HIPER DERECHO

Tecnología como libertad

Análisis de la plataforma e infraestructura de Identidad Digital de RENIEC

Edgar Huaranga Junco

Análisis de la plataforma e infraestructura de Identidad Digital de RENIEC

Edgar Huaranga Junco

Hiperderecho

Asociación civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Fundada en el 2013, investiga e interviene en debates de políticas públicas sobre libertad de expresión, derechos de autor, privacidad, ciberseguridad y delitos informáticos.

Análisis de la plataforma e infraestructura de Identidad Digital del Registro Nacional de Identificación y Estado Civil RENIEC
https://hiperderecho.org/publicaciones

Investigación:
Edgar Huaranga Junco

Foto de portada: Sharon McCutcheon para Unsplash

Lima, noviembre de 2020
Asociación Civil Hiperderecho
Av. Benavides 1944, oficina 901, Miraflores, Lima
hola@hiperderecho.org

Esta investigación ha sido financiada gracias al apoyo de Privacy International durante el 2020.

1. Resumen

La Identidad Digital puede ser entendida como el conjunto de información personal, pública o privada que existe en Internet sobre las personas. Sin embargo, en este informe utilizaremos como concepto el hecho de que la Identidad Digital es el conjunto de mecanismos utilizados para validar la identidad de una persona en un entorno digital.

En los últimos años, además de comercios (tiendas online, bancos y empresas de telecomunicaciones), fueron los gobiernos quienes le pusieron énfasis al tema de digitalización de procesos por su acercamiento a la ciudadanía. Sin embargo, el gran reto para lograr su objetivo y aprovechar el conjunto de ventajas que se han comprobado en otros países era necesario definir un sistema de reconocimiento de Identidad Digital.

RENIEC, siendo el organismo autónomo encargado de la identificación de los peruanos, se encargó del diseño, implementación y validación de los mecanismos tecnológicos para que los peruanos podamos hacer uso de diversos trámites y procesos provistos por el estado donde requiera una validación de nuestra identidad.

En el presente documento, se abordará las diversas maneras en las que RENIEC ha puesto en marcha la validación de identidad digital de los peruanos, mediante diversos canales y herramientas. Desde el uso de hardware, como el DNI-electrónico, hasta el uso exclusivo de software mediante reconocimiento facial.

2. Introducción

En el presente capítulo se presentan los motivos por el que se decidió realizar este informe y los objetivos que se desean alcanzar.

1.1. Motivación

Este proyecto busca entender el entorno de Identidad Digital desarrollado por RENIEC, además de localizar posibles brechas de seguridad acerca de la protección de datos personales en los servicios desarrollados por RENIEC y utilizados por instituciones públicas o privadas.

1.2. Estructura del informe

Para brindar al lector una idea global del contenido de este trabajo, a continuación se hace una breve descripción del propósito de cada capítulo presente en este documento.

- Introducción

  Este capítulo hace mención de las motivaciones que han conducido al estudio en este campo de la tecnología. Además de los objetivos y estructura del trabajo.

- La arquitectura de Identidad Digital

  En este capítulo se hace una descripción de la arquitectura sobre la que está basada el concepto de Identidad Digital desarrollado por RENIEC. Se describen las capas y el rol que cumplen dentro de esta arquitectura, detalles técnicos y observaciones según la documentación encontrada.

- PKI: El núcleo de la Identidad Digital

  Esta es la capa más baja en el entorno de Identidad Digital, es la fábrica de certificados digitales desarrollado por RENIEC en la que se basa todo el ecosistema de Identidad Digital. PKI que es la encargada de la generación y la gestión del ciclo de vida de los certificados digitales para las personas naturales y jurídicas.

- La capa de servicios: El punto de acceso a entidades públicas y privadas

  RENIEC pone a disposición de entidades públicas y privadas una capa de servicios de validación de identidad. En este capítulo se exponen las diferentes modalidades y requisitos para acceder a estos servicios.

- DNI electrónico

  En este capítulo se hace una revisión específica de la versión electrónica del DNI. Este documento es el token principal por el cual el RENIEC pretende promover la inclusión digital de todos los ciudadanos peruanos.

- Portales y apps

  Las iniciativas del gobierno para acercar servicios/procesos al ciudadano donde no requiere su presencia tienen como resultado múltiples páginas web y aplicativos móviles. En este capítulo se hace el estudio de estas soluciones.

- Conclusiones

  En este capítulo se exponen las conclusiones recopiladas de la observación de todo el entorno de Identidad Digital, dudas y preocupaciones respecto al desarrollo de futuros desarrollos tecnológicos.

2. PKI – El origen de Identidad Digital

La implementación de una plataforma digital donde el ciudadano pueda interactuar con diversos organismos del estado y los servicios que estos proveen lleva consigo algunos requisitos para lograr un aceptable grado de confiabilidad. Algunos de estos requisitos incluyen seguridad y privacidad de la transacción, capacidad para identificar a quien hace y procesa la solicitud.Ante estas necesidades, un entorno PKI es el más adecuado y calza bien con las necesidades antes mencionadas.

2.1 ¿Qué es el PKI?

Es el conjunto de hardware, software, políticas y procedimientos necesarios para controlar el ciclo de vida de certificados digitales y claves públicas. Este ciclo de vida comprende creación, administración, distribución, almacenamiento y revocamiento.

