ANEXO N° 1A

ESPECIFICACIONES TÉCNICAS

"ADQUISICIÓN DE MÓDULOS RFID Y ALAMBRE DE COBRE PARA PASAPORTES ELECTRÓNICOS"
Código: SOBYS-INT-007-2022

Módulos – Chips RFID

CARACTERÍSTICA	REQUERIMIENTO MÍNIMO	CUMPLIMIENTO
Requisitos funcionales	El módulo ofertado debe ser 100% compatible con el actual sistema de personalización de la DIGERCIC, en su proyecto S.E.D.I.P. de manera que pueda trabajar de forma inmediata. El circuito electrónico sin contacto se ajustará a las recomendaciones de aplicaciones de identidad OACI Doc 9303/vigente	CUMPLE
Memoria EEPROM /FLASH	Módulo de 144 KB.	CUMPLE
Memoria ROM (tecnologías diferentes a Flash)	Para almacenamiento del Sistema operativo y componentes embebidos (aplications) que no deben alojarse en la memoria para el usuario (EEPROM/FLASH).	CUMPLE
Memoria RAM	6 KB o mayor	CUMPLE
Tiempo de retención de datos	20 años mínimo.	CUMPLE
Capacidad de almacenamiento	32 kB	CUMPLE
Durabilidad	Mayor a 500.000 ciclos de lectura/escritura (a 25ºC). ESD protección mínima 4000V en los pines (ISO y RF), y 5000V luego de que módulo esté laminado.	CUMPLE
Velocidad de transferencia	424 y 848 Kbps.	CUMPLE
Frecuencia de Operación	13,56 MHZ (nominal).	CUMPLE
Tamaño del módulo (en la oferta debe indicar las dimensiones del módulo ofertado)	Longitud del módulo: 8 ± 0,1 [mm] Ancho del módulo: 5,1 ± 0,1 [mm] Longitud del encapsulado: 5,1 ± 0,1 [mm] (aproximado) Ancho del encapsulado: 4,8 ± 0,1 [mm] (aproximado) Grosor total máximo módulo: 250 µm (10 mil) Grosor placa conductiva: 60 ± 10 µm Groso máximo encapsulado (nominal): 200 µm (8 mil) Diámetro del perforado de rechazo: 2 [mm]	CUMPLE
Presentación de los módulos	Rollos (carretes / reel) de 35 mm de 10.000 a 18.000 unidades listas para ser empleadas. Características en el rollo: • Módulos por fila 3. • Pitch horizontal (distancia entre filas de módulos): 9,5 ± 0,1 [mm]. • Pitch vertical (distancia entre módulos): 9,65± 0,1 [mm] • Ancho de la cinta : 35 ± 0,1 [mm]. • Tamaño de las perforaciones de arrastre, cuadrado de 1,42 x1,42 [mm]. • Diámetro de perforación de rechazo 2mm	CUMPLE

