valores de la otra parte, o la liquidación, disolución o terminación de las actividades comerciales de la otra parte.

8.5 Efecto de la Finalización. Una vez expirado o finalizado el presente Acuerdo por el motivo que sea, cesará todo uso que haga el Cliente de los Productos y Servicios, y éste pagará a E-Sign todas las tasas y otros montos acumulados.

8.6 Mantenimiento de la Vigencia de Ciertos Términos. Las disposiciones de las Secciones 2, 3, 4, 5, 6.5, 7, 8.4, 8.5, 8.6 y 9 se mantendrán vigentes después del término del presente Acuerdo.

9. GENERAL.

9.1 Ley Vigente. El presente Acuerdo estará regido por las leyes de la jurisdicción de Chile (independientemente de su alternativa jurídica). Las partes acuerdan que la Convención de las Naciones Unidas sobre Contratos de Venta Internacional de Mercaderías no será aplicable a este Acuerdo.

9.2 Obligatoriedad para los Sucesores; Cesión. El presente Acuerdo será obligatorio para los sucesores, ejecutores, herederos, representantes, administradores y cesionarios de las partes de éste. Sin perjuicio de lo anterior, ninguna de las partes tiene derecho a efectuar una Cesión del presente Acuerdo sin el previo consentimiento por escrito de la otra parte. Dicha supuesta Cesión del presente Acuerdo sin obtener el consentimiento por escrito será considerada nula y sin efecto, y le permitirá a la otra parte finalizar el presente Acuerdo conforme a la Sección 8.3.

9.3 Divisibilidad; Aplicación; Sin Renuncia. La inaplicabilidad de cualquiera de las disposiciones del presente Acuerdo no afectará la aplicabilidad de ninguna de las partes de éste. Si alguna de las disposiciones del presente Acuerdo se considera inválida o inaplicable, en su totalidad o en parte, el presente Acuerdo se considerará modificado para eliminar o alterar, según corresponda, la disposición inválida o inaplicable con el fin de volverla válida, aplicable y, en el grado posible, consecuente con la intención original de las partes. La imposibilidad de una de las partes, en cualquier momento u ocasionalmente, de exigir el cumplimiento de las obligaciones de la otra parte en virtud del presente Acuerdo, no será considerada una renuncia y no afectará su derecho para hacer cumplir cualquiera de las disposiciones de éste en un momento posterior.

9.4 Indivisibilidad del Acuerdo. El presente Acuerdo y los Anexos de éste responden por entero a lo que se ha acordado y convenido entre las partes, ya sea por escrito u oralmente, con respecto al tema objeto de éste, y sustituyen todos los acuerdos o convenios previos y coetáneos entre las partes, con respecto a los Productos y Servicios adquiridos por el Cliente conforme al presente Acuerdo.

9.5 Modificación y Renuncias. Cualquiera de los términos o disposiciones del presente Acuerdo podrá ser modificado, y se podrá renunciar al cumplimiento de cualquier término de éste, únicamente por medio de un escrito firmado por las partes obligadas por éste.

9.6 Uso Permitido. El uso permitido por parte del Cliente de los Productos o Servicios, o cualquier tipo de software o hardware provisto con estos, se limita únicamente al uso establecido en el presente Acuerdo.

9.7 Comisiones de Abogados. En cualquiera de las acciones para hacer cumplir o interpretar alguna de las partes del presente Acuerdo, la parte prevaleciente tendrá derecho a recuperar, como elemento de los costos de juicio y no como daños, las comisiones de abogados razonables que serán fijadas por el tribunal (incluyendo, entre otros, los costos, gastos y comisiones sobre cualquier apelación).

9.8 Avisos. Salvo según lo indiquen los Anexos del presente Acuerdo, cualquier notificación, demanda o solicitud con respecto al presente Acuerdo se hará por escrito y será efectiva en la fecha de recepción (a menos que la notificación especifique una fecha posterior), únicamente si se envía a través de un servicio de mensajería que confirme la entrega por escrito, o si se envía por correo certificado, franqueo pagado, acuse de recibo del remitente solicitado, a la siguiente dirección:

E-Sign: A la dirección que se indica en la página 1.
Atención:
Cliente: Al Contacto del Cliente en la dirección que se indica en la página 1.

Ninguna de las notificaciones, demandas o solicitudes con respecto al presente Acuerdo podrá entregarse por medio de correo electrónico, a menos que así lo indiquen los Anexos del presente Acuerdo, y E-Sign retenga la evidencia de tal entrega. Cualquiera de las partes podrá cambiar su dirección para tales comunicaciones, dando notificación de ello a la otra parte de conformidad con la presente Sección. Cada una de las partes notificará de inmediato a la otra sobre cualquier aviso legal recibido que pudiera afectar a la otra parte, y enviará oportunamente el original o una copia de tal aviso a dicha parte.

9.9 No Revelación de los Términos del Acuerdo. Ninguna de las partes revelará los términos y condiciones del presente Acuerdo sin el previo consentimiento por escrito de la otra parte, salvo que cada una de ellas pueda: (i) hacer tales revelaciones ya que son necesarias para cumplir con las leyes, normas y reglamentos vigentes, o son necesarias para hacer cumplir el presente Acuerdo, (ii) revelar los términos del presente Acuerdo a los auditores, abogados, agentes bancarios o aseguradores de dicha parte, según sea necesario para el cumplimiento de los servicios para una de las partes o (iii) revelar que el Cliente es un cliente de E-Sign y los productos del Cliente anunciados públicamente que dan acceso a los Certificados. Las partes elaborarán un comunicado de prensa, que aprobarán para su publicación, el cual anuncia su relación conforme al presente Acuerdo.

9.10 Terceros Beneficiarios. Ninguna de las disposiciones del presente Acuerdo tiene la intención, ni se interpretará como si la tuviera, de proporcionar o crear derechos de terceros beneficiarios, o ningún otro derecho de ningún tipo para ninguna otra parte, salvo según se establezca en la presente Sección. Sin prejuicio de lo anterior, los proveedores de los productos de E-Sign que se entregan conforme al presente documento gozarán de los mismos descargos de garantía, limitaciones de responsabilidad y disposiciones liberadoras con respecto a tales productos similares a las de E-Sign. El Cliente ha sido, en este acto, notificado que VeriSign, Inc., una sociedad constituida bajo las leyes de Delaware, ubicada en 487 East Middlefield Road, Mountain View, California 94043, es un tercero beneficiario en este Acuerdo en la medida que el presente Acuerdo contenga disposiciones que se relacionen con el uso que el Cliente hace de los Productos o Servicios de E-Sign licenciados o proporcionados por este medio. Dichas disposiciones están expresamente hechas para el beneficio de E-Sign y son exigibles por VeriSign adicionalmente a E-Sign.

9.11 Ejemplares. El presente Acuerdo podrá ejecutarse en uno o más ejemplares, cada una de los cuales será considerado un original, pero que conjuntamente constituirán el mismo instrumento.

9.12 Autorización Debida. Cada una de las partes, en este acto, asevera y garantiza a la otra parte que el particular que ejecuta el presente Acuerdo en nombre de dicha parte, está debidamente autorizado para hacerlo, y para obligar a dicha parte por este medio.

9.13 Partes Independientes. La relación entre E-Sign y el Cliente es la de contratistas independientes. Ninguna de las partes, ni sus empleados, consultores, contratistas o agentes, son representantes, empleados o sociedades conjuntas de la otra parte, ni tienen ninguna autoridad para comprometer a ésta a través de un contrato u otro medio a ninguna obligación. Cada una de las partes garantizará que las personas recién indicadas no se representarán, ya sea de modo expreso o implícito, en apariencia o de algún otro modo. E-Sign retendrá el derecho a llevar a cabo el trabajo y proporcionar los Productos o Servicios a terceros durante el período de vigencia del presente Acuerdo.

10. DEFINICIONES.

Además de los términos definidos en otras partes del presente Acuerdo, los siguientes términos en mayúscula, cuando se usen en el presente Acuerdo, responden a los siguientes significados:

Equipo del Administrador consiste en una tarjeta inteligente, un lector de tarjetas inteligentes, el software y un (1) Certificado de Administrador.

Certificado del Administrador se refiere al Certificado emitido por E-Sign al empleado del Cliente designado como Administrador Managed PKI para acceder al Centro de Control Managed PKI para cumplir las funciones de Administrador.

Entidad Afiliada se refiere a una entidad que tiene relación con otra entidad en la forma de: (i) compañía matriz, Universal Service Center, filial, socio, sociedad conjunta, socio conjunto, contratista o representante de tal entidad, (ii) miembro de una comunidad de interés registrada de E-Sign o (iii) entidad que mantiene una relación con la otra entidad en el lugar donde ésta realiza actividades comerciales u otros registros que proporcionen garantías apropiadas de la identidad de dicha entidad.

Particular Afiliado se refiere a una persona que se afilia a una organización en la forma de: (i) funcionario, directivo, empleado, socio, contratista, residente u otra persona dentro de la organización o (ii) persona que mantiene una relación contractual con la organización en el lugar donde ésta mantiene registros comerciales que proporcionen garantías sólidas de la identidad de dicha persona.

Cesión se refiere a la cesión, sub-licencia, venta, transferencia por una parte, salvo cualquier transferencia por fusión, adquisición, consolidación, reorganización o cualquier transferencia de participación mayoritaria del cincuenta por ciento (50%) o más de los valores con derecho a voto de la parte.

Unidad de Procesamiento Central ("CPU") se refiere a un dispositivo único que ejecuta un sistema operativo único que aparece en la red como un solo aparato.

Certificado, Certificado Digital o Certificado de Clave Pública se refiere a un mensaje que, como mínimo, declara un nombre o identifica la CA, identifica al Suscriptor, contiene la clave pública del Suscriptor, identifica el período operativo del Certificado, contiene un número de serie del Certificado y está firmado digitalmente por la CA.

Solicitante de Certificado se refiere a una persona o representante autorizado que solicita la emisión de un Certificado de Clave Pública a la CA.

Solicitud de Certificado se refiere a un Solicitante de Certificado (o un representante autorizado) que solicita a una CA o RA la emisión de un Certificado.

Lista de Revocación de Certificados ("CRL") se refiere a una lista emitida periódicamente (o según se exija), firmada digitalmente por una CA, de los Certificados identificados que han sido suspendidos o revocados antes de las fechas de expiración. La lista generalmente indica el nombre del emisor de la CRL, la fecha de emisión, la fecha de la próxima emisión de CRL programada, los números de serie de los certificados suspendidos o revocados y los momentos y razones específicas para la suspensión y revocación.

