BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

NORMA COMPLEMENTARIA

FIRMA DIGITAL

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

NC-FDI

BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

N O R M A C O M P L E M E N T A R I A

F I R M A D I G I T A L

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

NC-FDI

Tabla de contenido

Sistema Nacional de Pagos Electrónicos

1. Introducción

Esta normativa establece las reglas y disposiciones de carácter complementario al Reglamento del Sistema de Pagos, con respecto al servicio denominado Firma Digital (FDI), provisto por el Banco Central de Costa Rica (BCCR), por medio del Sistema Nacional de Pagos Electrónicos (SINPE).

2. Alcance

Esta normativa aplica para todas aquellas entidades que funjan como Oficinas de Registro y los Agentes de Registro que ésta asigne para gestionar la solicitud, emisión, entrega, renovación, revocación y cualquier otra función de acuerdo con las leyes, reglamentos, políticas y demás disposiciones aplicables al Sistema Nacional de Certificación Digital.

3. Términos empleados

Para los fines del presente documento, se entenderá por:

- Acuerdo de suscriptor: se refiere al “Acuerdo de Suscriptor para Suscriptores de Certificados de Firma Digital y de Autenticación de Persona Física Emitidos por la Autoridad Certificadora CA SINPE-Persona Física” en el cual, entre otros aspectos, se establecen los deberes y responsabilidades entre la CA del SINPE y el suscriptor.
- AD: Administrador de dispositivos
- BCCR: Banco Central de Costa Rica.
- CA del SINPE: CA SINPE – Persona Física: Autoridad certificadora emisora registrada en el Sistema Nacional de Certificación Digital, subordinada a la autoridad certificadora CA POLITICAS – PERSONA FISICA que a su vez está subordinada a la CA RAIZ NACIONAL – COSTA RICA, cuyo ámbito de acción es el Sistema Financiero Nacional.
- CA: Autoridad Certificadora autorizada o registrada ante la Dirección de Certificadores de Firma Digital (DCFD).
- Certificado Digital: Un certificado digital es un documento electrónico que contiene la identidad, la llave pública y la información personal del suscriptor. Es creado y firmado digitalmente por una persona jurídica prestadora del servicio de creación, emisión y operación de certificados digitales, conocida como Autoridad Certificadora.
- Datos de activación: Valores de datos (que no son las llaves), que son requeridos para operar los dispositivos criptográficos y que necesitan ser protegidos (ejemplos: PIN, frase clave, biométricos o llaves distribuidas manualmente).
- DCFD: se refiere a la “Dirección de Certificadores de Firma Digital”, es la dependencia del Ministerio de Ciencia y Tecnología (MICIT), encargada de la administración y supervisión del sistema de certificación digital.
- Dispositivo: módulo seguro que resguarda las claves y los certificados digitales de un suscriptor, utilizados para autenticarse y generar su firma digital. Para el caso de la CA del SINPE se trata de una Smart card, de acuerdo a las disposiciones transitorias.

- Documento de identidad: Es el documento formal que según el ordenamiento jurídico costarricense, sirve para identificar legalmente a un suscriptor. En el caso de las personas físicas costarricenses, es la cédula de identidad y en el caso de extranjeros residentes es el Documento de Identidad Migratorio para Extranjeros (DIMEX) y para los diplomáticos es el Documento de Identificación para Diplomáticos (DIDI).
- ECA: Ente Costarricense de Acreditación: La dependencia pública a que se refiere la "Ley del Sistema Nacional para la Calidad", número 8279 del 2 de mayo del 2002.
- FIPS 140-2: Estándar para los dispositivos criptográficos (FIPS por sus siglas en inglés Federal Información Processing Standard).
- Frase de desafío: Conjunto de datos suministrados por un suscriptor que combinados de cierta forma le permitirán validar su identidad en el sistema. Son utilizados para revocar un certificado cuando el suscriptor lo requiera.
- Inventario de dispositivos: Registro en el sistema del número de serie, marca y modelo de los dispositivos criptográficos en los cuales se generarán los certificados digitales que serán entregados a los suscriptores. Los dispositivos en inventario son responsabilidad de la OR.
- No repudio: En un ambiente físico, el "no repudio" es el concepto de asegurar que en una disputa, una de las partes no pueda refutar la validez de una declaración o de un contrato. En ambientes digitales, se refiere a un mecanismo que provee prueba de la autoría y la integridad de los datos y que garantiza con un alto nivel de certeza que el proceso de autenticación es genuino. Con base en la Ley 8454, bajo la figura del "no repudio", una determinada comunicación o mensaje electrónico adquiere fuerza vinculante o efectos jurídicos, ante el posible rechazo de su autor.
- OR: Oficina de Registro, entidad delegada por la CA del SINPE para la verificación de la identidad de los solicitantes de certificados digitales y otras funciones dentro del proceso de expedición y manejo de los certificados. Representa el punto de contacto entre el suscriptor y la CA del SINPE. Realiza todas sus funciones en cumplimiento de lo establecido en la política de certificación nacional y en concordancia con las políticas y procedimientos definidos por la CA DEL SINPE.
- OTP: Por sus siglas en inglés "One Time Password", es una clave que sirve para ser usada una sola vez. En el servicio de Firma Digital se usará para desbloquear el dispositivo que contiene los certificados cuando esta acción no pueda ser realizada mediante las huellas dactilares del suscriptor del certificado.
- PIN - Número de identificación personal: es el tipo de dato de activación seleccionado por la CA del SINPE para operar los módulos criptográficos. El PIN es definido por el suscriptor, de acuerdo con las reglas de complejidad establecidos por la CA-SINPE. El suscriptor puede actualizar el PIN de su tarjeta utilizando las herramientas que le provee el sistema operativo de su computador y tiene que ser protegido por el suscriptor con el fin de prevenir el uso no autorizado de las llaves privadas de los certificados de firma digital y autenticación de persona física, almacenadas en el dispositivo.
- Quiosco de activación de dispositivos: área dedicada exclusivamente para la activación de los certificados digitales del suscriptor donde se garantiza total privacidad para la definición del PIN como dato de activación y uso de los certificados digitales.
- SINPE: Sistema Nacional de Pagos Electrónicos.
- Smart card: Tarjeta inteligente, es una tarjeta similar en diseño y materiales a una tarjeta de crédito que contiene un chip de circuito integrado con microprocesador criptográfico seguro. Es el tipo de dispositivo criptográfico seleccionado por la CA del SINPE para el almacenamiento de certificados digitales de autenticación y de firma digital cuyas características se definen en el Estándar Físico – Firma Digital.

