Microservicio MsAdaptadorPKI

Documento Versión: 1.0

Gestión de Seguridad Electrónica

Fecha generación: **01/12/2025**

CONTROL DE VERSIÓN

VERSIÓN	FECHA DE ACTUALIZACIÓN	CARGO	DESCRIPCIÓN
1.0	01/12/2025	Arquitecto de Software	Versión inicial del documento

Tabla de contenido

1 CONTEXTO

El Registro Nacional de Identificación y Estado Civil (RENIEC) es el organismo técnico autónomo encargado de la identificación de los peruanos, otorgar el Documento Nacional de Identidad (DNI) y registrar los hechos vitales. En el marco de la modernización y transformación digital del Estado peruano, RENIEC ha desarrollado el DNI Electrónico (DNIe), un documento de identidad que incorpora tecnología de chip y biometría, permitiendo la autenticación electrónica de ciudadanos y facilitando servicios digitales seguros.

2 INTRODUCCIÓN

Este documento describe el **catálogo de microservicios** identificados para la solución de Personalización del DNIe de RENIEC. El objetivo es establecer una arquitectura técnica moderna, escalable y mantenible que reemplace o complemente los sistemas monolíticos actuales mediante una transición ordenada hacia una arquitectura orientada a microservicios.

2.1 Justificación de la Arquitectura de Microservicios

La adopción de microservicios para esta solución responde a necesidades técnicas y operativas concretas:

Escalabilidad Independiente: Componentes con cargas diferenciadas pueden escalar de forma independiente según demanda real, optimizando recursos de infraestructura.

Resiliencia y Tolerancia a Fallos: El fallo de un microservicio no compromete servicios críticos. Los patrones Circuit Breaker y Retry garantizan continuidad operativa.

Agilidad en el Desarrollo: Equipos autónomos pueden desarrollar, probar y desplegar servicios de manera independiente, reduciendo tiempos de entrega.

Mantenibilidad y Evolución Tecnológica: Cada servicio puede evolucionar tecnológicamente sin afectar al ecosistema completo.

Trazabilidad y Observabilidad: Arquitectura distribuida permite implementar logging centralizado, distributed tracing y métricas granulares.

2.2 Arquitectura de Referencia

La solución se estructura en tres capas principales:

Capa de Exposición (API Management Layer): API Manager como punto único de entrada con gestión centralizada de seguridad, throttling y versionado.

Capa de Representación (Microservices Layer): Microservicios de negocio con lógica específica de dominio y responsabilidad única.

Capa de Integración (Integration Layer): Event Streaming para comunicación asíncrona y conectores a sistemas legados.

2.3 Códigos de Respuesta HTTP Estándar

Todos los microservicios implementan un conjunto estandarizado de códigos de respuesta HTTP para garantizar consistencia:

Código	Descripción
200	OK - Operación completada exitosamente
201	Created - Recurso creado exitosamente

400	Bad Request - Parámetros inválidos o datos incompletos
401	Unauthorized - Token JWT inválido, expirado o ausente
403	Forbidden - Sin permisos suficientes para ejecutar la operación
404	Not Found - Recurso no encontrado en el sistema
408	Request Timeout - Tiempo de espera agotado al conectar
409	Conflict - Conflicto con el estado actual del recurso
422	Unprocessable Entity - Datos válidos, pero no procesables por reglas de negocio
429	Too Many Requests - Límite de rate limit excedido
500	Internal Server Error - Error interno del servicio (información generalizada al exterior, detalle en logs)
502	Bad Gateway - Servicio externo no disponible o respuesta inválida
503	Service Unavailable - Servicio temporalmente no disponible o Circuit Breaker abierto
504	Gateway Timeout - Servicio externo no respondió en tiempo esperado

3 CATÁLOGO DE MICROSERVICIOS

3.1 Microservicio MsAdaptadorPKI

El **Microservicio Adaptador PKI** es un componente de tipo **Adaptador** dentro de la plataforma SIIRC. Su propósito principal es actuar como una fachada o puente entre los microservicios internos que requieren servicios de certificados digitales y el **Servicio Externo de PKI** de RENIEC (ECEP - Entidad de Certificación para el Estado Peruano).

Este diseño es fundamental para abstraer a los microservicios de dominio de cualquier cambio futuro, actualización de protocolos, o migración del servicio PKI subyacente.

