Nueva Autoridad Certificadora Raíz Nacional

Consulta Pública N° 03/2026

AGESIC

(Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento)

Contenido

1. **Antecedentes** 3
2. **Objetivo** 4
3. **Requerimientos generales** 6
4. **Alcance de la Consulta Pública** 11
5. **Procedimiento** 11
6. **Presentaciones** 12
7. **Información confidencial** 15
8. **Aceptación** 15

1. Antecedentes

La Autoridad de Certificación Raíz Nacional (ACRN) que opera desde 2011, es la raíz de la cadena de confianza de la Infraestructura de claves públicas (PKI por sus siglas en inglés) de Uruguay. Su certificado es autofirmado y aceptado expresamente por los terceros que establecen confianza en la PKI Uruguay (todo el ecosistema nacional, otros países con los que tenemos reconocimiento, soluciones de empresas y organizaciones internacionales, entre otros).

De acuerdo a lo estipulado en la Ley N° 18.600[1] - Documento Electrónico y Firma Electrónica, la operación de la ACRN es realizada por AGESIC. A través de la ACRN, AGESIC habilita tecnológicamente la operación de los Prestadores de Servicios de Certificación Acreditados (PSCA) firmando certificados electrónicos para sus Autoridades Certificadoras (ACPA – Autoridad Certificadora del Prestador Acreditado). De esta forma, las ACPA pasan a ser parte de la cadena de confianza de la PKI Uruguay y quedan habilitados para brindar servicios basados en certificados digitales a la ciudadanía como Firma Electrónica Avanzada, Identificación Digital, sellado de tiempo, entre otros.

Los certificados de las ACPA firmados por la ACRN se rigen por la Política de Certificación y por la Declaración de Prácticas de Certificación de la ACRN[2]. Por lo tanto, las ACPA y los Terceros Aceptantes de dichos certificados cuentan con el respaldo de PKI Uruguay para las operaciones de firma electrónica que correspondan.

Los certificados emitidos por la ACRN y dirigidos a las ACPA, así como todos los demás aspectos vinculados a la ACRN se rigen por las políticas emitidas por la Unidad de Certificación Electrónica (UCE). La UCE es el órgano regulador del ecosistema de firma electrónica avanzada (o firma digital) e identificación digital, entre otros servicios de confianza donde la PKI es la estructura tecnológica que garantiza la confianza en todo el ecosistema. La UCE cuenta con facultades de acreditación, control, instrucción, regulación y sanción.

La ACRN actual tiene los siguientes componentes, dentro del marco normativo elaborado y

[1] https://www.impo.com.uy/bases/leyes/18600-2009
[2] https://www.gub.uy/unidad-certificacion-electronica/comunicacion/publicaciones/declaracion-de-practicas-de-certificacion-de-la-autoridad-0

mantenido por la UCE:

1. Tres unidades HSM (Hardware Security Module), dispositivo criptográfico donde se aloja la clave privada de la raíz y el certificado autogenerado (la clave privada nunca sale de este contexto).
2. Servidores idénticos de Producción, Contingencia y Testing (hardware) donde residen los HSM.
3. Sistema operativo y sistema de gestión de la ACRN. Este sistema gestiona funcionalidades habilitadas para firmar certificados de prestadores acreditados, generar nuevos certificados y emitir listas de revocación, entre otras. Realiza el nexo entre los usuarios con sus diferentes roles y los objetos criptográficos que residen en los HSM cumpliendo con todas las políticas y requerimientos de seguridad de la UCE.
4. Manuales, procedimientos y guiones para que los operadores, administradores y custodios realicen las diferentes actividades sobre la ACRN.

AGESIC viene trabajando en un proyecto para el desarrollo del ecosistema de credenciales verificables. En particular, el desarrollo de un Producto Mínimo Viable (MVP por sus siglas en inglés) para el Documento Nacional de Identidad (DNI) digital bajo la norma ISO/IEC 23220 (mDoc), extensión de la ISO/IEC 18013 (mDL), la cual exige la implementación de una Autoridad Certificadora Raíz, denominada IACA (Issuing Authority Certification Authority). Esta autoridad certificadora, actuará como ancla de confianza, firmando los certificados que los emisores utilizarán para emitir el DNI digital y las licencias de conducir digitales (Document Signer) y también firmará las listas de revocación de los emisores.