- Solicitante: Persona física que, facultada por las políticas establecidas por la CA del SINPE, presenta a la OR una solicitud de emisión de un certificado.
- Suscriptor: todo usuario final a quien se le ha emitido un certificado digital por parte de la CA del SINPE, válido dentro de la jerarquía nacional de certificadores registrados.

Para consultar algún otro término que aparezca en este documento, remítase a la "Norma complementaria - Glosario general".

4. Documentos aplicables y anexos

Siglas	Nombre del documento
Ley 8454	Ley de Certificados, Firmas Digitales y Documentos Electrónicos
Reglamento a la Ley 8454	Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos
	Política de Certificados para la Jerarquía Nacional de Certificados Registrados
	Directrices para las Autoridades de Registro. Características de Cumplimiento de Autoridades de Registro (RA) de la Jerarquía Nacional de Certificadores Registrados de Costa Rica, (Oficinas de Registro para efectos de esta normativa).
RSP	Reglamento del Sistema de Pagos.
EF-FDI	Estándar Físico – Firma Digital
EE-FDI	Estándar Electrónico-Firma Digital
EE -FDI	Estándar electrónico - Servicios Firma Digital en Internet
NC-AES	Norma complementaria Administración de Esquemas de Seguridad
NC-TCS	Norma complementaria – Tarifas y Cobros

5. Normas operativas

5.1. Definición del servicio

Es el servicio que permite al BCCR y a los asociados al SINPE gestionar la solicitud, emisión, entrega y la revocación de certificados digitales de conformidad con la Ley 8454, su reglamento, Políticas y demás directrices aplicables.

5.2. De los Agentes de Registro (AR)

La OR debe realizar el nombramiento de los Agentes de Registro (AR) en estricto cumpliendo de las disposiciones establecidas en el "Apartado 2 Controles del Personal" de las "Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (OR) de la jerarquía nacional de certificadores registrados".

Para la operación del servicio Firma Digital (FDI), los Agentes de Registro podrán desempeñar uno o varios de los siguientes roles:

- Emisor: Rol bajo el cual un AR realiza todas las actividades definidas para la emisión y entrega de certificados digitales a los suscriptores, las cuales contemplan el registro de solicitudes y la generación de certificados digitales, la generación de la clave de desbloqueo. Se debe tomar en cuenta que, por restricciones del sistema, una persona que ejerza este rol no puede ejecutar funciones del rol de Administrador de Dispositivos.
- Revocador: Rol bajo el cual un AR ejecuta en el servicio Firma Digital (FDI) las funciones de revocación de certificados digitales.

- Administrador de registros de pago del servicio: rol mediante el cual una entidad asociada al SINPE, que no opera como OR, realiza el registro de pago por la emisión y entrega de certificados para clientes determinados.
- Administrador de Dispositivos: rol responsable de registrar en el inventario los dispositivos criptográficos admitidos por la CA del SINPE para emitir sus certificados digitales.
- Además el AR puede desempeñar los roles de Consultante de Solicitudes de Certificados, Consultante de Dispositivos y Consultante de solicitudes de pago, mediante los cuales puede monitorear el estado de cada uno de estos tópicos.

Toda OR es responsable de mantener dentro del expediente de personal de los empleados designados como AR, evidencia documental de su compromiso de ejecutar las labores del servicio de firma digital de conformidad con las regulaciones aplicables de acuerdo con los roles que le hayan sido asignados en el servicio de firma digital, así como de las capacitaciones recibidas de acuerdo con los requerimientos en dichas regulaciones.

Para la operación del servicio de Firma Digital, la designación de los AR debe realizarse por medio del servicio Administración de Esquemas de Seguridad (AES) del SINPE de conformidad con lo estipulado en las normas complementarias correspondientes.

Como requisito indispensable para autorizar la operación de una OR, todos los AR independientemente del rol que ejecuten en el servicio Firma Digital deben estar certificados por el SINPE en dicho servicio.

5.3. Prestación y pago del servicio

El servicio de entrega de certificados puede ser pagado por alguna entidad asociada al SINPE que haya hecho el registro de pago para la emisión y entrega de certificados para el solicitante o bien directamente por el solicitante.

En caso de que el costo de la emisión de los certificados de un cliente vaya a ser cubierto por una entidad asociada al SINPE, la atención de este cliente por parte de la OR será voluntaria, no obstante, en caso de que lo atienda, deberá cobrar la tarifa interbancaria establecida en el Reglamento del Sistema de Pagos de conformidad con los procedimientos establecidos en la Norma complementaria – Tarifas y Cobros.

En caso de que el solicitante pague directamente por el servicio, se debe aplicar las políticas de cobro definidas para tal efecto por la entidad.