Servicio de Certificado se refiere al servicio desarrollado por E-Sign para el Cliente según se describe en mayor detalle en los Anexos "A" y "B".
Unidad de Firma de Certificado ("CSU") se refiere a una unidad de hardware o software diseñados para el uso en la firma de Certificados y el almacenamiento de claves.
Información de Estado de Certificado se refiere a la información relacionada con la suspensión o revocación de Certificados antes de su expiración normal. Dicha información generalmente incluye los números de serie de los certificados suspendidos o revocados y los momentos y razones específicas para la suspensión y revocación.
Autoridad de Certificación ("CA") se refiere a una Persona (ver definición para Persona) autorizada para emitir, gestionar, revocar y renovar Certificados en la red VTN.
Normativa del Proceso de Certificación ("CPS") se refiere a la Normativa del Proceso de certificación de E-Sign, según se modifique ocasionalmente, a la cual puede accederse en el HYPERLINK "http://www.e-sign.cl/repository/cps" http://www.e-sign.cl/repositorio/cps.
Certificado de Cliente se refiere a un Certificado x.509 que se emite para el uso en sistemas de usuario final, tales como exploradores, software de correo electrónico y dispositivos inalámbricos.
Información Confidencial se refiere al significado que se le atribuye en la Sección 3.1 del presente Acuerdo.
Productos del Cliente se refiere a cualquier producto desarrollado o proporcionado por el Cliente para el uso por los Suscriptores de éste con un Certificado emitido por E-Sign conforme al presente Acuerdo.
Firmas Digitales se refiere a la transformación de un mensaje, utilizando un sistema criptográfico asimétrico, de tal forma que una persona que tenga el mensaje inicial y la clave pública del firmante, pueda determinar de manera exacta si la transformación fue creada usando la Clave Pública que corresponde a la Clave Pública del firmante, y si el mensaje ha sido alterado desde que se hizo la transformación.
Recuperación de Claves Erróneas se refiere a: (a) la recuperación y transmisión de una Clave Privada en un modo no fundamentalmente de acuerdo con los procedimientos exigidos en el Manual del Administrador Managed PKI, (b) la recuperación y transmisión de una Clave Privada para una Persona que no sea el Suscriptor que es el poseedor legítimo de la Clave Privada y (c) la recuperación y transmisión de una Clave Privada sin la autorización del Suscriptor que es el poseedor legítimo de dicha Clave Privada. Sin perjuicio de los anterior, la "Recuperación de Claves Erróneas" no incluye: (a) la recuperación que haga el Cliente de la Clave Privada de un Suscriptor y la transmisión a las autoridades judiciales en respuesta a un mandato de registro o citación legal; (b) la recuperación que haga el Cliente de la Clave Privada de un Suscriptor y la transmisión en respuesta a un proceso judicial o administrativo o (c) la recuperación que haga el Cliente de la Clave Privada de un Suscriptor para obtener acceso a mensajes que se pretende descifrar por medio del uso de dicha Clave Privada, incluso sin la autorización del Suscriptor, para los fines comerciales legítimos y legales del Cliente.
Emisión Errónea se refiere a: (a) la emisión de un Certificado de una manera que no concuerda fundamentalmente con los procedimientos exigidos por la normativa CPS o el Manual del Administrador Managed PKI; (b) la emisión de un Certificado (que no sea el Certificado de Clase 1) a una Persona que no es sujeto de tal Certificado o (c) la emisión de un Certificado (que no sea el Certificado de Clase 1) sin la autorización de la Persona que es sujeto de tal Certificado.
Global Server ID se refiere a un Certificado de Servidor que se utiliza para soportar sesiones SSL entre clientes Web y servidores Web que son cifradas utilizando protección criptográfica conforme a las leyes de exportación vigentes.
Jerarquía se refiere a un dominio que consiste en un sistema de CA que emitió Certificados en una cadena que va desde una CA superior, pasando por una o más CA subordinadas, hasta los Suscriptores.
Suplantación de Personalidad se refiere a la solicitud y la emisión de un Certificado que se basa en información falseada o adulterada que tiene relación con el nombre o la identidad.
Internet se refiere a la red informática global.
Generación de Claves se refiere a los procedimientos de E-Sign para la apropiada generación de la Clave Pública y la Clave Privada del Cliente vía un proceso confiable, y para el almacenamiento de la Clave Privada del Cliente y los documentos de ésta.

Administrador de Claves se refiere a la persona que utilizará sistemas confiables para generar pares de claves, enviar la información de recuperación de Claves Públicas y Claves Privadas a E-Sign, almacenar las Claves Privadas y transmitir las Claves Privadas a los Suscriptores.
Guía del Administrador de Servicios de Gestión de Claves se refiere al documento que define las obligaciones, responsabilidades y funciones básicas disponibles para los Administradores de Claves, y que se publica en http://www.e-sign.cl.
Suplantación de Identidad de la Recuperación de Claves se refiere a la solicitud y la recepción que hace una Persona al Cliente de la Clave Privada del Suscriptor entregando información falsa o adulterada que tiene relación con el nombre o la identidad que indica que tal Persona es dicho Suscriptor.
Autoridad de registro ("RA") se refiere a una entidad que ha recibido la autorización de una CA para asistir a las personas que solicitan Certificados, revocan (o cuando se les autoriza, suspenden) sus Certificados o ambos, y también aprobar dichas solicitudes. Una RA no es representante de un solicitante de Certificado. Una RA podrá delegar la autoridad para aprobar las solicitudes de certificado únicamente a los RAA de la RA autorizados.
Administrador de Autoridad de Registro ("RAA") se refiere a un empleado de una RA que es responsable de llevar a cabo las funciones de tal RA.
Certificado RAA se refiere al Certificado de Clase 3 de E-Sign emitido para un RAA.
OCSP se refiere al "Protocolo de Estado de Certificado en Línea", que es un protocolo para proporcionar a los Destinatarios del Acuerdo de Confianza la Información de Estado de Certificado en tiempo real, y al que los clientes que adquirieron el soporte OCSP pueden acceder consultando el Contestador OCSP apropiado de E-Sign en la URL especificada por E-Sign.
Manual del Administrador Managed PKI se refiere al documento que define las obligaciones, responsabilidades y funciones básicas disponibles para los Administradores Managed PKI, y que se publica en http://www.e-sign.cl.
Centro de Control Managed PKI se refiere a la interfaz del Cliente para las tareas que se llevarán a cabo en la administración del programa de Certificado de la organización. Cada una de las páginas html en el Centro de Control incluye ayuda en línea para guiar al Cliente durante el proceso. El Centro de Control se organiza en áreas funcionales que reflejan las responsabilidades del Cliente en relación con Managed PKI.
Managed PKI para SSL se refiere a un Servicio que permite al Cliente convertirse en una RA dentro del subdominio de E-Sign en la red VTN para asistir a una CA en la emisión de Certificados de Servidor dentro de los dominios designados.
Managed PKI para SSL Premium se refiere a un Servicio que permite al Cliente convertirse en una RA dentro del subdominio de E-Sign en la red VTN para asistir a una CA en la emisión de Global Server ID dentro de los dominios designados.
Período Operativo se refiere al período que se inicia con la fecha y hora de emisión del Certificado (o la fecha y hora posteriores confirmadas en el Certificado) y que termina con la fecha y hora en que dicho Certificado expira o se suspende o revoca prematuramente.
Persona se refiere a una persona u organización (o un dispositivo bajo el control de una persona u organización) capaz de firmar o verificar un mensaje, ya sea legalmente o de hecho.
CRL Premium se refiere a las CRL que E-Sign actualiza con mayor frecuencia que las CRL estándar, y las pone disponibles a los clientes que hayan adquirido el acceso de CRL Premium en una URL especificada por E-Sign.
Autoridad de Certificación Primaria ("PCA") se refiere a una persona u organización que establece prácticas para todas las Autoridades de Certificación y los usuarios dentro de su dominio.
Jerarquía Privada se refiere a un dominio que consiste en un sistema de CA que emitió Certificados en una cadena que va desde la PCA del Cliente, pasando por una o más CA, hasta los Suscriptores, de acuerdo con las prácticas del Cliente. Los Certificados emitidos en una Jerarquía Privada tienen la intención de satisfacer las necesidades de las organizaciones que autorizan su emisión, y no pretenden utilizarse en la interacción entre las organizaciones y/o particulares a través de canales públicos.
Clave Privada se refiere a una clave matemática (mantenida en secreto por el portador) que se utiliza para crear Firmas Digitales y, dependiendo del algoritmo, para descifrar mensajes o archivos cifrados (para fines de confidencialidad) con la correspondiente Clave Pública.

Productos se refiere a cualquier producto proporcionado por E-Sign conforme al presente Acuerdo y los Anexos pertinentes, incluyendo, entre otros, el Software.
Jerarquía Pública se refiere a un dominio que consiste en un sistema de CA que emitió Certificados en una cadena que va desde VeriSign Root o la PCA pertinente, pasando por una o más CA, hasta los Suscriptores, de acuerdo con la normativa CPS. Los Certificados emitidos en una Jerarquía Pública pretenden ser interoperables entre las organizaciones, permitiendo a los Suscriptores interactuar a través de canales público con diversos particulares, organizaciones y redes.
Clave Pública se refiere a una clave matemática que puede hacerse disponible al público, y que se utiliza para verificar las firmas creadas con su correspondiente Clave Privada. Según el algoritmo, las Claves Públicas se utilizan también para descifrar mensajes o archivos que puede luego descifrarse con la correspondiente Clave Privada.
Puesto – se refiere a una persona que se identifica en la primera solicitud de certificado de la persona aprobada por el Cliente conforme al presente Acuerdo. Si el Cliente aprueba cualquier solicitud de certificado posterior entregada por tal persona, la solicitud de certificado posterior no se considerará como un puesto adicional.
Certificado de Servidor se refiere a un Certificado X.509 que se emite a una organización para permitir el uso del protocolo Secure Sockets Layer ("SSL") en su sitio Web. Los Certificados de Servidor le permiten al destinatario del acuerdo de confianza constatar la identidad de la organización con la cual establecerá una sesión SSL.
Servicios se refiere a cualquier Servicio proporcionado por E-Sign conforme al presente Acuerdo y los Anexos pertinentes.
Acuerdo de Nivel de Servicios ("SLA") se refiere a la versión vigente en ese momento del Acuerdo de Nivel de Servicios de E-Sign, según se modifique ocasionalmente, que detalla los términos para los Servicios proporcionados por E-Sign al Cliente para la operación de los Servicios Managed PKI de éste, incluyendo los Servicios de Certificado Managed PKI Private Label y los Servicios de Certificado Co-Comercializado Managed PKI que se establecen en los Anexos "A" y "B", respectivamente y según corresponda.
Software se refiere a todo el software de E-Sign licenciado al Cliente conforme al presente Acuerdo y según se indique en el Anexo "E" o según E-Sign lo licencie posteriormente al Cliente conforme al presente Acuerdo.
Suscriptores se refiere a una persona que es sujeto de, o ha recibido un Certificado y es capaz de utilizar, y está autorizado a utilizar, la Clave Privada que corresponde a la Clave Pública que aparece en el Certificado.
Acuerdo del Suscriptor se refiere al acuerdo celebrado entre un suscriptor y una CA o RA para prestar servicios de certificación pública designada dentro del subdominio de E-Sign de la red VTN de acuerdo con la normativa CPS.
VeriSign Root es una CA que registra las PCA por medio del registro de la Clave Pública auto-firmada de cada PCA.
VeriSign Trust NetworkSM ("VTN") se refiere a la infraestructura de clave pública global que proporciona Certificados tanto para las aplicaciones fijas como inalámbricas, y que es provista por VeriSign, Inc., y su red global de filiales de acuerdo con la Políticas de Certificados VeriSign Trust Network, la principal declaración de política que regula la red VTN (a la que se puede tener acceso en http://www.verisign.com/repository/vtnCp.html).
Web se refiere al sistema denominado "World Wide Web", un sistema de información distribuida por medio de enlaces que se basa en hipertextos, en la cual los usuarios pueden crear, editar, publicar, enlazar, navegar y recuperar documentos de hipertexto que residen en la Internet.
Servicios Managed PKI Inalámbricos se refiere al Servicio de Certificado por medio del cual E-Sign proporciona Certificados a los clientes que utilizan dispositivos inalámbricos.
Portal WPKI se refiere al software que facilita la emisión y administración de los Certificados del Cliente para los dispositivos inalámbricos.