Funciones Principales

- **Traducción de Protocolos**: Convierte las solicitudes de certificación estandarizadas del SIIRC a los formatos y protocolos específicos requeridos por el servicio PKI externo de RENIEC.
- **Obtención de Certificados Digitales**: Proporciona la función para solicitar, generar y obtener los certificados digitales necesarios para los DNIe (Firma Digital, Autenticación y Cifrado).
- **Generación de Identificadores**: Genera números de solicitud únicos para el seguimiento y trazabilidad de las operaciones con el PKI.
- **Aislamiento de Cambios**: En caso de que el proveedor o la tecnología de PKI cambien, solo este microservicio necesita ser modificado, protegiendo al resto de la arquitectura.

3.1.1 .Endpoint: Generar Certificado Digital DNIe

Endpoint principal que solicita al servicio PKI externo de RENIEC la generación de certificados digitales para un ciudadano. Ejecuta el proceso completo de generación de par de claves asimétricas (RSA 2048 bits) y emisión de certificados digitales X.509 para la inyección en el DNIe.

Atributo	Valor
Path	/api/v1/adaptador/MsAdaptadorPKI/generarCertificadoDigitalDniE
API Gateway	Interno
Método HTTP	POST

Protocolo	REST/HTTP
Headers	Authorization String - Bearer token JWT para autenticación del sistema Content-Type String - "application/json" X-Correlation-ID UUID - Identificador único de correlación para trazabilidad distribuida X-Request-ID UUID - Identificador único de la solicitud X-Office-Code String - Código de oficina donde se realiza la operación X-PKI-Transaction-ID String - Identificador de transacción PKI para seguimiento

Entrada	{
	"solicitudPkiId": "string",
	"numeroDocumento": "string",
	"tipoDocumento": "string",
	"ciudadano": {
	"nombres": "string",
	"apellidoPaterno": "string",
	"apellidoMaterno": "string",
	"nombreCompleto": "string",
	"fechaNacimiento": "YYYY-MM-DD",
	"sexo": "string",
	"correoElectronico": "string"
	},
	"configuracionCertificado": {
	"tipoCertificado": "string",
	"algoritmo": "string",
	"longitudClave": "integer",
	"vigenciaAnios": "integer",
	"usosClave": ["string"],
	"usosExtendidos": ["string"]
	},
	"datosSubject": {
	"commonName": "string",
	"serialNumber": "string",
	"country": "string",
	"organization": "string",
	"organizationalUnit": "string"
	},
	"metadatos": {
	"codigoSolicitudTramite": "string",
	"numeroTramite": "string",
	"oficinaOrigen": "string",
	"usuarioRegistrador": "string",
	"ipOrigen": "string",
	"timestampSolicitud": "YYYY-MM-DDThh:mm:ssZ"
	}
	}

Respuesta	{
	"success": true,
	"statusCode": "integer",
	"message": "string",
	"data": {
	"solicitudPkiId": "string",
	"certificado": {
	"certificadoId": "string",
	"numeroSerie": "string",
	"tipoCertificado": "string",
	"fechaEmision": "YYYY-MM-DDThh:mm:ssZ",
	"fechaVencimiento": "YYYY-MM-DDThh:mm:ssZ",
	"vigenciaAnios": 4,
	"estadoCertificado": "string",
	"subjectDN": "string",
	"issuerDN": "string",
	"algoritmoFirma": "string",
	"longitudClave": 2048,

	"huellaCertificado": "string",
	"certificadoBase64": "string",
	"clavePublicaBase64": "string"
	},
	"procesoGeneracion": {
	"estadoGeneracionClaves": "string",
	"estadoEmisionCertificado": "string",
	"fechaInicioGeneracion": "YYYY-MM-DDThh:mm:ssZ",
	"fechaFinGeneracion": "YYYY-MM-DDThh:mm:ssZ",
	"tiempoProcesamientoMs": 0,
	"intentosRealizados": 1
	},
	"pkiExterno": {
	"transaccionPkiId": "string",
	"codigoRespuestaPki": "string",
	"mensajeRespuestaPki": "string"
	}
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"version": "1.0.0",
	"tiempoRespuesta": "string"
	}
	}

Error Response	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": "integer",
	"errores": [
	{
	"codigo": "string"
	"campo": "string"
	"detalleError": "string"
	}
	]
	}

