Requisitos de experiencia (OBLIGATORIOS)

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Buenos Aires, 11 de junio del 2024

A quien pueda interesar,

Esta carta se entrega a solicitud de nuestro proveedor Magallanes Media S.A., quien ha cumplido y está cumpliendo satisfactoriamente con sus obligaciones contractuales con nosotros como proveedores de la tecnología utilizada para emitir la cedula nacional de identidad móvil denominada Smart DNI, que se aloja en la aplicación gubernamental argentina llamada "Mi Argentina" (Orden de Compra Nro. 78-0013-OCA23). Aplicación disponible en Android y iOS.

Por la presente, certificamos que los productos y servicios entregados por Magallanes Media S.A. se han entregado en buen estado, de forma completa, y en tiempo y forma. Los componentes entregados son los siguientes:

- Sistema de emisión de las credenciales
- Gateway
- SDK móvil Android & IOS

CONSORCIO IDSECURE IDS Santo Domingo, R.N.

Además, declaramos que Magallanes Media S.A. está al corriente con sus pagos y no se encuentra en ninguna la lista negra ni inhabilitados para participar en ninguna licitación dentro del país. También confirmamos y certificamos que los componentes suministrados por Magallanes Media S.A. cumplen totalmente con todas las normas ISO e ICAO, y que la solución además sigue los lineamientos establecidos en la norma ISO/IEC 18.013 parte 5.-

Proporcionamos a continuación algunos detalles del proyecto realizado por Magallanes Media S.A. para su referencia, pero le informamos que esta información es altamente confidencial y cualquier información adicional debe hacerse bajo NDA:

- Nombre del proyecto: Argentina Smart DNI
- Bienes suministrados y cantidad: 1.100.000 unidades cedulas de identidad móvil
- Plazo de entregas: Desde abril de 2024 hasta la fecha

Para la verificación de la información suministrada, o en caso de que necesiten detalles adicionales, puede contactarnos a través de los siguientes datos

Nombre de la entidad contratante: Registro Nacional de las Personas (RENAPER)

Persona de contacto: Flavio Brocca

Designación: director IT Dirección: Calle Tte. General Juan Domingo Perón N° 664, CABA, Argentina

Números de contacto: +54 911 3181-6963

Dirección de correo electrónico: fbrocca@mininterior.gob.ar

Attentamente

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2024-66285527-APN-DGTII#RENAPER

CIUDAD DE BUENOS AIRES
Martes 25 de Junio de 2024

Referencia: Certificación Renaper - 2023

El documento fue importado por el sistema GEDO con un total de 2 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.06.25 12:07:40 -03:00

Flavio Ramon Brocca
Director General
Dirección General de Tecnología e Innovación en Identidad
Dirección Nacional del Registro Nacional de las Personas

CONSORCIO ID SECURE ID S

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.06.25 12:07:41 -03:00

(/Default.aspx)

Viernes 29 de Diciembre, 17:23:26

Orden de Compra Abierta

Datos de la Orden de Compra Abierta

Número de la Orden de Compra Abierta:
78-0013-OCA23
Original
Orden de Compra Abierta
Descripción:
Orden de Compra Abierta generada por Proceso N° 78-0012-LPU23

Ejercicio:
2023
Fecha Autorización:
29/12/2023
Fecha Perfeccionamiento:
29/12/2023

Fecha Inicio:
29/12/2023
Fecha Finalización:
29/03/2025

Duración del Contrato:
15 Meses

CONSORCIO IDSECURE ID3 Santo Domingo, D.N.

Datos del Proceso de Compra

Número de Expediente:
EX-2023-73948483- -APN-DAYF#RENAPER
Número de Proceso de Compras:
78-0012-LPU23
Procedimiento de selección:
Licitacion Pública

Modalidad:
Orden de compra abierta
Encuadre Legal:
- Decreto Delegado N° 1023/2001 Art. 25
- Decreto N°1030/2016 Art. 25

Datos Comprador

Servicio Administrativo Financiero:
200 - Registro Nacional de las Personas
Unidad Ejecutora:
78/000 - División Compras
Oficina de Compra:
78/000 - División Compras

4393-0566 int. 2170/1
Fax:

Correo Electrónico:
compras@renaper.gov.ar

Datos del Proveedor Adjudicado

Razón social:
Magallanes Media SA
Número ente:
365661
CUIT:
30-71037547-6

Domicilio:
Magallanes 1315
Código postal:
1288
Localidad:
Ciudad Autónoma de Buenos Aires

Provincia:
Ciudad Autónoma de Buenos Aires
Teléfono:
43032305
Fax:

Correo Electrónico:
lisandro.carlomagno@ipesa.net

Detalle de la Orden de Compra Abierta

Número renglón	Número alternativa	Código ítem	Descripción	Cantidad	Unidad medida	Especificaciones de proveedor	Observaciones	Precio unitario	Moneda	Precio Total
1	1	3.5.9-5910.1	S. PROCESAMIENTO ARCHIVO; DESCRIPCION: PROCESAMIENTO DE ARCHIVOS	8.000.000,00	SERVICIO	Ver Detalle		1,02	Dolar Estadounidense	8.160.000,00

Total de la Orden de Compra Abierta: 8.160.000,00 USD

Documento de Clausulas Particulares

Documento	Número GDE	Número especial	Fecha vinculación	Opciones
Clausulas Particulares	PLIEG-2023-87481684-APN-DAYF#RENAPER		29/12/2023	⋮

Anexos ingresados

Nombre	Acciones
PET__IF-2023-87307551-APN-DGTII#RENAPER.pdf	🔍

Ejercicio	Objeto del gasto	Jurisdicción	Servicio	Apertura programática	Descripción Apertura Programática	Fuente Financiamiento	Ubicación Geográfica	Moneda	Monto
24	3.5.9.0	30	200	16.0.0.1.0	Emisión del Documento Nacional de Identidad	1.1	2	Dolar Estadounidense	5059710000
2025	3.5.9.0	30	200	16.0.0.1.0	Emisión del Documento Nacional de Identidad	1.1	2	Dolar Estadounidense	1686570000

