RESPUESTAS A OBSERVACIONES FORMULADAS A NUEVA NORMA TÉCNICA PARA LA PRESTACIÓN DEL SERVICIO DE CERTIFICACIÓN DE FORMA ELECTRÓNICA AVANZADA

PROPUESTA ORIGINAL	OBSERVACIONES FORMULADAS	COMENTARIOS MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO
Artículo 1°.- La presente norma establece las condiciones bajo las cuales el Certificador o Prestador de Servicios de Certificación de Firma Electrónica Acreditado reconocerá al sistema denominado "Claveúnica", como medio de comprobación fehaciente de la identidad de solicitante de un certificado de firma electrónica avanzada, en los términos exigidos por el artículo 12 letra e) de la Ley 19.799, dado que el titular para su obtención ha comparecido personal y directamente ante el Registro Civil. Para los efectos de esta norma técnica la clave única es la identidad digital que el Estado le entrega a las personas que han comparecido personal y directamente al Registro Civil y han seguido el procedimiento de dicho servicio para demostrar su identidad. Esta identidad digital se compone del binomio RUN – Contraseña.	1. Cómo se identificará las claves únicas entregas por medios diferentes al registro civil (oficina Chileatiende). 2. Artículo 1.- La presente norma establece las condiciones bajo las cuales el Certificador o Prestador de Servicios de Certificación de Firma Electrónica Acreditado reconocerá al sistema denominado "Claveúnica", como medio de comprobación fehaciente de la identidad de solicitante de un certificado de firma electrónica avanzada, en los términos exigidos por el artículo 12 letra e) de la Ley 19.799, dado que el titular para su obtención ha comparecido personal y directamente ante **un oficial d**el Registro Civil. Para los efectos de esta norma técnica la clave única es **una contraseña única** que el Estado le entrega a las personas que han comparecido personal y directamente al Registro Civil y han seguido el procedimiento de dicho servicio para demostrar su identidad. Esta **contraseña** se compone del binomio RUN – Contraseña.	Se modifica el artículo 1°, estableciendo que se reconocerá el sistema denominado "ClaveÚnica", como medio de comprobación fehaciente de la identidad del solicitante de un certificado de firma electrónica avanzada, en los términos exigidos por el artículo 12 letra e) de la Ley N°19.799. Por lo tanto, las personas que hayan obtenido su clave de activación de la claveúnica habiendo comparecido ante un oficial del Servicio de Registro Civil e Identificación podrán utilizar dicho medio como comprobación de su identidad, según lo exige el artículo 12 letra e) de la ley N° 19.799.

Artículo 2°. - Para que el Certificador pueda utilizar el sistema denominado "Claveúnica" será obligación adherir a las condiciones y términos establecidos en dicha plataforma.	1. ¿Cuáles son esos términos y condiciones? No se han encontrado en el sitio claveunica.gob.cl 2. Al ser las condiciones de uso tan importantes sería interesante identificarlas en lo específico. Debería agregarse algo relativo a las actualizaciones o modificaciones a las condiciones, además podría establecerse su periodicidad. 3. No se entrega detalle técnico ni los términos de uso que los Certificadores deben cumplir para poder utilizar el sistema "Claveúnica". ¿Dónde pueden obtener los Certificadores la información requerida para incorporar el sistema "Claveúnica" a sus procesos y con quien aclarar eventuales dudas técnicas, por ejemplo, existe ambiente de testing? Podría ser un poco más claro para las empresas certificadoras el cómo ver el alcance de este punto. En la página de Clave única no queda claro cómo revisar estos términos	Los Términos y Condiciones de Uso de ClaveÚnica se encuentran publicados en el siguiente link: https://claveunica.gob.cl/activar
Artículo 3º.- El Certificador de firma electrónica avanzada una vez integrado al sistema denominado "Claveúnica" deberá, además, implementar un mecanismo complementario digital de comprobación de identidad del solicitante para la emisión de un certificado de firma electrónica avanzada.	1. Se sugiere establecer usando NIST 800-63b la fiabilidad para estos factores complementarios.	Se estima pertinente establecer la sugerencia el estándar NIST 800-63, por cuanto es una herramienta útil a efectos de mantener la integridad Digital, por lo que este estándar será considerado para las próximas actualizaciones técnicas.