Anexo "A":
Servicios de Certificación Private Label

Antecedentes

El Cliente desea: (i) emitir, administrar, revocar y/o renovar Certificados digitales para clientes fijos y/o inalámbricos en una Jerarquía Privada marcada con el nombre comercial del Cliente, que se basa en las Solicitudes de Certificado entregadas, validadas y aprobadas por éste y (ii) subcontratar con E-Sign las funciones de emisión, administración, revocación y/o renovación de tales Certificados; y al mismo tiempo no desea (iii) retener para sí las funciones de validación y aprobación de las Solicitudes de Certificado, y solicitar la revocación o renovación de éstos. VeriSign le ofrece al Cliente Certificados para lo clientes fijos conforme al programa Managed PKI de E-Sign, y Certificados para los clientes inalámbricos conforme al programa de Servicios Managed PKI Inalámbricos de E-Sign.

TÉRMINOS Y CONDICIONES

1. Servicios Aplicables.

El Anexo "A" regula los términos y condiciones por medio de los cuales E-Sign proporciona los servicios de certificación private label que se indican a continuación:

Servicios de Certificación Managed PKI Private Label para clientes fijos (marcar cuadro e inicial)
Servicios Managed PKI Inalámbricos Private Label para clientes inalámbricos (marcar cuadro e inicial)

2. Obligaciones del Cliente.

2.1 Nombramientos. El Contacto del Cliente nombrará uno o más empleados del Cliente autorizados como sus administradores (los "Administradores").

2.2 Funciones del Administrador. El Cliente, por medio de su Administrador, validará la información que aparece en las Solicitudes de Certificado, aprobará o rechazará tales Solicitudes de Certificado, utilizará el hardware y el software designados por E-Sign e instruirá a E-Sign con respecto a la emisión, renovación y revocación de los Certificados, de acuerdo con el Manual del Administrador Managed PKI. El Cliente transmitirá a E-Sign cualquier solicitud que pudiera tener para la revocación de Certificados emitidos por él. Si un Administrador ya no tiene la autoridad para actuar como tal en nombre del Cliente, el Contacto del Cliente solicitará oportunamente la revocación de su Certificado de Administrador.

2.3 Garantía Limitada del Cliente. Durante el período de vigencia del presente Acuerdo, y siempre que el Cliente continúe emitiendo Certificados, éste último garantiza a E-Sign que: (i) toda la información fundamental para la emisión de un Certificado y validada por el Cliente es verdadera y correcta en todos sus aspectos esenciales y (ii) sin limitar la generalidad de lo anterior, la aprobación del Cliente de las Solicitudes de Certificado no resultará en una Emisión Errónea, incluyendo, entre otros, la Emisión Errónea que resulta de la Suplantación de Identidad.

3. Obligaciones de E-Sign.

E-Sign le proporcionará al Cliente los Servicios indicados en el Anexo "A" por un período de doce (12) meses a partir de la Fecha de Vigencia del presente Acuerdo (el "Período de Servicio"). E-Sign emitirá, administrará, revocará y/o renovará los Certificados de acuerdo con las instrucciones provistas por el Cliente, y sus Administradores emitirán, administrarán, revocarán y/o renovarán los Certificados para clientes fijos y/o inalámbricos de acuerdo con las instrucciones provistas por el Cliente y sus Administradores.

3.1 Certificado del Administrador. Una vez aprobada la Solicitud de Certificado del Administrador, E-Sign emitirá un Certificado de Administrador para cada uno de los Administradores. Tales Certificados tendrán una validez de doce (12) meses junto con el Período de Servicio Managed PKI.

3.2 Emisión de Certificado. Después de la aprobación de una Solicitud de Certificado por el Cliente, E-Sign: (i) tendrá derecho a confiar en la exactitud de la información de cada una de las Solicitudes de Certificado aprobadas y (ii) emitirá un Certificado para el Solicitante de Certificado que presenta dicha Solicitud de Certificado.

3.3 Ciclo Vital de Certificado. Los Certificados emitidos o licenciados conforme al presente Acuerdo tienen un período máximo de validez de doce (12) meses a partir de la fecha en que se emite cada Certificado.

3.4 Generación de Claves CA. Durante un evento único de Generación de Claves CA, E-Sign generará pares de claves CA para que el Cliente utilice en todos los Certificados emitidos por E-Sign que se usan en la Jerarquía Privada del Cliente. La Clave Privada del Cliente de cada uno de los pares de claves se almacenará en una o más Unidades de Firma de Certificados. Podrán generarse pares de claves extras para CA adicionales en una fecha posterior, si el Cliente solicita una tasa adicional.

Anexo "B":
Servicios de Certificación Co-Comercializada

Antecedentes
El Cliente desea convertirse en una Autoridad de Certificación y/o Autoridad de registro que no tenga relación con E-Sign dentro del subdominio de E-Sign en la red VTN. En la medida que el Cliente desea emitir Certificados de Cliente para los clientes fijos y/o inalámbricos, busca convertirse en una Autoridad de Certificación dentro del subdominio de E-Sign en la red VTN, y busca subcontratar con E-Sign las funciones de emisión, administración, revocación y/o renovación de los Certificados de Cliente, mientras retiene para sí las funciones de Autoridad de Registro de una Autoridad de Certificación, es decir, la validación y aprobación de Solicitudes de Certificado y la solicitud de revocación o renovación de los Certificados de acuerdo con la normativa CPS y el Manual del Administrador Managed PKI. En la medida que el Cliente desea convertirse en una Autoridad de Registro dentro del subdominio de E-Sign en la red VTN, busca validar y aprobar Solicitudes de Certificado y solicitar la revocación o renovación de Certificados de Servidor de acuerdo con la normativa CPS y el Manual del Administrador Managed PKI, en nombre de la Autoridad de Certificación de E-Sign, que emitirá, administrará, revocará y/o renovará los Certificados de acuerdo con las instrucciones del Cliente y la normativa CPS. E-Sign le ofrece al Cliente Certificados para lo clientes fijos conforme al programa Managed PKI de E-Sign, y Certificados para los clientes inalámbricos conforme al programa de Servicios Managed PKI Inalámbricos de [E-Sign]. Los Certificados de Servidor se emiten conforme a los Programas Managed PKI para SSL y Managed PKI para SSL Premium.

TÉRMINOS Y CONDICIONES
1. Servicios Aplicables.
El Anexo "B" regula los términos y condiciones por medio de los cuales E-Sign proporciona los servicios de certificación co-comercializados que se indican a continuación:

Servicios de certificación co-comercializados Managed PKI para clientes fijos. □ (marcar cuadro e inicial)
Servicios Managed PKI Inalámbricos co-comercializados para clientes inalámbricos □ (marcar cuadro e inicial)
Managed PKI para SSL □ (marcar cuadro e inicial)
Servicios Managed PKI para SSL Premium □ (marcar cuadro e inicial)

2. Nombramientos.
En la medida que el Cliente desea emitir Certificados de Cliente para clientes fijos y/o inalámbricos, E-Sign, en este acto, nombra al Cliente como Autoridad de Certificación ("CA") que no tiene relación con E-Sign, dentro del subdominio de E-Sign en la red VTN, y el Cliente acepta tal nombramiento. En la medida que el Cliente desea obtener Certificados de Servidor, E-Sign, en este acto, nombra al Cliente como Autoridad de registro ("RA"), dentro del subdominio de E-Sign en la red VTN conforme a la normativa CPS, y el Cliente acepta tal nombramiento.

2.1 Autoridad de Certificación. La presente Sección 2.1 se aplica en la medida que el Cliente sea una CA dentro del subdominio de E-Sign en la red VTN. Salvo por las funciones subcontratadas a E-Sign conforme a la Sección 4 del presente Anexo, el Cliente cumplirá con todos los requisitos y todas las obligaciones que se imponen a una CA dentro del subdominio de E-Sign en la red VTN, conforme a la normativa CPS, según se modifique ocasionalmente, incluyendo, entre otros, las obligaciones que se indican en la Sección 3 del presente Anexo. Al actuar como una CA, los requisitos y obligaciones del Cliente incluirán aquellos que se imponen a una RA dentro del subdominio de E-Sign en la red VTN.

2.2 Autoridad de Registro. La presente Sección 2.2 se aplica en la medida que el Cliente sea una RA dentro del subdominio de E-Sign en la red VTN. El Cliente cumplirá con todos los requisitos y obligaciones que se imponen a una RA dentro del subdominio de E-Sign en la red VTN, conforme a la normativa CPS, según se modifique ocasionalmente, incluyendo, entre otros, las obligaciones que se indican en la Sección 4 del presente Anexo.

3. Normativa CPS y el Manual del Administrador Managed PKI.
La normativa CPS y el Manual del Administrador Managed PKI, según se modifiquen periódicamente, son incorporados en el presente documento a modo de referencia. E-Sign notificará al Administrador de Autoridad de Registro ("RAA") del Cliente sobre cualquier modificación, publicando la información en el Centro de Control Managed PKI.

4. Obligaciones del Cliente como CA y/o RA.
Sin importar si el Cliente es una CA o una RA, se le exigirá cumplir las funciones de una RA, es decir, validar y aprobar las Solicitudes de Certificado y solicitar la revocación o renovación de Certificados de acuerdo con la normativa CPS y el Manual del Administrador Managed PKI.

4.1 Administrador de Autoridad de Registro. El Contacto del Cliente nombrará uno o más empleados del Cliente autorizados como RAA. El Cliente nombrará las personas que se indicarán como RAA en el formulario de inscripción pertinente. Tales RAA tendrán derecho a nombrar RAA adicionales en nombre del Cliente.

4.2 Requisitos de la Autoridad de Registro. El Cliente cumplirá con los requisitos que se establecen en la normativa CPS y el Manual del Administrador Managed PKI, según se modifiquen ocasionalmente, incluyendo, entre otros, los requisitos para validar la información que aparece en las Solicitudes de Certificado, aprobar o rechazar dichas Solicitudes de Certificado, utilizar el hardware y software designados por E-Sign y revocar los Certificados. El Cliente aprobará una Solicitud de Certificado únicamente si el Solicitante del Certificado es un Particular Afiliado o Entidad Afiliada en lo que se refiere al Cliente. Si un Suscriptor que ha recibido un Certificado del Cliente deja de ser Particular Afiliado o Entidad Afiliada de éste, el Cliente solicitará oportunamente la revocación de dicho Certificado del Suscriptor. Si un RAA ya no tiene la autoridad para actuar como tal en nombre del Cliente, éste solicitará oportunamente la revocación de su Certificado RAA. El Cliente accederá al sitio Web de E-Sign al menos una vez al mes, ya sea para solicitar la revocación de Certificados o para confirmar a E-Sign que no se han presentado solicitudes de revocación en dicho mes.

4.3 Requisitos de Autoridad de Registro Adicionales para Certificados de Servidor. En la medida que el Cliente actúe como una RA aprobando las Solicitudes de Certificado para los Certificados de Servidor: (a) aprobará una Solicitud de Certificado únicamente si ha autorizado al Solicitante de Certificado a utilizar el nombre de organización del Cliente en dicho Certificado, y utilizar un nombre de dominio que termine en el nombre de dominio que se indica en el formulario de inscripción del Cliente. En el caso de que el Cliente cambie su registro de nombre de organización y/o de dominio, el Cliente solicitará oportunamente la revocación de todos los Certificados de Servicio conforme al presente documento, y obtendrá la autenticación de E-Sign del nuevo registro de nombre de organización y/o nombre de dominio del Cliente. La imposibilidad del Cliente para obtener tal autenticación puede ser motivo de término del presente Acuerdo conforme a la Sección 8.2. Además de las disposiciones establecida en la Sección 9.4 del presente Acuerdo, el Anexo "B", el Acuerdo y los Anexos de éste sustituirán todos los acuerdos "click-on" u "online" posteriores; estos son exigidos al Cliente mediante acuerdo "click-through to accept" con el fin de obtener los Productos y Servicios que tienen relación con los Certificados de servidor descritos en el presente Anexo.