2. Objetivo

El objetivo de la presente Consulta Pública es conocer soluciones de mercado para el desarrollo, puesta en producción y mantenimiento de Autoridades Certificadoras que permitan constituir la raíz de dos Infraestructuras de Claves Públicas:

1. Nueva Autoridad Certificadora Raíz Nacional (ACRN2): sustituirá a la actual ACRN que opera desde 2011, constituyendo la nueva raíz de la infraestructura nacional de claves públicas para servicios de confianza regulados por la UCE.

2. Nueva Autoridad Certificadora para Emisores de Credenciales Verificables (IACA): conforme a las normas ISO/IEC 23220 (mDoc) e ISO/IEC 18013 (mDL), será la raíz de confianza para la emisión de DNI digital y otras credenciales digitales.

Se desea conocer soluciones que, bajo una única infraestructura (HSM, hardware y software) puedan gestionar más de una Autoridad Certificadora, cada una con sus claves y certificados específicos y separados.

La presente consulta forma parte de un proceso orientado a formular un proyecto integral para el diseño y puesta en producción de la ACRN v2 y de la IACA. La solución propuesta deberá contemplar todos los componentes necesarios: software (sistema operativo, sistema de gestión y demás componentes), hardware (incluyendo HSMs), licencias si correspondiere, servicios de capacitación, manuales y guiones operativos (setup, firma de certificados, revocación, gestión de roles y usuarios), servicios de setup y hardening, soporte y mantenimiento (incluyendo posibles upgrades) y garantía.

En particular, se solicita presentar información relativa a las capacidades de la solución para abordar con igual profundidad las siguientes dos dimensiones estratégicas respecto a la criptografía post-cuántica (PQC):

- Estrategia de migración gradual y coexistencia: capacidad de operar en modo híbrido con algoritmos clásicos y post-cuánticos durante un período de transición ordenado.
- Readiness y capacidad futura para PQC: arquitectura, roadmap del fabricante y mecanismos que garanticen la adopción completa de PQC cuando los estándares y el ecosistema estén maduros.

Las nuevas autoridades raíces emitirán cada una un certificado autofirmado y firmarán los certificados de los prestadores acreditados (ACRN2) y emisores de credenciales (IACA). Las funciones generales que debe contemplar en cada caso son:

- Gestión de claves y certificados digitales
- Emisión de claves y certificados digitales

- Validación de claves y certificados digitales
- Revocación de certificados digitales
- Firma de certificados digitales de autoridades intermedias

3. Requerimientos generales

A continuación, se aclaran algunos requerimientos que deben cumplir:

Entornos de operación

Las dos Autoridades Certificadoras deben tener por lo menos tres entornos idénticos con respecto al hardware y software: testing, contingencia y producción. El entorno de contingencia mantendrá una copia de la clave privada y el certificado de producción, asegurando la disponibilidad.

Modo de operación (On-Premise / Offline)

Tanto la ACRN2 como la IACA deberán operar en modalidad on-premise, en instalaciones que AGESIC disponga. Los tres ambientes deberán estar completamente offline, sin ningún tipo de conexión a redes de datos externas. Los servidores estarán apagados y se encenderán únicamente para realizar operaciones específicas. La única operación recurrente es la emisión de la lista de revocación, conforme a la periodicidad definida por la normativa vigente.

Los servidores de producción y contingencia deberán estar ubicados en localizaciones geográficas distintas y distantes, a fin de garantizar la continuidad operativa ante catástrofes, incendios u otros eventos.

Requerimientos Técnicos del Sistema Actual (Referencia informativa)

A modo informativo, la Autoridad Certificadora Raíz Nacional que opera actualmente posee los siguientes requerimientos:

- Opera con autenticación fuera de banda M-N de claves criptográficas y cuenta con soporte para llaves físicas y pines para autorización fuera de banda con PED o equivalente.