Autorizadores

Nombre Autoridad	Cargo	Fecha Autorización
LAURA ELIZABETH SARAFOGLU	Director	29/12/2023

Volver

CONSORCIO IDSECURE IDS

Secretaría de Innovación Pública
Oficina Nacional de Contrataciones

PLIEGO DE ESPECIFICACIONES TÉCNICAS

A. OBJETO DE LA CONTRATACIÓN

El objeto de la contratación es la provisión de una solución integral interoperable de emisión y verificación de credenciales digitales móviles con tecnología QR (Quick Response code) y BLE (Bluetooth Low Energy) como medio de conexión entre los dispositivos contenedores de credenciales y verificadores de credenciales.

La contratación incluye la emisión de credenciales y la provisión de: SDK que será embebido y administrado por una APP de terceros; una API con tecnología REST que será invocada y administrada por el backend del RENAPER para generar las credenciales y se comunicará con el SDK para su descarga, revocación y/o actualización según corresponda; un DS que permitirá firmar los datos de la credencial que deberá estar conectado a la PKI del RENAPER. Estos componentes deberán ajustarse a lo solicitado en la presente especificación técnica, los cuales permitirán emitir los DNI desde el RENAPER hacia los dispositivos móviles de los ciudadanos.

Las soluciones propuestas deberán permitir la no dependencia tecnológica del proveedor y la adecuación a estándares internacionales en materia de credenciales de identificación contenidas en dispositivos móviles. Las credenciales que sean emitidas de acuerdo a este sistema serán denominadas con el nombre de DNI virtual del REGISTRO NACIONAL DE LAS PERSONAS, en reemplazo de la solución existente.

RENGLÓN	DETALLE	CANTIDAD	DESCRIPCIÓN	PLAZO DE ENTREGA
1	Credenciales digitales móviles (DNI Virtual).	OCHO MILLONES (8.000.000)	Solución integral interoperable de emisión y verificación de credenciales digitales móviles. La solución deberá proveer la emisión de credenciales contenidas en dispositivos móviles para la identificación y verificación de la identidad de ciudadanos. Conteniendo una REST API que pueda ser integrada a la plataforma del RENAPER, SDK para ser integrada al desarrollo de la APP, un DS para firmar los datos de las credenciales y el hardware asociado a la solución ofrecida. La provisión debe incluir el mantenimiento de la solución ofrecida.	QUINCE (15) MESES desde el perfeccionamiento de la Orden de Compra

B. ESPECIFICACIONES TÉCNICAS

En la figura 1 se describen los flujos de información para la emisión y la verificación de los DNI virtuales. Estos flujos contienen tanto las etapas a realizar por RENAPER así como las etapas a realizar por el proveedor y su vinculación. La emisión de las credenciales debe respetar el flujo de información descrito y ser interoperable permitiendo la no dependencia tecnológica del proveedor y la adecuación a estándares internacionales en materia de credenciales de identificación contenidas en dispositivos móviles. A su vez, la verificación debe respetar el flujo descrito para los casos online y offline por medio de canales de comunicación BLE, QR y NFC, siendo esta última opcional. La solución técnica del proveedor debe contener una REST API que pueda ser integrada a la plataforma del RENAPER, SDK para ser integrada al desarrollo de la APP y un DS para firmar los datos de las credenciales.