3.1.1.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud Mínima	Longitud Máxima
Solicitud PKI ID	solicitudPkiId	String	Sí	10	30
Número Documento	numeroDocumento	String	Sí	8	12
Tipo Documento	tipoDocumento	String (Enum)	Sí	2	3
ciudadano	nombres	String	Sí	1	100
ciudadano	apellidoPaterno	String	Sí	1	50
ciudadano	apellidoMaterno	String	No	1	50
ciudadano	nombreCompleto	String	Sí	3	200
ciudadano	fechaNacimiento	String (Date)	Sí	10	10

ciudadano	sexo	String (Enum)	Sí	1	1
ciudadano	correoElectronico	String (Email)	No	5	100
configuracionCertificado	tipoCertificado	String (Enum)	Sí	5	20
configuracionCertificado	algoritmo	String	Sí	3	10
configuracionCertificado	longitudClave	Integer	Sí	-	-
configuracionCertificado	vigenciaAnios	Integer	Sí	1	4
configuracionCertificado	usosClave	Array[String]	Sí	1	5
configuracionCertificado	usosExtendidos	Array[String]	No	1	5
datosSubject	commonName	String	Sí	3	200
datosSubject	serialNumber	String	Sí	10	20
datosSubject	country	String	Sí	2	2
datosSubject	organization	String	Sí	3	100
datosSubject	organizationalUnit	String	No	3	100
metadatos	codigoSolicitudTramite	String	Sí	1	30
metadatos	numeroTramite	String	Sí	1	30
metadatos	oficinaOrigen	String	Sí	1	50
metadatos	usuarioRegistrador	String	Sí	1	30
metadatos	ipOrigen	String (IPv4/IPv6)	No	7	45
metadatos	timestampSolicitud	String (DateTime)	Sí	20	30

3.1.1.2 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa
statusCode	Integer	Sí	Código HTTP de respuesta
message	String	Sí	Mensaje descriptivo del resultado
data.solicitudPkiId	String	Sí	ID de la solicitud PKI procesada
data.certificado.certificadoId	String	Sí	Identificador único del certificado emitido

data.certificado.numeroSerie	String	Sí	Número de serie del certificado (hexadecimal)
data.certificado.tipoCertificado	String	Sí	Tipo de certificado emitido
data.certificado.fechaEmision	String (DateTime)	Sí	Fecha y hora de emisión del certificado
data.certificado.fechaVencimiento	String (DateTime)	Sí	Fecha y hora de vencimiento (4 años)
data.certificado.vigenciaAnios	Integer	Sí	Años de vigencia del certificado
data.certificado.estadoCertificado	String	Sí	Estado: ACTIVO, REVOCADO, SUSPENDIDO, PENDIENTE
data.certificado.subjectDN	String	Sí	Distinguished Name del titular
data.certificado.issuerDN	String	Sí	Distinguished Name del emisor (RENIEC CA)
data.certificado.algoritmoFirma	String	Sí	Algoritmo de firma utilizado (SHA256withRSA)
data.certificado.longitudClave	Integer	Sí	Longitud de la clave en bits (2048)
data.certificado.huellaCertificado	String	Sí	Fingerprint SHA-256 del certificado
data.certificado.certificadoBase64	String	Sí	Certificado X.509 codificado en Base64
data.certificado.clavePublicaBase64	String	Sí	Clave pública codificada en Base64
data.procesoGeneracion.estadoGeneracionClaves	String	Sí	Estado de generación de claves
data.procesoGeneracion.estadoEmisionCertificado	String	Sí	Estado de emisión del certificado
data.procesoGeneracion.fechaInicioGeneracion	String (DateTime)	Sí	Inicio del proceso de generación
data.procesoGeneracion.fechaFinGeneracion	String (DateTime)	Sí	Fin del proceso de generación

data.procesoGeneracion.tiempoProcesamientoMs	Integer	Sí	Tiempo de procesamiento en milisegundos
data.procesoGeneracion.intentosRealizados	Integer	Sí	Número de intentos realizados
data.pkiExterno.transaccionPkiId	String	Sí	ID de transacción del PKI externo
data.pkiExterno.codigoRespuestaPki	String	Sí	Código de respuesta del PKI
data.pkiExterno.mensajeRespuestaPki	String	No	Mensaje del PKI externo
metadata.timestamp	String (DateTime)	Sí	Timestamp del procesamiento
metadata.correlationId	String (UUID)	Sí	ID de correlación para trazabilidad
metadata.version	String	Sí	Versión del API
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta
error	Object	No	Objeto de error si la operación falló
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título descriptivo del error
error.estado	Integer	No	Código de estado HTTP del error
error.errores[]	Array	No	Lista detallada de errores
error.errores[].codigo	String	No	Código interno del error
error.errores[].campo	String	No	Campo que generó el error
error.errores[].detalleError	String	No	Descripción específica del error