- Certificación FIPS 140-2 level 3 (múltiples factores, PED).
- Soporte para llaves RSA 4096 y superior.
- Algoritmos criptográficos soportados:
    - Asimétricos: RSA, Diffie-Hellman y familia de Elliptic Curve Cryptoghraphy
    - Simétricos: AES, AES-GCM, Triple DES, ARIA, SEED, RC5, etc.
    - Hash: familia de algoritmos SHA-2, como SHA256 y SHA512
- Los HSM pueden ser PCI, externos mediante red o cualquier otra conectividad.
- Soportar certificados X.509 v3, según el estándar RFC 5280.
- Permite listas de Revocación (CRL) X.509 v2, según estándar RFC 5280.
- Procesamiento de solicitudes de certificado PKCS10.

Marco normativo de referencia (alineamiento con eIDAS)

La solución deberá permitir que la ACRN2 y la IACA operen en conformidad con las normas técnicas que el marco europeo eIDAS 2.0 exige a los prestadores cualificados de servicios de confianza, de modo de facilitar un eventual reconocimiento mutuo con la Unión Europea (artículo 14 del Reglamento (UE) N° 910/2014). Se solicita a los proveedores indicar el grado de cumplimiento de su solución respecto de:

- Reglamento (UE) N° 910/2014, modificado por el Reglamento (UE) 2024/1183 (eIDAS 2.0), y Reglamento de Ejecución (UE) 2025/1943 (normas de referencia para certificados cualificados de firma y sello electrónicos).
- ETSI EN 319 401: requisitos generales de política para prestadores de servicios de confianza.
- ETSI EN 319 411-1 y EN 319 411-2: requisitos de política y seguridad para autoridades de certificación que emiten certificados y certificados cualificados.
- ETSI EN 319 412 (partes 1, 2, 3 y 5): perfiles de certificados.
- CEN/TS 419 261: requisitos de seguridad para sistemas confiables de gestión de certificados.
- EN 419 221-5: Perfil de Protección para módulos criptográficos de servicios de confianza (HSM).
- Mecanismos Criptográficos Acordados publicados por ENISA y ETSI TS 119 312: algoritmos y longitudes de clave.

- ETSI TS 119 612: Listas de Confianza (Trusted Lists).
- ETSI EN 319 403-1: evaluación de la conformidad de prestadores de servicios de confianza (auditabilidad de la solución).

Requerimientos técnicos para ACRN2 e IACA (Nueva Solución)

La nueva solución deberá cumplir, como mínimo, con los siguientes requerimientos técnicos:

Sistema operativo:

- Versión actualizada dentro de distribuciones comúnmente utilizadas.
- Soporte vigente del fabricante o comunidad, incluida la publicación de parches de seguridad.
- Horizonte mínimo de soporte: se requiere conocer la fecha de fin de soporte (EOL) publicada por el fabricante.
- Estrategia documentada para migración ante fin de soporte del sistema operativo durante el período contractual.
- Hardening: servidor minimalista, cerrado por defecto, con superficie de ataque mínima.

Software de Gestión de la AC

- Cumplimiento integral de los requisitos de la norma ISO/IEC 18013 (mDL) y la norma ISO/IEC 23220 (mDoc), incluyendo todas las extensiones necesarias del certificado X.509 autofirmado para la IACA.
- Condiciones y modalidades de soporte del fabricante, incluyendo actualizaciones de seguridad y ciclo de vida del producto.
- Soporte para gestión de múltiples Autoridades Certificadoras sobre la misma infraestructura (ACRN2 e IACA), con separación lógica y física de claves y certificados.
- Perfiles de usuario diferenciados: operador, auditor, administrador, custodio y otros roles requeridos por las políticas de la UCE.