La importancia de estos certificados digitales y claves públicas es que nos ayuda a establecer y permite validar la identidad de los entes involucrados en los servicios que provee un entorno digital. Estos entes pueden ser personas, organizaciones, dispositivos, servicios, etc. Otro punto importante es que el esquema de certificados y claves nos permite tener un control adecuado de acceso a datos y recursos de cada organización.

En este punto podemos decir que un certificado de estos podría funcionar como un documento de identificación en el espacio digital (Internet).

¿Qué es un certificado digital?

Es un documento digital/archivo/fichero que contiene un conjunto de datos utilizados para firmar y encriptar información. El Estado Peruano, en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), otorgó al RENIEC la facultad de emitir certificados digitales para personas naturales y jurídicas que lo soliciten.

Estos certificados digitales son credenciales electrónicas que permiten lo siguiente:

- Acreditar la identidad de sus suscriptores.
- Firmar digitalmente documentos electrónicos con la misma validez y eficacia jurídica que posee la firma manuscrita.
- Cifrar datos y comunicaciones electrónicas.

El rol de RENIEC en el PKI

Como se mencionó anteriormente, el RENIEC provee el servicio de emisión de certificados digitales a personas naturales y personas jurídicas, contribuyendo al desarrollo e implementación del gobierno electrónico y comercio electrónico con total seguridad, confianza y valor legal.

Desde agosto del 2016 todos los ciudadanos peruanos pueden contar con certificados digitales de persona natural al obtener el Documento Nacional de Identidad Electrónico (DNIe). Este DNIe similar al tradicional y que incorpora chip que almacena información como el certificado digital de forma segura que permite al ciudadano validar su identidad y firmar digitalmente documentos.

2.2. Tecnologías de respaldo

Encriptación es el proceso (procesamiento matemático) por el cual un mensaje es codificado (escondido/procesado) de tal manera que no puede ser leído/entendido por un intermediario del mensaje.

Encriptación simétrica

Es el tipo de encriptación más sencillo, en el cual el emisor y receptor del mensaje comparten una clave, que puede ser un número, una palabra, una cadena de palabras que sirve para codificar y decodificar el mensaje compartido.

Encriptación asimétrica

También conocido como encriptación de clave pública. Este tipo de encriptación utiliza dos claves para codificar los mensajes. Una clave en el par se puede compartir con todos; Se llama la clave pública. La otra clave en el par se mantiene en secreto. Se llama la clave privada. Cualquiera de las claves se puede usar para codificar un mensaje; la clave opuesta a la que se usa para cifrar el mensaje se usa para descifrar.

2.3 Clases y Jerarquías en la arquitectura PKI

La forma en la que RENIEC sigue las reglas de unas jerarquías y clases definidas entre los años 2017 y 2018. Este flujo de los certificados digitales involucra entes como la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) y las Entidades de Certificación para el Estado Peruano (ECEP).

