GOBIERNO DE LA REPÚBLICA DOMINICANA INTERIOR Y POLICÍA DIRECCIÓN GENERAL DE MIGRACIÓN	**DIRECCIÓN GENERAL DE MIGRACION** Dirección De Tecnología De La Información y Comunicaciones CATÁLOGO EQUIPOS Y MATERIALES	Versión: 1.0 Fecha:30/09/2022 **DTIC-No. 0669/2022**

DATOS GENERALES

Descripción: Codificación De Tarjeta Inteligente Biométrica Encriptada

Cantidad: 100,000

CARACTERÍSTICAS TÉCNICAS

Codificación De Tarjeta Inteligente Biométrica Encriptada
Que Incluye:

- Aplicación para Captura, Validación y Generación
- Datos Biométricos (Huellas, Rasgos Faciales, Entre Otros)
- Documento Digital en Generación del Criptograma Encriptado tipo QR EN Policarbonato

Especificaciones Técnicas

Software de diseño e impresión de tarjetas
La solución debe incluir la capacidad de diseñar e imprimir una tarjeta de identificación física con los datos recopilados por el sistema ABIS. La aplicación de diseño de tarjetas de identificación podrá funcionar con una gama de diferentes impresoras de tarjetas de varios fabricantes con un mínimo de 600 dpi.

La aplicación de diseño de tarjetas de identificación tendrá la capacidad de diseñar los aspectos visuales y electrónicos de las tarjetas de identidad. Las capacidades visuales deben incluir logotipos, códigos de barras y criptógrafos.

Creación de credenciales
La solución propuesta debe integrarse con el software ABIS y card designer, ya sea en las instalaciones o en un entorno alojado para recibir los datos que se cifrarán y devolver el código criptógrafo respectivo que se utilizará para la tarjeta de identificación impresa y digital. La plataforma de creación de credenciales debe admitir la API REST con todas las comunicaciones en forma cifrada (HTTPS). Según la seguridad de los datos de cada identificación, en caso de que se solicite una identificación de reemplazo para un titular de tarjeta existente, se debe crear un nuevo código criptógrafo. No se permite archivar ningún dato personal, pero el sistema debe registrar registros de auditoría sin almacenar ninguna información de identificación personal. Dado que el código criptógrafo contiene información biométrica, debe ser altamente seguro con múltiples niveles de seguridad incorporados.

La solución debe admitir tecnologías para el cifrado de datos de identidad almacenados en la credencial y **DGM** debe poder emitir las claves utilizadas para el cifrado

Requisitos del código criptógrafo
La solución debe incluir **un único código** de alta densidad impreso en la tarjeta de identificación física y también disponible en formato digital como una identificación digital presentable por la pantalla como la de un teléfono inteligente. Se requieren tecnologías propietarias por razones de seguridad. Código abierto "Open-Source" o el uso de una tecnología disponible públicamente (p. ej., códigos QR, PDF417) que comprometerá la seguridad de los datos no se considera una solución viable y no está permitida . El código debe poder leerse usando teléfonos móviles que tengan capacidades de enfoque automático y flash para leer ciertas bibliotecas como un primer nivel de seguridad y que se requiere un código de autenticación específico para decodificar. Los datos que se configurarán dentro del código criptógrafo se pueden cifrar mediante el uso de mecanismos simétricos.

Continuación 1

Criptograma Encriptado tipo QR para contener Datos Biométricos de forma Offline

La identificación debe caducar y volverse ilegible después de que haya transcurrido la fecha de caducidad. Los datos a incluir en el criptógrafo son:

- Datos biográficos de la persona, nombres, apellidos
- Foto de la persona comprimida a 1.2KB
- Al menos dos plantillas biométricas de huellas dactilares y una plantilla biométrica facial
- Tipo y número de documento de identificación
- Nacionalidad
- Fecha de caducidad

La captura de la imagen facial debe ser una foto tipo pasaporte tomada con una cámara de al menos 640 x 480 DPI con una resolución entre ojos de al menos 120 píxeles.
El código criptógrafo debe tener la capacidad de imprimirse en un formato cuadrado o rectangular (la relación ancho-alto debe estar en el rango de 3,0 y 4,0). El código criptógrafo debe tener capacidad de corrección de errores para restaurar los datos si el código está sucio o dañado. El rango de corrección de errores debe estar entre el 17 % y el 25 %, lo que permite que el código se imprima en un factor de forma de tamaño de tarjeta de identificación estándar, lo que garantiza que el código sea legible incluso si se pierde entre el 15 % y el 25 % de los datos. El código criptógrafo solo debe ser legible por aplicaciones autorizadas y con licencias de DGM . Todos los datos contenidos en el código deben estar encriptados y protegidos. La seguridad de los datos debe lograrse en una arquitectura multicapa utilizando protocolos de seguridad simétricos.