- Se valorará que cumpla los requisitos de CEN/TS 419 261 (sistemas confiables de gestión de certificados), referenciada por el Reglamento de Ejecución (UE) 2025/1943, o que cuente con certificación Common Criteria equivalente.
- Roles de confianza y control dual: separación de funciones (administración, operación, auditoría y custodia) y autorización M de N para toda operación con las claves de las AC, conforme a ETSI EN 319 401 y EN 319 411-1.
- Registros de auditoría: registro íntegro y protegido contra alteraciones de todos los eventos relevantes (incluidas las ceremonias de claves), exportable para auditorías externas, conforme a ETSI EN 319 401.

HSM (Hardware Security Module)

- Custodia de claves: FIPS 140-3 nivel 3 o Common Criteria EAL4+ (AVA_VAN.5) contra Protection Profile EN 419221-5, múltiples factores “m-n”, PED.
- Estrategias y procedimientos a seguir ante el anuncio de fin de soporte de un equipo durante el contrato para la migración segura de las claves.
- Los modelos no podrán tener anunciado su fin de venta (EOS) ni su fin de vida (EOL) en los próximos 2 años. El fabricante deberá garantizar soporte, repuestos y actualizaciones de firmware durante al menos 5 años.
- Estrategias y formas para aplicar actualizaciones de firmware de los HSM, deberán mantener vigente la certificación exigida (FIPS 140-3 nivel 3 o Common Criteria EN 419221-5). El proveedor deberá informar previamente si una actualización afecta el estado de la certificación. No se aceptará la instalación de versiones de firmware no validadas sin autorización expresa del contratante.
- Vigencia de la certificación: indicar número de certificado, versión de hardware y firmware certificada, fecha de vencimiento y hoja de ruta de recertificación (incluidas las versiones de firmware con algoritmos PQC).
- Ceremonia de generación de claves: generación de las claves de la ACRN2 y de la IACA dentro del HSM, en ceremonia documentada con control dual, guion aprobado y presencia de un auditor independiente o registro audiovisual, conforme a ETSI EN 319 411-1.

- Respaldo y recuperación de claves: únicamente en forma cifrada, mediante mecanismos del propio HSM incluidos en el alcance de su certificación y bajo control M de N.
- Soluciones que incluyan HSM reconocidos y el estado práctico en implementación algoritmos PQC, no solo a nivel de estándares sino también en implementaciones concretas en uso actualmente. En particular, algoritmos criptográficos NIST[3] resistentes cuánticos como ML-KEM (FIPS 203, antes CRYSTALS-Kyber), ML-DSA (FIPS 204, antes CRYSTALS-Dilithium), SLH-DSA (FIPS 205, antes SPHINCS+), FN-DSA (FALCON, en estandarización) y firmas basadas en hash con estado LMS/XMSS (NIST SP 800-208), entre otros. Indicar si dichos algoritmos están incluidos en el alcance de la certificación FIPS 140-3 / Common Criteria del HSM y si la solución soporta certificados híbridos o compuestos.

Otras Características de Interés

- Modelos de negocio propuestos tales como arrendamiento, adquisición definitiva, etc. (teniendo en cuenta las necesidades de las dos autoridades raíces).
- Teniendo en cuenta la futura transición hacia algoritmos PQC, es importante conocer la visión de transición, así como las posibilidades que brinda la solución bajo un concepto “crypto-agility”, en un escenario donde sea posible reemplazar los algoritmos utilizando la misma infraestructura y solución para cada una de las autoridades certificadoras. Para este caso, es importante tener en cuenta que en la solución residirán 2 ACs (ACRN2 e IACA).
- Estrategias previstas por la solución ofrecida con respecto a la transición ante algoritmos resistentes a la computación cuántica.
- Costos estimados de referencia, en particular la relación entre los costos de adquisición y puesta en funcionamiento con los de garantía y soporte.
- Metodología y necesidades técnicas que la solución propone en caso de necesidad de actualización (software, hardware, HSM), incluyendo la posibilidad de migrar las claves criptográficas.

