

WEB.CERTICAMARA.COM

certicámara.

FICHA TÉCNICA PRODUCTO

Huella Biometrica Certificada

Índice

Objetivo 3

Glosario 3

Normatividad asociada 6

Descripción detallada de la solución 7

Productos y servicios requeridos18

Usos19

Reportes19

Requisitos20

 - Funcionales

 - Técnicos

Arquitectura22

Tiempos de instalación e implementación25

Entregables25

Objetivo

Prestar un servicio mediante el cual se permite realizar procesos de verificación de identidad haciendo uso de la huella digital cotejada 1:1 contra una réplica de la base de datos biográfica y biométrica de la Registraduría Nacional del Estado Civil, adicionando la aplicación de captura de huellas (minucias) y los dispositivos de captura de huella.

Glosario

- Autoridad de Registro (RA): Persona jurídica, con excepción de los notarios públicos, o parte interna de las ECD necesariamente independiente de su CA, que acorde con la normatividad vigente, es la encargada de recibir las solicitudes relacionadas con certificación digital, para:
 - Registrar las peticiones que hagan los solicitantes para obtener un certificado.
 - Comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones.
 - Enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas
- Autoridad de Sellado de Tiempo (TSA): Entidad de confianza que emite sellos de tiempo.
- Autoridad de Validación (VA): Entidad de confianza que proporciona información sobre la validez de los certificados digitales.
- OID: Identificador único de objeto (object identifier). OID. acrónimo del término en idioma inglés “object identifier”, que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.
- CA Raíz: Autoridad certificadora de primer nivel, base de confianza.
- CA Subordinada: Autoridad certificadora de segundo nivel o más niveles.

- **Certificado Digital:** Mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de éste último.
- **Cliente:** En los servicios de certificación digital, el término cliente identifica a la persona natural o jurídica con la cual la ECD establece una relación comercial.
- **Datos de Creación de Firma (Llave Privada):** Son valores numéricos únicos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.
- **Datos de Verificación de Firma (Llave Pública):** Son los datos, como códigos o claves criptográficas públicas, que son utilizados para verificar que una firma digital fue generada con la llave privada del suscriptor.
- **Declaración de Prácticas de Certificación (DPC):** Es el documento en el que consta de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios. Una declaración de las prácticas que una ECD emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.
- **Entidad de Certificación:** De acuerdo con lo indicado en la ley 527 de 1999, artículo 2, literal d, es aquella persona natural o jurídica que, autorizada conforme a dicha ley, está facultada para emitir certificados digitales en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.
- **Firma Digital:** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
- **PKI (Public Key Infrastructure):** Es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran:

- Algoritmo: Es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.
- AFIS – Automatic Fingerprint Identification System: Sistema Automático de Identificación Dactilar.
- Aplicante: Persona natural sobre la cual se requiere realizar el proceso de verificación de identidad por medio de las huellas dactilares.
- ATDP: Autorización de Tratamiento de Datos Personales. Documento que debe ser informado al aplicante antes de consultar la base de datos réplica II y almacenado electrónicamente para consulta en línea por la RNEC.
- Autenticación: Proceso de COTEJO 1:1 de minucias de huellas de un aplicante contra las minucias de huellas de un candidato.
- Autenticación Biométrica: Es el proceso tecnológico de verificación y validación de la identidad de las personas por medio de las huellas dactilares.
- Cotejo 1:1: Proceso de verificación de correspondencia biométrica entre las minucias de huellas de un aplicante contra las minucias de huellas de un candidato.
- Enrolar: Registrar en una base de datos información relacionada con personas, usuarios o elementos para su posterior consulta
- Función HASH: Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.
- Iframe: Es un elemento HTML que permite insertar o incrustar un documento HTML dentro de un documento HTML principal.
- ISO-FMR: Formato ISO de minucias de huellas dactilares. Su mención en este documento estará relacionada con el formato de minucias de huellas dactilares ISO-FMR-19794-2:2011.
- Log: Servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.
- Minucia: Son un conjunto de puntos únicos sobre la completitud de la huella que permiten establecer un patrón de la misma
- Neutralidad Tecnológica: Principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, así mismo la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.
- Niveles de Seguridad: Son los diversos niveles de garantía que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.
- NUT: Número Único de Transacción.
- Operador Biométrico: Aliado tecnológico del CLIENTE o CLIENTE certificado por la REGISTRADURÍA con la infraestructura tecnológica para consumir el servicio web y realizar el cotejo biométrico con las minucias suministradas por la REGISTRADURÍA.

Normatividad asociada

Descripción general de la normativa vigente que aplica a la solución que se va a presentar a continuación:

NORMOGRAMA				
TIPO DE NORMA	NO. Y FECHA DE EXPEDICIÓN	TITULO	EXPEDIDO POR	SÍNTESIS O APLICACIÓN ESPECIFICA
Ley	No. 1753 del 9 de Junio 2015	Plan Nacional de Desarrollo 2014-2018.	Congreso de la República	Artículo 159: permite el acceso a la información biográfica y biométrica de la RNEC a particulares que desarrollen actividades del art. 335 de la Constitución Política y los demás que autorice la ley.
Resolución	No. 5633 del 29 de Junio de 2016	Se reglamentan las condiciones y el procedimiento para el acceso a las bases de datos de la información que produce y administra la RNEC.	Registraduría Nacional del Estado Civil	Reglamenta las condiciones y procedimientos a seguir por parte de las entidades públicas y de los particulares autorizados por la ley, para el acceso de las bases de datos de la RNEC.
Ley estatutaria	No. 1581 del 17 de octubre de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Congreso de la república.	Constituye el marco general de la protección y tratamiento de los datos personales en Colombia.
Ley	No. 527 del 18 de agosto de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.	Congreso de la república.	Marco legal de las entidades de certificación digital y característica, condiciones y requisitos aplicables a su operación. Establece los términos bajo los cuales será prestado el servicio de certificación digital. Capítulo II artículo 12 y 13.
Decreto ley	019 del 10 de enero de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la administración pública.	Departamento administrativo de la función pública.	Artículo 17, eliminación huella dactilar: suprímase el requisito de imponer la huella dactilar en todo documento, trámite, procedimiento o actuación que se deba surtir ante las entidades públicas y los particulares que cumplan funciones administrativas.