En cualquier caso, dentro del proceso de concertación de citas o antes de solicitarle al cliente que realice el pago correspondiente, la OR debe verificar previamente si existe un “Registro de pago por la emisión y entrega de certificados” realizado por otra entidad, a efecto de evitar duplicidades en el cobro al cliente por el servicio de emisión de certificados digitales.

Por otra parte, el proceso de emisión de certificados digitales se tiene por completado cuando el suscriptor posea en su haber el dispositivo activo con certificados activos y el Acuerdo de Suscriptor firmado digitalmente.

Cuando falte alguno de estos elementos, ya sea porque se presenten problemas técnicos que imposibiliten completar el proceso de emisión de certificados o porque el cliente decida no continuar con el proceso antes de firmar digitalmente el Acuerdo Suscriptor, el servicio se tendrá por no prestado y por ende no corresponderá realizar ningún cobro al suscriptor, o en su defecto, lo que procede es la devolución de lo pagado en caso de que ya lo hubiere realizado.

El sistema realizará automáticamente el cobro de las tarifas por transacción hasta que el suscriptor firma digitalmente el Acuerdo de Suscriptor, con lo cual, se demuestra que el dispositivo y los certificados están funcionando correctamente.

Una vez que el cliente ya haya firmado digitalmente el Acuerdo de Suscriptor no procede la devolución del dinero, ya que en este punto el servicio se da por completado.

5.4. De los módulos de operación del servicio

El servicio Firma Digital opera de conformidad con los siguientes módulos:

1. Inventario de Dispositivos.
2. Registro de pago por la emisión y entrega de certificados.
3. Registro de Solicitudes:
   - **a)** -Autenticar la identidad del solicitante del certificado.
   - **b)** -Verificar registros de pago del servicio.
   - **c)** -Validar datos del solicitante mediante consulta al TSE.
   - **d)** -Verificar impedimentos para emisión del certificado.
   - **e)** -Recolectar evidencia presencial.
   - **f)** -Recopilar información de contacto y revocación.
   - **g)** -Firmar digitalmente resumen de la información recopilada.
4. Generar certificados digitales.
5. Generar contraseña de desbloqueo (OTP).
6. Activación de dispositivos.
7. Revocación de certificados.

La CA del SINPE mantendrá el servicio disponible durante las 24 horas los 7 días de la semana, no obstante cada OR podrá brindar el servicio dentro del horario de operación de sus oficinas.

5.5. Esquema de operación

5.5.1. Inventario de Dispositivos

El registro del inventario de dispositivos es un requisito previo por medio del cual se llevan a cabo todas las labores de gestión de certificados digitales, el cual debe ser realizado por un Agente de Registro con rol de Administrador de Dispositivos (AD) del Centro de Operaciones del SINPE. Las OR podrán ejercer el rol de Consultante de Dispositivos, además del rol de emisor y cualquier otro relacionado, si así lo requiriera y solicita la OR al Responsable de Seguridad de cada entidad.

Los dispositivos se podrán agregar en el sistema en forma individual o en lotes.

Cuando los dispositivos se agreguen en forma individual, el AD deberá seleccionar en el sistema: la marca, el modelo y el tipo de dispositivo (Smart card) y el sistema obtendrá en forma automática el número de serie del dispositivo para lo cual, el AD debe introducir cada uno de los dispositivos en el lector correspondiente. Toda esta información se almacenará en el sistema junto con el nombre de la entidad que lo registró y la fecha del registro. El AD debe garantizar la integridad de la información asociada a cada dispositivo.

En caso que el registro de los dispositivos se realice en lotes, el AD deberá cargar en el sistema un archivo XML de conformidad con las especificaciones contenidas en el Estándar electrónico – Firma Digital. Todos los dispositivos que conformen el lote deben ser de la misma marca y modelo, motivo por el cual, si la OR posee dispositivos de diferentes marcas y/o modelos deberá cargar en el sistema un archivo por cada marca y modelo. El AD debe garantizar la integridad de la información del lote de dispositivos incluida en cada archivo que se cargue en el sistema.

Todo dispositivo que no haya sido registrado en el inventario no podrá ser utilizado para la emisión de certificados digitales, el sistema validará el cumplimiento de este requisito.

El AD debe garantizar que todo dispositivo criptográfico que forme parte de este inventario, cumpla con las características técnicas especificadas en el Estándar físico – Firma Digital que hayan sido sometidas al "Proceso de verificación y aceptación de dispositivos requeridos para funcionamiento del servicio de Firma Digital" detallado en la sección 5.1 de dicho estándar. Los modelos y marcas aceptados por la CA del SINPE serán accesibles a través del sistema. No deberá incluirse en el inventario, ningún dispositivo que no cumpla con estos requisitos. La OR es responsable por las implicaciones que se deriven del incumplimiento de esta disposición.

5.5.2. Registro de pago por la emisión y entrega de certificados

El servicio de Firma Digital provee funcionalidad para que, las entidades asociadas al SINPE que no funjan como OR, pero que requieran certificados digitales para sus clientes o empleados, puedan voluntariamente, suscribirse al servicio. Esta funcionalidad permite a la entidad registrar el nombre de las personas a las que requiere que se le emitan certificados digitales, por las cuales está dispuesta a pagar la tarifa interbancaria establecida en el Reglamento del Sistema de Pagos con este propósito.

Las entidades que así lo hagan deberán cargar en el sistema el registro de pago correspondiente. Para ello, deberán asignar al menos un AR para que desempeñe el rol de "Administrador de registros para el pago del servicio".