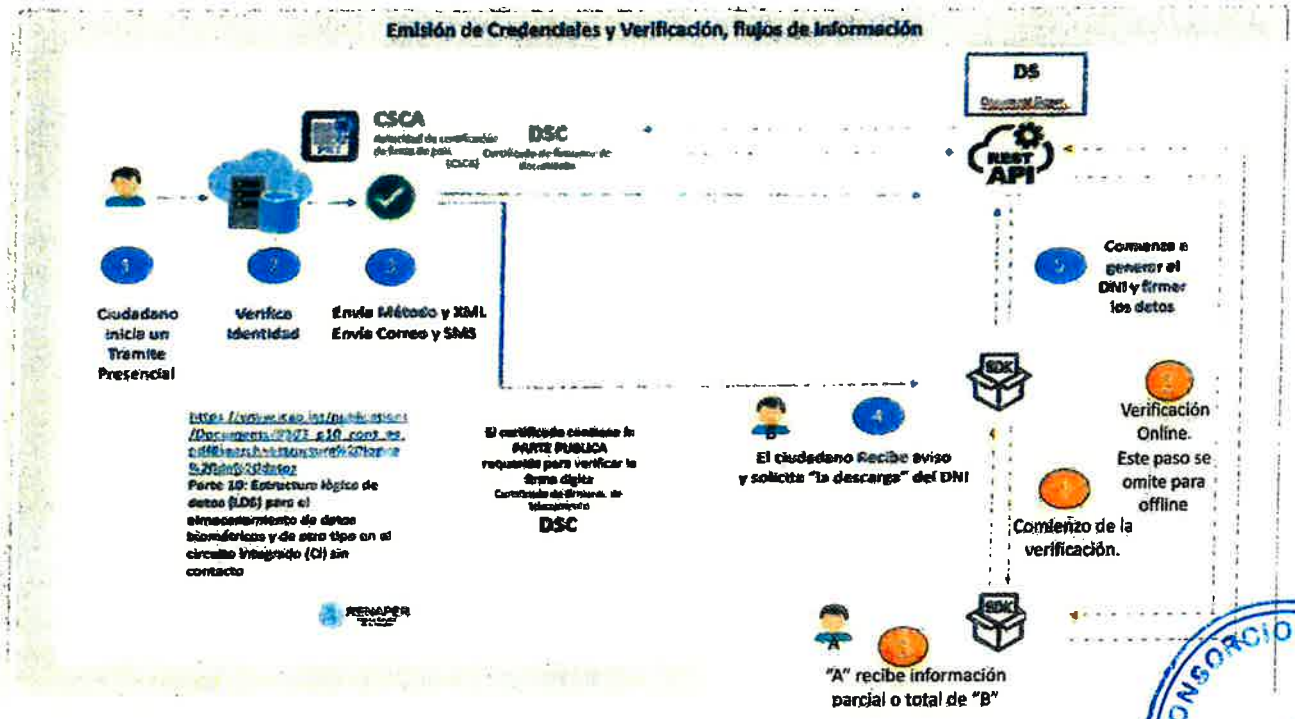

Figura 1. Flujo de Información

1. REQUERIMIENTOS

Los elementos a proporcionar por el proveedor, de acuerdo al flujo de información descrito, deberán cumplir con lo siguiente:

1.1. UNA (1) REST API, que pueda ser integrada a la plataforma del RENAPER que sea capaz de soportar las siguientes acciones:

a) Generar un nuevo DNI virtual, a partir de los datos enviados por RENAPER

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

b) Actualizar los datos del DNI virtual almacenado en la APP contenedora, ante un nuevo trámite que modifique cualquiera de ellos.

c) Revocar (eliminar) de la APP contenedora un DNI virtual.

d) Responder sobre el estado actual de un "trámite" o "trabajo" en cualquiera de las fases del ciclo de vida del DNI.

e) Garantizar conexiones seguras utilizando TLS 1.2 o superior, usando algoritmos criptográficos AES128 o superior, como capa de transporte entre:

- la plataforma del RENAPER y la API de emisión de DNI.
- la plataforma del API de emisión de DNI y el componente en la nube.
- el componente en la nube a la aplicación del ciudadano.

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

f) Garantizar la firma digital del DNI basada en la recomendación 9303 de OACI para documentos de viaje.

g) Generar un código QR que deberá incluir: nombre, apellido, numero de documento, sexo y foto en baja calidad para poder comparar con la imagen que se muestra en pantalla. El código QR vendrá ya firmado con la clave privada de Renaper usando criptografía, RSA (Rivest, Shamir y Adleman) . El código QR firmado será devuelto en formato base64. La clave privada será comunicada al integrador de la App para poder realizar los controles criptográficos necesarios y verificar que el código QR es firmado por RENAPER

La API REST será exclusivamente gestionada desde las instalaciones del RENAPER utilizando su plataforma de identificación de ciudadanos, ambos componentes deberán ser integrados de forma conjunta entre los equipos técnicos del RENAPER y los del adjudicatario.

La preparación de los datos, la firma de estos por el DS, el cifrado del DNI y el almacenamiento de la información necesaria para obtener la trazabilidad de los estados de las fases de emisión de DNI, deberán ser ejecutadas y mantenidas dentro de las instalaciones del centro de datos del RENAPER, con el objeto de mantener la privacidad de los datos de identidad y su historial de emisión.

Con el fin de evitar costos operacionales adicionales a RENAPER, el sistema debe tener un componente en la nube para la provisión del DNI en los dispositivos de los ciudadanos, en cuyo caso, los datos que transiten desde la API al SDK deberán estar debidamente encriptados y deberán ser eliminados al finalizar dicha descarga.

El proveedor deberá incluir la infraestructura asociada al componente de nube durante el plazo de contratación definido en el presente pliego. El componente nube debe ser administrado y operado por el proveedor.

El almacenamiento de datos deberá ser ejecutado y mantenido dentro de las instalaciones del centro de datos del RENAPER y la comunicación entre la API y la SDK deberán estar debidamente encriptados y deberán ser eliminados al finalizar dicha descarga.

1.2. SDK (del inglés Software Development Kit) que permita ser integrado a la APP contenedora y que contemple las siguientes funciones:

a) Ejecutar la descarga, actualización y revocación segura del DNI virtual desde la plataforma de emisión al dispositivo del ciudadano.

b) Permitir visualizar el DNI en Pantalla Completa, cambiando de anverso y reverso mediante el desplazamiento de los dedos sobre la credencial en caso de ser requerido.

c) Permitir visualizar la Información ampliada en formato de lista de datos con una imagen ampliada de la fotografía en caso de ser requerida.

d) La información del ciudadano a visualizarse debe ser la réplica exacta de los datos de identificación del Documento Nacional de Identidad en formato tarjeta. A su vez, RENAPER proporcionará la imagen a mostrarse en conjunto con los datos.

e) Con el objeto de avanzar en la interoperabilidad de las credenciales digitales (DNI virtual) presentes y futuras los oferentes deberán encontrarse en proceso o haber superado con éxito la evaluación de conformidad según el estándar ISO / IEC 18.013-5 y se valorará especialmente que la verificación electrónica del DNI de todos sus datos, o un subconjunto de ellos, en modos en línea (en inglés, online) o fuera de línea (en inglés, offline), estén alineados a lo establecido en la ISO/IEC 23.220 o DTC (Digital Travel Credentials) de ICAO. En caso de incompatibilidad entre algunas de las normas mencionadas debe prevalecer la DTC de ICAO.

f) Al momento que la ISO/IEC 23.220 - la cual aún se encuentra en desarrollo - sea publicada como estándar internacional, el adjudicatario deberá realizar los cambios necesarios para lograr adecuarse a ella. En caso de incompatibilidad entre la norma mencionada y DTC (Digital Travel Credentials) de ICAO debe prevalecer esta última.