[3] NIST, Post-Quantum Cryptography: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

- Características técnicas de los HSM (conectividad a través de PCI, red, etc.), forma de interacción con las claves criptográficas, equipos para la gestión (notebooks, etc.).
- Características técnicas y requerimientos del software de gestión, sistema operativo y todos los componentes de la solución.
- Visión del fabricante sobre el cronograma global de adopción de PQC y su impacto en los ecosistemas de PKI gubernamentales.
- Impacto del uso de algoritmos PQC sobre el rendimiento (tiempos de firma, verificación, tamaño de claves y certificados).

4. Alcance de la Consulta Pública

La presente Consulta Pública tiene como alcance exclusivo la obtención de información respecto a las diferentes herramientas y/o soluciones informáticas disponibles en el mercado para el diseño y puesta en producción de una nueva ACRN2 y la IACA.

AGESIC no asume al realizar la presente Consulta Pública, compromiso alguno de elegir, contratar o implementar los productos y servicios propuestos.

La realización de la presente consulta no implica que, si en el futuro se realiza efectivamente la implementación de esta solución informática, se efectúe obligatoriamente seleccionando una solución de las presentadas en este proceso. Tampoco implica que los participantes tendrán privilegios o preferencias en futuros llamados.

Quienes se presenten a esta Consulta Pública, por el solo hecho de presentarse, asumen el alcance mencionado anteriormente y lo aceptan como satisfactorio en todos sus términos.

5. Procedimiento

El procedimiento de la Consulta Pública será el siguiente:

- Los interesados podrán realizar preguntas únicamente por correo electrónico a adquisiciones@agesic.gub.uy hasta el viernes 27 de noviembre a las 13:00 hs.

- AGESIC responderá a las consultas formuladas y publicará dichas respuestas en el sitio web de la Agencia Reguladora de Compras Estatales (ARCE): LINK
- Se solicita a los interesados ingresar sus presentaciones en el sitio web de Compras Estatales hasta el martes 01 de diciembre a las 13:00 hs.
  La Consulta Pública se encuentra publicada en Compras Estatales en el Inciso 2 – Unidad Ejecutora 10, **Solicitud de Información N° 03/2026.**

Respecto del contenido a incluir en el sitio web de Compras Estatales, se solicita a los interesados ingresar únicamente la presentación a realizar para la presente Consulta Pública.

Dichas presentaciones deben incluir los datos de la empresa, persona de contacto, un resumen de los antecedentes de la empresa en este rubro y la propuesta correspondiente con el objeto del llamado.

No se requiere ingresar al mencionado sitio un precio general de la solución presentada.

El único requisito que solicita el sistema para poder subir la presentación en línea es estar registrado en el Registro Único de Proveedores del Estado (RUPE), en cualquiera de los siguientes estados: EN INGRESO o ACTIVO.

Por dudas o consultas sobre cómo cargar en línea la presentación en el mencionado sitio, podrán comunicarse con Atención a Usuarios de ARCE al (+598) 2604 5360 de lunes a viernes 9:00 a 18:00 horas, o a través del formulario web.

6. Presentaciones

Las sesiones serán virtuales (vía MS Teams) y serán grabadas.

Posteriormente a la fecha límite para manifestar interés y subir las presentaciones en el sitio web de ARCE, AGESIC propondrá a cada uno de los interesados, la fecha y hora para la presentación, que tendrá una duración máxima de 60 (sesenta) minutos.

Los interesados podrán solicitar a AGESIC una fecha y hora diferentes a la propuesta.

Se requiere que en la presentación participen técnicos y encargados de negocio que puedan

evacuar todas las dudas que se presenten, así como la experiencia de la empresa en la implementación de casos similares de la solución propuesta.

No hay un formato estándar para la presentación, plantilla ni formato de archivo preferido para la entrega. El contenido de la presentación se deberá ajustar al siguiente esquema:

Tema	Duración máxima estimada en minutos
Experiencia de la empresa y en particular de la solución presentada	10
Casos de uso relevantes de la solución para la ACRN2 y la IACA	10
Características técnicas de la solución, estándares, componentes, formas de integración, escalamiento y situación de algoritmos PQC. Certificaciones de los HSM (Common Criteria/EUCC, FIPS 140-3)	10
Estrategia de implementación teniendo en cuenta el contexto y objetivo propuesto	10
Costos de instalación, operación y mantenimiento de referencia	10
Modalidades de licenciamiento, soporte y operación y al menos 2 modalidades de modelo de negocio	
Preguntas y respuestas	10
Tiempo máximo total	**60**