Resistencia en procesamiento	• Laminación con temperatura estándar no menor a 150ºC por 30 minutos y 200°C por 20 minutos. • Soldadura eléctrica: 25[ms] a 450°C • Soldado con cautín: 3[s] a 380°C	CUMPLE
Numeración de los chips	Cada chip provisto tendrá un número serial único, cargado durante el proceso de fabricación, información que es requerida en el sistema de inventarios de DIGERCIC, este número debe poder leerse tanto en la etapa de personalización, pre–personalización y pos-emisión	CUMPLE
Interfaz	Interfaz sin contacto La interfaz sin contacto debe cumplir con el estándar ISO/IEC 14443 vigente.	CUMPLE
Distancia de Lectura	Hasta 10 cm según se indica en la ISO/IEC14443.	CUMPLE
Estándares que cumple	ISO/IEC 14443-1 (Características Físicas). ISO/IEC 14443-2 (Modulación). ISO/IEC 14443-3 (inicialización y anticolisión). ISO/IEC 14443-4 (protocolos de transmisión). ISO/IEC 14443 Type A Protocol.	CUMPLE
Características electromagnéticas, físicas y mecánicas	Conforme a las recomendaciones: **a.** OACI Doc 9303 /2015 – Documentos de viaje de lectura mecánica. **b.** OACI NTWG, Informe técnico del uso de circuitos integrados sin contacto en documentos de viaje de lectura mecánica.	CUMPLE
Uso esperado	Soportar la estructura lógica de datos (LDS) especificada por la OACI en su documento 9303 /2015. Compatibilidad con las especificaciones del documento 9303/2015 de la OACI para el intercambio de información.	CUMPLE
Criptografía	Dispondrá de un coprocesador criptográfico con soporte para criptografía simétrica y asimétrica basada en: DES y Triple DES RSA (Permitirá un tamaño mínimo de: 4096 bit, mayor tamaño es aceptado). ECC (Permitirá un tamaño mínimo de: 512 bit, mayor tamaño es aceptado). SHA (Permitirá un tamaño mínimo de: 512 bit, mayor tamaño es aceptado).	CUMPLE
Certificación de seguridad	Certificación CommonCriteria nivel EAL6+ para hardware FIPS 140-2 Nivel 4.	CUMPLE
Resistencia a ataques	Protección a ataques DEMA / SEMA. Monitores de frecuencia voltaje, temperatura. Protección contra luz. Protección contra ataques físicos; debe demostrarse que en el diseño del chip incluye el ocultamiento de bloques funcionales y blindaje activo.	CUMPLE
Documentación	Se debe entregar toda la documentación técnica del circuito, a nivel de usuario y administración, hasta la fecha de la primera entrega.	CUMPLE
Certificación	Se entregará copias simples de las certificaciones de seguridad del módulo, que también se deberá encontrar disponible en la página WEB de la entidad que registra los certificados (common criteria).	CUMPLE

Sistema Operativo

CARACTERÍSTICA	ESPECIFICACIÓN	CUMPLIMIENTO
Sistema Operativo	JCOP (Java Card OpenPlatform).	CUMPLE
Identificación y requisitos funcionales	Indicar el fabricante del sistema operativo, denominación y versión ofertada. El S. O. ofertado debe permitir ser integrado al nuevo sistema de personalización de la DIGERCIC, en su proyecto S.E.D.I.P. de manera que pueda trabajar de forma inmediata.	CUMPLE
Tipo de Sistema Operativo	Sistema operativo Java (Java Card) plataforma abierta Global Plataform Mínima 2.2.1 Versión de Java Card : 3.X.X classic.	CUMPLE
Ubicación	En el área ROM del circuito no ocupa el espacio destinado al usuario (EEPROM), para tecnologías flash, el área ocupada por el S.O. no disminuirá el área libre del usuario es la indicada en la memoria para el usuario en el CHIP.	CUMPLE
Funcionalidades principales	• Soporte de APDU extendido. • Generador de número aleatorios. • Soporte de dominios supletorios de seguridad (SSD). • Recolector de basura controlada. • Al menos 1 canal lógico. • Generación de llaves internas. • Buffer APDU (RAM/bytes) > 1 KB. • Soporte de transcientes en RAM > 3KB. • Permite Post-emisión. • Permite múltiples aplicaciones identificadas con su propio AID y con su propio control de acceso.	CUMPLE
Protocolo de Canal Seguro (SCP)	• SCP 03 de acuerdo a Global Plataform • SCP 02 de acuerdo a Global Plataform • SCP 01 (opcional por encontrarse depredicado)	CUMPLE
Certificación de Seguridad	Sistema Operativo tendrá una certificación vigente CommonCriteria nivel EAL5+. Deben tener un perfil de protección: Java Card System con perfil de protección de configuración mínima versión 2.6 o superior. (Ej.3.x)	CUMPLE
Seguridad criptográfica	Soporte de criptografía asimétrica y simétrica RSA longitudes mínimas de 4096 bits, mayor tamaño es aceptado ECC longitudes mínimas de 521 bits, mayor tamaño es aceptado SHA-1, SHA-2 (hasta 512 bits) DES y Triple DES, AES	CUMPLE
Componentes a soportar	eGovernment - Documentos de identificación (ICAO) con controles de acceso BAC, EAC, SAC/PACE.	CUMPLE
Documentación	Se debe entregar toda la documentación técnica del circuito, a nivel de usuario y administración, hasta la primera entrega.	CUMPLE
Certificación	Se entregará copias simples de las certificaciones de seguridad y funcionalidad del sistema operativo, en conjunto con el componente embebido ICAO, hasta la primera entrega.	CUMPLE

Componente embebido para identificación ICAO BAC/EAC/SAC (PACE)(en ROM / FLASH)