3.1.1.3 Valores para el Atributo statusCode

Código	Respuesta	Descripción
201	Created	Certificado digital generado exitosamente
400	Bad Request	Parámetros de entrada inválidos o incompletos
401	Unauthorized	Token JWT inválido, expirado o ausente
403	Forbidden	Sin permisos para generar certificados

404	Not Found	Ciudadano no encontrado en el APD
409	Conflict	Ya existe un certificado activo para este ciudadano y tipo
422	Unprocessable Entity	Ciudadano no cumple requisitos para certificado digital
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno del microservicio
502	Bad Gateway	Error de comunicación con servicio PKI externo de RENIEC
503	Service Unavailable	Servicio PKI externo temporalmente no disponible
504	Gateway Timeout	Timeout en comunicación con servicio PKI (> 30 segundos)

3.1.2 Endpoint: Generar Números de Solicitud

Endpoint que genera números de solicitud únicos para identificar y dar seguimiento a las transacciones de certificados digitales. Esta es la versión 2 del servicio con mejoras en el formato y soporte para múltiples tipos de solicitud.

Atributo	Valor
Path	/api/v1/adaptador/MsAdaptadorPKI/generarNumerosSolicitud2
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String - Bearer token JWT para autenticación Content-Type String - "application/json" X-Correlation-ID UUID - Identificador único de correlación X-Office-Code String - Código de oficina origen

Entrada	{
	"tipoSolicitud": "string",
	"cantidad": 1,
	"prefijoPersonalizado": "string",
	"metadatos": {
	"oficinaOrigen": "string",
	"usuarioSolicitante": "string",
	"sistemaOrigen": "string",
	"timestampSolicitud": "YYYY-MM-DDThh:mm:ssZ"
	}
	}

Respuesta	{
	"success": true,
	"statusCode": 201,
	"message": "string",
	"data": {
	"numerosSolicitud": [
	{
	"solicitudPkiId": "string",
	"secuencia": 0,
	"anio": 2025,
	"tipoSolicitud": "string",
	"fechaGeneracion": "YYYY-MM-DDThh:mm:ssZ",
	"estado": "string",
	"vigenciaHoras": 24
	}
	],
	"totalGenerados": 1,

	"rangoSecuencias": {
	"inicio": 0,
	"fin": 0
	}
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"version": "2.0.0",
	"tiempoRespuesta": "string"
	}
	}

Error Response	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": "integer",
	"errores": [
	{
	"codigo": "string"
	"campo": "string"
	"detalleError": "string"
	}
	]
	}

3.1.2.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Long. Mín.	Long. Máx.
Tipo Solicitud	tipoSolicitud	String (Enum)	Sí	3	20
Cantidad	cantidad	Integer	No	1	100
Prefijo Personalizado	prefijoPersonalizado	String	No	2	10
metadatos	oficinaOrigen	String	Sí	1	50
metadatos	usuarioSolicitante	String	Sí	1	30
metadatos	sistemaOrigen	String	Sí	3	50
metadatos	timestampSolicitud	String (DateTime)	Sí	20	30

3.1.2.1 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa
statusCode	Integer	Sí	Código HTTP de respuesta
message	String	Sí	Mensaje descriptivo del resultado
data.numerosSolicitud[]	Array	Sí	Lista de números de solicitud generados