Verificación de credenciales

La solución propuesta debe tener la capacidad de realizar la verificación de identidad de una manera totalmente fuera de línea (sin necesidad de conexión a Internet) utilizando solo la cámara integrada de un teléfono inteligente o tableta de gama media a alta. El código criptógrafo debe ser legible solo con aplicaciones que tengan licencias de software autorizadas, claves de cifrado y códigos de autorización. El lector no debe leer el código si las llaves autorizadas no están presentes para evitar ataques de intermediarios (no debe leer el código y descartar la información si no hay códigos presentes). El código criptógrafo debe incluir un atributo biométrico para permitir la autenticación mediante reconocimiento facial y de huellas dactilares para verificar la identidad del titular de la credencial, así como un retrato facial para permitir la verificación visual. La autenticación biométrica debe incluir la detección de vida y usar tecnologia "contactless" para la captura del rostro y las huellas dactilares.

Estándares biométricos para verificación

La solución debe ser una secuencia completa de eventos que incluya la captura, la extracción de funciones y la comparación departe la propiedad intelectual de un solo proveedor. Los algoritmos biométricos deben ser evaluados, reconocidos y verificables por el NIST (Instituto Nacional de Estándares y Tecnología) para los siguientes estándares:

- Huella Dactilar
  - MINEX III
  - PFT III
  - Algoritmo certificado por el FBI WSQ
- Facial
  - FRVT

Además, la solución propuesta debe incluir las siguientes características:

- Detección de vida pasiva local por dispositivo
- Detección de dedos basada en NN
- Detección de mano izquierda y mano derecha
- NFIQ-2, rango 0-100
- ISO 30107-3 nivel de cumplimiento 1/A

Continuación 2

Criptograma Encriptado tipo QR para contener Datos Biométricos de forma Offline

Requisitos del dispositivo para la verificación

El modelo del dispositivo no debe tener más de 4 años y debe tener un sistema operativo ANDROID o iOS auténtico certificado por Google y Apple con las especificaciones mínimas:

- Sistema operativo: Android 5.1 o superior / iOS 11 o superior
- Cámara: 8MP con flash y enfoque automático
- Arquitectura: ARMv7, ARMv8 para Android y ARM64 para iOS

Precalificación

La solución propuesta debe cumplir con los siguientes criterios de calificación

- Despliegue de una solución similar de lectura de código de alta densidad en al menos tres (3) países y al menos uno en la región de América
- Contar con personal para el soporte en habla hispana.

El oferente debe estar certificado con por lo menos los siguientes estandares, cumplir con los ISOS descritos y haber participado en pruebas de algoritmos evaluados por el NIST de la lista descrita a continuación

- SO/IEC 27001:2013 con certificado vigente durante 2022
- ISO 9001:2015 con certificado vigente durante 2022
- FRVT Evaluado por el NIST
- PFTIII Evaluado por el NIST
- MINEX III Evaluado por el NIST
- SQ certificado por el FBI

GOBIERNO DE LA REPÚBLICA DOMINICANA INTERIOR Y POLICÍA DIRECCIÓN GENERAL DE MIGRACIÓN	**DIRECCIÓN GENERAL DE MIGRACION** Dirección De Tecnología De La Información y Comunicaciones CATÁLOGO EQUIPOS Y MATERIALES	Versión: 1.0 Fecha:30/09/2022 **DTIC-No. 0669/2022**

DATOS GENERALES

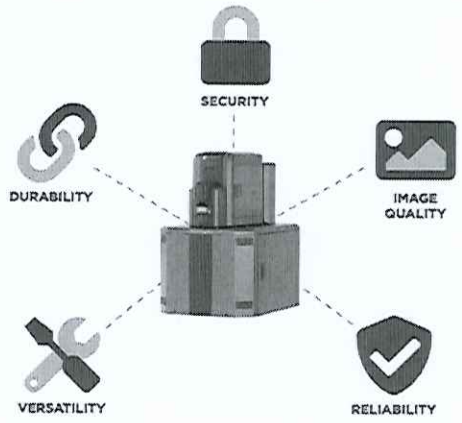
Descripción: ENTRUST (DATACARD) CL900 – MODULO LASER EXPANSIÓN DE LA IMPRESORA ENTRUST DATACARD CR805

Cantidad : 4 Unidades

CARACTERÍSTICAS TÉCNICAS

Descripción Funcional:

Realiza un grabado láser en los documentos (Secuencias, Diseños, Elemento de Seguridad, Entre Otros). Robusteciendo el documento en términos físico buscando mitigar las alteraciones o falsificaciones, ya que el sustrato cambia permanentemente cuando se personaliza.



Características técnicas:

Marca: Entrust Datacard

Modelo: CL900

Modelo de Impresora compatible: Entrust DataCard CR805

Caracteristica de el Laser:

- ✓ Láser de fibra de 25 vatios.
- ✓ Grabado láser a dos caras.
- ✓ Registro de la vista (opcional).
- ✓ MLI (opcional).
- ✓ Microimpresión láser, LaserTact, PersoCurve™, sombra láser.
- ✓ Cerraduras de seguridad para los suministros.
- ✓ Cifrado triple AES/DES.
- ✓ Memoria de la impresora.
- ✓ Estándar de 128 MB.
- ✓ CR805: 4 GB (placa R4).
- ✓ Cable USB.
- ✓ Fuente de alimentación.
- ✓ Cable de alimentación (específico de la región).