Descripción detallada de la solución

Huella Biométrica Certificada

Servicio que permite realizar la verificación y validación de identidad de una persona a través de medios electrónicos, mediante el acceso y consulta de los patrones de su huella dactilar conocidos como minucia, frente a una fuente confiable como es la réplica de la Base de Datos Biográfica y Biométrica de la Registraduría Nacional del Estado Civil (RNEC) contra la cual, se realizará el cotejo de la huella, dando cumplimiento a la normativa vigente para la prestación de este servicio, los contratos comerciales, acuerdos comerciales y la promesa de valor ofrecida a los clientes.

Para tal efecto, Certicámara se ha acreditado como operador de autenticación de identidad digital ante la RNEC como lo confirma el siguiente enlace <https://wsp.registraduria.gov.co/biometria/operadores/listar>

Actividades ante la RNEC

A continuación, se indican las actividades que el solicitante autorizado por la normativa vigente para la utilización del servicio de Huella Biométrica Certificada, para acceder y consultar la Base de Datos Biográfica y Biométrica de la Registraduría Nacional del Estado Civil (RNEC) y las cuales debe llevar a cabo.

- Elevar una solicitud escrita a la RNEC con la intención de celebrar un contrato o convenio con esta última. Dicha solicitud debe encontrarse soportada en el estudio de necesidad que el solicitante elabore de conformidad con lo establecido en la Resolución 27145 de 2023.
- Presentación del modelo técnico y funcional a implementar.
- Revisión y análisis de la viabilidad técnica y jurídica de la solución a implementar por parte de la RNEC.
- Revisión del software implementado.
- Suscripción y legalización del contrato o convenio entre el solicitante y la RNEC.

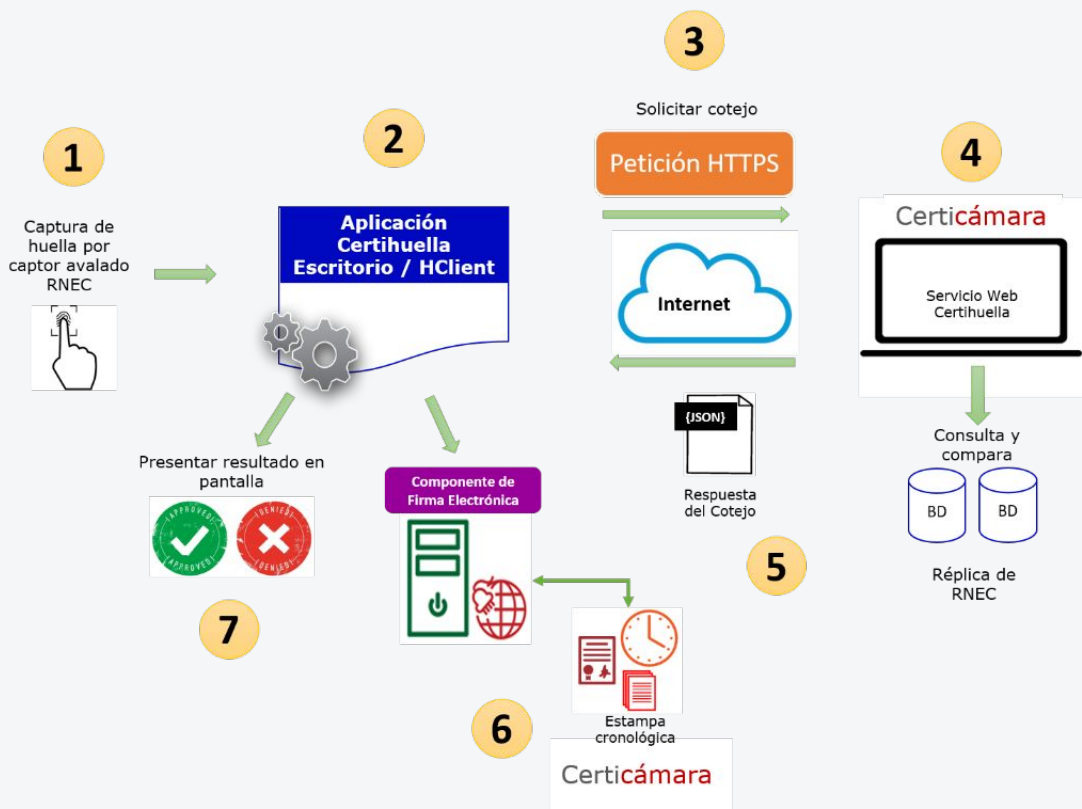
Descripción detallada de la solución

Servicio Web CertiHuella

Servicio web provisto desde la infraestructura de Certicámara, el cual permite realizar la validación de identidad de una persona mediante la comparación de los patrones de la huella dactilar conocidos como minucia, con respecto a una fuente confiable como es la réplica de base de datos biográfica y biométrica de la RNEC.

Este servicio recibe como parámetros de entrada, entre otros, dos minucias de huella dactilar únicamente en formato ISO-FMR, el número de cédula de ciudadanía de la persona a consultar. El servicio como parámetros de salida, retorna los datos biográficos de la persona consultada junto con una respuesta positiva o negativa según el resultado del cotejo entre las dos minucias de huella dactilar recibidas y las dos minucias de huella dactilar correspondientes en la base de datos réplica de la RNEC.

El consumo de este servicio se lanza desde el aplicativo front-end de toma de huellas en esta propuesta se ofertan CertiHuella de Escritorio o HClient, en la siguiente gráfica, se presenta un diagrama general de entendimiento:



Descripción detallada de la solución

Funcionamiento:

A continuación, se describe el Funcionamiento general de la solución integrada, acorde al diagrama de entendimiento:

1. El funcionario ya autenticado en la aplicación CertiHuella de Escritorio o HClient, solicitará al usuario que ubique la huella dactilar del dedo indicado en el captor. Se solicitarán dos dedos por cotejo para que en una única transacción se realicen dos verificaciones y de esta manera se reduzca la posibilidad de una respuesta negativa.
2. La aplicación CertiHuella de Escritorio o HClient realiza la comunicación con el captor biométrico y prepara los datos para hacer el consumo del servicio web de CertiHuella mediante el API que administra la conexión al servicio, la cual se encuentra integrada dentro de la aplicación.
3. Se solicita el cotejo con respecto al número de documento suministrado y la información necesaria de los parámetros de entrada del servicio web de CertiHuella.
4. El servicio web CertiHuella realiza el cotejo de las huellas para el número de cédula recibido.
5. Una vez hecha la validación, el servicio web CertiHuella retorna a la aplicación CertiHuella de Escritorio o HClient la información biográfica de la persona, junto con el resultado de la verificación biométrica.
6. La aplicación CertiHuella de Escritorio o HClient recibe esta respuesta de la validación y le entrega al Componente de Firma Electrónica el NUT para realizar la firma y estampa cronológica del documento de Autorización de Tratamiento de Datos Personales (ATDP).
7. La aplicación CertiHuella de Escritorio o HClient muestra en pantalla la respuesta de la validación.