El registro de pago debe contener el número del Documento de Identidad y el costo a cubrir para cada cliente o empleado de la entidad, el cual, según el Reglamento del Sistema de Pagos, podrá cubrir:

- ⊡ Emisión del certificado.
- ⊡ Emisión del certificado y costo del Smart Card.
- ⊡ Emisión del certificado, costo del Smart Card y costo del lector correspondiente

El sistema controla que una misma entidad no realice un registro duplicado. No obstante, el sistema aceptará que dos entidades diferentes realicen un registro de pago para un mismo cliente. En este caso, cuando el cliente se presente ante una OR para que le emitan su certificado digital, el sistema seleccionará la mejor oferta para el cliente, esto es, la que cubra el mayor costo posible.

El AR en su rol de "Administrador de registros de pago del servicio" puede realizar los registros en forma individual o en lotes. En ambos casos, el AR debe garantizar la integridad de los datos incluidos.

Si el registro de pago se realiza en lotes, el "Administrador de registros para el pago del servicio" deberá incluir en el sistema un archivo XML de conformidad con las especificaciones contenidas en el Estándar Electrónico – Firma Digital.

Adicionalmente, los AR podrán desempeñar el rol de “Consultante de registros para el pago del servicio”, mediante el cual, podrán consultar los registros de pago incluidos por la misma entidad. Los registros de pago se presentan en tres estados: registrado, aplicado y eliminado.

Todo registro que se encuentre en estado aplicado significa que el certificado correspondiente ya fue emitido y se podrá identificar la fecha y el nombre de la OR que lo emitió. El cobro correspondiente se realizará conforme lo establecido en la Norma complementaria – Tarifas y Cobros.

Los registros cargados en el sistema se podrán eliminar únicamente si ninguna OR ha aplicado el pago.

5.5.3. Registro de solicitudes

Las funciones descritas en este apartado deben ser ejecutadas por AR en su rol de Emisor.

5.5.3.1. Autenticar la identidad del solicitante del certificado

La autenticación de la identidad del solicitante debe realizarse en forma presencial, cara a cara, entre el solicitante y el AR, para lo cual, el AR debe evaluar, que el documento de identidad presentado por el solicitante sea un documento legalmente aceptado, que esté vigente y que no presente ningún deterioro físico que invalide o imposibilite la identificación del solicitante. La aceptación de los documentos de identidad presentados deberá tratarse de conformidad con los parámetros establecidos en la entidad para los otros servicios que requieren la verificación de documentos de identidad.

Para el caso de ciudadanos costarricenses, el documento legalmente aceptado es la Cédula de Identidad y para el caso de los residentes es el Documento de Identidad Migratorio para Extranjeros (DIMEX) y para el caso de los diplomáticos es el Documento de Identidad para Diplomáticos (DIDI). No se permite el uso de ningún otro documento.

5.5.3.2. Verificar registros de pago del servicio

En caso de que una entidad asociada al SINPE haya registrado una solicitud para el pago del servicio en favor de sus clientes, el sistema le indicará al AR cuál entidad paga y qué tipo de pago aplica (Certificado, Certificado y dispositivo o Certificado, dispositivo y lector). En este caso debe verificar con el cliente que la OR no le haya cobrado previamente por la emisión de los certificados en caso contrario el AR debe gestionar el reintegro al cliente de la suma que le hayan cobrado.

En su caso, cuando el sistema indique que no existe ningún registro de pago para el cliente, el AR debe solicitarle a éste la cancelación del costo por la emisión de los certificados, o bien que le muestre el comprobante de pago correspondiente de conformidad con los procedimientos que la OR tenga establecidos al respecto.

5.5.3.3. Validar datos del solicitante

Para el caso de los solicitantes costarricenses, el sistema le suministrará la información oficial del TSE correspondiente al último documento de identidad emitido al solicitante.

En el caso de extranjeros residentes la validación se realizará con base en los datos del Documento de Identidad Migratorio para Extranjeros (DIMEX) obtenido, en línea, de la base de datos oficial de Migración y Extranjería. El AR es responsable validar que los datos sean idénticos a los consignados en el DIMEX aportado por el cliente.

Cuando se trate de Diplomáticos y hasta tanto el SINPE no posea conexión con las bases de datos del Ministerio de Relaciones Exteriores, el AR es responsable de ingresar en el sistema los datos contenidos en el Documento de Identificación para Diplomáticos presentado por el solicitante. El AR es responsable de que los datos ingresados sean idénticos a los consignados en el DIDI.

En todos los casos, el AR debe verificar que el documento de identidad sea el oficial, que pertenece al solicitante presente frente a él y en el caso específico de una cédula de identidad y el DIMEX que la información consignada en estos documentos es la misma desplegada por el sistema y concierne a la persona frente a él, es decir que el AR pueda dar una seguridad razonable de la correspondencia entre el documento de identidad, los datos suministrados por el TSE o en su caso Migración y Extranjería y el solicitante. Cualquier diferencia que ponga en duda la autenticidad del documento de identidad, debe ser razón suficiente para no procesar la solicitud de certificado.

En los casos en que la cédula de identidad no tenga consignada la fecha de nacimiento, éste no será motivo para no emitir el certificado digital, siempre y cuando el AR tenga la seguridad que la persona frente a él es mayor de edad.

El AR debe garantizar que la persona que solicita el certificado es quien dice ser y por ende la OR es responsable de la autenticidad de los datos suministrados por el solicitante. En consecuencia, la CA del SINPE emitirá el certificado con base en los datos incluidos en el sistema por el AR bajo la presunción de su veracidad.

5.5.3.4. Verificar impedimentos para la emisión del certificado

El sistema verificará contra las fuentes oficiales:

- ⊡ Para el caso de nacionales, que el solicitante sea mayor de edad y que no se encuentra registrado por el TSE como una persona difunta.
- ⊡ Para el caso de residentes, que el solicitante cuente con un DIMEX en estado "Activo" y que este contenga toda la información necesaria para emitir el certificado
- ⊡ En todos los casos, que el solicitante no tenga ningún impedimento legal dictado por una autoridad judicial competente o revocatoria que le impida legalmente realizar la solicitud de certificados digitales.
- ⊡ El solicitante no tiene un certificado activo.