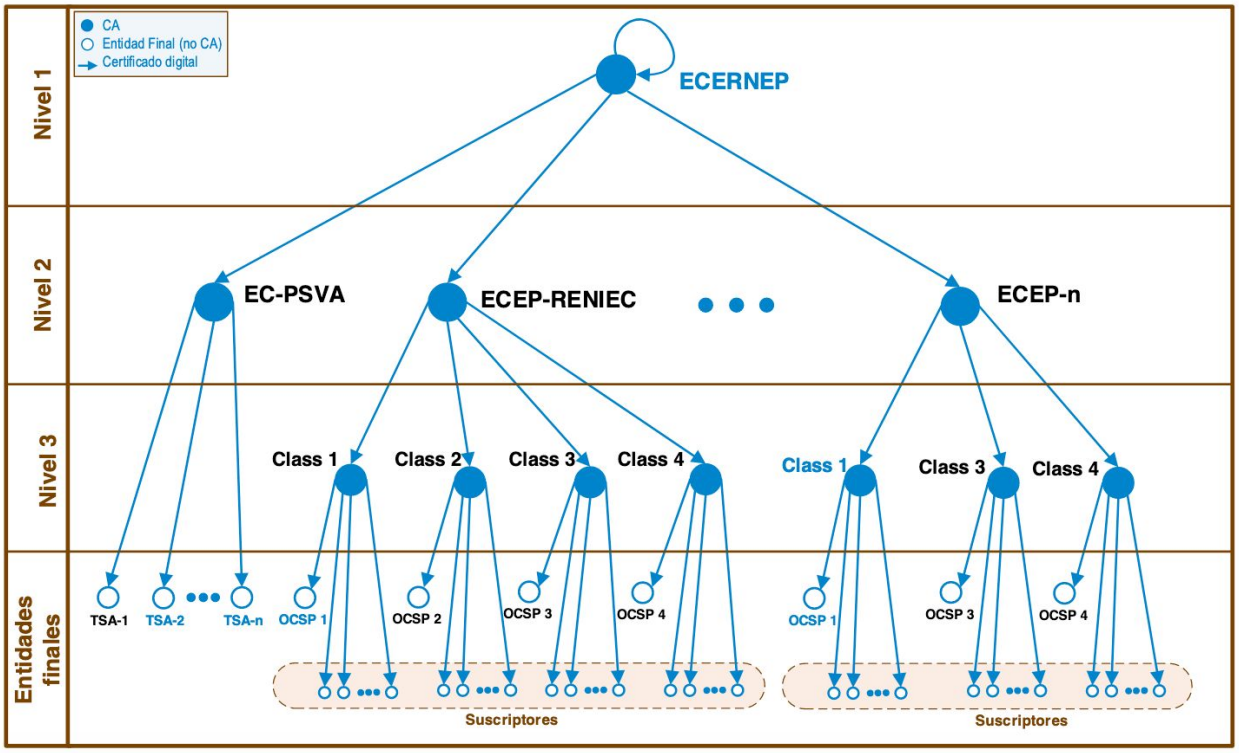

FIGURA 2.1: Jerarquía de emisión de Certificados Digitales -RENIEC

Los ECENERP son los encargados de emitir certificados raíz a los ECEP, estos últimos son los responsables de proporcionar, emitir y cancelar certificados digitales a personas naturales o jurídicas.

Los certificados entregados en el nivel 3 de la jerarquía están categorizados por clases, la descripción de cada una de estas es la siguiente:

Clase	Descripción
Class 1	Certificados digitales para uso específico
Class 2	Certificados digitales para Ciudadanos(contenidos en el DNI electrónico)
Class 3	Certificados digitales para Trabajadores dela Administración Pública
Class 4	Certificados digitales para Sistemas de Información

CUADRO 2.1: Clases de certificados digitales de nivel 3 - RENIEC

2.4. Resumen

Para una implementación acorde a las tecnologías actuales, se decide implementar un PKI donde sea el RENIEC la institución responsable de la generación y manejo del ciclo de vida de los certificados digitales. Estos certificados vienen a ser las credenciales en el entorno digital para cualquier persona natural o jurídica.

Esta es la base de todo el entorno de Identidad Digital, pues a partir de esto se pueden contruir servicios y herramientas para el ciudadano.

3. La capa de servicios

En el capítulo anterior se pudo ver la base sobre la que se construye el concepto de identidad digital. Estos certificados, en conjunto con la información que el RENIEC posee, les permite construir un objeto/identidad de cada uno de los ciudadanos.

Uno de los objetivos de implementar una plataforma de Identidad Digital es que se pueda disponer para las personas un Gobierno Electrónico.

3.1 Gobierno electrónico

Un gobierno electrónico puede ser definido como "la provisión de información y servicios gubernamentales y la apertura de canales adicionales para la participación política, transparencia y responsabilidad por medio de tecnologías de la información y comunicación (TIC)". [1]

Según la interacción que se tenga entre los actores, se pueden definir diferentes tipos de gobierno electrónico.

- Gobierno - Gobierno:

  Destinado a facilitar la operaciones internas y entre instituciones gubernamentales.

- Gobierno - Empresa:

  Que consiste en brindar información dirigida específicamente a empresas.

- Gobierno - Ciudadano

[1] Yıldız, Mete, and Ayşegül Saylam. "E-government discourses: An inductive analysis." Government Information Quarterly 30, no. 2 (2013): 141-153. https://www.sciencedirect.com/science/article/abs/pii/S0740624X13000051

Abarca las iniciativas destinadas a favorecer servicios administrativos o de gobierno, información pública y nuevos canales de conexión a los ciudadanos.

- Gobierno - Empleados

  Iniciativas con el objetivo de prestar servicios o capacitar en el uso de las TIC a los empleados agentes, o funcionarios de la Administración Pública.

Desde un punto de vista del ciudadano, se buscan los siguientes beneficios:

- Reducción de tiempo y costos en servicios del Estado.
- Fortalece la transparencia con su gobierno y fomenta la participación ciudadana.

3.2 Niveles de información

El núcleo de los servicios que provee RENIEC es validar si una persona es quien dice ser haciendo uso de software y hardware dedicado para esa actividad. En tal sentido, provee servicios según el tipo de validación que la parte solicitante envía como parámetro.

Información	**Nivel I**	**Nivel II**	**Nivel III**
Número de DNI	X	X	X
Apellido paterno, materno y pre nombres	X	X	X
Lugar y fecha de nacimiento	X	X	X
Estatura Sexo Estado civil	X	X	X
Grado de instrucción	X	X	X
Fecha de emisión	X	X	X
Multas electorales	X	X	X
Datos del padre y de la madre		X	X
Foto		X	X
Dirección y lugar de domicilio		X	X
Fecha de inscripción			X

Firma			X

CUADRO 3.1: Niveles de información en la ficha RENIEC

Existen dos formas de acceder a la información antes mencionada, estas son:

- Consulta en línea vía Internet

  Donde haciendo uso de un usuario y contraseña o el DNI electrónico se realiza la consulta.

- Consulta en línea vía Línea dedicada

  El usuario accede a la información a través de una línea dedicada establecida entre éste y el RENIEC. En esta modalidad es necesario que el usuario posea un servidor y realice un desarrollo utilizando las APIS del RENIEC disponibles para diversos lenguajes de programación.[2]

Ambas consultas requieren la firma entre el RENIEC y la empresa/servicio mediante el convenio de suministro de información.

4. DNI electrónico

Como se explicó anteriormente, el DNI electrónico se usa como una versión de identificación digital. Esto es posible porque dentro de su composición almacena los certificados digitales emitidos por RENIEC por los cuales el ciudadano puede autenticarse y también firmar documentos con valor legal.