Se espera que la empresa presente al menos la siguiente información:

- Presentación general de la empresa.
- Experiencia en diseño, desarrollo, puesta en funcionamiento y mantenimiento de Autoridades Certificadoras, especialmente en los servicios de la presente Consulta.
- Modelos de negocio y costo asociado.
- Proyecto en alto nivel para el diseño, armado y puesta en funcionamiento de una posible AC según las necesidades de AGESIC y UCE.

- Detalles de los HSM ofrecidos.
- Detalles de los servicios ofrecidos.
- Cumplimiento de normativas, estándares y certificaciones internacionales relevantes para el caso. Indicar número y vigencia de los certificados Common Criteria/EUCC y FIPS 140-3 de los HSM, y referencias de implementación en Prestadores Cualificados de Servicios de Confianza incluidos en Listas de Confianza de la UE.
- Situación actual, incluyendo casos de uso prácticos y concretos, de la implementación de algoritmos criptográficos PQC en la solución propuesta.
- Estrategia y posibilidades de migración hacia algoritmos PQC una vez la nueva AC esté en producción.
- Mecanismos y posibilidades de soporte y mantenimiento evolutivo. Cómo se resuelve el soporte en forma remota teniendo en cuenta el ambiente offline donde residirá el sistema.
- Posibilidad de exportar las claves y certificados hacia un HSM de otro fabricante en el futuro. Alternativamente, describir la estrategia de migración propuesta (p. ej., renovación de claves con certificación cruzada), considerando que cualquier traslado de claves privadas solo podrá hacerse en forma cifrada y conforme a la configuración certificada del HSM.
- Formas de gestionar más de una Autoridad Certificadora en la misma infraestructura.
- Mecanismos para publicar las anclas de confianza de la IACA (VICAL según ISO/IEC 18013-5 y listas de entidades de confianza según ETSI TS 119 602) y, para la ACRN2, una Lista de Confianza nacional según ETSI TS 119 612.
- Capacidades para la administración y auditoría de todo el sistema.
- Opciones de capacitación.
- Grado de alineamiento con el marco eIDAS 2.0 (Reglamento (UE) N° 910/2014 modificado por el Reglamento (UE) 2024/1183 y sus actos de ejecución) y las normas ETSI/CEN indicadas en la sección 3, así como con estándares NIST (FIPS 140-3, FIPS 186-5, FIPS 203/204/205). Indicar experiencias con prestadores auditados por organismos de evaluación de la conformidad según ETSI EN 319 403-1.
- Toda información que la empresa considere de interés para el caso.

A todas las presentaciones asistirán representantes de las áreas sustantivas de AGESIC,

técnicos especialistas en diversas temáticas y asesores.

Toda información que se entregue o se pretenda entregar que NO esté relacionada con la presente Solicitud de Información, se descartará o rechazará en el acto.

AGESIC no emitirá juicio de valor sobre ninguna propuesta en particular, tampoco se puntuará técnicamente, ni generará ningún ranking, resumen o informe para los interesados.

Los resultados obtenidos luego del análisis de las presentaciones realizadas serán de uso exclusivo de AGESIC y tendrán carácter confidencial.

Pueden participar empresas de cualquier nacionalidad, siendo necesario realizar la presentación en idioma español; en caso contrario deberá contar con un traductor por parte de la empresa.

7. Información confidencial

En caso de que los oferentes presentaren información considerada confidencial, al amparo de lo dispuesto en el artículo 10 literal I) de la Ley N° 18.381 de Acceso a la Información Pública de 17 de octubre de 2008 y del art. 65 del TOCAF, la misma deberá ser ingresada indicando expresamente tal carácter.

8. Aceptación

Por el solo hecho de presentarse al presente llamado se entenderá que el interesado conoce y acepta sin reservas los términos y condiciones establecidos en el presente documento.