Descripción detallada de la solución

Aplicación CertiHuella de Escritorio:

Aplicación de escritorio para equipos de cómputo con sistema operativo Windows (7,8,10,11) en adelante, se instalará en cada una de las estaciones de trabajo previstas para realizar las actividades de verificación de identidad con huella dactilar.

El software de CertiHuella de Escritorio:

- o No tendrá ningún tipo de integración con el sistema de la entidad
- o Incorpora en su funcionamiento los componentes que permite interactuar con los dispositivos biométricos de captura de huella dactilar Morpho MSO 1300 E3 o Suprema Biomini Slim S
- o Se encarga del consumo de los servicios web de CertiHuella para efectuar los cotejos de validación de identidad.
- o En el caso de emplearse el captor Morpho MSO 1300 E3, los archivos ca.crt, host.der y host.key, estarán ubicados en una ruta por defecto, para ser empleados por el aplicativo de CertiHuella de Escritorio si es SECURISE

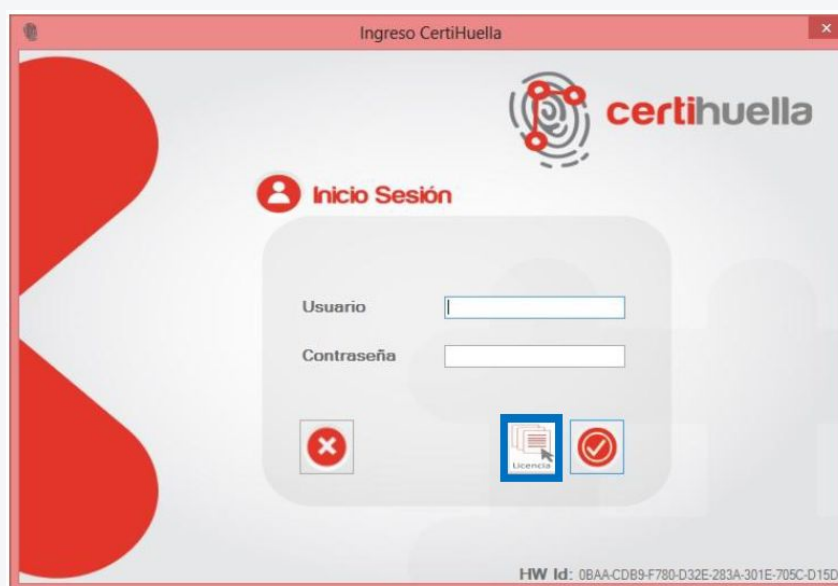
A continuación, se describe CertiHuella de Escritorio a nivel funcional, indicando entradas proceso y salidas:

1. El aplicativo inicia su ejecución por acción del usuario.
2. Requiere autenticación de Usuario y Contraseña para acceder a la aplicación.
3. El aplicativo verifica la autenticación contra el Directorio Activo de la entidad.
4. Presenta el texto de Autorización de Tratamiento de Datos Personales (ATDP) solicitando su aprobación.
5. Permite ingresar el número de cédula del ciudadano y la captura de dos Minucias de huella dactilar para verificación de identidad con el servicio web CertiHuella.
6. CertiHuella de Escritorio envía al servicio web CertiHuella la información biométrica capturada y la solicitud de cotejo.
7. CertiHuella de Escritorio obtiene el resultado del cotejo.
8. CertiHuella de Escritorio muestra en pantalla la respuesta del cotejo, indicando tanto los datos biográficos como el resultado "Exitoso" o "No Exitoso" según la verificación realizada por el servicio web CertiHuella.

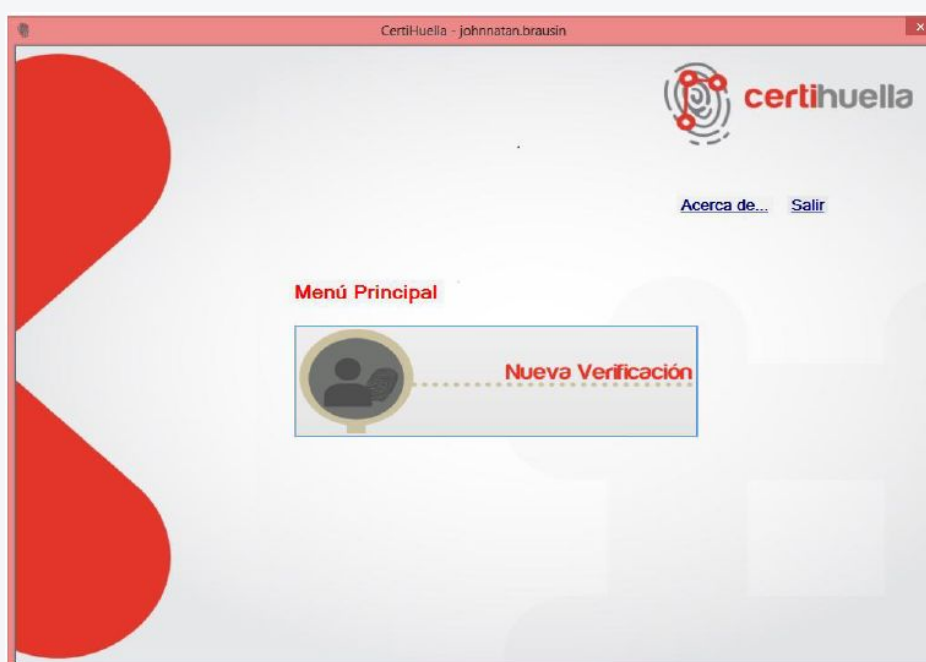
Descripción detallada de la solución

Flujo de pantallas:

1. Autenticación con el directorio activo:



2. Dar la orden de nueva verificación:



Descripción detallada de la solución

3. Ingresar número de identificación del ciudadano, seleccionar de la lista desplegable la operación y mostrar el acuerdo de Tratamiento de Datos Personales (ATDP):

CertiHuella Versión 1.0.1 -

Proceso de captura de información CÉDULA DE CIUDADANÍA

Información personal

No. Documento

Operación

AUTORIZACIÓN DE CONSULTA Y TRATAMIENTO DE DATOS BIOMÉTRICOS PARA VALIDACIÓN DE IDENTIDAD

Autorizo a Banco Popular S.A. de manera voluntaria, expresa, completa, informada e inequívoca para darle tratamiento a los datos personales, incluyendo datos biométricos, suministrados con el diligenciamiento del presente formato o los que suministre a futuro, para: a. diligenciar, complementar y/o actualizar las bases de datos de Banco Popular S.A., b. tramitar la apertura y/o vinculación de productos y/o servicios, c. validar mi identidad en el uso de productos y/o servicios y d. para que la validación de mi identidad mediante datos biométricos pueda ser utilizada como modo de prueba. De manera particular, con la imposición de mis huellas digitales a través de medios electrónicos, autorizo de manera expresa y previa a Banco Popular S.A. para que valide mis huellas digitales, con la finalidad de que a través de una entidad certificada como operador biométrico o en forma directa, realice la validación de mi identidad contra la base de datos que

☐ Se ha leído la Autorización al Usuario

Menu Siguiente

4. Seleccionar dedo y capturar primera huella, el aplicativo muestra en orden aleatorio la selección de la huella a capturar y muestra una imagen dummy de la huella:

Proceso de captura de primera huella digital

Selección dedo:

INDICE - DER (N° 2)

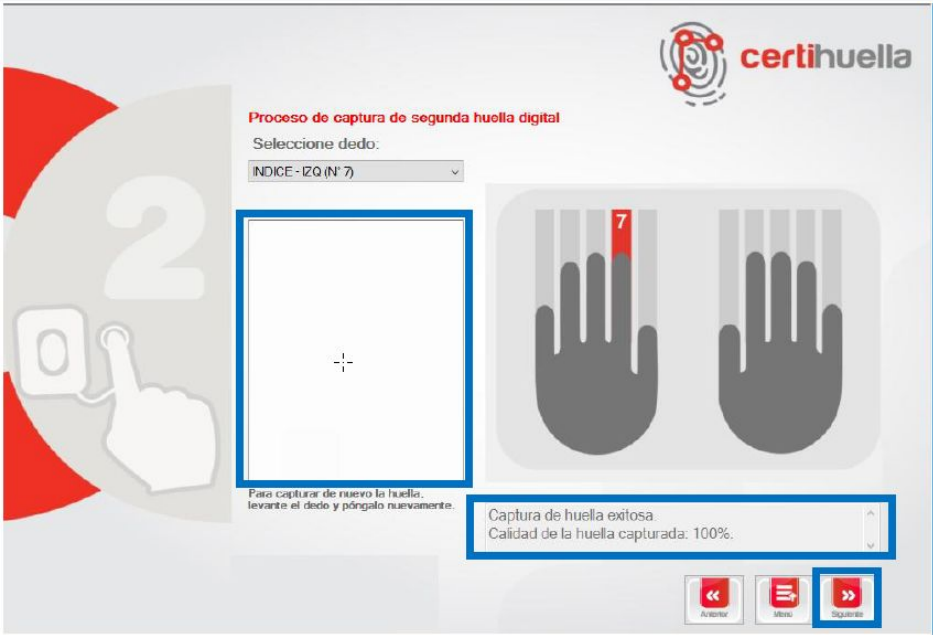
Captura de huella

Captura de huella exitosa.
Calidad de la huella capturada: 100%

Anterior Menu Siguiente

Descripción detallada de la solución

5. Seleccionar dedo y capturar segunda huella, el aplicativo muestra en orden aleatorio la selección de la huella a capturar y muestra una imagen dummy de la huella:



6. Mostrar la respuesta de la validación de identidad:



Descripción detallada de la solución

Aplicación Hclient

Aplicación de escritorio para equipos de cómputo con sistema operativo Windows (7,8.10 y 11), se instalará en cada una de las estaciones de trabajo previstas para realizar las actividades de validación de identidad con huella dactilar. El HClient permite:

- Se integra con el sistema de la entidad permitiendo realizar el proceso de captura de huellas dactilares.
- Incorpora en su funcionamiento los componentes que permite interactuar con los dispositivos biométricos de captura de huella dactilar Morpho MSO 1300 E3 o Suprema Biomini Slim S
- Se encarga del consumo de los servicios web de CertiHuella para efectuar los cotejos de validación de identidad.
- En el caso de emplearse el captor Morpho MSO 1300 E3, los archivos ca.crt, host.der y host.key, estarán ubicados en una ruta por defecto, para ser empleados por el aplicativo de HClient de ser Securizados.

A continuación, se describe HClient a nivel funcional, indicando entradas, proceso y salidas:

1. El aplicativo está diseñado para ser llamado a ejecución desde una aplicación web.
2. Una vez realizado el llamado a ejecución autorizado, el HClient presenta en pantalla su interfaz, permitiendo la captura de dos Minucias de huella dactilar, para verificación de identidad con el servicio web CertiHuella.
3. HClient envía al servicio web CertiHuella la información biométrica capturada y la solicitud de cotejo.
4. HClient obtiene el resultado del cotejo.
5. HClient muestra en pantalla la respuesta del cotejo, indicando tanto los datos biográficos como el resultado "Exitoso" o de ser "No Exitoso" solo muestra la información del documento número respuesta y Número único de Transacción según la verificación realizada por el servicio web CertiHuella.
6. HClient proporciona la respuesta del cotejo y la muestra en pantalla.