4.1. Composición

Es importante describir los componentes del DNI electrónico tanto del ladode hardware como el de software y la forma en la que estos interactúan con elentorno PKI implementado por el RENIEC.

Hardware

Se ha dividido la descripción de hardware en dos partes. Por un lado la tarjeta misma además de sus elementos de seguridad, y por el otro se describe el chip y sus especificaciones técnicas.

[2] Consultado de: https://cel.reniec.gob.pe/celweb/resources/img/Requisitos.pdf

La tarjeta

La tarjeta es una tarjeta constituida por cinco láminas de materialpolicarbonato, consistencia firme y dura resistente al calor y rayos ultravioleta.Además contiene elementos de seguridad incrustrados al momento de laimpresión, estos son descritos en la figura 4.1.

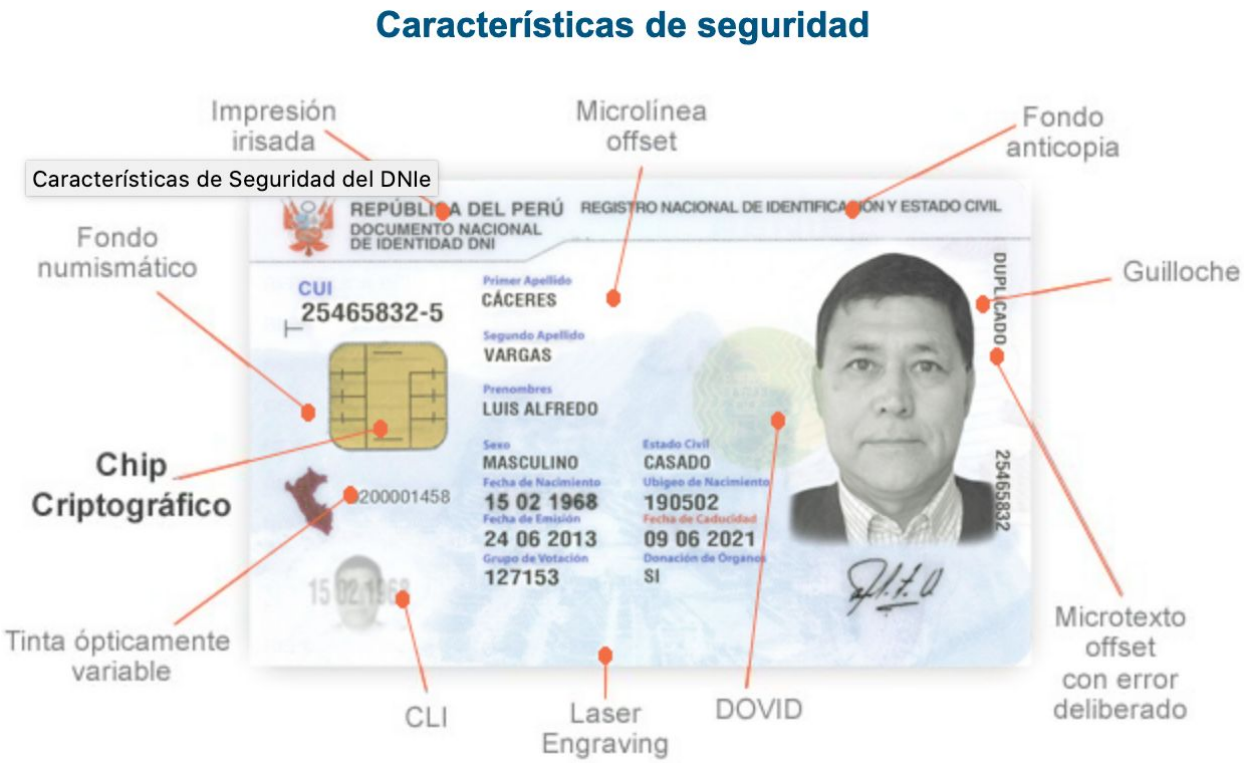

FIGURA 4.1: Elementos de seguridad del DNI electrónico

El chip

El chip adherido al DNI electrónico es un micro-procesador compuesto por lo siguiente:

- Unidad de Procesamiento de Tecnología C-MOS.
- Memoria ROM y RAM.
- Memoria EEPROM.
- Unidad de administración de memoria.
- Coprocesadores para ejecución de algoritmos criptográficos y generación de números aleatorios. \item Interfaz con contactos ISO/IEC 7816.

Software

El microprocesador presente en el chip ejecuta el sistema operativo ID-One-Cosmo-V7 provisto por la empresa Oberthur Technologies que implementa una especificación de Java Card. El diagrama lógico está descrito en la figura 4.2. Java Card ha sido un concepto que se adaptó muy bien para tarjetas inteligentes porque entre sus beneficios tenemos que puede ejecutar

diferentes *applets* que realizan una tarea específica. En el DNI electrónico tenemos por ejemplo el PKI para firma digital de documentos, verificación de identidad en sistemas ICAO , Match On Card (MOC) que permite una verificación biométrica de manera interna con la huella dactilar.