CARACTERÍSTICA	ESPECIFICACIÓN	CUMPLIMIENTO
Identificación y requisitos funcionales	Indicar el fabricante del componente embebido ICAO, denominación y versión ofertada. El componente ICAO ofertado debe permitir ser integrado al nuevo sistema de personalización de la DIGERCIC, en su proyecto S.E.D.I.P. de manera que pueda trabajar de forma inmediata.	CUMPLE
Ubicación	En el área ROM/FLASH del circuito, no ocupa el espacio destinado al usuario (la EEPROM/FLASH), La instanciación es optimizada para requerir el mínimo de memoria de usuario.	CUMPLE
Funcionalidades	• Almacena la información del ciudadano en un formato que cumple con las normas electrónicas de documentos de viaje ICAO 9303/2015. Esta información está organizada en una estructura de datos lógicos (LDS) de acuerdo a lo establecido por la OACI (ICAO). • Las tarjetas electrónicas con este componente embebido pueden ser leídas mediante el software Golden Reader del BCI usado por la OACI para probar pasaportes o cédulas de identidad. • BAC – Control de Acceso Básico. • SAC – Control de Acceso Suplementario implementa PACE-CAM. • ISO 18013: SAC/EAC [BAP/EAP aún soportados]. • Los campos siguen el formato TLV (Rótulo – Largo – Valor), según las especificaciones del documento 9303/2015 OACI. • La ID (código identificador del componente embebido), puede ser cualquiera, la estándar ICAO o la que desee la DIGERCIC. • El componente embebido ICAO soporta BAC, SAC(PACE), EAC v1/v2, AA, PA, CA. • Puede configurarse para una sola escritura / muchas lecturas. (durante la personalización). • Los algoritmos HASH será el especificado en el documento 9303 /2015de la OACI.	CUMPLE
Datos a almacenar	La estructura de los grupos de LDS sigue lo establecido en el documento OACI 9303 y debe contener los 16 grupos de datos, entre los que deben estar los siguientes: • EF.COM (listado de contenido). • DG1 (obligatorio) – MRZ (Tipo de documento, Estado que lo expidió, nombre del titular, número de documento, dígito de control del número de documento, nacionalidad, fecha de nacimiento, dígito control de fecha de nacimiento, sexo, fecha de expiración, dígito control fecha de expiración, datos opcionales (No. Cédula), dígito de control datos opcionales, dígito de control compuesto). • DG2 (obligatorio) – Cara (JPEG) ; al menos 300 dpi. • DG3 (opcional) – FingerPrint (WSQ) 500 dpi, con calidad	CUMPLE

CARACTERÍSTICA	ESPECIFICACIÓN	CUMPLIMIENTO
	AFIS. • DG7 (opcional) – Imagen de la firma. • DG11 (opcional) – Datos adicionales del ciudadano (Lugar de nacimiento, profesión del ciudadano, teléfonos de la persona (fijos y móvil), domicilio de la persona, nombres completos de la persona). • DG12 (opcional) – Datos adicionales del documento (autoridad expedidora, fecha de expedición, imágenes anteriores y posteriores del documento, número de serie personalización, fecha y hora de expedición). • DG14 Información para autentificación de chip (CA si se implementa). • DG15 – AA de ser requerido. • DG16 (opcional) – Datos de personas que ha de notificarse (fecha de registro, nombre de persona, teléfono , dirección). • EF.SOD – El objeto de seguridad que tiene el HASH de cada DG gravado y firma digital de este elemento de seguridad para verificar que los datos no han sido alterados.	
Certificación de Seguridad	El componente ICAO, tiene los siguientes perfiles de seguridad: • En un perfil BAC una certificación vigente CommonCriteria nivel EAL4+. • En un perfil SAC/EAC una certificación vigente CommonCriteria nivel EAL5+. Estos certificados deben poder visualizarse en el portal de Common Criteria.	CUMPLE
Pre-personalización	Las claves criptográficas de acceso pueden ser cargadas durante la pre personalización o durante la personalización a elección de la DIGERCIC.	CUMPLE
Pruebas de operación	La LDS (Logical Data Structure) del chip cumple con el documento 9303/2015 de la OACI (Identificaciones de grupos de datos para documentos de viaje). Un laboratorio externo debe certificar las pruebas de conformidad 9303/2015 de la OACI. Una copia simple del certificado de laboratorio que compruebe la conformidad de las pruebas deberá ser entregado hasta la primera entrega.	CUMPLE
Rendimiento	Como prueba ICAO estándar, tendrá los siguientes rendimientos: • Recuperación de datos de la foto con un tamaño de 17 Kbytes en modo BAC; menor a 2 segundos (dato únicamente, sin contar tiempos de autentificación) • Recuperación de 40 Kbytes de datos eGob SAC+EAVv1 ePP; 4 segundos o menor tiempo (dato únicamente sin contar tiempos de autentificación). • Grabación completa de datos ICAO (DG1, DG2, DG3 (2 huellas), DG7, DG11, DG12, EF.COM. SOD) 55 KB aproximadamente, < 25 segundos (lector externo habilitado APDU largos).	CUMPLE
Integración al sistema de personalización de la	En caso de suscitarse un nuevo sistema de personalización, modificación al sistema actual o por requerirlo la DIGERCIC, será	CUMPLE