g) Ofrecer los canales de comunicación encriptados QR (Quick Response code) y BLE (Bluetooth Low Energy) como tecnologías de apareamiento entre dispositivos y transferencia de datos, de manera opcional NFC (Near Field Communications); como medios de conexión entre el

dispositivo del ciudadano y el del verificador para ejecutar el proceso de verificación. Se valorará que este proceso no requiera contacto entre el dispositivo ciudadano - verificador.

h) Permitir mediante una acción deliberada del ciudadano prestar consentimiento al acceso de la totalidad de los datos o parte de ellos cuando sea requerido por un tercero.

i) Proteger el acceso al DNI virtual del ciudadano mediante un PIN que se genere a través del SDK en la primera inicialización con el fin de incrementar la seguridad.

j) El SDK debe permitir la verificación de la integridad de este antes de permitir la emisión del DNI virtual.

k) Proporcionar toda la seguridad necesaria para proteger las credenciales y garantizar que no se requiera experiencia específica en seguridad de software móvil para los desarrolladores de la aplicación.

l) El sistema debe ser compatible con la protección de código estático contra ingeniería inversa, como:

a. Ofuscación de nombre

b. Ofuscación de flujo de control

c. Ofuscación de código nativo

d. Ofuscación aritmética

e. Código de embalaje y encriptación

f. Ocultamiento de llamadas API

m) El sistema debe ser compatible con la protección de código dinámico como:

a. Detección de sabotaje

b. Detección de gancho

c. Detección de raíz (del inglés root)

d. Tener protección contra la inserción de malware

n) Seguridad propia de la aplicación contra la clonación de códigos y datos, la piratería, la manipulación y la extracción de claves. Ofrecer la posibilidad de usar el SDK por RENAPER y/o terceros autorizados para desarrollar la APP del DNI para el ciudadano.

o) Ofrecer la posibilidad de usar el SDK por RENAPER y/o terceros autorizados para desarrollar APPs de verificación para el total del DNI o una cantidad parcial de sus datos (Ej: Mayoría de edad).

p) Asegurar la encriptación punto a punto desde el subsistema de emisión de DNI con el objeto de garantizar el almacenamiento seguro en la App.

q) Permitir la visualización local de los datos de los DNI sin exponer la firma digital.

r) En caso de algún error en el momento de generación o visualización de la credencial se debe informar dicho error al usuario con un código identificatorio del mismo.

s) Permitir al ciudadano la descarga y uso del DNI digital de un tercero, sólo para el caso de menores a cargo. Posibilitando tener más de una credencial en un dispositivo móvil, solo para el caso de menores a cargo.

t) El SDK para la APP del ciudadano debe estar disponible para los sistemas operativos iOS y Android.

u) El SDK para la APP de verificación debe estar disponible para los sistemas operativos iOS y Android, de modo de tener una red de aceptación lo más amplia posible.

Se prevé la instalación de dos SDK si fuera necesario (uno para visualización y almacenamiento de credenciales y otro para verificación de credenciales). La implementación de la App que los administre estará en manos del equipo de desarrollo correspondiente y estará fuera de las responsabilidades de los adjudicatarios.

1.3. UN (1) DS (Document Signer)

Su objeto será firmar digitalmente el DNI, de acuerdo a lo establecido en la recomendación OACI 9303 ya que el DNI es un documento de viaje. Este DS debe estar ubicado en dependencias de RENAPER.

Esta capa de software deberá ejecutar las acciones necesarias para que la CSCA existente en RENAPER, utilizada para la generación de firmas en los chips de los pasaportes, certifique la validez de los datos a ser almacenados en el DNI virtual según el esquema determinado en la norma OACI mencionada.

El módulo DS (Firmante de Documentos) utilizará un Nivel 3 de FIPS-140-2 certificado por HSM para realizar toda la operación criptográfica.

El módulo DS generará los pares de claves DS y exportará una solicitud de firma de certificado, CSR, para que la CSCA firme.

El certificado DS (firmado por CSCA) se importará al módulo DS.

El DS verificará que la clave pública coincida con la clave privada generada anteriormente. El módulo DS verifica si el certificado DS está firmado por la CSCA correcta, ya que se importó previamente el certificado CSCA en el almacén de certificados DS.

El módulo DS puede tener múltiples certificados DS importados. Utilizará el que tenga la última fecha de emisión.

El DS no utilizará un certificado caducado. Si no hubiera certificados válidos disponibles en el almacén de certificados, el DS generará un error.

El DS no debe eliminar los certificados de DS y las claves relacionadas, una vez caducadas.

El módulo DS funciona en un modo de agrupamiento activo-activo. Cada nodo del clúster tiene su propia clave privada y su propio certificado DS.

Los procedimientos de captura de datos, verificación de identidad deberán ser los existentes, reutilizando toda la infraestructura de oficinas de trámites y todos los procesos existentes en el punto de fabricación. Se adicionará un proceso, por el cual, los datos son enviados a una API que procesará la información para generar el formato necesario para que luego la APP pueda recibir y gestionar el DNI.

El DS para la firma de los DNI virtuales se integrará a la PKI que esté en utilización en el momento de la implementación de la solución.

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

2. BIENES Y SERVICIOS A PROVEER POR EL ADJUDICATARIO

2.1. API REST, SDK y DS

El adjudicatario deberá proveer UNA (1) API REST, SDK, UN (1) DS y la totalidad del hardware necesario y suficiente para brindar la solución integral en un todo de acuerdo a las especificaciones definidas en el punto 1 - REQUERIMIENTOS, de la presente especificación técnica.

2.2. Emisión de credenciales de identificación contenidas en dispositivos móviles (DNI virtual)

El proveedor deberá emitir credenciales (DNI virtual) hasta un máximo de 8.000.000 en un plazo total de DOCE (12) meses. La emisión de las credenciales deberá realizarse de acuerdo a la

demanda que vaya surgiendo por parte de los ciudadanos y deberá responder satisfactoriamente al dimensionamiento establecido en el apartado número 4 de la presente especificación técnica.