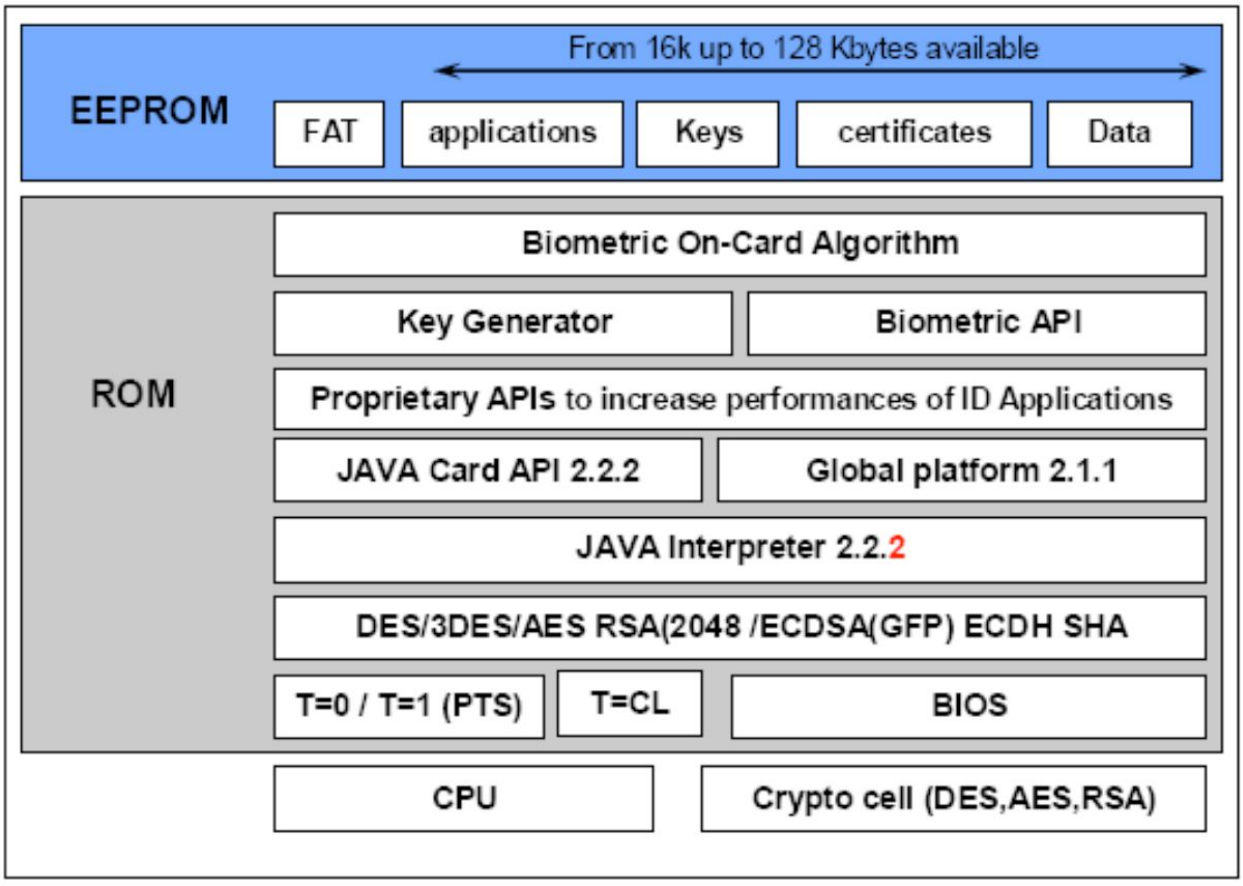

FIGURA 4.2: Diagrama lógico del chip en el DNI electrónico

Adicional a estas características se puede también mencionar lo siguiente:

- Tiene capacidad para gestión de encriptamiento RSA y firma digital.
- Seguridad a nivel estándares internacionales Common Criteria EAL4+ ó FIPS 140-2.
- Basic Access Control (BAC), para cuando agentes externos quieran manipular el chip.
- Active Authentication (AA), clave RSA de 1024 bits que garantiza la autenticidad del chip e impide su clonación.

4.2 Applets

Los applets permiten agregar funcionalidades al DNI electrónico según necesidad y requerimiento. Sin embargo, los applets por defecto que vienen instalados con la emisión del DNI-e son los siguientes

PKI

Comprende los métodos criptográficos aceptados en la Infraestructura PKI para el manejo de los certificados digitales, realización de la firma y la autenticación digital y generación, custodia y acceso a las claves secretas almacenadas.

Las tareas ejecutables por el applet PKI son las siguientes:

1. Genera y maneja claves de cifrado asimétrico RSA de hasta 2048 bits, y ejecuta el cifrado y el descifrado correspondientes.

2. Genera y maneja claves de cifrado simétrico DES de 64 bits, 2DES de 128 bits, 3DES de 192 bits, y AES de hasta 256 bits, y ejecuta el cifrado y el descifrado correspondientes.

3. Ejecuta funciones criptográficas de resumen en algoritmos de Hash Seguro SHA-160, SHA-256, SHA-384, SHA-512, aplicadas a procedimientos de autenticación digital.

4. Tiene almacenadas cuatro claves simétricas 2DES de 128 bits, a ser operadas por aplicaciones externas en la lectura o escritura de datos del ciudadano bajo cuatro estructuras implementadas.

