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	24/11/2025	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.

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

3.1.1 Endpoint: generarCertificadoDigitalDniE

Endpoint que invoca al método generarCertificadoDigitalDniE del servicio PKI externo de RENIEC (certificadosdnie2 o certificadosdnie3) para solicitar la generación de **2 o 3 certificados digitales** para un ciudadano.

Atributo	Valor
Path	/api/v1/certificadosDigitales/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	{
	"numeroCertificados": "integer",
	"certificadoAutenticacion": {
	"caName": "string",

	"certificateProfileName": "string",
	"clearPwd": "boolean",
	"email": "string",
	"endEntityProfileName": "string",
	"keyRecoverable": "boolean",
	"password": "string",
	"sendNotification": "boolean",
	"status": "integer",
	"subjectDN": "string",
	"tokenType": "string",
	"username": "string",
	"nuSolicitud": "string",
	"pkcs10Str": "string"
	},
	"certificadoFirma": {
	"caName": "string",
	"certificateProfileName": "string",
	"clearPwd": "boolean",
	"email": "string",
	"endEntityProfileName": "string",
	"keyRecoverable": "boolean",
	"password": "string",
	"sendNotification": "boolean",
	"status": "integer",
	"subjectDN": "string",
	"tokenType": "string",
	"username": "string",
	"nuSolicitud": "string",
	"pkcs10Str": "string"
	},
	"certificadoCifrado": {
	"caName": "string",
	"certificateProfileName": "string",
	"clearPwd": "boolean",
	"email": "string",
	"endEntityProfileName": "string",
	"keyRecoverable": "boolean",
	"password": "string",
	"sendNotification": "boolean",
	"status": "integer",
	"subjectDN": "string",
	"tokenType": "string",
	"username": "string",
	"nuSolicitud": "string",
	"pkcs10Str": "string"
	},
	"datosAdicionales": {
	"dni": "string",
	"sesionUsuario": "string"
	}
	}

Respuesta	{
	"success": true,
	"statusCode": integer,
	"message": "string",
	"data": {
	"certificados": [
	{
	"tipoCertificado": "string",
	"certificadoBase64": "string",
	"numeroSerie": "string"
	},
	{
	"tipoCertificado": "string",

	"certificadoBase64": "string",
	"numeroSerie": "string"
	},
	{
	"tipoCertificado": "string",
	"certificadoBase64": "string",
	"numeroSerie": "string"
	}
	],
	"totalCertificados": integer,
	"pkiExterno": {
	"result": "integer",
	"mensaje": "string"
	}
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"version": "string",
	"tiempoRespuesta": "string"
	}
	}

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

3.1.1.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud Mínima	Longitud Máxima
Número de Certificados	numeroCertificados	Integer	Sí	-	-
DNI	datosAdicionales.dni	String	Sí	8	8
Sesión Usuario	datosAdicionales.sesionUsuario	String	No	0	50
Nombre CA	certificadoFirma.caName	String	No	0	100
Perfil Certificado	certificadoFirma.certificateProfileName	String	No	0	100
Limpiar Password	certificadoFirma.clearPwd	Boolean	Sí	-	-
Email	certificadoFirma.email	String	Sí	5	100
Perfil Entidad Final	certificadoFirma.endEntityProfileName	String	No	0	100
Clave Recuperable	certificadoFirma.keyRecoverable	Boolean	Sí	-	-
Password	certificadoFirma.password	String	Sí	0	20

Enviar Notificación	certificadoFirma.sendNotification	Boolean	Sí	-	-
Estado	certificadoFirma.status	Integer	Sí	-	-
Subject DN	certificadoFirma.subjectDN	String	Sí	50	500
Tipo Token	certificadoFirma.tokenType	String	Sí	10	20
Username	certificadoFirma.username	String	Sí	10	50
Número Solicitud	certificadoFirma.nuSolicitud	String	Sí	5	20
CSR	certificadoFirma.pkcs10Str	String	Sí	100	10000
Nombre CA	certificadoCifrado.caName	String	No	0	100
Perfil Certificado	certificadoCifrado.certificateProfileName	String	No	0	100
Limpiar Password	certificadoCifrado.clearPwd	Boolean	Sí	-	-
Email	certificadoCifrado.email	String	Sí	5	100
Perfil Entidad Final	certificadoCifrado.endEntityProfileName	String	No	0	100
Clave Recuperable	certificadoCifrado.keyRecoverable	Boolean	Sí	-	-
Password	certificadoCifrado.password	String	Sí	0	20
Enviar Notificación	certificadoCifrado.sendNotification	Boolean	Sí	-	-
Estado	certificadoCifrado.status	Integer	Sí	-	-
Subject DN	certificadoCifrado.subjectDN	String	Sí	50	500
Tipo Token	certificadoCifrado.tokenType	String	Sí	10	20
Username	certificadoCifrado.username	String	Sí	10	50
Número Solicitud	certificadoCifrado.nuSolicitud	String	Sí	5	20
CSR	certificadoCifrado.pkcs10Str	String	Sí	100	10000