data.numerosSolicitud[].solicitudPkiId	String	Sí	ID único de solicitud (formato: PKI-[TIPO]-[AÑO]-[SECUENCIA])
data.numerosSolicitud[].secuencia	Integer	Sí	Número de secuencia correlativo
data.numerosSolicitud[].anio	Integer	Sí	Año de generación
data.numerosSolicitud[].tipoSolicitud	String	Sí	Tipo de solicitud asociada
data.numerosSolicitud[].fechaGeneracion	String (DateTime)	Sí	Fecha y hora de generación
data.numerosSolicitud[].estado	String	Sí	Estado: RESERVADO, UTILIZADO, EXPIRADO
data.numerosSolicitud[].vigenciaHoras	Integer	Sí	Horas de vigencia del número reservado
data.totalGenerados	Integer	Sí	Total de números generados
data.rangoSecuencias.inicio	Integer	Sí	Secuencia inicial del rango
data.rangoSecuencias.fin	Integer	Sí	Secuencia final del rango
metadata.timestamp	String (DateTime)	Sí	Timestamp del procesamiento
metadata.correlationId	String (UUID)	Sí	ID de correlación
metadata.version	String	Sí	Versión del API (2.0.0)
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta
error	Object	No	Objeto de error si la operación falló
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título descriptivo del error
error.estado	Integer	No	Código de estado HTTP del error
error.errores[]	Array	No	Lista detallada de errores
error.errores[].codigo	String	No	Código interno del error
error.errores[].campo	String	No	Campo que generó el error
error.errores[].detalleError	String	No	Descripción específica del error

3.1.2.3 Valores para el atributo statusCode

Código	Respuesta	Descripción
201	Created	Números de solicitud generados exitosamente
400	Bad Request	Parámetros de entrada inválidos
401	Unauthorized	Token JWT inválido, expirado o ausente
403	Forbidden	Sin permisos para generar números de solicitud

422	Unprocessable Entity	Cantidad solicitada excede el límite permitido
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno al generar secuencias
503	Service Unavailable	Servicio de secuencias temporalmente no disponible

3.1.3 Endpoint: Generar Números de Solicitud Batch

Endpoint optimizado para generación masiva de números de solicitud, diseñado para procesos batch de emisión de certificados en oficinas de alto volumen.

Atributo	Valor
Path	/api/v1/adaptador/MsAdaptadorPKI/generarNumerosSolicitudBatch
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String - Bearer token JWT para autenticación Content-Type String - "application/json" X-Correlation-ID UUID - Identificador único de correlación X-Office-Code String - Código de oficina origen X-Batch-ID UUID - Identificador del proceso batch
Entrada	{ "tipoSolicitud": "string", "cantidadSolicitada": 500, "configuracionBatch": { "prefijoLote": "string", "vigenciaHoras": 48, "reservarSecuencias": true }, "metadatos": { "oficinaOrigen": "string", "usuarioSolicitante": "string", "sistemaOrigen": "string", "procesoOrigen": "string", "timestampSolicitud": "YYYY-MM-DDThh:mm:ssZ" } }
Respuesta	{ "success": true, "statusCode": 201, "message": "string", "data": { "batchId": "string", "rangoAsignado": { "secuenciaInicio": 0, "secuenciaFin": 0, "prefijoCompleto": "string", "formatoNumero": "string" }, "cantidadGenerada": 500, "vigenciaReserva": { "fechaInicio": "YYYY-MM-DDThh:mm:ssZ", "fechaExpiracion": "YYYY-MM-DDThh:mm:ssZ", "horasVigencia": 48 }, "estadoBatch": "string"

	<pre>},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"version": "1.0.0",
	"tiempoRespuesta": "string"
	},
	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": 0,
	"errores": [
	{
	"detalleError": "string"
	}
	]
	}
	}</pre>

Error Response	<pre>"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": "integer",
	"errores": [
	{
	"codigo": "string"
	"campo": "string"
	"detalleError": "string"
	}
	]
	}</pre>

3.1.3.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Long. Mín.	Long. Máx.
Tipo Solicitud	tipoSolicitud	String (Enum)	Sí	3	20
Cantidad Solicitada	cantidadSolicitada	Integer	Sí	100	10000
configuracionBatch	prefijoLote	String	No	2	10
configuracionBatch	vigenciaHoras	Integer	No	1	168
configuracionBatch	reservarSecuencias	Boolean	Sí	-	-
metadatos	oficinaOrigen	String	Sí	1	50
metadatos	usuarioSolicitante	String	Sí	1	30
metadatos	sistemaOrigen	String	Sí	3	50
metadatos	procesoOrigen	String	No	3	100
metadatos	timestampSolicitud	String (DateTime)	Sí	20	30