Descripción detallada de la solución

Datos de entrada del HClient:

Parámetros de configuración desde el aplicativo de la entidad:

- o Usuario de la suscripción para cotejo
- o Contraseña de la suscripción para el proceso
- o Identificador del proceso de negocio asociado al servicio
- o Identificador de la sucursal desde la que se inicia la transacción
- o Número de intentos de cotejo contra RNEC
- o Valor mínimo de calidad aceptado para la captura
- o Número de intentos de captura para cumplir la calidad mínima de la huella
- o Número de cédula del cliente a validar su identidad
- o Identificador del usuario/funcionario que solicita la transacción

Datos de salida del HClient en la actividad de captura:

- Las dos minucias de huella capturadas, correspondiente a dos dedos diferentes.
- Número de cédula del cliente.
- Usuario de la suscripción para cotejo.
- Contraseña de la suscripción para cotejo.
- Dirección IP del equipo de cómputo desde donde se inicia la transacción.
- Dirección MAC del equipo de cómputo desde el cual se inicia la transacción. HClient deberá obtener este dato.
- Identificador del proceso de negocio asociado al servicio.
- Identificador de la sucursal de la entidad desde la cual se inicia la transacción

Descripción detallada de la solución

Datos de salida del HClient en la actividad de validación de identidad:

Datos biográficos de la persona verificada:

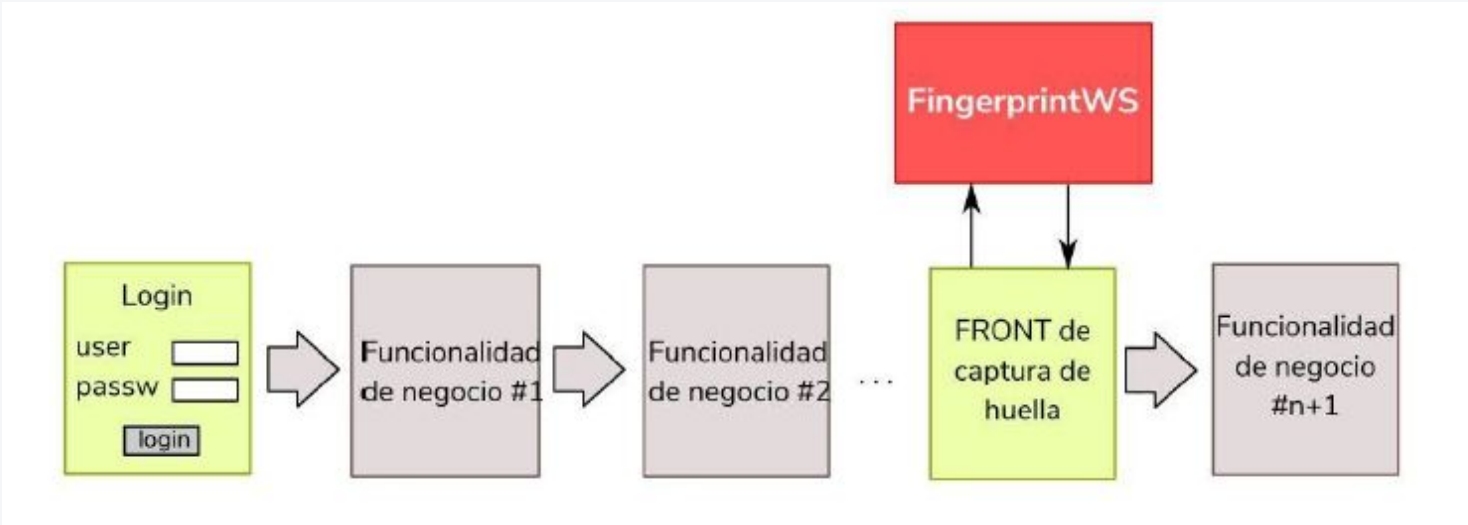
- Número de cédula.
- Nombre completo.
- Lugar de expedición de la cédula.
- Fecha de expedición de la cédula.
- Vigencia del documento. Los posibles estados son:
 - Vigente
 - Pérdida o suspensión de derechos políticos
 - Cancelada por muerte
 - Cancelada por doble cedula
 - Cancelada por suplantación
 - Cancelada por extranjería
 - Cancelada por mala elaboración
 - Cancelada por cambio o reasignación de sexo
 - Cancelada por falsa identidad
 - Revocatorias de cancelación
- NUT, Número Único de Transacción.
- Resultado de la verificación de identidad mediante el cotejo de huellas: "Autorizado" o "No Autorizado" según el caso.

Descripción detallada de la solución

Componente FingerPrint WS

El componente FingerprintWS, consiste en una aplicación que se instala en una estación con sistema operativo Microsoft Windows 7/8/10 y un lector biométrico Suprema BioMini Slim S XXX o Morpho MSO1300 E3 conectado, la cual expone un servicio web HTTPS en el puerto TCP/IP 8020, diseñado para ser llamado de forma local.

Un escenario común en que se usa el componente es en la validación de huella desde aplicaciones web, la invocación en este caso se hace desde el browser usando JavaScript, los templates de huella son transferidos al servidor que aloja la aplicación web o directamente al servicio de CertiHuella, dependiendo de la arquitectura de la aplicación.



Productos y servicios requeridos

A continuación, se detallan los productos y servicios requeridos para la implementación de la alternativa de solución presentada.

CANT.	PRODUCTO/SERVICIO	DESCRIPCIÓN
1	Suscripción para uso de los servicios expuestos por CertiHuella	Derecho al uso del servicio web expuesto por Certicámara a través del protocolo REST sobre internet.
N	Volumen de verificaciones anuales	Cantidad de transacciones esperadas para la validación de identidad.
N	Aplicativo de captura de huellas CertiHuella de Escritorio/HClient	Aplicativo front para la toma de huellas digitales y consumo de los servicios web CertiHuella. Incluye el Api de integración con el servicio web CertiHuella y componente local de interacción con el captor biométrico.
1	Componente Centralizado de firma WS-Sign	Componente a nivel de servidor que permitirá realizar la firma electrónica certificada de documentos PDF, en el esquema de licencia Anual
N	Firmas electrónicas del documento ATDP	Esta firma incluye la implementación del mecanismo de Firma Electrónica a través del NUT (Número Único de Transacción), la generación de la Firma Digital y el estampado cronológico certificado en el documento del ATDP.
1	Servicio de soporte técnico, mantenimiento y actualizaciones	Servicio de soporte posterior al primer año de garantía.