4.4 Modo de Cumplimiento. El Cliente llevará a cabo las tareas de las Secciones 3.2 y 3.3 anteriores de modo competente, profesional y diligente.

4.5 Suscriptores del Cliente. El Cliente hará que los Suscriptores que reciben Certificados conforme el presente documento cumpla con los términos del Acuerdo de Suscripción pertinente, al cual accedieron como condición para inscribirse con el fin de obtener los Certificados.
4.6 Mantenimiento de la Vigencia. Además de las disposiciones de finalización establecidas en la Sección 8.6 del presente Acuerdo, los requisitos de revocación según la Sección 3.2 del presente Anexo "B", la normativa CPS y el Manual del Administrador Managed PKI, y los requisitos de seguridad según el Manual del Administrador Managed PKI, se mantendrán vigentes una vez finalizado el presente Acuerdo hasta terminar el Período Operativo de todos los Certificados emitidos conforme al presente Acuerdo.

4.7 Garantía Limitada del Cliente. Durante el período de vigencia del presente Acuerdo, y siempre que el Cliente continúe emitiendo Certificados, éste último garantiza a E-Sign que: (i) toda la información fundamental para la emisión de un Certificado y validada por el Cliente es verdadera y correcta en todos sus aspectos esenciales y (ii) sin limitar la generalidad de lo anterior, la aprobación del Cliente de las Solicitudes de Certificado no resultará en una Emisión Errónea, incluyendo, entre otros, la Emisión Errónea que resulta de la Suplantación de Identidad.

4.8 Garantías del Cliente. Además de las garantías limitadas expresas que se establecen en la Sección 6.1 del presente Acuerdo, el Cliente garantiza a E-Sign que ha cumplido substancialmente con la normativa CPS y el Manual del Administrador Managed PKI.

5. Obligaciones de E-Sign.
E-Sign le proporcionará al Cliente los Servicios indicados en el Anexo "B" por un período de doce (12) meses a partir de la Fecha de Vigencia del presente Acuerdo (el "Período de Servicio Managed PKI"). E-Sign emitirá, administrará, revocará y/o renovará los Certificados de acuerdo con las instrucciones provistas por el Cliente y sus RAA.

5.1 Certificado RAA. Una vez aprobada la Solicitud de Certificado de las RAA, E-Sign emitirá un Certificado de RAA para cada una de las RAA. Tales Certificados RAA tendrán una validez de doce (12) meses junto con el Período de Servicio Managed PKI. Cualquier Certificado RAA adicional emitido durante el transcurso del año expirará conjuntamente dentro del Período de Servicio Managed PKI inicial.

5.2 Emisión de Certificado. Después de la aprobación de una Solicitud de Certificado por el Cliente, E-Sign: (i) tendrá derecho a confiar en la exactitud de la información de cada una de las Solicitudes de Certificado aprobadas y (ii) emitirá un Certificado para el Solicitante de Certificado que presenta dicha Solicitud de Certificado.

5.3 Ciclo Vital de Certificado. Los Certificados emitidos conforme al presente Acuerdo tienen un período máximo de validez de doce (12) meses a partir de la fecha en que se emite cada Certificado.

5.4 Generación de Claves CA. La presente Sección 4,5 se aplica en la medida que el Cliente se una CA dentro del subdominio de E-Sign en la red VTN. Durante un evento único de Generación de Claves CA, E-Sign generará pares de claves CA para que el Cliente utilice en la firma de Certificados emitidos por E-Sign en nombre del Cliente que se usan en el subdominio de E-Sign en la red VTN. La Clave Privada del Cliente de cada uno de los pares de claves se almacenará en una o más Unidades de Firma de Certificados. Podrán generarse pares de claves extras para CA adicionales en una fecha posterior, si el Cliente solicita una tasa adicional.

6. Indemnización.
Sujeta a la Sección 7 del presente Acuerdo titulada "Limitación de Responsabilidad", cada una de las partes (la "Parte Indemnizante") indemnizará a la otra parte y VeriSign y sus directivos, funcionarios, agentes, empleados, contratistas, compañías matrices, filiales o subsidiarias de la otra parte y VeriSign (conjuntamente, las "Partes Indemnizadas"), y mantendrá a las Partes Indemnizadas a salvo y en contra de cualquier pérdida, costo, daño y comisión (incluyendo las

comisiones de abogados) en que incurran las Partes Indemnizadas en relación con: (a) el incumplimiento de cualquier garantía u obligación conforme al presente Acuerdo, la normativa CPS o el Manual del Administrador Managed PKI por la Parte Indemnizante; (b) las acciones u omisiones de la Parte Indemnizante, la utilización de cualquier Producto o Servicio proporcionado por la Parte Indemnizante, o cualquier otro artículo provisto por ésta a los Suscriptores (conjuntamente, las "Condiciones Indemnizadas"). El Cliente, como Parte Indemnizante, indemnizará a las Partes Indemnizadas de E-Sign y las mantendrá a salvo y en contra de cualquier pérdida, costo, daño y comisión (incluyendo las comisiones de abogados) en que incurran las Partes Indemnizada de E-Sign en relación con el incumplimiento del Acuerdo de Suscripción por parte del Suscriptor que recibe un Certificado conforme al presente documento. Mediante una notificación apropiada, la Parte Indemnizante defenderá, a su costa, cualquier demanda presentada en contra de una o más de las Partes Indemnizadas basada en o que surja de una o más de las Condiciones de Indemnización.

Anexo "C":
Servicio de Gestión de Claves Managed PKI

Antecedentes
El Cliente desea utilizar el Servicio de Gestión de Claves Managed PKI para generar pares de claves en nombre de los Suscriptores, respaldar las Claves Privadas de los Suscriptores en forma cifrada, administrar dichas Claves Privadas y utilizar el Servicio de Recuperación de Claves de E-Sign para recuperar tales Claves Privadas de acuerdo con la Guía del Administrador de Servicios de Gestión de Claves y el presente Anexo. E-Sign está dispuesto a permitir al Cliente utilizar el Servicio de Gestión de Claves Managed PKI conforme a los términos y condiciones que se mencionan a continuación y en la Guía del Administrador de Servicios de Gestión de Claves.

TÉRMINOS Y CONDICIONES

1. Guía del Administrador de Servicios de Gestión de Claves.
La Guía del Administrador de Servicios de Gestión de Claves publicado en http://www.e-sign.cl, según se modifique periódicamente, se incorpora en el presente documento a modo de referencia. E-Sign notificará al Administrador nombrado por el Cliente sobre cualquier modificación, publicando la información en el Centro de Control Managed PKI.

2. Obligaciones de Recuperación de Claves del Cliente.

2.1 Administrador de Claves. El Contacto del Cliente nombrará uno o más empleados del Cliente autorizados como sus Administradores de Claves ("KMA"). Tales KMA tendrán derecho a nombrar KMA adicionales en nombre del Cliente. Si algún KMA no recibe la autorización adicional para actuar como Administrador según el Anexo "A" o como RAA según el Anexo "B" del presente Acuerdo, el Cliente configurará el Centro de Control Managed PKI para evitar que dicho KMA lleve a cabo las funciones de Administrador o RAA.

2.2 Requisitos de Autoridad de Registro de Gestión de Claves. El Cliente cumplirá con los requisitos que se establecen en la Guía del Administrador de Servicios de Gestión de Claves, según se modifique periódicamente, incluyendo, entre otros, los requisitos para generar Pares de Claves en nombre de los Solicitantes de Certificado, transmitir Claves Públicas a E-Sign para su inclusión en los Certificados que se emitirán a tales Solicitantes de Certificado, transmitir información de recuperación de claves a E-Sign, validar las solicitudes de los Suscriptores que recuperan sus Claves Privadas para asegurar que pertenezcan en realidad a tales Suscriptores, aprobar o rechazar tales solicitudes, utilizar el hardware y el software designado por E-Sign, utilizar el Servicio de gestión de Claves Managed PKI para solicitar la información necesaria para recuperar las Claves Privadas y (cuando corresponda) transmitir las Claves Privada recuperadas a los Suscriptores que las solicitan. El Cliente utilizará sistemas confiables para generar pares de claves, enviar la información de recuperación de Claves Públicas y Claves Privadas a E-Sign, almacenar las Claves Privadas y transmitir las Claves Privadas a los Suscriptores. Si un KMA ya no tiene la autoridad para actuar como tal en nombre del Cliente, éste cambiará oportunamente la contraseña utilizada por el KMA para obtener acceso al software de Servicio de Gestión de Claves Managed PKI, y solicitará a E-Sign revocar cualquier Certificado RAA operativo o el Certificado de Administrador de tal KMA.

2.3 Modo de Cumplimiento. El Cliente llevará a cabo las tareas de la Sección 2.2 anterior de modo competente, profesional y diligente. El Cliente utilizará los Productos y Servicios de E-Sign proporcionados según el presente Anexo, única y exclusivamente para fines legales y de acuerdo con la Guía del Administrador de Servicios de Gestión de Claves y, en el caso de que el Anexo "B" sea parte del presente Acuerdo, la normativa CPS.

2.4 Cumplimiento de la Ley de Exportación. No obstante cualquier revelación hecha por el Cliente a E-Sign con respecto a la ubicación de los Suscriptores que reciben Claves Privadas generadas por el Cliente conforme a este Anexo y, sin perjuicio de ninguna de las partes contenidas en el presente

Acuerdo al contrario, el Cliente no generará, ya sea directa o indirectamente, ni enviará Claves Privadas a Personas fuera de Chile y/o proporcionará Certificados a tales Personas que contengan Claves Públicas que correspondan a tales Claves Privadas, sin obtener antes cualquiera y todas las licencias necesarias del gobierno o agencias chilenos, o cualquier otro país para el cual dicho gobierno o cualquiera de sus agencias, requiere de una licencia de exportación u otra aprobación gubernamental en el momento en que tales Claves Privadas son enviadas a dichas Personas, o en el momento en que se entregan los Certificados a tales Personas.

2.5 Garantías del Cliente. Además de las garantías limitadas expresas que se establecen en la Sección 6.1 del presente Acuerdo, el Cliente garantiza a E-Sign que: (i) cada una de las solicitudes de información que el Cliente entrega a E-Sign para recuperar las Claves Privadas de un Suscriptor, después de haber recibido una solicitud por lo mismo de alguien que pretende ser dicho Suscriptor, ha sido entregada de hecho al Cliente, y autorizada por tal Suscriptor, (ii) las solicitudes de información generadas por el Cliente para recuperar la Clave Privada de un Suscriptor sin el permiso de éste son autorizadas por el primero para sus fines comerciales legítimos y legales, (iii) sin limitar la generalidad de lo anterior, una solicitud de información que el Cliente entrega a E-Sign para recuperar la Clave Privada de un Suscriptor no resultará en una Recuperación de Clave Errónea, incluyendo, entre otros, la Recuperación de Clave Errónea que resulta de la Suplantación de Identidad de la Recuperación de Clave y (iv) el Cliente ha cumplido substancialmente con la Guía del Administrador de Servicios de Gestión de Claves.