5. Tiene almacenadas dos claves RSA privadas de 2048 bits, asignadas a sendos certificados digitales aplicados en la Autenticación o la Firma digital. Cada una de estas claves tiene asociado un número de identificación personal PIN, que al ser ingresado por el ciudadano, invoca la realización de la autenticación o de la firma digital, según corresponda.

6. Almacena los certificados digitales para autenticación y para firma digital, además de los certificados de la cadena de confianza que corresponden a las entidades de certificación intermedia y raíz.

7. Implementa contadores de intentos erróneos para el ingreso de los números personales de identificación PIN, asociados a la realización de la autenticación o la firma digital. Al completarse tres intentos erróneos consecutivos, el acceso al uso del PIN queda bloqueado y sólo puede ser recuperado con intervención del RENIEC.

8. Almacena las plantillas biométricas de dos huellas dactilares del ciudadano, para ser usadas como credencial para la generación y activación o desbloqueo del número PIN a manera de un PUK (PIN Unblock Key).Con intervención del RENIEC, tales plantillas son cotejadas con la plantilla biométrica capturada de la huella dactilar del ciudadano, arrojando el resultado sobre su reconocimiento. De ser positivo, procede la activación del número PIN para el ciudadano,y en caso de ser negativo no es posible activar el PIN.

9. Para aquellos ciudadanos que RENIEC considere no elegibles para verificación biométrica dactilar, la aplicación PKI provee la asignación de un código clave personal de desbloqueo PUK, el que cumpleuna función similar al posibilitar la generación y activación del número PIN cuando su valor es invocado por el ciudadano en las instalaciones del RENIEC.

10. El applet PKI se adhiere al estándar ISO/IEC 7816, en sus partes:

    - Parte 4.-Estructura de comandos APDU.
    - Parte 5.-Asignación de números de identificación de aplicaciones.
    - Parte 6.-Definición de propiedades de los elementos de datos usados para intercambio de aplicaciones.
    - Parte 8.-Especificación de comandos para operaciones de seguridad.
    - Parte 9.-Comandos para la administración de la tarjeta y sus archivos.
    - Parte 15.-Aplicación de Información Criptográfica.

11. Implementa cuatro estructuras de datos destinadas al almacenamiento de información del ciudadano. El applet PKI provee acceso a lectura, modificación o escritura en las mismas mediante procedimientos con claves simétricas.Las estructuras pueden utilizarse para almacenar, por ejemplo:

    - Datos de identidad del ciudadano, conforme lo hace ya el RENIEC en la denominada Aplicación Básica de Identidad, ABI.
    - Constancias de votación para procesos electorales.
    - Subvenciones percibidas en programas sociales.-Datos de salud en lo referido a emergencias, vacunas y transfusiones.

Identificación ICAO

Esta característica permite que el DNI electrónico actúe como Electronic Machine Readable Travel Document (eMRTD). El DNI electrónico almacena información en grupos descritos en la tabla 4.1

Grupo de datos tipo 1	Grupo de datos tipo 2	Grupo de datos tipo 7
● Tipo de Documento. ● País o Entidad Emisora. ● Nombre del titular y	● Codificación de la imagen del rostro del ciudadano en formato JPEG2000.	● Codificación de la imagen de la firma manuscrita o rúbrica del ciudadano, en

nacionalidad. ● Número del documento con dígito de control. ● Fecha de nacimiento con dígito de control. ● Sexo. ● Fecha de expiración con dígito de control. ● Dígito de control compuesto.		formato JPEG2000.

CUADRO 4.1: Grupos de datos para acceso en el DNI electrónico parte del applet ICAO

Match on Card

El DNIe incorpora la tecnología de verificación biométrica de huellas dactilares mediante procesamiento en el mismo chip. Las funcionalidades para esta aplicación dependen fundamentalmente de tres componentes cuales son el motor biométrico, el API biométrico y un applet biométrico. No obstante, el acceso a las mismas se hace a través del applet PKI para lo cual debe seleccionarse previamente.

5. Portales y Apps

Según lo descrito en el Capítulo 3 acerca del gobierno electrónico y sus bondades de transparencia de cara al ciudadano, el estado peruano ha desarrollado herramientas para agilizar trámites a través de medios digitales.

Es importante notar que a pesar que muchas herramientas requieren el DNI electrónico como componente de autenticación, últimamente se está apostando por tecnologías de reconocimiento facial a través de aplicativos móviles.

5.1 Portales del Gobierno

Diversas instituciones deciden poner a disposición del ciudadano herramientas para agilizar trámites o consultar información.

Portal del ciudadano

Usuarios: Ciudadanos usuarios de DNI electrónico.

Institución: RENIEC

URL: https://serviciosportal.reniec.gob.pe/portalciudadano/

Servicios:

- Consultar ficha RENIEC.
- Saber quién consultó sus datos RENIEC.
- Saber quién usa su dirección y qué empresas han consultado sus datos.
- Actualizar los datos del DNI electrónico o del DNI de su hijo.
- Inscribir el nacimiento de tu hijo o solicitar duplicado de su DNI.
- Trámite de inscripción de nacimiento de hijo.
- Trámite de inscripción de defunción.
- Obtener copia certificada de nacimiento, matrimonio o defunción.
- Tramitar el duplicado del DNI de sus hijos.
- Solicitar constancias, documentos archivados, impugnaciones, devoluciones.
- Acceso a información pública.
- Solicitar la devolución de tasas pagadas y no utilizadas.