En los casos de credenciales revocadas se deberá emitir nuevamente la credencial; teniendo en cuenta que la nueva emisión deberá realizarse sin costo alguno para el RENAPER siempre y cuando la credencial haya sido revocada por causas atribuibles al sistema provisto por el proveedor.

2.3. Generación de credenciales existentes

Con el fin de incorporar la última tecnología en verificación e interoperabilidad se revocarán y volverán a generar en el nuevo sistema las credenciales ya emitidas por el sistema de DNI virtual que posee el RENAPER actualmente. El adjudicatario deberá emitir adicionalmente a los 8.000.000 de nuevas credenciales hasta un total de 2.500.000 credenciales existentes. Esta generación se realizará a partir del cumplimiento de la **etapa 4 del plan de instalación** detallado en el presente apartado de Especificaciones Técnicas.

2.4. Registro de eventos y trazabilidad

El proveedor deberá ofrecer un registro del total de las transacciones realizadas por día, indicando la cantidad y tipo de errores que se hayan producido (en caso de corresponder) e invocando a una API que el RENAPER dispondrá a tal efecto.

Este registro de eventos deberá permitir visualizar la trazabilidad en todo el flujo de información tanto para la emisión, revocación, visualización y verificación de credenciales.

2.5. Documentación técnica

El proveedor deberá proporcionar toda la documentación necesaria para la integración de/los SDK para aplicaciones móviles y de la API en los sistemas del RENAPER. Toda la documentación referida al DS y la documentación correspondiente al mantenimiento de la solución ofrecida.

3. PRUEBAS DE ACEPTACIÓN

Una vez cumplido el plazo establecido en el plan de instalación, punto 7 de la presente especificación técnica, se procederá a realizar las pruebas de aceptación.

El adjudicatario deberá proveer las herramientas necesarias para la ejecución de las siguientes pruebas, las que deberán cumplir con el protocolo establecido en cada una de ellas:

Prueba 1.- Generación de una credencial.

Se deberá disponer de la SDK para que la misma pueda ser utilizada en una aplicación a definir por el RENAPER y gestionar el ciclo de vida de la credencial y una cuenta de correo habilitada. La APP definida por RENAPER será instalada en dos teléfonos móviles uno con sistema operativo Android y otro teléfono con sistema operativo iOS.

Se deberá proveer la lista de parámetros que recibirá la API con sus características de formato y dimensión, los métodos que soporta cada uno de ellos y la lista de mensajes esperados.

El RENAPER generará en su plataforma, específicamente en un legajo de ciudadano, un botón de formulario que permita la recuperación de los datos de un DNI firmado digitalmente y que se consideren necesarios para ejecutar la invocación de la API. Esta prueba se considerará satisfactoria cuando se puedan corroborar las siguientes situaciones:

a) La API recibe los datos enviados y responde con el mensaje apropiado de acuerdo a la documentación entregada.

b) La cuenta de correo configurada en la invocación recibe el código de habilitación para generar la credencial.

c) Se responde sobre el mensaje recibido, se abre la APP y se genera la credencial con los datos enviados por la invocación del RENAPER.

<u>Prueba 2.- Eliminación de una credencial</u>

El RENAPER generará en su plataforma, específicamente en un legajo de ciudadano, un botón de formulario que permita la eliminación de una credencial generada en la Prueba 1).

Esta prueba se considerará satisfactoria cuando se puedan corroborar las siguientes situaciones:

a) La API recibe los datos enviados y responde con el mensaje apropiado de acuerdo a la documentación entregada.

b) La APP conectada a la red elimina la credencial generada.

<u>Prueba 3.- Modificación de los datos de una credencial existente</u>

El RENAPER generará en su plataforma, específicamente en un legajo de ciudadano, un botón de formulario que permita el envío de un nuevo ejemplar de DNI a una credencial existente, para lo cual, deberá seleccionar un ciudadano con más de un trámite firmado digitalmente.

Esta prueba se considerará satisfactoria cuando se puedan corroborar las siguientes situaciones:

a) La API recibe los datos enviados del primer trámite y res[illegible]

b) La cuenta de correo configurada en la invocación recibe el código de habilitación para generar la credencial.

c) Se responde sobre el mensaje recibido, se abre la APP y se genera la credencial con los datos enviados por la invocación del RENAPER.

d) Se invoca a la API con el segundo trámite seleccionado, la misma responde con el mensaje apropiado de acuerdo a la documentación entregada.

e) La APP muestra los datos del segundo trámite enviado.

Prueba 4.- Funcionalidades del SDK. Verificación de Autenticidad del DNI

La autenticidad y vigencia del DNI, en este sistema, es el proceso por el cual, mediante el uso de tecnología, se pueden exhibir medios de prueba que excedan la simple visualización de la imagen del DNI.

Tal como se describe en la funcionalidad del SDK, el titular del DNI, deberá permitir, si lo desea, el acceso a una solicitud de verificación de un tercero.

Para realizar estas verificaciones, y cumplir con las características descritas, el sistema ofertado deberá demostrar, la capacidad de la APP de prueba, que contenga el SDK a proveer, de verificar el DNI, transfiriendo para su visualización la totalidad de los datos o parte de ellos, de manera tal, que el RENAPER, pueda generar distintas "plantillas" de acuerdo a casos de uso más habituales.

Esta prueba se considerará satisfactoria cuando se puedan corroborar las siguientes situaciones:

a) Verificación con transferencia de la totalidad de los datos:

DEMOSTRACIÓN DE LA CAPACIDAD DE VERIFICACIÓN ENTRE CIUDADANOS A TRAVÉS DE BLE, NFC o QR:

El caso de uso debe efectuarse como se describe a continuación:

- El ciudadano B ha recibido una credencial DNI en su teléfono móvil.
- Ambos ciudadanos comenzarán el proceso de verificación de mutuo acuerdo.
- El ciudadano A activa un requerimiento de enlace y lectura de ciudadano al ciudadano B a través de su aplicación instalada en su teléfono móvil.