3. Obligaciones de E-Sign. E-Sign le proporcionará al Cliente el uso del Servicio de Gestión de Claves Managed PKI, según se establece en el presente documento, para que lo utilice conjuntamente con los Servicios Managed PKI según se establece en los Anexos “A” y “B”, respectivamente.

3.1 Certificado RAA. Después de la aprobación de las Solicitudes de Certificado de los KMA, si las hay, E-Sign emitirá un Certificado RAA o Certificado de Administrador para cada KMA según corresponda para obtener acceso a los Servicios proporcionados conforme al presente Anexo.

3.2 Inclusión de las Claves Públicas en los Certificados. Después de que el Cliente genera un Par de Claves en nombre de un Solicitante de Certificado (una vez aprobada la Solicitud de Certificado) y transmite la Clave Pública a E-Sign, este último incluirá dicha Clave Pública en un Certificado y emitirá el Certificado conforme al Anexo “A” o “B” del presente Acuerdo.

3.3 Servicio de Gestión de Claves de E-Sign. E-Sign autenticará las solicitudes recibidas del KMA del Cliente para la Clave Privada de un Suscriptor que fue generada y aprobada por el Cliente de acuerdo con la Guía del Administrador de Servicios de Gestión de Claves. Si E-Sign autentifica la solicitud, le entregará al Cliente la información de Recuperación de Claves necesaria para recuperar la Clave Privada de tal Suscriptor.

4. Responsabilidad del Cliente en Relación con la Generación o Validación de Solicitudes para Claves Privadas. EL CLIENTE SERÁ EL ÚNICO RESPONSABLE ANTE CUALQUIERA Y TODAS LAS PERSONAS POR LA GENERACIÓN O AUTENTICACIÓN DE TODAS LAS SOLICITUDES DE CLAVES PRIVADA QUE PRESENTE A E-SIGN Y POR LA CONDUCCIÓN DE LOS KMA. E-SIGN Y SUS VENDEDORES RENUNCIAN A TODA RESPONSABILIDAD.

5. Indemnización. Sujeta a la Sección 7 del presente Acuerdo titulada “Limitación de Responsabilidad”, cada una de las partes (la “Parte Indemnizante”) indemnizará a la otra parte y VeriSign y sus directivos, funcionarios, agentes, empleados, contratistas, compañías matrices, filiales o subsidiarias de la otra parte y VeriSign (conjuntamente, las “Partes Indemnizadas”), y mantendrá a las Partes Indemnizadas a salvo y en contra de cualquier pérdida, costo, daño y comisión (incluyendo las comisiones de abogados) en que incurran las Partes Indemnizadas en relación con: (a) el incumplimiento de cualquier garantía u obligación conforme al presente Acuerdo o la Guía del Administrador de Servicios de Gestión de Claves por la Parte Indemnizante; (b) las

acciones u omisiones de la Parte Indemnizante, la utilización de cualquier Producto o Servicio proporcionado por la Parte Indemnizante, o cualquier otro artículo provisto por ésta a los Suscriptores (conjuntamente, las “Condiciones Indemnizadas”). Mediante una notificación apropiada, la Parte Indemnizante defenderá, a su costa, cualquier demanda presentada en contra de una o más de las Partes Indemnizadas basada en o que surja de una o más de las Condiciones de Indemnización.

Anexo "D":
Acuerdo de Nivel de Servicios

1. Visión General.
El presente Acuerdo de Nivel de Servicios ("SLA") detalla los términos para el servicio de producción proporcionado por E-Sign a sus Clientes para la operación del Servicio del Cliente, incluyendo los Servicios de Certificado Managed PKI Private Label, los Servicios de Certificado Co-Comercializado Managed PKI y el Servicio de Gestión de Claves Managed PKI conforme a los Anexos "A", "B" y "C" del presente Acuerdo. Aborda específicamente: (i) la definición de niveles de servicio, las mediciones y la norma mínima de servicios vigente para el Servicio y (ii) la definición de soporte del cliente, la disponibilidad y los marcos de tiempo de respuesta.

2. Definiciones.
"Administrador de Compañía" se refiere a un empleado del Cliente que sea fiable, designado por éste como su administrador con respecto al Servicio en cuestión, de acuerdo con el Anexo pertinente para tal Servicio.
"Tiempo de Respuesta" se refiere a la cantidad de tiempo que transcurre entre el informe que entrega el Cliente a E-Sign sobre un problema de servicio y la respuesta de éste reconociendo el informe e indicando que se ha iniciado una respuesta al problema.
"Tiempo de Inactividad Programado" se refiere a los períodos programados en que el sistema y Servicio de E-Sign no está disponible para llevar a cabo el mantenimiento de servicio, las actualizaciones y las pruebas de capacidades failover rutinarias.
"Nivel de Gravedad" se refiere a la clasificación de nivel de gravedad que identifica un problema de servicio como "Gravedad 1", "Gravedad 2" o "Gravedad 3" basándose en los criterios especificados en la Sección 4(a) del presente Anexo D.
"Tiempo de Actividad" se refiere al porcentaje de tiempo en que los sistemas de E-Sign están disponibles y son capaces de recibir y procesar los datos de la Compañía en relación con los Servicios. Salvo según pueda indicarse de manera explícita en uno de los Anexos con respecto al Servicio descrito en este documento, "Tiempo de Actividad" se refiere únicamente a la disponibilidad de los sistemas de E-Sign, y no incluye la disponibilidad o funcionamiento del sistema de ningún Socio de Servicio o un tercero.

3. Disponibilidad de Servicio.
(a) Medición de Tiempo de Actividad. El Tiempo de Actividad se calcula en un período de noventa (90) días sucesivos como un porcentaje igual a (i) el número total de minutos en cualquier período de noventa (90) días en que los sistemas de E-Sign estén disponibles y sean capaces de recibir y procesar los datos de lo clientes en relación con los Servicios, dividido por (ii) el número total de minutos en tal período.
(b) Porcentaje de Tiempo de Actividad. El porcentaje de Tiempo de Actividad mensual de E-Sign durante todo el Período de Vigencia no será inferior al noventa y nueve por ciento (99%).
(c) Tiempo de Inactividad Programado. E-Sign notificará al Cliente vía correo electrónico de los tiempos de inactividad programados y el impacto previsto sobre la funcionalidad específica del Servicio con una anticipación no inferior a los treinta (30) días antes de la ventana de tiempo de inactividad planificada. El Tiempo de Inactividad Programado no excederá las cuatro (4) horas en una semana común y corriente, y se iniciará y finalizará dentro de la ventana programada que se especifica en la notificación entregada por E-Sign no menos del noventa y ocho por ciento (98%) del tiempo durante el período de doce (12) meses sucesivos.

4. Soporte del Cliente.
(a) Niveles de Gravedad. Los tiempos de Respuesta y Recuperación asociados con el suministro de soporte del cliente que entrega E-Sign en relación con los Servicios, se basarán en parte en la clasificación de los problemas informados por el nivel de gravedad de la siguiente manera:

(i) Gravedad 1. Los problemas de Gravedad 1 incluyen cualquier evento que tenga un impacto mayor sobre las operaciones del sistema y sobre el uso que hacen los usuarios del Servicio, como por ejemplo:

- Falta de disponibilidad del sistema o la aplicación que impide el procesamiento de las transacciones críticas.
- Interrupciones de la aplicación en línea que tienen un impacto significativo sobre la disponibilidad en línea del Servicio.
- Interrupciones en las telecomunicaciones que llevan a una interrupción mayor del Servicio.
- Degradación consistente de la disponibilidad que afecta significativamente la utilidad del Servicio.

(ii) Gravedad 2. Los problemas de Gravedad 2 incluyen cualquier evento (que no sean problemas de Gravedad 1) que tenga un impacto moderado sobre las operaciones del sistema y sobre el uso que hacen los usuarios del Servicio, como por ejemplo:

- Errores que deshabilitan sólo ciertas funciones no esenciales del Servicio y que pueden resultar en operaciones degradadas, incluyendo, entre otros, errores que producen demoras importantes en el procesamiento de las transacciones.
- Degradación intermitente de la disponibilidad que afecta moderadamente la utilidad del Servicio.

(iii) Gravedad 3. Los problemas de Gravedad 3 incluyen cualquier evento (que no sean problemas de Gravedad 1 o 2) que tenga un impacto menor sobre las operaciones del sistema y sobre el uso que hacen los usuarios del Servicio.

(b) Tiempos de Respuesta y Recuperación. E-Sign le proporcionará a los Administradores de la Compañía soporte telefónico de primer nivel las 24 horas del día, los 7 días de la semana, las 52 semanas del año para los problema de Gravedad 1, y de 9:00 AM a 6:00 PM, de lunes a viernes, las 52 semana del año para los problemas de Gravedad 2 y 3, salvo [los festivos nacionales de Chile y los períodos de Inactividad Programada]. Durante tales horas, las llamadas de soporte entrantes de primer nivel serán respondida de inmediato por un sistema de llamada automático. E-Sign tendrá disponible una opción de sistema de llamada que permite hablar directamente con un representante de soporte al cliente entrenado. El 80% de las veces que se elige esta opción, los clientes hablan con un representante de soporte al cliente entrenado en el plazo de 120 segundos a partir del momento de seleccionar dicha opción. Todas las llamadas de soporte de primer nivel serán registradas y tales registros se mantendrán al menos durante un año. Los Tiempos de Respuesta y Recuperación de E-Sign, divididos en Tipo de Sistema y Nivel de Gravedad, aparecen en la Tabla A siguiente. Sin perjuicio de la Tabla A, los Tiempos de Respuesta y Recuperación y los procedimientos indicados en este documento pueden estar sujetos a ampliaciones y/o modificaciones comercialmente razonables, cuando la llama de problema tiene que ver con un Servicio que involucra a un Socio de Servicio de E-Sign.

TABLA A: Respuesta de Problemas de Soporte al Cliente (durante las horas indicadas en la Sección 4(b) anterior)

Definición de Problema	Respuesta dentro de
Gravedad 1	4 horas
Gravedad 2	8 horas
Gravedad 3	siguiente día hábil

(c) Escalamiento. Los problemas de Gravedad 1 y 2 serán escalados internamente en la siguiente maneta para asegurar la resolución efectiva:

(i) Gravedad 1.

- Hora 0 a Hora 4: El Director de los Servicios de Producción y Servicio al Cliente, la gerencia de producción y el personal de ingeniería de E-Sign son notificados del problema, y la gerencia de producción y el personal de ingeniería trabajan activamente en su solución.
- Hora 5: Los Vicepresidentes de Operaciones e Ingeniería de E-Sign son notificados y, junto con el Director de los Servicios de Producción y Servicio al Cliente, se abocan a solucionar el problema.
- Hora 8: El equipo de gerencia ejecutiva de E-Sign, incluyendo CEO, son notificados y se abocan a solucionar el problema.

(ii) Gravedad 2.

- Hora Cero a Hora 72: E-Sign trabajará para resolver el problema e intentará entregar una solución en un plazo de 72 horas a partir de la identificación del problema. En el caso de que E-Sign no desarrolle un plan, dentro de los primeros 4 días hábiles a partir del momento en que se informó el problema, para solucionar el inconveniente dentro del siguiente período de 10 días, y el problema no se debe a una falla de la Compañía, E-Sign escalará el problema de acuerdo con los procedimientos de escalamiento de Gravedad 1 descritos anteriormente.