3.1.3.2 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa

statusCode	Integer	Sí	Código HTTP de respuesta
message	String	Sí	Mensaje descriptivo del resultado
data.batchId	String (UUID)	Sí	Identificador único del lote generado
data.rangoAsignado.secuencialnicio	Integer	Sí	Primera secuencia del rango
data.rangoAsignado.secuenciaFin	Integer	Sí	Última secuencia del rango
data.rangoAsignado.prefijoCompleto	String	Sí	Prefijo completo para formar números
data.rangoAsignado.formatoNumero	String	Sí	Formato ejemplo del número generado
data.cantidadGenerada	Integer	Sí	Total de números reservados
data.vigenciaReserva.fechalnicio	String (DateTime)	Sí	Inicio de la reserva
data.vigenciaReserva.fechaExpiracion	String (DateTime)	Sí	Expiración de la reserva
data.vigenciaReserva.horasVigencia	Integer	Sí	Horas de vigencia
data.estadoBatch	String	Sí	Estado
metadata.timestamp	String (DateTime)	Sí	Timestamp del procesamiento
metadata.correlationId	String (UUID)	Sí	ID de correlación
metadata.version	String	Sí	Versión del API
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta
error	Object	No	Objeto de error si la operación falló
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título descriptivo del error
error.estado	Integer	No	Código de estado HTTP del error
error.errores[]	Array	No	Lista detallada de errores
error.errores[].codigo	String	No	Código interno del error
error.errores[].campo	String	No	Campo que generó el error
error.errores[].detalleError	String	No	Descripción específica del error

3.1.3.3 Valores para el atributo statusCode

Código	Respuesta	Descripción
201	Created	Rango de números batch generado exitosamente
400	Bad Request	Parámetros de entrada inválidos

401	Unauthorized	Token JWT inválido, expirado o ausente
403	Forbidden	Sin permisos para generación batch
422	Unprocessable Entity	Cantidad excede límite (máx 10,000)
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno al generar rango batch
503	Service Unavailable	Servicio temporalmente no disponible

3.1.4 Endpoint: Consultar Estado de Certificado

Endpoint que permite consultar el estado actual de un certificado digital emitido, incluyendo su vigencia, estado de revocación y metadatos asociados.

Atributo	Valor
Path	/api/v1/adaptador/MsAdaptadorPKI/consultarEstadoCertificado
API Gateway	Interno
Método HTTP	GET
Protocolo	REST/HTTP
Headers	Authorization String - Bearer token JWT para autenticación X-Correlation-ID UUID - Identificador único de correlación X-Request-Reason String - Motivo de la consulta (obligatorio para auditoría)

Entrada	{
	"numeroSerie":"string",
	"incluirCertificado":"boolean",
	"verificarOCSP":"boolean"
	}

Respuesta	{
	"success": true,
	"statusCode": 200,
	"message": "string",
	"data": {
	"certificado": {
	"numeroSerie": "string",
	"certificadoId": "string",
	"tipoCertificado": "string",
	"estadoCertificado": "string",
	"fechaEmision": "YYYY-MM-DDThh:mm:ssZ",
	"fechaVencimiento": "YYYY-MM-DDThh:mm:ssZ",
	"diasRestantesVigencia": 0,
	"subjectDN": "string",
	"issuerDN": "string",
	"algoritmoFirma": "string",
	"longitudClave": 2048,
	"huellaCertificado": "string",
	"certificadoBase64": "string"
	},
	"titular": {
	"numeroDocumento": "string",
	"nombreCompleto": "string"
	},
	"validacionOCSP": {
	"estadoOCSP": "string",
	"fechaConsultaOCSP": "YYYY-MM-DDThh:mm:ssZ",
	"respuestaOCSP": "string"

	},
	"revocacion": {
	"estaRevocado": false,
	"fechaRevocacion": "YYYY-MM-DDThh:mm:ssZ",
	"motivoRevocacion": "string",
	"codigoMotivo": "string"
	}
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"version": "1.0.0",
	"tiempoRespuesta": "string"
	}
	}

Error Response	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": "integer",
	"errores": [
	{
	"codigo": "string"
	"campo": "string"
	"detalleError": "string"
	}
	]
	}

Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Long. Mín.	Long. Máx.
Número de Serie	numeroSerie	String	Sí	1	100
Incluir Certificado	incluirCertificado	Boolean	Sí	-	-
Verificar OCSP	verificarOCSP	Boolean	Sí	-	-