Usos

- Verificación de identidad de ciudadanos colombianos contra la réplica de la Base de Datos Biográfica y Biométrica de la RNEC.
- Posibilidad de hacer uso de las 10 huellas de las manos para verificar la identidad de un ciudadano colombiano.
- Conocer el estado de vigencia de la cédula.
- Conocer los datos biográficos públicos del ciudadano verificado:
 - o Nombre completo.
 - o Lugar y fecha de expedición de la cédula.
- Sitio web de gestión, en donde es posible:
 - o Consultar la cantidad de verificaciones de identidad realizadas.
 - o Llevar el registro de usuarios y equipos de cómputo que accederán al servicio.
- Posibilidad de integración con otros sistemas del cliente a través de Web Service.

La verificación y validación de identidad con huella biométrica ante la RNEC, puede utilizarse por el solicitante que se encuentre habilitado en virtud de la normativa vigente, con el fin de realizar la validación de identidad de ciudadanos colombianos con cédula de ciudadanía debidamente expedida y adicionalmente para aplicar firma electrónica certificada sobre el documento electrónico de Autorización de Tratamiento de Datos Personales (ATDP), Mecanismo para prevención de Fraude, mecanismo para Servicios al Ciudadano.

Reportes

La aplicación cuenta con un Portal Web el cual permite a los usuarios generar, visualizar y exportar reportes detallados sobre las actividades de validación de identidad (consumos), proporcionando una visión clara y estructurada de los datos recogidos por el sistema.

Requisitos

En esta sección se especifican los requerimientos técnicos de la solución:

- Permitir la conectividad por internet usando el protocolo de comunicación para los ambientes de Pruebas y Producción.
- Cumplir a cabalidad con la resolución 5633 de 2016 de la RNEC y sus Anexos técnicos en su versión más reciente.
- El procedimiento de Descifrado de minucias es compatible con captores Morpho MSO 1300 E3 y Suprema Biomini Slim S, en caso de ser distinto se debe documentar el requerimiento y aplicar el procedimiento descrito en el Capítulo 2.4.
- Los aplicativos de captura de huella Cumplen a cabalidad con la Resolución 5633 de 2016 de la RNEC y sus anexos técnicos, en los ítems relacionados con estaciones fijas.

HClient:

- Los equipos de cómputo en los cuales se va a instalar el HClient deben contar con sistema operativo Windows 7 o superior.
- Conectividad en la comunicación entre el HClient y el servicio web CertiHuella.
- Únicamente al momento de la instalación, permisos de administrador en el sistema operativo para el HClient.
- Cumplir a cabalidad con la Resolución 5633 de 2016 de la RNEC y sus anexos técnicos.
- Los equipos de cómputo desde los cuales se realizarán las transacciones deben contar con las actualizaciones de seguridad necesarias para operar en condiciones seguras, de manera que los reportes de seguridad del fabricante se encuentran cubiertos en su totalidad.
- Contar con un procedimiento para permitir el soporte técnico remoto.

CertiHuella de Escritorio:

- Los equipos de cómputo en los cuales se va a instalar el CertiHuella De Escritorio deben contar con sistema operativo Windows 7 o superior.
- Conectividad en la comunicación entre el CertiHuella de Escritorio y el servicio web CertiHuella.
- Permisos de administrador al momento de la instalación para el CertiHuella de Escritorio.
- Cumplir a cabalidad con la resolución 5633 de 2016 de la RNEC y sus anexos técnicos.
- Los equipos de cómputo desde los cuales se realizan las transacciones deben contar con las actualizaciones de seguridad necesarias para operar en condiciones seguras, de manera que los reportes de seguridad del fabricante se encuentran cubiertos en su totalidad.
- Contar con un procedimiento para permitir el soporte técnico remoto.

Requisitos

Actualizador de CRL:

El componente Actualizador de la CRL es compatible con los siguientes sistemas operativos:

- Microsoft Windows 2010
- Microsoft Windows 2011
- Cualquier distribución de Linux

WS-SIGN:

El WS-Sign es un componente Java que estará desplegado en la infraestructura tecnológica del CLIENTE, teniendo en cuenta el siguiente esquema de trabajo:

1. Un servidor de aplicaciones GlassFish 7, Weblogic 14c.
2. Motor de bases de datos SQL Server, Oracle o MySQL.
3. Servidor con al menos las siguientes características:
 - Mínimo 1 GB de espacio libre en disco para la instalación del servidor de aplicaciones y el aplicativo.
 - Mínimo 8 GB de memoria RAM.
 - Procesador 3.2 GHz de dos núcleos.
 - Espacio en disco para el almacenamiento de los documentos PDF a ser conservados. La capacidad requerida dependerá directamente del volumen de documentos a almacenar y el tamaño de los mismos.
4. Certicámara asesorará al equipo técnico del banco en la instalación y configuración del componente.