Consultas en línea

Usuarios: Notarios Públicos, las Entidades Públicas,las Personas Jurídicas de Derecho Privado Constituidas en el Perú y que desarrollen actividades en el territorio nacional.

Institución: RENIEC

URL: https://cel.reniec.gob.pe/celwe

Sistema de Acta de Celebración Electrónica de Matrimonio en Municipalidad

Usuarios: Municipalidades.

Institución: RENIEC

URL: https://actacelebracion.reniec.gob.pe/actacelebracion/

Domicilio electrónico

Usuarios: Usuarios del DNI electrónico.

Institución: RENIEC

URL: https://midomicilio.reniec.gob.pe/e-domicilioc

Plataforma Integrada de la Entidad de Registro

Usuarios: Entidades Públicas que firmaron Contrato de Prestación de Servicios de Certificación.

Institución: RENIEC

URL: https://erep.reniec.gob.pe/pier/login.jsf

Plataforma de autenticación Nacional

Usuarios: Usuarios e-Pan.

Institución: RENIEC

URL: https://idperu.reniec.gob.pe/site/

Declaración jurada de intereses

Usuarios: Funcionarios públicos

Institución: Presidencia del Consejo de Ministros

URL: https://dji.pide.gob.pe

SIAF - Acreditación Electrónica de Responsables de Cuentas

Usuarios: Responsables de cuentas en Instituciones Públicas

Institución: Ministerio de Economía y Finanzas

URL: https://apps4.mineco.gob.pe/siafregrespjws/

Sistema integrado de Empadronamiento Electrónico SIEE

Usuarios: Alcaldes Provinciales y Distritales a nivel nacional

Institución: Ministerio de Inclusión Social

URL: http://operaciones.midis.gob.pe/siee/login

Intranet del Becario

Usuarios: Becarios del Programa Beca 18

Institución: PRONABEC

URL: https://intranet.beca18.gob.pe/

Autorización de Usuario de empresa para los sistemas del MTC

Usuarios: Empresas usuarias del MTC

Institución: Ministerio de Transportes y Comunicaciones

URL: https://sso.mtc.gob.pe/MTC.STS/

Autorización de Usuario de empresa para los sistemas de Provias Nacional

Usuarios: Empresas Provias

Institución: Provias Nacional

URL: http://identidades.proviasnac.gob.pe/Provias.STS/

Sede digital de la SMV

Usuarios: Usuarios administrados por SMV

Institución: Superintendencia de Mercado de Valores

URL: http://supervisionq.smv.gob.pe/mvnetF/Autenticacion/frmInicio.aspx

Sistema de intermediación Digital de SUNARP

Usuarios: Notarios Públicos

Institución: Superintendencia de Nacional de Registros Públicos

URL: https://sid.sunarp.gob.pe/sid/login.htm?method=validarCert

5.2 Identidad Digital - versión móvil

El lanzamiento de las plataformas de acceso a la información de los ciudadanos hace que se propongan métodos para ampliar los canales donde se pueda atender estos servicios y soluciones. Un canal muy importante hoy en día son los aplicativos móviles.

A pesar de que existieron comunicados de prensa acerca del lanzamiento del DNI móvil, este aún no está disponible. De cara al ciudadano lo que sí existe son aplicativos que forman una parte de algunos procesos.

RENIEC Móvil Facial

Es una aplicación que autentica al usuario mediante biometría facial. Esta aplicación permite gestionar cambios en el DNI, consultar el estado de estos y tiene información de otros trámites.

FIGURA 5.1: Ficha en Play Store de RENIEC Móvil Facial

RENIEC Bio Facial

A pesar de estar con una cuenta de desarrollador distinta a la anterior. Esta aplicación también hace verificación biométrica a manera de autenticación. Esta aplicación se hace mención en el portal del ciudadano como parte del proceso de actualizar la foto presente en el DNI o el DNI electrónico.