El o los mecanismos complementarios que decida implementar el Certificador deberán declararse en las Políticas y Prácticas de Certificación, conforme a lo dispuesto en el artículo 6° del Decreto Supremo N°181, de 2002, del Ministerio de Economía, Fomento y Turismo; con expresa mención de la fiabilidad que estos mecanismos tienen.	2. Las empresas Certificadoras (y sus relacionadas) ofrecen múltiples servicios o productos. ¿El sistema "Claveúnica" podrá utilizarse únicamente, por parte de los Certificadores, para las solicitudes de certificado digital o podrá ser utilizado para otro propósito?. De no limitarse el uso del sistema "Claveúnica" por parte de los Certificadores, podría afectarse el rendimiento de los sistemas computacionales de los Organismos Públicos que usen dicha componente.	Como se establece en el artículo 1°, se limitará el uso de la clave única para los prestadores de servicios de certificación para emitir certificados de firma electrónica avanzada.
	¿Serán opcionales los mecanismos complementarios? Para los casos de personas extranjeras, no se indica si será presencial o no el mecanismo de comprobación de identidad.	Como se indica en el artículo 3°, será obligatorio para el certificador la implementación de mecanismos complementarios digitales de comprobación de identidad del solicitante. Respecto de personas extranjeras podrán hacer uso de la Claveúnica como método de comprobación de su identidad, en la medida que hayan obtenido su claveúnica dando cumplimiento a lo dispuesto en el artículo 12 letra e) de la ley N° 19.799, según se explica en la respuesta dada a las observaciones al artículo 1°.
Artículo 4°. – Una vez que el Certificador se haya adherido a los términos y condiciones del sistema denominado "Clave Única" y haya implementado el mecanismo complementario establecido en el artículo precedente, podrá comenzar a emitir certificados de firma electrónica avanzada a los solicitantes que sean titulares de una Claveúnica.	1. Una vez que el Certificador se haya adherido a los términos y condiciones del sistema denominado "Clave Única" y haya implementado el mecanismo complementario establecido en el artículo precedente, podrá comenzar a emitir certificados de firma electrónica avanzada a los solicitantes que sean titulares de una Claveúnica. **La emisión de dichos certificados deberá cumplir con lo establecido en el artículo 2 letra g) de la Ley N° 19.799, en orden a garantizar que la firma electrónica avanzada sea creada usando medios que**	La propuesta de incorporación de ese inciso segundo ya es materia establecida en la ley N° 19.799 y en su Reglamento.

	el titular mantiene bajo su exclusivo control. Por lo tanto, la Clave Única del titular no bastará para que se identifique al momento de suscribir documentos con su firma electrónica avanzada, debiendo el Certificados utilizar algunos de los medios técnicos que permite la disposición primera transitoria de reglamento de la ley N° 19.799, Decreto Supremo de Economía N° 181 de 2002.	
	3. No se especifica el registro (evidencias) que el Certificador debe mantener en caso de que la solicitud se haya realizado al Certificador, a través del sistema "Claveúnica" (Ej. Rut del solicitante, fecha, hora, dirección IP u otra identificación del dispositivo utilizado para realizar la solicitud, Tipo de transacción: solicitud, renovación o revocación de certificado). Esto puede ser de utilidad en caso de que una persona reclame haber sido suplantada usando certificado digital.	El art. 17 del Decreto N° 181 de 2002, del Ministerio de Economía, Fomento y Turismo, establece lo siguiente: La acreditación es voluntaria, sin perjuicio de lo cual para obtenerla el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones: a. Demostrar la fiabilidad necesaria de sus servicios. b. Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos. Es por este motivo que no se hace necesario el tener que destacarlo o replantearlo.
	Sólo norma cuando se podría emitir certificados, no dice nada respecto al tiempo de validez del certificado extendido.	Dependerá del formato de contrato adquirido entre el Prestador de Servicios de Certificación (PSC) y el usuario contratante.
	En este punto no es una norma técnica sobre la FEA que se está presentando economía.	La presente norma ha sido elaborada dando cumplimiento a lo dispuesto en el art. 5 del Decreto Supremo N°181, de 2002, del Ministerio de Economía, Fomento y Turismo, que establece el procedimiento de fijación de normas técnicas.
	¿Esto aplica a los que actualmente están acreditados por el SII como empresas certificadoras?	La norma técnica se aplicará a todas las PSC

	¿Qué entidad realiza estas validaciones? (que la empresa se ha adherido a los términos y condiciones, junto con implementar un mecanismo complementario válido).	La Entidad Acreditadora velará por el cumplimiento de esta norma técnica, sin perjuicio que Segpres lo realiza respecto del uso de Clave Única.
Artículo 5º. Los certificados de firma electrónica avanzada que se emitan a través de la forma regulada en esta norma técnica podrán ser almacenados en dispositivos, individuales o masivos, que cumplan con el estándar FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001). Los datos de creación de firma, almacenados en dispositivos masivos, deberán encontrarse protegidos mediante un segundo factor de seguridad que permita al titular controlar que el acceso y utilización de éstos únicamente puede ser realizado por él. Estos factores de seguridad deberán encontrarse declarados de manera clara en las Políticas y Prácticas de Certificación, con expresa mención de la fiabilidad que éstos tienen.	1. ¿El FIPS 140-2 puede ser cualquier nivel? Tener presente que el 2do factor de seguridad que debe proteger los datos de creación de firma, almacenados en dispositivos masivas, debe permitir que sólo el titular pueda acceder y utilizar esos datos. Este es un requisito esencial para estar en presencia de una firma electrónica avanzada. 2. Respecto del estándar FIPS, si bien está establecido en el reglamento de la ley de firma, creemos que por la naturaleza de este reglamento, se siguiere también puedan adscribir a las normas internacionalmente reconocidas, que contienen las exigencias que se buscan establecer de acuerdo a la interoperabilidad internacional: - EN 419241-1-:2016 Trustworth systems supporting server signing part 1: general system security requirements. - EN 419241-2:2017 Trustworth systems supporting server signing part 2: protection profile for QSCD for server signing.	El Decreto Supremo N°181, de 2002, del Ministerio de Economía, Fomento y Turismo, establece en sus disposiciones transitorias, literal b), el uso de: - FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001). En la Guía de Acreditación en el control "PS06 Plan de administración de Llaves", dentro de los estándares de Evaluación, se señala el uso: Estándares de evaluación - ETSI TS 102 042 - FIPS 140-2 L3 El cual en el aspecto de evaluación establece el uso, definiendo el nivel "3".
	3. Se sugiere que la forma regulada en este artículo, aplique también para el enrolamiento para firma avanzada, en particular para el almacenamiento masivo, no solo para los que utilicen Clave única que es este caso.	Se analizará la sugerencia para futuras actualizaciones técnicas.