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

- El ciudadano B aceptando la verificación de todos sus datos, prepara su aplicación para ser enlazada con la del ciudadano A a través de BLE, NFC o QR. Se realizará una prueba para cada método de comunicación.

- El ciudadano A será informado, a través de su APP, que el ciudadano B ha aceptado la petición de ser verificado y que el proceso de verificación ha comenzado.

- El ciudadano B será informado en la APP instalada en su teléfono móvil, que la verificación está produciéndose.

- Una vez terminada la comunicación entre ambos dispositivos (A y B):

- El ciudadano A visualizará, en la pantalla de su dispositivo, la información del ciudadano B.

- El ciudadano B recibirá una confirmación en su dispositivo de que la verificación se ha efectuado satisfactoriamente.

- Se eliminarán todos los datos del ciudadano B en el dispositivo de A luego del periodo de visualización. Es decir, cuando el ciudadano A cierre la aplicación o cuando haya transcurrido un tiempo máximo de 5 minutos desde iniciada la visualización de los datos del ciudadano B en el dispositivo del ciudadano A.

b) Verificación con transferencia de un dato, para este ejemplo, la edad:

<u>VERIFICACIÓN DE LA EDAD DEL TITULAR DEL DNI:</u>

El caso de uso será como se describe a continuación:

- El ciudadano B ha recibido una credencial DNI en su teléfono móvil.

- Ambos ciudadanos comenzarán el proceso de verificación de mutuo acuerdo.

- El ciudadano A activa un requerimiento de enlace y lectura de ciudadano al ciudadano B a través de su APP instalada en su teléfono móvil.

- El ciudadano B aceptando la verificación de su edad, prepara su APP para ser enlazada con la del ciudadano A a través de BLE, NFC o QR y sólo transferir la información requerida.

- El ciudadano A será informado, a través de su APP, que el ciudadano B ha aceptado la petición de verificación de edad y que el proceso de verificación ha comenzado.

- El ciudadano B será informado en su APP instalada en su teléfono móvil, que la verificación está produciéndose.

- Una vez terminada la comunicación entre ambos dispositivos (A y B):

- El ciudadano A visualizará, en la pantalla de su dispositivo, la información de edad del ciudadano B.

- El ciudadano B recibirá una confirmación en su dispositivo de que la verificación se ha efectuado satisfactoriamente.

- Se eliminarán todos los datos del ciudadano B en el dispositivo de A luego del periodo de visualización. Es decir, cuando el ciudadano A cierre la aplicación o cuando haya transcurrido un tiempo máximo de 5 minutos desde iniciada la visualización de los datos del ciudadano B en el dispositivo del ciudadano A.

4. DIMENSIONAMIENTO

El sistema del adjudicatario debe estar preparado para soportar los siguientes escenarios de tráfico productivo:

Deberá soportar picos de solicitud de trámites de 60 transacciones por minuto con tiempos de respuesta no mayores a 1 segundos el 99% de los casos.

El volumen de transacciones, incluyendo las nuevas emisiones, las revocaciones y la modificación de datos del DNI serán como mínimo de 35.000 transacciones en 24 horas. Si este volumen fuera superado, la plataforma deberá "encolar" las peticiones para resolverlas cuando la potencia de procesamiento lo permita.

El adjudicatario deberá ofrecer un entorno de Pre-Producción separado del entorno de producción para pruebas que pudieran surgir en los sistemas implicados.

5. SERVICIO DE MANTENIMIENTO Y SOPORTE TÉCNICO

- El adjudicatario deberá brindar como parte de la contratación un mantenimiento preventivo, correctivo y evolutivo de la misma por el término del contrato desde aceptada la etapa 3 del plan de instalación detallado en la presente especificación técnica.

- La misma debe incluir todos los componentes de software, hardware y actualizaciones; licencias, servicios e integraciones a APIS que conecten la solución con la plataforma RENAPER y que sean parte integral del sistema ofrecido. Incluyendo actualizaciones evolutivas y correctivas.

- Se deberá brindar soporte técnico del SDK para los desarrolladores de la APP durante el tiempo de vigencia del contrato.

6. ACUERDO DE NIVEL DE SERVICIO (SLA)

El adjudicatario deberá ofrecer un nivel de servicio tal que pueda ofrecer la realización de al menos 70 (setenta) transacciones por minuto con tiempos de respuesta no mayores a 5 segundos el 99% de los casos. Se considera una transacción a cualquier tipo de ejecución del servicio, es decir, generación (emisión), eliminación, modificación y verificación de credenciales.

Para la medición se tendrá en cuenta el tiempo transcurrido entre la correcta recepción de la solicitud por parte de la API REST hasta el momento en que finaliza la operación de generación, revocación o modificación de la credencial, lo anterior, excluyendo del cálculo cualquier tiempo de espera por intercambio de datos entre la API REST y sistemas externos a ella.

Para el caso que el sistema del proveedor presente incidentes que puedan comprometer su correcto funcionamiento y por ende la imposibilidad de cumplir con el nivel de servicio establecido, se establecen unos criterios de severidad que permitan ofrecer tiempos de respuesta y resolución adecuados. Estos criterios se definen como:

- A – Impacto crítico: Incidentes atribuibles al sistema del proveedor (software, hardware, etc.) que implican la imposibilidad de realizar más de un 10% de transacciones de emisión y/o visualización y/o verificación en el lapso de 1 día.