(d) Ambiente Preproducción. La Compañía tendrá acceso al ambiente preproducción de E-Sign por un período de 60 días a partir de la Fecha de Vigencia. Ninguna otra disposición de este SLA será aplicable a la disponibilidad o rendimiento del ambiente de preproducción.

(e) Servicio de Reemplazo Expedito de Hardware. Las piezas de reemplazo de hardware serán enviadas a la Compañía en el plazo de 72 horas vía entrega de dos días.

Anexo "E":
Tasas

Costo Total de los Productos y Servicios Ordenados en la Fecha de Vigencia:

SERVICIO MANAGED PKI - LICENCIA DE APLICACIÓN ÚNICA

	#Puestos	Año 1	
Recurrente Anual			
Tasa de Configuración (una vez)		$	No válido
Tasa Anual de Aplicación Única Managed PKI (_____)		$	$
Autenticación Subcontratada	## (Autenticaciones		
Certificación Notarial Digital	# (Notarizaciones		
Servicio de Roaming Managed PKI			
TASAS TOTALES			

Managed PKI Incluye:

- Custom Key Ceremony; 1 CA incluida
- (1) copia del Software Managed PKI (incluye Hosting Local, módulos de Administración Automatizada)
- Aplicación Go Secure! (Seleccionar (1) de las siguientes)
  - ____ Go Secure! para Microsoft Exchange
  - ____ Go Secure! para Aplicaciones Web
  - ____ Go Secure! para Notas Lotus
  - ____ Go Secure! para Checkpoint
  - ____ Go Secure! para SAP

- (1) serie de hardware de Administración Automatizada (Especificar: ___NT o ____ Solaris)
- Hasta (___) días de la Instalación de los módulos de software en el sitio del Cliente en el hardware con soporte de E-Sign seleccionado.
- Soporte Gold y Plan de Mantenimiento de E-Sign
- El Plan de Mantenimiento incluye actualizaciones de software, cambios, parches, correcciones de errores y mejoras desarrolladas por E-Sign o sus vendedores y disponible generalmente para los Clientes de E-Sign.

Términos y Condiciones:

- El cliente puede adquirir un determinado volumen de CA adicionales (para utilizar con Managed PKI completo), pero no puede activarlas bajo Managed PKI de aplicación única.
- Los días de instalación acumulados deberán utilizarse en el plazo de noventa (90) días a partir de la Fecha de Vigencia del presente Acuerdo. Deberá utilizarse un mínimo de cinco (5) días en una sola visita. Los desplazamientos y los gastos son adicionales.
- En el nivel de puesto 1k y 2k, se incluye la capacitación Managed PKI y la instalación del software de Hosting Local Managed PKI. Se recomienda adquirir días de consulta adicionales para la instalación de módulos adicionales.

- En los niveles de puesto más altos, se incluye la instalación y configuración del software de Administración Automatizada Managed PKI. Se recomienda adquirir días de consulta adicionales para la instalación de módulos adicionales.
- los Puestos sin utilizar o, si corresponde (las Autorizaciones o Notarizaciones) no podrán trasladarse a los años siguientes.
- Los componentes de hardware se vuelven propiedad del Cliente, pero si éste termina su Servicio, cualquiera de los Certificados e E-Sign almacenado en el hardware será revocado.

La tasa anual (si corresponde) de los Servicios de Autenticación de E-Sign se basa en el número de autenticaciones intentadas, y no el número de usuarios aprobados o certificados emitidos.

SERVICIO MANAGED PKI - LICENCIA DE APLICACIÓN MÚLTIPLE

	#Puestos	Año 1	
Recurrente Anual			
Tasa de Configuración (una vez)		$	No válido
Tasa de Puesto Anual Managed PKI (_____ o _____)		$	$
Autenticación Subcontratada	## (Autenticaciones		
Certificación Notarial Digital	# (Notarizaciones		
Servicio de Roaming Managed PKI			
TASAS TOTALES			

Managed PKI Incluye:

- Custom Key Ceremony; (____) CA incluidas
- Software Managed PKI (incluye Hosting Local y módulos de Administración Automatizada)
- Aplicaciones Go Secure! (Seleccionar (2) de las siguientes)
  - ____ Go Secure! para Microsoft Exchange
  - ____ Go Secure! para Aplicaciones Web
  - ____ Go Secure! para Notas Lotus
  - ____ Go Secure! para Checkpoint
  - ____ Go Secure! para SAP
- (x) Kits de Hardware de Administración Automatizada (Especificar: ___NT o ____ Solaris)
- Hasta (___) días de la Instalación de los módulos de software en el sitio del Cliente en el hardware con soporte de E-Sign seleccionado.
- Soporte Gold y Plan de Mantenimiento de E-Sign
- El Plan de Mantenimiento incluye actualizaciones de software, cambios, parches, correcciones de errores y mejoras desarrolladas por E-Sign o sus vendedores y disponible generalmente para los Clientes de E-Sign.

Términos y Condiciones:

- Los días de instalación acumulados deberán utilizarse en el plazo de noventa (90) días a partir de la Fecha de Vigencia del presente Acuerdo. Deberá utilizarse un mínimo de cinco (5) días en una sola visita. Los desplazamientos y los gastos son adicionales.
- En el nivel de puesto 1k y 2k, se incluye la capacitación Managed PKI y la instalación del software de Hosting Local Managed PKI.
- En los niveles de puesto más altos, se incluye la instalación y configuración del software de Administración Automatizada Managed PKI.
- El número de Puestos licenciados corresponde al número total de usuarios a quienes puede emitirse Certificados. El Cliente no podrá tener más de un número licenciado de usuarios a la vez que posean Certificados válidos en cualquier momento. Los usuarios tienen múltiples Certificados por puesto si sus aplicaciones lo requieren.
- los Puestos sin utilizar o, si corresponde (las Autorizaciones o Notarizaciones) no podrán trasladarse los años siguientes.
- Los componentes de hardware se vuelven propiedad del Cliente, pero si éste termina su servicio, cualquiera de los Certificados e E-Sign almacenado en el hardware será revocado.

- La tasa anual (si corresponde) de los Servicios de Autenticación Subcontratada se basa en el número de autenticaciones intentadas, y no el número de usuarios aprobados o certificados emitidos.

Costo Total de los Productos y Servicios Ordenados en la Fecha de Vigencia:

SERVICIOS DE AUTENTICACIÓN LICENCIA DE APLICACIÓN ÚNICA

#Autenticaciones Año 1 Recurrente Anual

Tasa de Configuración (una vez)		$	No válido
Tasa Anual de Servicios de Autenticación (_____)		$	$
TASAS TOTALES			

Incluye:

- Custom Key Ceremony; 1 CA incluida
- (1) copia del Software Managed PKI (incluye Hosting Local)
- (1) Go Secure! para Aplicaciones Web
- Hasta (3) días de la Instalación de los módulos de software en el sitio del Cliente en el hardware con soporte de E-Sign seleccionado.
- Soporte Gold y Plan de Mantenimiento de E-Sign
- El Plan de Mantenimiento incluye actualizaciones de software, cambios, parches, correcciones de errores y mejoras desarrolladas por E-Sign o sus vendedores y disponible generalmente para los Clientes de E-Sign.

Términos y Condiciones:

- Los días de instalación acumulados deberán utilizarse en el plazo de treinta (30) días a partir de la Fecha de Vigencia del presente Acuerdo. Los desplazamientos y los gastos son adicionales. Deberá utilizarse un mínimo de tres (3) días en una sola visita. Los días adicionales de Servicios Profesionales podrán adquirirse en la tasa de E-Sign vigente en ese momento.
- Las autenticaciones no utilizadas no podrán trasladarse a los años siguientes.
- La tasa anual de Servicios de Autenticación se basa en el número de autenticaciones intentadas, y no el número de usuarios aprobados o certificados emitidos.

SERVICIO MANAGED PKI INALÁMBRICO

	#Puestos	Año 1	
Recurrente Anual			
Tasa de Configuración (una vez)		$	No válido
Tasa Anual de Servicio Managed PKI Inalámbrico (Público o Privado)		$	$
TASAS TOTALES			

Incluye:

- Custom Key Ceremony; 1 CA incluida
- (1) copia del Software utilizada en conjunto con el Servicio Managed PKI Inalámbrico (incluye Hosting Local (Solaris), Administración Automatizada y módulos de Portal WPKI)
- (1) serie de hardware de Administración Automatizada (Solaris)
- Hasta (___) días de la Instalación de los módulos de software en el sitio del Cliente en el hardware con soporte de E-Sign seleccionado.
- Soporte Gold y Plan de Mantenimiento de E-Sign
- El Plan de Mantenimiento incluye actualizaciones de software, cambios, parches, correcciones de errores y mejoras desarrolladas por VeriSign y disponibles generalmente para los Clientes de E-Sign.

Términos y Condiciones:

- Los días de instalación acumulados deberán utilizarse en el plazo de noventa (90) días a partir de la Fecha de Vigencia del presente Acuerdo. Deberá utilizarse un mínimo de cinco (5) días en una sola visita. Los desplazamientos y los gastos son adicionales.
- Los Puestos no utilizados no podrán trasladarse a los años siguientes.
- Los componentes de hardware se vuelven propiedad del Cliente, pero si éste termina su Servicio, cualquiera de los Certificados e E-Sign almacenado en el hardware será revocado.Anexo “F”:

Servicio de Roaming Managed PKI
(hosting dividido)

Antecedentes

El Cliente desea utilizar el Servicio de Roaming Managed PKI para permitir a sus usuarios finales descargar de modo seguro su Clave Privada y el Certificado desde cualquier terminal de clientes entregando así al usuario final las “capacidades de roaming”. E-Sign garantiza al Cliente el derecho a utilizar el Servicio de Roaming Managed PKI conforme a los términos y condiciones que se establecen en el presente Anexo, y de acuerdo con la Guía del Administrador de Servicios de Roaming de E-Sign.

TÉRMINOS Y CONDICIONES

1. Definiciones.

Datos Privados Cifrados se refiere a la información cifrada que tiene relación con la Clave Privada y Certificado de un Suscriptor.
Clave Simétrica se refiera a una clave que se utiliza para descifrar o cifrar los Datos Privados Cifrados de un Suscriptor.

Información de Clave Simétrica se refiere a la información que se utiliza para generar una Clave Simétrica.

2. Guía del Administrador de Servicios de Roaming.

La Guía del Administrador de Servicios de Roaming publicada en http://www.e-sign.cl/empresa/libreria/index.html#doc, según se modifique periódicamente, se incorpora en el presente documento a modo de referencia. E-Sign notificará al Cliente sobre cualquier modificación, publicando la información en el Centro de Control Managed PKI.

3. Obligaciones del Cliente.

3.1. Nombramientos. El Contacto del Cliente nombrará uno o más empleados del Cliente autorizados como Administradores del Centro de Servicios de Roaming ("RSCA"), o hará uso de sus Administradores o RAA existentes, cualquiera sea el caso, para acceder al Centro de Servicios de Roaming y llevar a cabo las funciones descritas anteriormente.