No se emitirá ningún certificado a la persona que no cumpla con estos requisitos.

Cuando el sistema detecte que el solicitante tiene alguno de los impedimentos señalados en los incisos anteriores, el sistema no permitirá continuar con el proceso y el AR debe proceder a explicarle al solicitante la causa del impedimento y recomendarle que se dirija a la autoridad competente para resolver su problema.

Cuando el impedimento se debe a que existe un certificado digital activo para el solicitante, el AR debe consultar, en el sistema, si este certificado fue emitido por la CA del SINPE, en cuyo caso, debe preguntar al solicitante si desea revocarlo y proceder conforme a lo estipulado en el apartado “Revocación de certificados”. Una vez revocado el certificado debe iniciar nuevamente todo el proceso de registro para la emisión del nuevo certificado.

5.5.3.5. Recolectar evidencia presencial

En cumplimiento de la Política de Certificados, Firmas Digitales y Documentos Electrónicos, la OR debe recolectar y guardar en el sistema evidencia que permita dejar constancia de la presencia física del solicitante durante el proceso de registro de solicitudes.

Por esta razón, el AR debe tomar una fotografía al solicitante, capturar sus huellas digitales y especificar la información de contacto y revocación. Los certificados para diplomáticos serán tramitados única y exclusivamente en la Oficina de Registro del Banco Central, en cuyo caso el AR del Centro de Operaciones del SINPE debe escanear el documento de identidad (DIDI) presentado por el solicitante.

El AR debe, ratificar, firmando digitalmente, que toda la evidencia recolectada corresponde al solicitante presente ante él, que la información de identificación incluida en el sistema corresponde a dicho solicitante y que es correcta.

El AR no debe firmar ni continuar el proceso en caso de duda con respecto a lo anterior.

El certificado digital utilizado por el AR para firmar la evidencia debe ser válido dentro de la cadena de confianza de la jerarquía nacional y corresponder al usuario SINPE que inicio la sesión de registro.

El sistema guiará al AR en todas las acciones necesarias para la recolección de la evidencia presencial (toma de fotografía, toma de huella dactilar y escaneo del documento de identidad en el caso de la atención de diplomáticos por parte de la OR del BCCR), los datos de contacto y revocación y la firma digital del AR. La recolección de toda esta documentación electrónica debe realizarse en presencia del solicitante.

Para garantizar esto, el AR debe realizar dichos pasos en un tiempo máximo de 30 minutos, de lo contrario, el sistema cancelará el proceso de registro y el AR deberá iniciarlo nuevamente.

Toma de fotografía

La fotografía deberá tomarse con el equipo fotográfico adecuado y ajustado de acuerdo con las especificaciones contenidas en el Estándar Físico – Firma Digital.

Cuando el solicitante sea una persona no vidente el AR debe darle todas las indicaciones pertinentes tomando en cuenta la limitación visual de éste; de modo que pueda comprenderlas con facilidad y el proceso pueda llevarse a cabo de la forma más ágil posible. En este sentido debe girar instrucciones tales como: “mantenga su cara en dirección al sonido de mi voz” con el propósito de poder encuadrar la fotografía, De igual forma, en caso necesario, deberá ayudar a posicionar la silla contra el fondo para la toma de la fotografía. Como apoyo adicional, en la siguiente dirección electrónica se muestra una guía para la atención de personas no videntes para la emisión de certificados digitales:

http://www.bccr.fi.cr/sistema_pagos/servicios_sinpe/seguridad/Guia_Nv.pdf

El AR debe garantizar que la fotografía tomada corresponde al solicitante presente frente a él, que está siendo tomada en ese mismo instante y que la calidad de la imagen es apropiada para identificarlo posteriormente.

El AR debe validar visualmente que la fotografía tomada cumpla con las especificaciones contenidas en el Estándar Físico – Firma Digital, lo cual, deberá realizar comparando las proporciones de la misma con la fotografía guía que le proveerá el sistema.

Escaneo del documento de identidad

El escaneo del documento se debe realizar solo cuando el solicitante del certificado es un diplomático y solo se puede tramitar la OR del BCCR operada por el Centro de Operaciones del SINPE (COS). En este caso el AR del COS debe escanear el anverso y el reverso del documento de identidad del solicitante.

El sistema validará que ambas imágenes cumplan con las dimensiones establecidas. Adicionalmente, el AR debe verificar visualmente que las imágenes sean claras y que la información (nombre, la firma, el número de identificación y demás información) es legible.

El AR debe garantizar que las imágenes capturadas corresponden al documento presentado por el solicitante, que fueron capturadas en ese mismo instante y que incluyen toda la información consignada en el documento físico.

Captura de huellas digitales

El AR debe capturar dos huellas dactilares del solicitante, una de cada mano, respetando el siguiente orden: en primera instancia debe capturar las huellas de los dedos índices y en caso de que esto no sea posible deberá continuar con el pulgar, el medio (o corazón), anular y meñique.

En cada caso, el AR debe indicar en el sistema a qué dedo y a qué mano corresponde cada una de las huellas capturadas.

No obstante, si del todo no es posible capturar las huellas del solicitante, sea porque estas resultan ilegibles para el lector de huellas digitales o bien por una condición física del solicitante, el AR deberá dejar constancia de esta condición mediante la opción que el sistema tiene prevista para estos casos. El AR no debe utilizar esta opción a menos que sea estrictamente necesario, habiendo confirmado la imposibilidad de capturar las huellas.