	4. ¿Cuál es el primer factor de seguridad para los datos de creación de firma?	El primer factor de seguridad viene dado por Clave Única.
	¿Dónde se deben manejar las Políticas y Prácticas de Certificación por parte de las empresas Certificadoras?	Dentro de la Guía de Acreditación FEA se establece en el control PO01 Políticas de Certificados de Firma Electrónica Avanzada. Las políticas y prácticas de certificación se encuentran publicadas en los portales de cada PSC. A modo de ejemplo de muestra un caso: http://www.acepta.com/politicas-practicas/po01.pdf
	Se debe especificar qué nivel de validación FIPS 140-2 que se exigirá para el almacenamiento individual (FIPS posee 4 niveles de seguridad)	El Decreto Supremo N°181, de 2002, del Ministerio de Economía, Fomento y Turismo, establece en sus disposiciones transitorias, literal b) el uso de: - FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001). En la Guía de Acreditación en el control "PS06 Plan de administración de Llaves", dentro de los estándares de Evaluación, se señala el uso: Estándares de evaluación - ETSI TS 102 042 - FIPS 140-2 L3 El cual en el aspecto de evaluación establece el uso, definiendo el nivel "3".

Artículo transitorio: Los Certificadores o Prestadores de Servicios de Certificación deberán tomar todas las medidas para adecuarse a la presente norma técnica en un plazo máximo de 30 días, a contar de la fecha de su publicación en el diario oficial.	1. Se sugiere un plazo de al menos 90 días para realizar las adecuaciones a esta norma técnica. 2. Los certificadores o prestadores de servicios de certificación deberán tomar todas las medidas para adecuarse a la presente norma técnica en un plazo máximo de 90 días, a contar de la fecha de su publicación en el diario oficial.	Se acogen las sugerencias propuestas y se amplió el plazo a 90 días corridos contados desde la publicación de la norma en el diario oficial.
	3. ¿Supervisará la Entidad Acreditadora del Ministerio de Economía el correcto uso por parte de los Certificadores del sistema "Claveúnica" ?, se incluirá por ejemplo una revisión del uso de este sistema en las Inspecciones que habitualmente realiza?	La Entidad Acreditadora continuará realizando las tareas de aseguramiento y cumplimiento en los estándares expresados en las Guías de Acreditación y los avances tecnológicos correspondientes.
	¿Qué sanciones se aplicaría a los Certificadores en caso de incumplimiento?	El cumplimiento de las normas técnicas es parte de los elementos cuya observación se verificará por la Entidad Acreditadora a través de las fiscalizaciones que realizada en virtud de su facultad inspectora (art. 15 del Decreto N° 181, de 2002, del Ministerio de Economía, Fomento y Turismo)

Otras observaciones:

1. La firma electrónica avanzada emitida con clave única tendrá el mismo uso de la actual FEA o tendrá alguna restricción.

Respuesta: Tendrá el mismo uso.

2. ¿Cuál es la firma en que se realizará la integración? ¿es posible tener un documento?

Respuesta: El modelo de firma en cuestión es F.E.A. y la documentación de integración entregada se encuentra disponible y publicada en https://claveunica.gob.cl/institucional/manual-de-instalacion

3. ¿Cuáles serán los protocolos de seguridad para validar clave única?

Respuesta: Técnico En el sitio de clave Única https://claveunica.gob.cl/institucional/manual-de-instalacion se establecen los protocolos de seguridad y verificación.

4. Para el artículo 2 se requiere que la Clave única entregue a la PSC toda la información del solicitante del certificado, de esta forma pasará a formar parte del registro de la validación del certificado digital.

Respuesta: La clave Única deberá entregar el Prestador de Servicio (PSC) los datos de enrolamiento necesarios para que el PSC pueda realizar la acción de enrolamiento interno y de este modo se pueda cumplir con el convenio antes señalado.