3.2. Funciones del Administrador de Roaming. El Cliente cumplirá con los requisitos que se establecen en el Anexo "A" o "B", según sea el caso, para validar la información en las Solicitudes de Certificado, aprobar o rechazar tales Solicitudes de Certificado, utilizar el hardware y el software designados por E-Sign e instruir a E-Sign en la emisión de Certificados para dichos Solicitantes de Certificado. El Cliente, por medio del Agente de Confianza Personal ("PTA"), (i) asegurará que los Datos Privados Cifrados de un Suscriptor necesarios para recuperar la Clave Privada de éste se almacenan en los servidores de roaming y almacenamiento designados por el Cliente y (ii) almacenará la información que se utiliza para generar la Clave Simétrica de un Suscriptor en los servidores de roaming del Cliente, de acuerdo con la Guía del Administrador de Servicios de Roaming de E-Sign.

3.3. Suscriptores de Roaming. El Cliente será el único responsable de asegurar que sólo los Suscriptores validados y aprobados por el Cliente recibirán acceso a los Servicios de Roaming provistos en el presente documento.

4. Obligaciones de E-Sign.

E-Sign le proporcionará al Cliente el uso del Servicio de Roaming Managed PKI según se establece en este documento, para utilizarlo conjuntamente con los Servicios que se establecen en los Anexos "A" y "B" según corresponda.

4.1. Emisión de Certificado. E-Sign emitirá los Certificados conforme al Anexo "B" o "C", según corresponda, a aquellos Solicitantes de Certificado aprobados por el Cliente.

4.2. Datos de Clave Simétrica. E-Sign, por medio del PTA, almacenará la información que se utiliza para generar la Clave Simétrica de un Suscriptor (la "Información de Clave Simétrica") necesaria para cifrar o descifrar los Datos de Clave Simétrica de un Suscriptor. La Información de Clave Simétrica del Suscriptor se almacenará en los servidores de roaming diseñados por E-Sign y será borrada automáticamente por el PTA una vez que se utilice para generar una Clave Simétrica.

4.3. Servicio de Roaming. El software del PTA lo utilizará el Cliente para (i) obtener los Datos Privados Cifrados de un Suscriptor desde el servidor de almacenamiento designado por el Cliente, (ii) obtener la información desde los servidores de roaming del Cliente y E-Sign para generar la Clave Simétrica de un Suscriptor y (iii) utilizar la Clave Simétrica para descifrar los Datos Privados Cifrados de un Suscriptor, permitiendo así que éste descargue su Clave Privada y Certificado.

5. Responsabilidad del Cliente en Relación con los Datos Privados Cifrados de un Suscriptor.

EL CLIENTE SERÁ EL ÚNICO RESPONSABLE ANTE CUALQUIERA Y TODAS LAS PERSONAS POR LA SEGURIDAD DE LOS DATOS PRIVADOS CIFRADOS DE SUS SUSCRIPTORES. E-SIGN Y SUS VENDEDORES RENUNCIAN A TODA RESPONSABILIDAD.

6. Indemnización.

Sujeta a la Sección 7 del presente Acuerdo titulada "Limitación de Responsabilidad", cada una de las partes (la "Parte Indemnizante") indemnizará a la otra parte y VeriSign y sus directivos, funcionarios, agentes, empleados, contratistas, compañías matrices, filiales o subsidiarias de la otra parte y VeriSign (conjuntamente, las "Partes Indemnizadas"), y mantendrá a las Partes Indemnizadas a salvo y en contra de cualquier pérdida, costo, daño y comisión (incluyendo las comisiones de abogados) en que incurran las Partes Indemnizadas en relación con: (a) el incumplimiento de cualquier garantía u obligación conforme al presente Acuerdo, la normativa CPS o la Guía del Administrador de Servicios de Roaming por la Parte Indemnizante; (b) las acciones u omisiones de la Parte Indemnizante, la utilización de cualquier Producto o Servicio proporcionado por la Parte Indemnizante, o cualquier otro artículo provisto por ésta a los Suscriptores (conjuntamente, las "Condiciones Indemnizadas"). Mediante una notificación apropiada, la Parte Indemnizante defenderá, a su costa, cualquier demanda presentada en contra de una o más de las Partes Indemnizadas basada en o que surja de una o más de las Condiciones de Indemnización.

Anexo "F":
Servicio de Roaming Managed PKI
(hosting empresarial)

Antecedentes

El Cliente desea utilizar el Servicio de Roaming Managed PKI para permitir a sus usuarios finales descargar de modo seguro su Clave Privada y el Certificado desde cualquier terminal de clientes entregando así al usuario final las "capacidades de roaming". E-Sign garantiza al Cliente el derecho a utilizar el Servicio de Roaming Managed PKI conforme a los términos y condiciones que se establecen en el presente Anexo, y de acuerdo con la Guía del Administrador de Servicios de Roaming de E-Sign.

TÉRMINOS Y CONDICIONES

Definiciones.

Datos Privados Cifrados se refiere a la información cifrada que tiene relación con la Clave Privada y Certificado de un Suscriptor.
Clave Simétrica se refiera a una clave que se utiliza para descifrar o cifrar los Datos Privados Cifrados de un Suscriptor.
Información de Clave Simétrica se refiere a la información que se utiliza para generar una Clave Simétrica.

2. Guía del Administrador de Servicios de Roaming.

La Guía del Administrador de Servicios de Roaming publicada en http://www.e-sign.cl/empresa/libreria/index.html#doc, según se modifique periódicamente, se incorpora en el presente documento a modo de referencia. E-Sign notificará al Cliente sobre cualquier modificación, publicando la información en el Centro de Control Managed PKI.

Obligaciones del Cliente.

3.1 Nombramientos. El Contacto del Cliente nombrará uno o más empleados del Cliente autorizados como Administradores del Centro de Servicios de Roaming ("RSCA"), o hará uso de sus Administradores o RAA existentes, cualquiera sea el caso, para acceder al Centro de Servicios de Roaming y llevar a cabo las funciones descritas anteriormente.

3.2 Funciones del Administrador de Roaming. El Cliente cumplirá con los requisitos que se establecen en el Anexo "B" o "C", según sea el caso, para validar la información en las Solicitudes de Certificado, aprobar o rechazar tales Solicitudes de Certificado, utilizar el hardware y el software designados por E-Sign o sus vendedores, e instruir a E-Sign en la emisión de Certificados para dichos Solicitantes de Certificado. El Cliente, por medio del Agente de Confianza Personal ("PTA"), (i) asegurará que los Datos Privados Cifrados de un Suscriptor necesarios para recuperar la Clave Privada de éste se almacenan en los servidores de roaming y almacenamiento designados por el Cliente y (ii) almacenará la información que se utiliza para generar la Clave Simétrica de un Suscriptor en los servidores de roaming del Cliente, de acuerdo con la Guía del Administrador de Servicios de Roaming de E-Sign.

3.3 Suscriptores de Roaming. El Cliente será el único responsable de asegurar que sólo los Suscriptores validados y aprobados por el Cliente recibirán acceso a los Servicios de Roaming provistos en el presente documento.

4. Obligaciones de E-Sign.

E-Sign le proporcionará al Cliente el uso del Servicio de Roaming Managed PKI, según se establece en el presente documento, para que lo utilice conjuntamente con los Servicios Managed PKI de acuerdo con los Anexos "B" y "C", según corresponda.

4.1 Emisión de Certificado. E-Sign emitirá los Certificados conforme al Anexo "B" o "C", según corresponda, a aquellos Solicitantes de Certificado aprobados por el Cliente.

4.2 Servicio de Roaming. El software del PTA lo utilizará el Cliente para (i) obtener los Datos Privados Cifrados de un Suscriptor desde el servidor de almacenamiento designado por el Cliente, (ii) obtener la información desde los servidores de roaming y almacenamiento del Cliente para generar la Clave Simétrica de un Suscriptor y (iii) utilizar la Clave Simétrica para descifrar los Datos Privados Cifrados de un Suscriptor, permitiendo así que éste descargue su Clave Privada y Certificado.

5. Responsabilidad del Cliente en Relación con los Datos Privados Cifrados de un Suscriptor.

EL CLIENTE SERÁ EL ÚNICO RESPONSABLE ANTE CUALQUIERA Y TODAS LAS PERSONAS POR LA SEGURIDAD DE LOS DATOS PRIVADOS CIFRADOS DE SUS SUSCRIPTORES. E-SIGN Y SUS VENDEDORES RENUNCIAN A TODA RESPONSABILIDAD.

6. Indemnización.

Sujeta a la Sección 7 del presente Acuerdo titulada "Limitación de Responsabilidad", cada una de las partes (la "Parte Indemnizante") indemnizará a la otra parte y VeriSign y sus directivos, funcionarios, agentes, empleados, contratistas, compañías matrices, filiales o subsidiarias de la otra parte y VeriSign (conjuntamente, las "Partes Indemnizadas"), y mantendrá a las Partes Indemnizadas a salvo y en contra de cualquier pérdida, costo, daño y comisión (incluyendo las comisiones de abogados) en que incurran las Partes Indemnizadas en relación con: (a) el incumplimiento de cualquier garantía u obligación conforme al presente Acuerdo, la normativa CPS o la Guía del Administrador de Servicios de Roaming por la Parte Indemnizante; (b) las acciones u omisiones de la Parte Indemnizante, la utilización de cualquier Producto o Servicio proporcionado por la Parte Indemnizante, o cualquier otro artículo provisto por ésta a los Suscriptores (conjuntamente, las "Condiciones Indemnizadas"). Mediante una notificación apropiada, la Parte Indemnizante defenderá, a su costa, cualquier demanda presentada en contra de una o más de las Partes Indemnizadas basada en o que surja de una o más de las Condiciones de Indemnización.

Anexo "G":
Servicios de Certificación Notarial Digital

Antecedentes

El Cliente desea suscribirse al servicio de Certificación Notarial Digital que ofrece E-Sign, y que le permite hacer una impresión de tiempo de los documentos, todo de acuerdo con los términos y condiciones que se establecen a continuación.

TÉRMINOS Y CONDICIONES

1. DEFINICIONES.

1.1 Recibo Digital se refiere a una ficha que incluye (i) el hash del documento sometido que se entrega para la Certificación Notarial Digital y (ii) el momento en que el documento sometido o el hash de éste fue recibido por E-Sign para la Certificación Notarial Digital, los cuales son firmados por E-Sign.

1.2 Registro Digital se refiere a un registro que contiene la siguiente información: (a) Recibo Digital y (b) demás información solicitada a E-Sign e ingresada por el usuario final en el momento de la Certificación Notarial Digital, como por ejemplo el nombre y la descripción del documento Digitalmente Certificado por Notario.

1.3 Certificación Notarial Digital y Digitalmente Certificado por Notario se refiere al proceso por medio del cual E-Sign (a) interpreta el momento en que recibe un documento o el hash de un documento presentado por un usuario final, (b) crea un hash de documento si la información presentada es un documento (en oposición al hash de un documento), (c) crea una ficha que incluye el momento de recibo y el hash, (d) añade una firma digital de E-Sign a la ficha para crear un Recibo Digital, (e) entrega el Recibo Digital al usuario final que lo solicita y (f) almacena el Registro Digital.

2. SERVICIO DE CERTIFICACIÓN NOTARIAL DIGITAL.

2.1 Acceso al Servicio de Certificación Notarial Digital. El Cliente puede acceder al servicio de Certificación Notarial Digital utilizando cualquiera de los siguientes métodos: (a) acceso vía las aplicaciones personalizadas del Cliente que pueden integrar y utilizar el kit de desarrollo de software de Certificación Notarial Digital para llevar a cabo la Certificación Notarial Digital (sujeto al pago que haga el Cliente de las tasas por dicho kit de desarrollo, si las hay, y las tasas para el servicio de Certificación Notarial Digital); (b) acceso vía la interfaz de sitio Web de E-Sign (sujeto al pago de las tasas aplicables por el servicio de Certificación Notarial Digital).