El AR debe garantizar que las huellas capturadas corresponden al solicitante presente frente a él, que fueron tomadas en el mismo instante y que las huellas capturadas o la ausencia de las mismas son el resultado del seguimiento estricto del proceso aquí descrito.

5.5.3.6. Recopilar información de contacto y revocación

El AR debe garantizar que la información de contacto y revocación especificada fue definida por el solicitante durante el proceso de registro y que la misma fue confirmada. El AR debe comunicarle al solicitante la importancia de suministrar información veraz y que pueda recordar con facilidad ya que esta podrá ser utilizada para contactarlo o bien en caso de un eventual proceso de revocación del certificado.

5.5.3.7. Firmar digitalmente resumen de la información recopilada

El AR debe firmar digitalmente el documento electrónico presentado por el sistema que contiene el resumen de la información recopilada del solicitante durante el proceso de registro.

La firma del AR constituye una declaración, mediante la cual, él garantiza que comprobó la identidad del solicitante, que éste estuvo en su presencia durante todo el proceso de registro y que toda la información recopilada corresponde al él.

5.5.4. Generar certificados digitales

Antes de proceder con la generación de los certificados digitales y con el propósito de garantizar transparencia en este proceso, el AR debe verificar si el solicitante anteriormente era suscriptor de certificados digitales de la jerarquía nacional, en cuyo caso se podrá reutilizar el dispositivo criptográfico, siempre y cuando se respete lo descrito en la sección "5.6.2 Reutilización del dispositivo". Por su parte, si el dispositivo criptográfico que se utilizará es nuevo, el AR debe entregar al solicitante el dispositivo en el cual se almacenarán sus certificados. En cualquier caso, el dispositivo debe ser insertado por el solicitante en el lector correspondiente y debe permanecer visible ante él, desde el inicio hasta la finalización del proceso de generación.

Es responsabilidad del AR asegurar que el dispositivo se mantenga dentro del lector durante el todo el proceso por lo tanto deberá instruir al solicitante para que no haga retiro del mismo excepto en caso de que el dispositivo falle.

El número de serie del dispositivo debe estar registrado en el inventario de dispositivos de la CA del SINPE conforme lo indicado en el punto "5.5.1 Inventario de Dispositivos".

Los certificados se emitirán a nombre del solicitante utilizando para ello el nombre y los apellidos especificados por el AR en la solicitud durante el proceso de registro, en consecuencia, la CA del SINPE emitirá el certificado con base en los datos incluidos bajo la presunción de su veracidad.

A fin de garantizar el “No Repudio” la emisión de certificados digitales no admite anonimato ni discrepancias con la información remitida por la OR. El pseudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del certificado.

El AR solamente debe generar los certificados digitales correspondientes a procesos de registro de solicitudes que él mismo ejecutó, lo cual es controlado por el sistema. Esto significa que el AR no podrá generar certificados de solicitudes registradas por otro AR.

Después de generar el certificado el sistema leerá el número de serie y validará que el dispositivo en que se generaron los certificados está incluido en el inventario. En caso contrario el sistema procederá a revocar automáticamente los certificados.

El AR deberá conservar el documento de identidad del solicitante mientras se ejecuta el proceso de activación, con la meta de verificar posteriormente la ejecución correcta de dicho proceso.

5.5.5. Generar contraseña de desbloqueo (OTP)

Cuando conforme lo indicado en el apartado “Captura de huellas digitales” no haya sido posible capturar las huellas del solicitante y el AR dejó constancia de esta condición en el sistema, el AR debe proceder a generar una contraseña temporal (OTP). Esta contraseña debe escribirla en una hoja y entregarla al solicitante, a efecto de que este la utilice en la activación del dispositivo conforme lo dispuesto en el apartado “6 Activación de dispositivos.”, de la presente norma.

Asimismo, el AR también podrá generar un OTP cuando el solicitante tenga problemas de activación de su dispositivo por medio del uso de su huella dactilar; en este caso, previo a la entrega del OTP, el AR debe validar la identidad del solicitante verificando que este es la misma persona a quien corresponde el documento de identidad que el AR mantiene en su poder.

5.5.6. Activación de dispositivos para habilitar el uso de certificados

Para que la activación del dispositivo sea segura, la OR debe disponer de un Quiosco de Activación de Dispositivos que cumpla con todas las medidas de seguridad y de infraestructura especificadas en el Estándar Físico - Firma Digital.

El AR debe indicarle al suscriptor que se dirija al Quiosco inmediatamente después de generados los certificados digitales y que, por medio del uso de su huella digital o en su defecto, cuando así corresponda, por medio del uso del OPT, active su dispositivo definiendo su número de identificación personal (PIN) en completo estado de privacidad.

Adicionalmente, cuando el suscriptor sea una persona no vidente, antes de que éste pase a realizar la activación de su dispositivo, el AR debe indicar dónde está ubicado el Quiosco de activación, dar una explicación del proceso que deberá seguir durante la activación de su certificado, así como la

ubicación física que tienen en el Quiosco, cada uno de los dispositivos que requerirá (teclado, lector de huellas, lector de tarjetas y mouse), de modo que la persona no vidente pueda localizarlos con facilidad y no tenga dificultades para poder llevar a cabo el proceso. En la siguiente dirección se muestra un video con ejemplo de los cuatro pasos que se necesitan para activar y firmar el acuerdo suscriptor, el cual es recomendable que sea revisado por los solicitantes antes de acudir a la cita, especialmente si éste es no vidente, lo cual le permitirá familiarizarse con el proceso que va a realizar: http://www.youtube.com/watch?v=pf0I852SfU4.