PROVEEDORES Y REFERENCIAS

Los oferentes deben ser partner de la marca y estar autorizado para prestar este servicio en el país. Presentar Constancia.	

USO AL QUE VA DESTINADO

Para ser utilizadas en el proceso de regularización de extranjeros.

DIRECCIÓN GENERAL DE MIGRACIÓN
Santo Domingo, R.D.

GOBIERNO DE LA REPÚBLICA DOMINICANA INTERIOR Y POLICÍA DIRECCIÓN GENERAL DE MIGRACIÓN	**DIRECCIÓN GENERAL DE MIGRACION** Dirección De Tecnología De La Información y Comunicaciones CATÁLOGO EQUIPOS Y MATERIALES	Versión: 1.0 Fecha:30/09/2022 **DTIC-No. 0669/2022**

DATOS GENERALES

Descripción: Laminado de Retransferencia Gráfico Personalizado Para la Dirección General De Migración

Código DataCard 515062-512

Cantidad: 500 Unidades

CARACTERÍSTICAS TÉCNICAS

Descripción Funcional:

- Prevención contra falsificación, alteración y duplicación de tarjetas.
- Protección contra el descoloramiento, el desteñido y el desgaste normal por manejo y uso.
- Laminados personalizados incorporados disponibles con características visibles, ocultas y forenses.

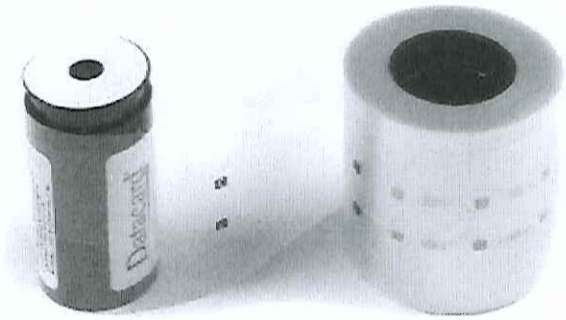
Marca: Data Card
DuraGard Optiselect

Código DataCard: 515062-512

Compatibilidad: Datacard CR805

Dimensiones: 26 x 16 x 12 cm

Grosor: 1 mm



PROVEEDORES Y REFERENCIAS

Los oferentes deben ser partner de la marca y estar autorizado para prestar este servicio en el país. Presentar Constancia.	

USO AL QUE VA DESTINADO

Para ser utilizadas en la emisión de carnets por la Dirección de Extranjería.

DIRECCIÓN GENERAL DE MIGRACIÓN
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, R.D.

GOBIERNO DE LA REPÚBLICA DOMINICANA INTERIOR Y POLICÍA DIRECCIÓN GENERAL DE MIGRACIÓN	**DIRECCIÓN GENERAL DE MIGRACION** Dirección De Tecnología De La Información y Comunicaciones CATÁLOGO EQUIPOS Y MATERIALES	Versión: 1.0 Fecha:30/09/2022 **DTIC-No. 0669/2022**

DATOS GENERALES

Descripción : Contrato de Mantenimiento Preventivo Correctivo de Hardware y Actualización de Software Para la Plataforma de las Impresoras de Extranjería

Cantidad : 1 Unidades

Tiempo : 2 Años de Contrato

CARACTERÍSTICAS TÉCNICAS

Descripción Funcional:

El objeto del contrato es garantizar la continuidad de la operación de la generación de documentos. Dicho servicio cubre la parte de Hardware y Software.

En adición estamos actualizando la codificación de las tarjetas inteligentes para que el documento pueda soportar la solución que se va a implementar de Biometria y Digitalidad.

Características del Contrato del Mantenimiento Preventivo Correctivo de Hardware para la Plataformas de las Impresoras de Extranjería

Printer: CL900, CR-805, CD-800
CLM: para CL900, CR-805 y CD-800

Alcance del Mantenimiento Hardware:

- Preventivo Entrust CL900, _CR-805 y CD-800
- Correctivo Entrust CL900, _CR-805 y CD-800
- Partes Entrust CL900, _CR-805 y CD-800

Alcance del Mantenimiento Software:

- Preventivo Aplicativo
- Correctivo Aplicativo
- Asistencia Remota Aplicativo

SLAs:

- **Tiempo de Atención:** 24x7
- **Tiempo de Respuesta Incidente Critico:** Máximo 1 Hora
- **Tiempo de Respuesta Solicitud:** Máximo 4 Hora

Características del Labor de Actualización Software :

Se actualizarán las codificaciones de las tarjetas inteligentes con nuevas llaves de encripción para dar seguridad a los datos biométricos contenido.

Tiempo : 2 Años de Contrato

Mantenimiento Preventivo Correctivo de Hardware

Y

Actualización de Software

PROVEEDORES Y REFERENCIAS

Los oferentes deben ser partner de la marca y estar autorizado para prestar este servicio en el país. Presentar Constancia.	

USO AL QUE VA DESTINADO

Para ser utilizadas en el proceso de regularización de extranjeros.

DIRECCIÓN GENERAL DE MIGRACIÓN · DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN · Santo Domingo, R.D.