CARACTERÍSTICA	ESPECIFICACIÓN	CUMPLIMIENTO
DIGERCIC	necesario que el IGM realice las siguientes acciones para la integración de los componentes suministrados por el desarrollador del componente: • El beneficiario de la orden de compra debe proporcionar toda la información técnica pertinente del chip, sistema operativo, componentes y aplicaciones (Applets) al personal que designe el administrador del contrato por parte del IGM. • El beneficiario de la orden de compra debe proporcionar asesoría técnica del chip, sistema operativo, aplicaciones, componentes, y en caso de ser necesario establecer los canales de comunicación con los fabricantes del chip, del sistema operativo y de las aplicaciones para tener una asesoría técnica.	
Documentación	Se entregará toda la documentación técnica del componente ICAO, al realizar la primera entrega. La información que no se considere pública requiere la respectiva firma de un acuerdo de confidencialidad con el desarrollador del componente embebido, y protocolo de transferencia de información (usualmente archivos PDF de acceso restringido con certificados personalizados para poder acceder a ellos).	CUMPLE
Certificación	Deberá entregar el documento (copia simple) a la recepción de la orden de compra, el cual certifique la seguridad y funcionalidad del componente ICAO.	CUMPLE

2.- Alambre para Antena

CARACTERÍSTICA	ESPECIFICACIÓN	CUMPLIMIENTO
Norma IEC/JIS	ICE 60317-35, 60317-2 (norma NEMA MW131-C).	CUMPLE
Tipo de alambre	Alambre de cobre esmaltado autoadhesivo (Self Bonding Wire).	CUMPLE
Recubrimiento del alambre (esmaltado)	Polyurethano / Polyurethano modificado.	CUMPLE
Capa adhesivo	Polyvinylbutyral.	CUMPLE
Índice de temperatura	Entre 155 y 160°C (aprox).	CUMPLE
Aplicaciones	Adecuado para fabricar transponders.	CUMPLE
Temperatura de ablandamiento del adhesivo	> 100°C	CUMPLE
Condiciones de soldadura	De 0,8 a 1,5 seg a temperaturas de 390°C (menor que norma IEC 60851-4.5).	CUMPLE
Diámetro del alambre	0,100 mm (100 micras) nominal.	CUMPLE
Tipo de bobina (spool)	Bicónica o cilíndrica, eje de 16 mm, diámetro exterior máximo 125 mm, altura máxima de la bobina 125 mm.	CUMPLE
Kilos aproximados por bobina	2,5 Kg de alambre.	CUMPLE
Longitud aproximada del alambre	De 10 a 12 Km / kg.	CUMPLE