El AR debe instruir al suscriptor acerca las características del PIN que deberá definir para activar su tarjeta en el Quiosco, el cual debe cumplir con las siguientes especificaciones:

- Máximo 14 caracteres
- Mínimo 4 caracteres
- Máximo 2 caracteres repetidos
- Máximo 2 caracteres consecutivos
- Incluir sólo números

Ejemplos válidos:

- 551243014089
- 986501
- 1278

Ejemplos Inválidos:

- 9876 (incumple la característica d)
- 73338 (Incumple característica c)
- AA2234ci (incumple la característica e y la d)
- 101 (no reúne el tamaño mínimo)

Bajo ninguna circunstancia el AR debe acompañar al suscriptor al Quiosco de Activación, ni asistirlo o realizar alguna acción por medio de la que pueda llegar a tener conocimiento del PIN del usuario.

El certificado se da por aceptado cuando el suscriptor firma digitalmente el “Acuerdo de Suscriptor” el cual, contiene el detalle de los derechos y obligaciones relacionados con el uso de certificados digitales incluyendo lo relativo a los mecanismos de validación y revocación y, se constituye en sí mismo en el comprobante de aceptación del certificado digital.

El sistema revocará automáticamente los certificados digitales generados al suscriptor cuando éste no firme digitalmente el “Acuerdo Suscriptor”.

Una vez que el AR verifique que el solicitante ejecutó correctamente el proceso de activación debe solicitar al suscriptor que firme, en forma manuscrita el dispositivo; luego de esto debe proceder a devolverle el documento de identidad e informarle sobre sus deberes y responsabilidades con respecto al uso de sus certificados digitales y sobre el buen uso y custodia del dispositivo así como la importancia de mantener el PIN en forma secreta.

El AR deberá informar al suscriptor que podrá obtener una copia del Acuerdo de Suscriptor en la dirección http://fdi.sinpe.fi.cr/documentacion.html.

5.5.7. Revocación de certificados

Es responsabilidad de la OR brindar el servicio de revocación de certificados al suscriptor en un horario de 24 horas diarias los 7 días de la semana, ya sea por medio del Sitio Web http://fdi.sinpe.fi.cr/revocar.aspx, o bien utilizando el módulo de Revocación que se incluye en el servicio FDI del SINPE, para lo cual, el suscriptor puede gestionar la solicitud de revocación de sus certificados, presencialmente ante la OR o por teléfono.

Con el objeto de dejar mayor evidencia de lo actuado por el AR en la ejecución de su rol de Agente de Revocación, cuando el servicio de revocación se realice dentro del horario bancario, es recomendable que se realice por medio del Módulo de Revocación que, con este propósito, está disponible en el servicio de firma digital.

Para revocar los certificados, el AR debe verificar la información de revocación obtenida durante el proceso de registro y emisión de su certificado. En caso de que el procedimiento no pueda completarse, el AR podrá trasladar el caso al Centro de Operaciones del SINPE para que por su medio se realice el trámite de revocación correspondiente.

5.6. Particularidades del servicio

5.6.1. Renovación y Re-emisión de certificados

Los certificados digitales emitidos por la CA del SINPE tienen una vigencia de dos años contados a partir de la fecha de su expedición.

La Política de Certificados para la Jerarquía Nacional de Certificadores Registrados no permite la renovación ni la re-emisión de certificados por lo que, si por cualquier motivo, se requiere alguna de estas acciones lo que procede es emitir un nuevo certificado

5.6.2. Reutilización del dispositivo

Un suscriptor podrá solicitar la emisión de un nuevo certificado utilizando el mismo dispositivo que contiene sus certificados anteriores, siempre y cuando se encuentre en buen estado, los certificados contenidos sean del suscriptor que solicita el nuevo certificado y estos hayan sido revocados. Previo a la emisión del nuevo certificado, el AR debe retirar del dispositivo los certificados anteriores.

Cuando no sea posible la reutilización del dispositivo, el Agente de Registro debe emitir los certificados solicitados en un nuevo dispositivo de conformidad con lo dispuesto en este cuerpo normativo.

5.6.3. Acreditación de Oficinas de Registro

Toda entidad asociada al SINPE, interesada en constituir oficinas de registro (OR), debe cumplir con los requisitos establecidos en el EF- FDI, así como con los procedimientos para autorizar la operación de una OR administrados por el COS los cuales, entre otros requisitos, contempla los siguientes:

1. Carta de solicitud
   - **a)** Presentar una carta dirigida al Director de la División de Sistemas de Pago manifestando su deseo de constituir un OR y solicitando el envío de la información necesaria acerca de los requisitos que debe cumplir para tal efecto.
2. Verificación del cumplimiento de requisitos:
   - **a)** Una vez que la entidad asociada al SINPE considere que ha cumplido con todos los requisitos para constituirse en una OR, debe solicitar al COS la verificación correspondiente.

b) Dicha verificación será realizada por el COS, utilizando como herramienta una lista de verificación elaborada para el efecto, la cual, formará parte del expediente de instalación de la oficina de registro.

c) Una vez verificados y aprobados los requisitos establecidos en la lista de verificación, las entidades deben coordinar con el COS los procesos de instalación de los nodos y los equipos periféricos requeridos con sus drivers. Este proceso debe realizarse conjuntamente entre el personal del BCCR y el personal técnico de la entidad con el objetivo de que pueda realizarse esta labor en una sola visita.

d) Todos los requisitos incluidos en la lista de verificación son de cumplimiento obligatorio, no obstante algunos de ellos pueden cumplirse en una fecha posterior que no deberá exceder de 6 meses contados a partir de la fecha en que sea dada de alta la OR. La fecha en que se deberá verificar los requisitos pendientes deberá consignarse en dicha lista.

e) El objetivo del otorgamiento de esta flexibilidad en el cumplimento de requisitos tiene el propósito de permitir que la OR quede habilitada lo más pronto posible.