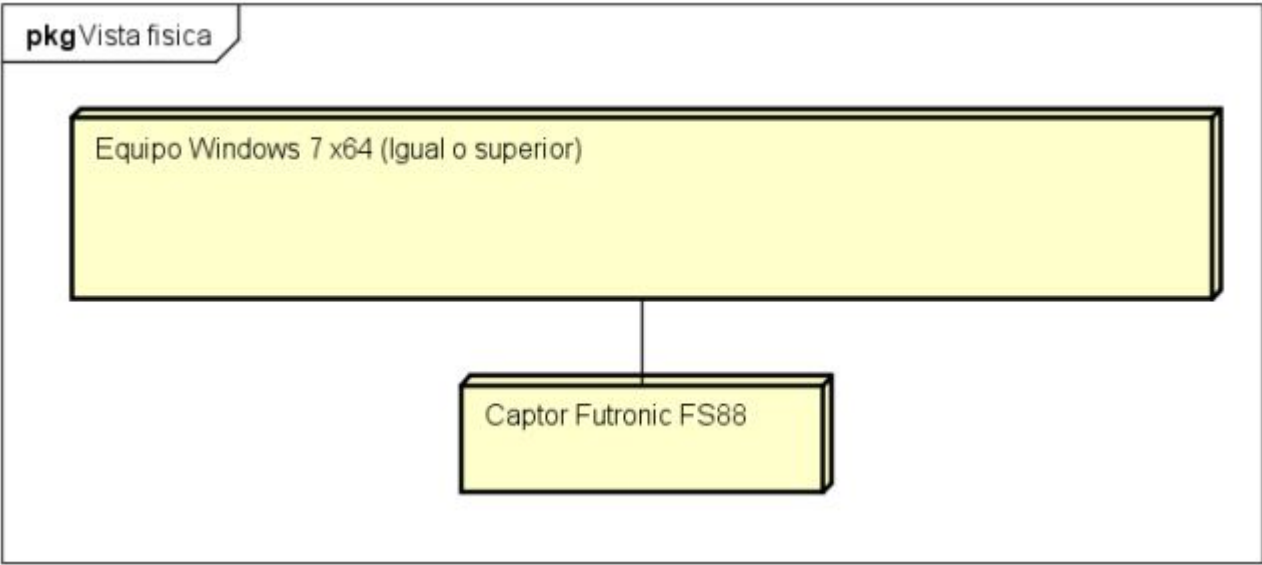
Arquitectura

CertiHuella es un aplicativo orientado a verificar la identidad de las personas. A continuación, se realizará la presentación de las vistas de arquitectura más relevantes de la solución, siguiendo el marco de trabajo 4+1 de Philippe Kruchten (1).

Vista Física:

En esta vista se presentan los componentes de hardware que hacen parte de la solución CertiHuella. Por cada componente se describen las características o restricciones, y la interacción con otros componentes de hardware. Con el objetivo de simplificar esta vista, no se incluyen los servicios CertiHuella de Certicámara, cuya infraestructura física es compleja, y se ven como componentes cerrados.

A continuación, se presenta la vista física de la aplicación CertiHuella que se ejecuta sobre máquinas de escritorio.



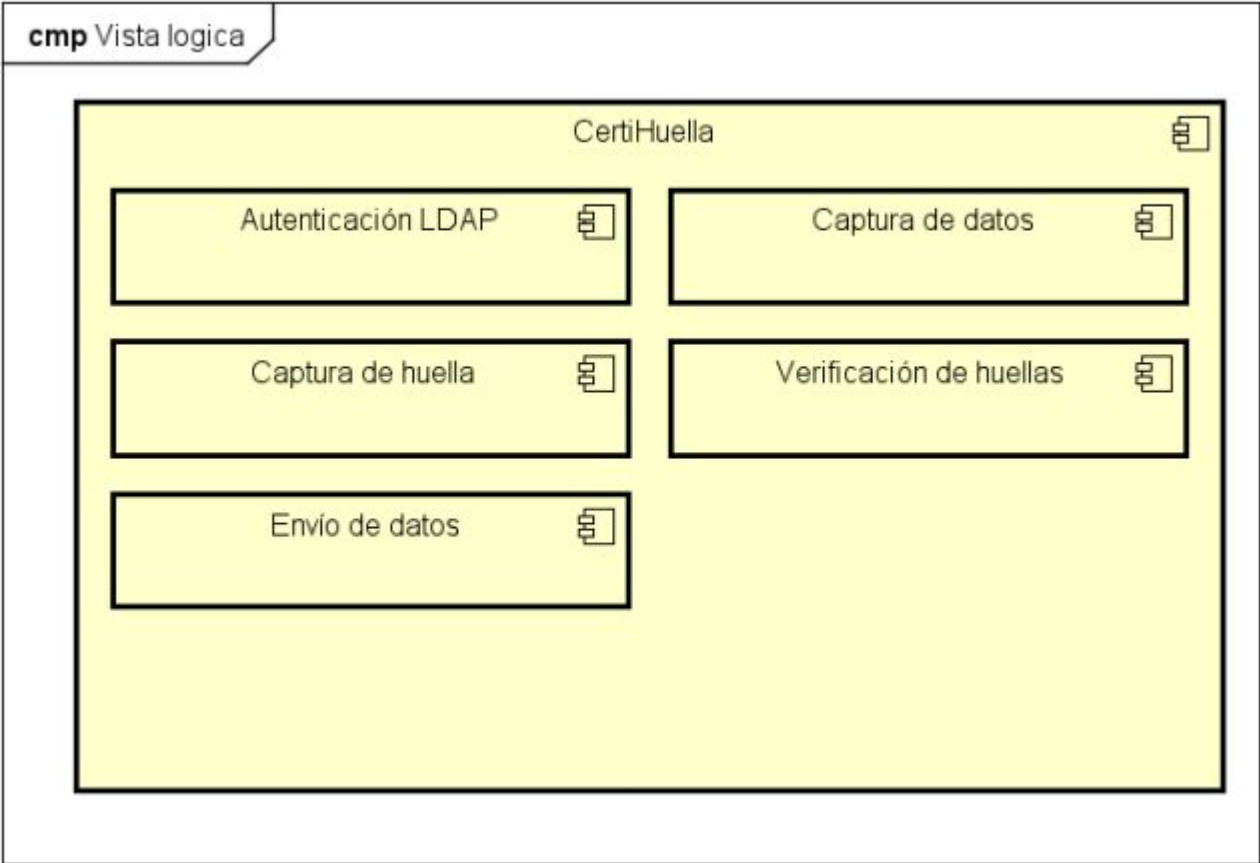
Los componentes de esta vista son:

- Equipo Windows 7 x64(Igual o superior): Se requiere un equipo de escritorio o portátil que cuente con sistema operativo Windows 7 de 64 bits o superior el cual debe pertenecer al directorio activo de la organización, también debe tener conexión a los WS de CertiHuella.
- Captor de Huellas: Se requiere de un captor biométrico que cumpla con los criterios establecidos por la RNEC para la captura de las huellas.

Arquitectura

Vista de lógica:

En esta vista se presentan los principales componentes que hacen parte de la aplicación CertiHuella y que contienen todas las funcionalidades requeridas para la solución.