2.2 Verificación. E-Sign puede generar y enviar junto con el Recibo Digital un texto HTML que explique los contenidos de un Recibo Digital al usuario final del Cliente. El Cliente reconoce que dicho texto HTML tiene el único propósito de servir de referencia al Cliente y no es necesariamente seguro. Para verificar que un documento Digitalmente Certificado por Notario no ha sido alterado desde el momento en que se generó el Recibo Digital, y para obtener la hora de recepción del documento o hash del documento por E-Sign, el destinatario del acuerdo de confianza deberá (a) verificar la firma digital en el Recibo Digital, leer el hash

contenido en éste y comparar el hash en dicho Recibo Digital con el hash del documento que se está comprobando para verificar que los dos sean iguales o (b) acceder a la base de datos de Registros Digitales de E-Sign vía la interfaz de sitio Web de E-Sign.

2.3 Almacenamiento. El Cliente retendrá todos sus Recibos Digitales y documentos Digitalmente Certificados por Notario. E-Sign almacena un Registro Digital por un período de al menos un (1) año a partir de la creación de éste. El almacenamiento por un período adicional está sujeto a la oferta que haga E-Sign de tales servicios adicionales y el pago que haga el Cliente de las tasas pertinentes. E-Sign no almacena una copia de los documentos Digitalmente Certificados por Notario.

2.4 Disponibilidad del Registro Digital. El Cliente reconoce que E-Sign puede entregar Registros Digitales del Cliente a terceros si así lo exige la ley, una citación legal, una garantía o una solicitud, requerimiento u orden judicial o gubernamental.

3. SUSCRIPTORES DEL CLIENTE.

El Cliente hará que los Suscriptores que reciben Certificados cumplan con los términos del presente Acuerdo.

4. DESCARDO DE RESPONSABILIDAD.

EL CLIENTE RECONOCE QUE EL SERVICIO DE CERTIFICACIÓN NOTARIAL DIGITAL PROPORCIONA IMPRESIÓN DE TIEMPO DE UN DOCUMENTO Y NO ES UNA “CERTIFICACIÓN NOTARIAL”, UN “ACTO NOTARIAL” O CUALQUIER OTRO ACTO DE UNA “NOTARIA” O “NOTARIO PÚBLICO” SEGÚN PUEDAN DEFINIRSE DICHOS TÉRMINOS CONFORME A LA LEY VIGENTE.

Anexo "H":
Identrus Express

Antecedentes
El Cliente desea: (i) emitir, administrar, suspender, revocar y/o renovar Certificados digitales para Identrus LLC PKI Solutions que son compatibles con Identrus, en una Jerarquía Privada que se enlazará directamente con la CA Identrus root y marcada con el nombre comercial del Cliente, que se basa en las Solicitudes de Certificado entregadas, validadas y aprobadas por éste y (ii) subcontratar con E-Sign las funciones de emisión, administración, suspensión, revocación y/o renovación de tales Certificados; y al mismo tiempo no desea (iii) retener para sí las funciones de validación y aprobación de las Solicitudes de Certificado, y solicitar la revocación o renovación de éstos.

TÉRMINOS Y CONDICIONES

Obligaciones del Cliente.

1.1 Nombramientos. El Contacto del Cliente nombrará uno o más empleados del Cliente autorizados como sus administradores (los "Administradores").

1.2 Funciones del Administrador. El Cliente, por medio de su Administrador, validará la información que aparece en las Solicitudes de Certificado, aprobará, suspenderá o rechazará tales Solicitudes de Certificado, utilizará el hardware y el software designados por E-Sign e instruirá a E-Sign con respecto a la emisión, suspensión, renovación y revocación de los Certificados, de acuerdo con el Manual del Administrador Managed PKI y de conformidad con las especificaciones de Identrus LLC. El Cliente transmitirá a E-Sign cualquier solicitud que pudiera tener para la revocación de Certificados emitidos por él. Si un Administrador ya no tiene la autoridad para actuar como tal en nombre del Cliente, el Contacto del Cliente solicitará oportunamente la revocación de su Certificado de Administrador.
1. Obligaciones de E-Sign.
E-Sign le proporcionará al Cliente:
Los Servicios indicados en el Anexo "A" por un período de doce (12) meses a partir de la Fecha de Vigencia del presente Acuerdo (el "Período de Servicio Managed PKI"). E-Sign emitirá, administrará, revocará y/o renovará los Certificados de acuerdo con las instrucciones provistas por el Cliente y sus Administradores, y en conformidad con los requisitos de auditoria y seguridad de Identrus LLC.

2.1 Certificado del Administrador. Una vez aprobada la Solicitud de Certificado del Administrador, E-Sign emitirá un Certificado de Administrador para cada uno de los Administradores. Tales Certificados tendrán una validez de doce meses junto con el Período de Servicio Managed PKI.

2.2 Emisión de Certificado. Después de la aprobación de una Solicitud de Certificado por el Cliente, E-Sign: (i) tendrá derecho a confiar en la exactitud de la información de cada una de las Solicitudes de Certificado aprobadas y (ii) emitirá un Certificado para el Solicitante de Certificado que presenta dicha Solicitud de Certificado.

2.3 Ciclo Vital de Certificado. Los Certificados emitidos o licenciados conforme al presente Acuerdo tendrán un período de validez según lo determinen las especificaciones de Identrus LLC.

2.4 Generación de Claves. Durante un evento único de Generación de Claves, E-Sign generará pares de claves CA para que el Cliente utilice en todos los Certificados emitidos por E-Sign que se usan en la Jerarquía Privada del Cliente conforme a la CA Identrus root. La Clave Privada del Cliente de cada uno de los pares de claves se almacenará en una o más Unidades de Firma de Certificados. Podrán generarse pares de claves extras para CA adicionales en una fecha posterior, si el Cliente solicita una tasa adicional.

2.5 Compatible con Identrus. Además de las garantías limitadas expresas contenidas en cada uno de los Anexos pertinentes conforme al presente Acuerdo, E-Sign garantiza al Cliente que ha cumplido substancialmente con la mayor parte de los Reglamentos de Identrus LLC presentados a E-Sign. Los servicios son totalmente compatibles con Identrus al utilizarlos para las soluciones Identrus PKI.

3. Renuncia de Responsabilidad.

SALVO POR LAS GARANTÍAS LIMITADAS EXPRESAS CONTENIDAS EN LA SECCIÓN 6 Y EN EL PRESENTE ANEXO, E-SIGN NO OTORGA NINGUNA OTRA GARANTÍA DE NINGÚN MODO, Y RENUNCIA, EN ESTE ACTO, A TODA RESPONSABILIDAD POR LA EMISIÓN ERRÓNEA O VALIDACIÓN IMPROPIA DE CUALQUIER SOLICITUD DE FIRMA DE CA RECIBIDA DE IDENTRUS EN NOMBRE DEL CLIENTE. ADEMÁS, EL CLIENTE RECONOCE QUE ES MIEMBRO DE BUENA REPUTACIÓN DE IDENTRUS LLC, Y DICHA CONDICIÓN DE BUENA REPUTACIÓN ES UN REQUISITO DE LA ORGANIZACIÓN FINANCIERA IDENTRUS LLC, LA CUAL EL CLIENTE TIENE LA RESPONSABILIDAD DE MANTENER Y QUE NO TENDRÁ CONEXIÓN CON LOS SERVICIOS QUE LE PROPORCIONA E-SIGN.

Anexo "I":
SERVICIOS DE AUTENTICACIÓN DE DISPOSITIVOS

Antecedentes
El Cliente desea obtener Certificados digitales en una Jerarquía Privada marcada con su nombre comercial que se basan en solicitudes de firma de Certificados por lotes validadas y aprobadas por él, y entregadas a E-Sign por medio del Agente de Fabricación de Dispositivos de VeriSign ("DMA").

TÉRMINOS Y CONDICIONES

1. OBLIGACIONES DEL CLIENTE.

1.1 Nombramientos. El Contacto del Cliente nombrará uno o más empleados del Cliente autorizados como sus administradores (los "Administradores DA").

1.2 Funciones de los Administradores DA. El Cliente, por medio de sus Administradores DA, validará la información enviada a través e la solicitud de firma de Certificados, y utilizará el hardware y el software designados por E-Sign para instruir a éste en la emisión de dichos Certificados. Si un Administrador DA ya no tiene la autoridad para actuar como tal en nombre del Cliente, el Contacto del Cliente solicitará oportunamente la revocación de su Certificado de Administrador DA.

1.3 Garantía Limitada del Cliente. Durante el período de vigencia del presente Acuerdo, y siempre que el Cliente continúe solicitando [E-Sign] la emisión Certificados, éste último garantiza a E-Sign que: (i) toda la información esencial para la emisión de un Certificado y validada por el Cliente es verdadera y correcta en todos sus aspectos fundamentales.

2. OBLIGACIONES DE E-SIGN.
E-Sign le proporcionará al Cliente los Servicios de Autenticación de Dispositivos indicados en el Anexo "A" por tres períodos consecutivos de doce (12) meses a partir de la Fecha de Vigencia del presente Acuerdo (el "Período de Servicio de Autenticación de Dispositivos"). E-Sign emitirá los Certificados de acuerdo con las instrucciones proporcionadas por el Cliente y sus Administradores DA.

2.1 Certificado del Administrador DA. Una vez aprobada la Solicitud de Certificado del Administrador DA, VeriSign emitirá un Certificado de Administrador DA para cada uno de los Administradores DA. Tales Certificados tendrán una validez de doce (12) meses junto con el Período de Servicio de Autenticación de Dispositivos.

2.2 Emisión de Certificado. Una vez que el Cliente aprueba la solicitud de firma de Certificado por lotes, E-Sign: (i) tendrá derecho a confiar en la exactitud de la información contenida en cada una de las solicitudes de firma de Certificados aprobadas, (ii) emitirá los Certificados al Administrador DA que presente dichas solicitudes de firma de Certificados por lotes y, (iii) junto con dichos Certificados, le entregará al Cliente los pares de claves privadas y públicas asociados con tales Certificados de Autenticación de Dispositivos. E-Sign no retendrá ninguna copia de dicho pares de claves, ni llevará a cabo ninguna revocación o renovación de tales Certificados de Autenticación de Dispositivos.

2.3 Generación de Claves CA. Durante un evento único de Generación de Claves CA, E-Sign generará pares de claves CA para que el Cliente utilice en todos los Certificados emitidos por E-Sign que se usan en la Jerarquía Privada. La Clave Privada CA del Cliente de cada uno de los pares de claves se almacenará en una o más Unidades de Firma de Certificados. Podrán generarse pares de claves extras para CA adicionales en una fecha posterior, si el Cliente solicita una tasa adicional.

3. RENUNCIA DE RESPONSABILIDAD. E-SIGN, EN ESTE ACTO, RENUNCIA A TODA RESPONSABILIDAD QUE RESULTE DE CUALQUIER RECLAMACIÓN DE UN TERCERO SOBRE EMISIÓN ERRÓNEA O SUPLANTACIÓN DE PERSONALIDAD, QUE SE ORIGINE EN LOS CERTIFICADOS DE AUTENTICACIÓN DE DISPOSITIVOS, UNA VEZ QUE TALES CERTIFICADOS HAN SIDO EMITIDOS Y TRANSFERIDOS AL CLIENTE.