- B – Impacto moderado: Incidentes atribuibles al sistema del proveedor (software, hardware, etc.) que implican la imposibilidad de realizar entre un 5% y un 9.99% de transacciones de emisión y/o visualización y/o verificación en el lapso de 1 día.

- C – Impacto mínimo: Incidentes atribuibles al sistema del proveedor (software, hardware, etc.) que implican la imposibilidad de realizar hasta un 4.99% de transacciones de emisión y/o visualización y/o verificación en el lapso de 1 día.

Respecto a los tiempos de respuesta y solución se establecen los siguientes niveles de servicio:

SEVERIDAD	COMUNICACIÓN	CRITERIO	TIEMPO DE RESPUESTA	TIEMPO DE SOLUCIÓN
A	Vía telefónica, correo electrónico o web	**Impacto crítico**	Respuesta inmediata en 1 hora o menos	Máximo 4 horas
B	Vía telefónica, correo electrónico o web	**Impacto moderado**	Respuesta inmediata en 2 horas o menos Esfuerzo únicamente durante horario comercial, pero pueden solicitar 24x7 en caso de ser necesario	Máximo 8 Horas

SEVERIDAD	COMUNICACIÓN	CRITERIO	TIEMPO DE RESPUESTA	TIEMPO DE SOLUCIÓN
C	Vía telefónica, correo electrónico o web	**Impacto mínimo**	Respuesta inmediata en 4 horas o menos Esfuerzo solamente durante horario comercial	Máximo 24 horas

"TIEMPO DE RESPUESTA": Tiempo transcurrido entre la comunicación al adjudicatario de la existencia del mal funcionamiento de el/los componente/s (llamada de servicio) hasta que el mismo toma contacto a los efectos de iniciar el tratamiento del incidente.

"TIEMPO DE SOLUCIÓN": Tiempo transcurrido entre el registro de un incidente hasta su corrección y puesta en funcionamiento del sistema.

Ante la existencia de anomalías o cualquier falla, RENAPER comunicará a la adjudicataria el reclamo a través de correo electrónico o web.

Se informará indicando tipo de falla o anomalía y fecha y hora de producida la misma.

Una vez efectuado el reclamo por cualquiera de las vías mencionadas el prestador del servicio enviará a RENAPER la notificación de aceptación del reclamo, incluyendo en dicha notificación un número de reclamo.

A partir de la fecha y hora indicada en el reclamo, se computará el tiempo de reposición del servicio (tiempo de solución).

Producida la normalización del sistema, la contratista lo comunicará al Organismo por el mismo medio. Lo expresado precedentemente será la base para el cálculo de las penalidades que correspondan.

7. PLAN DE INSTALACIÓN

El plan de instalación se realizará de acuerdo al siguiente detalle:

- ETAPA 1: Disponibilidad de los SDKs: Dentro de las TRES (3) semanas desde la notificación de la orden de compra.

- ETAPA 2: Implementación de componentes nube: Dentro de las NUEVE (9) semanas desde la notificación de la orden de compra.

- ETAPA 3: Implementación en RENAPER: Dentro de las ONCE (11) semanas desde la notificación de la orden de compra.

- ETAPA 4: Pruebas de aceptación: UNA (1) semana desde finalizadas las etapas 1, 2 y 3.

- ETAPA 5: Emisión de credenciales, hasta un total de 8.000.000 de unidades, las que deberán ser emitidas en un plazo máximo de DOCE (12) meses contados a partir del cumplimiento de la etapa 4.

El plazo de implementación de las etapas 1, 2, 3 y 4 será dentro de los NOVENTA (90) días desde el perfeccionamiento de la Orden de compra.

El plazo de entrega de los bienes y servicios objeto de la presente contratación será dentro de los DOCE (12) meses, contados a partir del cumplimiento de la ETAPA 4.

Nota: Este plan es tentativo y las partes ajustarán permitiendo adaptar etapas de acuerdo a lo propuesto por el proveedor previa aceptación del RENAPER.

CM

CONSORCIO IDSECURE

8. LUGAR DE INSTALACIÓN

- Centro de datos del RENAPER de la calle Pedro Chutro N° 2780 – CABA.
- Ministerio del Interior (Back up externo).

9. PRUEBAS DE ACEPTACIÓN PARA LA RECEPCIÓN DEFINITIVA

A modo de realizar la aceptación de los entregables de cada etapa las partes acordarán al menos DIEZ (10) días previos a iniciar las pruebas el alcance de las mismas.

C. MUESTRAS

Será obligatorio para los oferentes la presentación de muestras de acuerdo al siguiente detalle:

a) DOS (2) teléfonos inteligentes conteniendo una/s APP de muestra programada sobre el SDK ofrecido con las funcionalidades de emisión y verificación descritas. Uno de los teléfonos deberá contener sistema operativo Android y el otro teléfono deberá contener sistema operativo iOS.

b) Dispositivos verificadores que no sean teléfonos inteligentes, en caso de existir su inclusión en la propuesta técnica del proveedor.

c) La documentación técnica del SDK y los manuales correspondientes.

d) La documentación técnica de la API.

e) La documentación técnica del DS

f) La documentación básica para ejecutar una URL pública o privada con credenciales de acceso si fueran necesarias, que permita en un ambiente de test, invocar a un método o endpoint que permita la generación de una credencial para ser descargada en la APP de prueba, la modificación de los datos de una credencial generada anteriormente para poder verificar los cambios en la APP de pruebas y la revocación de una credencial que se puede verificar su eliminación desde la APP de pruebas.

Las muestras deberán ser presentadas en la en la División Compras, sita en Av. Pte. Roque S. Peña 671, Piso 6, Oficina 601, Ciudad. Autónoma de Buenos. Aires., en el horario de 09:00 a 17:00 hs. En ese momento se labrará el Acta de Entrega de Muestras, la que obligatoriamente deberá adjuntarse a la oferta.