3.1.4.1 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa
statusCode	Integer	Sí	Código HTTP de respuesta
message	String	Sí	Mensaje descriptivo del resultado
data.certificado.numeroSerie	String	Sí	Número de serie del certificado
data.certificado.certificadoId	String	Sí	Identificador interno del certificado
data.certificado.tipoCertificado	String	Sí	Tipo: FIRMA_DIGITAL, AUTENTICACION, CIFRADO
data.certificado.estadoCertificado	String	Sí	Estado: ACTIVO, REVOCADO, SUSPENDIDO, VENCIDO

data.certificado.fechaEmision	String (DateTime)	Sí	Fecha de emisión
data.certificado.fechaVencimiento	String (DateTime)	Sí	Fecha de vencimiento
data.certificado.diasRestantesVigencia	Integer	Sí	Días restantes de vigencia
data.certificado.subjectDN	String	Sí	Distinguished Name del titular
data.certificado.issuerDN	String	Sí	Distinguished Name del emisor
data.certificado.algoritmoFirma	String	Sí	Algoritmo de firma
data.certificado.longitudClave	Integer	Sí	Longitud de clave en bits
data.certificado.huellaCertificado	String	Sí	Fingerprint SHA-256
data.certificado.certificadoBase64	String	No	Certificado en Base64 (si se solicitó)
data.titular.numeroDocumento	String	Sí	DNI del titular
data.titular.nombreCompleto	String	Sí	Nombre completo del titular
data.validacionOCSP.estadoOCSP	String	No	Estado OCSP: GOOD, REVOKED, UNKNOWN
data.validacionOCSP.fechaConsultaOCSP	String (DateTime)	No	Fecha de consulta OCSP
data.validacionOCSP.respuestaOCSP	String	No	Respuesta raw del OCSP
data.revocacion.estaRevocado	Boolean	Sí	Indica si está revocado
data.revocacion.fechaRevocacion	String (DateTime)	No	Fecha de revocación
data.revocacion.motivoRevocacion	String	No	Descripción del motivo
data.revocacion.codigoMotivo	String	No	Código CRL del motivo
metadata.timestamp	String (DateTime)	Sí	Timestamp del procesamiento
metadata.correlationId	String (UUID)	Sí	ID de correlación
metadata.version	String	Sí	Versión del API
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta
error	Object	No	Objeto de error si la operación falló
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título descriptivo del error
error.estado	Integer	No	Código de estado HTTP del error
error.errores[]	Array	No	Lista detallada de errores
error.errores[].codigo	String	No	Código interno del error

error.errores[].campo	String	No	Campo que generó el error
error.errores[].detalleError	String	No	Descripción específica del error

3.1.4.1 Valores para el atributo statusCode

Código	Respuesta	Descripción
200	OK	Estado del certificado consultado exitosamente
400	Bad Request	Número de serie con formato inválido
401	Unauthorized	Token JWT inválido, expirado o ausente
403	Forbidden	Sin permisos para consultar certificados
404	Not Found	Certificado no encontrado
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno del microservicio
502	Bad Gateway	Error de comunicación con servicio OCSP
503	Service Unavailable	Servicio PKI temporalmente no disponible

3.1.5 Endpoint: Revocar Certificado Digital

Endpoint que permite solicitar la revocación de un certificado digital activo. Esta operación es irreversible y debe utilizarse en casos de compromiso de clave privada, pérdida del DNIe, o solicitud expresa del titular.

Atributo	Valor
Path	/api/v1/adaptador/MsAdaptadorPKI/revocarCertificado
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String - Bearer token JWT para autenticación Content-Type String - "application/json" X-Correlation-ID UUID - Identificador único de correlación X-Request-Reason String - Motivo de la revocación (obligatorio) X-Supervisor-Approval String - ID de aprobación del supervisor (requerido)
Entrada	{ "certificado": { "numeroSerie": "string", "certificadoId": "string" }, "revocacion": { "motivoRevocacion": "string", "codigoMotivo": "string", "descripcionAdicional": "string", "fechaEfectiva": "YYYY-MM-DDThh:mm:ssZ" }, "solicitante": { "tipoSolicitante": "string", "numeroDocumento": "string", "nombreCompleto": "string", "relacion": "string"

	<pre>},
	"autorizacion": {
	"supervisorId": "string",
	"codigoAutorizacion": "string",
	"fechaAutorizacion": "YYYY-MM-DDThh:mm:ssZ"
	},
	"metadatos": {
	"oficinaOrigen": "string",
	"usuarioRegistrador": "string",
	"ipOrigen": "string",
	"timestampSolicitud": "YYYY-MM-DDThh:mm:ssZ"
	}
	}</pre>