3.1.1.2 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa.
statusCode	Integer	Sí	Código de estado asociado a la respuesta del servicio.
message	String	Sí	Mensaje informativo sobre el resultado de la operación.
data	Object	Sí	Contenedor principal de los datos resultantes.

data.certificados	Array	Sí	Lista de certificados generados o recuperados.
data.certificados[].tipoCertificado	String	Sí	Tipo del certificado emitido.
data.certificados[].certificadoBase64	String	Sí	Certificado codificado en Base64.
data.certificados[].numeroSerie	String	Sí	Número de serie único del certificado.
data.totalCertificados	Integer	Sí	Cantidad total de certificados incluidos en la respuesta.
data.pkiExterno	Object	Sí	Información del proceso realizado con el PKI externo.
data.pkiExterno.result	String	Sí	Resultado de la operación en el sistema PKI externo.
data.pkiExterno.mensaje	String	Sí	Mensaje descriptivo del sistema PKI externo.
metadata	Object	Sí	Información adicional para trazabilidad.
metadata.timestamp	String (ISO 8601)	Sí	Fecha y hora exacta en que se generó la respuesta.
metadata.correlationId	String	Sí	Identificador único para seguimiento de la transacción.
metadata.version	String	Sí	Versión del servicio que generó la respuesta.
metadata.tiempoRespuesta	String	Sí	Tiempo total de procesamiento del servicio.
error	Object	No	Objeto que especifica algún error existente
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título del error
error.estado	Integer	No	Código del estado de error
error.errores	Array	No	Listado de errores
error.errores[].detalleError	String	No	Detalle del error generado

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)

3.1.2Endpoint: Generar Números de Solicitud v2

Endpoint que invoca al método generarNumerosSolicitud2 del servicio PKI externo de RENIEC (certificadosdnie2 o certificadosdnie3) para generar 3 números de solicitud únicos correspondientes a los tres tipos de certificados digitales: AUT (Autenticación), FIR (Firma) y CIF (Cifrado).

Atributo	Valor
Path	/api/v1/certificadosDigitales/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	{
	"agenciaErep": "string",
	"apellidos": "string",
	"celular": "string",
	"comprobante": "string",
	"departamento": "string",
	"direccion": "string",
	"distrito": "string",
	"dni": "string",
	"email": "string",
	"ficha": "string",
	"nombres": "string",
	"nombreOperador": "string",
	"provincia": "string",
	"telefono": "string",
	"tipo": "string"
	}

Respuesta	{
	"success": true,
	"statusCode": integer,
	"message": "string",
	"data": {
	"idSolicitudAut": "string",
	"idSolicitudFir": "string",
	"idSolicitudCif": "string",
	"result": "string"
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"version": "string",
	"tiempoRespuesta": "string"
	}
	}

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

3.1.2.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud Mínima	Longitud Máxima
Agencia EREP	agenciaErep	String	Sí	1	100
Apellidos	apellidos	String	Sí	2	100
Celular	celular	String	No	9	15
Comprobante	comprobante	String	Sí	10	200
Departamento	departamento	String	Sí	3	50
Dirección	direccion	String	Sí	5	200
Distrito	distrito	String	Sí	3	50
DNI	dni	String	Sí	8	8
Email	email	String	Sí	5	100
Ficha	ficha	String	Sí	5	20
Nombres	nombres	String	Sí	2	100
Nombre Operador	nombreOperador	String	Sí	5	100
Provincia	provincia	String	Sí	3	50
Teléfono	telefono	String	No	6	15
Tipo	tipo	String	Sí	1	1

3.1.2.2 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.idSolicitudAut	String	Sí	Número de solicitud para certificado de tipo autenticación
data.idSolicitudFir	String	Sí	Número de solicitud para certificado de tipo firma
data.idSolicitudCif	String	Sí	Número de solicitud para certificado de tipo cifrado
data.result	String	Sí	Código de salida

metadata.timestamp	String (Date ISO 8601)	Sí	Timestamp del procesamiento
metadata.correlationId	String	Sí	ID de correlación
metadata.version	String	Sí	Versión del API
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta
error	Object	No	Objeto que especifica algún error existente
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título del error
error.estado	Integer	No	Código del estado de error
error.errores	Array	No	Listado de errores
error.errores[].detalleError	String	No	Detalle del error generado

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 (DNI incorrecto, campos obligatorios faltantes)
401	Unauthorized	Token JWT inválido, expirado o ausente
403	Forbidden	Sin permisos para generar números de solicitud
422	Unprocessable Entity	Datos válidos pero no procesables por el servicio PKI
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno al generar secuencias
502	Bad Gateway	Error de comunicación con servicio PKI externo
503	Service Unavailable	Servicio PKI externo temporalmente no disponible
504	Gateway Timeout	Timeout en comunicación con servicio PKI (> 30 segundos)