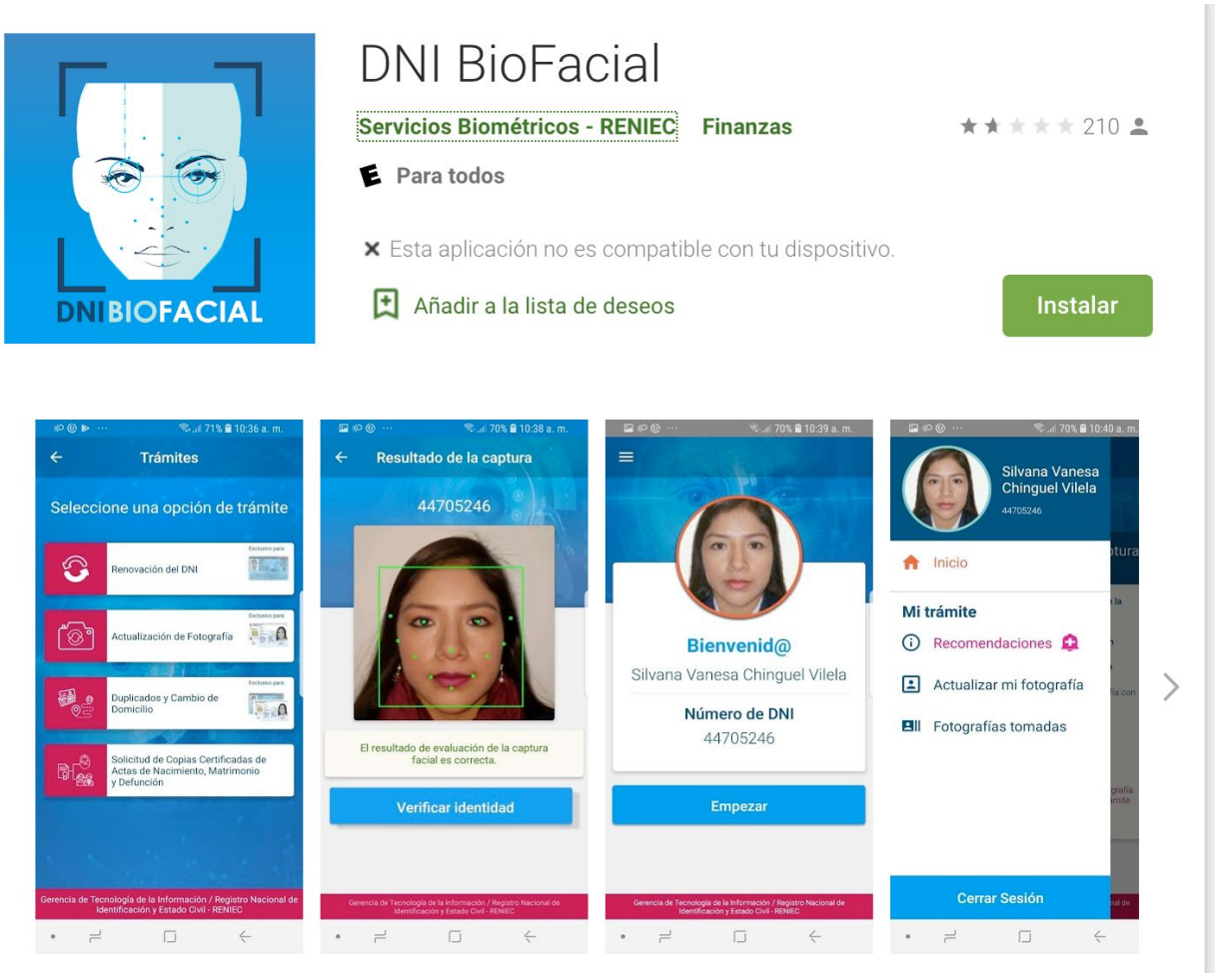

FIGURA 5.2: Ficha en Play Store de DNI BioFacial

ID Perú

ID Perú es una aplicación que hace verificación de identidad mediante lectura de las huellas dactilares. Aún se encuentra en desarrollo y es incierta la manera en que esta interactúa con alguna otra plataforma que no sea la Plataforma de Autenticación Nacional.

Identidad Digital Móvil

Es una aplicación donde puedes gestionar tus certificados digitales. Sin embargo aún no está en fase de publicación, a la fecha del informe se encuentra en fase beta/cerrada.

5.3 El problema de seguridad con aplicativos Android

Por el momento, todas las aplicaciones lanzadas por el RENIEC están siendo desarrolladas únicamente para la plataforma Android. El principal inconveniente de seguridad con estos aplicativos es el proceso llamado decompilación del APK. APK no es más que un archivo que permite instalar una aplicación en un teléfono con sistema operativo Android. El APK puede decompilarse y esto nos permite acercarnos en cierto nivel al código fuente original del aplicativo.

DNI BioFacial

Si bien es cierto Google no pone a disposición el APK para la instalación, es posible a través de páginas espejo tener acceso a estos archivos y analizar el código luego del proceso de decompilación.

Al analizar la aplicación DNI BioFacial, se pudo encontrar lo siguiente:

- Se hace uso de paquetes externos para mejorar la interfaz gráfica.
- Se hace uso de la herramienta de Firebase Face Recognition. No está claro si lo hacen desde el servicio cloud o de manera local en el dispositivo.
- Dentro del código decompilado existen credenciales y endpoints de web services activas.

6. Conclusiones

El concepto de Identidad Digital desarrollado por el RENIEC se ha ido adaptando según las necesidades recogidas en las distintas secciones del gobierno que tienen mayor interacción con el ciudadano. Sin embargo, esto también conlleva que en cierto punto la implementación de cierto módulo sea obsoleto y requiere de componentes particulares para su uso. Un claro ejemplo es el portal del ciudadano, el cual únicamente funciona para computadoras con el sistema operativo Windows y es necesario un lector de tarjetas inteligente.

Un enfoque, el cual no hace necesario el uso de un DNI electrónico, es donde se aprovecha el concepto de biometría. Esto se ve reflejado en las aplicaciones puestas a disposición por el RENIEC. A pesar de existir protocolos y que se tomen medidas improvisadas de seguridad, una aplicación como RENIEC Móvil Facial se presta como herramienta fundamental para intentos de robo de identidad en línea.

Otra propuesta es la plataforma Nacional de Autenticación, la que en primera instancia hace una validación biométrica con las huellas dactilares, y posteriormente el ciudadano debe crear una clave única para acceder a la plataforma. Esta plataforma no solo permite a instituciones del estado crear aplicaciones sino también para cualquier persona que quiera tener como método de acceso su Usuario Nacional en su página web o negocio.