El plazo máximo para la presentación de las MUESTRAS será el día y hora fijados para la apertura de las ofertas.

Las muestras presentadas, serán consideradas para la evaluación de las Propuestas Técnicas recibidas por cada uno de los oferentes que participen en la presente Licitación. Se probarán las funcionalidades solicitadas a modo de muestra. Por lo tanto, los teléfonos inteligentes deberán contener modelos de credenciales digitales que se puedan visualizar y verificar a través de una/s APP instalada en los teléfonos.

Los procesos de visualización y verificación deberán poder realizarse de manera recíproca en ambos teléfonos inteligentes, es decir, se probarán las funcionalidades de visualización y verificación en ambos dispositivos ya que de acuerdo a lo solicitado un dispositivo deberá estar provisto de sistema operativo Android y el otro de sistema operativo iOS.

Deberán ser suministradas en sobre o caja o paquete o contenedor completamente cerrado, debidamente identificado, labrándose el acta de recepción correspondiente. Los sobres o cajas que contengan las muestras, los que deberán encontrarse fehacientemente identificados, serán abiertos en el momento en el que se formalice el acto de apertura de la oferta técnica.

D. CRITERIO DE EVALUACIÓN. PARÁMETROS

El criterio de evaluación será el de la oferta más económica para la DIRECCIÓN NACIONAL DEL REGISTRO NACIONAL DE LAS PERSONAS, teniendo en cuenta únicamente las propuestas que cumplan con los requisitos mínimos de capacidad e idoneidad técnica.

1.- Capacidad e Idoneidad Técnica

Las propuestas técnicas de las firmas deberán cumplir con los siguientes requisitos mínimos:

- Cumplimiento de la ET en la oferta presentada y funcionalidad de las muestras de acuerdo al detalle establecido en la presente.

- El oferente deberá demostrar que la tecnología ofertada para soluciones de credenciales digitales contenidas en dispositivos móviles ha sido implementada en mínimamente UN (1) proyecto similar en los últimos CINCO (5) años, debiéndose acompañar las constancias documentales correspondientes.

- El oferente deberá demostrar al menos UNA (1) referencia donde se hayan aplicado las soluciones propuestas para el intercambio de información y verificación de credenciales contenidas en dispositivos móviles en modo en línea (*online*) o fuera de línea (*offline*), debiéndose acompañar las constancias documentales correspondientes.

- El oferente deberá demostrar que el proveedor de la tecnología cuenta con una antigüedad en el rubro de al menos CINCO (5) años, debiéndose acompañar las constancias documentales correspondientes.

- El oferente deberá acreditar mediante declaración jurada que la solución ofertada ha sido desarrollado en base a estándares internacionales en materia de credenciales de identificación contenidas en dispositivos móviles lo que permitirá su interoperabilidad y la no dependencia tecnológica del adjudicatario en futuras contrataciones de servicios en la misma materia.

2.- Factor Económico

La oferta económica deberá contener de manera desglosada el precio por unidad de credencial emitida en el que se encuentra incluido la SDK, API, DS, hardware asociado, generación de credenciales ya existentes y su mantenimiento. Se deberá detallar de manera diferenciada el precio asociado al hardware ofrecido.

El plazo de la contratación se establece en QUINCE (15) meses, contados a partir del perfeccionamiento de la orden de compra.

PENALIDADES

Mensualmente se hará una evaluación del nivel de servicio verificando que todas las transacciones enviadas desde la plataforma de identidad del RENAPER tengan su correspondiente proceso en los servicios mencionados y con el nivel de servicio indicado.

En caso de que esto no se verifique, se aplicará el siguiente esquema de penalidades, estableciendo desvíos leves y graves según los siguientes criterios:

INCUMPLIMIENTO	DESVÍO LEVE	DESVÍO GRAVE
Tiempo de respuesta excedido Severidad A	Entre 2 y 4 horas	Más de 4 horas
Tiempo de respuesta excedido Severidad B	entre 4 y 6 horas	Más de 6 horas
Tiempo de respuesta excedido Severidad C	entre 8 y 12 horas	Más de 12 horas
Acumulado de Incidentes por mes	20% de transacciones fallidas	30% de transacciones fallidas

INCUMPLIMIENTO	PENALIZACIÓN POR INCUMPLIMIENTO LEVE	PENALIZACIÓN POR INCUMPLIMIENTO GRAVE
Tiempo de respuesta excedido Severidad A	2 veces el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.	3 veces el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.
Tiempo de respuesta excedido Severidad B	1 vez el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.	1,5 veces el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.
Tiempo de respuesta excedido Severidad C	0,5 veces el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.	0.75 veces el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.
Acumulado de Incidentes por mes	2 veces el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.	3 veces el valor de emisión de una credencial multiplicado por la cantidad absoluta de transacciones fallidas que dieron lugar al reclamo.

En caso de caída total del sistema por cuestiones atribuibles al proveedor y que dieran como resultado CERO (0) transacciones correctas en UN (1) día, se aplicará una penalidad del valor correspondiente a las transacciones promedio efectuadas en los últimos SIETE (7) días.

Las penalidades serán descontadas de la factura mensual que corresponda al mes en el que se generó el incidente que derivó en la penalidad.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Pliego Especificaciones Tecnicas

Número: IF-2023-87307551-APN-DGTII#RENAPER

CIUDAD DE BUENOS AIRES
Viernes 28 de Julio de 2023

Referencia: Pliego de especificaciones técnicas

El documento fue importado por el sistema GEDO con un total de 18 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.07.28 11:59:28 -03:00

Flavio Ramon Brocca
Director General
Dirección General de Tecnología e Innovación en Identidad
Dirección Nacional del Registro Nacional de las Personas

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Digitally signed by Gestion Documental Electronica
Date: 2023.07.28 11:59:28 -03:00