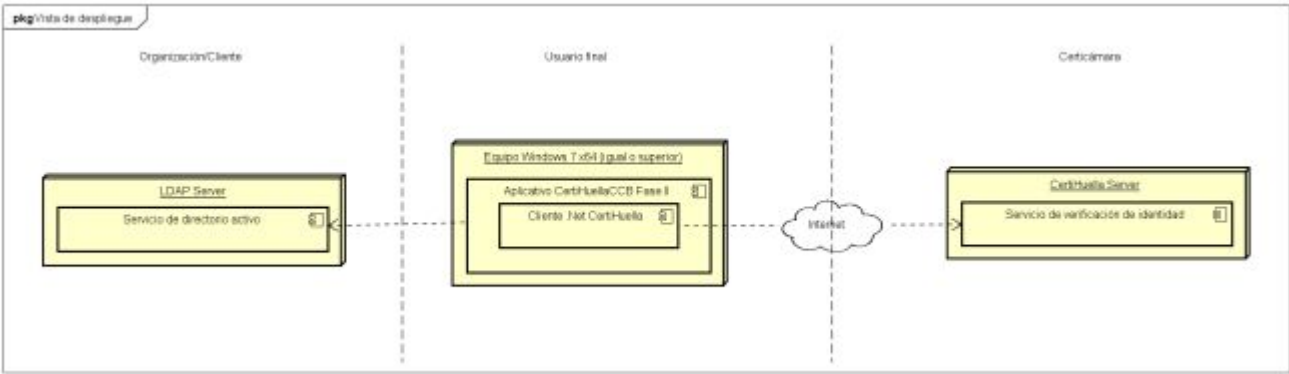
Los componentes de esta vista son:

- Autenticación LDAP: Este componente se encarga de realizar la autenticación de la aplicación contra el directorio activo de la organización.
- Captura de datos: Este componente se encarga de capturar los datos necesarios de la persona en el proceso de verificación de identidad.
- Captura de huella: Este componente se encarga de realizar la captura de la huella de uno de los dedos de la persona a través de dispositivo captor biométrico suministrado.
- Verificación de huellas: Este componente se encarga de solicitar a la RNEC una huella con un número de cédula y numero de dedo suministrados y compararla con la huella capturada, finalmente retorna el resultado de la comparación y los datos biográficos correspondientes al número de cédula con que se realizó la consulta.
- Envío de datos: Este componente se encarga de enviar a un servicio web expuesto por la organización los datos biográficos asociados al número de cédula suministrado y el resultado de la comparación de las huellas.

Arquitectura

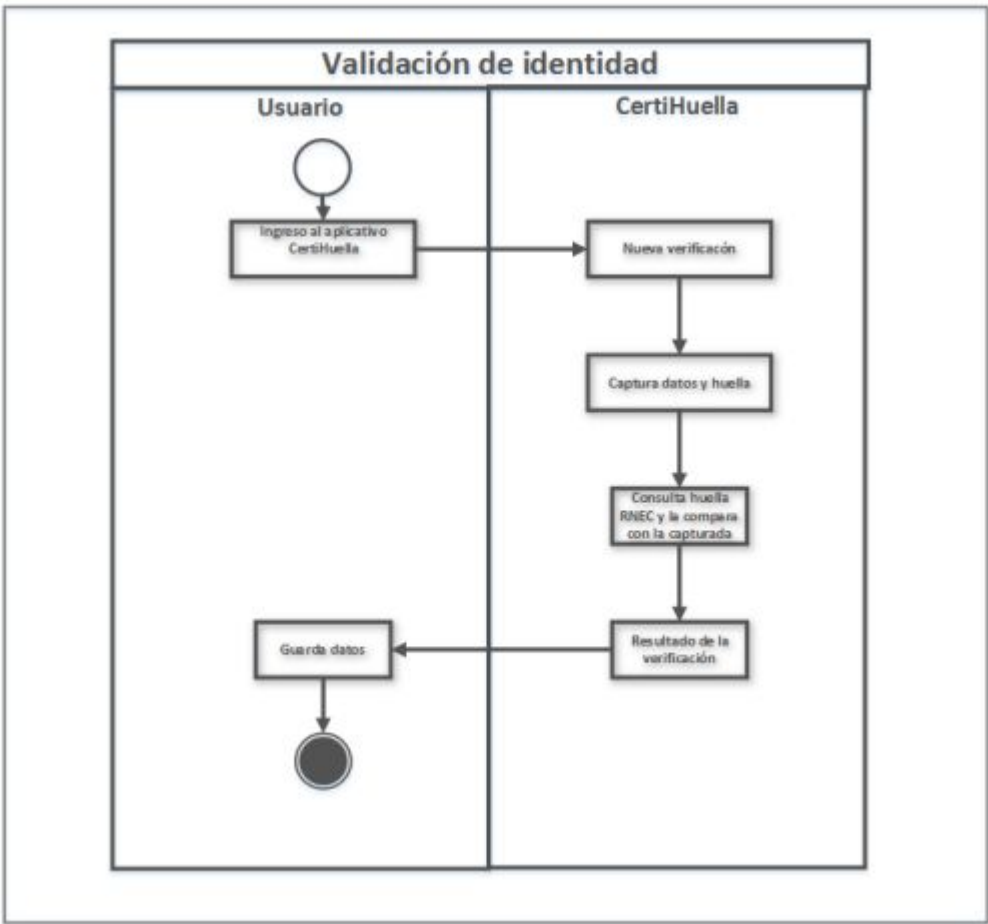
Vista de despliegue:

En esta vista se presenta la distribución de las maquinas requeridas y los servicios necesarios en cada una de estas para la operación de la aplicación en ambiente productivo.



Vista de procesos:

En esta vista se presenta el flujo de proceso realizado en la aplicación desde que el usuario ingresa hasta que obtiene el resultado de la verificación.



Tiempos de instalación e implementación

Al tratarse de un servicio web, este puede ser integrado de manera ágil a cualquier sistema y/o proceso.

- Implementación: 3 meses
- Instalación: 15 días

Nota: Si el tiempo de implementación se excede, existirá un cobro adicional de acuerdo con lo establecido a nivel comercial entre las partes. *(Si durante el tiempo de Implementación existe algún tipo corrección o modificación del producto o servicio que amplíe los tiempos de implementación establecidos desde Certicámara, no se incurrirá en cobros adicionales.)*

Entregables

El entregable de la suscripción de CertiHuella consta de:

- URL de publicación del servicio web CertiHuella para ambiente de Pruebas y Producción.
- Credenciales de acceso para ambiente de Pruebas y Producción.
- Certificado digital de persona jurídica.
- Instalador del aplicativo CertiHuella de Escritorio / HClient, manual de instalación y desinstalación y manual de usuario.

Para el WS-Sign:

- Instalador
- Librerías dependientes
- Manual de instalación
- Manual de usuario
- Scripts para poblar la base de datos (configuraciones iniciales) en caso de usar WS-Sign.

Para Lambda de Firma

- Url del Servicio
- Credenciales de Autenticación
- Manual de usuario
- Ejemplo de Consumo