Soporte Técnico

CARACTERÍSTICA	ESPECIFICACIÓN	CUMPLIMIENTO
Soporte en producción al Instituto Geográfico Militar	El beneficiario de la orden de compra brindará al Instituto el siguiente soporte: • Asistencia durante el inicio de la producción, por 30 días o 120.000 tarjetas, en el proceso de pre-personalización para cada aplicación, y registro de cada número de serie de cada módulo para el sistema de inventario de la DIGERCIC. • El Instituto posee para la pre-personalización, maquinaria en su fábrica de tarjetas, que puede realizar la pre-personalización mediante APDUs en hexadecimal.	CUMPLE
Pre-personalización en maquinaria que cuenta el IGM	El IGM dispone para la producción de pasaportes una máquina para realizar la pre-personalización del mismo, para lo cual cuenta con un módulo que interactúa con el chip RFID el cual debe quedar totalmente integrado con el chip propuesto. • La máquina que dispone actualmente el IGM es la ID-6000 de marca Mühlbauer. • Los costos de derivados de esta integración corren por cuenta del el proveedor. • Alcances de la integración: • Changing historical bytes of ATR. • Installation of Security Domain and ICAO applet • Storage of Global Platform Secure Channel Keys • Personalization of Security Domains. • Fused Card	CUMPLE
Diseño de antenas	El beneficiario de la orden de compra deberá entregar el diseño en formato de CAD (dwg o DXF) debidamente acotado (longitudes, arcos, espaciamiento, etc) de la antena, con el alambre provisto, que trabajen en el material de soporte de la tarjeta (plástico), que debe estar acorde a la norma 14443-1 (clase 1). El plástico previsto es: • Núcleo de PETG • Espaciadores de PETG • Capa Impresa en Offset (ambos lados) PETG • Overlay PETF	CUMPLE
Pruebas de inlays (parte electrónica)	El beneficiario de la orden de compra realizará pruebas de laboratorio de los inlays con los diseños de antenas proporcionados, y entregará un reporte del comportamiento y cumplimiento de conformidad con la ISO 14443 o las recomendaciones de modificación pertinentes para mejora del diseño. • El costo de estas pruebas de laboratorio corre por cuenta del beneficiario de la orden de compra.	CUMPLE
Soporte permanente durante la ejecución del contrato	Debe existir una línea de soporte de personal especializado en forma directa, para solventar problemas que surjan en las áreas de: Sistema Operativo Aplicación Seguridades Los canales de soporte deben estar establecidos a la fecha de la entrega de lo módulos de prueba	CUMPLE
Seguridad de pre-	Deberá proporcionar un plan de seguridad para la pre-	CUMPLE

personalización	personalización, basado en normas internacionales tales como la norma EN14890, ISO 7816, u otras plataformas reconocidas mundialmente las cuales permiten el uso de criptografía asimétrica, manteniendo la confidencialidad de la información sensible. También se deberá incluir mecanismos de autentificación mutua que ayuden a detectar chips falsos de una manera sencilla durante la pre-personalización.	
Contingencia en caso de vulnerar las seguridades del módulo	En la eventualidad que, durante la entrega de módulos y/o durante la vigencia de la garantía técnica (12 meses a partir de la firma del acta de entrega recepción definitiva), exista un ataque exitoso (hackeo) al módulo, al sistema operativo, al aplicativo de identificación, el beneficiario de la orden de compra deberá solucionar el problema de seguridad en forma de minimizar el impacto de este riesgo.	CUMPLE

Para la entrega de la orden de compra, se incluirá la transferencia de conocimientos conforme lo siguiente:

CARACTERÍSTICA	ESPECIFICACIÓN	CUMPLIMIENTO
Módulo y Sistema Operativo	20 horas de transferencia de conocimiento que abarquen el funcionamiento del CI, Sistema Operativo, Inicialización, APDU's, Aplets, instanciación, Criptografía, Seguridad, Global Plataform	CUMPLE
Aplicación ICAO	20 horas de transferencia de conocimientos que abarquen estándares para eID (documento de identificación electrónico), estructura de las aplicaciones, configuración, seguridad, ciclo de vida, personalización, configuración para el documento ecuatoriano	CUMPLE
Plan de transferencia de conocimientos	El beneficiario de la orden de compra, luego de la recepción de la orden de compra presentará un plan detallado de esta transferencia de conocimientos, que deberá realizarse hasta la primera entrega de módulos.	CUMPLE
Número de personas	6 personas un total de 40 horas.	

COMISIÓN TÉCNICA

Firmado electrónicamente por:
BYRON PATRICIO PUGA CASTRO

Crnl. de CSM. Byron Puga.
Profesional designado por la Máxima Autoridad

Firmado electrónicamente por:
LUIS EDUARDO GARCES CALDERON

Ing. Luis Garcés
Delegado del titular del Área Requirente

Firmado electrónicamente por:
PABLO XAVIER SINCHIGUANO CALVOPINA

S.P. Pablo Sinchiguano
Profesional afín al objeto de la contratación