Respuesta	<pre>{
	"success": true,
	"statusCode": 200,
	"message": "string",
	"data": {
	"revocacionId": "string",
	"certificado": {
	"numeroSerie": "string",
	"estadoAnterior": "string",
	"estadoActual": "string"
	},
	"revocacion": {
	"fechaRevocacion": "YYYY-MM-DDThh:mm:ssZ",
	"motivoRevocacion": "string",
	"codigoMotivo": "string",
	"incluidoEnCRL": true,
	"fechaPublicacionCRL": "YYYY-MM-DDThh:mm:ssZ"
	},
	"pkiExterno": {
	"transaccionPkiId": "string",
	"codigoRespuestaPki": "string",
	"mensajeRespuestaPki": "string"
	}
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"version": "1.0.0",
	"tiempoRespuesta": "string"
	}
	}</pre>

Error Response	<pre>"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": 0,
	"errores": [
	{
	"detalleError": "string"
	}
	]
	}</pre>

3.1.5.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Long. Mín.	Long. Máx.
certificado	numeroSerie	String	Sí	8	40
certificado	certificadoId	String	No	10	50

revocacion	motivoRevocacion	String (Enum)	Sí	5	30
revocacion	codigoMotivo	String	Sí	1	2
revocacion	descripcionAdicional	String	No	10	500
revocacion	fechaEfectiva	String (DateTime)	No	20	30
solicitante	tipoSolicitante	String (Enum)	Sí	5	20
solicitante	numeroDocumento	String	Sí	8	12
solicitante	nombreCompleto	String	Sí	3	200
solicitante	relacion	String	No	3	50
autorizacion	supervisorId	String	Sí	5	30
autorizacion	codigoAutorizacion	String	Sí	10	50
autorizacion	fechaAutorizacion	String (DateTime)	Sí	20	30
metadatos	oficinaOrigen	String	Sí	1	50
metadatos	usuarioRegistrador	String	Sí	1	30
metadatos	ipOrigen	String (IPv4/IPv6)	No	7	45
metadatos	timestampSolicitud	String (DateTime)	Sí	20	30

3.1.5.2 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa
statusCode	Integer	Sí	Código HTTP de respuesta
message	String	Sí	Mensaje descriptivo del resultado
data.revocacionId	String	Sí	ID único de la revocación
data.certificado.numeroSerie	String	Sí	Número de serie del certificado revocado
data.certificado.estadoAnterior	String	Sí	Estado antes de la revocación
data.certificado.estadoActual	String	Sí	Estado actual (REVOCADO)
data.revocacion.fechaRevocacion	String (DateTime)	Sí	Fecha efectiva de revocación
data.revocacion.motivoRevocacion	String	Sí	Motivo de la revocación
data.revocacion.codigoMotivo	String	Sí	Código RFC 5280
data.revocacion.incluidoEnCRL	Boolean	Sí	Si se incluyó en la CRL
data.revocacion.fechaPublicacionCRL	String (DateTime)	No	Fecha de publicación en CRL
data.pkiExterno.transaccionPkiId	String	Sí	ID de transacción del PKI externo
data.pkiExterno.codigoRespuestaPki	String	Sí	Código de respuesta del PKI
data.pkiExterno.mensajeRespuestaPki	String	No	Mensaje del PKI externo

metadata.timestamp	String (DateTime)	Sí	Timestamp del procesamiento
metadata.correlationId	String (UUID)	Sí	ID de correlación
metadata.version	String	Sí	Versión del API
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta
error	Object	No	Objeto de error si la operación falló
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título descriptivo del error
error.estado	Integer	No	Código de estado HTTP del error
error.errores[]	Array	No	Lista detallada de errores
error.errores[].codigo	String	No	Código interno del error
error.errores[].campo	String	No	Campo que generó el error
error.errores[].detalleError	String	No	Descripción específica del error

3.1.5.3 Valores para el atributo statusCode

Código	Respuesta	Descripción
200	OK	Certificado revocado exitosamente
400	Bad Request	Parámetros de entrada inválidos
401	Unauthorized	Token JWT inválido, expirado o ausente
403	Forbidden	Sin permisos para revocar certificados
404	Not Found	Certificado no encontrado
409	Conflict	Certificado ya se encuentra revocado
422	Unprocessable Entity	Autorización de supervisor inválida
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno del microservicio
502	Bad Gateway	Error de comunicación con servicio PKI
503	Service Unavailable	Servicio PKI temporalmente no disponible