3. Plan Piloto previo a dar de alta a la OR:

a) Ninguna OR será acreditada como tal y por lo tanto no podrá emitir certificados hasta tanto haya finalizado exitosamente las pruebas de funcionamiento correspondientes al Plan Piloto.

b) Estas pruebas se realizarán una vez que cada oficina de registro haya cumplido con todos los requisitos, conforme la verificación realizada por el COS.

c) Estas pruebas son realizadas en ambiente de producción y por ende permiten comprobar el funcionamiento de la emisión de certificados de la CA del SINPE. La OR debe tomar en cuenta que los certificados digitales emitidos, durante el Plan Piloto, tienen la validez jurídica otorgada por la Ley 8454 y por lo tanto deben emitirse con toda la rigurosidad requerida en el cuerpo normativo del servicio Firma Digital.

5.6.4. Obligaciones de la OR respecto a los suscriptores

Toda entidad que ponga en operación una o más OR tiene la obligación de realizar las siguientes actividades como parte del servicio que presta:

Informar sobre los requisitos técnicos de la computadora

Toda oficina de registro al momento de otorgar las citas y especialmente antes de emitir el certificado digital debe informar sobre los requisitos técnicos que debe poseer el equipo de cómputo en el que los clientes van a operar los certificados digitales, con el fin de evitar inconvenientes posteriores en la instalación de los drivers requeridos para los dispositivos de firma digital. Esta información debe estar disponible para los potenciales suscriptores en un medio de acceso público de la OR.

Contar con un servicio de soporte a clientes en la instalación de drivers de Smart cards y lectores para la operación correcta de la Firma Digital

La OR debe proveer un servicio de soporte, ya sea propio o contratado, que le garantice a sus clientes, tener la ayuda de personal calificado en la instalación de las Smart cards, lectores y software necesarios para el adecuado funcionamiento de la firma digital, a fin de asegurar que los clientes realicen y concluyan el proceso de instalación de los drivers en sus computadores personales en forma exitosa. Adicionalmente, la OR deberá mantener el servicio de soporte disponible de modo que el cliente tenga donde recurrir toda vez que requiera asistencia para la instalación y configuración de los dispositivos.

Entregar información relevante al cliente

Toda OR debe implementar los mecanismos necesarios para que, cada vez que el AR entregue un certificado digital a un cliente, éste le informe, al menos sobre los siguientes tópicos:

- Servicio de soporte: los datos básicos que le permitan al cliente acceder a dicho servicio (números de teléfono, direcciones URL, correo electrónico, etc.) y cualquier otra información relevante relacionada con éste.
- Revocación de certificados: Informar al cliente que la revocación de los certificados la puede realizar por medio de la página Web http://fdi.sinpe.fi.cr/revocar.aspx, presencialmente o por teléfono ante la OR. Se debe instruir al cliente que la revocación procede cuando sospeche del compromiso de su llave privada (robo, pérdida, extravío de la tarjeta o un potencial riesgo de conocimiento de su PIN por un tercero) o por voluntad propia decida no poseer más certificados digitales a su nombre.
- Cambio de PIN: Recomendar al cliente el cambio periódico del PIN de su Smart card e indicar la forma en que lo puede realizar.

Proveer el software de instalación de dispositivos

La OR debe proveer al cliente todo el software requerido para instalar el Smart card y el lector así como para configurar el equipo adecuadamente para que opere con los certificados digitales de la CA del SINPE.

De preferencia la OR debe proveer al cliente un programa instalador que automáticamente instale todas los drivers y configure el equipo sin intervención del usuario o en su defecto, como mínimo deberá entregar el cliente todos los drivers y piezas de software requeridas junto con un manual de instrucciones detallado que permita al usuario hacer la instalación paso a paso.

5.6.5. Auditorías de cumplimiento y otras evaluaciones

En cumplimiento de lo estipulado en el artículo 21 de la Ley de Firma Digital, “Todo certificador registrado estará sujeto a los procedimientos de evaluación y auditoría que acuerde efectuar la DCFD o el ECA”

Adicionalmente, de conformidad con lo estipulado en la Sección 8 de la Política de Certificados para la Jerarquía Nacional de Certificadores Registrados, cada CA debe implementar un programa de auditorías internas para la verificación de su sistema de gestión. Dicho programa de auditorías debe estar basado en la INTE_ISO/IEC 19011 “Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental”.

En consecuencia toda OR estará sujeta y deberá permitir la realización de los procedimientos de evaluación y auditoría que determinen la DCFD y/o la CA del SINPE y que serán ejecutadas por parte de los entes o los funcionarios que dichas organizaciones designen para este propósito.

5.7. Situaciones contingentes

5.7.1. Disponibilidad

Por su parte, la CA del SINPE Personas Físicas garantiza que los servicios de Revocación y Validación del Estado de los Certificados para Firma o Autenticación de Firmas Digitales de Personas Físicas estarán disponibles y contará con soporte todos los días del año durante las veinticuatro horas del día. El servicio de emisión de certificados, también estará disponible en un horario 24/7, sin embargo, el soporte se dará dentro del horario bancario

5.8. Responsabilidades

Sin perjuicio de lo establecido en el Reglamento del Sistema de Pagos, los derechos, obligaciones y responsabilidades de los participantes en el servicio de Firma Digital son los establecidos por la Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº8454 y su reglamento, la Política de Certificados para la Jerarquía Nacional de Certificadores Registrados y las Directrices para las autoridades de Registro y demás disposiciones aplicables, así como las que se derivan de lo estipulado en la presente norma, la cual es complementaria a las disposiciones contenidas en el Reglamento del Sistema de Pagos.